



SECUROS

Версия 11

Руководство администратора

Руководство администратора SecurOS (AG - RU, сборка 97 от 17.08.2024).

© Copyright Intelligent Security Systems, 2024.

Intelligent Security Systems оставляет за собой право вносить изменения как в данное Руководство, так и в описываемый продукт. Изменения могут вноситься в спецификацию системы без уведомления. Содержимое Руководства не является офертой, гарантией, обещанием или условием договора, и не должно восприниматься подобным образом.

Никакая часть данной документации не может быть воспроизведена, передана, процитирована, размещена в поисковой системе, переведена на любой язык или машинный код в любой форме и любыми средствами без явного письменного согласия со стороны правообладателя. Несанкционированное копирование этой публикации может не только нарушить авторские права, но и ослабить возможность Intelligent Security Systems предоставлять точную и актуальную информацию пользователям продукта.

Содержание

1 Предисловие	13
1.1 Назначение	13
1.2 Целевая аудитория	13
1.3 Использование руководства	13
1.4 Обращение за технической поддержкой	13
1.5 Соглашение по наименованию редакций SecurOS	14
1.6 Соглашение по оформлению	14
1.7 Элементы оформления	15
2 Назначение, реализация и принципы функционирования	16
2.1 Архитектура SecurOS	16
2.1.1 Виды серверов и рабочих мест	16
2.1.1.1 Классификация по функциональному назначению	16
2.1.1.1.1 Видеосервер	16
2.1.1.1.2 Рабочее место оператора	17
2.1.1.2 Классификация по роли в управлении конфигурацией	17
2.1.1.2.1 Сервер конфигураций	17
2.1.1.2.2 Управление конфигурацией сети с помощью сервера конфигураций	17
2.1.1.2.2.1 Порядок настройки серверов при развертывании сети	18
2.1.1.2.2.2 Процедура обновления и синхронизации	18
2.1.1.2.2.3 Восстановление конфигурации из резервной копии	18
2.1.2 Программная реализация	19
2.2 Аппаратно-программная платформа	19
2.2.1 Требования к Видеосерверу	20
2.2.2 Требования к Рабочему месту оператора	21
2.2.3 Требования к Аудиоподсистеме	22
2.2.4 Требования к Подсистеме оповещения	22
2.2.5 Требования к Подсистемам СКУД/ОПС	22
2.2.6 Требования к окружению	22
2.2.6.1 Ограничения имени компьютера	22
2.3 Подсистемы SecurOS	23
3 Установка и обновление SecurOS на Windows	24
3.1 Установка, настройка и запуск Сервера конфигураций	24
3.1.1 Установка аппаратного обеспечения	24
3.1.1.1 Установка ключа Guardant	25
3.1.1.2 Установка драйвера ключа Guardant в ручном режиме	25
3.1.2 Лицензионный ключ	25
3.1.2.1 Ключ входит в состав продукта	26
3.1.2.2 Заказ ключа по электронной почте	26
3.1.3 Установка программного обеспечения	27
3.1.3.1 Использование параметров текущей учетной записи Windows для PostgreSQL	27
3.1.3.2 Использование текущих параметров БД и учетной записи администратора	28
3.1.3.3 Процедура установки программного обеспечения на Сервере конфигураций	29
3.1.4 Первоначальная настройка	37
3.1.4.1 Настройка при помощи Мастера первоначальной настройки	37
3.1.4.2 Восстановление конфигурации	43
3.1.4.3 Запуск с пустой базой данных	44
3.1.5 Запуск SecurOS на Сервере конфигураций	44

3.2 Установка, настройка и запуск Периферийных серверов	47
3.2.1 Добавление в сеть и настройка Периферийных серверов	47
3.2.2 Установка SecurOS на периферийных серверах	49
3.2.3 Запуск и настройка SecurOS на периферийных серверах	49
3.3 Установка, настройка и запуск Рабочих мест оператора	51
3.3.1 Установка SecurOS на Рабочем месте оператора	51
3.3.2 Профили Рабочих мест оператора	52
3.3.2.1 Ограничения в использовании	52
3.3.2.2 Создание Профиля Рабочего места оператора	53
3.3.3 Фиксированные Рабочие места оператора	54
3.3.3.1 Добавление в сеть и настройка фиксированных Рабочих мест оператора	54
3.3.4 Запуск SecurOS на Рабочем месте оператора	55
3.4 Порядок обновления SecurOS	57
4 Установка и обновление SecurOS на Linux	59
4.1 Установка, настройка и запуск Сервера конфигураций	59
4.1.1 Установка аппаратного обеспечения	59
4.1.1.1 Установка ключа Guardant	59
4.1.2 Лицензионный ключ	60
4.1.2.1 Заказ ключа по электронной почте	60
4.1.3 Установка программного обеспечения на Сервере конфигураций	62
4.1.4 Первоначальная настройка	67
4.1.5 Настройка количества дескрипторов для записи видеоархива на диск	67
4.1.6 Запуск SecurOS на Сервере конфигураций	68
4.2 Установка, настройка и запуск Периферийных серверов	68
4.3 Установка, настройка и запуск Рабочих мест оператора	69
4.4 Порядок обновления SecurOS	69
5 Установка программного обеспечения для работы нейросетевых алгоритмов	70
5.1 Установка драйверов NVIDIA для работы нейросетевых алгоритмов на базе Caffe2Server в ОС Linux	70
6 Администрирование SecurOS	73
6.1 Работа с Панелью управления	73
6.1.1 Вызов, настройка и скрытие Панели управления	74
6.1.2 Вызов и закрытие Центра администрирования	76
6.1.3 Выбор Рабочего окружения	78
6.1.4 Управление сеансами пользователя и завершение работы Клиента	78
6.1.5 Завершение работы системы	79
6.1.6 Вызов справочной документации	79
6.2 Центр администрирования	81
6.2.1 Работа с объектами	83
6.2.1.1 Создание объекта	85
6.2.1.2 Изменение параметров объекта	85
6.2.1.3 Удаление объекта	85
6.2.1.4 Отключение/включение объекта	86
6.2.1.5 Переименование объекта	86
6.2.1.6 Поиск объектов	87
6.2.1.6.1 Поиск при помощи Панели поиска объектов	87
6.2.1.6.2 Поиск при помощи Окна поиска	89
6.2.1.7 Избранные объекты	90
6.2.1.8 Объекты, требующие настройки	91
6.2.2 Работа с табличными параметрами объектов	93

6.2.3 Работа со списками флажков	94
6.2.4 Добавление IP-устройств	95
6.2.5 Менеджер IP-устройств	96
6.2.5.1 Описание экранной формы	97
6.2.5.2 Базовые операции	100
6.2.5.2.1 Запуск Менеджера	101
6.2.5.2.2 Поиск устройств в сети	101
6.2.5.2.3 Добавление IP-устройства	102
6.2.5.2.4 Редактирование параметров IP-устройства	104
6.2.5.2.5 Копирование IP-устройства	104
6.2.5.2.6 Удаление IP-устройства	106
6.3 Пользователи и Права	106
6.3.1 Пользователи в SecurOS	107
6.3.1.1 Смена пароля суперпользователя	107
6.3.1.2 Смена/сброс пароля типового пользователя	108
6.3.2 Регистрация и настройка прав пользователей	113
6.3.3 Пример настройки прав пользователей сетевого домена	117
6.3.3.1 Настройки для провайдера Windows NT	117
6.3.3.2 Настройки для провайдера LDAP	118
6.4 Протоколирование работы SecurOS	118
6.5 Обновление лицензионного ключа на всех серверах	119
6.5.1 Настройка оповещения об окончании лицензии	119
6.6 Модуль самодиагностики Health Monitor	121
6.6.1 Система	127
6.6.2 Видеосервер	127
6.6.3 Камера	138
6.6.4 Микрофон	141
6.6.5 Луч	141
6.6.6 Удаленная система	142
6.7 Синхронизация файлов SecurOS	142
7 Основная подсистема	144
7.1 Принципы работы	144
7.2 Протоколы обмена данными	144
7.3 Описание объектов	145
7.3.1 Система	145
7.3.2 Объект охраны	149
7.3.2.1 Закладка Общие	151
7.3.2.2 Закладка Серверы для подключения	152
7.3.2.3 Закладка Ограничение подключений	153
7.3.2.4 Закладка Управление паролями	154
7.3.3 База данных	157
7.3.4 Отдел	159
7.3.5 Пользователь	160
7.3.6 Active Directory / LDAP	161
7.3.7 Права пользователя	163
7.3.7.1 Двухфакторная аутентификация в SecurOS	168
7.3.8 Компьютер	171
7.3.8.1 Архив	176
7.3.8.2 Автоматическая авторизация	180
7.3.9 Водяной знак	181
7.3.10 Фильтр событий	183
7.3.11 Сценарий поведения	187
7.3.12 SNMP агент	187
7.3.12.1 Настройка средств управления и мониторинга Windows	188
7.3.13 Внешнее приложение	191

7.3.14 Database Partitioner	192
7.3.15 Репликатор баз данных	193
8 Подсистема интерфейса	195
8.1 Описание объектов	195
8.1.1 Рабочий стол	195
8.1.1.1 Операции настройки Рабочего стола	197
8.1.2 Карта	201
8.1.2.1 Принципы работы с картой	203
8.1.2.2 Изображения уровней карты	204
8.1.2.3 Работа с уровнями карты	204
8.1.2.4 Работа с объектами	207
8.1.3 Карта: Интерфейс оператора	209
8.1.4 Протокол событий	211
8.1.5 Внешнее окно	212
8.1.6 HTML5 FrontEnd	213
9 Видеоподсистема	216
9.1 Аппаратная декомпрессия	216
9.1.1 Настройка аппаратной декомпрессии для ОС Windows	218
9.1.2 Настройка аппаратной декомпрессии для ОС Linux	218
9.2 Аппаратная компрессия	219
9.3 Настройка аппаратного ускорения в ОС Linux	219
9.3.1 Установка дополнительных пакетов в ОС Linux	219
9.3.2 Установка дополнительных пакетов в ОС Debian	220
9.3.3 Проверка работы аппаратного ускорения	221
9.3.4 Решение типовых проблем аппаратного ускорения	222
9.4 Многопоточность	224
9.5 Прореживание видеопотока	225
9.6 Принципы работы зон обнаружения движения	225
9.6.1 Создание зон	226
9.7 Архивы SecurOS	226
9.8 Локальное хранилище камеры (Edge Storage)	227
9.8.1 Требования к системе	227
9.8.2 Настройка системы для работы с Edge Storage	228
9.8.3 Ограничения экспорта архива Камеры, просматриваемого через EdgeStorage Gate	231
9.9 Ретроспективный поиск	231
9.10 Наложение водяных знаков	232
9.11 Специальные настройки элементов видеоподсистемы	232
9.11.1 Настройки изображения	232
9.11.2 Запись архива на диск	232
9.11.2.1 Настройка дисков для записи	232
9.11.2.1.1 Разметка и монтирование локальных дисков в ОС Linux	233
9.11.2.2 Горячая замена диска	239
9.12 Описание объектов	240
9.12.1 Системные объекты	241
9.12.1.1 Устройство видеозахвата	241
9.12.1.1.1 Закладка Подключение	242
9.12.1.1.2 Закладка Прошивка	246
9.12.1.1.3 Active Camera Recorder (AC Recorder)	247
9.12.1.2 Камера	247
9.12.1.2.1 Закладка Общие	248
9.12.1.2.2 Закладка Поток	251
9.12.1.2.3 Закладка Запись	256

9.12.1.2.4	Закладка Аудио	260
9.12.1.2.5	Закладка Детекторы	262
9.12.1.2.6	Закладка PTZ	263
9.12.1.2.7	Закладка Дополнительные	265
9.12.1.2.8	Мультикаст	276
9.12.1.2.9	Настройка панорамных камер	278
9.12.1.3	Детектор расфокусировки	279
9.12.1.3.1	Рекомендации по настройке	281
9.12.1.4	Раскладка	282
9.12.1.5	Вид	284
9.12.1.6	Зона	284
9.12.1.7	Световой детектор	288
9.12.1.8	Конвертер архива	289
9.12.1.8.1	Цифровая подпись	297
9.12.1.8.2	Отображение субтитров в экспортированном видео	298
9.12.1.9	Профиль экспорта архива	298
9.12.1.10	Архиватор	299
9.12.1.11	Image Processor	305
9.12.1.12	RTSP-сервер	306
9.12.1.13	ONVIF-сервер	309
9.12.1.13.1	Закладка Общие	310
9.12.1.13.2	Закладка Встроенный RTSP-сервер	312
9.12.2	Объекты пользовательского интерфейса	314
9.12.2.1	Медиа Клиент	315
9.12.2.1.1	Закладка Отображение	316
9.12.2.1.2	Закладка Раскладки	321
9.12.2.1.3	Закладка Виды	324
9.12.2.1.4	Закладка Камеры	326
9.12.2.1.5	Закладка Экспорт и архив	330
9.12.2.1.6	Закладка Аудио	333
9.12.2.1.7	Закладка Дополнительные	335
9.12.2.1.8	О Видях	337
9.12.2.1.9	Операции с Видями	338
9.12.2.1.9.1	Создание Вида	340
9.12.2.1.9.2	Редактирование Вида	340
9.12.2.1.9.3	Переименование Вида	341
9.12.2.1.9.4	Удаление Вида	341
9.13	Примеры настройки	342
9.13.1	Одиночная конфигурация	342
9.13.2	Видеосервер и Рабочие места оператора	343
9.13.3	Настройка камеры	344
9.13.3.1	Добавление устройства видеозахвата в систему	344
9.13.3.2	Добавление камеры в систему	345
9.13.3.3	Выбор камеры для работы с Медиа Клиентом	346
9.13.3.4	Добавление прав пользователя	347
9.13.3.5	Настройка телеметрии	349
9.13.3.5.1	Настройка телеметрии для IP-устройств	349
9.13.3.5.1.1	Совместное управление телеметрией	351
9.13.3.5.1.2	Раздельное управление телеметрией	351
9.13.4	Настройка джойстика	353
10	Аудиоподсистема	354
10.1	Режимы работы	354
10.1.1	Синхронная запись и воспроизведение аудио- и видеопотока	354
10.1.2	Независимая запись и воспроизведение произвольного аудиопотока	354
10.2	Описание объектов	355
10.2.1	Устройство аудиозахвата	355
10.2.2	Микрофон	357

10.3 Пример настройки для синхронного прослушивания, записи и воспроизведения аудио- и видеопотока	358
11 Подсистема ввода/вывода	360
11.1 Описание объектов	360
11.1.1 Луч	360
11.1.2 Реле	362
11.1.3 CCTV Клавиатура или джойстик	363
11.1.3.1 Bosch IntuiKey	364
11.1.3.2 Hikvision DS-1100KI	367
11.1.3.3 Hikvision DS-1200KI/DS-1600KI(B)	368
11.1.3.4 Panasonic WV-CU950	369
11.1.3.5 Pelco KBD300A	370
11.2 Настройка системы для работы с Дворниками и Омывающими устройствами.	371
12 Подсистема оповещения	372
12.1 Описание объектов	372
12.1.1 Всплывающее окно HTML5	372
12.1.2 Сервис почтовых сообщений	373
12.1.3 Почтовое сообщение	375
12.1.4 Сервис коротких сообщений	377
12.1.5 Короткое сообщение	378
12.1.6 Сервис звукового оповещения	378
12.1.7 Служба реагирования	379
12.1.7.1 Список типов происшествий. Формат файла	382
12.1.8 Интеграция с SIP-устройствами	384
12.1.8.1 Подсистема SIP	384
12.1.8.2 SIP-устройство	386
12.1.8.3 SIP: Интерфейс оператора	388
13 Подсистема автоматизации	390
13.1 Описание объектов	390
13.1.1 Расписание	390
13.1.2 Макрокоманда	393
13.1.3 Скрипт Node.js	396
13.1.4 Интерфейс IIDK	399
13.1.5 HTTP Event Gate	400
13.1.6 REST API	401
13.2 Настройка макрокоманд и скриптов	402
13.2.1 Настройка макрокоманд	402
13.2.2 Настройка скриптов Node.js	403
14 Компьютерное зрение	405
14.1 Общие рекомендации по настройке и расположению камер	406
14.2 Настройка системы	407
14.2.1 Выбор видеопотока для аналитики	408
14.2.2 Настройка плагина Tracking Kit III и встроенных видеоаналитических детекторов	409
14.2.2.1 Настройка плагина Tracking Kit III	410
14.2.2.1.1 Залкадка Сцена	412
14.2.2.1.2 Залкадка Трекер	416
14.2.2.1.3 Залкадка Классификация	417
14.2.2.1.4 Залкадка Ретроспективный поиск	419
14.2.2.2 Настройка встроенных видеоаналитических детекторов	419
14.2.2.2.1 Настройка контролируемой зоны	421
14.2.2.2.2 Детектор бега	427

14.2.2.2.1	Настройка перспективы для Детектора бега	429
14.2.2.3	Детектор движения в запрещенном направлении	430
14.2.2.3.1	Настройка перспективы для Детектора движения в запрещенном направлении	433
14.2.2.4	Детектор оставленных и унесенных предметов	433
14.2.2.5	Детектор пересечения линии	436
14.2.2.6	Детектор празднования	438
14.2.2.7	Детектор пребывания в зоне	441
14.2.2.8	Детектор проникновения в запрещенную зону	442
14.2.2.9	Детектор скопления людей	445
14.2.2.9.1	Настройка перспективы для Детектора скопления людей	447
14.2.2.10	Счетчик объектов	447
14.2.2.10.1	Настройка перспективы для Счетчика объектов	450
14.2.3	Настройка независимых видеоаналитических детекторов	450
14.2.3.1	Детектор дыма	451
14.2.3.1.1	Рекомендации по настройке камер для Детектора дыма	452
14.2.3.2	Детектор людей без касок	452
14.2.3.2.1	Рекомендации по настройке камер для Детектора людей без касок	455
14.2.3.3	Нейросетевой детектор драк	455
14.2.3.3.1	Рекомендации по настройке камер для Нейросетевого детектора драк	457
14.2.3.4	Нейросетевой детектор дыма и огня	457
14.2.3.4.1	Рекомендации по настройке камер для Нейросетевого детектора дыма и огня	459
14.2.3.5	Нейросетевой детектор празднования	460
14.2.3.5.1	Рекомендации по настройке камер для Нейросетевого детектора празднования	462
14.2.3.6	Нейросетевой детектор уклонения от оплаты	462
14.2.3.6.1	Рекомендации по настройке камер для Нейросетевого детектора уклонения от оплаты	464
14.2.3.7	Нейросетевой детектор упавших людей	464
14.2.3.7.1	Рекомендации по настройке камер для Нейросетевого детектора упавших людей	466
14.2.3.8	Нейросетевой счетчик людей	466
14.2.3.8.1	Рекомендации по настройке камер для Нейросетевого счетчика людей	468
14.2.4	Оптимизация производительности NUMA-систем	468
14.3	Представление результатов работы видеоаналитического детектора	469
15	Центр Мониторинга и Контроля	471
15.1	Прямое подключение	471
15.1.1	Ограничения	472
15.1.2	Настройка Прямого подключения	472
15.1.2.1	Шлюз MCC DC	474
15.1.2.2	MCC DC HTTP Proxy	475
15.1.2.3	Удаленная система	476
15.1.2.3.1	Закладка Общие	477
15.1.2.3.2	Закладка Шлюз и прокси	478
15.1.3	Настройка для работы с SecurOS Auto	479
15.2	Привилегированный доступ	482
15.2.1	Функционирование	482
15.2.2	Ограничения	483
15.2.3	Настройка системы	484
15.2.4	Перенос архива между Удаленной системой и Центром Мониторинга	486
16	Резервирование	488
16.1	Отказоустойчивый кластер	488
16.1.1	Структура кластера	488
16.1.1.1	Конфигурация кластера	489
16.1.1.2	Функционирование кластера. Кворум	489
16.1.1.3	Рекомендации	490
16.1.2	Конфигурирование кластера	490
16.1.2.1	Создание кластера	491
16.1.2.1.1	Перенастройка конфигурации SecurOS на работу с кластером	492

16.1.2.1.2	Создание конфигурации SecurOS с кластером	492
16.1.2.2	Получение текущей конфигурации кластера	493
16.1.2.3	Создание Объекта охраны	494
16.1.2.4	Добавление Хоста	494
16.1.2.5	Подключение компьютера к кластеру резервных серверов	495
16.1.2.6	Удаление Хоста	495
16.1.2.7	Перевод в режим Видеосервера	496
16.1.2.8	Добавление Ноды	496
16.1.2.9	Удаление Ноды	497
16.1.2.10	Получение списка Нод	497
16.1.2.11	Выбор приоритетного Хоста для Ноды	497
16.1.2.12	Ручной перенос Ноды на Хост	498
16.1.2.13	Пересоздание кластера	498
16.1.2.14	Восстановление конфигурации SecurOS из файла	499
16.1.2.15	Выбор Сервера конфигураций	499
16.1.2.16	Преобразование независимого Видеосервера в Ноду кластера	500
16.1.2.17	Сервисный режим	500
16.1.2.18	Изменение сетевого интерфейса для виртуальных адресов	501
16.1.2.19	Настройка временных интервалов	501
16.1.3	Подключение Рабочих мест оператора к серверам кластера	502
16.1.4	Организация хранилища в кластере	502
16.1.4.1	iSCSI-диск	503
16.1.4.2	Использование iSCSI-диска для хранения видеоархива	505
16.1.4.3	Перемещаемый PostgreSQL	505
16.1.4.4	Хранение видеоархива на локальных дисках Хостов	507
16.1.5	Примеры создания и настройки кластера	508
16.1.5.1	Создание конфигурации SecurOS с кластером. Пример	508
16.1.5.1.1	Задача	508
16.1.5.1.2	Требования	508
16.1.5.1.3	Параметры компьютеров	509
16.1.5.1.4	Шаги	509
16.1.5.2	Перенастройка конфигурации SecurOS на работу с кластером. Пример	510
16.1.5.2.1	Задача	511
16.1.5.2.2	Требования	511
16.1.5.2.3	Параметры компьютеров	511
16.1.5.2.4	Шаги	512
16.1.6	Решение типовых проблем	513
16.1.6.1	Потеря кворума	513
16.1.6.2	Восстановление операционных систем Хостов из резервной копии	513
16.1.6.3	Отсутствие возможности подключиться с Рабочего места оператора	514
16.1.6.4	Обновление программного и аппаратного обеспечения в системе с кластером	514
16.1.7	Ограничения	515
16.2	Кластер резервных серверов	516
16.2.1	Создание конфигурации на основе кластера резервных серверов	516
16.2.1.1	Задача	516
16.2.1.2	Шаги	516
16.2.2	Перенастройка конфигурации SecurOS на работу с кластером «1+1». Пример	517
16.2.2.1	Задача	517
16.2.2.2	Параметры компьютеров	517
16.2.2.3	Шаги	517
17	Взаимодействие с внешней Службой реагирования	519
18	Модули специального назначения	522
18.1	Термометр	522
19	Легкая интеграция	524

19.1	Общее описание	524
19.2	Точка интеграции	525
20	Горячие клавиши	526
20.1	Панель инструментов администратора	526
21	Приложения	527
21.1	Приложение 1. Обновление/удаление программного обеспечения	527
21.1.1	Обновление программного обеспечения	527
21.1.2	Удаление программного обеспечения	527
21.1.3	Особенности обновления версий SecurOS	529
21.1.3.1	Обновление версии 9.3 и более ранних	529
21.1.3.2	Обновление версии 9.6 и более ранних	530
21.1.3.3	Обновление версии 10.0 и более ранних	531
21.1.3.4	Обновление версии 10.1 и более ранних	531
21.1.3.5	Обновление версии 10.2 и более ранних	531
21.1.3.6	Обновление версии 10.3 и более ранних	531
21.1.3.7	Обновление версии 10.6 и более ранних	532
21.1.3.8	Обновление версии 10.7 и более ранних	532
21.1.3.9	Обновление версии 10.9 и более ранних	533
21.1.3.10	Обновление версии 10.10 и более ранних	533
21.1.3.11	Обновление версии 11.2 и более ранних	533
21.1.3.12	Обновление версии 11.3 и более ранних	533
21.1.3.13	Обновление версии 11.4 и более ранних	533
21.1.3.14	Обновление версии 11.5 и более ранних	534
21.1.3.15	Обновление версии 11.6 и более ранних	534
21.1.3.16	Обновление версии 11.7 и более ранних	534
21.1.3.17	Обновление версии 11.8 и более ранних	534
21.2	Приложение 2. Обновление версии PostgreSQL	534
21.3	Приложение 3. Быстрая настройка видеоподсистемы	538
21.4	Приложение 4. Системные утилиты	540
21.4.1	Утилита Server Manager	540
21.4.1.1	Панель управления	542
21.4.1.1.1	Работа со списком хостов	542
21.4.1.1.2	Управление кластером	543
21.4.1.1.3	Управление состоянием Видеосервера	544
21.4.1.1.4	Подключение к хосту для конфигурирования	544
21.4.1.1.5	Восстановление конфигурации SecurOS	544
21.4.1.1.6	Управление нодами	545
21.4.1.1.7	Расширенные настройки кластера	546
21.4.1.1.8	Строка поиска	548
21.4.1.2	Таблица хостов	548
21.4.2	Утилита Hardware Report Utility	550
21.4.3	Утилита SystemInfo	552
21.4.4	Утилита Media Export Utility	556
21.4.4.1	Диалоговое окно настройки экспорта	558
21.4.4.2	Параметры командной строки	560
21.4.5	Утилита настройки подключений к БД (DSAdmin)	562
21.4.6	Утилита обновления БД (Database Update Utility)	565
21.4.7	Утилита Редактор регистрационных файлов (DDI)	567
21.4.8	Утилита Server Role Manager	573
21.4.9	Утилита Server Control Agent	575
21.4.10	Утилита восстановления индексов медиаархива	577
21.4.11	Утилита обновления аудиофайлов устаревшего формата	578
21.4.12	Утилита Certificate Generator	580
21.4.13	Утилита AuditClient	583

21.4.13.1	Настройка таблицы результатов.	589
21.4.13.2	Пример анализа действий пользователя.	590
21.5	Приложение 5. Используемые в SecurOS сетевые порты.	591
21.6	Приложение 6. Дополнительные настройки Windows	593
21.6.1	Установка Media Foundation в среде MS Windows Server 2012 R2.	593
21.6.2	Установка и настройка почтового SMTP-сервера.	593
21.6.3	Отключение мастера очистки дисков.	596
21.7	Приложение 7. Дополнительные настройки SecurOS.	596
21.7.1	Масштабирование SecurOS при масштабировании Windows.	597
21.8	Приложение 8. Диагностика и решение технических проблем.	597
21.8.1	Создание дампов процессов.	597
21.8.1.1	Создание дампа процесса в ОС Windows	597
21.8.1.2	Создание дампа процесса в ОС Linux	598
21.9	Приложение 9. Возможные сообщения об ошибке при запуске системы.	598
21.10	Приложение 10. Информация для Службы технической поддержки.	600
Предметный указатель		602

1 Предисловие

Данный раздел содержит общую информацию о текущем документе, средствах его оформления и использования, а также о порядке получения дополнительной поддержки при эксплуатации продукта.

1.1 Назначение

Данное руководство дает общее представление об архитектуре SecurOS, описывает процесс настройки сети безопасности и системных объектов, содержит советы и рекомендации по настройке.

Предполагается, что уже настроена локальная сеть и на подключенные к ней компьютеры установлено ПО SecurOS.

1.2 Целевая аудитория

Руководство предназначено для системных инсталляторов и администраторов SecurOS — опытных пользователей компьютера, имеющих навыки по установке аппаратного обеспечения и построению сети на основе протокола TCP/IP, знающих основы технологий CCTV.

1.3 Использование руководства

Данный документ можно использовать как в печатном, так и в электронном виде. В последнем случае доступны такие возможности ПО Adobe Reader, как закладки и гипертекстовые ссылки для навигации по документу. Данное руководство ссылается на другие документы по SecurOS, которые можно найти на установочном диске SecurOS или на веб-сайте компании ISS (www.iss.ru).

Данный документ можно вызвать из SecurOS нажатием клавиши **F1**. В режиме администрирования можно открыть статью, посвященную настройкам какого-либо объекта/описанию утилиты, нажав на **F1** при открытом окне настроек данного объекта/окне утилиты. В режиме оператора с помощью клавиши **F1** можно открыть описание активного окна текущего интерфейса оператора или утилиты.

1.4 Обращение за технической поддержкой

При наличии вопросов, ответы на которые отсутствуют в данном руководстве, обратитесь к администратору системы или системному интегратору.

За дальнейшей информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems:

- По телефону: +7 (495) 645 21 21 (многоканальный, с понедельника по четверг с 9:00 до 18:00, в пятницу с 9:00 до 17:00 по московскому времени);
- Через Портал технической поддержки <http://help.iss.ru> для оперативной реакции на запрос.

Примечание. Инструкция по работе с Порталом размещена на <https://help.iss.ru/ru/site/instruction>.

Для более скорого разрешения проблем рекомендуем подготовить служебную информацию, указанную в разделе **Информация для Службы технической поддержки**.

1.5 Соглашение по наименованию редакций SecurOS

Данный документ представляет собой единое руководство для нескольких редакций продукта "Интеграционная платформа видеоменеджмента SecurOS", отличающихся по функциональным возможностям:

Редакция	Поддерживаемые ОС
<i>SecurOS Monitoring & Control Center</i>	Windows/Linux
<i>SecurOS Enterprise</i>	
<i>SecurOS Premium</i>	
<i>SecurOS Professional</i>	Windows
<i>SecurOS Xpress</i>	
<i>SecurOS Lite</i>	

Для обозначения продукта, вне зависимости от его редакции, в рамках данного документа используется единый термин *SecurOS*.

Разделы, в которых описаны функциональности, доступные для некоторых редакций Windows/Linux, отмечаются специальной сноской, пример которой представлен ниже:

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*, *SecurOS Xpress*, *SecurOS Lite*.

Разделы, в которых описаны функциональности, недоступные или частично доступные в ОС Linux, отмечаются следующей сноской:

В ОС **Linux** функциональность не поддерживается/ограничена.

1.6 Соглашение по оформлению

В данном документе для представления различных терминов и названий используются следующие шрифты и средства форматирования.

Параметр	Описание
жирный	Используется при написании названий рабочих мест, утилит или экранных форм, окон и диалоговых окон, а также названий их элементов.

Параметр	Описание
<i>курсив</i>	Используется для выделения объектов SecurOS.
<i>жирный курсив</i>	Используется для выделения элементов однородных списков.
моноширинный	Используется для выделения текстов макрокоманд и программных кодов, имен файлов и путей к ним. Также используется для указания необходимой опции, выделения значений, задаваемых пользователем с клавиатуры.
зеленый	Используется для выделения перекрестных ссылок внутри документа и ссылок на доступные внешние документы.

1.7 Элементы оформления

Внимание! Служит для привлечения внимания пользователя к информации, которая необходима для корректного восприятия изложенного далее текста. Как правило, данная информация имеет предупреждающий характер.

Примечание. Текст примечания в основном тексте.

Дополнительная информация

Используется для отображения информации дополнительного характера. В элементах такого типа размещается, например, описание вариантов выполнения операции или ссылка на дополнительную литературу.

2 Назначение, реализация и принципы функционирования

Программное обеспечение SecurOS предназначено для управления системами видеонаблюдения и видеоаналитики, разворачиваемых в локальной или глобальной сети. Простота масштабирования программной и аппаратной платформы позволяет создавать системы видеонаблюдения любого уровня — от локальных, обеспечивающих видеоконтроль небольших и средних объектов, до комплексных систем контроля объектов инфраструктуры уровня предприятия.

2.1 Архитектура SecurOS

В данном разделе приводится описание возможных типов серверов и рабочих мест SecurOS, их основные возможности, зависящие от типов установки программного обеспечения.

2.1.1 Виды серверов и рабочих мест

Компьютеры сети SecurOS различаются по функциональному назначению и по роли в процессе управления конфигурацией сети.

В данном разделе приводится общая информация о видах серверов и рабочих мест SecurOS, их назначение, основные возможности и особенности функционирования.

2.1.1.1 Классификация по функциональному назначению

Все компьютеры, входящие в сеть SecurOS, делятся по своему функциональному назначению на две группы, определяющие тип установки системного ПО SecurOS:

- **Видеосервер.**
- **Рабочее место оператора.**

Тип установки выбирается администратором при планировании архитектуры системы и задается непосредственно в процессе установки. На каждом сетевом компьютере допускается выполнять установку только одного выбранного типа. Краткое описание типов установки приводится ниже.

2.1.1.1.1 Видеосервер

Видеосервер представляет собой компьютер, предназначенный для непосредственного подключения IP-камер видеонаблюдения, получения видеопотока с этих камер, а также подключения устройств аудиозахвата. Помимо прямого подключения камер видеонаблюдения данный тип установки позволяет устанавливать или подключать различные охранные устройства (контроллеры охранно-пожарной сигнализации, подсистема контроля доступа и т. д.) и интеллектуальные программные модули ISS (например, модуль SecurOS Auto).

2.1.1.1.2 Рабочее место оператора

Рабочее место оператора представляет собой клиентский компьютер в сети безопасности, предназначенный для удаленного просмотра видео, получаемого с камер видеонаблюдения, прослушивания звука, управления различными устройствами, например поворотными устройствами, дверями, охранно-пожарной и другими подсистемами.

Если для оператора определены права конфигурирования системы, ему доступен **Центр администрирования**.

2.1.1.2 Классификация по роли в управлении конфигурацией

Роль *Видеосервера* определяет его место в процедуре управления конфигурацией сети SecurOS. Один из *Видеосерверов* сети должен быть *Сервером конфигураций*, а все прочие *Видеосерверы* – *Периферийными серверами*.

2.1.1.2.1 Сервер конфигураций

Надежное функционирование системы безопасности в сети, состоящей из нескольких типовых серверов, позволяющих независимо выполнять операции конфигурирования сети, обеспечивается в случае, если в каждый момент времени настройки системы на каждом из таких серверов являются актуальными.

Процедура обновления и синхронизации актуальных настроек системы на всех серверах сети выполняется с помощью *Сервера конфигураций*. *Сервер конфигураций* представляет собой выделенный сервер сети, типовые функциональные возможности которого дополнены соответствующими специфическими функциями.

Сервер конфигураций назначается в процессе установки системы из числа *Видеосерверов* сети SecurOS.

Внимание! В системе допускается наличие только одного *Сервера конфигураций*, который должен быть доступен для всех *Видеосерверов* и *Рабочих мест оператора*, с которых предполагается конфигурировать систему.

Конфигурация системы хранится на *Сервере конфигураций*. На каждом из *Периферийных серверов* системы хранится рабочая копия конфигурации.

В случае выхода *Сервера конфигураций* из строя, его можно восстановить из резервной копии после проведения необходимых работ (см. раздел **Восстановление конфигурации из резервной копии**), либо переназначить один из *Периферийных серверов* (см. раздел **Утилита Server Role Manager**).

Внимание! Время работы *Периферийных серверов*, не имеющих подключения к *Серверу конфигураций*, ограничено. Система завершит свою работу на *Периферийном Сервере* и всех подключенных к нему *Рабочих местах оператора*, если связь с *Сервером Конфигураций* не возобновлялась в течение 90 суток.

2.1.1.2.2 Управление конфигурацией сети с помощью сервера конфигураций

В данном разделе приводится описание порядка настройки серверов при развертывании сети, алгоритмов управления конфигурацией сети и ее восстановления.

2.1.1.2.2.1 Порядок настройки серверов при развертывании сети

При первоначальной настройке системы в первую очередь должен настраиваться (т. е. устанавливаться и конфигурироваться) *Сервер конфигураций* (см. раздел **Установка и настройка Сервера конфигураций**).

2.1.1.2.2.2 Процедура обновления и синхронизации

Обновление конфигурации системы выполняется в соответствии со следующим алгоритмом:

Примечание. Описанный алгоритм функционирования применим к любому типу операций с объектами дерева и их параметрами, включая операции создания, изменения, удаления.

1. С помощью *Рабочего места оператора* администратор (оператор) изменяет состав дерева объектов или настройки объектов того *Компьютера* (или *Компьютеров*), конфигурацию которых необходимо обновить.
2. *Рабочее место оператора*, с помощью которого изменяется конфигурация, формирует соответствующий запрос к *Серверу конфигураций*.

Примечания:

1. Если конфигурация системы изменяется с помощью *Сервера конфигураций*, запрос не формируется, изменения применяются непосредственно на *Сервере конфигураций*.
 2. В случае недоступности *Сервера конфигураций* настройка конфигурации системы с *Рабочих мест оператора* невозможна.
-

3. *Сервер конфигураций* обрабатывает запрос и применяет изменения, обновляя собственное дерево объектов и их настройки, после чего формирует и отправляет каждому из *Периферийных серверов* системы команду на обновление соответствующих объектов в их рабочих копиях. Если на момент применения изменений *Периферийный сервер* выключен, команда будет отправлена при восстановлении соединения с *Сервером конфигураций*.
4. После получения команды на обновление рабочей копии каждый из *Периферийных серверов* системы применяет произведенные изменения, обновляя собственное дерево и/или настройки соответствующих объектов.

Примечание. *Сервер конфигураций* обрабатывает запросы последовательно, в порядке их формирования. В каждый текущий момент времени *Сервер конфигураций* обрабатывает только текущий запрос. Обработка следующего запроса блокируется до завершения выполнения текущего запроса и применения изменений на *Сервере конфигураций*.

2.1.1.2.2.3 Восстановление конфигурации из резервной копии

В системе предусмотрено восстановление конфигурации из резервной копии. Резервная копия файла конфигурации может быть создана на любом из серверов сети, при этом процедура восстановления может быть выполнена только на *Сервере конфигураций*.

Внимание! Резервная копия может быть использована только в текущей версии SecurOS. Процедура создания резервной копии описана в разделе **Система**.

2.1.2 Программная реализация

Программное обеспечение SecurOS состоит из двух компонентов — *Серверной части* (далее *Сервер*) и *Клиентского приложения* (далее *Клиент*).

Сервер выполняет задачи получения и обработки видео, позволяет подключать различные охранные устройства и интеллектуальные программные Модули. После установки ПО этот компонент запускается автоматически на каждом компьютере с ролью *Видеосервер*.

Клиент устанавливается как на *Видеосервере*, так и на *Рабочем месте оператора*. При установке ПО SecurOS на *Видеосервере* *Клиент* устанавливается автоматически. Установка *Клиента* на *Рабочем месте оператора* выполняется отдельно. С помощью *Клиента* можно работать с объектами SecurOS — *Камерами*, *Картами* и пр. с помощью интерфейсных объектов SecurOS (*Медиа Клиента*, *Карта: Интерфейс оператора* и пр.). Также с помощью *Клиента* можно администрировать систему в случае, если администратор назначил пользователю (оператору) необходимые для этого права.

Серверная часть реализована как Служба ОС Video Management System Server. Запуск и остановка службы выполняется с помощью утилиты **Server Control Agent** или средствами ОС (см. **Завершение работы системы**).

Клиентская часть реализована в виде приложения client.exe. Данное приложение размещено в папке \SecurOS корневого каталога установки продукта.

Внимание! На всех *Компьютерах* сети SecurOS рекомендуется использовать одну и ту же кодировку символов для всех *Пользователей*. В противном случае на некоторых *Компьютерах* возможно некорректное отображение символов (в названиях объектов, событий и пр.).

2.2 Аппаратно-программная платформа

В данном разделе приводятся требования к аппаратно-программной платформе компьютеров, на которые предполагается установка типового системного программного обеспечения SecurOS.

2.2.1 Требования к Видеосерверу

Таблица 1. Системные требования к Видеосерверу

Параметр	Описание
Операционная система	Внимание! Поддерживаются только 64-битные версии указанных ниже ОС. • Windows 8.1 – все редакции. • Windows 10 – Home, Pro, Enterprise, Education. • Windows 11 – Home, Pro, Pro for Workstations, Enterprise (все вариации), Education, Education Pro. • Windows Server 2012 R2 – все редакции. • Windows Server 2016 – Standard, Datacenter. • Windows Server 2019 – Standard, Datacenter. • Windows Server 2022 – Standard, Datacenter. • Astra Linux – Special Edition 1.7. Примечание. Рекомендуется Astra Linux SE 1.7 с установленным оперативным обновлением 1.7.5 или новее. • Debian – Debian 12. Внимание! Для ОС семейства Linux поддерживаемым сервером отображения является X.Org Server, а поддерживаемой средой рабочего стола – Xfce.
Процессор	Intel Core i3-4330 или более производительный. Рекомендуется Intel Core i5-11600K.
Оперативная память	Видеосервер SecurOS: не менее 4 ГБ. Рекомендуется 12 ГБ Выделенный видеосервер SecurOS FaceX: не менее 6 ГБ. Рекомендуется 8 ГБ
Размер жесткого диска	Не менее 150 ГБ
Объем свободного места на жестком диске для установки ПО	Не менее 5 ГБ Примечание. Установка интеллектуальных модулей требует дополнительного места на жестком диске.
Объем свободного места на жестком диске для установки PostgreSQL	Не менее 500 МБ
Пропускная способность канала связи по протоколу TCP/IP	Не менее 100 Мбит/с. Рекомендуется 1000 Мбит/с

2.2.2 Требования к Рабочему месту оператора

Внимание! В сети SecurOS все *Видеосерверы* и *Рабочие места операторов* должны функционировать под управлением одной и той же ОС (Windows или Linux).

Таблица 2. Системные требования к Рабочему месту оператора

Параметр	Описание
Операционная система	• Windows 8.1 – все редакции. • Windows 10 – Home, Pro, Enterprise, Education. • Windows 11 – Home, Pro, Pro for Workstations, Enterprise (все вариации), Education, Education Pro. • Windows Server 2012 R2 – все редакции. • Windows Server 2016 – Standard, Datacenter. • Windows Server 2019 – Standard, Datacenter. • Windows Server 2022 – Standard, Datacenter. • Astra Linux – Special Edition 1.7. Примечание. Рекомендуется Astra Linux SE 1.7 с установленным оперативным обновлением 1.7.5 или новее. • Debian – Debian 12. Внимание! Для ОС семейства Linux поддерживаемым сервером отображения является X.Org Server, а поддерживаемой средой рабочего стола – Xfce.
Процессор	Intel Core i3-4130 или более производительный (например, Intel Core i5-11xxx).
Оперативная память	Не менее 4 ГБ. Рекомендуется 8 ГБ. Рекомендуемая частота – не менее 1600 МГц
Размер жесткого диска	Не менее 40 ГБ
Объем свободного места на жестком диске для установки ПО	Не менее 5 ГБ Примечание. Установка интеллектуальных модулей требует дополнительного места на жестком диске.
Видеоконтроллер	Рекомендуются: • Intel HD Graphics 4000 или более производительный с технологией Intel® Quick Sync Video (QSV) 2.0. или • NVIDIA GPU с 4 ГБ памяти (Ampere/Turing или новее для достижения лучшей производительности декодирования H.265 видеопотока).

Параметр	Описание
Разрешение экрана монитора	Не менее: • для ОС Windows — 1366x768 пикселей; • для ОС Linux — 1280x1024 пикселей. Внимание! При меньших разрешениях экрана монитора корректное отображение форм графического интерфейса пользователя для настройки и работы с системой не гарантируется.
Пропускная способность канала связи по протоколу TCP/IP	Не менее 100 Мбит/с. Для просмотра несжатого видео с множества камер одновременно рекомендуется не менее 1000 Мбит/с

2.2.3 Требования к Аудиоподсистеме

Для захвата и воспроизведения звука *Видеосервер* должен иметь либо встроенную звуковую плату (см. руководство для системной платы), либо любую дополнительную звуковую PCI-плату.

Примечание. Интегрированная или внешняя аудиоплата обеспечивает захват аудиопотока с одного микрофона.

2.2.4 Требования к Подсистеме оповещения

Для использования сервиса звукового оповещения (звуковое сопровождение событий) на отдельном компьютере потребуется либо встроенная, либо дополнительная звуковая плата.

2.2.5 Требования к Подсистемам СКУД/ОПС

Видеосервер должен иметь определенное количество свободных последовательных портов в зависимости от подключаемых контроллеров подсистем (подсистема контроля доступа, охранно-пожарная сигнализация).

2.2.6 Требования к окружению

В данном разделе содержится информация о системных и прочих требованиях, выполнение которых обеспечивает возможность установки, запуска и корректного функционирования SecurOS.

2.2.6.1 Ограничения имени компьютера

Имена компьютеров, на которые может быть установлено программное обеспечение SecurOS, должны удовлетворять следующим требованиям:

1. Длина имени не должна превышать 15 символов.
2. В имени запрещено использование пробелов, знаков табуляции и следующих символов:
` ~ ! @ # \$ % ^ & * () = + _ [] { } | ; : . ' \ " № , < > / ?

3. Имя не может состоять только из цифр.

Примечание. Шаги операций, в ходе которых предполагается задание/редактирование/проверка значения параметра **имя_компьютера**, снабжены ссылками на данный раздел.

2.3 Подсистемы SecurOS

В последующих разделах руководства описываются конфигурирование, основные особенности и объекты различных частей системы SecurOS. В структуре SecurOS выделяются следующие подсистемы:

- Основная подсистема, содержащая объекты и параметры основных составляющих системы, таких как пользователи и компьютеры. Также определяются параметры организационной структуры и хранения системных данных, сбора статистики работы приложений и системных компонентов (см. раздел **Основная подсистема**).
- Подсистема интерфейса, содержащая компоненты, предназначенные для визуального представления системной сети, объектов системы и графического интерфейса пользователя, используемые непосредственно операторами, работающими с системой. К этим компонентам относятся экраны, окна внешних приложений, карты, интерактивные формы и диалоги, журнал протокола событий системы (см. раздел **Подсистема интерфейса**).
- Видеоподсистема, компоненты которой управляют видеокамерами, видеопотоками и процессом видеозаписи, проигрыванием видеоархивов и мониторинга живого видео, обнаружением движения и записью в видеоархивы (см. раздел **Видеоподсистема**).
- Аудиоподсистема, содержащая объекты управления устройствами аудиозаписи и воспроизведения (см. раздел **Аудиоподсистема**).
- Подсистема ввода/вывода, содержащая объекты управления периферийными устройствами ввода/вывода (пожарные контроллеры, реле и различные датчики) (см. раздел **Подсистема ввода/вывода**).
- Подсистема оповещения, которая состоит из объектов управления оповещением пользователей о системных событиях посредством рассылки сообщений (см. раздел **Подсистема оповещения**).
- Подсистема автоматизации, содержащая средства для интеграции устройств, составления и интерпретации системных скриптов и макросов (см. раздел **Подсистема автоматизации**).
- Подсистема Компьютерного зрения, представляющая интегрированную среду, предназначенную для подключения и использования в SecurOS аналитических детекторов различного назначения (см. раздел **Компьютерное зрение**).
- Подсистема Мониторинга и Контроля, позволяющая организовать единый *Центр Мониторинга и Контроля* множества удаленных систем безопасности (см. раздел **Центр Мониторинга и Контроля**).

Примечание. Каждый из разделов содержит описание основных принципов работы и особенностей настройки объектов выбранной подсистемы.

3 Установка и обновление SecurOS на Windows

Данный раздел описывает последовательность шагов, необходимых для создания сети безопасности SecurOS и начала ее эксплуатации на платформе Windows.

Внимание! Убедитесь, что в настройках брандмауэра открыты все необходимые порты (см. [Приложение 5. Используемые в SecurOS сетевые порты](#)).

В первую очередь необходимо подготовить *Видеосерверы* (см. [Виды серверов и рабочих мест](#)). Порядок установки SecurOS на *Видеосерверы* описан в следующих разделах:

- [Установка, настройка и запуск Сервера конфигураций](#);
- [Установка, настройка и запуск Периферийных серверов](#).

Затем следует подготовить *Рабочие места оператора*. Порядок установки SecurOS на *Рабочие места оператора* описан в соответствующем разделе:

- [Установка, настройка и запуск Рабочих мест оператора](#).

Внимание!

1. На всех *Видеосерверах* и *Рабочих местах операторов* необходимо установить все компоненты всех интеллектуальных Модулей SecurOS, которые используются в системе.
2. Язык устанавливаемого программного обеспечения должен быть единым для всех подключаемых к сети компьютеров.
3. Системное время всех *Видеосерверов* в конфигурации должно быть синхронизировано.
4. Установка программного обеспечения SecurOS возможна только на компьютерах, имена которых соответствуют требованиям раздела [Ограничения имени компьютера](#).

3.1 Установка, настройка и запуск Сервера конфигураций

В данном разделе описываются операции установки и настройки управляющего сервера SecurOS.

3.1.1 Установка аппаратного обеспечения

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*, *SecurOS Xpress*.

В данном разделе содержится краткая информация о дополнительных аппаратных средствах, которые могут быть включены в комплект поставки продукта. К таким аппаратным средствам относятся ключи Guardant, контролирующие лицензионные ограничения.

3.1.1.1 Установка ключа Guardant

Ключ Guardant является электронным устройством, постоянно подключенным к компьютеру через USB-порт. Программное обеспечение SecurOS обращается к ключу для проверки лицензионной информации.

Ключ необходимо установить перед началом установки программного обеспечения SecurOS. Для установки ключа Guardant подсоедините его к свободному USB-порту компьютера.

Драйвер ключа Guardant устанавливается автоматически в случае выбора соответствующей опции Мастера установки SecurOS (см. раздел [Установка программного обеспечения](#)).

3.1.1.2 Установка драйвера ключа Guardant в ручном режиме

Чтобы установить драйвер ключа Guardant вручную после установки SecurOS, выполните следующие действия:

1. Перейдите в директорию установки SecurOS и далее в `\Drivers\Guardant32` или `\Drivers\Guardant64` для 32- и 64-битной ОС соответственно.
2. Запустите файл `GrdDrivers.msi`. Откроется окно приветствия Мастера установки.
3. Нажимайте кнопку **Далее**, пока Мастер установки не закончит работу.
4. По окончании процесса установки появится окно завершения. Нажмите кнопку **Заккрыть** для выхода из программы Мастера установки.

3.1.2 Лицензионный ключ

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*, *SecurOS Xpress*.

Лицензионный ключ определяет возможную конфигурацию сети безопасности и необходим для запуска SecurOS.

Лицензионный ключ создается на основе уникальных кодов аппаратных средств SecurOS (Guardant) или комбинации уникальных кодов аппаратных средств компьютера, на котором предполагается установка SecurOS.

При проверке лицензии ключи рассматриваются в соответствии со снижением приоритета в следующем порядке:

1. ключ Guardant;
2. ключ на основе комбинации уникальных кодов аппаратных средств компьютера (hardware-код).

Кроме уникальных кодов оборудования при генерации лицензионного ключа также учитываются следующие данные:

- язык программы, выбранный при установке SecurOS;
- язык по умолчанию установленной операционной системы (параметр **Language** (*local ID*));
- номер релиза SecurOS;

- редакция SecurOS.

В зависимости от варианта поставки продукта лицензионный ключ может предоставляться одним из следующих способов:

- в комплекте поставки оборудования, на компакт-диске с программным обеспечением;
- по электронной почте.

3.1.2.1 Ключ входит в состав продукта

Если лицензионный ключ поставляется на диске в комплекте, местоположение ключа необходимо указать в окне **Выбор директории с лицензионным ключом** на соответствующем этапе процедуры установки SecurOS (см. раздел [Установка программного обеспечения](#)).

3.1.2.2 Заказ ключа по электронной почте

В случае, если лицензионный ключ не входит в комплект поставки SecurOS, его необходимо заказать в Intelligent Security Systems.

Для оформления заказа выполните следующие действия:

1. Установите аппаратное и программное обеспечение SecurOS на компьютер.
2. Для получения уникальных кодов оборудования запустите утилиту **Hardware Report Utility**, для чего нажмите кнопку **Пуск** в Панели задач Windows. Последовательно выберите пункты меню **Все программы** → **SecurOS** → **Hardware Report Utility**.
3. Утилита автоматически выведет данные отчета в окно **Hardware Report Utility** (например, см. рис. 1).

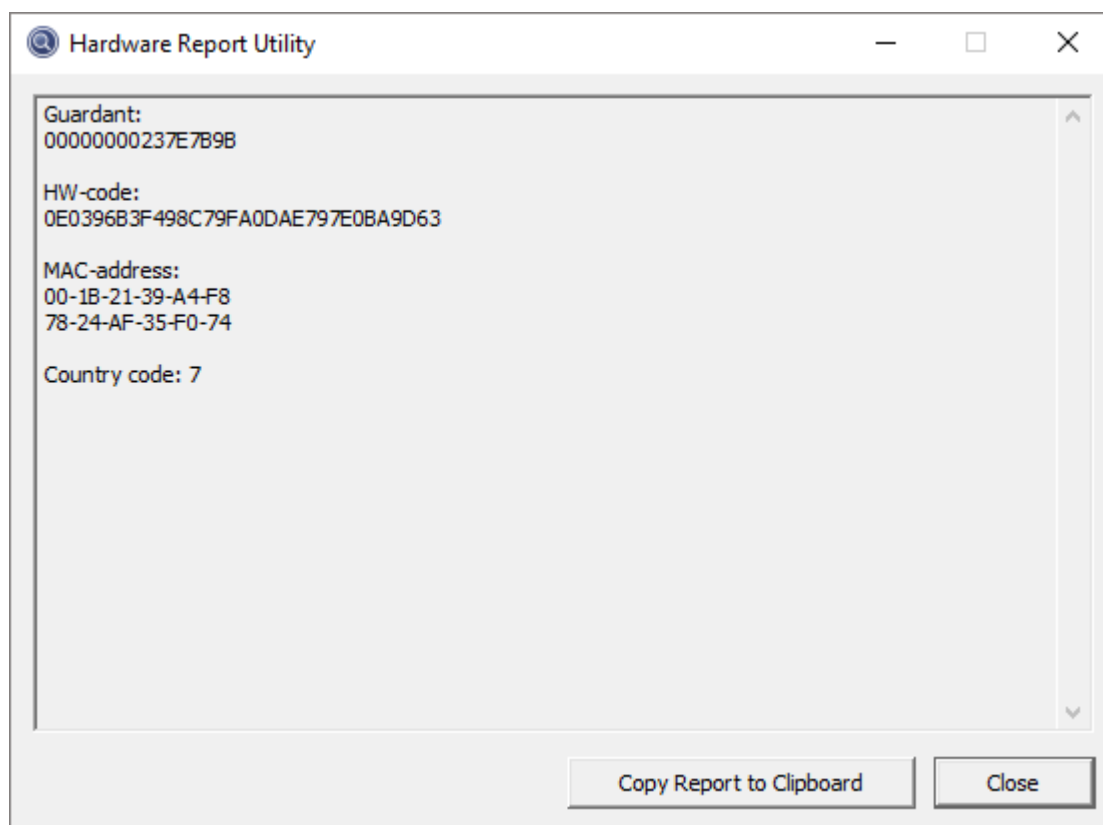


Рис. 1. Окно Hardware Report Utility

4. Щелкните кнопку **Copy Report to Clipboard**. Утилита скопирует отчет в буфер обмена.
5. Создайте и откройте новый текстовый файл любого формата. Вставьте в файл содержимое буфера обмена. Дополнительно укажите следующие значения:
 - язык программы, выбранный при установке SecurOS;
 - номер релиза SecurOS;
 - редакцию SecurOS.
6. Сохраните файл.
7. Отправьте файл с данными в Службу технической поддержки Intelligent Security Systems (см. раздел **Обращение за технической поддержкой**).

После получения файла лицензионного ключа скопируйте его в директорию установки SecurOS.

3.1.3 Установка программного обеспечения

В данном разделе приводится описание особенностей процедуры установки/обновления программного обеспечения, при которой сохраняется возможность использования ранее созданных объектов SecurOS и их параметров.

Внимание! Для установки программы в среде Windows необходимо обладать правами администратора. Приступайте к установке программного обеспечения только после установки на компьютеры всех необходимых дополнительных устройств и настройки сети.

3.1.3.1 Использование параметров текущей учетной записи Windows для PostgreSQL

При первоначальной установке программного обеспечения SecurOS учетная запись Windows, необходимая для работы PostgreSQL, по умолчанию создается с именем `postgres` и таким же паролем.

Примечание. В случае, если ограничения политики безопасности не позволяют создать учетную запись с параметрами по умолчанию, укажите пароль, отвечающий требованиям политики безопасности.

Если значения по умолчанию были изменены, но текущую учетную запись предполагается использовать после переустановки или обновления программного обеспечения, выполните следующие действия на определенном этапе установки:

1. В окне **Обновление и разметка БД** (см. рис. 2) введите пароль учетной записи PostgreSQL, который использовался для работы базы данных ранее.

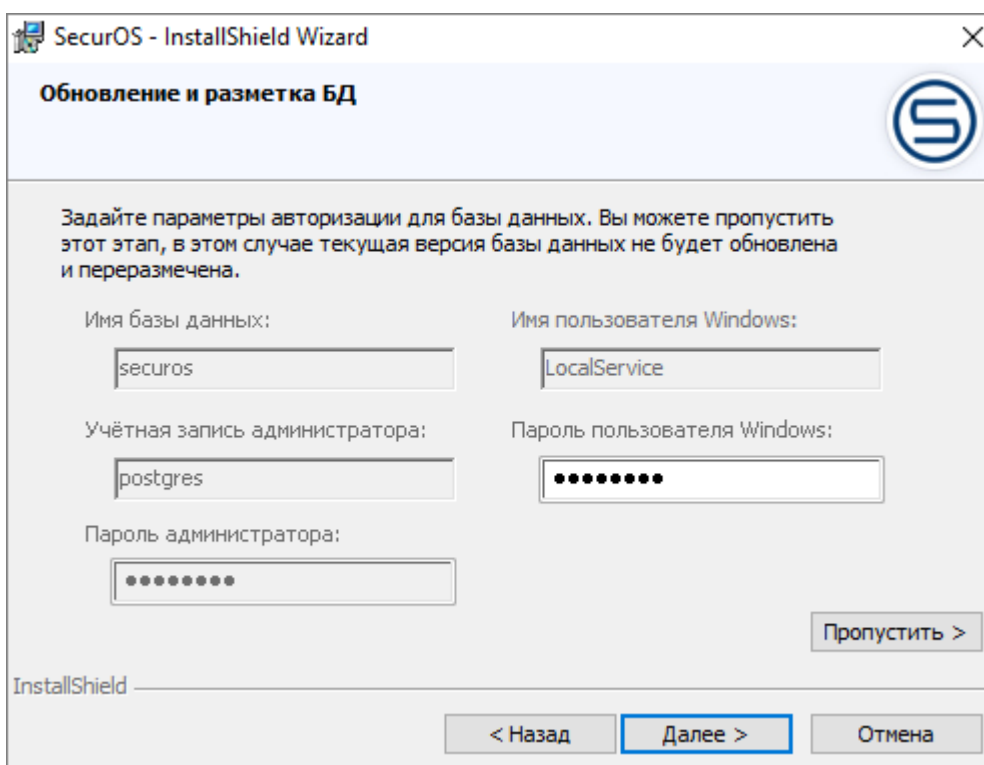


Рис. 2. Окно Обновление и разметка БД

2. Для продолжения обновления/переустановки нажмите кнопку **Далее**. Система пересоздаст учетную запись Windows с именем postgres и старым значением пароля.

Примечание. Данный этап установки может быть пропущен, однако в данном случае база данных не будет обновлена и переразмечена, что делает ее дальнейшее использование невозможным.

3.1.3.2 Использование текущих параметров БД и учетной записи администратора

При первоначальной установке программного обеспечения SecurOS учетная запись администратора PostgreSQL по умолчанию создается с именем postgres и таким же паролем, базе данных по умолчанию присваивается имя securOS.

Если значения по умолчанию были изменены, но текущую учетную запись администратора и имя базы данных предполагается использовать после переустановки или обновления программного обеспечения, выполните следующие действия на определенном этапе установки:

1. В окне **Обновление и разметка БД** (см. рис. 3) введите имя и пароль учетной записи администратора и имя базы данных, которые использовались для администрирования БД ранее.

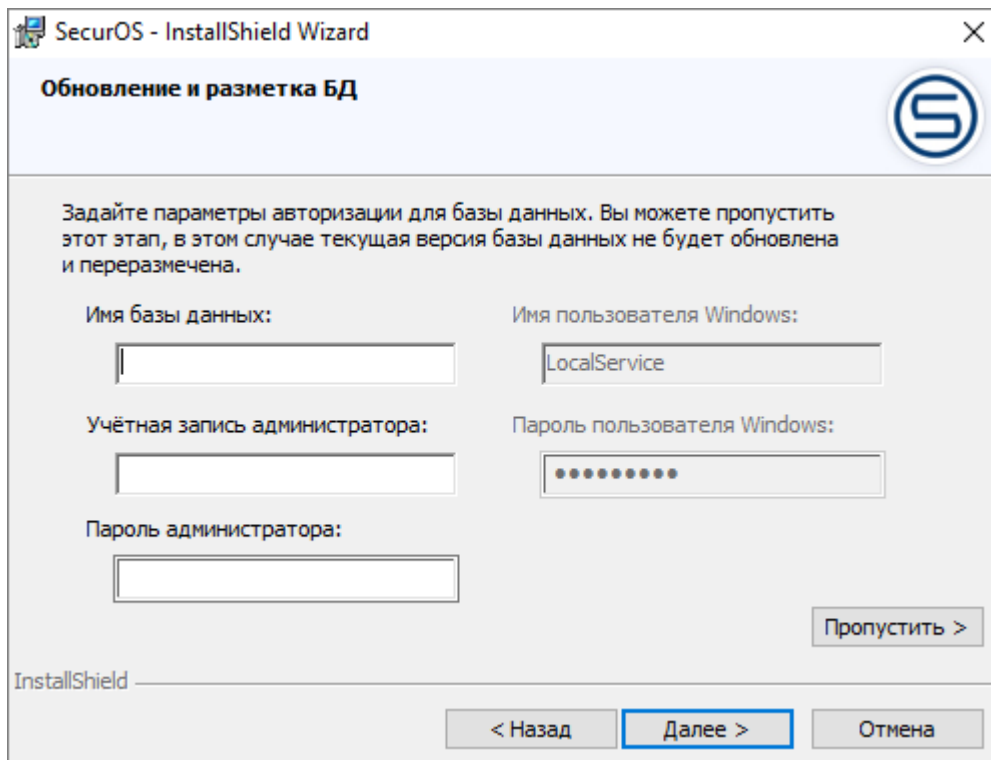


Рис. 3. Окно Обновление и разметка БД

2. Для продолжения установки нажмите кнопку **Далее**. Система выполнит обновление и переразметку базы данных с учетом старых значений параметров авторизации.

Примечание. Данный этап установки может быть пропущен, однако в данном случае база данных не будет обновлена и переразмечена, что сделает ее дальнейшее использование невозможным.

3.1.3.3 Процедура установки программного обеспечения на Сервере конфигураций

Для установки ПО на видеосервере выполните следующие действия:

1. Для начала установки программного обеспечения SecurOS на видеосервере запустите установочный файл продукта. Система выведет окно **Выбор языка** (см. рис. 4).

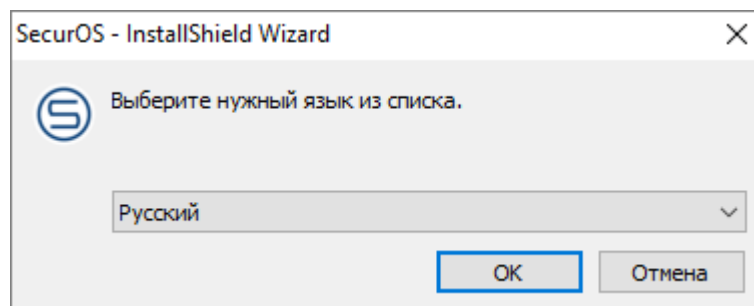


Рис. 4. Окно Выбор языка

В выпадающем списке выберите требуемый язык Мастера установки SecurOS. Нажмите кнопку **ОК**.

Дополнительная информация

Информационные сообщения окна **Выбор языка** зависят от значения языка по умолчанию операционной системы (значение параметра **Language** (*local ID*)).

2. Система выведет окно **Подготовка к установке**, в котором будут последовательно отображаться шаги процедуры подготовки системы к установке.

После завершения процедуры подготовки система автоматически выведет окно **Приветствие Мастера установки** (см. рис. 5).

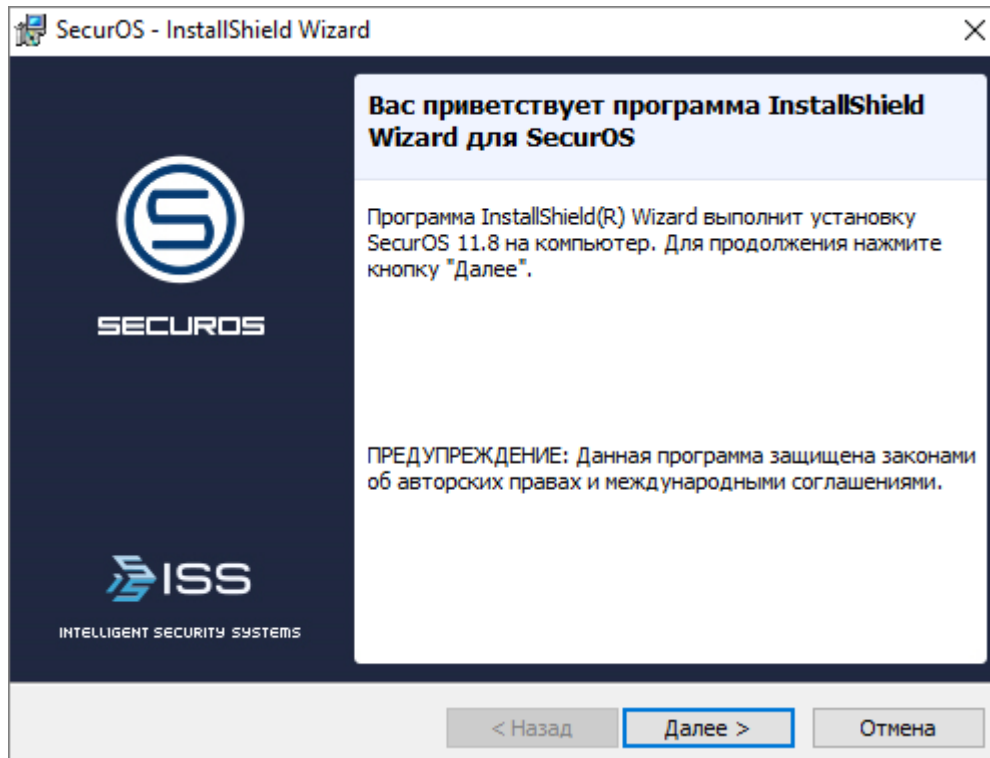


Рис. 5. Окно Приветствие Мастера установки

Для продолжения установки в окне **Приветствие Мастера установки** нажмите кнопку **Далее**.

3. Система выведет окно **Лицензионное соглашение** (см. рис. 6).

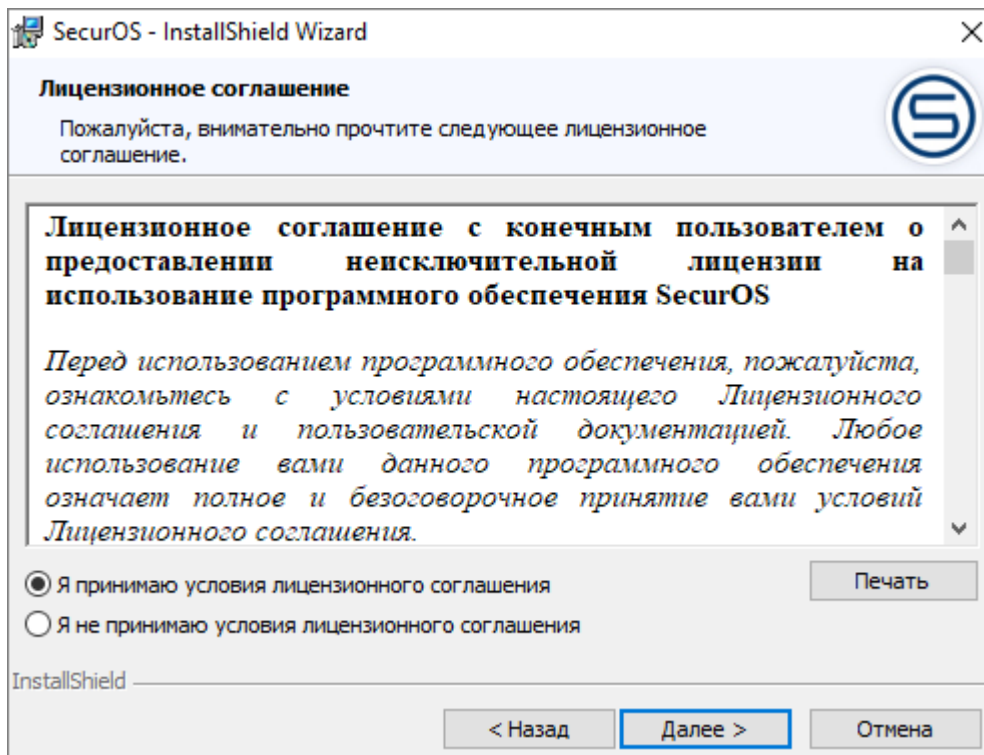


Рис. 6. Окно Лицензионное соглашение

Внимательно прочитайте лицензионное соглашение. Для продолжения установки программного обеспечения в окне лицензионного соглашения необходимо выбрать опцию **Я принимаю условия лицензионного соглашения**. Нажмите кнопку **Далее**.

4. Система выведет окно **Настройка установки** (см. рис. 7).

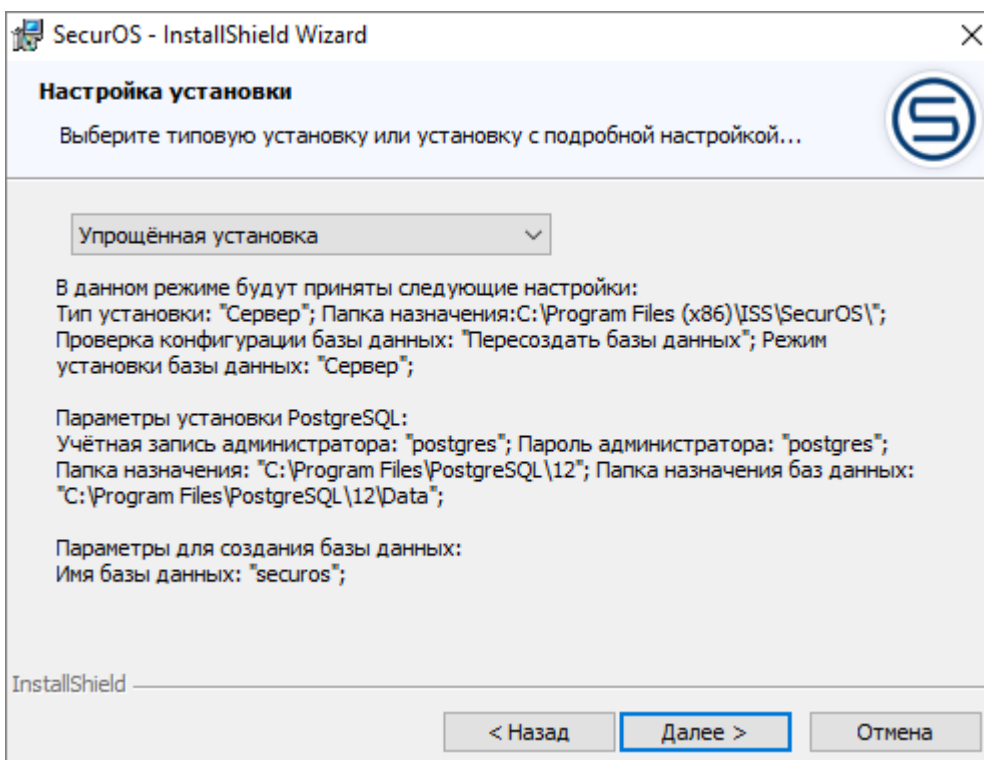


Рис. 7. Окно Настройка установки

По умолчанию в окне задан режим упрощенной установки, позволяющий установить ПО видеосервера с настройками по умолчанию. Нажмите кнопку **Далее**.

5. Система выведет окно **Тип сервера** (см. рис. 8).

В редакциях SecurOS Xpress, SecurOS Lite данный шаг исключен из процедуры установки.

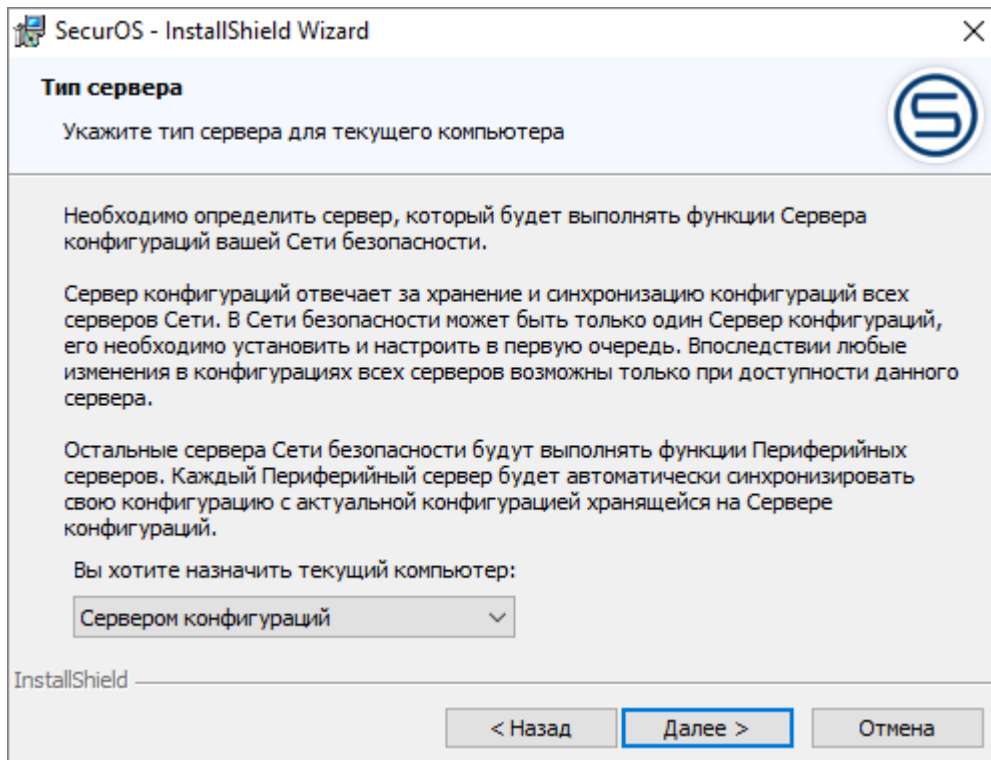


Рис. 8. Окно Тип сервера

Для установки программного обеспечения *Сервера конфигураций* выберите из выпадающего списка соответствующее значение. Нажмите кнопку **Далее**.

6. Система выведет окно **Выбор варианта установки файла лицензионного ключа** (см. рис. 9).

В редакции SecurOS Lite данный шаг исключен из процедуры установки.

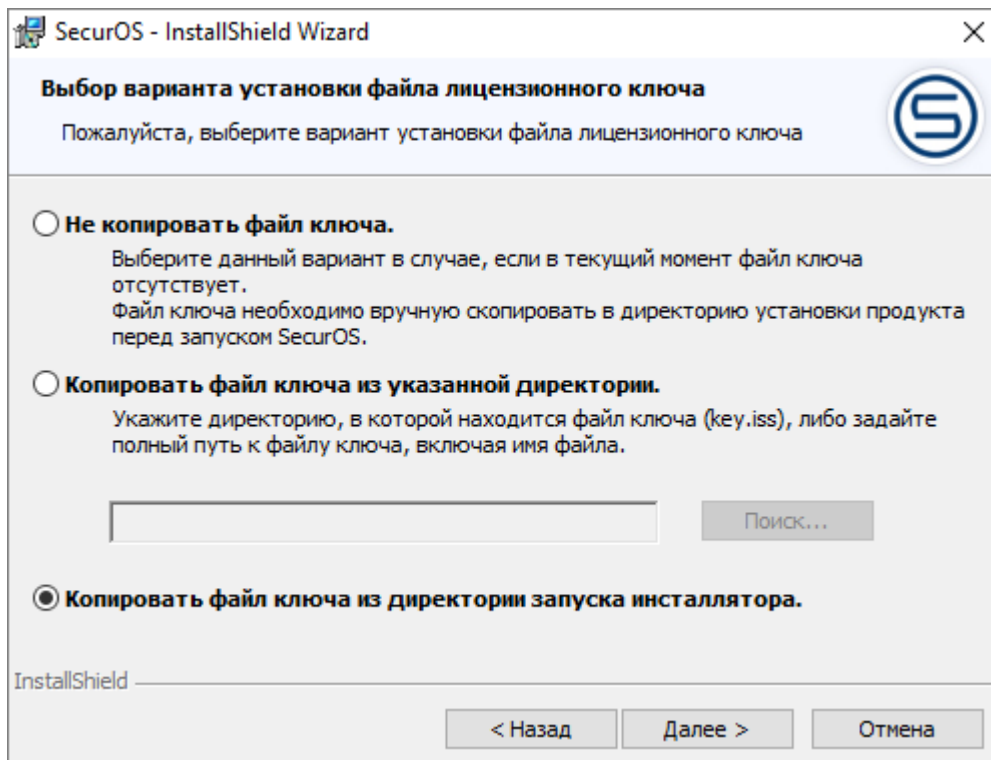


Рис. 9. Окно Выбор варианта установки файла лицензионного ключа

В зависимости от наличия лицензионного ключа выполните одно из следующих действий:

- *если ключ доступен:*

- выберите опцию **Копировать файл ключа из указанной директории**, нажмите кнопку **Поиск**, с помощью файлового менеджера укажите директорию, в которой находится файл ключа;
- выберите опцию **Копировать файл ключа из директории запуска инсталлятора**, если файл ключа находится в указанной директории.

Дополнительная информация

Опция **Копировать файл ключа из директории запуска инсталлятора** выводится в окне **Выбор варианта установки файла лицензионного ключа** только в том случае, если файл ключа расположен в той же директории, где и исполняемый файл инсталлятора SecurOS.

- *если ключ недоступен* — выберите опцию **Не копировать файл ключа**. Файл ключа может быть скопирован в директорию установки SecurOS после его установки. Подробнее о процедуре получения лицензионного ключа см. раздел **Лицензионный ключ**.

Нажмите кнопку **Далее**.

7. Система выведет окно **Выбор языка программы** (см. рис. 10).

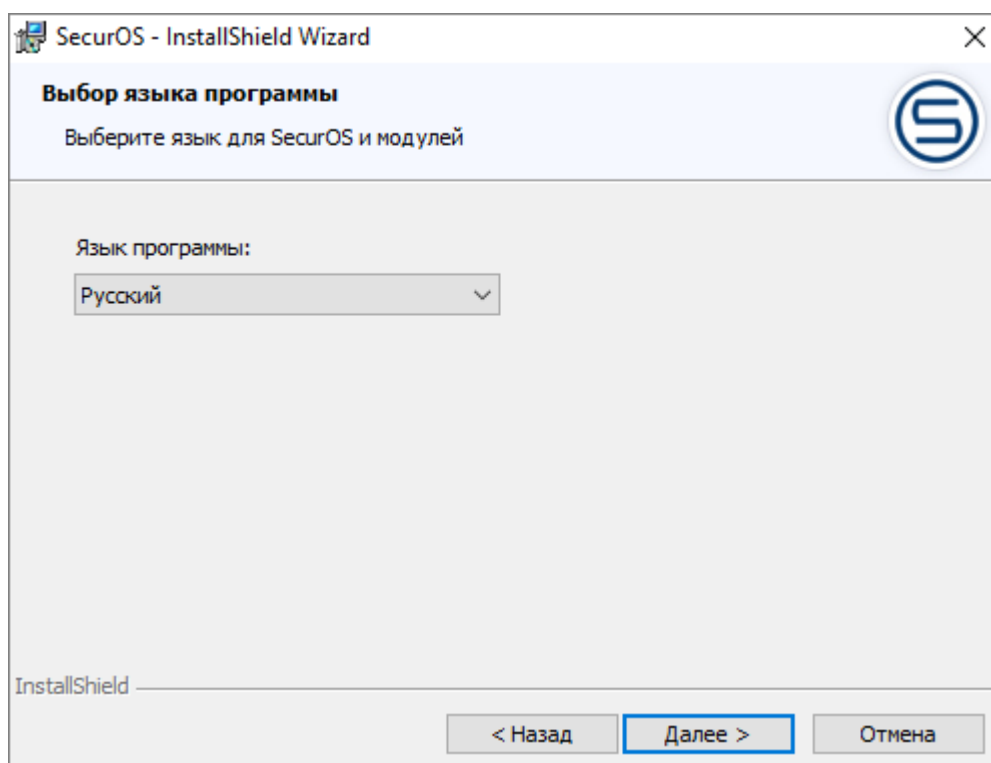


Рис. 10. Окно Выбор языка программы

Для задания языка программы SecurOS выберите из выпадающего списка нужное значение.

Внимание! Язык программы, выбранный на данном шаге установки продукта, должен соответствовать языку, заданному в файле лицензионного ключа. Подробнее о лицензионном ключе см. раздел [Лицензионный ключ](#).

Нажмите кнопку **Далее**.

8. Система выведет окно **Дополнительное программное обеспечение** (см. рис. [11](#)).

В редакции *SecurOS Lite* исключен из процедуры установки.

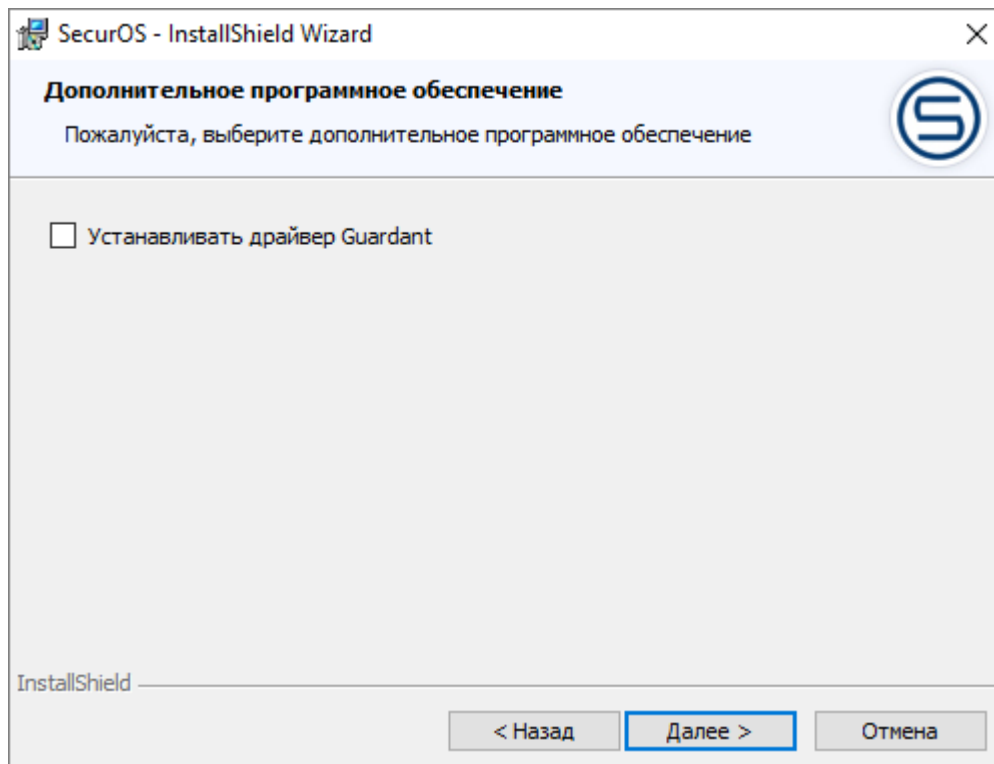


Рис. 11. Окно Дополнительное программное обеспечение

Отметьте флажок **Устанавливать драйвер Guardant**, если у вас USB-ключ Guardant. Для продолжения установки нажмите кнопку **Далее**.

Внимание! Если в настройках ОС включена опция **Целостность памяти**, в окне будет выведено соответствующее информационное сообщение. Возможность установки драйвера Guardant будет заблокирована. Для установки драйвера отключите опцию и перезагрузите компьютер. После установки драйвера не допускайте включения контроля целостности памяти. Это может привести к неполадкам в системе.

9. Система выведет окно **Готов к установке SecurOS** (см. рис. 12).

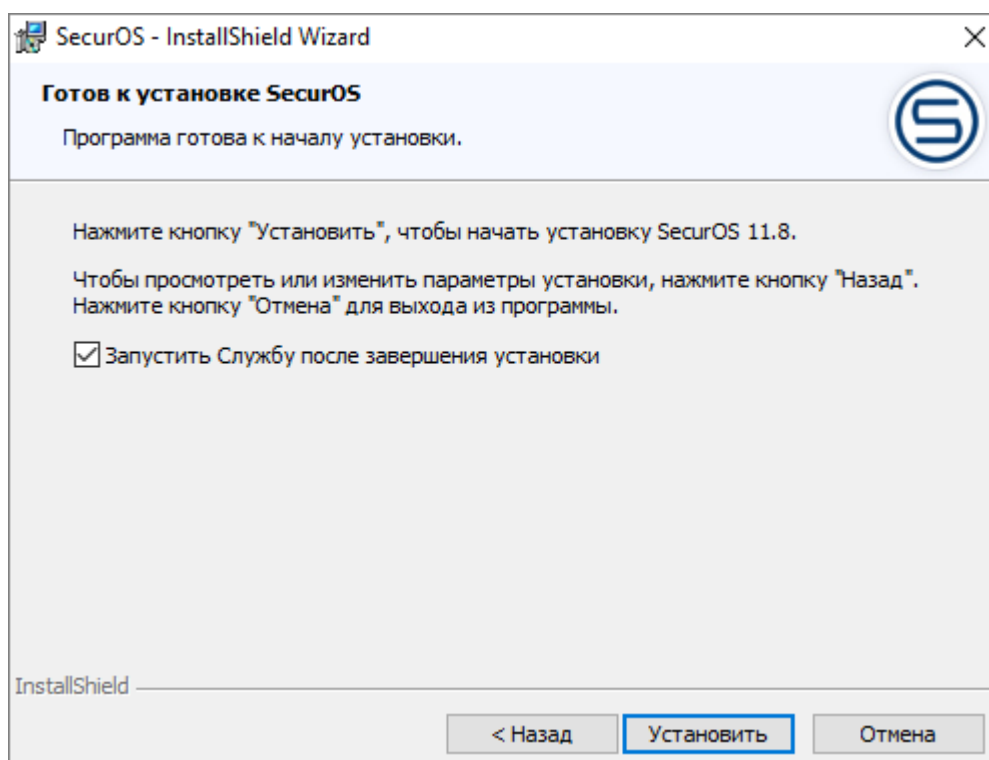


Рис. 12. Окно Готов к установке SecurOS

Если службу Video Management System Server не требуется запускать сразу после окончания установки, снимите отмеченный по умолчанию флажок **Запустить Службу после завершения установки**. Для начала процедуры установки нажмите кнопку **Установить**. Система распакует требуемые архивы, после чего начнет установку и выведет окно **Установка SecurOS**, в котором будет отображаться индикатор выполнения процесса. При успешном завершении установки система выведет окно **Программа InstallShield Wizard завершена** (см. рис. 13).

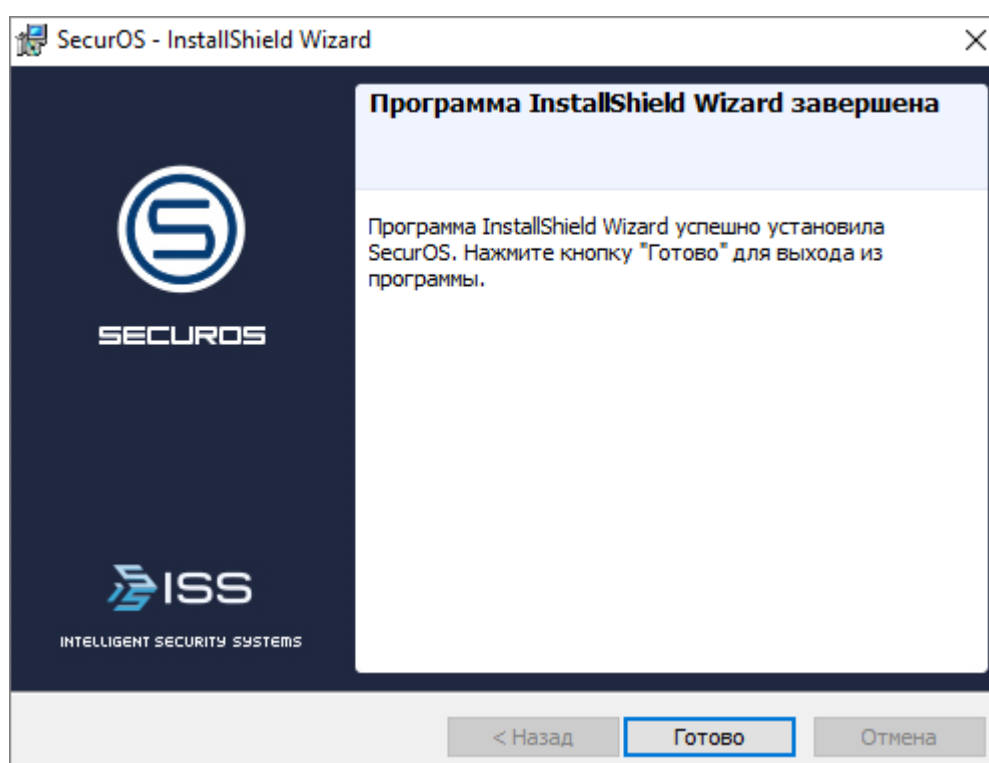


Рис. 13. Окно Программа InstallShield Wizard завершена

Для выхода из программы установки нажмите кнопку **Готово**.

3.1.4 Первоначальная настройка

Первоначальная настройка SecurOS на *Сервере конфигураций* выполняется при помощи *Мастера первоначальной настройки*, который предлагает различные варианты настройки. Базовая настройка, при которой конфигурационные данные вводятся администратором, выполняется с помощью *Мастера первого запуска*. По окончании настройки система будет полностью подготовлена к работе.

3.1.4.1 Настройка при помощи Мастера первоначальной настройки

Для первоначальной настройки SecurOS с помощью Мастера выполните следующие действия:

1. Запустите *Клиентскую часть* SecurOS, для чего в меню **Пуск** Windows выберите папку **SecurOS** → приложение **SecurOS** (см. рис. 14).

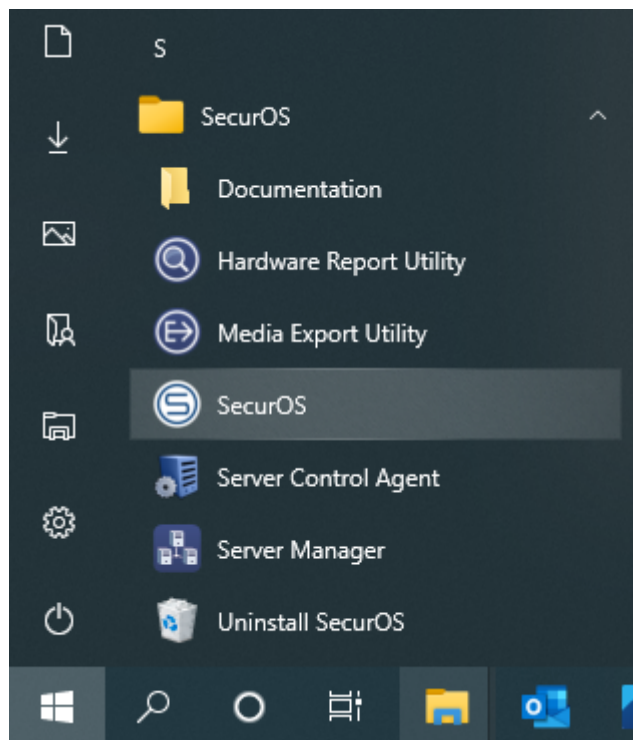


Рис. 14. Меню Пуск

2. При первом запуске *Клиента* на *Сервере конфигураций* запустится *Мастер первоначальной настройки*, в котором необходимо выбрать вариант (сценарий) настройки (см. рис. 15). Для выполнения базовой настройки используйте сценарий *Настроить* с помощью Мастера первого запуска, устанавливаемый по умолчанию.

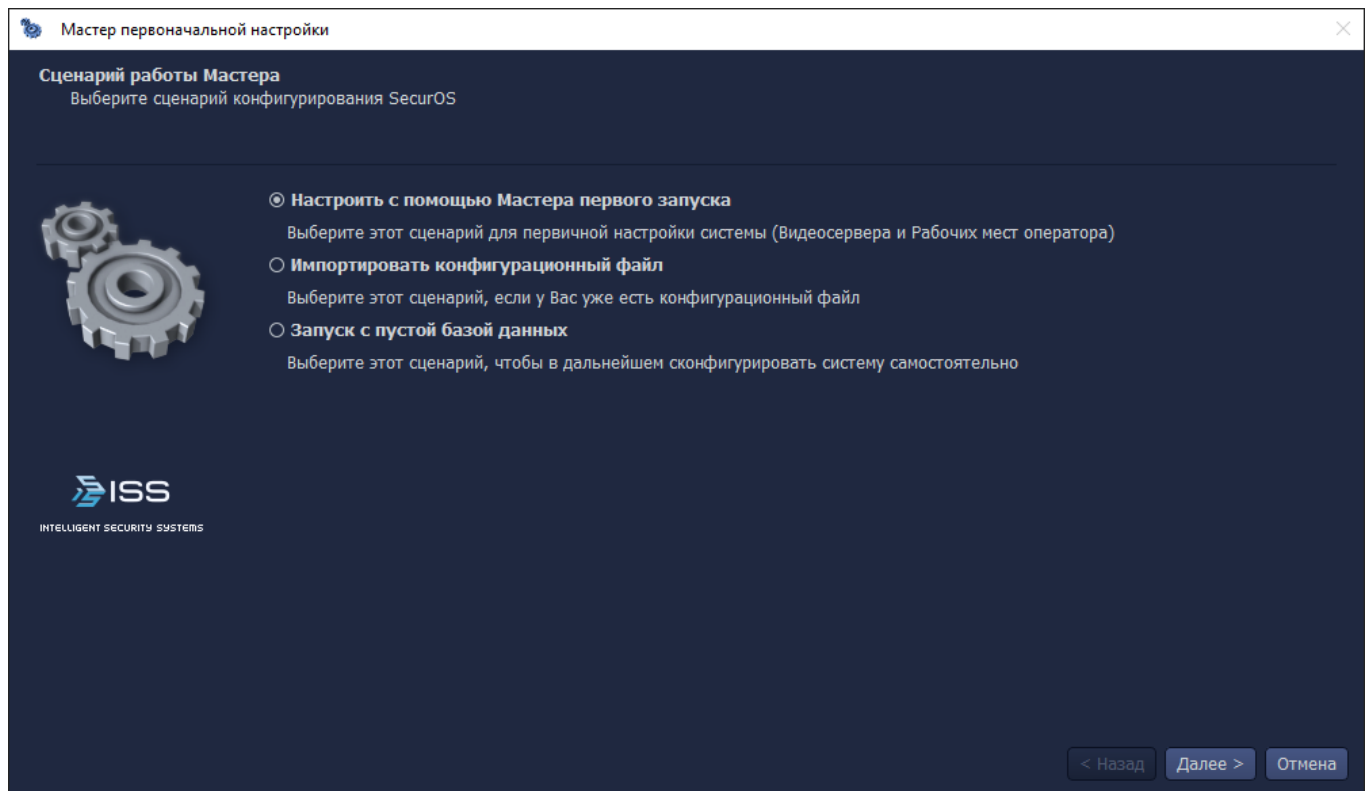


Рис. 15. Окно Сценарий работы Мастера

Нажмите кнопку **Далее**.

Примечание. Процедуры настройки с помощью сценариев **Импортировать конфигурационный файл** и **Запуск с пустой базой данных** описаны ниже.

3. Система выведет окно **Просмотр лицензии** (см. рис. 16).

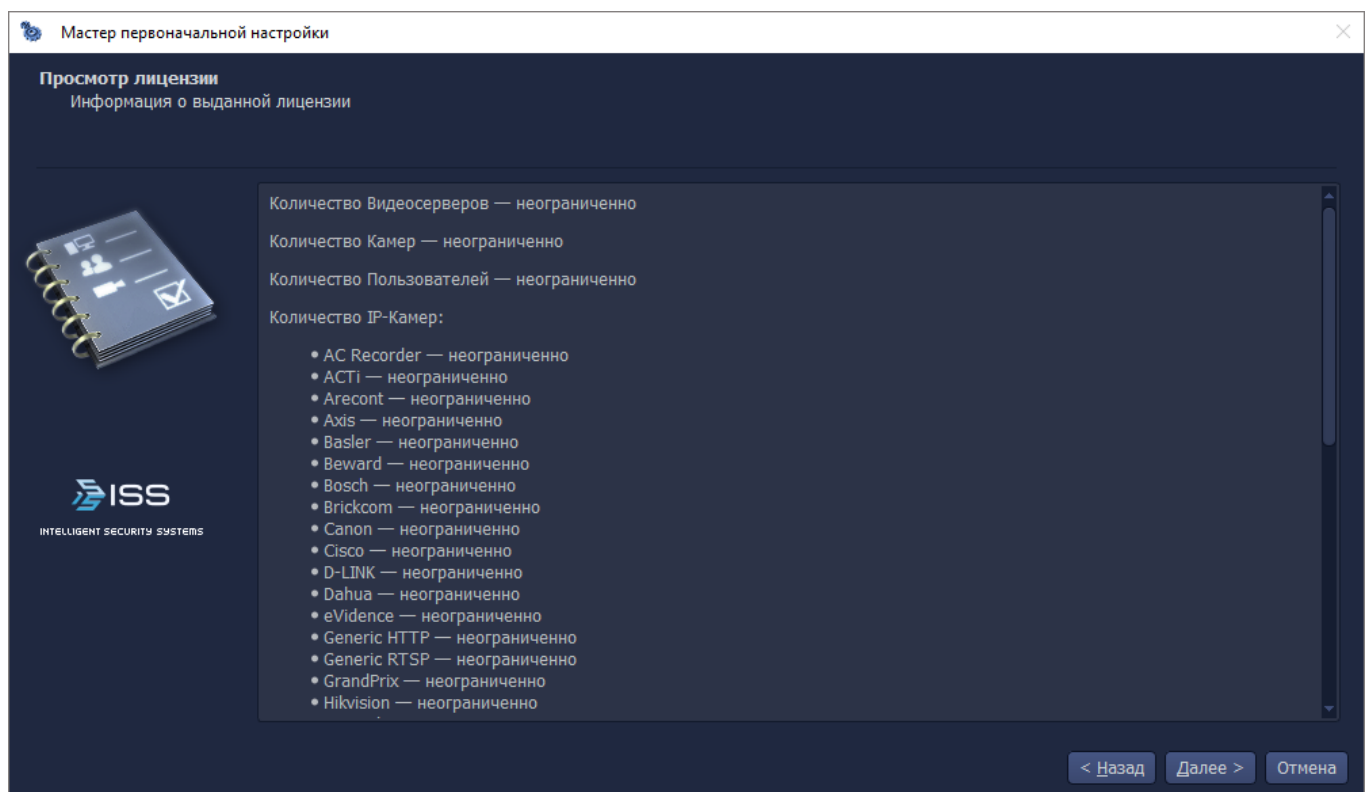


Рис. 16. Окно Просмотр лицензии

В окне отображается информация о лицензионных ограничениях текущей установки SecurOS. Нажмите кнопку **Далее**.

4. Система выведет окно **Настройка пароля суперпользователя** (см. рис. 17).

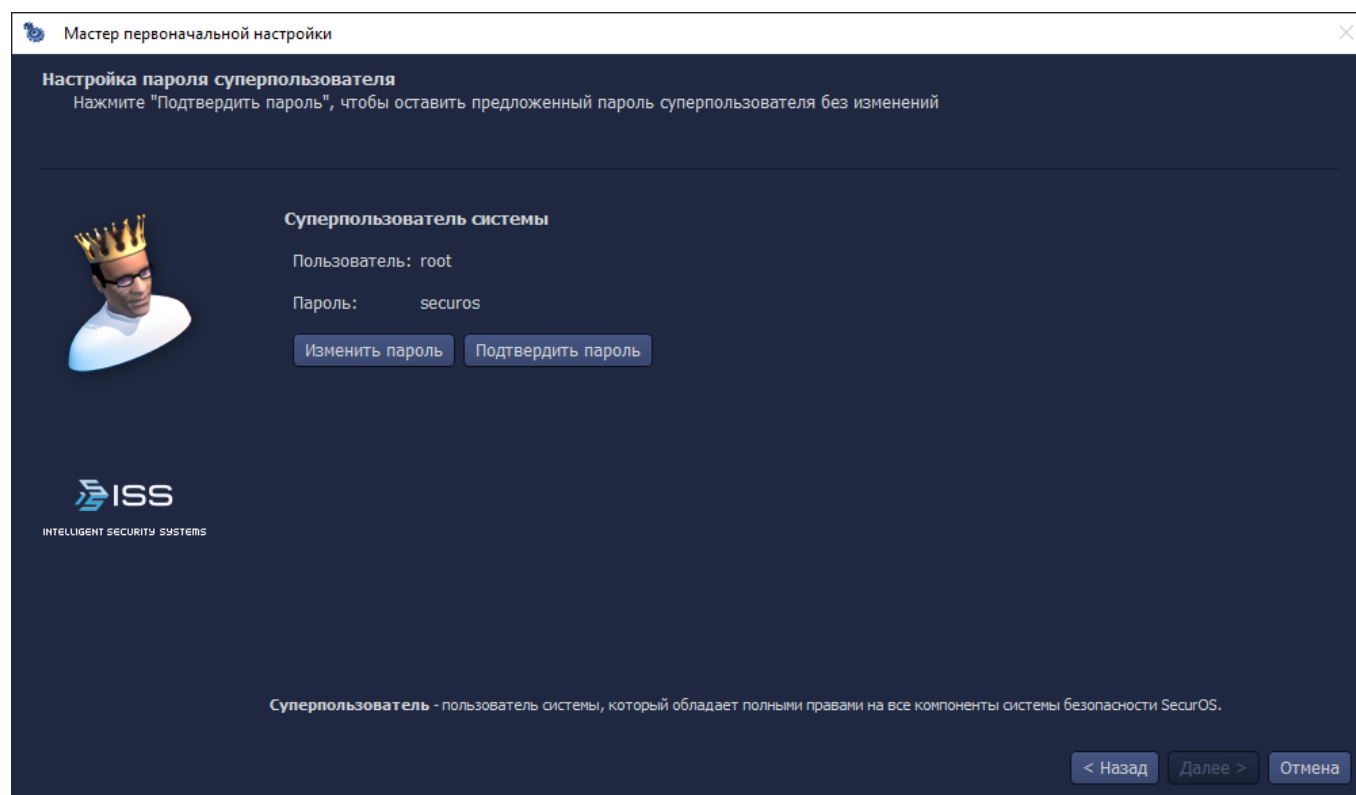


Рис. 17. Окно Настройка пароля суперпользователя

Для подтверждения заданного по умолчанию пароля суперпользователя нажмите кнопку **Подтвердить пароль**. Для смены пароля суперпользователя нажмите кнопку **Изменить пароль**.

Система выведет окно запроса новых параметров (см. рис. 18).

Мастер первоначальной настройки

Настройка пароля суперпользователя
Нажмите "Подтвердить пароль", чтобы оставить предложенный пароль суперпользователя без изменений

Суперпользователь системы

Пользователь: root

Пароль: [masked]

Повторите пароль: [masked]

Значение по умолчанию

ISS
INTELLIGENT SECURITY SYSTEMS

Суперпользователь - пользователь системы, который обладает полными правами на все компоненты системы безопасности SecurOS.

< Назад Далее > Отмена

Рис. 18. Окно запроса новых параметров

В соответствующих полях окна задайте и подтвердите новое значение пароля суперпользователя, либо нажмите кнопку **Значение по умолчанию** для возврата к исходному значению. Для продолжения настройки нажмите кнопку **Далее**.

5. Система выведет окно **Настройка пользователей системы** (см. рис. 19).

Мастер первоначальной настройки

Настройка пользователей системы
Для создания пользователя нажмите кнопку "Добавить пользователя"

Список пользователей:

	Пользователь	Пароль	Права пользователя
1	Пользователь 1	*****	Опытный пользователь
2	Пользователь 2	*****	Простой пользователь

Создано 2 пользователя

Добавить Удалить

< Назад Далее > Отмена

ISS
INTELLIGENT SECURITY SYSTEMS

Рис. 19. Окно Настройка пользователей системы

Добавьте пользователей системы, для чего задайте значения соответствующих полей.

Новые пользователи могут быть созданы со следующими правами учетных записей:

- Опытный пользователь.
- Простой пользователь.

Опытный пользователь может выполнять следующие действия:

- Наблюдать за объектами используя элементы пользовательского интерфейса.
- Управлять камерами видеонаблюдения, например, ставить камеру в режим охраны, начинать и останавливать запись.
- Управлять поворотным устройством (PTZ).
- Скрывать интерфейсы системы.
- Завершать сеанс работы текущего пользователя SecurOS и Клиентского приложения SecurOS.

Простой пользователь может выполнять следующие действия:

- Наблюдать за объектами используя элементы пользовательского интерфейса.
- Завершать сеанс работы текущего пользователя SecurOS и Клиентского приложения SecurOS.

Нажмите кнопку **Далее**.

6. Система выведет окно **Настройки Видеосервера** (см. рис. 20).

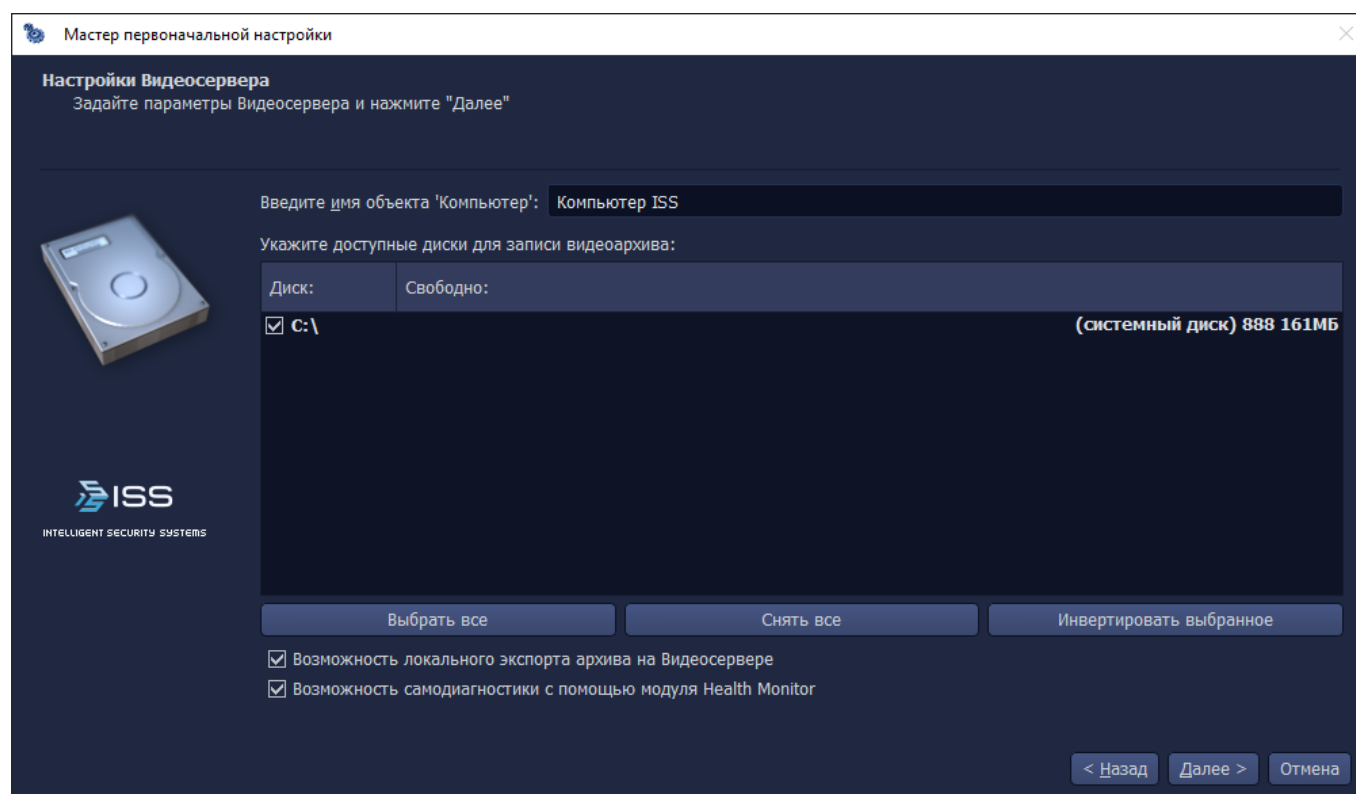


Рис. 20. Окно Имя объекта 'компьютер' и видеоархив

Выполните следующие действия:

- При необходимости измените в поле **Введите имя объекта 'Компьютер'** имя объекта *Компьютер*. По умолчанию имя компьютера задается системой в виде *Компьютер* <"имя_компьютера"> (см. раздел **Ограничения имени компьютера**).
- Выберите диски, на которых будут сохраняться видеозаписи, для чего в поле **Диск** блока **Укажите доступные диски для записи видеоархива** отметьте соответствующие чек-боксы.

SecurOS будет записывать видео и сохранять создаваемые файлы на дисках, указанных на данном этапе настройки.

- Если выполнение операции локального экспорта видеозаписей не предполагается, снимите заданный по умолчанию чек-бокс в поле **Возможность локального экспорта архива на Видеосервере**.

Дополнительная информация

Данный параметр регулирует возможность создания на *Видеосервере* дополнительных объектов, позволяющих сохранять видеозаписи на жесткий диск данного компьютера.

- Если самодиагностика системы на *Видеосервере* встроенными средствами не предполагается, снимите заданный по умолчанию чек-бокс **Возможность самодиагностики с помощью модуля Health Monitor**.

Нажмите кнопку **Далее**.

7. Система выведет окно **Итоговая информация** (см. рис. 21).

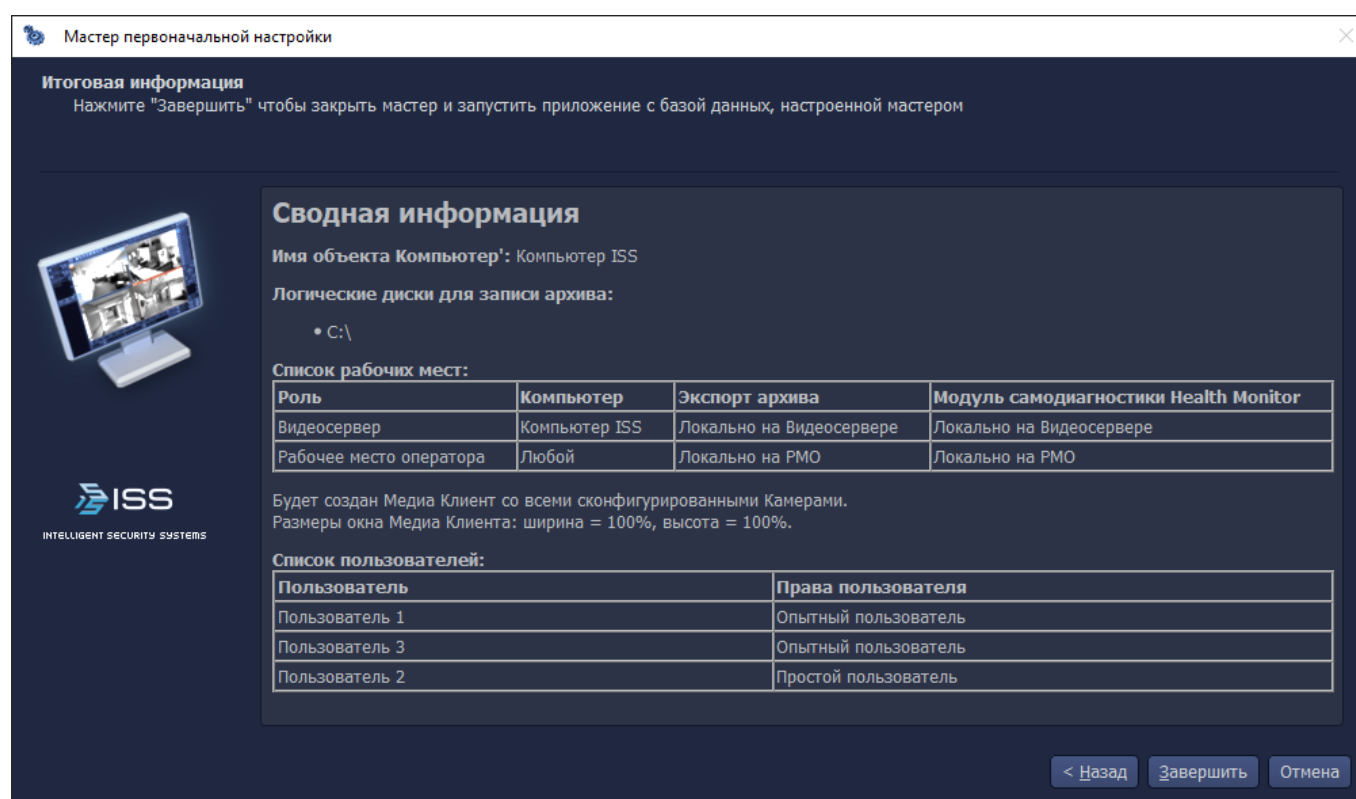


Рис. 21. Окно Итоговая информация

В таблице будет выведена информация о параметрах конфигурации сервера, заданных с помощью *Мастера первоначальной настройки*. Дополнительно к этим параметрам сервер будет сконфигурирован так, что к нему сможет подключиться любое *Рабочее место оператора*, расположенное на любом *Компьютере* сети SecurOS. На каждом из таких *Рабочих мест оператора* будут доступны следующие операции:

- Экспорт архива в форматы AVI и Evidence.
- Самодиагностика системы с помощью модуля *Health Monitor* (см. **Модуль самодиагностики Health Monitor**).

Просмотрите заданные параметры настройки системы. При необходимости изменения заданных значений нажмите кнопку **Назад**. Измените требуемое значение. Нажмите кнопку **Далее** для возврата в окно **Итоговая информация**. Для создания и сохранения конфигурации с заданными параметрами нажмите кнопку **Завершить**.

При успешном завершении процедуры создания и сохранения данных система выведет соответствующее информационное сообщение (см. рис. 22).

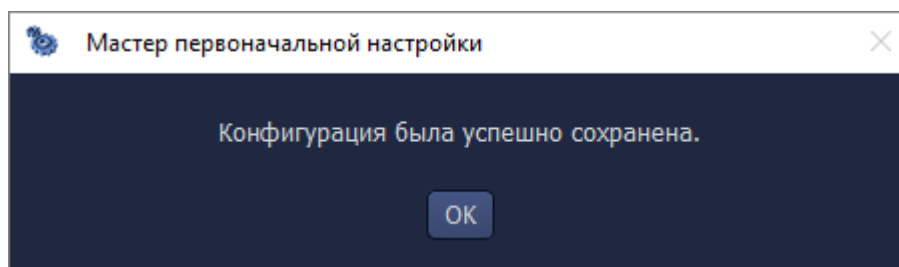


Рис. 22. Сообщение об успешном сохранении конфигурации

В результате выполнения указанных операций система будет полностью подготовлена к работе.

3.1.4.2 Восстановление конфигурации

При необходимости быстрого восстановления системы может быть использована резервная копия файла конфигурации.

Внимание!

1. Восстановление возможно только из той резервной копии файла конфигурации, версия которой соответствует текущей установленной версии SecurOS. Процедура создания резервной копии описана в разделе **Система**.
2. Восстановление конфигурации возможно только на *Сервере конфигураций* (см. раздел **Управление конфигурацией сети с помощью сервера конфигураций**).

Для восстановления конфигурации из резервной копии выберите сценарий **Импортировать конфигурационный файл** в окне **Сценарий работы Мастера** (см. рис. 23).

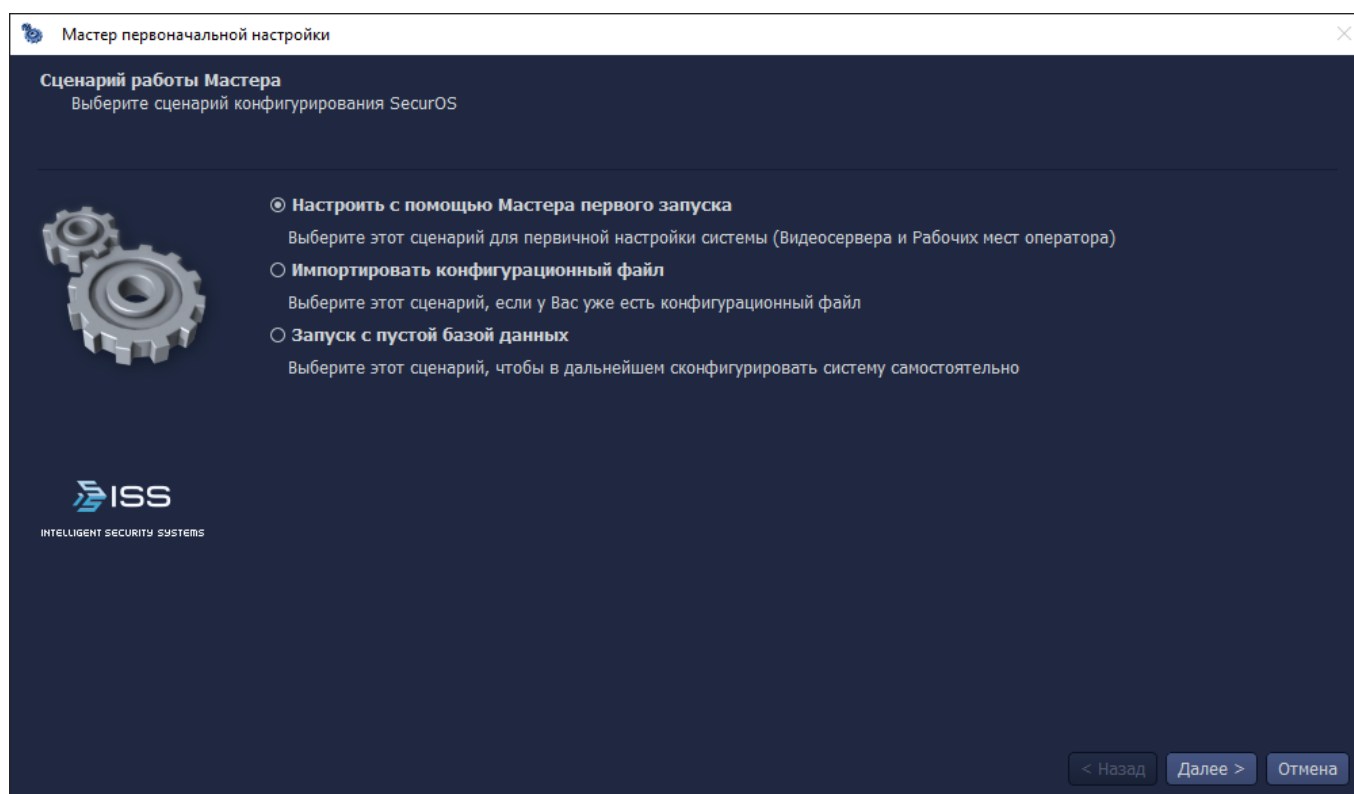


Рис. 23. Окно Сценарий работы Мастера

Для продолжения настройки нажмите кнопку **Далее** и следуйте дальнейшим указаниям Мастера.

3.1.4.3 Запуск с пустой базой данных

Для запуска с пустой базой данных выберите соответствующий сценарий в окне **Сценарий работы Мастера** (см. рис. 23). При использовании данного сценария система запускается с минимальной конфигурацией, содержащей по одному объекту следующих типов: *Объект охраны*, *Компьютер* и *Рабочий стол*. Дальнейшее конфигурирование системы осуществляется в ручном режиме.

3.1.5 Запуск SecurOS на Сервере конфигураций

По умолчанию, *Серверная часть* SecurOS запускается на *Сервере конфигураций* автоматически после завершения установки SecurOS и при каждом запуске ОС.

Для запуска *Клиентской части* SecurOS на *Видеосервере* выполните следующие действия:

Внимание! Для запуска *Клиентской части* SecurOS также может быть использована процедура двухфакторной аутентификации (см. [Двухфакторная аутентификация в SecurOS](#)).

1. В меню **Пуск** Windows выберите папку **SecurOS** → приложение **SecurOS** (см. рис. 24).

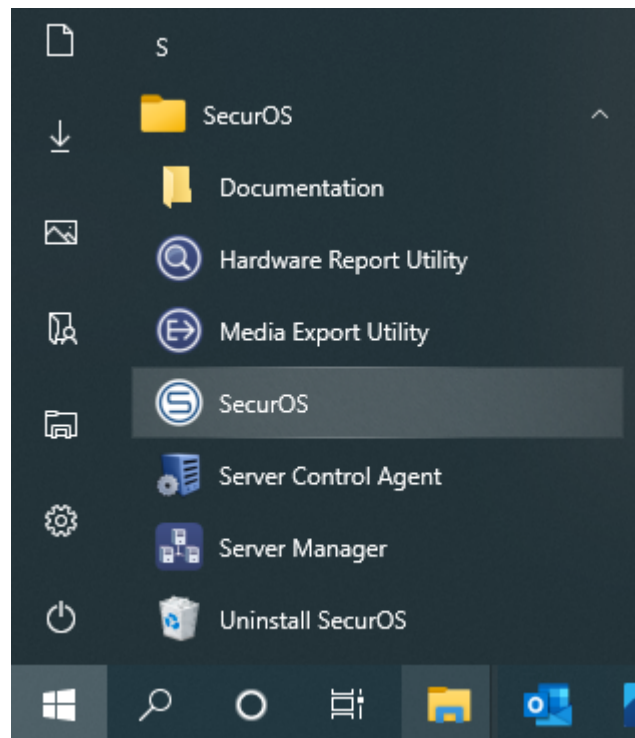


Рис. 24. Меню Пуск

Дополнительная информация

Клиент также может быть запущен с помощью утилиты **Server Control Agent**, ярлыков SecurOS в меню Пуск, на Рабочем столе или в Панели быстрого запуска Windows.

Вход в систему выполняется в окне **Авторизация**, которое выводится системой после успешного запуска и загрузки конфигурации (см. рис. 25).

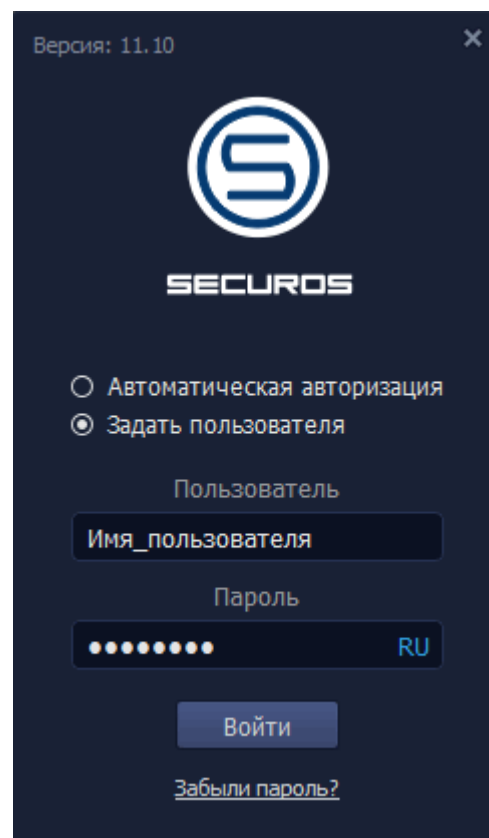


Рис. 25. Окно Авторизация

2. Выберите соответствующую опцию:

- **Автоматическая авторизация** — при выборе данной опции будут автоматически использована учетная запись пользователя, заданного администратором в настройках системы (подробнее см. раздел **Автоматическая авторизация**). При первом запуске данная опция выбрана по умолчанию.

Внимание! Вход в систему с помощью процедуры автоматической авторизации возможен в случае, если такая процедура настроена администратором.

- **Задать пользователя** — при выборе данной опции задайте **Пользователя** и **Пароль**, соответствующие персональным учетным данным *Пользователя* SecurOS.

Внимание! При первом запуске выберите данную опцию и используйте данные учетной записи суперпользователя (см. **Пользователи в SecurOS**) или других пользователей, если они были созданы с помощью Мастера первоначальной настройки.

3. Нажмите кнопку **Войти**.

Примечание. Для сброса пароля с помощью письма на электронную почту нажмите кнопку **Забыли пароль?** (см. **Смена/сброс пароля типового пользователя**). Функциональность не применима к пользователям Active Directory/LDAP, суперпользователю системы (root) и пользователям, использующим автоматическую авторизацию.

Внимание! Если после запуска наблюдаются искажения элементов графического интерфейса SecurOS, настройте автоматическое масштабирование SecurOS (см. **Масштабирование SecurOS при масштабировании Windows**).

4. Если в настройках **Пользователя**, которым осуществляется вход был отмечен флажок **Требовать смену пароля при следующем входе в систему**, то в открывшемся блоке **Новый пароль** введите новый пароль и подтвердите его, а затем нажмите кнопку **Сохранить** (см. рис. 26).

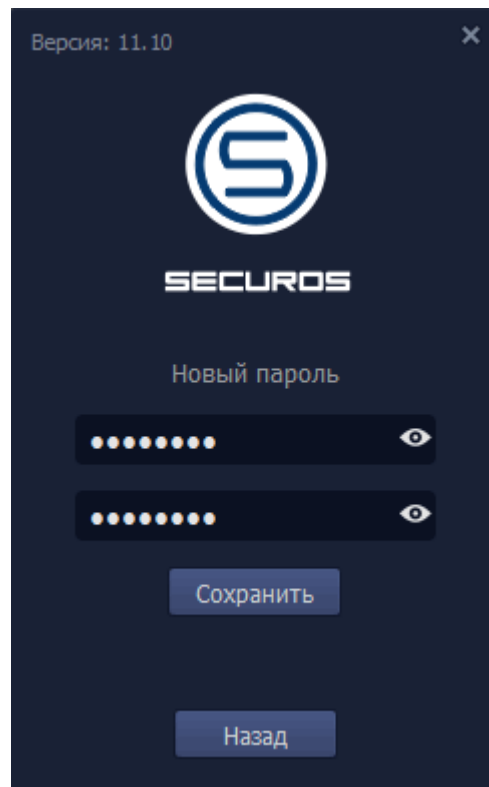


Рис. 26. Окно Авторизация. Блок Новый пароль

3.2 Установка, настройка и запуск Периферийных серверов

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*.

Для добавления в сеть других *Видеосерверов* необходимо выполнить следующие основные операции:

1. Добавить компьютеры в сеть, для чего создать и настроить соответствующие объекты в *Дереве объектов* текущего *Объекта охраны* на *Сервере конфигураций*.
2. Установить на добавленных компьютерах программное обеспечение SecurOS, соответствующее роли *Периферийный сервер* (см. раздел **Виды серверов и рабочих мест**).
3. Запустить SecurOS и выполнить настройку с помощью Мастера первоначальной настройки.

Внимание! Возможность добавления в сеть заданного количества компьютеров определенного типа регулируется лицензионными ограничениями.

3.2.1 Добавление в сеть и настройка Периферийных серверов

Для добавления компьютера в *Дерево объектов* выполните следующие действия:

1. На *Сервере конфигураций* войдите в режим администрирования (см. **Администрирование SecurOS**).
2. В *Дереве объектов* выберите группу *Серверы и Рабочие места*, создайте дочерний объект *Компьютер* с ролью *Видеосервер*.

3. В окне **Параметры создаваемого объекта** задайте необходимые значения:

- В поле **Идентификатор** задайте имя компьютера (см. раздел **Ограничения имени компьютера**). Имя компьютера должно соответствовать значению, заданному в настройках операционной системы (см. **Мой компьютер** → **Свойства** → **Имя компьютера**).
- В поле **Название** задайте имя объекта *Компьютер*, под которым он будет отображаться в *Дереве объектов* SecurOS.

4. В окне настроек параметров объекта (см. рис. 27) задайте следующие обязательные параметры:

Рис. 27. Окно настройки параметров компьютера

- **IP-адрес сервера** — сетевой адрес добавляемого объекта *Компьютер*.

Примечание. Параметр является обязательным только в случае, если компьютеры всей сети безопасности зарегистрированы в разных подсетях.

- **Архив** — диски для сохранения видео и аудиозаписей.

Примечание. Без задания параметра сохранение видео- и аудиозаписей будет невозможно.

5. При необходимости задайте остальные требуемые параметры. Примените новые настройки.
6. Создайте для добавленного объекта *Компьютер* собственное *Дерево объектов*. Вид и состав *Дерева объектов* определяется ролью компьютера в сети.
7. Повторите шаги операции для всех добавляемых в сеть компьютеров.

3.2.2 Установка SecurOS на периферийных серверах

Для установки программного обеспечения SecurOS на периферийных серверах (прочие *Видеосервера*, не являющиеся *Сервером конфигураций*) выполните следующие действия:

1. Для начала установки программного обеспечения SecurOS на периферийных серверах запустите установочный файл продукта на соответствующем компьютере.
2. До этапа выбора типа сервера в окне **Тип сервера**, шаги процедуры аналогичны установке программного обеспечения на *Сервере конфигураций* (см. раздел **Установка программного обеспечения**).
3. В окне **Тип сервера** (см. рис. 28) выберите значение *Периферийный сервер*.

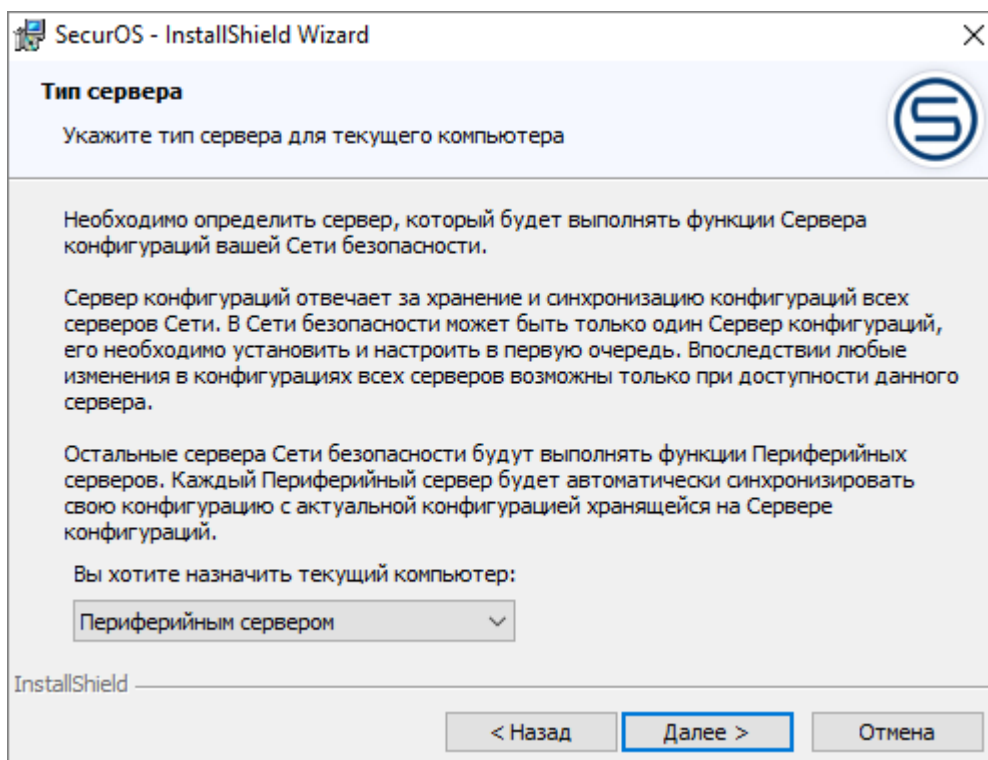


Рис. 28. Окно Тип сервера

4. Дальнейшие шаги процедуры установки аналогичны процедуре установки программного обеспечения на *Сервере конфигураций* (см. раздел **Процедура установки программного обеспечения на Сервере конфигураций**). При выборе параметров рекомендуется использовать значения, предлагаемые системой по умолчанию.

3.2.3 Запуск и настройка SecurOS на периферийных серверах

По умолчанию, *Серверная часть* SecurOS запускается на *Периферийном сервере* автоматически после завершения установки SecurOS и при каждом запуске ОС.

Первоначальная настройка SecurOS на *Периферийном сервере* выполняется с помощью *Мастера первоначальной настройки*. Для первоначальной настройки SecurOS с помощью Мастера выполните следующие действия:

1. Запустите *Клиентское приложение* SecurOS, для чего в меню **Пуск** Windows последовательно выберите пункты меню **Программы** → **SecurOS** → **SecurOS**. При первом запуске *Клиента* запустится *Мастер первоначальной настройки*.

Примечание. Клиент также может быть запущен с помощью утилиты **Server Control Agent**.

2. В окне **Присоединиться к сети безопасности** (см. рис. 29) выберите *Сервер конфигураций*, для чего выполните одну из следующих операций:
- Задайте имя или IP-адрес *Сервера конфигураций* в поле **Имя или IP-адрес конфигурационного сервера**.
 - Для автоматического поиска видеосервера в сети щелкните кнопку **Найти серверы в локальной сети**. Система выполнит поиск и выведет имя *Сервера конфигураций* в поле **Найдены серверы**. Выделите найденный *Сервер конфигураций* мышью.

Внимание! В момент выполнения операции *Сервер конфигураций* должен быть активен и на нем должна быть запущена система SecurOS.

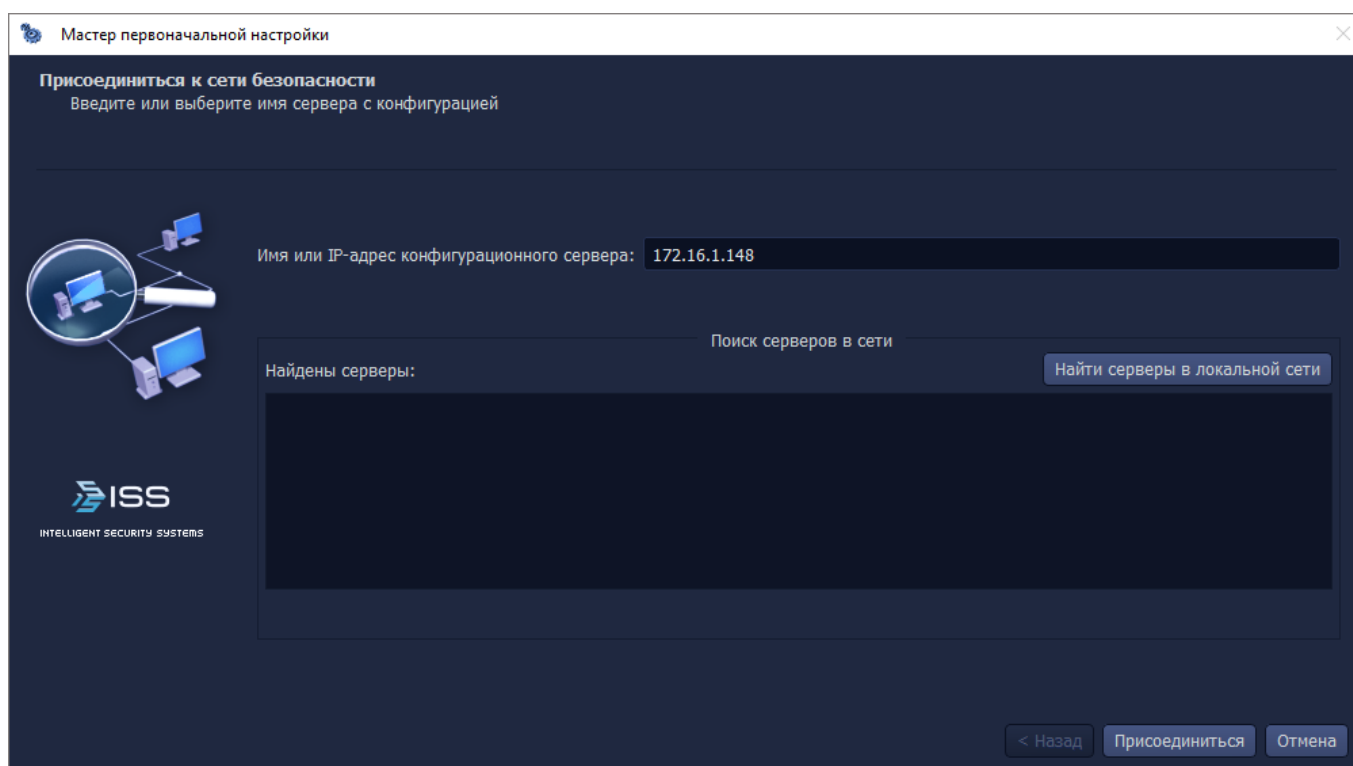


Рис. 29. Окно Присоединиться к сети безопасности

Нажмите кнопку **Присоединиться**. Система выведет окно **Загрузка конфигурации** с индикатором процесса загрузки.

3. После успешной загрузки конфигурации будет выведено соответствующее системное сообщение. Нажмите кнопку **ОК**. В окне **Загрузка конфигурации** нажмите кнопку **Завершить**.

Внимание! Если после запуска наблюдаются искажения элементов графического интерфейса SecurOS, настройте автоматическое масштабирование SecurOS (см. **Масштабирование SecurOS при масштабировании Windows**).

3.3 Установка, настройка и запуск Рабочих мест оператора

Для подготовки *Рабочего места оператора* к эксплуатации достаточно установить программное обеспечение SecurOS на компьютер. Процесс установки описан в разделе [Установка SecurOS на Рабочем месте оператора](#).

Запуск интерфейса на *Рабочем месте оператора* возможен сразу после установки (см. [Запуск SecurOS на Рабочем месте оператора](#)). Для подключения к *Видеосерверу* достаточно знать его IP-адрес или DNS/WINS-имя. Изначально возможен лишь доступ к средствам администрирования SecurOS: *Панели управления* и *Дереву объектов*.

Примечание. Средства администрирования доступны только при наличии у пользователя SecurOS прав на конфигурирование системы (см. [Права пользователя](#)).

Для дальнейшей работы необходимо сформировать оператору *Рабочее окружение*, которое представляет собой совокупность элементов интерфейса для мониторинга и других возможностей.

Существует два вида *Рабочего окружения*:

- **Профильное окружение.** Такое *Рабочее окружение* соответствует конфигурации *Профиля Рабочего места оператора* (см. [Профили Рабочих мест оператора](#)). Оно может быть использовано на любом количестве компьютеров.
- **Локальное окружение.** Такое *Рабочее окружение* соответствует конфигурации, созданной для объекта *Компьютер* с идентификатором, совпадающим с DNS/WINS-именем компьютера, за которым работает оператор. Оно может быть использовано только на этом компьютере. Использование локального окружения позволяет выполнять некоторые операции только на определенных компьютерах. *Рабочие места оператора*, использующие локальное окружение, называются **фиксированными**. Процесс добавления фиксированного *Рабочего места оператора* описан в разделе [Фиксированные Рабочие места оператора](#).

Примечания:

1. *Профили Рабочих мест оператора* могут быть использованы в том числе и на фиксированных *Рабочих местах оператора*.
 2. Локальное окружение по умолчанию доступно для *Видеосерверов*, на которых запускается интерфейс оператора.
-

3.3.1 Установка SecurOS на Рабочем месте оператора

Для установки программного обеспечения SecurOS на *Рабочем месте оператора* выполните следующие действия:

1. Для начала установки программного обеспечения SecurOS на рабочем месте оператора запустите установочный файл продукта.
2. До этапа выбора типа установки в окне **Настройка установки**, шаги процедуры аналогичны установке программного обеспечения на видеосервере (см. раздел [Установка программного обеспечения](#)).
3. В окне **Настройка установки** выберите тип **Установка с расширенными настройками**.
4. В окне **Тип установки** (см. рис. 30) выберите тип установки **Рабочее место оператора**.

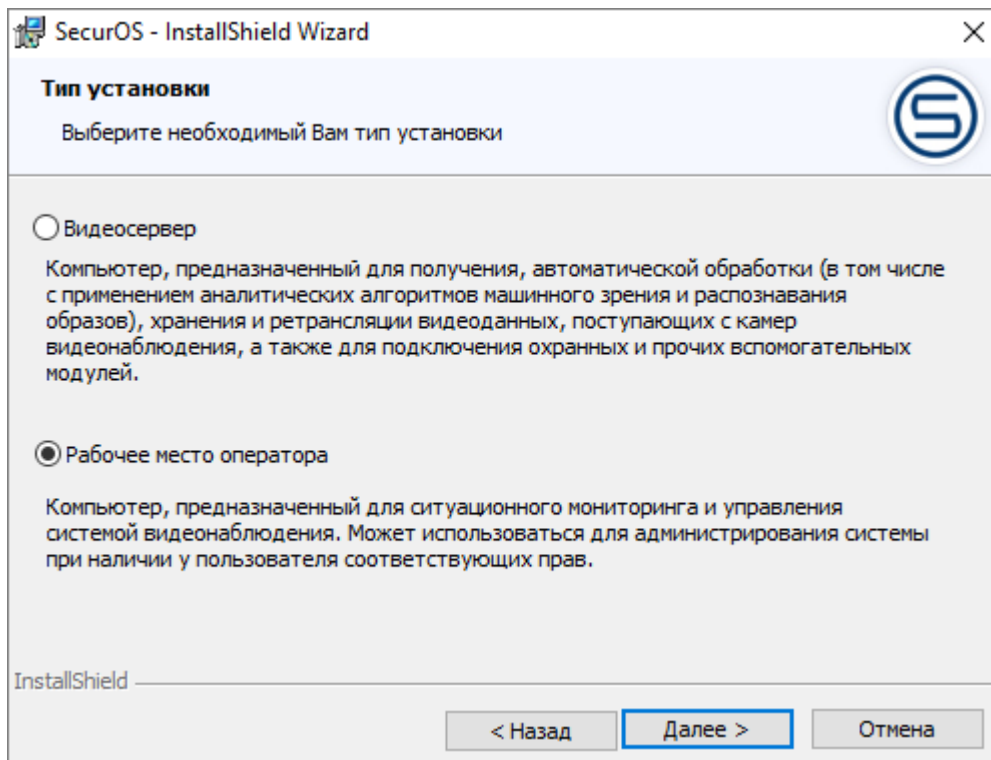


Рис. 30. Окно Тип установки

5. Следуйте дальнейшим инструкциям мастера установки.

3.3.2 Профили Рабочих мест оператора

Профили Рабочих мест оператора определяют внешний вид интерфейса оператора и доступные в нем модули. Каждый профиль может быть использован для неограниченного количества *Рабочих мест оператора*. Это обеспечивает единообразие интерфейса и упрощает внесение изменений. Любое изменение профиля автоматически применится на всех *Рабочих местах оператора*, которые его используют.

Чтобы предоставить операторам возможность использовать профиль, необходимо создать и настроить его (см. [Создание Профиля рабочего места оператора](#)), а затем выбрать на *Рабочем месте оператора* в качестве *Рабочего окружения* (см. [Выбор Рабочего окружения](#)).

Примечание. Доступность *Рабочего окружения* оператору определяется настройками системы. Ограничить доступ оператора к профилям позволяют [Права пользователя](#). Профиль доступен оператору при наличии на него прав уровня  ([Просмотр](#)) и выше.

3.3.2.1 Ограничения в использовании

При использовании *Рабочего окружения* (за исключением *Локального окружения*) на *Рабочем месте оператора* не поддерживается работа со следующими объектами и Модулями:

- [Active Camera Recorder \(AC Recorder\)](#).
- Интеграция RUSGUARD.

При использовании *Рабочего окружения* также налагаются ограничения на работу со *Скриптами Node.js* и сообщениями SecurOS:

- Чтобы *Скрипт Node.js* выполнялся на *Рабочем месте оператора*, он должен быть создан на том *Компьютере*, профиль которого используется этим *Рабочим местом оператора* в качестве *Рабочего окружения*. Если *Рабочее место оператора* использует *Локальное рабочее окружение*, *Скрипт Node.js* должны быть создан на текущем *Компьютере*.
- Сообщения SecurOS (события и команды), полученные на *Рабочем месте оператора*, использующем *Рабочее окружение*, далее в сеть SecurOS не передаются.

3.3.2.2 Создание Профиля Рабочего места оператора

Профиль Рабочего места оператора представлен в конфигурации SecurOS объектом *Компьютер* и его дочерними объектами. Чтобы создать профиль, выполните следующие действия:

1. Войдите в режим администрирования (см. [Администрирование SecurOS](#)).
2. В *Дереве объектов* выберите группу *Серверы и Рабочие места*, создайте дочерний объект *Компьютер*.
3. В окне **Параметры создаваемого объекта** введите необходимые значения:
 - В поле **Идентификатор** введите любое значение, удовлетворяющее требованиям к идентификатору (см. [Ограничение имени компьютера](#)). Для профилей идентификатор не обязан совпадать с DNS\WINS-именем компьютера.
 - В поле **Название** введите название, соответствующее назначению *Профиля* (например, **Охрана здания**). Это название будет отображаться в списке доступных оператору *Рабочих окружений*.
 - В выпадающем списке **Роль** выберите вариант *Рабочее место оператора*.
4. В окне настройки параметров компьютера (см. рис. 31) отметьте флажок **Использовать как Профиль Рабочего места оператора**.

Роль Компьютера: **Рабочее место оператора**

☒ Использовать как Профиль Рабочего места оператора

IP-адрес сервера:

☐ Резервировать Видеосервер и добавить его в кластер

Архив

Режим записи: ☒ Оптимальная производительность ☐ Экономия места

Директория		Емкость		Видео		Аудио	
				Чтение	Запись	Чтение	Запись

Добавить директорию Изменить Удалить

Старт системы

☒ Активировать Рабочий стол:

Автоматически

Автоматическая авторизация разрешена для Пользователя:

Локальная База данных

☐ Отключить локальный протокол

☐ Записывать дополнительные параметры событий в протокол

Использовать Фильтр событий:

Не использовать

Максимальный размер БД: 0 МБ

Закладки и Тревоги

База данных для записи:

Локальная (настраивается в DSAdmin)

☒ Удалять вместе с оперативным архивом

☐ Хранить: 7 дней

База данных СКУД/ОПС:

Не используется

OK Отмена Применить

Рис. 31. Окно настройки параметров компьютера

5. Для данного *Компьютера* создайте все необходимые оператору дочерние объекты интерфейса (например, *Медиа Клиент*, *Протокол событий*). Выполните настройку этих объектов согласно вашим требованиям к этому профилю (например, задайте режим работы и размеры *Медиа Клиента*, определите список доступных в нем *Камер*).

С этого момента созданный профиль может быть выбран оператором в качестве *Рабочего окружения* (см. **Выбор Рабочего окружения**).

3.3.3 Фиксированные Рабочие места оператора

В некоторых случаях может быть необходимо, чтобы определенный функционал был доступен операторам только на конкретных компьютерах. Для решения этой задачи следует использовать фиксированные *Рабочие места оператора*.

Для фиксированных *Рабочих мест оператора* в качестве основного *Рабочего окружения* используется **Локальное окружение**.

3.3.3.1 Добавление в сеть и настройка фиксированных Рабочих мест оператора

Фиксированные *Рабочие места оператора* представлены в конфигурации SecurOS объектами *Компьютер*. Для добавления компьютера в сеть выполните следующие действия:

1. Войдите в режим администрирования (см. **Администрирование SecurOS**).
2. В *Дереве объектов* выберите группу *Серверы и Рабочие места*, создайте дочерний объект *Компьютер*.
3. В окне **Параметры создаваемого объекта** введите необходимые значения:
 - В поле **Идентификатор** введите имя компьютера (см. раздел **Ограничения имени компьютера**). Имя компьютера должно соответствовать значению, заданному в настройках операционной системы (см. **Мой компьютер** → **Свойства** → **Имя компьютера**).
 - В поле **Название** введите имя объекта *Компьютер*, под которым он будет отображаться в *Дереве объектов* SecurOS.
 - В выпадающем списке **Роль** выберите вариант *Рабочее место оператора*.

Рис. 32. Окно настройки параметров компьютера

4. При необходимости задайте остальные параметры (см. рис. 32). Примените новые настройки.
5. Создайте для добавленного объекта *Компьютер* все необходимые дочерние объекты. Их набор определяется задачами этого *Рабочего места оператора*.
6. Повторите шаги операции для всех добавляемых в сеть *Рабочих мест оператора*.

3.3.4 Запуск SecurOS на Рабочем месте оператора

Для запуска *Интерфейса оператора SecurOS* на *Рабочем месте оператора* выполните следующие действия:

1. В меню **Пуск** Windows последовательно выберите пункты **Программы** → **SecurOS** → **SecurOS**.
2. В окне **Авторизация** (см. рис. 33) в поле **Сервер для подключения** задайте IP-адрес *Видеосервера*, к которому следует подключиться.
3. Выберите соответствующую опцию:
 - **Автоматическая авторизация** — при выборе данной опции будет автоматически использована учетная запись пользователя, заданного администратором в настройках системы. При первом запуске данная опция выбрана по умолчанию.

Внимание! Вход в систему с помощью процедуры автоматической авторизации возможен в случае, если такая процедура настроена администратором (см. [Автоматическая авторизация](#)).

- **Задать пользователя** — при выборе данной опции задайте **Пользователя** и **Пароль**, соответствующие персональным учетным данным *Пользователя*, созданного администратором ранее, или используйте учетную запись суперпользователя (см. [Пользователи в SecurOS](#)).
4. Нажмите кнопку **Войти**.

Внимание! Для запуска Интерфейса оператора SecurOS также может быть использована процедура двухфакторной аутентификации (см. [Двухфакторная аутентификация в SecurOS](#)).

Примечание. Для сброса пароля с помощью письма на электронную почту нажмите кнопку **Забыли пароль?** (см. [Смена/сброс пароля типового пользователя](#)). Функциональность не применима к пользователям Active Directory/LDAP, суперпользователю системы (root) и пользователям, использующим автоматическую авторизацию.

Детальное описание процедуры авторизации пользователя приведено в документе [Краткое руководство пользователя SecurOS](#).

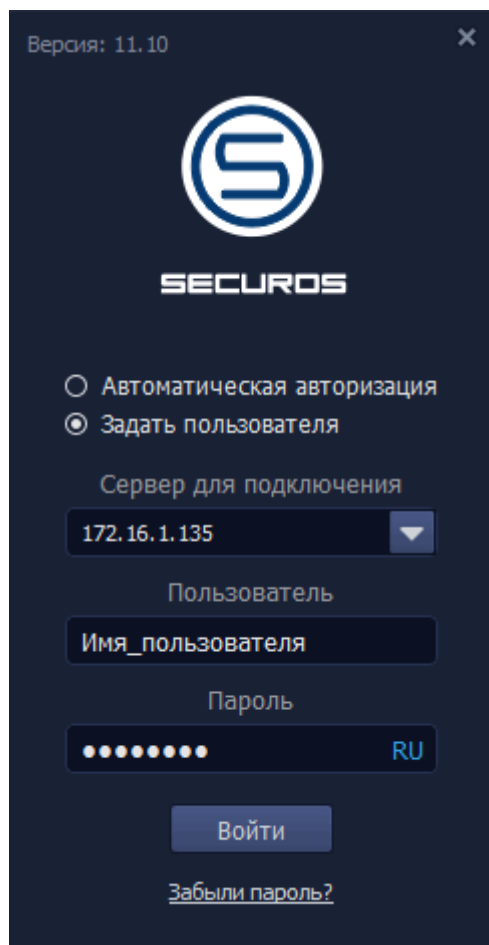


Рис. 33. Окно Авторизация

5. Если в настройках [Пользователя](#), которым осуществляется вход был отмечен флажок **Требовать смену пароля при следующем входе в систему**, то в открывшемся блоке **Новый пароль** введите новый пароль и подтвердите его, а затем нажмите кнопку **Сохранить** (см. рис. [34](#)).

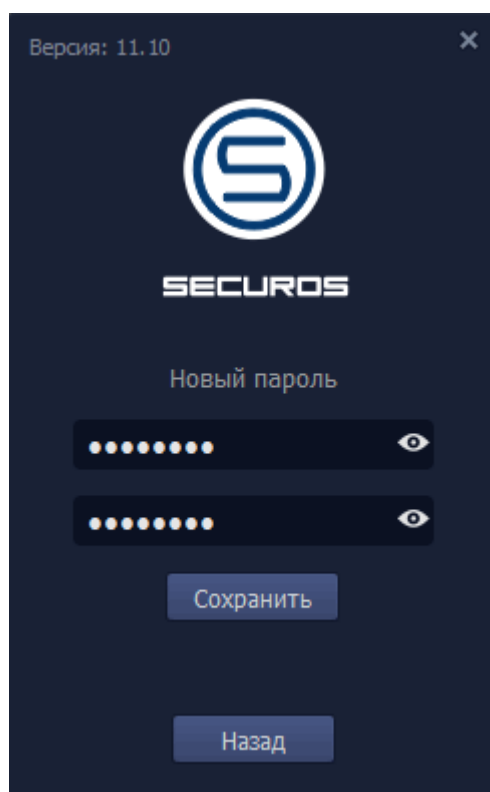


Рис. 34. Окно Авторизация. Блок Новый пароль

6. После успешной авторизации на экране отобразится интерфейс оператора. При первом подключении *Рабочее окружение* будет выбрано автоматически. Если для этого компьютера существует локальное окружение, будет использовано именно оно. В противном случае будет использовано случайное из доступных профильных окружений. В дальнейшем оператор может изменить *Рабочее окружение* (см. [Выбор Рабочего окружения](#)).

Примечания:

1. Возможность подключения к серверу регулируется настройками *Объекта охраны* (см. [Объект охраны](#)) и *Прав пользователя* (см. [Права пользователя](#)). *Права пользователя* также определяют доступные *Рабочие окружения*.
2. Для фиксированных *Рабочих мест оператора* в системе предусмотрена автоматическая авторизация того пользователя, для которого такая возможность настроена администратором. Для использования процедуры автоматической авторизации выберите опцию **Автоматическая авторизация**. Детальное описание процедуры настройки автоматической авторизации приведено ниже (см. описание параметров настройки объекта [Компьютер](#) и раздел [Автоматическая авторизация](#)).

Внимание! Если после запуска наблюдаются искажения элементов графического интерфейса SecurOS, настройте автоматическое масштабирование SecurOS (см. [Масштабирование SecurOS при масштабировании Windows](#)).

3.4 Порядок обновления SecurOS

Корректная работа SecurOS гарантируется в случае, если версии ПО SecurOS, установленного на каждом компьютере системы, совпадают.

Обычно обновление выполняется на всех компьютерах какой-либо системы одновременно. Если одновременно остановить SecurOS на всех компьютерах сети невозможно, обновление ПО должно выполняться в следующем порядке:

1. Остановите, обновите ПО и запустите SecurOS на *Сервере конфигураций*.
2. Последовательно остановите, обновите ПО и запустите SecurOS на *Периферийных серверах*.
3. Последовательно остановите, обновите ПО и запустите SecurOS на *Рабочих местах оператора*.

Обновление следует проводить с учетом следующих ограничений:

- Во время обновления крайне не рекомендуется изменять конфигурацию системы. В противном случае те *Периферийные сервера*, ПО на которых не обновлено, не смогут получить измененную конфигурацию от обновленного *Сервера конфигураций*.
- Обновление ПО на *Периферийном сервере* следует проводить только в том случае, если *Сервер конфигураций* включен и доступен по сети с того компьютера, на котором выполняется обновление.

При обновлении также необходимо учитывать особенности, характерные для некоторых версий SecurOS (см. раздел **Особенности обновления версий SecurOS** в Приложении 1).

Процедура обновления ПО на отдельном компьютере описана в Приложении 1 (см. **Обновление программного обеспечения**).

4 Установка и обновление SecurOS на Linux

Данный раздел описывает последовательность шагов, необходимых для создания сети безопасности SecurOS и начала ее эксплуатации на платформе Linux.

Внимание! Убедитесь, что в настройках брандмауэра открыты все необходимые порты (см. [Приложение 5. Используемые в SecurOS сетевые порты](#)).

В первую очередь необходимо подготовить *Видеосерверы* (см. [Виды серверов и рабочих мест](#)). Порядок установки SecurOS на *Видеосерверы* описан в следующих разделах:

- [Установка, настройка и запуск Сервера конфигураций](#);
- [Установка, настройка и запуск Периферийных серверов](#).

Затем следует подготовить *Рабочие места оператора*. Порядок установки SecurOS на *Рабочие места оператора* описан в соответствующем разделе:

- [Установка, настройка и запуск Рабочих мест оператора](#).

Внимание!

1. На всех *Видеосерверах* и *Рабочих местах операторов* необходимо установить все компоненты всех интеллектуальных Модулей SecurOS, которые используются в системе.
2. Язык устанавливаемого программного обеспечения должен быть единым для всех подключаемых к сети компьютеров.
3. Системное время всех *Видеосерверов* в конфигурации должно быть синхронизировано.
4. Установка программного обеспечения SecurOS возможна только на компьютерах, имена которых соответствуют требованиям раздела [Ограничения имени компьютера](#).

4.1 Установка, настройка и запуск Сервера конфигураций

В данном разделе описываются операции установки и настройки управляющего сервера SecurOS.

4.1.1 Установка аппаратного обеспечения

В данном разделе содержится краткая информация о дополнительных аппаратных средствах, которые могут быть включены в комплект поставки продукта. К таким аппаратным средствам относятся ключи Guardant, контролирующие лицензионные ограничения.

4.1.1.1 Установка ключа Guardant

Ключ Guardant является электронным устройством, постоянно подключенным к компьютеру через USB-порт. Программное обеспечение SecurOS обращается к ключу для проверки лицензионной информации.

На платформе ОС Linux применяются электронные ключи Guardant Sign. Для подготовки ключей Guardant Sign к работе выполните операции, описанные в статье [Установка ключей Guardant в операционных системах GNU/Linux](#).

Внимание!

1. Установка ПО Guardant Sign выполняется до первоначальной настройки ПО SecurOS (см. [Первоначальная настройка](#)).
2. Перед запуском файла `install.sh` ему необходимо добавить разрешение на выполнение с помощью команды `sudo chmod +x install.sh`.

4.1.2 Лицензионный ключ

Лицензионный ключ определяет возможную конфигурацию сети безопасности и необходим для запуска SecurOS.

Лицензионный ключ создается на основе уникальных кодов аппаратных средств SecurOS (Guardant) или комбинации уникальных кодов аппаратных средств компьютера, на котором предполагается установка SecurOS.

При проверке лицензии ключи рассматриваются в соответствии со снижением приоритета в следующем порядке:

1. ключ Guardant;
2. ключ на основе комбинации уникальных кодов аппаратных средств компьютера (hardware-код).

Кроме уникальных кодов оборудования при генерации лицензионного ключа также учитываются следующие данные:

- язык программы, выбранный при установке SecurOS;
- язык по умолчанию установленной операционной системы (параметр **Language** (*local ID*));
- номер релиза SecurOS;
- редакция SecurOS.

В зависимости от варианта поставки продукта лицензионный ключ может предоставляться одним из следующих способов:

- в комплекте поставки оборудования, на компакт-диске с программным обеспечением;
- по электронной почте.

4.1.2.1 Заказ ключа по электронной почте

В случае, если лицензионный ключ не входит в комплект поставки SecurOS, его необходимо заказать в Intelligent Security Systems.

Для оформления заказа выполните следующие действия:

1. Установите аппаратное и программное обеспечение SecurOS на компьютер.
2. Запустите консольное приложение *Терминал*.

3. Перейдите в директорию установки SecurOS (по умолчанию `opt/iss/securos`). Для этого выполните следующую команду:

```
cd <директория_установки_SecurOS>
```

4. Запустите исполняемый файл утилиты (см. [Утилита Hardware Report Utility](#)). Для этого выполните следующую команду:

```
./hru
```

Результат выполнения команды представлен на рис. 35.



```
user@computer:~$ cd /opt/iss/securos
user@computer:/opt/iss/securos$ ./hru
Guardant:
000000003EAB5D26

Hardware:
2AEE1A4F0C32B70F6ABEC98FEDC72E59

user@computer:/opt/iss/securos$
```

Рис. 35. Результат выполнения команды `./hru` в консоли

4. Скопируйте данные, выведенные в результате выполнения команды.
5. Создайте и откройте новый текстовый файл любого формата. Вставьте в файл содержимое буфера обмена. Дополнительно укажите следующие значения:
 - язык программы, выбранный при установке SecurOS;
 - номер релиза SecurOS;
 - редакцию SecurOS.
6. Сохраните файл.
7. Отправьте файл с данными в Службу технической поддержки Intelligent Security Systems (см. раздел [Обращение за технической поддержкой](#)).

После получения файла лицензионного ключа скопируйте его в директорию установки SecurOS.

4.1.3 Установка программного обеспечения на Сервере конфигураций

Внимание!

1. Перед началом установки вставьте диск с дистрибутивом Linux в дисковод или смонтируйте сетевой диск с образами установочных дисков Linux.
2. Создайте на жестком диске директорию, в которую скопируйте дистрибутив устанавливаемого ПО SecurOS.
3. В эту же директорию скопируйте файл лицензионного ключа SecurOS `key.iss`.

В зависимости от варианта поставки дистрибутива ПО SecurOS, для установки используется один из следующих методов:

- **Установка с использованием .deb-файла.**
- **Установка с использованием .run-файла.**

Установка с использованием .deb-файла

Для установки используется файл `securos_XXX-YYY_amd64.deb`, где XXX — версия ПО SecurOS, YYY — версия операционной системы.

Для установки ПО на *Видеосервере* выполните следующие действия:

1. Запустите консольное приложение *Терминал*.
2. Для перехода в директорию, куда был скопирован установочный файл SecurOS (<директория_с_дистрибутивом_SecurOS>), выполните следующую команду:

```
cd <директория_с_дистрибутивом_SecurOS>
```

3. Для начала установки программного обеспечения SecurOS запустите установочный файл продукта (например, `securos_11.4-deb10_amd64.deb`) следующей командой:

```
sudo apt install ./securos_11.4-deb10_amd64.deb
```

4. При отсутствии некоторых необходимых пакетов система выведет соответствующее сообщение. Установите эти пакеты с помощью следующей команды:

```
sudo apt install -f
```

5. Система выполнит распаковку архива и выведет окно выбора языка SecurOS (см. рис. 36):

Примечание. Все описанные ниже окна выводятся в указанной последовательности только при первоначальной установке SecurOS. При обновлении уже установленной версии выводится только одно окно, которое представлено на рис. 39.

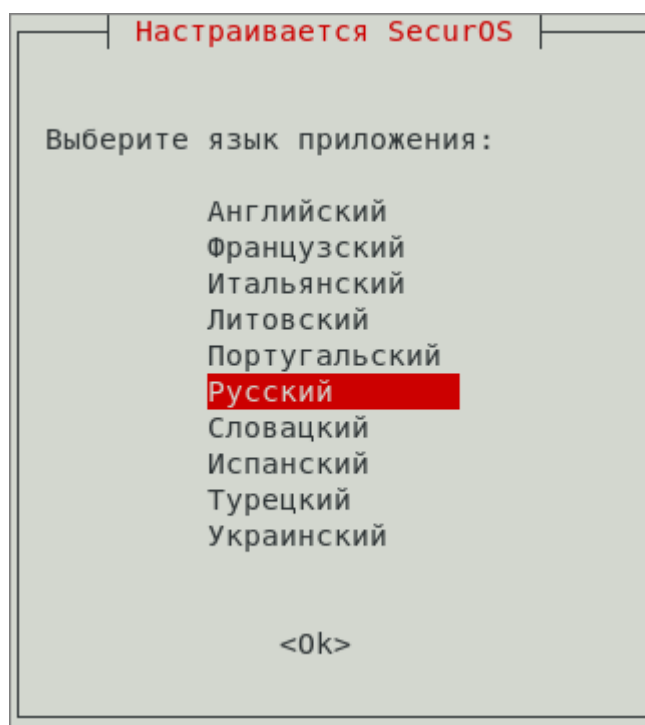


Рис. 36. Выбор языка приложения

Выберите требуемый язык из списка. Для продолжения установки нажмите **ОК** или клавишу **Enter**.

6. Система выведет окно выбора типа установки (см. рис. 37):

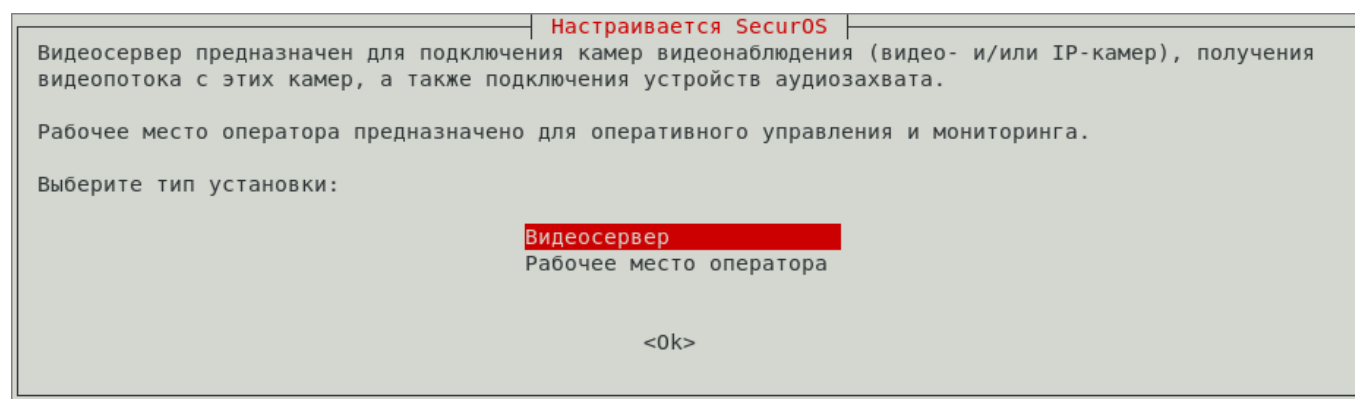


Рис. 37. Окно выбора типа установки

Для установки программного обеспечения *Видеосервера* выберите в списке соответствующее значение. Для продолжения установки нажмите **ОК** или клавишу **Enter**.

7. Система выведет окно выбора типа *Видеосервера* (см. рис. 38):

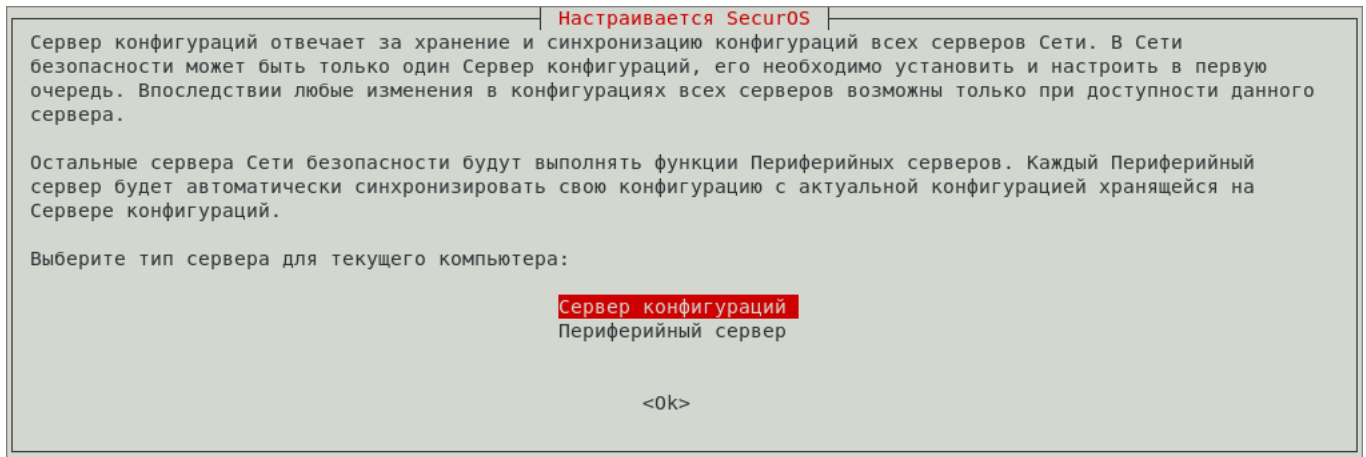


Рис. 38. Окно выбора типа Видеосервера

Для установки программного обеспечения *Сервера конфигураций* выберите из списка соответствующее значение. Для продолжения установки нажмите **OK** или клавишу **Enter**.

8. Система выведет окно запроса пароля администратора PostgreSQL (см. рис. 39):

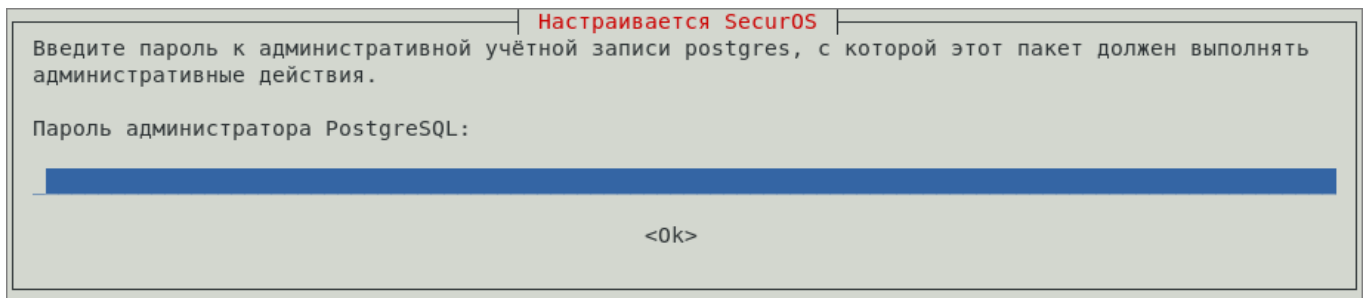


Рис. 39. Окно запроса пароля администратора PostgreSQL

Введите текущий пароль администратора БД. Для продолжения установки нажмите **OK** или клавишу **Enter**.

9. Если введен неправильный пароль, система выведет окно ошибки подключения (см. рис. 40):

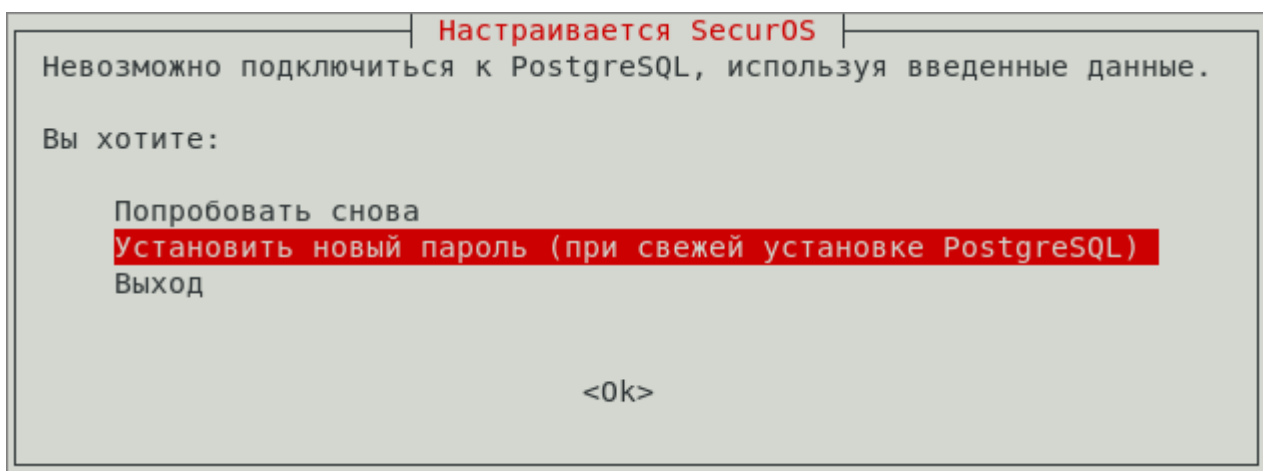


Рис. 40. Окно ошибки подключения

Введите корректный пароль администратора или задайте новый. При задании нового пароля система выведет окно настройки пароля (см. рис. 41):

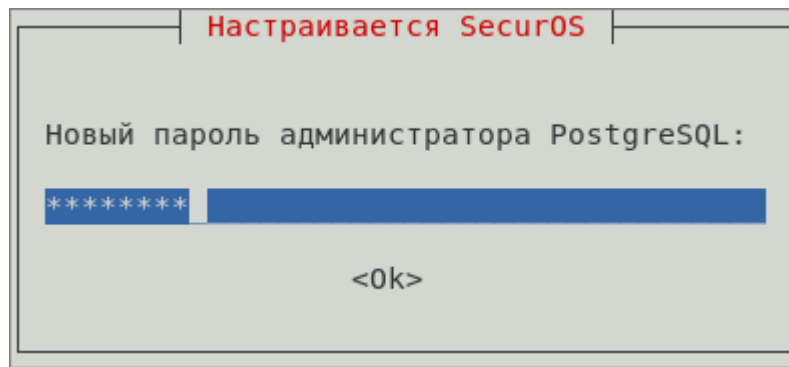


Рис. 41. Окно задания нового пароля администратора

Для продолжения установки нажмите **ОК** или клавишу **Enter**.

10. Система выведет окно подтверждения нового пароля (см. рис. 42):

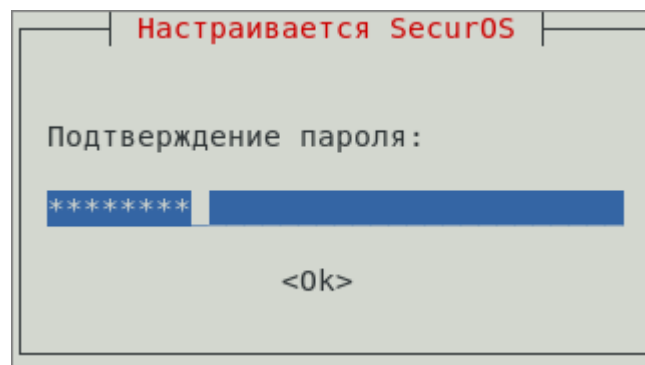


Рис. 42. Окно подтверждения нового пароля администратора

Повторно введите новый пароль. Для продолжения установки нажмите **ОК** или клавишу **Enter**.

11. Система выведет окно выбора пользователей (см. рис. 43):

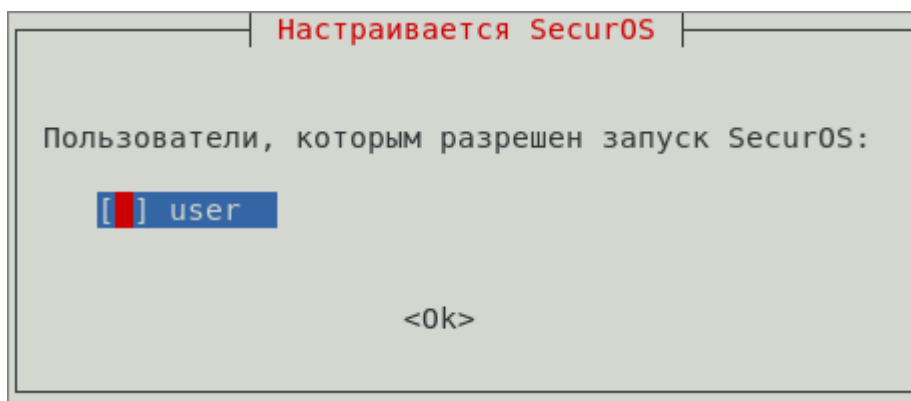


Рис. 43. Окно выбора пользователя

В списке пользователей выберите тех пользователей Linux, которым будет разрешен запуск SecurOS на этом компьютере. Для перемещения по списку используйте клавиши-стрелки. Для выбора пользователя выделите его в списке, нажмите клавишу **Пробел**. Слева от имени пользователя будет проставлен символ "*" (звездочка). Для продолжения установки нажмите **ОК** или клавишу **Enter**.

Чтобы разрешить запуск SecurOS новым пользователям ОС когда продукт уже установлен, необходимо добавить их в дополнительную группу `securos`. Если пользователь уже создан в ОС, выполните следующую команду:

```
sudo usermod -a -G securos <имя_пользователя>
```

Примечание. После добавления в группу пользователь сможет запустить SecurOS только в новой сессии.

Если пользователь еще не создан в ОС, выполните следующую команду:

```
sudo useradd -g <имя_первичной_группы> -G securos <имя_пользователя>
```

12. Система выполнит необходимые операции и выведет окно **Установка завершена** (см. рис. 44):

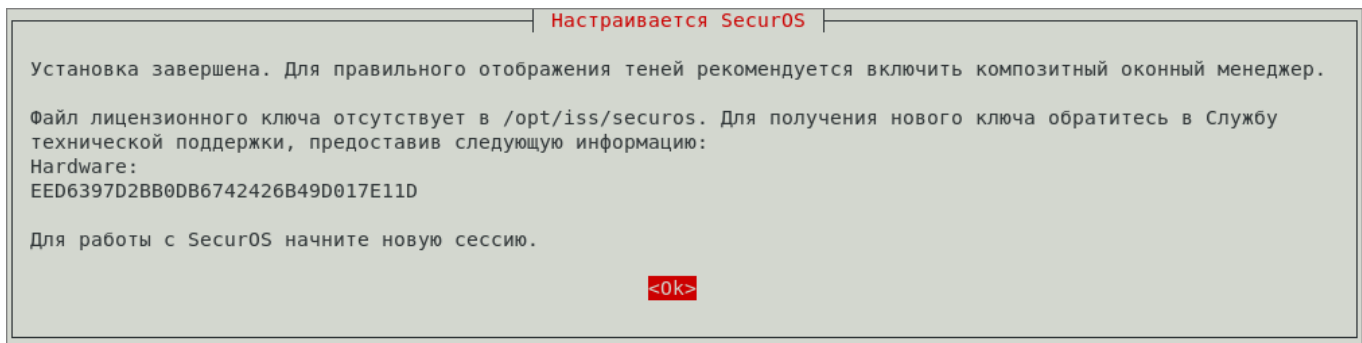


Рис. 44. Окно Установка завершена

Для завершения установки нажмите **ОК** или клавишу **Enter**.

Внимание! Для смены параметров, заданных при установке SecurOS в описанных выше окнах, используйте команду `sudo dpkg-reconfigure securos`. Без использования команды смена параметров будет возможна только после полного удаления SecurOS и повторной установки.

13. Определите директорию для записи архива. Рекомендуется использовать для этого жесткий диск, отличный от системного, или создать отдельный логический раздел на системном диске. Предоставьте системному пользователю securos права на чтение и запись для выбранной директории. Для этого используйте следующие команды:

```
sudo chown securos -R <директория_для_записи_архива>
sudo chmod 744 -R <директория_для_записи_архива>
```

14. Для первого запуска клиентской части SecurOS на данном компьютере начните новую сессию Linux для текущего пользователя.

15. Скопируйте файл лицензионного ключа из ранее созданной директории, где находится файл ключа (<директория_с_дистрибутивом_SecurOS>), в корневую директорию установки SecurOS (/opt/iss/securos), для чего выполните следующие команды:

```
cd <директория_с_дистрибутивом_SecurOS>
sudo cp key.iss /opt/iss/securos
```

16. Измените владельца файла и его права на операции с файлом ключа:

```
cd /opt/iss/securos/
sudo chown root:securos key.iss
sudo chmod 640 key.iss
```

17. Запустите демон `vms_server`, для чего выполните следующую команду:

```
sudo service vms_server start
```

Установка с использованием .run-файла

Для установки используется файл `securos_XXX-YYY_amd64.run`, где XXX — версия ПО SecurOS, YYY — версия операционной системы.

Для установки ПО на *Видеосервере* выполните следующие действия:

1. Запустите консольное приложение *Терминал*.
2. Для перехода в директорию, куда был скопирован установочный файл SecurOS (<директория_с_дистрибутивом_SecurOS>), выполните следующую команду:

```
cd <директория_с_дистрибутивом_SecurOS>
```

3. Для начала установки программного обеспечения SecurOS запустите установочный файл продукта (например, `securos_11.4_amd64.run`) следующей командой:

```
sudo ./securos_11.4_amd64.run
```

4. Дальнейшие шаги установки полностью аналогичны описанным выше (см. [Установка с использованием .deb-файла](#)).

4.1.4 Первоначальная настройка

Первоначальная настройка SecurOS на *Сервере конфигураций* выполняется при помощи *Мастера первоначальной настройки*, который предлагает различные варианты настройки. Базовая настройка, при которой конфигурационные данные вводятся администратором, выполняется с помощью *Мастера первого запуска*. По окончании настройки система будет полностью подготовлена к работе.

Внимание!

1. Процедура первоначальной настройки на платформе Linux полностью аналогична процедуре настройки на платформе Windows (см. раздел [Первоначальная настройка](#)).
2. Перед запуском процедуры первоначальной настройки установите электронный ключ Guardant Sign (см. [Установка ключа Guardant](#)).

4.1.5 Настройка количества дескрипторов для записи видеоархива на диск

При записи в видеоархив с большого количества камер одновременно может возникнуть ситуация, когда из-за переполнения очереди система не сможет открыть новый дескриптор, вызывая прореживание кадров. Количество одновременно открытых дескрипторов по умолчанию может быть недостаточно, поэтому, чтобы повысить производительность при записи, значение можно задать вручную.

Для настройки количества одновременно открытых дескрипторов выполните следующие действия:

1. Откройте для редактирования файл `/etc/security/limits.conf` и добавьте в него строки:

```
* soft nofile 8192
```

* hard nofile 8192

Примечание. Если количество одновременно открытых дескрипторов уже задано, и оно выше рекомендуемого значения (8192), то снижать его не требуется.

2. Откройте для редактирования файл `/etc/pam.d/common-session` и добавьте в него строку:

```
session required pam_limits.so
```

3. Перезагрузите компьютер.

4.1.6 Запуск SecurOS на Сервере конфигураций

Запуск SecurOS на *Сервере конфигураций* на платформе Linux аналогичен запуску на платформе Windows (см. [Запуск SecurOS на Сервере конфигураций](#)).

4.2 Установка, настройка и запуск Периферийных серверов

Начальные условия и шаги процедуры установки аналогичны установке ПО SecurOS на *Видеосервере* (см. [Установка программного обеспечения на Сервере конфигураций](#)).

Для установки программного обеспечения SecurOS на периферийных серверах (прочие *Видеосервера*, не являющиеся *Сервером конфигураций*), в окне **Тип сервера** (см. рис. 45) выберите тип **Периферийный сервер**. Далее следуйте инструкциям Мастера установки. После завершения установки начните новую сессию пользователя и присвойте необходимые права файлу лицензионного ключа (см. [Установка программного обеспечения на Сервере конфигураций](#)).

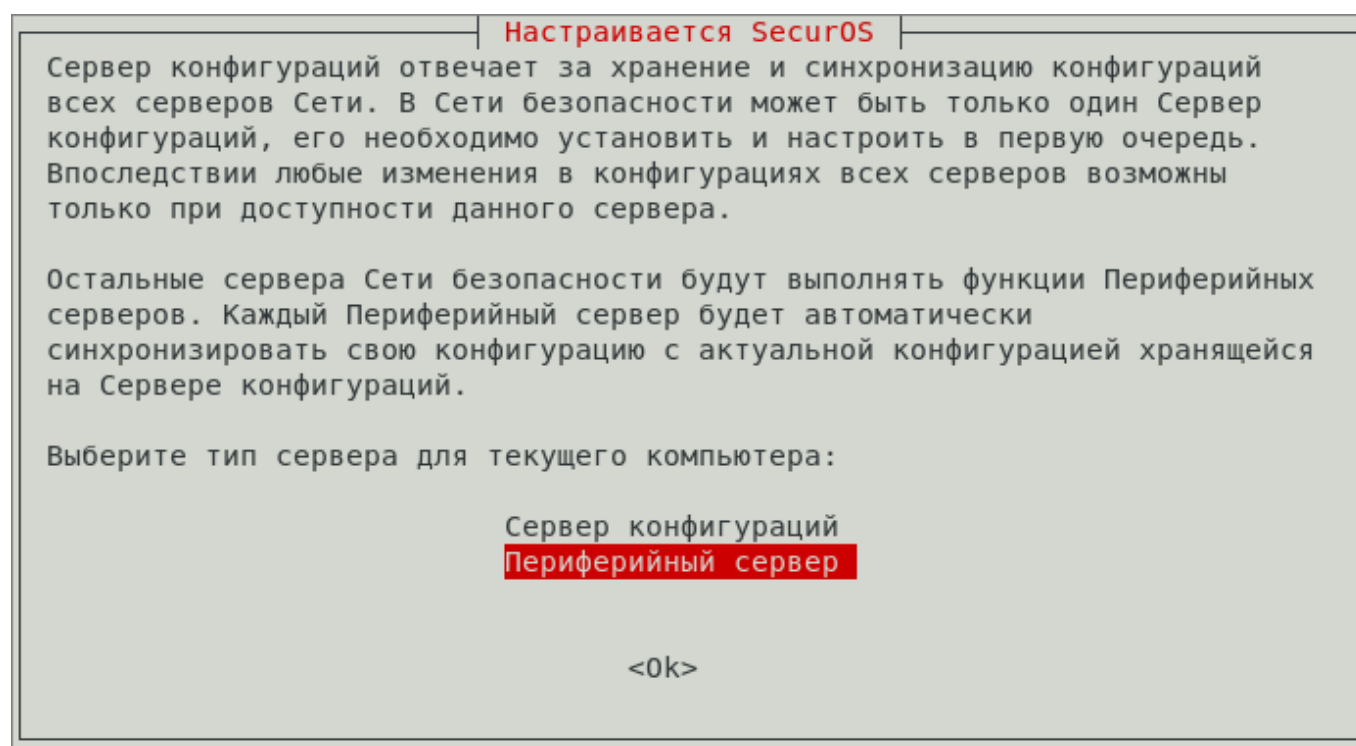


Рис. 45. Окно выбора типа Видеосервера

Процедура запуска и настройки SecurOS на *Периферийном сервере* на платформе Linux аналогична процедуре настройки на платформе Windows (см. [Установка, настройка и запуск Периферийных серверов](#)).

4.3 Установка, настройка и запуск Рабочих мест оператора

Начальные условия и шаги процедуры установки аналогичны установке ПО SecurOS на *Видеосervere* (см. [Установка программного обеспечения на Сервере конфигураций](#)).

Для установки программного обеспечения SecurOS на *Рабочем месте оператора*, в окне **Тип установки** (см. рис. 46) выберите тип **Рабочее место оператора**. Далее следуйте инструкциям Мастера установки. После завершения установки начните новую сессию пользователя и присвойте необходимые права файлу лицензионного ключа (см. [Установка программного обеспечения на Сервере конфигураций](#)).

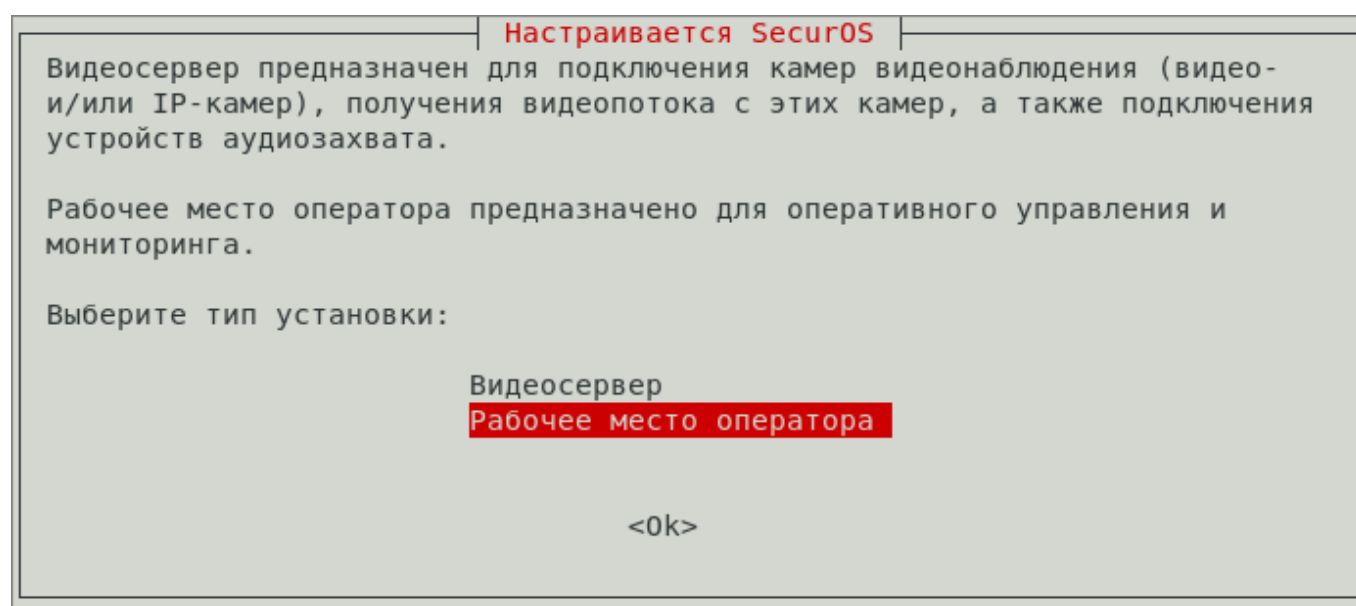


Рис. 46. Окно выбора типа установки

Процедура запуска и настройки *Рабочего места оператора* на платформе Linux аналогична процедуре настройки на платформе Windows (см. [Установка, настройка и запуск Рабочих мест оператора](#)).

4.4 Порядок обновления SecurOS

Порядок обновления ПО SecurOS на платформе Linux аналогичен порядку обновления на платформе Windows (см. [Порядок обновления SecurOS](#)).

5 Установка программного обеспечения для работы нейросетевых алгоритмов

Внимание! Установка данного программного обеспечения необходима только в том случае, если вы используете модули, которые включают в себя функциональность нейросетей. Информацию о наличии функциональности нейросетей в конкретном модуле вы можете найти в соответствующем разделе документации на модуль.

Программное обеспечение для работы нейросетевых алгоритмов

Для интеграции нейросетевых алгоритмов с SecurOS используются специальные приложения, которые называются нейросетевые серверы.

Используемые нейросетевые серверы

Модули и компоненты SecurOS могут использовать следующие нейросетевые серверы:

- Caffe2Server (см. также [Установка драйверов NVIDIA для работы нейросетевых алгоритмов на базе Caffe2Server в ОС Linux](#));
- OpenVINOServer.

Для работы нейросетевого сервера Caffe2Server в ОС Windows/Linux требуется установить драйверы NVIDIA. Для обеих операционных систем рекомендуется использовать драйверы версии 470 и выше.

Примечание. Для работы нейросетевых алгоритмов на базе OpenVINOServer в ОС Windows/Linux драйверы NVIDIA устанавливать не требуется, достаточно установить ПО OpenVINOServer.

Для установки нейросетевого сервера выполните следующие действия:

1. Для получения ссылки на ресурс с инсталлятором необходимого нейросетевого сервера обратитесь в Службу технической поддержки Intelligent Security Systems.
2. Скачайте инсталлятор с указанного ресурса.
3. Запустите инсталлятор на компьютере, где необходимо установить сервер.
4. Дождитесь окончания установки программного обеспечения.
5. Перезапустите службу Video Management System Server (см. раздел [Утилита Server Control Agent](#)).

5.1 Установка драйверов NVIDIA для работы нейросетевых алгоритмов на базе Caffe2Server в ОС Linux

При использовании нейросетевого сервера Caffe2Server в ОС Linux требуется установить драйвер NVIDIA начиная с версии 470 и новее.

Установка драйверов в Debian 12

Для установки драйвера NVIDIA выполните следующие действия:

1. Откройте файл `/etc/apt/sources.list` в текстовом редакторе с правами суперпользователя.
2. Удалите или закомментируйте строку, начинающуюся с `deb cdrom`.
3. Добавьте в файл строки:

```
deb http://deb.debian.org/debian/ bookworm
main contrib non-free non-free-firmware

deb http://security.debian.org/debian-security bookworm-security
main contrib non-free non-free-firmware

deb http://deb.debian.org/debian/ bookworm-updates
main contrib non-free non-free-firmware
```

В файле уже могут быть строки, начинающиеся с:

```
deb http://deb.debian.org/debian/ bookworm
deb http://security.debian.org/debian-security bookworm-security
deb http://deb.debian.org/debian/ bookworm-updates
```

В этом случае добавлять их повторно не нужно, достаточно убедиться, что в конце каждой строки указано:

```
main contrib non-free non-free-firmware
```

4. Сохраните изменения и закройте файл.
5. Обновите индексацию пакетов:

```
sudo apt update
```

6. Установите драйвер:

```
sudo apt install nvidia-driver
```

Примечание. Предупреждение `Conflicting nouveau kernel module loaded` можно проигнорировать, нажав клавишу **Enter**.

7. Перезагрузите компьютер.

Установка драйверов в Astra Linux 1.7

Драйверы NVIDIA доступны в расширенном репозитории Astra 1.7.

1. Добавьте репозиторий в `/etc/apt/sources.list`:

```
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/  
repository-main/ 1.7_x86-64 main contrib non-free  
  
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/  
repository-update/ 1.7_x86-64 main contrib non-free  
  
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/  
repository-base/ 1.7_x86-64 main contrib non-free  
  
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/  
repository-extended/ 1.7_x86-64 main contrib non-free
```

2. Обновите индексацию пакетов:

```
sudo apt update
```

3. Выполните шаги, описанные в разделе "Действия перед установкой драйверов NVidia" (<https://wiki.astralinux.ru/pages/viewpage.action?pageId=1212463>).
4. Установите драйвер. Ниже приведен пример команды для установки драйвера версии 510.

```
sudo apt install nvidia-driver-510
```

5. Перегрузите компьютер.

6 Администрирование SecurOS

Режим администрирования используется для конфигурирования сети безопасности и ее компонентов. Он доступен с любого *Видеосервера* и *Рабочего места оператора*, если для оператора определена возможность конфигурирования системы (см. [Права пользователя](#)). При переходе в режим администрирования компоненты охранной системы продолжают полноценно функционировать.

Внимание! После установки ПО SecurOS и СУБД PostgreSQL в ОС Windows создается учетная запись postgres. Для настройки системы SecurOS используйте учетную запись Windows администратора, но не postgres.

6.1 Работа с Панелью управления

Панель управления предназначена для вызова *Центра Администрирования*, управления *Рабочими столами*, сеансами пользователя, а также для настройки свойств самой панели. Дополнительно с помощью панели можно вызвать справочную документацию и запускать специальные команды управления системой (см. раздел [Макрокоманда](#)). Внешний вид панели представлен на рис. 47.

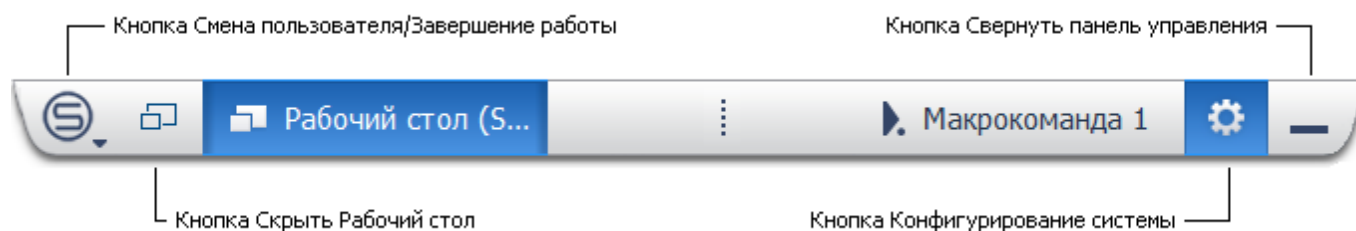


Рис. 47. Панель управления SecurOS

На панели располагаются кнопки вызова активных *Рабочих столов* и *Макрокоманд* (см. [Отключение/включение объекта](#)), количество которых определяется в настройках системы. Если это количество превышено, избыточные кнопки скрываются, на панель выводится меню вызова соответствующих объектов:

-  — для *Рабочих столов*;
-  — для *Макрокоманд*.

Текущий *Рабочий стол* отображается кнопкой голубого цвета (см. рис. 47). Таким же цветом отображается кнопка **Конфигурирование системы**, если пользователь открыл *Центр администрирования*.

Для организации пространства на *Панели управления* перемещайте разделитель . Это позволит при необходимости увеличить количество отображаемых кнопок *Рабочих столов* или *Макрокоманд*. На количество отображаемых элементов также влияет размер кнопок, который можно изменить в настройках *Панели управления* (см. раздел **Вызов, настройка и скрытие Панели управления**).

С помощью перетаскивания (метод drag-and-drop) можно менять порядок кнопок в областях *Рабочих столов* и *Макрокоманд* (см. рис. 48).

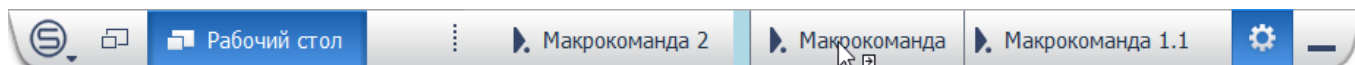


Рис. 48. Метод drag-and-drop на Панели управления SecurOS

Аналогичным методом можно перемещать кнопки из *Панели управления* в выпадающие списки областей *Рабочих столов* или *Макрокоманд* и обратно.

См. также:

- **Вызов, настройка и скрытие Панели управления.**
- **Вызов и закрытие Центра администрирования.**
- **Выбор Рабочего окружения.**
- **Управление сеансами пользователя и завершение работы Клиента.**
- **Вызов справочной документации.**
- **Смена/сброс пароля типового пользователя.**
- **Завершение работы системы.**

6.1.1 Вызов, настройка и скрытие Панели управления

В разделе описаны типовые операции с *Панелью управления*:

- **Вызов Панели управления;**
- **Настройка Панели управления;**
- **Скрытие Панели управления.**

Вызов Панели управления

По умолчанию, после входа в систему, *Панель управления* отображается на рабочем столе Windows. Если к компьютеру оператора подключено несколько физических мониторов, панель отображается на первом из них.

Если *Панель управления* не отображается на рабочем столе Windows, нажмите клавишу **Ctrl** и, удерживая ее нажатой, переместите указатель мыши к верхнему краю экрана. Чтобы *Панель управления* отобразилась с открытым *Центром администрирования*, вместо клавиши **Ctrl** используйте сочетание клавиш **Ctrl + Alt**.

Примечание. В зависимости от режима работы, *Панель управления* может быть вызвана различными способами (см. **Краткое руководство пользователя SecurOS**).

Дополнительная информация

Панель управления также может быть вызвана щелчком мыши по значку приложения в области уведомлений панели задач Windows (системном трее), либо с помощью команды **Показать Панель управления** контекстного меню значка приложения.

Настройка Панели управления



Для настройки метода вызова и скрытия *Панели управления* нажмите кнопку **(Смена пользователя/Завершение работы)**, выберите команду **Настроить Панель управления**. В окне **Настройка Панели управления** (см. рис. 49) задайте требуемые параметры.

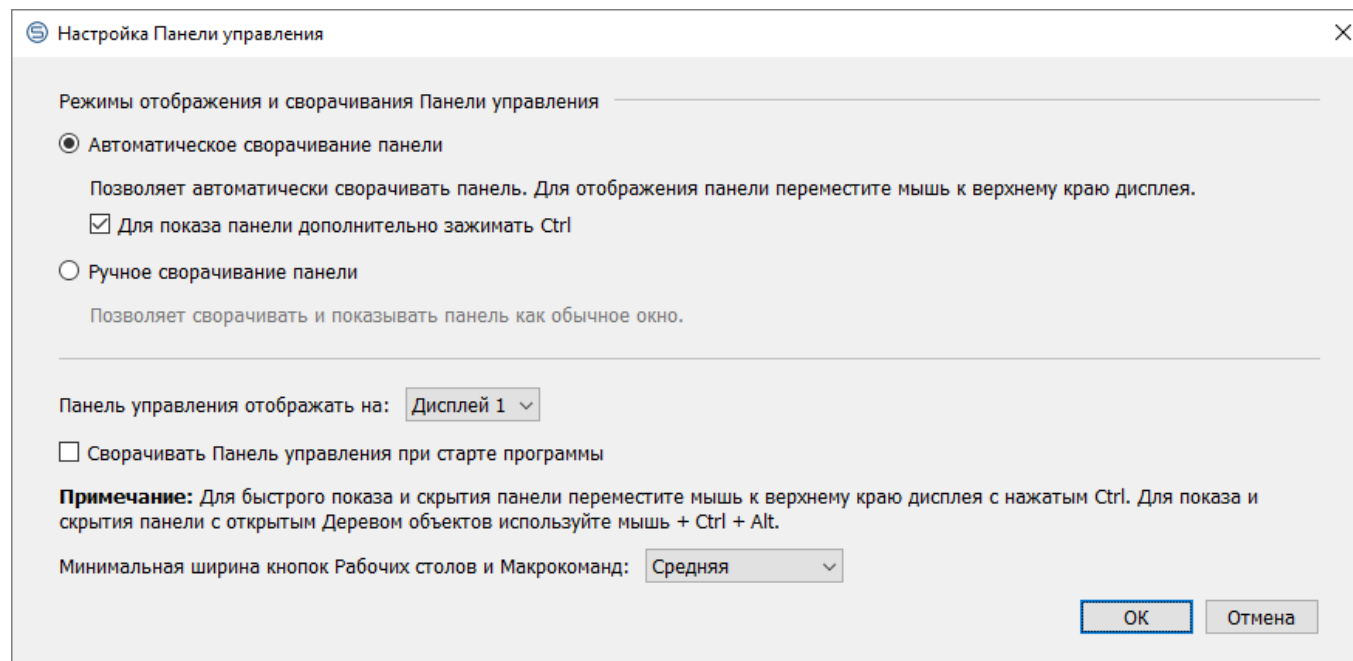


Рис. 49. Окно Настройка Панели управления

Для задания ширины кнопок, расположенных на *Панели управления*, выберете одно из значений параметра **Минимальная ширина кнопок Рабочих столов и Макрокоманд**.

Примечание. Кнопки, которые не поместились на *Панели управления*, будут перенесены в выпадающий список соответствующей области.

Скрытие Панели управления

Метод скрытия *Панели управления* зависит от ее текущих настроек (см. **Настройка панели управления**):

- В режиме **Автоматического сворачивания** панель скрывается самостоятельно, если указатель мыши больше не находится поверх панели, и *Центр администрирования* не отображается. При открытом *Центре администрирования* нажмите клавишу **Ctrl** и, удерживая ее нажатой, переместите указатель мыши к верхнему краю экрана.

Примечание. Автоматическое скрытие *Панели управления* невозможно, если открыт **Центр администрирования**.



- В режиме **Ручного сворачивания**, для скрытия панели нажмите кнопку **(Свернуть Панель управления)** или нажмите клавишу **Ctrl** и, удерживая ее нажатой, переместите указатель мыши к верхнему краю экрана.

Примечание. *Панель управления* также можно скрыть щелкнув мышью значок приложения в области уведомлений панели задач Windows (системном трее), на Панели задач Windows или с помощью контекстного меню значка приложения в системном трее.

6.1.2 Вызов и закрытие Центра администрирования

Чтобы открыть *Центр администрирования*, нажмите на **Панели управления** кнопку  (Конфигурирование системы).

Система выведет главное окно *Центра администрирования* (см. рис. 50).

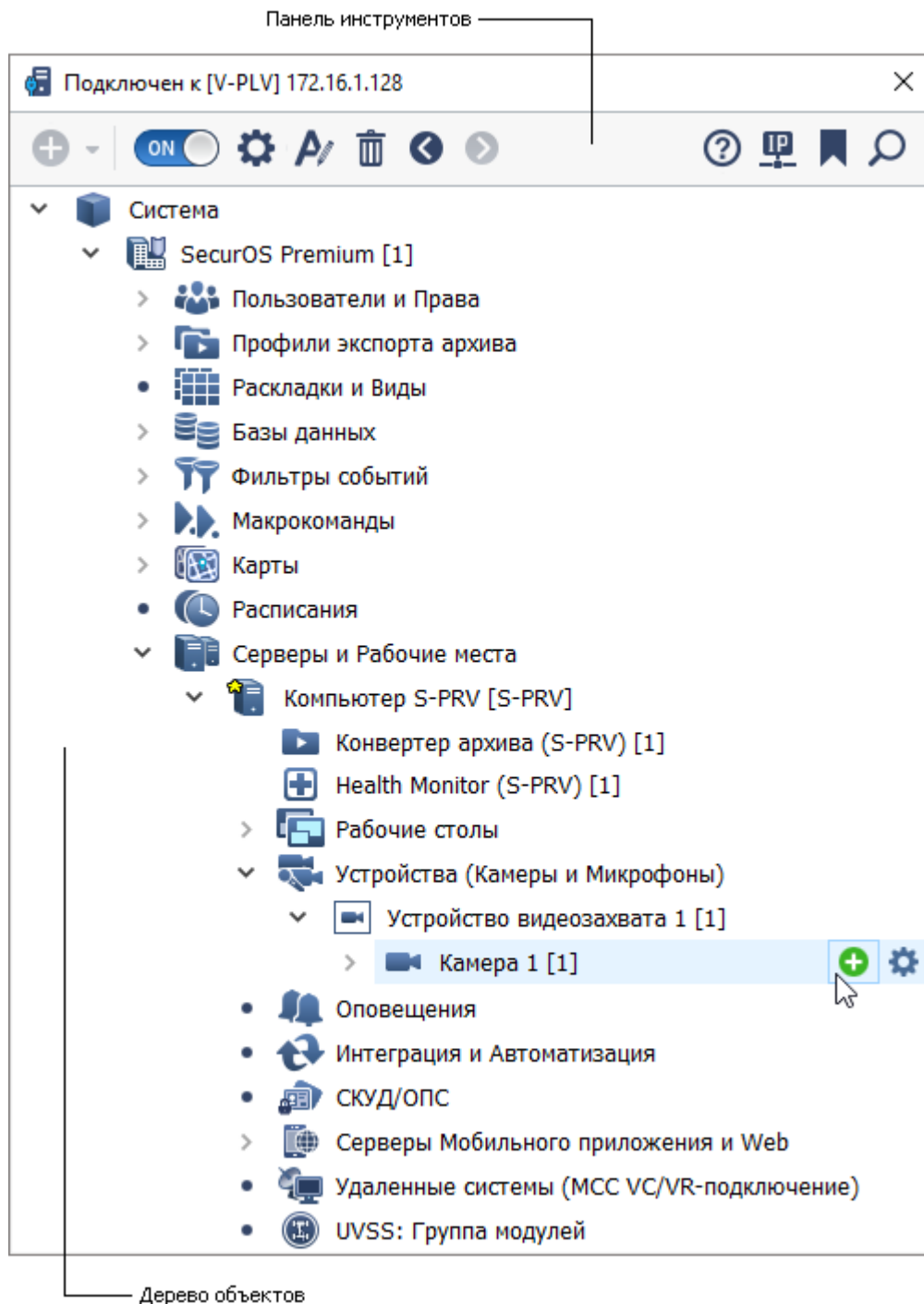


Рис. 50. Центр администрирования

Чтобы закрыть *Центр администрирования*, снова нажмите кнопку



См. также:

Центр администрирования.

6.1.3 Выбор Рабочего окружения

Созданные *Профили Рабочего места оператора* (см. [Профили Рабочих мест оператора](#)) доступны в интерфейсе оператора в качестве *Рабочего окружения*. *Рабочее окружение* определяют внешний вид интерфейса оператора и доступные в нем модули. *Рабочее окружение* может быть использовано для неограниченного количества *Рабочих мест оператора*. С помощью *Панели управления* можно сменить текущее *Рабочее окружение*. Для этого нажмите кнопку **Смена пользователя/Завершение**

работы () , в выпадающем списке выберите пункт **Выбрать Рабочее окружение**, далее щелкните мышью желаемый вариант (см. рис. 51).

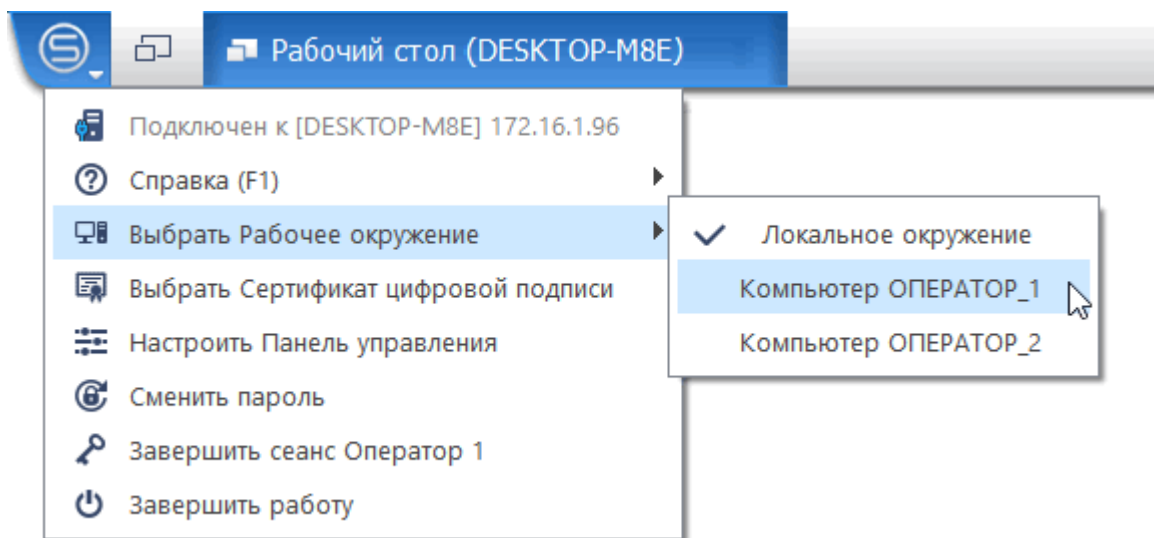


Рис. 51. Выбор Рабочего окружения

Текущее *Рабочее окружение* будет выделено в списке галочкой ✓. *Рабочее окружение*, настроенное на фиксированном *Рабочем месте оператора* (см. [Фиксированные Рабочие места оператора](#)), называется *Локальным*.

Внимание! Последнее выбранное *Рабочее окружение* запоминается для пользователя Windows.

Детальное описание работы с *Рабочим окружением* приведено в документе [Краткое руководство пользователя SecurOS](#).

6.1.4 Управление сеансами пользователя и завершение работы Клиента

С помощью *Панели управления* можно сменить пользователя или завершить работу *Клиента*.

Нажмите кнопку **Смена пользователя/Завершение работы** () , в выпадающем списке выберите необходимую команду (см. рис. 52).

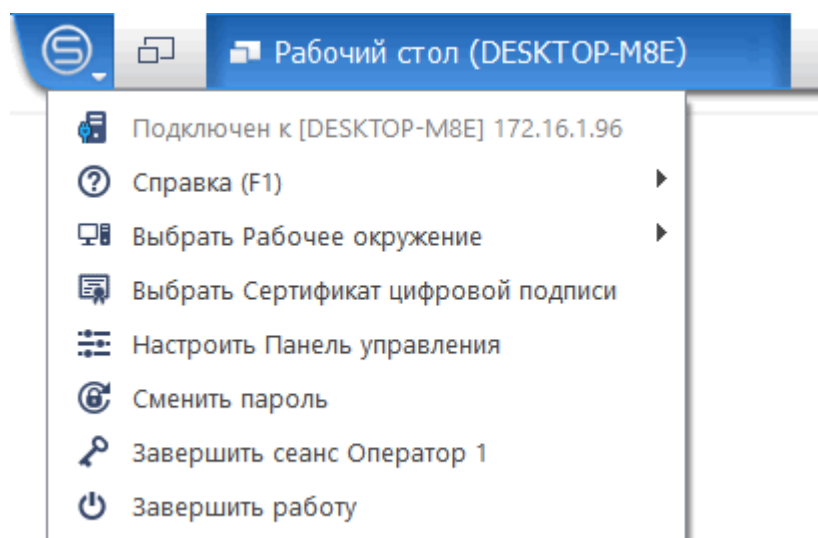


Рис. 52. Команды меню Смена пользователя/Завершение работы

В случае автоматической или ручной блокировки рабочего стола происходит автоматическое завершение сеанса текущего пользователя в *Интерфейсе оператора* (при условии, что выбран параметр **Автоматическое завершение сеанса пользователя при блокировке экрана объекта Компьютер**).

6.1.5 Завершение работы системы

Завершить работу системы (*Серверной части SecurOS*) можно одним из следующих способов:

- Остановить *Серверную часть SecurOS* с помощью утилиты **Server Control Agent**.
- Остановить службу Video Management System Server. При остановке службы *Серверная часть SecurOS* будет остановлена автоматически. Службу также можно остановить с помощью утилиты **Server Control Agent** или, при работе с ОС Windows, с помощью консоли **Управление компьютером** (**Компьютер** → **Управление** → **Службы и приложения** → **Службы**).

6.1.6 Вызов справочной документации

При вызове справки можно открыть следующие описания:

- **Список всех Руководств пользователя;**
- **Раздел с описанием Центра администрирования;**
- **Раздел с описанием настроек объекта SecurOS.**

Список всех доступных Руководств пользователя SecurOS можно открыть одним из следующих способов:

1. Из панели управления SecurOS, нажав кнопку  (**Смена пользователя/Завершение работы**) (см. рис. 53):

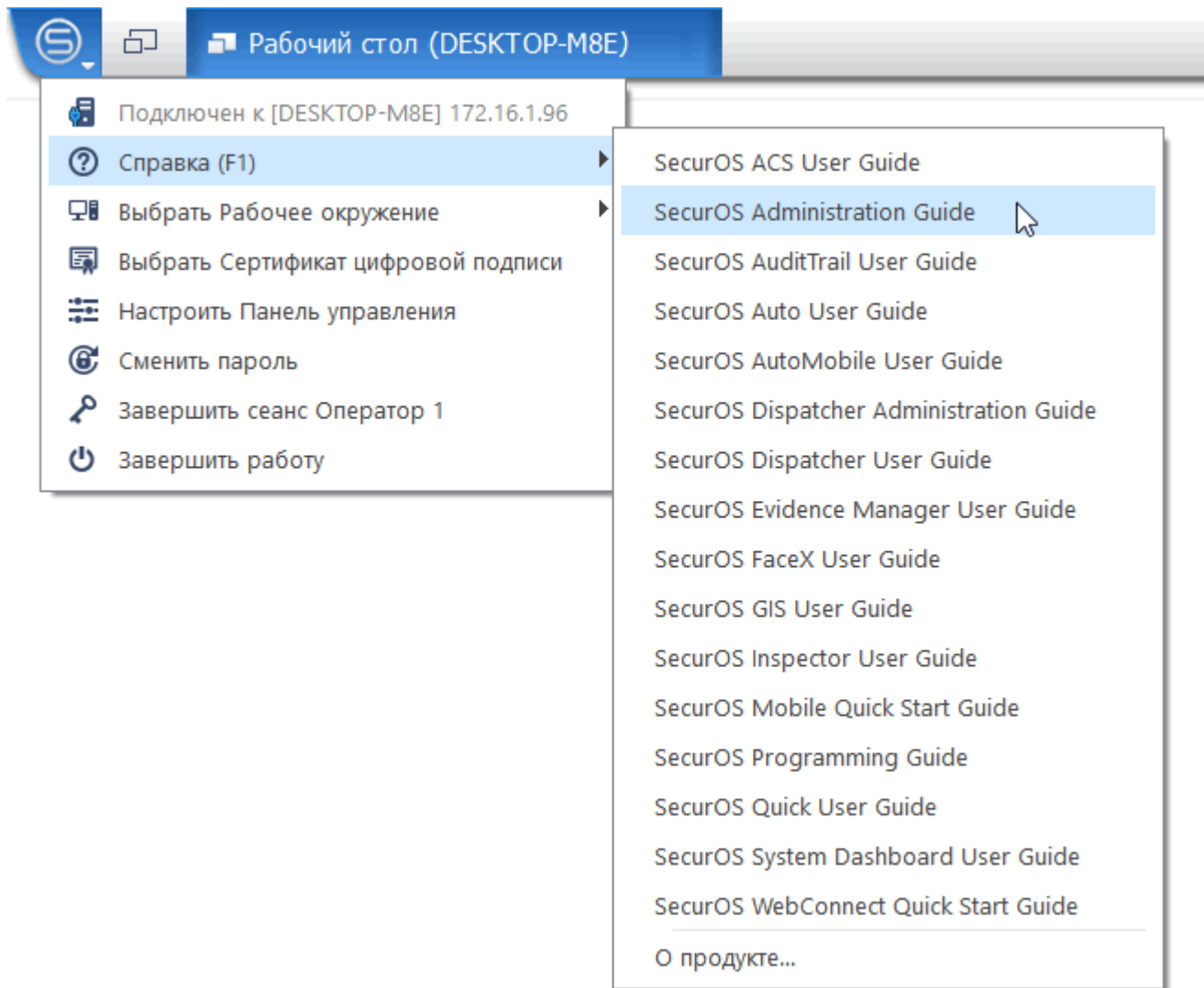


Рис. 53. Вызов справки из панели управления

2. Из области уведомлений панели задач Windows (системного трее), щелкнув правой кнопкой мыши значок SecurOS (см. рис. 54):

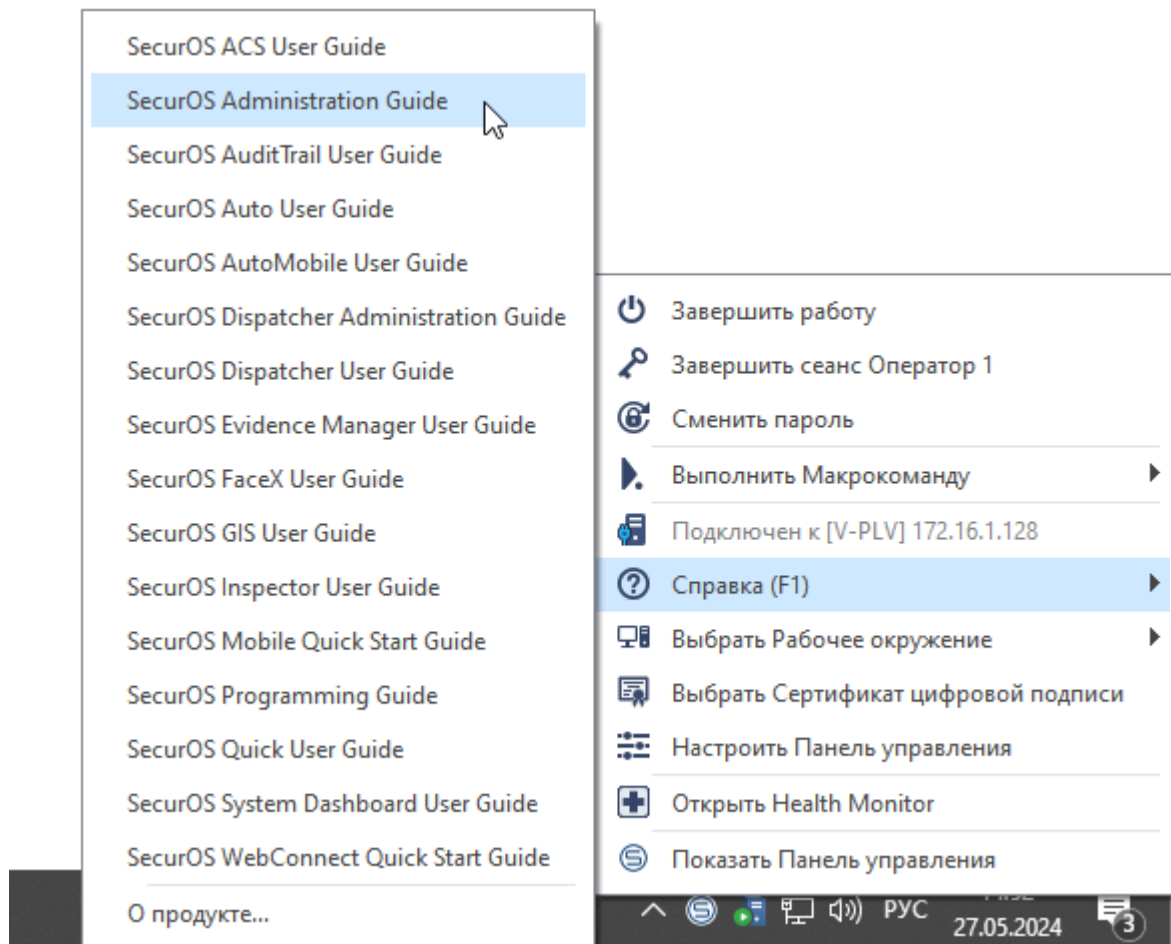


Рис. 54. Вызов справки из области уведомлений Windows

3. Из Панели задач Windows (Пуск → Все программы → SecurOS → Documentation).

Раздел с описанием **Центра администрирования** можно открыть из *Центра администрирования* с помощью клавиши **F1** или кнопки

Раздел с описанием параметров настройки объекта можно открыть из *Центра администрирования*, открыв настройки объекта в *Дереве объектов* и нажав клавишу **F1** или кнопку .

6.2 Центр администрирования

Чтобы вызвать *Центр администрирования*, нажмите на **Панели управления** кнопку (Конфигурирование системы).

Центр администрирования состоит из **Панели инструментов** и **Дерева объектов** (см. рис. 55):

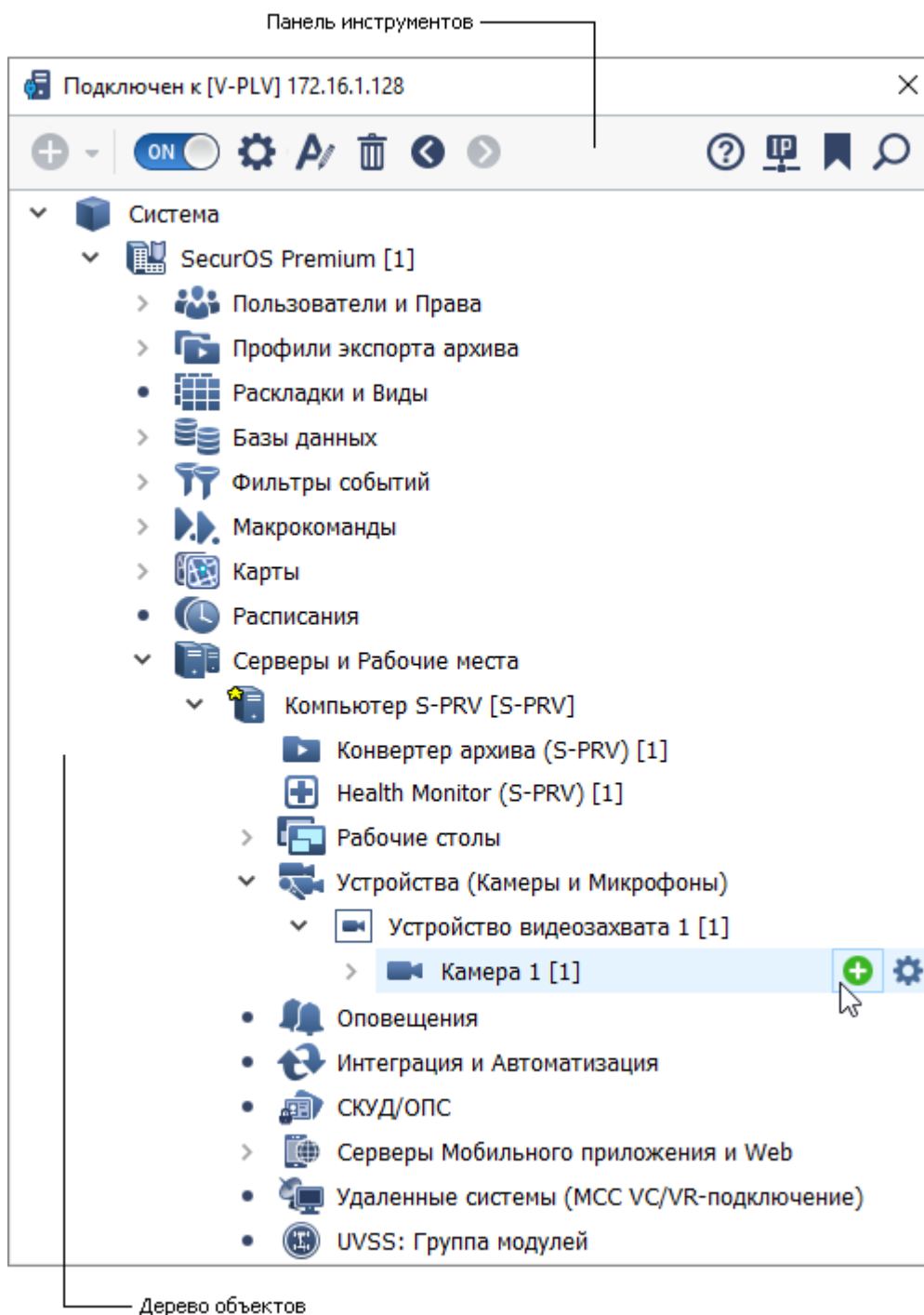


Рис. 55. Центр администрирования

В заголовке окна *Центра администрирования* отображается имя и IP-адрес *Видеосервера*, к которому в настоящее время подключен *Клиент SecurOS*. Имя и IP-адрес *Видеосервера* также можно посмотреть в меню *Панели управления* или в контекстном меню значка *Клиента SecurOS* в системном древе (например, см. [Вызов справочной документации](#)).

Панель инструментов

Панель администратора содержит элементы управления (кнопки), позволяющие выполнять типовые операции администрирования сети (см. [Работа с объектами](#)).

Операции администрирования выполняются с объектом SecurOS, выделенным в *Дереве объектов*. Список операций, которые могут быть выполнены с объектом (т.е. доступность каждой из кнопок панели), определяется свойствами выделенного объекта.

Дерево объектов

Элементы, входящие в сеть безопасности, представлены в виде дерева — иерархической структуры, отражающей взаимосвязи между ними. Корневым элементом дерева является объект *Система*. Все прочие объекты SecurOS являются его дочерними элементами.

Дополнительная информация

Объекты, которые содержатся "внутри" других объектов, называются *дочерними*. В свою очередь объекты, содержащие дочерние, называются *родительскими*.

В дереве существуют два типа элементов:

1. *Группа* — элемент, предназначенный для объединения *Объектов* по функциональному признаку. *Группа* создается автоматически и не может быть удалена администратором. Для обозначения состояния групп используются следующие индикаторы, которые располагаются слева от значка группы:

- — группа, не содержащая дочерних объектов ("пустая" группа).
- — группа, содержащая дочерние объекты.

Большинство групп являются дочерними *Объекту охраны*. Некоторые группы могут быть дочерними прочим объектам SecurOS, например, группа *Рабочие столы* является дочерней объекту *Компьютер*.

2. *Объект* — функциональный элемент сети безопасности. В дереве SecurOS может располагаться только в пределах *Группы*, если она определена для данного типа объекта. *Объект* может быть создан, изменен и удален администратором.

В сети SecurOS существуют два класса *объектов*: системные объекты и объекты интерфейса пользователя. Системные объекты отражают функциональность сети, объекты интерфейса пользователя предназначены для мониторинга и управления сетью безопасности.

Дерево объектов используется при выполнении любых операций по изменению конфигурации сети.

6.2.1 Работа с объектами

На *Панели инструментов* расположены следующие кнопки работы с объектами (см. рис. 56):



Рис. 56. Кнопки Панели инструментов Центра администрирования

Примечание. Если какая-либо операция невозможна, соответствующая кнопка блокируется.

- **Создать** — создать новый объект (дочерний по отношению к выделенному объекту/группе);

Внимание! Объекты с одинаковым уровнем иерархии можно создать только из контекстного меню родительского объекта/группы.

- **Отключить/Включить** — отключить/включить объект. При выполнении операции кнопка меняет внешний вид; действие кнопки изменяется на обратное;
- **Настроить** — открыть/закрыть окно настройки параметров объекта;
- **Переименовать** — переименовать объект;
- **Удалить** — удалить объект;
- **Назад/вперед** — кнопки перехода между объектами *Дерева объектов* в порядке, в котором эти объекты выбирались пользователем;
- **Справка** — вызвать справку (контекстно-зависимо от текущего объекта в *Дереве объектов*);
- **Менеджер IP-устройств** — вызов приложения для поиска и управления настройками IP-устройств в сети безопасности SecurOS;
- **Избранные объекты** — открыть *Панель избранных объектов*;
- **Панель поиска объектов** — открыть *Панель поиска объектов*.

Кнопки *Панели инструментов* продублированы командами контекстного меню объекта (например, см. рис. 57):

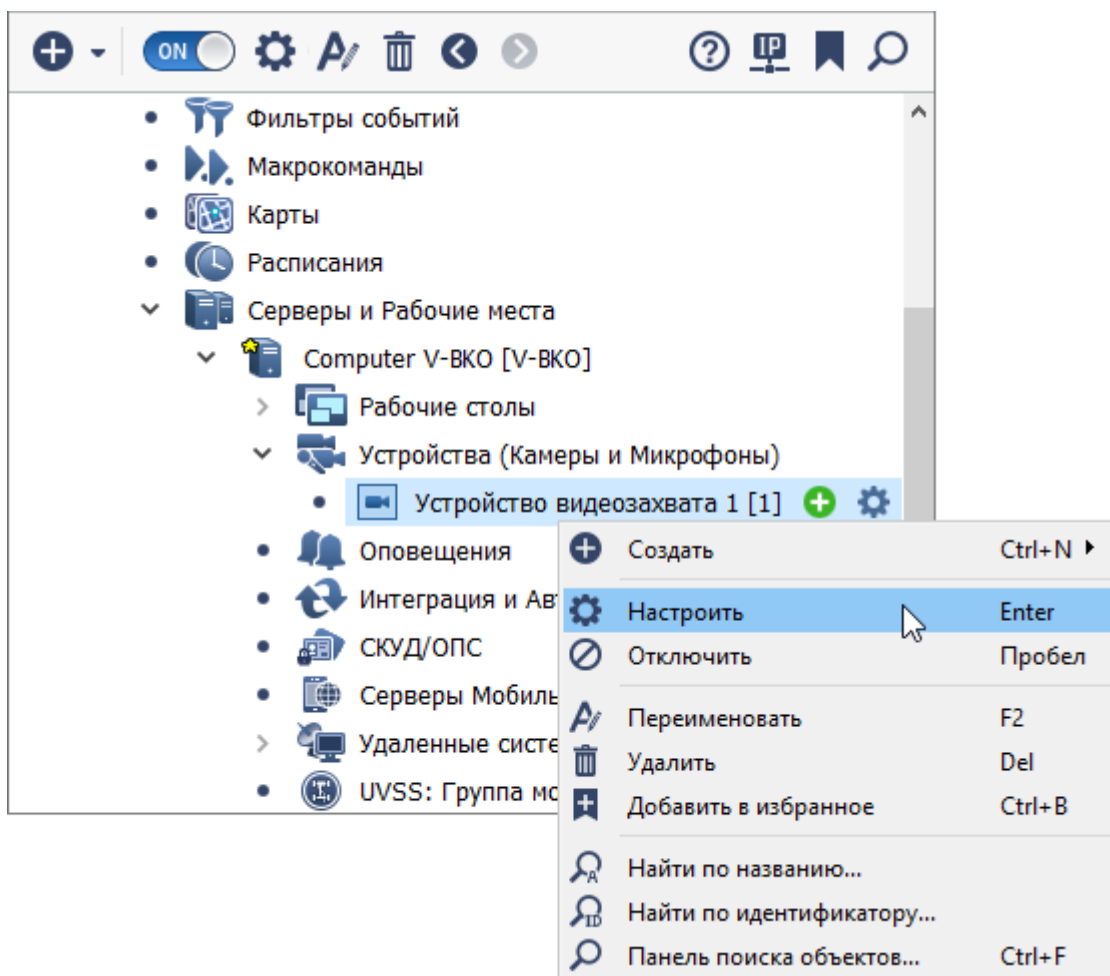


Рис. 57. Контекстное меню объекта в Дереве объектов

Для вызова контекстного меню щелкните требуемый объект правой кнопкой мыши. Из контекстного меню доступны дополнительные операции поиска объектов: **Поиск по названию** и **Поиск по идентификатору** (см. **Поиск объектов**).

6.2.1.1 Создание объекта

Чтобы создать новый объект:

1. Выделите родительский объект в *Дереве объектов*.
2. На панели инструментов или справа от объекта нажмите кнопку  (**Создать**) и выберите из списка необходимый тип объекта.
3. В окне **Параметры создаваемого объекта** задайте **Идентификатор** и **Название** создаваемого объекта. Нажмите кнопку **ОК**.
4. В окне настройки параметров объекта задайте требуемые значения. Примените изменения.

Ограничения на создание объекта

Возможная конфигурация системы (число объектов каждого типа в сети безопасности) задается в файле лицензионного ключа (key.iss). Если создано максимально допустимое количество объектов определенного типа, дополнительные объекты данного типа в сеть SecurOS добавить нельзя. Чтобы увеличить этот показатель, обратитесь в Службу технической поддержки для получения нового ключа (см. раздел **Обновление лицензионного ключа на всех серверах**).

Внимание! Если допустимое количество объектов превышено при копировании объектов с помощью *Менеджера IP-устройств*, система выведет соответствующее информационное сообщение. При этом будет создано только допустимое количество копий объекта.

6.2.1.2 Изменение параметров объекта

Чтобы просмотреть или изменить параметры объекта:

1. Выделите его в *Дереве объектов* и нажмите кнопку  (**Настроить**) на панели инструментов или справа от объекта.
2. Измените текущие параметры объекта.

Примечания:

1. Элементы окна параметров объекта описаны в разделе, соответствующем данному объекту, для каждой подсистемы (см. раздел **Программная реализация. Подсистемы SecurOS**).
 2. При выборе объектов, которые не имеют редактируемых параметров, или редактирование запрещено **Правами пользователя**, кнопка **Настройка** будет не активна.
-

3. Примените изменения.

6.2.1.3 Удаление объекта

Чтобы удалить объект:

1. Выделите его в *Дереве объектов* и нажмите кнопку  (**Удалить**) на панели инструментов.
2. Для подтверждения удаления объекта нажмите кнопку **Да**.

Внимание! Удаление объекта — необратимая процедура. При удалении объекта его дочерние объекты также будут удалены. При удалении группового объекта будут удалены все объекты группы.

6.2.1.4 Отключение/включение объекта

Чтобы временно исключить объект из сети SecurOS, не удаляя его (и, соответственно, не сбрасывая текущие настройки объекта), его можно отключить.

Чтобы отключить объект, выберите его в *Дереве объектов*, нажмите кнопку  (Отключить). Отключенный объект будет помечен значком в виде бирюзового креста (см. рис. 58).

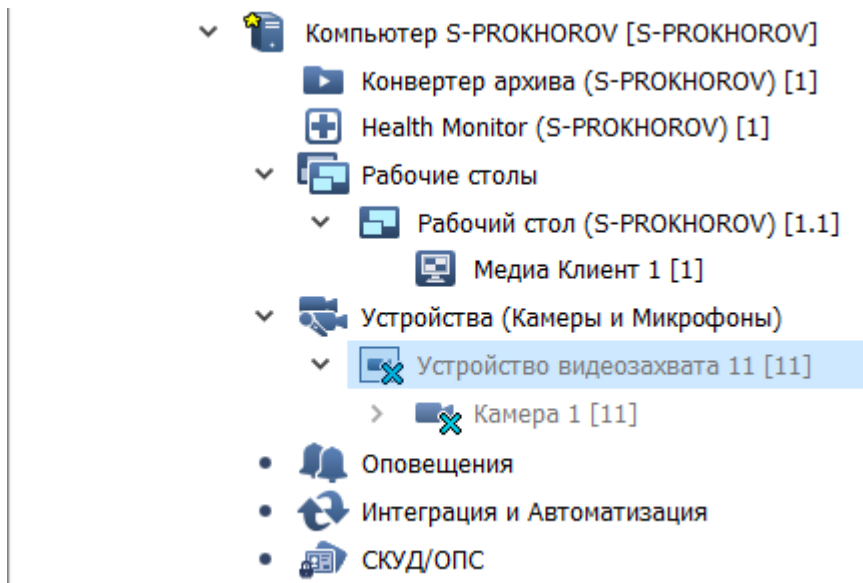


Рис. 58. Отключенный объект

Чтобы включить отключенный объект, выберите его в *Дереве объектов*, нажмите кнопку  (Включить).

Дополнительная информация

Вы можете отключить/включить все объекты группы. Для этого отключите/включите *Группу* или *Родительский объект*. При этом название объекта/группы будет выделено серым цветом.

6.2.1.5 Переименование объекта

Система позволяет переименовать любой объект с сохранением всех его настроек.

Чтобы переименовать объект:

1. Выделите объект в *Дереве объектов* и нажмите кнопку  (Переименовать).
2. Задайте новое имя объекта в появившемся диалоговом окне.
3. Для сохранения изменений нажмите кнопку **ОК**.

6.2.1.6 Поиск объектов

Поиск объектов в *Дереве объектов* осуществляется через *Панель поиска объектов* или *Окно поиска*.

- Поиск при помощи **Панели поиска объектов**.
- Поиск при помощи **Окна поиска**.

6.2.1.6.1 Поиск при помощи Панели поиска объектов

Чтобы открыть *Панель поиска объектов*, нажмите на кнопку  (**Панель поиска объектов**) на **Панели инструментов** или выберите соответствующий пункт в контекстном меню (см. рис. 59).

Для поиска объектов задайте **Параметры поиска** и нажмите на кнопку  (**Искать**). Найденная информация отображается в блоке **Результаты поиска**.

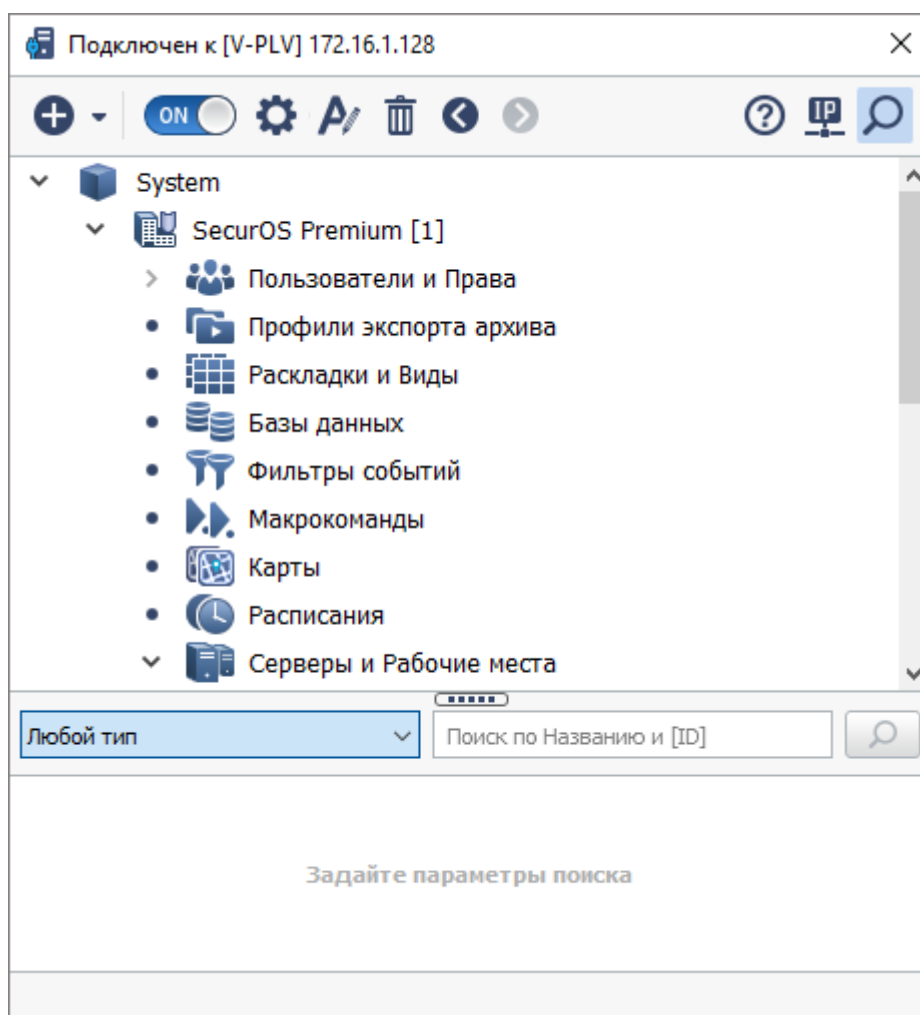


Рис. 59. Панель поиска объектов

Параметры поиска:

- **Фильтр по типу**.
- **Поиск по названию и идентификатору**.

Фильтр по типу

Выберите тип объекта, чтобы в результатах поиска содержались объекты только выбранного типа (см. рис. 60). По умолчанию выбран Любой тип, позволяющий вести поиск среди всех типов объектов. Найти нужный тип можно с помощью ввода первых символов названия типа объекта в текстовое поле **Фильтр....**

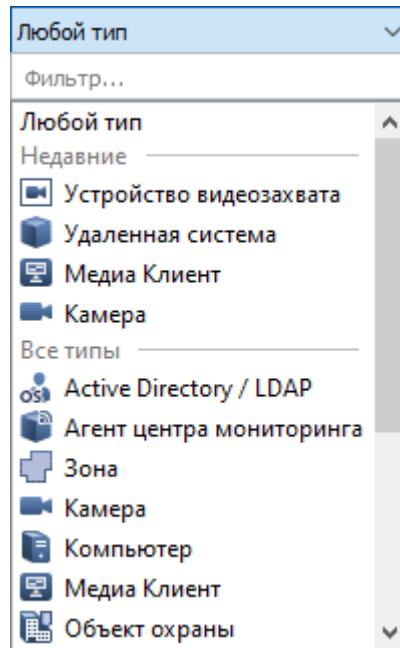


Рис. 60. Фильтр по типу

Примечание. После закрытия *Панели поиска объектов* выбранный фильтр и все поля для ввода сбрасываются. Ранее использованные фильтры могут быть найдены в списке типов объектов под заголовком **Недавние**.

Поиск по названию и идентификатору

При задании строки поиска (см. рис. 61) используйте следующие правила:

- Для поиска объекта по названию введите в текстовое поле название или часть названия объекта.
- Для поиска объекта по полному совпадению идентификатора введите идентификатор в квадратных скобках. Например, [23].
- Для поиска объектов по неполному совпадению идентификатора введите часть идентификатора с открывающей квадратной скобкой. Например, [1.
- Для поиска объекта по названию и идентификатору введите название и идентификатор, используя правила, приведенные выше. Например, при заданной строке Камера [2 будут найдены все объекты, в название которых входит слово Камера и идентификатор с цифрой 2.

Для очистки текстового поля нажмите .

Примечание. Поиск выполняется без учета регистра.

Просмотр результатов поиска

При выделении объекта в результатах поиска этот объект будет выделен и в *Дереве объектов* (см. рис. 61). С объектами на *Панели поиска объектов* можно взаимодействовать как в *Дереве объектов*.

На *Панели поиска объектов* отображаются изменения найденных объектов:

- Если объект был переименован, он выделяется курсивом.
- Если объект был удален, он зачеркивается и становится недоступным для взаимодействия.

Примечание. *Панель поиска объектов* отображает изменения (переименование и удаление) относительно состояния этих объектов на момент выполнения поиска.

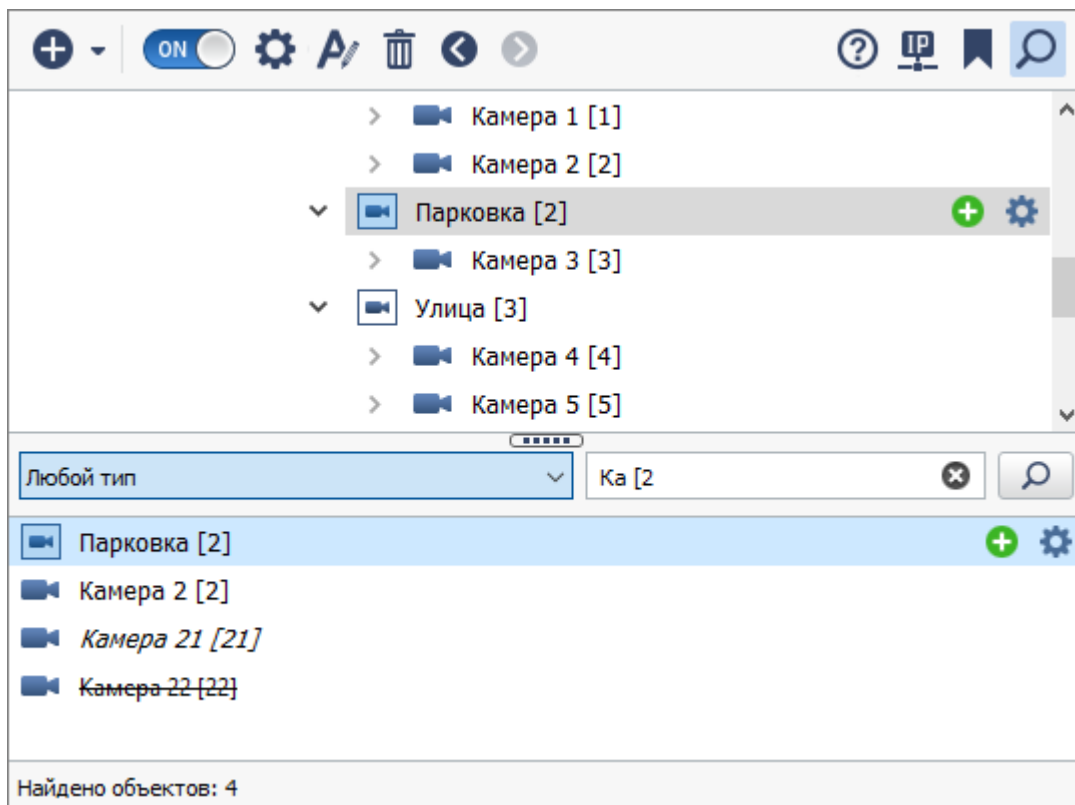


Рис. 61. Просмотр результатов поиска

Примечание. Результаты поиска отображаются только после того, как найден каждый соответствующий заданным параметрам объект. В редких случаях, если *Дерево объектов* содержит множество объектов, поиск может занимать продолжительное время. Полоса состояния отображает готовность результатов поиска.

Повторное нажатие на кнопку  (**Панель поиска объектов**) закрывает *Панель поиска объектов*.

6.2.1.6.2 Поиск при помощи Окна поиска

Чтобы найти объект по типу и названию (части названия), выполните следующие действия:

1. Вызовите контекстное меню объекта/группы в *Дереве объектов*, выберите пункт **Найти по названию**.

- В окне поиска (см. рис. 62) выберите тип объекта и введите название (или часть названия) объекта, нажмите клавишу **Enter** или кнопку **Искать**. Если такие объекты существуют, то в *Дереве объектов* будет выделен объект, соответствующий условиям поиска. Кнопки **Предыдущий** и **Следующий** станут активными.

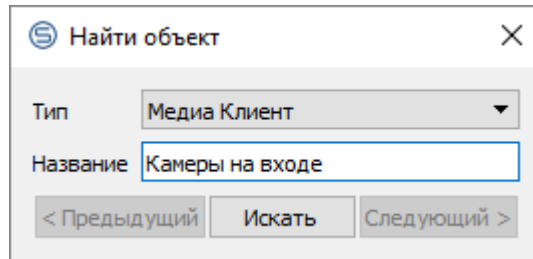


Рис. 62. Окно поиска объекта по названию

- Для продолжения поиска нажмите клавишу **Enter** (или кнопки **Предыдущий** и **Следующий** в окне поиска).
- Чтобы прекратить поиск и закрыть окно, нажмите клавишу **Esc**.

Чтобы найти объект по типу и идентификатору, выполните следующие действия:

- Вызовите контекстное меню объекта/группы в *Дереве объектов*, выберите пункт **Найти по идентификатору**.
- В окне поиска (см. рис. 63) выберите тип объекта и введите идентификатор объекта, нажмите клавишу **Enter** или кнопку **Искать**. Если объект с заданным типом и идентификатором существует, он будет выделен в *Дереве объектов*.

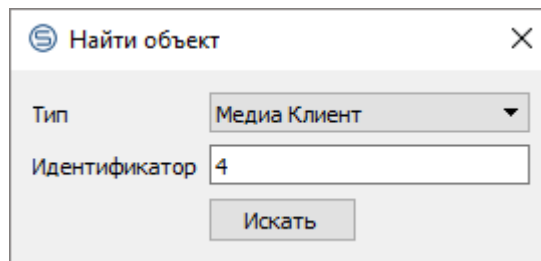


Рис. 63. Окно поиска объекта по идентификатору

- Чтобы прекратить поиск и закрыть окно нажмите клавишу **Esc**.

6.2.1.7 Избранные объекты

Для быстрого доступа к часто используемым объектам они могут быть добавлены в *Избранное*.

Нажмите на кнопку  (**Избранные объекты**) на **Панели инструментов**, чтобы вызвать *Панель избранных объектов* (см. рис. 64). Чтобы добавить объект в *Избранное*, вызовите его контекстное меню и выберите пункт **Добавить в избранное**. Чтобы удалить объект из *Избранного*, в контекстном меню выберите пункт **Убрать из избранного**. Добавленные в *Избранное* объекты помечаются в *Дереве объектов*, на *Панели избранных объектов* и на *Панели поиска объектов* особым значком .

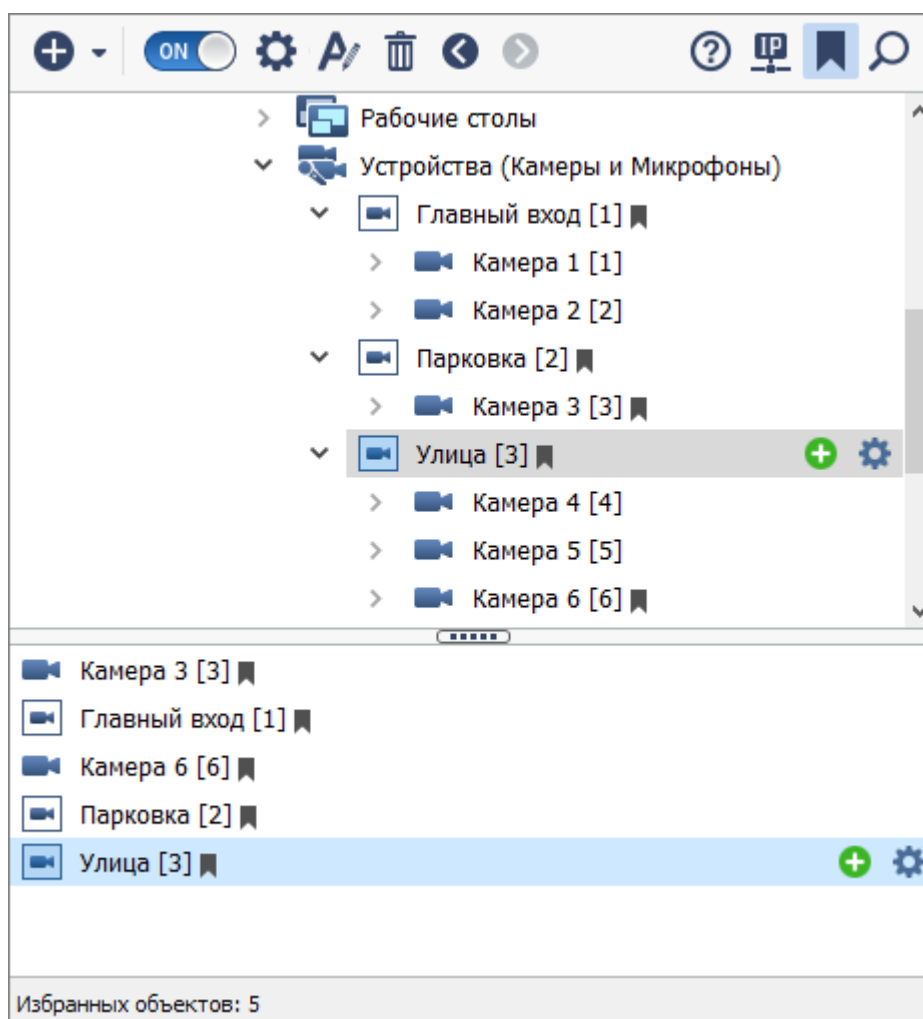


Рис. 64. Избранные объекты

Примечание. Каждый пользователь SecurOS или AD/LDAP имеет уникальный список *Избранного*, который доступен только на том компьютере, где был создан.

Повторное нажатие на кнопку  (**Избранные объекты**) закрывает *Панель избранных объектов*.

6.2.1.8 Объекты, требующие настройки

При наличии в системе проблемных объектов (объектов, настройки которых требуют изменений для корректного функционирования данных или связанных объектов) *Центр администрирования* выглядит следующим образом (см. рис. 65):

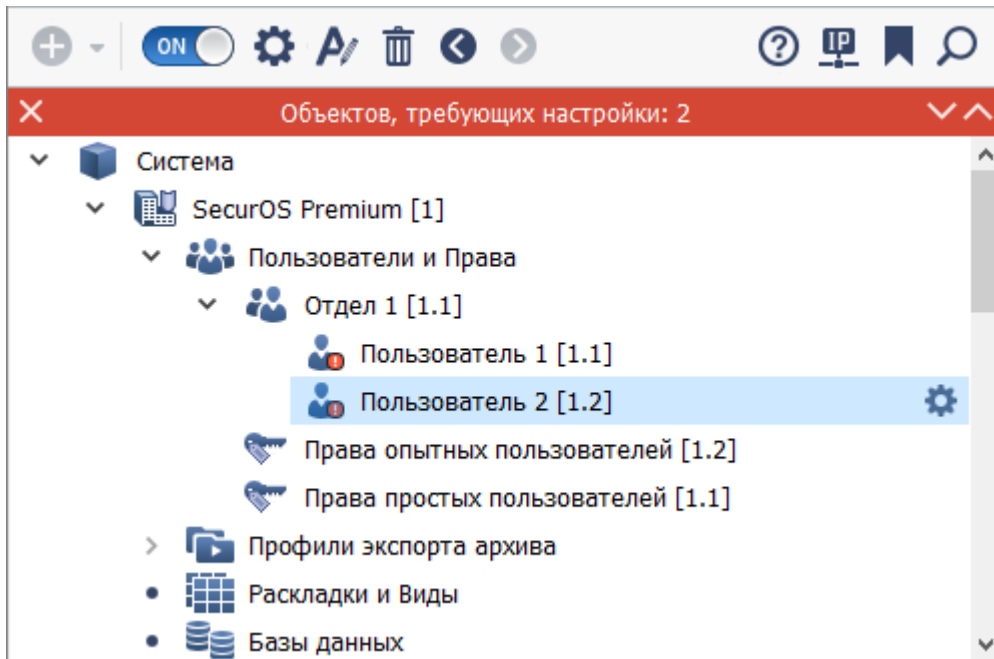


Рис. 65. Центр администрирования при наличии в системе проблемных объектов

Между **Панелью инструментов** и **Деревом объектов** отображается баннер красного цвета. В заголовке баннера выводится строка **Объектов, требующих настройки:** и количество таких объектов в **Дереве**. Проблемные объекты помечаются значком . Для поиска проблемных объектов в *Дереве объектов* используйте кнопки , расположенные в правой части баннера. Поиск будет выполняться в выбранном направлении, начиная от текущего активного объекта.

Примечание. Баннер можно скрыть, нажав кнопку в левой части. Работа с *Деревом объектов* будет продолжена в обычном режиме. При этом скрытый баннер будет отображаться автоматически при каждом следующем вызове *Центра администрирования*.

Описание проблемы выводится непосредственно в окне настройки параметров проблемного объекта, например, см. рис. [66](#).

Необходим повторный ввод пароля ⓘ

Пароль:

Телефон:

E-mail:

Дополнительная информация:

ОК Отмена Применить

Рис. 66. Окно настройки параметров проблемного объекта Пользователь

6.2.2 Работа с табличными параметрами объектов

Окно настройки параметров объекта может содержать как простые текстовые поля, так и таблицы. Пример табличного параметра (**Праздничные дни**) представлен на рис. 67.

Общие Серверы для подключения Ограничение подключений Управление паролями

Размер базы протокола (дней):

При старте запускать Макрокоманду:

Праздничные дни:

01.01.2024
08.03.2024
09.05.2024

+

-

ОК Отмена Применить

Рис. 67. Пример табличного параметра объекта

При работе с табличным параметром используются следующие приемы:

- Чтобы добавить строку в таблицу, используйте клавишу ↓ или щелкните мышью поле ниже последней записи списка.
- Чтобы удалить элемент из таблицы, выделите требуемую строку и нажмите на клавиатуре клавишу **Delete**.

6.2.3 Работа со списками флажков

Список флажков в параметрах объекта может содержать большое количество элементов и состоять из нескольких уровней. Пример параметра (**Медиа Клиент, Закладка Камеры**) со списком флажков приведен на рис. 68.

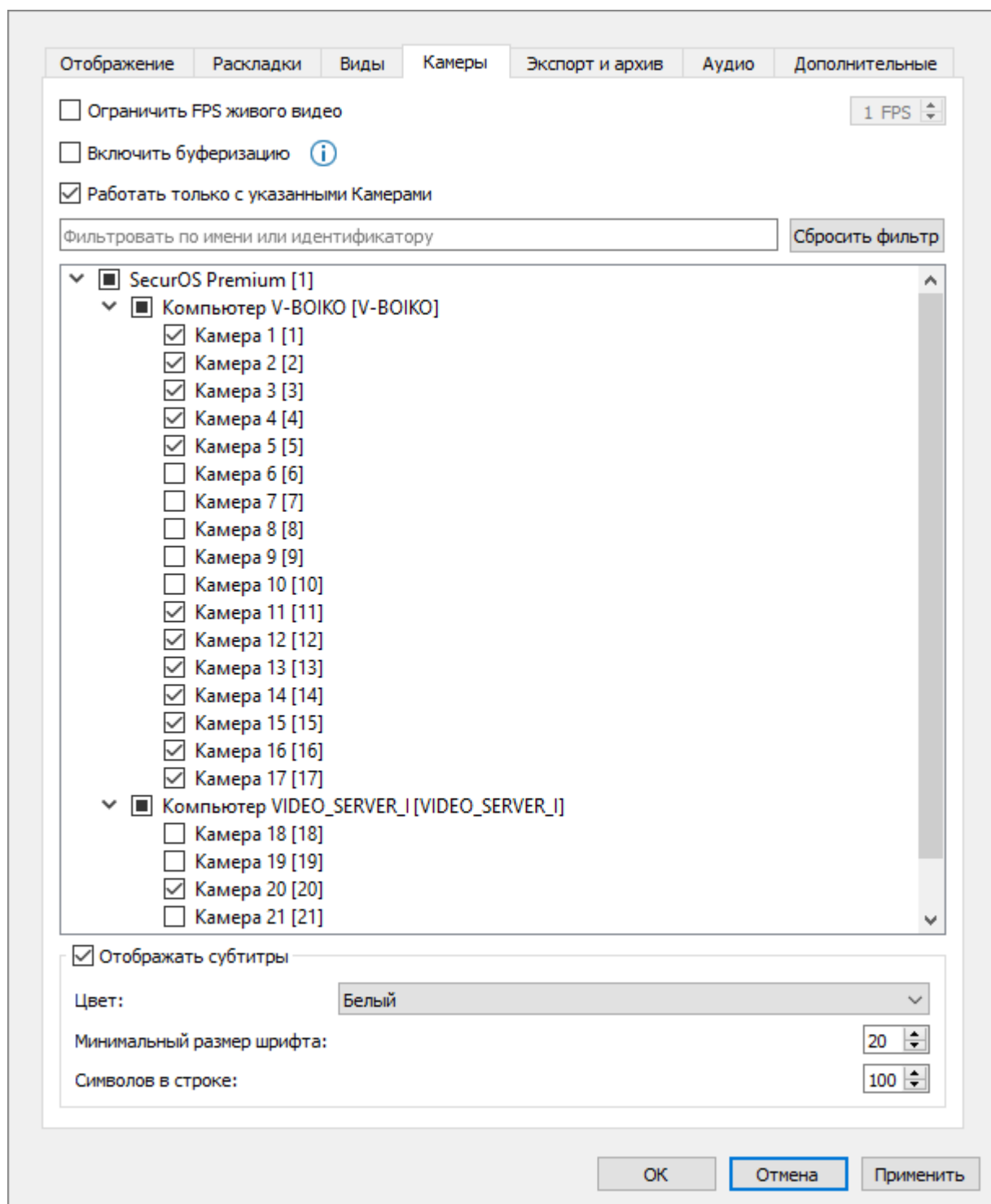


Рис. 68. Пример параметра со списком флажков

Для настройки параметров со списком флажков предусмотрена функция массовой установки/снятия флажков:

- Чтобы установить или снять **все** дочерние флажки, установите/снимите флажок родительского элемента.
- Чтобы установить или снять **несколько** флажков, сначала выберите первый флажок. Зажмите клавишу **Shift** и выберите второй флажок, все флажки до которого (включительно) должны быть установлены/сняты.

Массовый выбор флажков действует согласно следующим правилам:

- Массовый выбор флажков возможен только в пределах одного уровня списка.
- Состояние второго флажка определяет результат массового выбора. Например, если с зажатой клавишей **Shift** выбирается уже отмеченный флажок, все массово выбранные флажки становятся неотмеченными.
- Второй флажок определяет начало для следующего действия массового выбора.

6.2.4 Добавление IP-устройств

Чтобы иметь возможность управлять сетевым IP-устройством из SecurOS, необходимо выполнить следующие операции:

1. Подключить новое устройство к физической сети. При подключении IP-устройству будет назначен IP-адрес и, при необходимости, некоторые другие параметры.
2. Создать в *Дереве объектов SecurOS* объекты, соответствующие типу подключенного устройства (*Устройство видеозахвата* с дочерней *Камерой* или *Устройство аудиозахвата* с дочерним *Микрофоном*).
3. Настроить созданные объекты, т.е. присвоить им IP-адреса, назначенные устройствам при добавлении в физическую сеть, и указать прочие параметры доступа к устройствам (например, пароль доступа к устройству и имя пользователя).

После выполнения указанных операций устройством можно управлять из SecurOS.

IP-устройство можно добавить в *Дерево объектов SecurOS* несколькими способами:

- **Добавление копированием.**
- **Добавление с помощью Менеджера IP-устройств.**
- **Добавление с помощью Центра администрирования.**

Добавление копированием

При добавлении копированием используется как **Центр администрирования**, так и **Менеджер IP-устройств**. Способ используется для добавления в *Дерево объектов SecurOS* большого количества устройств со сходными параметрами (например, множества камер одного и того же **Типа** и **Модели**, у которых отличаются только последние цифры IP-адреса).

Чтобы добавить множество устройств копированием:

1. С помощью **Центра администрирования** создайте в *Дереве объектов* одно устройство и его дочерний объект (см. **Создание объекта**). Например, *Устройство видеозахвата* и *Камеру*.
2. Настройте добавленные объекты (см. **Устройство видеозахвата**, **Камера**, **Изменение параметров объекта**).
3. С помощью **Менеджера IP-устройств** выполните копирование созданных объектов (см. **Копирование IP-устройства**).

Примечание. При копировании во вновь создаваемых устройствах полностью дублируются настройки копируемых устройств. Это удобно, например, если все такие устройства имеют одинаковое предназначение в сети безопасности SecurOS.

4. В *Дереве объектов SecurOS* донастройте созданные устройства вручную.

Добавление с помощью Менеджера IP-устройств

С помощью **Менеджера IP-устройств** можно добавить в *Дерево объектов SecurOS* большое количество устройств разных типов с различными настройками. Чтобы добавить IP-устройство (-а), выполните операции **Поиск устройств в сети** и **Добавление IP-устройства**.

Внимание! При добавлении многие параметры устройств принимают значения по умолчанию. При необходимости настройте добавленные устройства вручную (см. **Изменение параметров объекта**).

Добавление с помощью Центра администрирования

Центр администрирования используется, как правило, для добавления в *Дерево объектов SecurOS* небольшого количества IP-устройств с сильно отличающимися настройками (например, камеры разных типов). Чтобы добавить камеру, создайте и настройте объекты **Устройство видеозахвата** и **Камера** (см. **Создание объекта**). Чтобы добавить микрофон, создайте и настройте объекты **Устройство аудиозахвата** и **Микрофон** (см. **Создание объекта**).

6.2.5 Менеджер IP-устройств

Менеджер IP-устройств разработан для поиска и управления настройками найденных IP-устройств в сети безопасности SecurOS.

Поиск устройств осуществляется с помощью стандартных сетевых технологий (см. раздел **Поиск устройств в сети**) в локальной сети того *Компьютера*, на котором запущен *Менеджер*. Вновь найденные устройства считаются ненастроенными; с таким устройствами можно выполнять следующие операции:

- **Добавление IP-устройства;**
- **Редактирование параметров IP-устройства.**

С устройствами, уже зарегистрированными в сети (с помощью *Менеджера* или стандартными средствами) можно выполнять следующие операции:

- **Редактирование параметров IP-устройства;**
- **Удаление IP-устройства.**

6.2.5.1 Описание экранной формы

Главное окно приложения представлено на рис. 69.

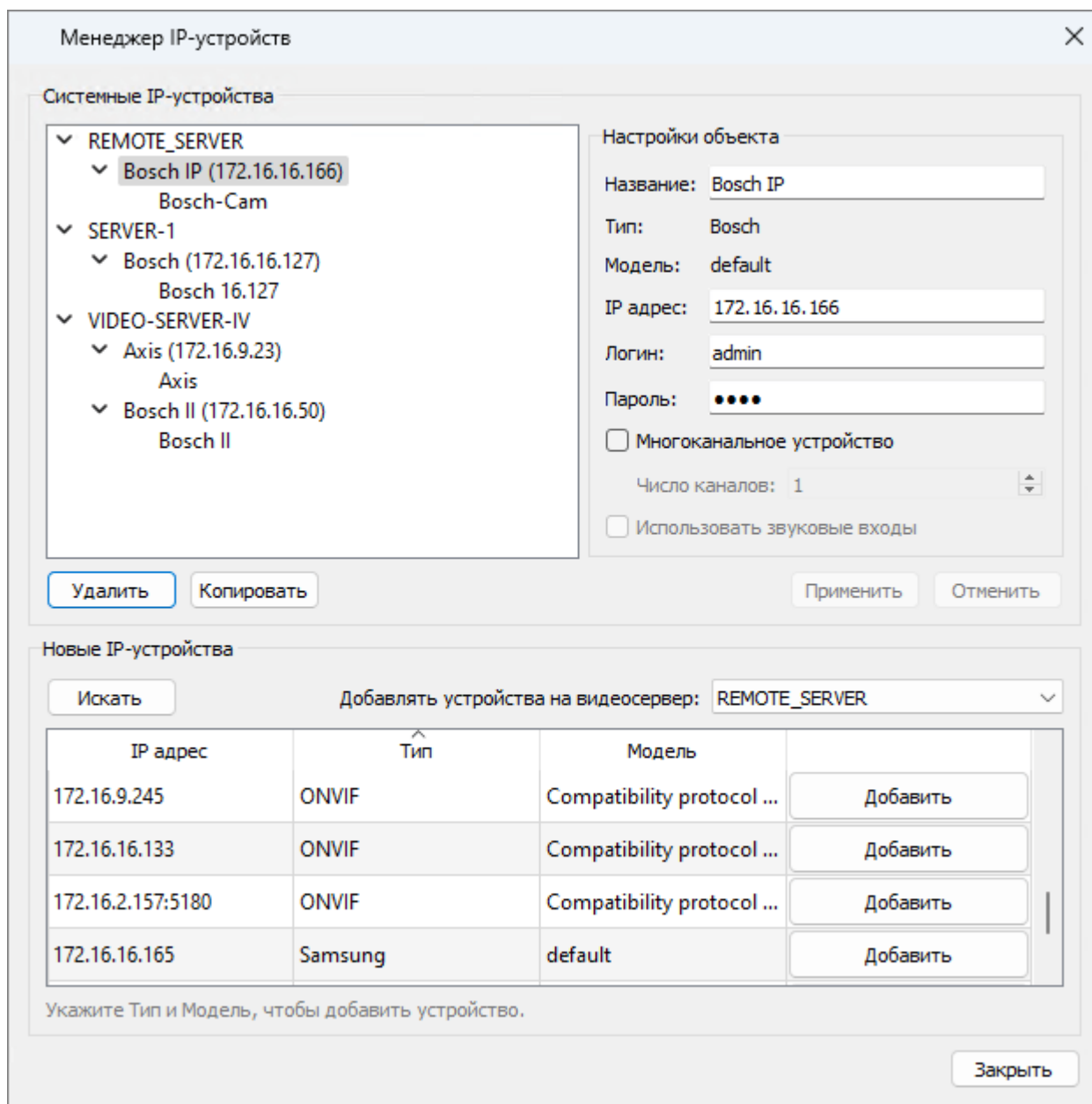


Рис. 69. Менеджер IP-устройств

Окно содержит следующие элементы управления (см. табл. 3):

Таблица 3. Элементы управления окна Менеджера IP-устройств

Параметр	Описание
Системные IP-устройства	

Параметр	Описание
Дерево объектов	Дерево <i>Компьютеров</i> с ролью <i>Видеосервер</i>, существующих в сети SecurOS. При развертывании узла для каждого <i>Видеосервера</i> отображаются все дочерние <i>Устройства видеозахвата</i> с дочерними <i>Камерами</i>. Если в устройстве используется встроенный аудиоканал или оно настроено на синхронный режим записи (см. раздел Синхронная запись и воспроизведение аудио- и видеопотока), в дереве также отображаются все соответствующие устройству объекты <i>Микрофон</i>. Примечания: 1. Объекты, настройки которых редактируются в текущий момент времени, отображаются в Дереве объектов <i>курсивом</i>. 2. Объекты, отключенные в SecurOS, отображаются в Дереве объектов серым (затеняются), аналогично неактивным объектам Windows.
Настройки объекта	
Название	Имя объекта, выделенного в Дереве объектов (см. выше). Примечание. На имена объектов накладываются следующие ограничения: 1. Имя не может быть пустым. 2. Имя должно быть уникальным.
Тип, Модель	Тип и модель устройства, выделенного в Дереве объектов. Информационные поля, недоступны для редактирования пользователем.
IP-адрес	IP-адрес устройства.
Логин, Пароль	Логин/Пароль доступа к устройству. По умолчанию, при добавлении устройства, присваиваются значения admin/admin. Внимание! Если логин и пароль были присвоены устройству ранее (при физическом добавлении устройства в сеть) с помощью web-интерфейса, введите данные значения, в противном случае доступ к устройству будет невозможен.
Многоканальное устройство	Отметьте флаг, если добавленное устройство представляет собой IP-видеосервер со множеством физических видео входов, либо IP-камеру с несколькими объективами. Ограничения. Для использования функциональности в системе должны выполняться следующие условия: 1. Устройство должно поддерживать несколько независимых видеопотоков. 2. Программное обеспечение интеграции устройства должно поддерживать многоканальность.

Параметр	Описание
Число каналов	Количество используемых независимых видеоканалов многоканального устройства. Примечание. Максимальное количество видео каналов устройства определяется Типом и Моделью устройства.
Использовать звуковые входы	Отметьте флаг, если необходимо использовать звуковые входы (или встроенный микрофон) устройства. Максимальное количество аудио каналов устройства зависят от Типа и Модели устройства, и определяется в программном обеспечении интеграции устройства. При этом, в общем случае, количество аудио каналов $\leq$ количеству каналов видео. Ограничения. Для использования функциональности в системе должны выполняться следующие условия: 1. Устройство должно быть оборудовано звуковыми входами. 2. В программном обеспечении интеграции устройства в SecurOS должна быть предусмотрена поддержка звука.
Кнопки	
Удалить	Удаление <i>Устройства видеозахвата</i> , выделенного в Дереве объектов Менеджера .
Копировать	Копирование <i>Устройства видеозахвата</i> , выделенного в Дереве объектов Менеджера (см. раздел Копирование IP-устройства).
Применить, Отменить	Сохранение новых или измененных настроек устройства/Отмена изменений с сохранением предыдущего набора параметров. Примечания: 1. Кнопки активны только в случае присвоения значений/изменения текущих настроек устройства на закладках Настройка и/или Использование. 2. Если после изменения текущих настроек устройства до сохранения или отказа от изменений была нажата кнопка Заккрыть, система выведет запрос на сохранение произведенных изменений.
Новые IP-устройства	
Искать	Запуск процедуры поиска ненастроенных сетевых IP-устройств в локальной сети того <i>Компьютера SecurOS</i> , на котором был запущен <i>Менеджер IP-устройств</i> .

Параметр	Описание
Добавлять устройства на видеосервер	Укажите <i>Видеосервер</i> , в дереве объектов которого будет создано новое <i>Устройство видеозахвата</i> , ассоциированное с выбранным ниже сетевым IP-устройством (см. Таблица IP-устройств ниже), и на котором будет создаваться и храниться видеоархив данного устройства. По умолчанию принимает значение имени <i>Компьютера</i> , с которого запущен <i>Менеджер IP-устройств</i> .
Таблица IP-устройств	Таблица найденных ненастроенных IP-устройств. Примечание. Ненастроенным считается IP-устройство, для которого в сети SecurOS не существует родительского объекта <i>Устройство видеозахвата</i> с IP-адресом, указанным в поле IP-адрес (см. ниже). • IP-адрес — IP адрес обнаруженного устройства. Примечание. Если при первоначальном присвоении IP-адреса устройству был назначен порт, то его значение дополнительно отображается в данном поле в стандартном формате (например, 192.16.0.185:8080). • Тип — тип IP-устройства. Заполняется автоматически в зависимости от результатов распознавания. • Модель — модель IP-устройства. Заполняется автоматически в зависимости от результатов распознавания. • Добавить — добавление выбранного сетевого IP-устройства на выбранный <i>Видеосервер</i>.

Для завершения приложения и закрытия окна **Менеджер IP-устройств** нажмите кнопку **Закрыть**.

6.2.5.2 Базовые операции

Раздел содержит описание следующих операций, выполняемых с помощью *Менеджера IP-устройств*:

- **Поиск устройств в сети;**
- **Добавление IP-устройства;**
- **Редактирование параметров IP-устройства;**
- **Копирование IP-устройства;**
- **Удаление IP-устройства.**

Внимание! В случае потери соединения с **Сервером конфигураций** выполнение операций блокируется до восстановления соединения.

6.2.5.2.1 Запуск Менеджера

Для запуска *Менеджера IP-устройств* выполните следующие действия:

1. Откройте **Центр администрирования**.
2. На *Панели инструментов* (см. рис. 70) нажмите кнопку  (**Менеджер IP-устройств**).

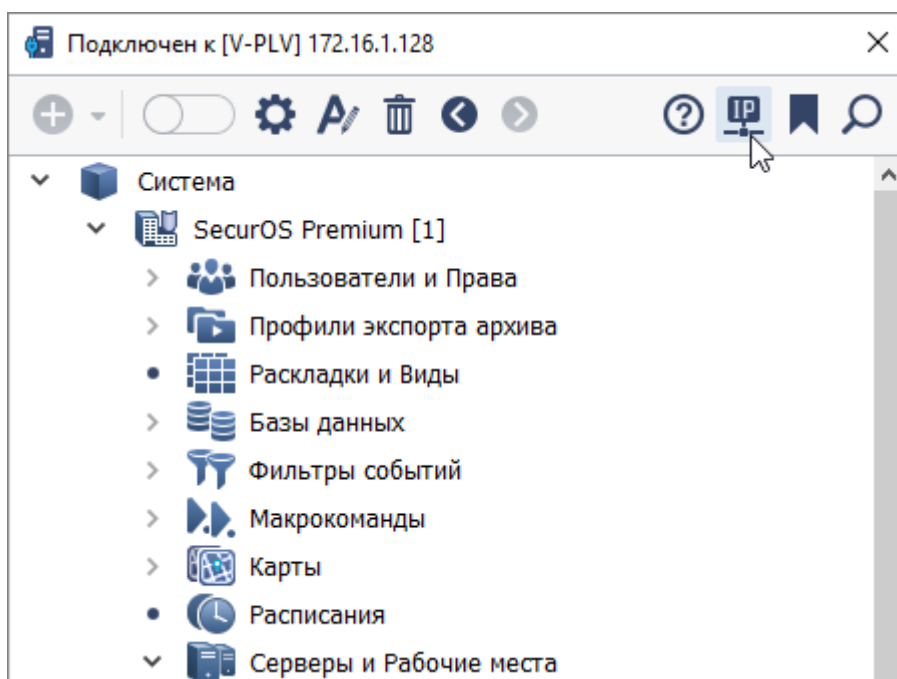


Рис. 70. Запуск Менеджера IP-устройств

Примечания: Кнопка **Менеджер IP-устройств** недоступна в следующих случаях:

1. Открыто окно настройки параметров какого-либо объекта SecurOS.
2. Потеряна связь с *Сервером конфигураций*.

3. Система выведет окно **Менеджер IP-устройств** (см. раздел **Описание экранной формы**).

Внимание! Если окно **Менеджер IP-устройств** активно, режим редактирования параметров объектов SecurOS блокируется (т.е. вызов окна настройки параметров объекта из *Дерева объектов* SecurOS невозможен).

6.2.5.2.2 Поиск устройств в сети

Для поиска IP-устройств в сети SecurOS выполните следующие действия:

1. Войдите в режим администрирования и запустите *Менеджер IP-устройств*.
2. В блоке **Новые IP-устройства** нажмите кнопку **Искать**. Система выполнит поиск и отобразит все найденные устройства в **Таблице IP-устройств** (см. рис. 71).

Новые IP-устройства

Искать

Добавлять устройства на видеосервер: SERVER-1

IP адрес	Тип	Модель	
172.16.9.23	Axis	P1354	Добавить
172.16.16.228	Axis	P1365	Добавить
172.16.16.127	Bosch	default	Добавить
172.16.16.166	Bosch	default	Добавить

Укажите Тип и Модель, чтобы добавить устройство.

Рис. 71. Результат поиска устройств

Параметры и результаты процедуры поиска не имеют каких-либо ограничений (например, по времени поиска) со стороны SecurOS.

Дополнительная информация

При наведении курсора на поле **IP адрес** выводится всплывающая подсказка, в которой отображается ответ устройства, полученный при опросе сети. В общем случае строка подсказки состоит из 3 полей в следующем формате: <Производитель устройства> <Модель устройства> (<Название устройства>). Например, Beward BD2570 (H.264 5M box camera).

Внимание! В Таблице IP-устройств отображаются все найденные в сети устройства, включая принтеры, сканеры и т.д.

6.2.5.2.3 Добавление IP-устройства

Для добавления IP-устройства выполните следующие действия:

1. Войдите в режим администрирования и запустите *Менеджер IP-устройств*.
2. В блоке **Новые IP-устройства** окна *Менеджера* нажмите кнопку **Искать**. *Менеджер* проведет опрос сети и выведет список ненастроенных IP-устройств в **Таблицу IP-устройств**.
3. В поле **Добавлять устройство на видеосервер** выберите тот *Компьютер* сети SecurOS, на который следует добавить устройство.
4. В **Таблице IP-устройств** выберите устройство, которое необходимо добавить в сеть, далее выполните следующие действия:
 - Для нераспознанного устройства (определен только **IP-адрес**):
 - В строке выбранного устройства щелкните мышью ячейку **Тип**, в выпадающем списке выберите тип устройства (см. рис. 72).

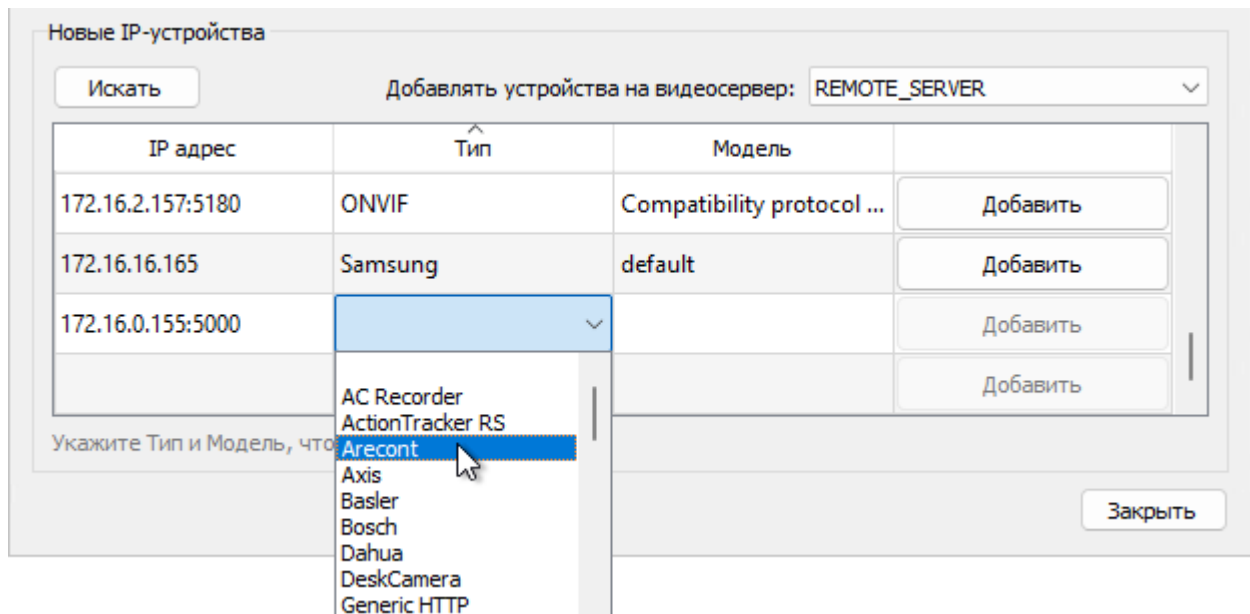


Рис. 72. Выбор Типа добавляемого устройства

- Щелкните мышью ячейку **Модель**, в выпадающем списке выберите модель устройства. Если требуемая модель отсутствует в списке, выберите значение default. Система активирует кнопку **Добавить**.
 - Для распознанного устройства (определены параметры **IP-адрес**, **Тип** и **Модель**):
 - Выберите устройство из **Таблицы IP-устройств**.
 - Для произвольного устройства (таблица не содержит информации об устройстве):
 - В последней (пустой) строке таблицы щелкните мышью ячейку **Тип**, в выпадающем списке выберите тип устройства.
 - Щелкните мышью ячейку **Модель**, в выпадающем списке выберите модель устройства.
5. Нажмите кнопку **Добавить**.

Примечание. В случае, если добавление устройства невозможно вследствие лицензионных ограничений или потери связи с *Сервером конфигураций*, система выведет соответствующее информационное сообщение.

Система создаст новое *Устройство видеозахвата* с заданными параметрами и добавит его в **Дерево объектов Менеджера** на выбранный *Компьютер*; добавленное устройство будет текущим выделенным устройством дерева. Для добавленного *Устройства видеозахвата* будет автоматически создан объект *Камера*, детальное редактирование параметров которого возможно в режиме администрирования из *Дерева объектов SecurOS*.

Примечание. Каждому добавляемому устройству по умолчанию присваивается имя *Устройство видеозахвата N*, где N — очередной порядковый цифровой идентификатор объектов данного типа в системе.

6. Далее выполните операцию **Редактирование параметров IP-устройства**.

6.2.5.2.4 Редактирование параметров IP-устройства

Для задания/изменения параметров устройства выполните следующие действия:

1. В **Дереве объектов Менеджера** выберите устройство, параметры которого следует задать/отредактировать.
2. В блоке **Настройки объекта** (см. рис. 73) отредактируйте параметры добавленного устройства:

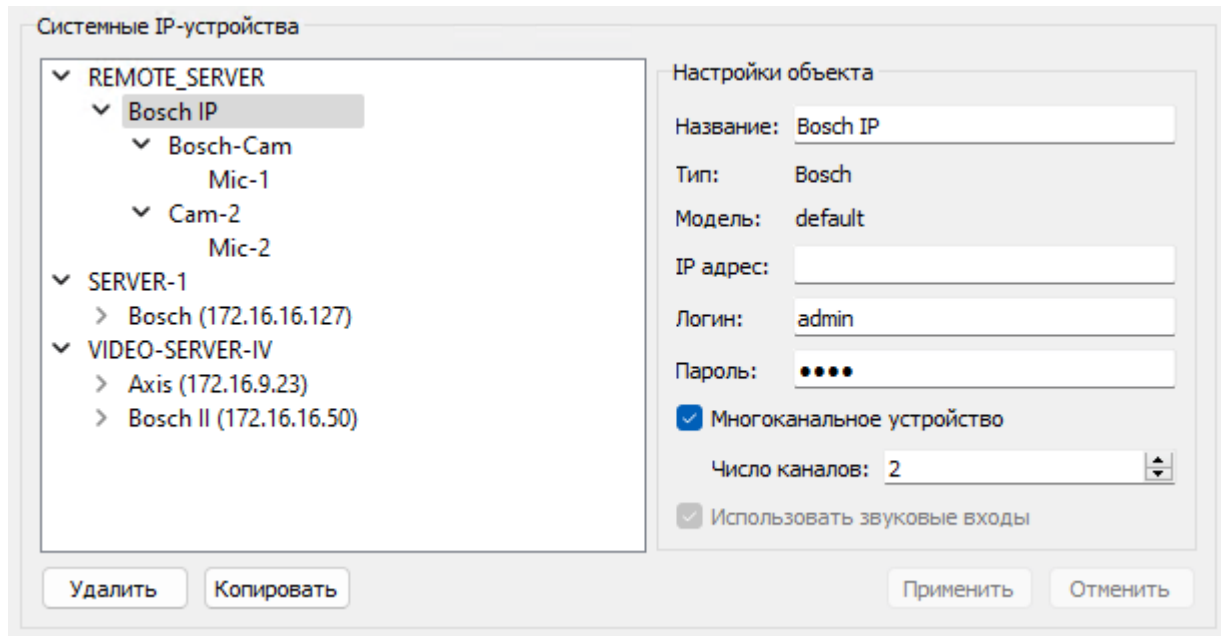


Рис. 73. Настройка звуковых входов устройства

- При необходимости в поле **Название** измените имя устройства.
 - При необходимости укажите или измените **IP-адрес** устройства.
 - При необходимости измените присвоенные по умолчанию **Логин/Пароль** доступа к *Устройству видеозахвата* (admin/admin).
 - В случае, если добавленное устройство является многоканальным, активируйте поле **Многоканальное устройство** и задайте требуемое число каналов. В зависимости от заданного значения в *Дереве объектов SecurOS* будет создано соответствующее количество объектов *Камера*, дочерних данному *Устройству видеозахвата*, которые также будут отображаться в *Дереве объектов Менеджера*. *Камере* с наименьшим идентификатором присваивается **Номер канала** равный 1, далее каналы нумеруются с шагом 1.
 - В случае, если добавленное устройство поддерживает звук, активируйте флаг **Использовать звуковые входы**. В *Дереве объектов SecurOS* будет автоматически создан объект *Устройство аудиозахвата* с одним или несколькими, в случае многоканального устройства, дочерними объектами *Микрофон*. В *Дереве объектов Менеджера* такие микрофоны будут привязаны к соответствующему количеству камер устройства (см. рис. 73), а в *Дереве объектов SecurOS* — прописаны в настройках соответствующих *Камер*.
3. Нажмите кнопку **Применить**.

6.2.5.2.5 Копирование IP-устройства

Операция позволяет быстро создавать до 99 копий существующего в SecurOS настроенного *Устройств видеозахвата*.

Для каждой копии сохраняются следующие основные параметры и дочерние объекты выбранного исходного устройства:

1. **Тип** устройства;
2. **Модель** устройства;
3. Прочие параметры, определяемые **Типом** и **Моделью** устройства;
4. Дочерние *Камеры*. Количество дочерних *Камер* каждой копии будет соответствовать количеству *Камер* исходного устройства.

Не копируются следующие связанные объекты и параметры:

1. *Устройства аудиозахвата*.
2. *Микрофоны*.
3. Параметры *Камеры*:
 - **Микрофон**;

Примечание. За исключением встроенных микрофонов. Т.е. если в настройках *Камеры* отмечен флаг **Микрофон** и выбрано значение *Встроенный* (см. [Закладка Аудио](#)), то такой *Микрофон* и все его параметры будут скопированы без ограничений.

- **Препозиции**;
- **Туры**;
- **Дворник**;
- **Омывающее устройство**;
- **Зоны**. Создается одна зона по умолчанию (Main).

Для копирования *Устройства видеозахвата* выполните следующие действия:

1. В блоке **Системные IP-устройства** (см. [Описание экранной формы](#)) выберите объект, который необходимо скопировать.

Внимание! Устройство, настройки которого не сохранены в *Менеджере IP-устройств*, не может быть скопировано.

2. Нажмите кнопку **Копировать**. В зависимости от типа исходного *Устройства видеозахвата* система выведет определенное окно **Копирование** (см. рис. 74).

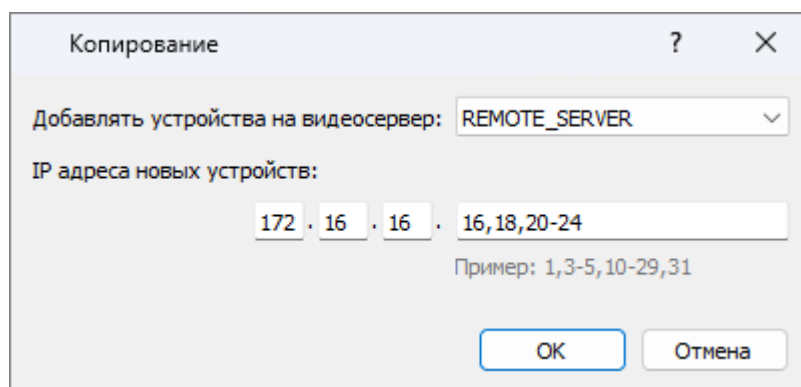


Рис. 74. Окно параметров копирования для IP-камер

3. Выберите **Видеосервер**, на который будут добавлены новые устройства, задайте **Количество копий** устройства или укажите **IP-адреса** новых устройств. Нажмите кнопку **ОК**.

Примечание. В случае, если в параметре **IP-адрес** копируемого устройства был задан **Порт**, этот порт будет указан в каждой копии устройства без изменений.

4. Система создаст требуемое количество копий исходного устройства на указанном *Видеосервере*.
5. При необходимости настройте каждую созданную копию устройства (закладка **Настройка объекта**). Нажмите кнопку **Применить**.

6.2.5.2.6 Удаление IP-устройства

Для удаления устройства выполните следующие действия:

1. Войдите в режим администрирования и запустите *Менеджер IP-устройств*.
2. В **Дереве объектов Менеджера** выберите устройство, которое необходимо удалить.
3. В блоке **Системные IP-устройства** нажмите кнопку **Удалить**. Указанное устройство будет удалено со всех **Видеосерверов** вместе со всеми дочерними/связанными объектами.

6.3 Пользователи и Права

Разграничение доступа к объектам SecurOS и операциям с ними осуществляется на основе прав, назначаемых каждому пользователю. Пользователи и их права могут быть заданы как на этапе первоначальной настройки системы (см. **Настройка при помощи Мастера первоначальной настройки**), так и при ее дальнейшей эксплуатации (см. **Регистрация и настройка прав пользователей**).

Управление пользователями и их правами осуществляется с помощью следующих объектов SecurOS:

- **Отдел** — используется для объединения *Пользователей* в группы, например, в зависимости от роли пользователя в системе.
- **Пользователь** — служит для создания персональной учетной записи пользователя SecurOS (содержит логин и пароль, которые используются для авторизации в системе).
- **Active Directory / LDAP** — с помощью объекта возможна авторизация в SecurOS пользователей ОС Windows, зарегистрированных в домене Active Directory Windows.

Внимание! В ОС Linux функциональность *Active Directory / LDAP* не поддерживается.

- **Права пользователя** — используется для назначения пользователям (как типовым *Пользователям* SecurOS, так и пользователям ОС) *Прав доступа* к объектам SecurOS и операциям с ними. Подробнее см. **Регистрация и настройка прав пользователей**.

Детальная информация о пользователях, их правах, объектах SecurOS, используемых для настройки приведена в следующих подразделах:

- **Пользователи в SecurOS**;
- **Регистрация и настройка прав пользователей**;
- **Пример настройки прав пользователей сетевого домена**.

6.3.1 Пользователи в SecurOS

Авторизоваться и работать с SecurOS могут следующие пользователи:

- **Суперпользователь SecurOS.**
- **Типовой пользователь SecurOS.**
- **Пользователь ОС, зарегистрированный в домене.**

Суперпользователь SecurOS

Учетная запись суперпользователя со значениями root (имя пользователя) и паролем, указанным администратором (по умолчанию securos), создается при настройке системы с помощью Мастера первоначальной настройки. Набор прав такой учетной записи предоставляет пользователю полный доступ ко всем объектам сети безопасности и права на выполнение любых действий в сети. Объекты учетной записи суперпользователя не отображаются в *Дереве объектов* SecurOS. Изменить имя и набор прав суперпользователя невозможно.

Внимание! Пароль учетной записи суперпользователя можно сменить с помощью Мастера первого запуска (см. п. 4 в разделе **Настройка при помощи Мастера первоначальной настройки**) или при дальнейшей эксплуатации системы (см. **Смена пароля суперпользователя**).

Типовой пользователь SecurOS

Учетная запись типового пользователя SecurOS может быть создана как с помощью Мастера первоначальной настройки, так и при дальнейшей эксплуатации системы. Операции создания учетной записи типового пользователя и настройки его прав описаны в разделе **Регистрация и настройка прав пользователей**.

Для смены/сброса паролей уже созданных учетных записей типовых пользователей см. **Смена/сброс пароля типового пользователя**.

Пользователь ОС, зарегистрированный в домене

Кроме указанных выше пользователей, с SecurOS может работать любой пользователь операционной системы Windows, зарегистрированный в домене Active Directory Windows. Операции регистрации такого пользователя в SecurOS и настройки его прав описаны в следующих разделах:

- **Регистрация и настройка прав пользователей.**
- **Пример настройки прав пользователей сетевого домена.**

6.3.1.1 Смена пароля суперпользователя

Чтобы сменить пароль суперпользователя:

1. Войдите в систему под учетной записью суперпользователя (см. **Пользователи в SecurOS**).
2. Откройте окно настройки параметров корневого объекта *Система* (см. рис. 75).

Пароль суперпользователя

Новый пароль: [маска]

Подтвердите новый пароль: [маска]

Доступ из Центра Мониторинга и Контроля

☒ Разрешить доступ: [маска]

☐ Запретить привилегированный доступ

Центр Мониторинга и Контроля

☒ Привилегированный доступ к Удаленным системам

Прокси-сервер для FaceX: [i] Не использовать [v]

Сохранение и восстановление конфигурации

[Сохранить] [Восстановить]

☒ Автоматическое создание резервных копий [i]

Максимальное количество копий: 10 [v]

Аудит

☐ Записывать данные аудита системы

Период аудита: [i] 5 минут [v]

Безопасность

☐ Использовать защищённые соединения [i]

☒ Разрешить незащищённые подключения

☐ Принимать только TLS-подключения

[OK] [Отмена] [Применить]

Рис. 75. Окно настройки параметров объекта Система

3. В блоке **Пароль суперпользователя** введите и подтвердите новый пароль. Для сохранения изменений нажмите кнопку **ОК**.

Внимание! Минимальная длина пароля суперпользователя 7 символов. После изменения пароля храните его в секрете.

6.3.1.2 Смена/сброс пароля типового пользователя

Сменить/сбросить пароль для учетной записи типового пользователя можно следующими способами:

- **Смена пароля в Панели управления.**
- **Сброс пароля в окне авторизации.**

Смена пароля в Панели управления

Внимание! Для работы функциональности необходимо предварительно отметить флажок **Разрешить смену пароля через Панель управления** в настройках *Объекта охраны*, которому принадлежит пользователь (подробнее см. [Закладка Управление паролями](#)). Функциональность, описанная ниже, недоступна для пользователей Active Directory/LDAP и суперпользователя системы (root).

Чтобы сменить пароль в *Панели управления*:

1. Вызовите *Панель управления* (см. **Вызов, настройка и скрытие Панели управления**).
2. Выберите команду **Сменить пароль**.
3. В открывшемся окне **Смена пароля** введите текущий пароль, а затем два раза введите новый в соответствующих полях (см. рис. 76). Если в *Объекте охраны* настроены требования к длине и сложности пароля (см. **Закладка Управление паролями**), то новый пароль должен соответствовать этим требованиям. В случае несоответствия нового пароля заданным требованиям в окне отобразится уведомление.

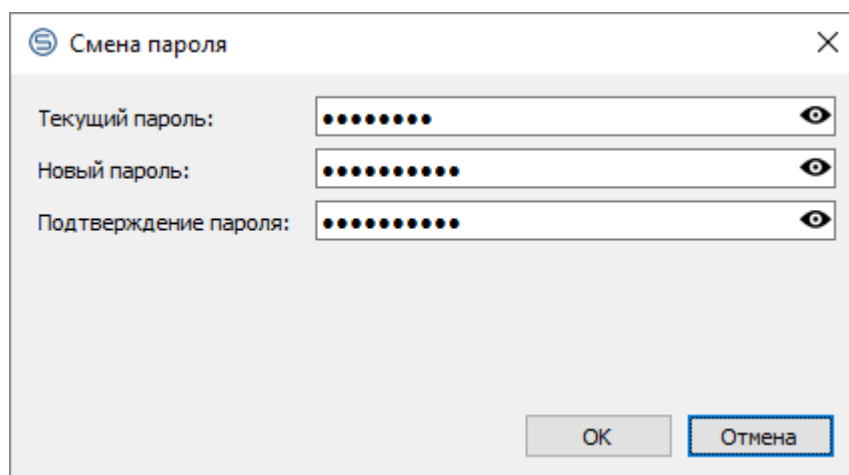


Рис. 76. Окно Смена пароля

4. Нажмите кнопку **ОК**.

Примечание. Смена пароля для типового пользователя также доступна из контекстного меню значка *Клиента SecurOS* в системном трее.

Сброс пароля в окне авторизации

Внимание! Для работы функциональности необходимо предварительно отметить флажок **Разрешить сброс пароля через e-mail при авторизации** в настройках *Объекта охраны*, которому принадлежит пользователь (подробнее см. **Закладка Управление паролями**). Функциональность, описанная ниже, недоступна для пользователей Active Directory/LDAP, суперпользователя системы (root) и пользователей, использующих автоматическую авторизацию.

Чтобы сбросить пароль в окне авторизации:

1. Запустите SecurOS (подробнее см. **Запуск SecurOS на Сервере конфигураций** и **Запуск SecurOS на Рабочем месте оператора**).
2. В окне **Авторизация** нажмите кнопку **Забыли пароль?**.

Внимание! Кнопка **Забыли пароль?** может быть неактивна в следующих случаях:

1. Пользователь превысил количество попыток отправки кода или ввода неверных кодов (не более 5-ти попыток). Время блокировки кнопки: 30 с.
2. Поле **Сервер для подключения** не заполнено, например, при удаленном запуске *Клиента* на *Рабочем месте оператора*. Кнопка становится доступной после ввода IP-адреса или названия сервера в указанное поле.

3. Введите имя пользователя и его e-mail, на который будет отправлено письмо с кодом сброса пароля, в соответствующие поля и нажмите кнопку **Отправить код на почту** (см. рис. 77). Е-

mail должен совпадать с тем, который указан в объекте **Пользователь**, иначе письмо не будет отправлено.

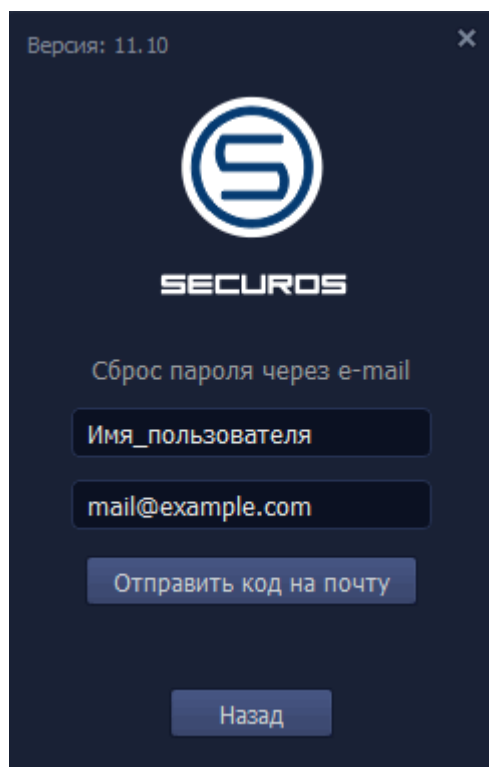


Рис. 77. Окно Авторизация. Блок Сброс пароля через e-mail

4. Введите код, полученный на e-mail, в поле **Введите код сброса пароля** и нажмите кнопку **Подтвердить** (см. рис. 78).

Внимание! Код сброса пароля действителен в течение 2-х минут и может быть использован только один раз.

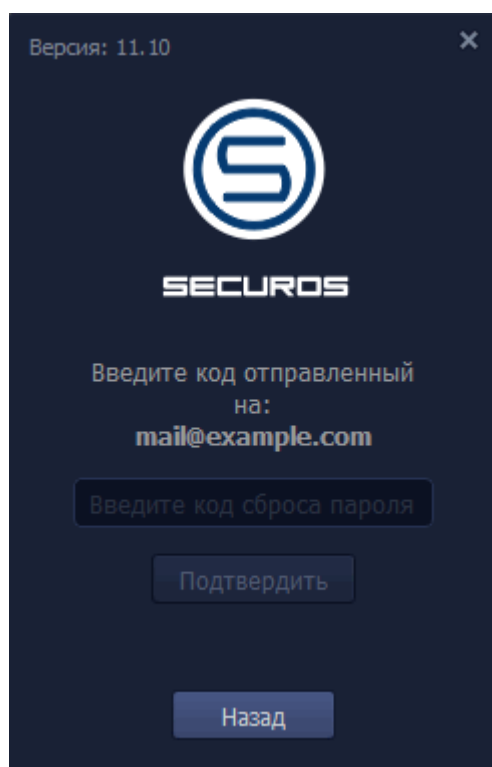


Рис. 78. Окно Авторизация. Блок ввода кода

5. Введите новый пароль и подтвердите его в соответствующем поле (см. рис. 79). Если в *Объекте охраны* настроены требования к длине и сложности пароля (см. [Закладка Управление паролями](#)), то новый пароль должен соответствовать этим требованиям. В случае несоответствия нового пароля заданным требованиям в окне отобразится уведомление.

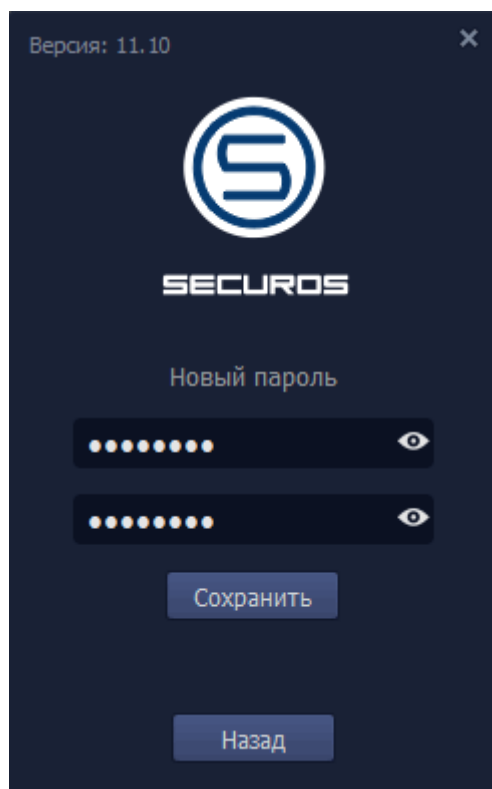


Рис. 79. Окно Авторизация. Блок ввода нового пароля

6. Нажмите кнопку **Сохранить**.

При возникновении проблем с отправкой кода на e-mail система выведет сообщение об ошибке. Пример такого сообщения см. на рис. 80:

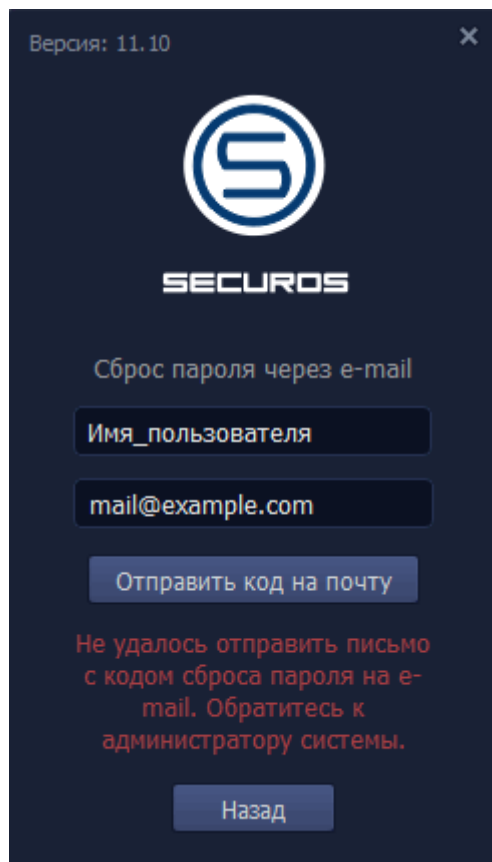


Рис. 80. Пример сообщения об ошибке

Наиболее распространенные причины ошибок:

- Не отмечен флажок **Разрешить сброс пароля через e-mail при авторизации** в настройках соответствующего *Объекта охраны* (см. [Закладка Управление паролями](#)).
- Объект **Сервис почтовых сообщений** в настройках соответствующего *Объекта охраны* не выбран, отключен или некорректно настроен.
- Пользователь не является типовым пользователем системы (пользователь Active Directory/LDAP или суперпользователь системы (root)).
- Пользователь не найден в конфигурации, находится в отключенном состоянии или не указан в **Правах пользователя**.
- Для выбранного **Пользователя** не указан e-mail.
- Введен e-mail, не совпадающий с указанным в настройках выбранного объекта *Пользователь*.
- Нет связи с сервером.

При работе с одноразовыми кодами сброса пароля существуют следующие ограничения:

- Количество запросов кода сброса пароля равно 5. Если все 5 попыток исчерпаны, нажмите кнопку **Назад** для возврата в главное окно авторизации.
- Количество попыток ввода кода сброса пароля равно 5. Если все 5 попыток исчерпаны, нажмите кнопку **Назад** для возврата в главное окно авторизации.

6.3.2 Регистрация и настройка прав пользователей

Внимание! Если в системе нет прочих *Пользователей*, кроме *Суперпользователя* (см. [Пользователи в SecurOS](#)), доступ к системе будет предоставлен без учета имени и пароля пользователя.

Для выполнения операций регистрации и настройки учетных записей новых пользователей в системе создаются следующие объекты:

- объект *Отдел* (**Объект охраны** → *группа Пользователи и Права* → **Отдел**) — содержит список объектов *Пользователь*. Название каждого объекта *Пользователь* используется при авторизации в системе в качестве параметра **Имя пользователя**. **Пароль** пользователя задается в настройках соответствующего объекта *Пользователь*. Новые пользователи могут быть зарегистрированы как в данном объекте *Отдел*, так и в любом другом созданном администратором системы объекте *Отдел*.

Примечание. Объект *Отдел* создается в дереве объектов только в том случае, если на этапе настройки системы с помощью Мастера первого запуска в системе были зарегистрированы пользователи с правами *Опытный пользователь* или *Простой пользователь*.

- группа *Пользователи и Права* (**Объект охраны** → *группа Пользователи и Права*) — содержит объекты *Права пользователя*. Каждый из существующих объектов *Права пользователя* может использоваться повторно (т. е. может быть назначен любому пользователю). В группе содержится два предустановленных набора прав (*Права опытных пользователей* и *Права простых пользователей*), которые различаются по уровню доступа к объектам и операциям с ними.

Процедуры регистрации и настройки прав пользователя описаны в следующих разделах ниже:

- [Регистрация нового пользователя](#);
- [Присвоение прав пользователю/группе пользователей](#);
- [Проверка возможности авторизации указанного пользователя сетевого домена ОС](#).

Регистрация нового пользователя

Примечание. Процедура регистрации в SecurOS пользователя ОС, зарегистрированного в домене Active Directory, описана в разделе [Пример настройки прав пользователей сетевого домена](#).

Чтобы зарегистрировать в SecurOS нового пользователя SecurOS:

Внимание! Если в системе более одного *Объекта охраны*, то необходимо определить пользователя и его права для каждого объекта. Пользователи, зарегистрированные в отдельном *Объекте охраны*, могут авторизоваться только на *Компьютерах*, дочерних данному *Объекту охраны*. С правами суперпользователя (см. [Пользователи в SecurOS](#)) войти в систему можно с любого компьютера, принадлежащего любому *Объекту охраны*.

1. В группе *Пользователи и Права* создайте новый объект *Отдел* или используйте существующий.
2. Создайте объект *Пользователь*, дочерний выбранному *Отделу*.
3. В окне **Параметры создаваемого объекта** в поле **Название** задайте имя пользователя, которое будет использоваться для его авторизации в системе (см. рис. 81).

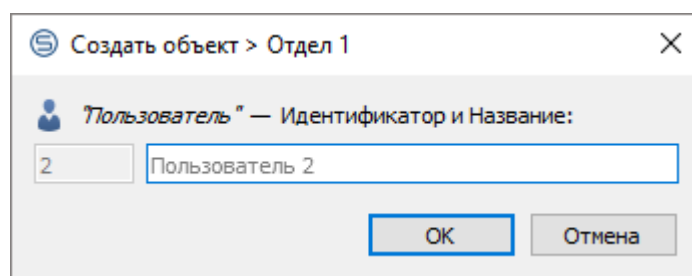


Рис. 81. Окно Параметры создаваемого объекта

4. В окне настройки параметров объекта (см. рис. 82) задайте обязательный параметр **Пароль**, который будет использоваться для авторизации в системе. В случае необходимости задайте прочие параметры (подробнее о прочих параметрах см. [Пользователь](#)).

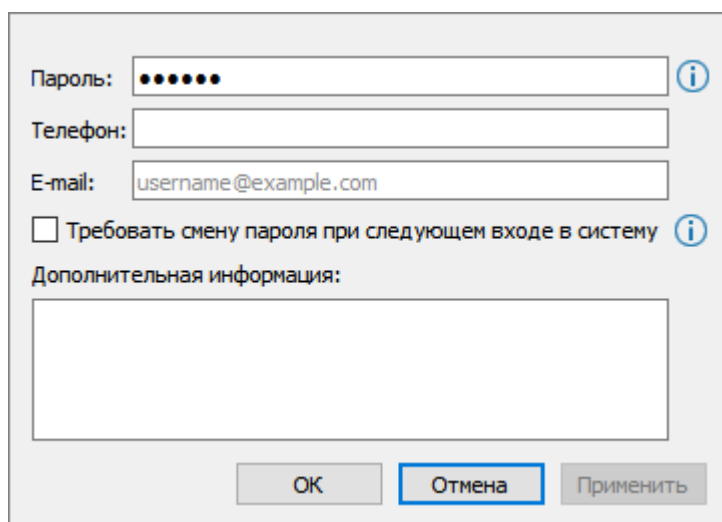


Рис. 82. Окно настройки параметров объекта Пользователь

5. Сохраните изменения.

Присвоение прав пользователю/группе пользователей

Чтобы организовать схему безопасности с ограничением доступа пользователей:

1. Определите, сколько различных уровней доступа необходимо для *Объекта охраны* и какие пользователи будут наделены этими правами.
2. Создайте необходимое количество объектов [Пользователь](#) (см. [Регистрация нового пользователя](#)).
3. В группе *Пользователи и Права* создайте объект [Права пользователя](#) или используйте один из предустановленных наборов прав пользователей ([Права опытных пользователей](#)/[Права простых пользователей](#)).
4. В окне настройки параметров объекта [Права пользователя](#) (см. рис. 83):
 - В дереве объектов (расположено вверху окна настройки) определите для каждого объекта SecurOS уровень доступа (значок слева от объекта в дереве). Заданный уровень доступа будет назначен каждому пользователю из списка блока **Пользователи и группы, обладающие этими правами**.

Примечание. Подробное описание уровней доступа пользователей к объектам и операциям приведено в разделе [Права пользователя](#).

- Отметьте необходимые флажки.
- В поле **Провайдеры** выберите провайдера, в базе данных которого хранятся учетные записи пользователей.
- В списке блока **Пользователи и группы, обладающие этими правами** задайте пользователя или список пользователей, которые должны обладать правами доступа, определенными для этой группы. В зависимости от выбранного **Провайдера**, список пользователей, которым будут присвоены настраиваемые права, формируется по-разному:
 - для пользователей SecurOS – нажмите на кнопку  и сделайте двойной щелчок по появившейся в области списка записи. В выпадающем списке выберите требуемого пользователя.

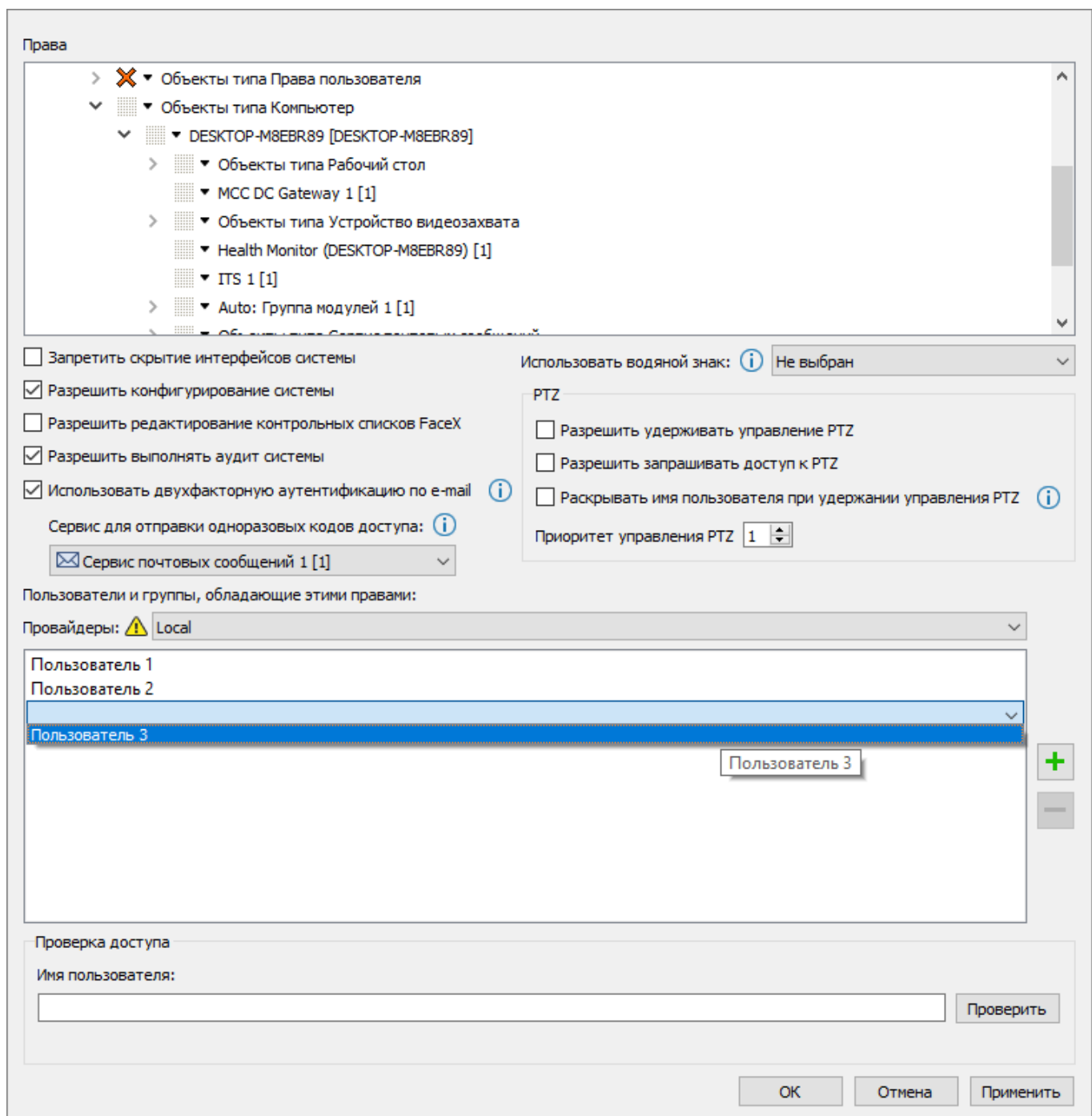


Рис. 83. Окно настройки параметров объекта Права пользователя

- для пользователей Windows, зарегистрированных в сетевом домене Active Directory – правила настройки прав для группы пользователей ОС описаны в разделе **Пример настройки прав пользователей сетевого домена**.
5. Выполните пп. 2 - 4 для каждого Объекта охраны в сети безопасности. *Дерево объектов SecurOS* для каждого Объекта охраны будет содержать элементы, показанные на рис. 84.

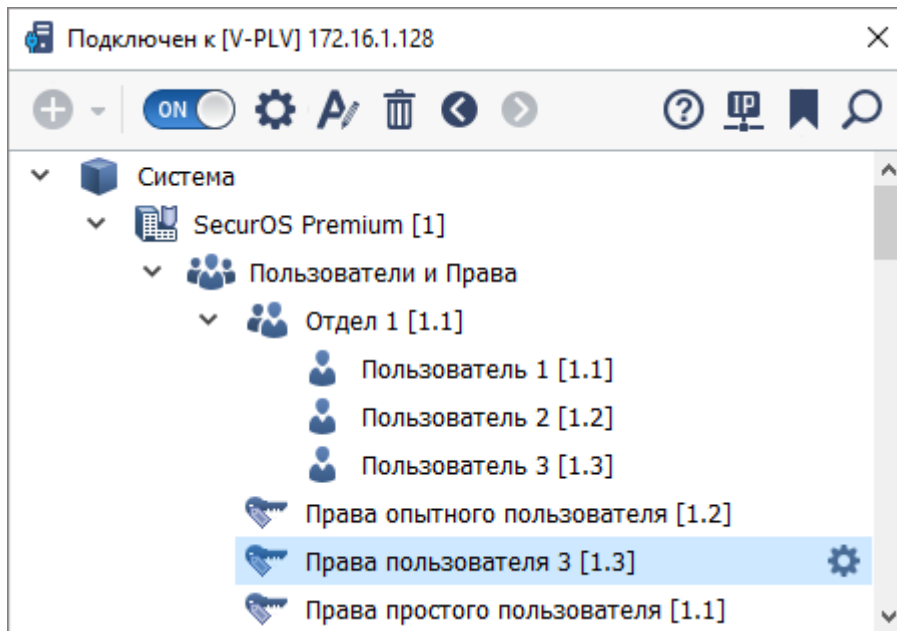


Рис. 84. Дерево объектов (объекты Отдел, Пользователь, Права пользователя)

Проверка возможности авторизации указанного пользователя сетевого домена ОС

В окне настройки параметров объекта *Права пользователя* можно выполнить проверку возможности авторизации указанного пользователя сетевого домена. Для проверки выполните следующие действия:

1. Настройте права пользователя ОС (см. **Пример настройки прав пользователей сетевого домена**).
2. В блоке **Проверка доступа** (см. рис. 85):

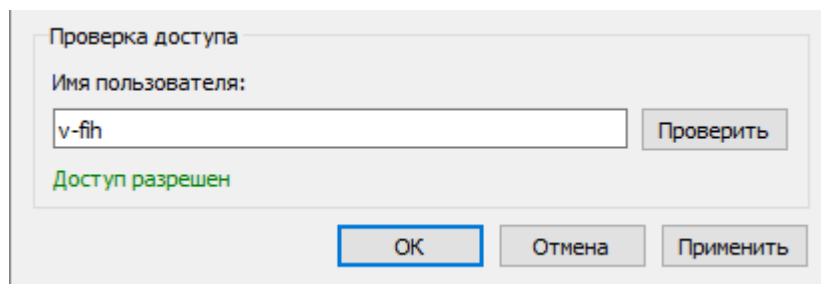


Рис. 85. Блок Проверка доступа

- Задайте **Имя пользователя** ОС, для которого следует проверить возможность авторизации в SecurOS;
- Нажмите кнопку **Проверить**.

В ходе проверки анализируется:

- корректность настроек выбранного провайдера (см. **Active Directory / LDAP**);

- корректность заданного LDAP-фильтра для определения пользователя/группы пользователей (при использовании провайдера LDAP);
- наличие в AD учетной записи указанного пользователя/группы пользователей.

3. Проверка может завершаться со следующими исходами:

- Доступ разрешен — настройки выполнены корректно. Данный пользователь ОС может авторизоваться в SecurOS;

Внимание! Уровень доступа, заданный в настраиваемых *Правах пользователя* для объектов *Компьютер*, при проверке не учитывается.

- Доступ запрещен — настройки выполнены некорректно или указанный пользователь не зарегистрирован в домене ОС;
- Ошибка проверки — превышен таймаут запроса к контроллеру домена.

Аналогичным способом может быть проверена возможность авторизации указанного нативного пользователя SecurOS.

6.3.3 Пример настройки прав пользователей сетевого домена

В данном разделе описывается процедура настройки объектов *Active Directory / LDAP* (см. **Active Directory / LDAP**) и *Права пользователя* для домена провайдера Windows NT или LDAP, на который будет поступать запрос при авторизации пользователя SecurOS. Содержит следующие подразделы:

- **Настройки для провайдера Windows NT;**
- **Настройки для провайдера LDAP.**

Примечание. Авторизация пользователя через Active Directory возможна, если компьютер сети SecurOS состоит в домене Active Directory Windows.

6.3.3.1 Настройки для провайдера Windows NT

Чтобы настроить домен для провайдера Windows NT:

1. Выберите в поле **Провайдер** окна параметров объекта *Active Directory / LDAP* (см. раздел **Active Directory / LDAP**) значение Windows NT (локальный или доменный).
2. Отметьте флажок **Использовать контроллер домена** для использования основного домена, в котором зарегистрирован данный компьютер, или укажите в поле **Сервер** IP-адрес сервера контроллера домена. Значение поля **Порт** (порт для провайдера Windows NT) указывать не требуется.
3. Отметьте флажок **Использовать текущую учетную запись операционной системы** для соединения с контроллером домена с использованием текущего системного имени и пароля пользователя в MS Windows, либо заполните поля **Имя пользователя** и **Пароль** (пользователь должен быть уже определен в контроллере домена, указанного в п. 2).

Чтобы задать права для отдельного пользователя, в окне настройки объекта **Права пользователя** добавьте в список блока **Пользователи и группы, обладающие этими правами** запись с системным именем пользователя Windows (например, i-ivanov).

Чтобы задать права для группы пользователей, в окне настройки объекта *Права пользователя* добавьте в список блока **Пользователи и группы, обладающие этими правами** запись с системным именем группы пользователей Windows с постфиксом `,group` без пробела (например, `Users,group`). Постфикс `,group` является обязательным.

6.3.3.2 Настройки для провайдера LDAP

Чтобы настроить домен для провайдера LDAP:

1. Выберите в поле **Провайдер** окна настройки параметров объекта *Active Directory / LDAP* (см. раздел **Active Directory / LDAP**) значение **LDAP (доменный)**.
2. При необходимости, для шифрования данных при взаимодействии с контроллером домена, отметьте флажок **Использовать шифрование**.
3. Отметьте флажок **Использовать контроллер домена** для использования основного домена, в котором зарегистрирован данный компьютер, или укажите в поле **Сервер** IP-адрес сервера контроллера домена. При нестандартных настройках сервера задайте номер порта в поле **Порт**.
4. Отметьте флажок **Использовать текущую учетную запись операционной системы** для соединения с контроллером домена с использованием текущего системного имени и пароля пользователя в MS Windows, либо заполните поля **Имя пользователя** и **Пароль** (пользователь должен быть уже определен в контроллере домена, указанного в п. 3).

Чтобы задать права отдельного пользователя, в окне настройки объекта *Права пользователя* добавьте в список блока **Пользователи и группы, обладающие этими правами** следующую строку:

```
&(objectClass=user)(sAMAccountName=i-ivanov)
```

где указывается системное имя пользователя (например, `i-ivanov`).

Чтобы задать права для группы пользователей, в окне настройки объекта *Права пользователя* добавьте в список блока **Пользователи и группы, обладающие этими правами** следующую строку:

```
&(objectClass=user)(memberOf=cn=Users,cn=Builtin,dc=test-dev,dc=test)
```

где `Builtin` — системная папка, в которой находится группа `Users`.

6.4 Протоколирование работы SecurOS

При работе SecurOS осуществляется постоянное протоколирование работы системы. Запись информации ведется отдельно каждым из серверов, в собственную, локальную базу данных. По умолчанию на каждом из серверов сохраняется информация обо всех происходящих в системе событиях. Единое для всех серверов системы время хранения информации в базе данных задается в настройках **Объекта охраны**.

Дополнительно, для каждого из серверов могут быть установлены собственные правила записи и хранения информации в локальной базе данных, которые задаются в блоке параметров **Локальная База данных** объекта **Компьютер**:

- **Список событий, разрешенных для записи в локальную базу данных** — в локальной базе данных будут сохранены только те события, которые определены в настройках объекта

Фильтр событий. Применение фильтра событий при записи регулируется параметром **Использовать Фильтр событий**;

- **Размер базы данных** — ограничение размера локальной базы данных. Задается в параметре **Максимальный размер БД**. При достижении заданного значения информация перезаписывается "по кольцу" — удаляются самые старые записи протокола. Если максимальный размер не достигнут, учитывается единое для всех серверов время хранения информации в базе данных;
- **Режим отключения записи в базу данных** — при включении данного режима информация в локальную базу данных протокола событий не записывается. Задается в параметре **Отключить локальный протокол**.

Доступ оператора к протоколу событий системы осуществляется с помощью интерфейсного объекта **Протокол событий**. В окне интерфейсного объекта *Протокол событий* выводится информация из базы данных того сервера, с которым установлено соединение. То есть, для *Видеосервера* это собственная, локальная база данных соответствующего компьютера, а для *Рабочего места оператора* — база данных того *Видеосервера*, с которым связан компьютер оператора. Таким образом, при подключении *Рабочего места оператора* к серверам, на которых настроены различные правила записи информации в базу данных, в окне *Протокола событий* может выводиться различная информация.

Контроль доступа к операциям с базой данных обеспечивается системой разграничения доступов СУБД PostgreSQL, что исключает возможность несанкционированной модификации или удаления записей простым пользователем. Возможность несанкционированной модификации или удаления данных средствами интерфейсного объекта *Протокол событий* отсутствует.

6.5 Обновление лицензионного ключа на всех серверах

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*, *SecurOS Xpress*.

Чтобы обновить лицензионный ключ на всех серверах:

1. Скопируйте новый файл `key.iss` в каталог установки SecurOS на *Сервере конфигураций*.
2. При первом соединении любого из *Периферийных серверов* с *Сервером конфигураций* система автоматически обновит лицензионный ключ на данном сервере.

Дополнительная информация

Устаревший лицензионный ключ сохраняется в системе в корне директории установки SecurOS в файле `key.iss.bak`.

Внимание! После обновления лицензионного ключа возможна автоматическая перезагрузка системы SecurOS на *Периферийном сервере*.

6.5.1 Настройка оповещения об окончании лицензии

Все рабочие станции можно настроить на одновременное оповещение об окончании срока действия файла лицензионного ключа.

Если до конца лицензии остается меньше определенного количества дней, то на всех компьютерах будет показываться окно предупреждения об этом во время работы оператора (см. рис. 86). Окно можно закрыть и продолжить работу.

Предупреждение показывается с определенной периодичностью (например, 3 раза в день, с периодом не менее 3 часов между сообщениями).

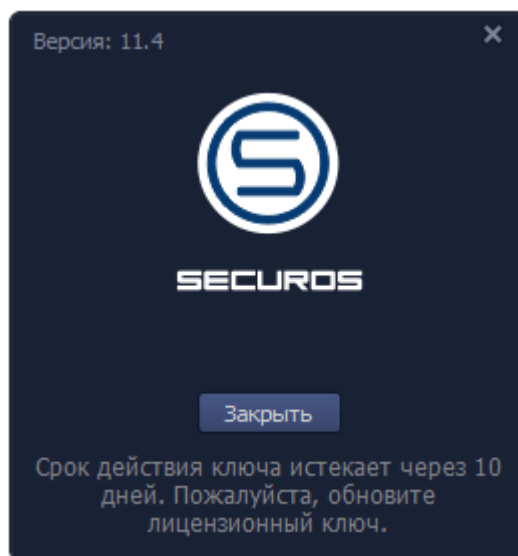


Рис. 86. Окно предупреждения об окончании лицензии

Чтобы настроить параметры оповещения, выполните следующие действия на каждом компьютере, где должно выводиться окно предупреждения:

1. Откройте файл `client_config.xml`, находящийся в директории `%ProgramData%\ISS` (для ОС Windows) или `/var/opt/securos/` (для ОС Linux).
2. В секции `<Main>` файла создайте следующие параметры:
 - `DaysForRemaining` – задайте значение, равное количеству дней до окончания срока действия лицензии, за которое необходимо начать предупреждать пользователей;
 - `RemaindersPerDay` – задайте значение, равное количеству предупреждений в день;

Внимание! Нулевое значение данного параметра приведет к тому, что предупреждения вообще не будут выводиться!

- `MinRemaindPeriod` – задайте значение, равное минимальному промежутку времени (в минутах) между предупреждениями (должно быть всегда больше 30).
3. Сохраните изменения и закройте файл.

Листинг 1. Пример файла `client_config.xml`

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<client>
  <params name="Common">
    <param name="CoreAddress" value="localhost"/>
  </params>
  <params name="Main">
    <param name="AutoLogin" value="false"/>
    <param name="CoreRestartTimeout" value="30000"/>
    <param name="CurDayRemaindCount" value="0"/>
  </params>
</client>
```

```
<param name="DaysForRemaining" value="15"/>
<param name="KeepCoreAlive" value="true"/>
<param name="KeepProcessesAlive" value="true"/>
<param name="LastRemaind" value="2013-03-22 13:58:39"/>
<param name="LastUser" value="root"/>
<param name="MinRemaindPeriod" value="180"/>
<param name="ProcessWaitTimeout" value="30000"/>
<param name="RemaindersPerDay" value="10"/>
</params>
<params name="ServersList">
  <param name="0" value="192.168.3.35"/>
</params>
<params name="UserServersList">
  <param name="0" value="192.168.3.35"/>
  <param name="1" value="192.168.0.51"/>
  <param name="2" value="s-zhulev"/>
</params>
</client>
```

6.6 Модуль самодиагностики Health Monitor

Модуль самодиагностики *Health Monitor* предназначен для мониторинга состояния системы с целью выявления возникающих в ней проблем.

Порядок работы с модулем описан в следующих подразделах:

- **Настройка и запуск.**
- **Режимы работы.**
- **Окно Health Monitor.**
- **Диагностируемые проблемы.**

Настройка и запуск

Родительский объект — **Компьютер**.

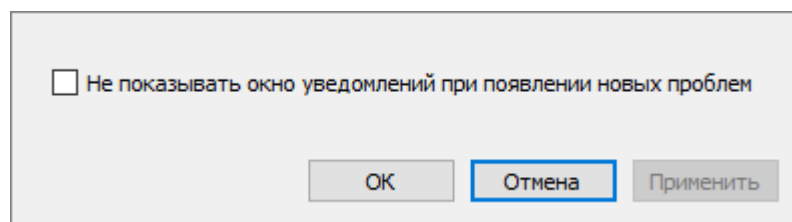


Рис. 87. Окно настройки параметров объекта Health Monitor

Таблица 4. Параметры объекта Health Monitor

Параметр	Описание
Не показывать окно уведомлений при появлении новых проблем	С помощью флажка выбирается режим уведомления оператора о новых проблемах: • флажок не отмечен (значение по умолчанию) — Режим автоинформирования — информирование о новых проблемах выполняется с помощью всплывающего окна. • флажок отмечен — Режим скрытого информирования — информирование о новых проблемах выполняется с помощью значка приложения в системном трее.

Health Monitor может быть размещен на произвольном *Компьютере* сети (*Видеосервере* или *Рабочем месте оператора*) и, независимо от расположения, позволяет контролировать состояние системы в целом.

После запуска приложения его значок всегда отображается в системном трее. Внешний вид значка обозначает текущее состояние системы:

-  — проблемы отсутствуют;
-  — проблемы присутствуют;
-  — обнаружены новые проблемы (используется только для *Режима скрытого информирования*). Отображается общее количество проблем, возникших после завершения предыдущего сеанса работы с окном **Health Monitor**.

Режимы работы

В зависимости от настроек объекта (см. **Настройка и запуск**), оповещение о новых проблемах осуществляется в одном из режимов:

- **Режим автоинформирования (с помощью всплывающего окна)** — при возникновении новой проблемы автоматически отображается окно-информер, содержащее список проблемных объектов и краткое описание проблемы (см. рис. 88). При отсутствии новых проблем окно автоматически скрывается через 10 секунд. Если окно-информер скрыто, его можно вызвать щелчком мыши по значку приложения в системном трее.
- **Режим скрытого информирования (с помощью значка приложения в системном трее)** — при изменении общего количества проблем в системе автоматически обновляется счетчик проблем ( на значке приложения (см. рис. 89). Чтобы просмотреть список текущих проблем, вызовите окно-информер, для чего щелкните значок приложения мышью.

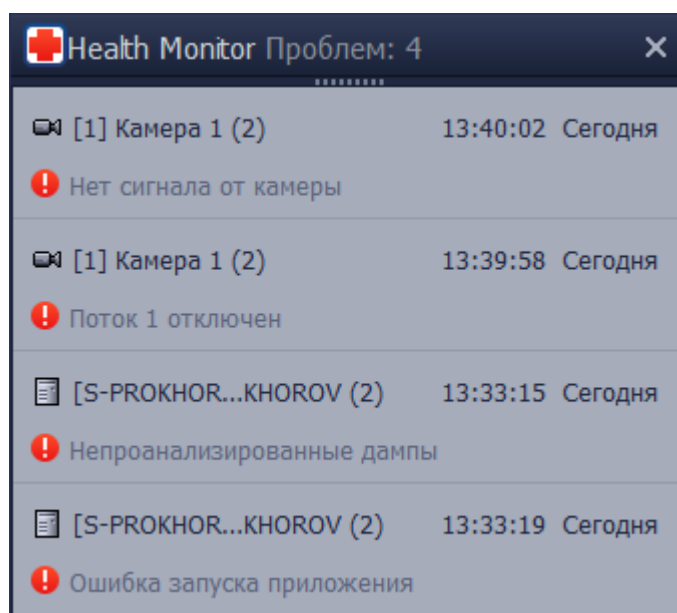


Рис. 88. Окно информера о новых проблемах



Рис. 89. Информирование с помощью иконки приложения

Чтобы просмотреть детальное описание проблемы, вызовите окно **Health Monitor**, для чего щелкните мышью требуемую запись списка в окне-информере. Окно также можно вызвать из контекстного меню значка SecurOS в системном трее (см. рис. 90).

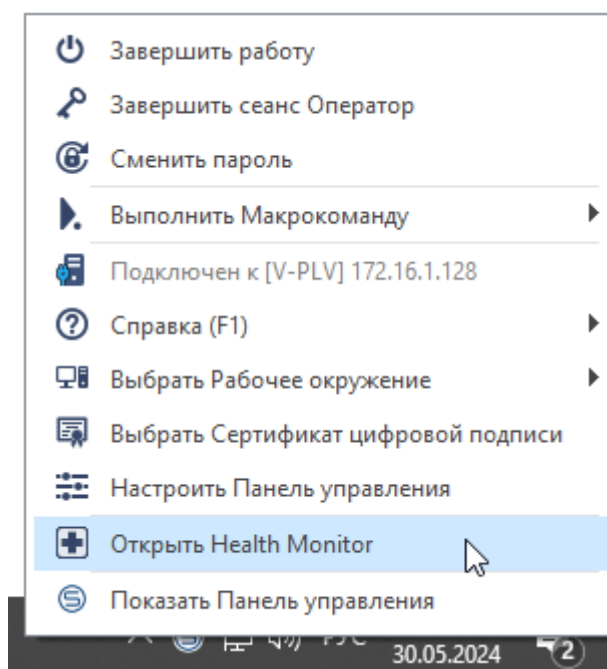


Рис. 90. Вызов окна Health Monitor

Окно Health Monitor

В окне отображается детальная информация о проблемных объектах. Внешний вид окна представлен на рис. 91.

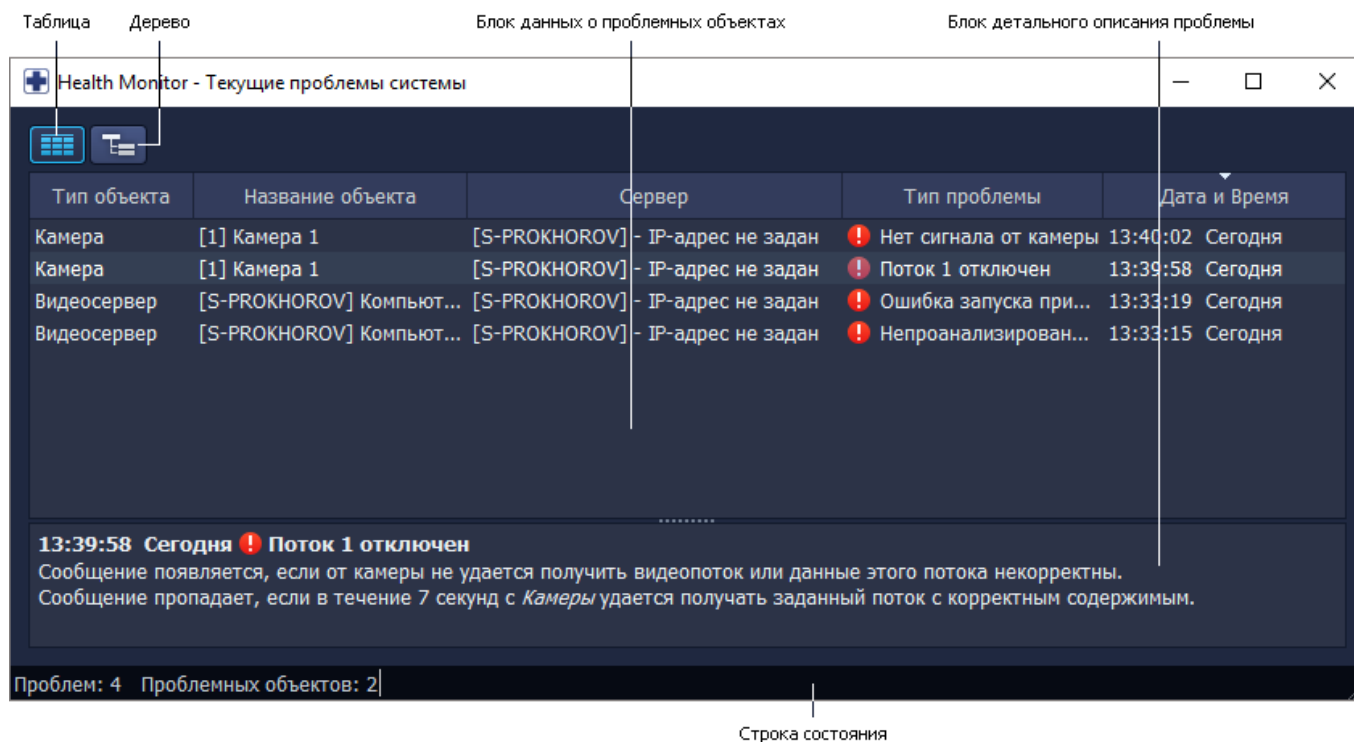


Рис. 91. Окно Health Monitor. Табличное представление

Примечание. При первом запуске окна информация выводится в *Табличном* представлении.

Окно включает следующие компоненты и элементы управления:

- **Блок данных о проблемных объектах** — содержит данные о проблемных объектах системы. Информация в блоке может быть выведена в *Табличном* или *Древовидном* представлении.
- **Блок детального описания проблемы** — содержит детальное описание условий возникновения и сброса проблемы. Информация выводится при выборе проблемы в **Блоке данных о проблемных объектах** либо в списке проблем окна-информера.
- **Строка состояния** — содержит общее количество проблем и проблемных объектов в системе.
- Кнопка  (Таблица) — переход к *Табличному представлению* данных.
- Кнопка  (Дерево) — переход к *Древовидному представлению* данных.

Примечание. Текущая форма представления данных обозначается кнопкой бирюзового цвета.

Табличное представление данных

Внешний вид окна **Health Monitor** при табличном представлении данных показан на рис. 91. Данные в таблице содержатся в следующих столбцах:

- **Тип объекта** — тип проблемного объекта.
- **Название объекта** — идентификатор и название проблемного объекта.
- **Сервер** — идентификатор и IP-адрес *Видеосервера*, на котором возникла проблема. Если IP-адрес не указан в настройках объекта *Компьютер*, выводится строка "IP-адрес не задан".
- **Тип проблемы** — название проблемы, возникшей на указанном объекте.
- **Дата и время** — дата и время возникновения проблемы в формате ОС. Проблемы текущего дня датируются словом "Сегодня".

Ширину столбцов таблицы можно изменять. Для изменения ширины наведите курсор мыши на разделитель столбцов. Курсор примет форму, указанную на рис. 92.

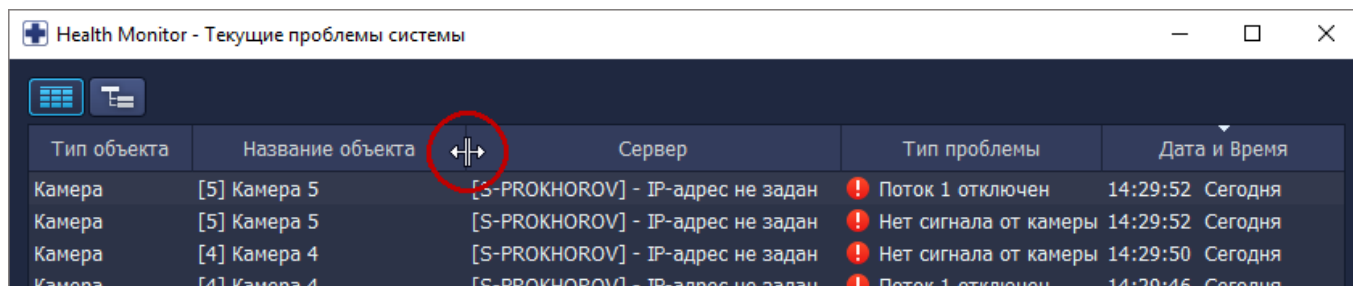


Рис. 92. Изменение ширины столбца таблицы

Нажмите кнопку мыши, и, удерживая кнопку нажатой, переместите курсор в требуемом направлении.

Примечание. Ширину последнего столбца таблицы изменить нельзя.

Данные в таблице можно сортировать по возрастанию/убыванию значения в столбце. Для сортировки записей таблицы по какому-либо полю, щелкните мышью требуемый столбец в заголовке таблицы, затем щелкните символ "стрелка вверх/стрелка вниз" (см. рис. 93). Записи в таблице будут отсортированы по возрастанию/убыванию значения в выбранном столбце.

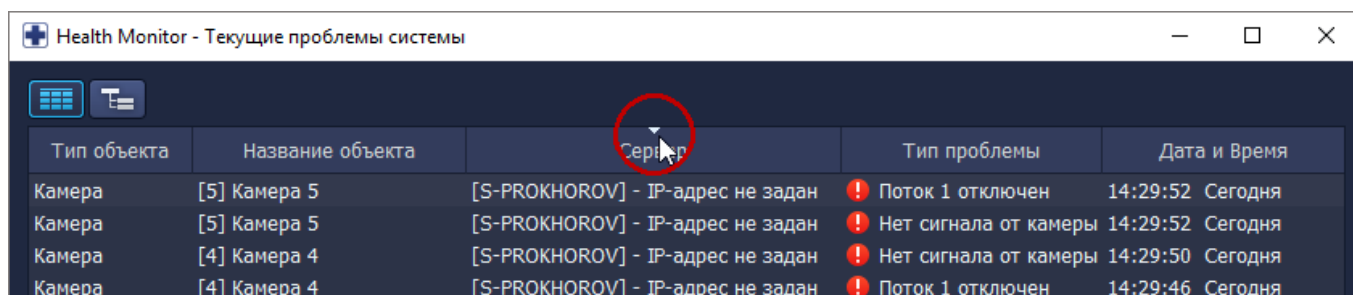


Рис. 93. Сортировка списка

Древовидное представление данных

Внешний вид окна **Health Monitor** при древовидном представлении данных показан на рис. 94.

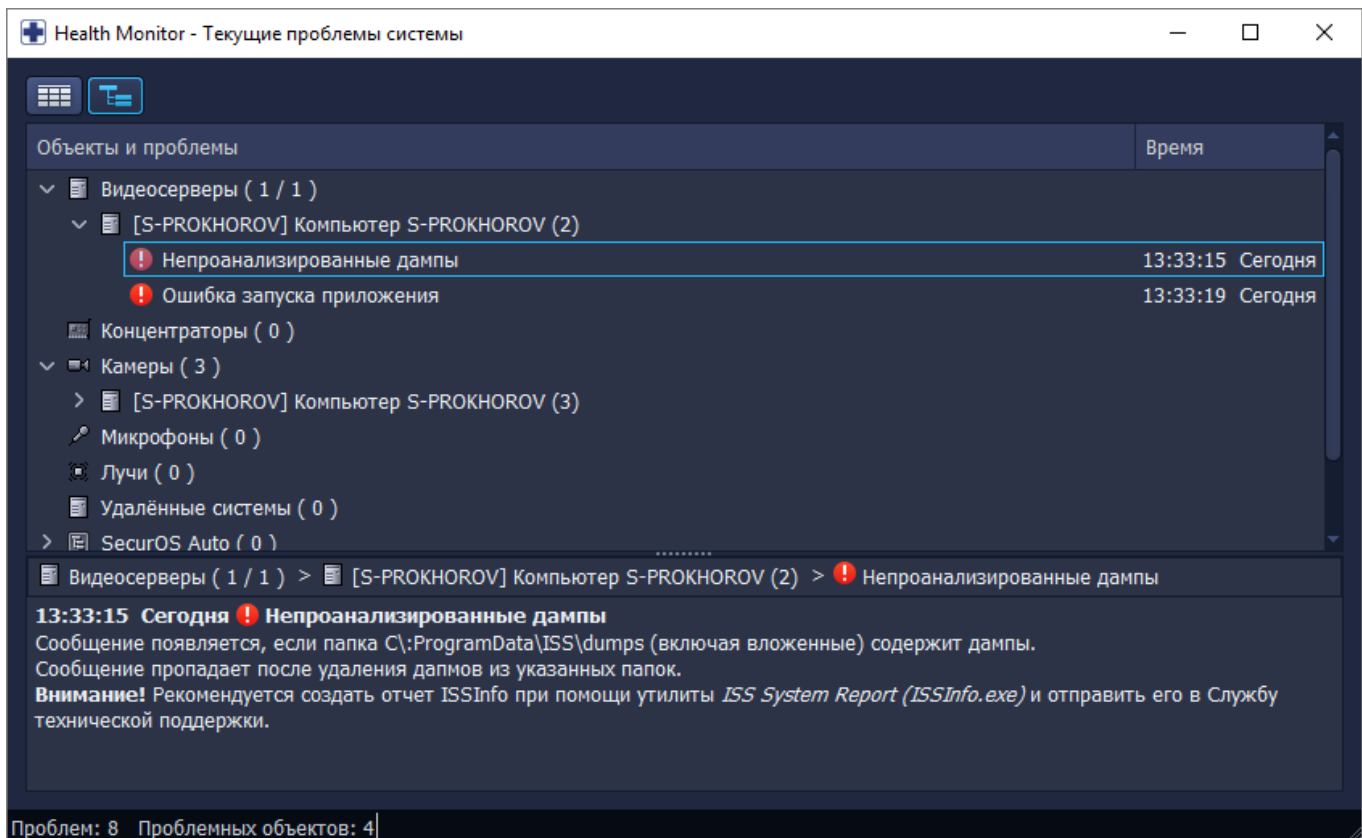


Рис. 94. Окно Health Monitor. Древоподобное представление

Проблемные объекты SecurOS представлены в виде дерева и объединены в восьми основных узлах, представляющих тип объекта или интеллектуальный Модуль SecurOS: *Системы*, *Видеосерверы*, *Концентраторы*, *Камеры*, *Микрофоны*, *Лучи*, *Удаленные системы*, *SecurOS Auto* и *SecurOS Cargo*. Справа от названия узла выводится количество проблемных объектов данного типа. Для узла *Видеосерверы* дополнительно выводится общее количество объектов данного типа в сети SecurOS. Внутри узла проблемные объекты сгруппированы по имени сервера. Справа от имени сервера выводится общее количество проблемных объектов данного типа на этом сервере.

Для быстрой навигации по ветвям **Дерева проблемных объектов** можно использовать адресную строку **Блока детального описания проблемы**. Чтобы перейти на требуемый уровень, щелкните мышью его название (см. рис. 95).

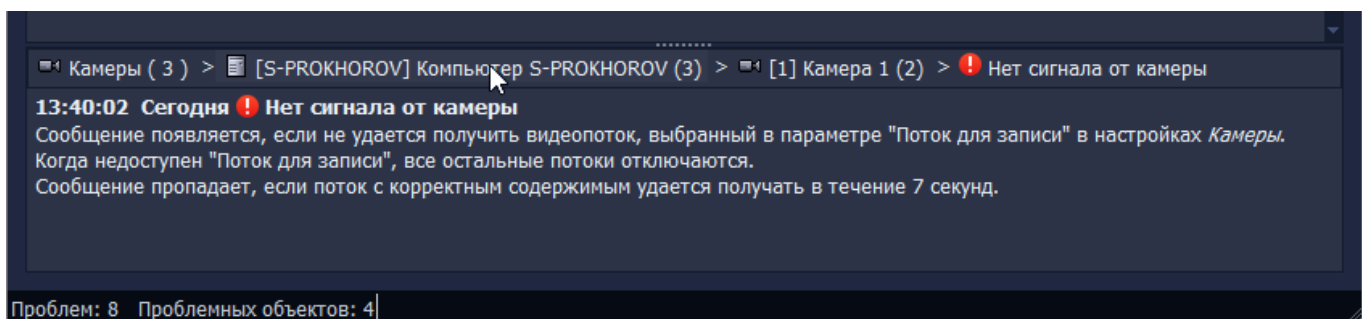


Рис. 95. Навигация по Дереву проблемных объектов из адресной строки

После такого перехода в **Блоке детального описания проблемы** будут отображены все проблемные объекты, находящиеся на выбранном уровне (например, *Камеры*, см. рис. 96). Для перехода к детальному описанию проблем какой-либо из *Камер*, щелкните ее мышью. Таким образом возможно перемещение по любым ветвям дерева в пределах выбранного узла **Дерева проблемных объектов**.



Рис. 96. Результат перехода по уровням

Диагностируемые проблемы

Модуль выявляет проблемы различной степени важности. Список диагностируемых проблем с их подробным описанием приведен в следующих разделах (соответствующих узлам **Дерева проблемных объектов**):

- Система.
- Видеосервер.
- Камера.
- Микрофон.
- Луч.
- Удаленная система.
- SecurOS Auto (см. **Руководство пользователя SecurOS Auto**).
- SecurOS Cargo (см. **Руководство пользователя SecurOS Cargo**).
- SecurOS EDBE (см. **Руководство пользователя SecurOS EDBE**).

6.6.1 Система

Для объекта *Система* диагностируется следующая проблема:

Ненастроенные объекты

- Сообщение появляется, если некоторые объекты в конфигурации системы требуют изменения настроек для корректной работы. Перейдите к дереву объектов, чтобы увидеть объекты, с которыми возникли проблемы.
- Сообщение пропадает, если все настройки обновлены.

Найти ненастроенные объекты можно с помощью *Дерева объектов SecurOS* (см. **Объекты, требующие настройки**).

6.6.2 Видеосервер

Для объекта *Видеосервер* диагностируются следующие проблемы:

- **Auto: Контроллер EdgeStorage: внешняя БД недоступна;**
- **Auto: Контроллер EdgeStorage: отсутствуют Обработчики EdgeStorage, использующие базовый алгоритм захвата номеров;**
- **Auto: Контроллер EdgeStorage: отсутствуют Обработчики EdgeStorage, использующие нейросетевой алгоритм захвата номеров;**

- Auto: Контроллер EdgeStorage: очередь задач на выгрузку изображений переполнена;
- Database Partitioner: БД недоступна;
- Database Partitioner: некорректная схема БД;
- Database Partitioner: некорректные настройки;
- Database Partitioner: не удалось получить доступ к базе данных;
- Database Partitioner: ошибки в процессе секционирования;
- Image Processor: очередь задач переполнена;
- REST API: превышен максимальный размер очереди на сохранение кадров;
- REST API: очередь событий для подписчиков переполнена;
- Архив удален из-за отсутствия свободного места;
- Архиватор: нет доступа к диску;
- Архиватор: обнаружен поврежденный файл;
- Архиватор: ошибка записи архива;
- БД Аудита недоступна;
- БД видеоподсистемы недоступна;
- БД конфигурации недоступна;
- БД СКУД/ОПС недоступна;
- БД событий недоступна;
- БОЛИД: время не синхронизировано;
- Версия продукта на сервере не совпадает с версией на Сервере конфигураций;
- В системе обнаружено более одного Сервера конфигураций;
- Детектор нарушений ПДД: ошибка работы детектора;
- Конфигурация сервера неактуальна: очередь обновлений в данный момент переполнена;
- Критическая загрузка CPU;
- Лицензия истекает в течение 24 часов;
- Медленная обработка команд;
- Настройки Детектора пропуска пешехода и Распознавателя номеров не согласованы;
- Не удалось загрузить синхронизируемые файлы;
- Не удалось записать метаданные в БД видеоподсистемы;
- Не удалось запустить Перемещаемый PostgreSQL;
- Не удалось подключить iSCSI-диск;
- Не удалось получить доступ к Удаленной системе;
- Недостаточная скорость записи;
- Недостаточная скорость записи в реплицированную БД;
- Недостаточно места на системном диске;
- Недостаточно памяти;
- Непроанализированные дампы;
- Нет доступа к диску;
- Нет соединения с СКУД/ОПС;

- Обнаружен поврежденный файл долговременного архива;
- Отключен;
- Очередь событий переполнена;
- Ошибка записи архива;
- Ошибка записи аудиоархива;
- Ошибка записи Тревог в БД;
- Ошибка запуска приложения;
- Ошибка обновления конфигурации: Модули, установленные на серверах, не совпадают;
- Перекресток: GNSS-приемник не синхронизирован;
- Перекресток: Некорректные настройки объекта Auto: Распознаватель номеров;
- Потеря запросов к БД - недостаточная скорость БД;
- Превышены лицензионные ограничения на объекты из Удаленных систем;
- Репликатор баз данных: несоответствие копируемых данных;
- Репликатор баз данных: ошибка записи в БД;
- Реплицированная БД недоступна;
- Сбой работы Auto: Распознавателя номеров с типом "Обработчик EdgeStorage";
- Сервер диагностики: очередь запросов к БД на сохранение статистики переполнена;
- Сервер диагностики: текущая версия PostgreSQL не поддерживается;
- Сервер конфигураций недоступен;
- СКУД/ОПС: время не синхронизировано;
- Стерео: Детектор людей. Ошибка работы модуля;
- Шлюз MCC DC: недоступен Видеосервер для шлюзования живого видео.

Auto: Контроллер EdgeStorage: внешняя БД недоступна

- Сообщение появляется, если потеряно соединение между *Auto: Контроллером EdgeStorage* и БД, указанной в его настройках.
- Сообщение пропадает сразу после восстановления соединения с БД.

Auto: Контроллер EdgeStorage: отсутствуют Обработчики EdgeStorage, использующие базовый алгоритм захвата номеров

- Сообщение появляется, если в текущей конфигурации нет ни одного *Обработчика EdgeStorage*, использующего базовый алгоритм захвата номеров, но есть как минимум один *Распознаватель номеров*, использующий базовый алгоритм захвата номеров.
- Сообщение пропадает, если у всех *Распознавателей номеров* был включен нейросетевой алгоритм захвата номеров или если был настроен хотя бы один *Обработчик EdgeStorage*, использующий базовый алгоритм захвата номеров.

Auto: Контроллер EdgeStorage: отсутствуют Обработчики EdgeStorage, использующие нейросетевой алгоритм захвата номеров

- Сообщение появляется, если в текущей конфигурации нет ни одного *Обработчика EdgeStorage*, использующего нейросетевой алгоритм захвата номеров, но есть как минимум один *Распознаватель номеров*, использующий нейросетевой алгоритм захвата номеров.

- Сообщение пропадает, если у всех *Распознавателей номеров* был отключен нейросетевой алгоритм захвата номеров или если был настроен хотя бы один *Обработчик EdgeStorage*, использующий нейросетевой алгоритм захвата номеров.

Auto: Контроллер EdgeStorage: очередь задач на выгрузку изображений переполнена

- Сообщение появляется, если в очереди задач объекта *Auto: Контроллер EdgeStorage* более 10000 задач. Очередь может расти в случае отсутствия связи с *Видеосервером*, *Edge Storage камер* или если сохраняемые кадры еще не записаны в видеоархив.
- Сообщение пропадает, если ошибка не повторяется в течение 3 минут.

Database Partitioner: БД недоступна

- Сообщение появляется, если потеряно соединение с базой данных модуля.
- Сообщение пропадает сразу после восстановления соединения с БД.

Database Partitioner: некорректная схема БД

- Сообщение появляется, если схема базы данных не соответствует требованиям системы.
- Сообщение пропадает, когда несоответствия требованиям устранены или при потере связи с базой данных.

Database Partitioner: некорректные настройки

- Сообщение появляется, если текущие настройки модуля некорректны. Например, не заданы обязательные параметры в настройках модуля или связанной с ним *Базе данных*.
- Сообщение пропадает, если модуль получил корректные настройки.

Database Partitioner: не удалось получить доступ к базе данных

- Сообщение появляется, когда база данных уже занята другим объектом *Database Partitioner*.
- Сообщение пропадает после успешного получения доступа к базе данных.

Database Partitioner: ошибки в процессе секционирования

- Сообщение появляется, если в процессе секционирования возникли ошибки.
- Сообщение пропадает, если проблема не возникает в течение 10 минут.

Image Processor: очередь задач переполнена

- Сообщение появляется, если в очереди задач какого-либо из объектов *Image Processor* более 10000 задач. Очередь может расти в случае отсутствия связи с *Видеосервером* или если сохраняемые кадры еще не записаны в видеоархив.
- Сообщение пропадает, если ошибка не повторяется в течение 3 минут.

REST API: превышен максимальный размер очереди на сохранение кадров

- Сообщение появляется, если превышен максимальный размер очереди *REST API* на сохранение кадров. Новые запросы на сохранение изображений будут отклонены.
- Сообщение пропадает, если ошибка не повторяется в течение 3 минут.

REST API: очередь событий для подписчиков переполнена

- Сообщение появляется, если превышен максимальный размер очереди событий объекта *REST API* (больше 10000 событий суммарно по всем подписчикам). Новые события не добавляются в очередь и будут потеряны.
- Сообщение пропадает, если ошибка не повторяется в течение 3 минут.

Архив удален из-за отсутствия свободного места

- Сообщение появляется в случае, если был удален архив, для которого не истекло минимальное время хранения (указывается в параметре **Хранить не менее** в настройках объекта *Камера*, см. **Закладка Запись**). Данная ситуация может произойти, если места на дисках для записи (указывается в блоке **Архив** в настройках объекта **Компьютер**) недостаточно для хранения заданного количества дней архива.
- Сообщение пропадает, если ошибка не повторяется в течение 1 часа.

Архиватор: нет доступа к диску

- Сообщение появляется, если запись или чтение долговременного архива с одного из дисков или сетевых директорий, указанных в настройках объекта *Архиватор*, невозможна по одной из следующих причин:
 - нет соединения с диском;
 - ошибка оборудования/драйвера.
- Сообщение пропадает после восстановления связи с диском.

Архиватор: обнаружен поврежденный файл

- Сообщение появляется, если файл *Оперативного архива* поврежден и не был скопирован в *Долговременный архив*.
- Сообщение пропадает, если проблема не возникает в течение 10 минут.

Архиватор: ошибка записи архива

- Сообщение появляется, если запись файла долговременного архива невозможна по какой-либо причине. Например, недостаточно места на диске.
- Сообщение пропадает, если ошибка не повторяется в течение 3 минут.

БД Аудита недоступна

- Сообщение появляется, если потеряно соединение с БД Аудита.
- Сообщение пропадает сразу после восстановления соединения с БД.

БД видеоподсистемы недоступна

- Сообщение появляется, если потеряно соединение с БД видеоподсистемы. Информация о тревогах, закладках, метаданных, а также дополнение архивов с помощью технологии EdgeStorage Sync временно недоступны.
- Сообщение пропадает сразу после восстановления соединения с БД.

БД конфигурации недоступна

- Сообщение появляется, если потеряно соединение с БД конфигурации.
- Сообщение пропадает сразу после восстановления соединения с БД.

БД СКУД/ОПС недоступна

- Сообщение появляется, если потеряно соединение с БД СКУД/ОПС.
- Сообщение пропадает сразу после восстановления соединения с БД.

БД событий недоступна

- Сообщение появляется, если потеряно соединение с БД событий.
- Сообщение пропадает сразу после восстановления соединения с БД.

БОЛИД: время не синхронизировано

- Сообщение появляется, если время сервера БОЛИД отличается от времени в системе более, чем на 10 секунд.
- Сообщение пропадает после устранения проблемы.

Версия продукта на сервере не совпадает с версией на Сервере конфигураций

- Сообщение появляется, если версия продукта, установленного на *Периферийном сервере*, не совпадает с версией продукта, установленного на *Сервере конфигураций*.
- Сообщение пропадает сразу после того, как на *Периферийном сервере* будет установлена требуемая версия продукта.

В системе обнаружено более одного Сервера конфигураций

- Сообщение появляется в случае, если в сети присутствует сразу несколько компьютеров с ролью *Сервер конфигураций*.
- Сообщение пропадает сразу после того, как в сети останется только один компьютер с ролью *Сервер конфигураций*.

Детектор нарушений ПДД: ошибка работы детектора

- Сообщение появляется в случае, если произошла критическая ошибка при работе детектора. Возможные причины:
 - настройки детектора не указаны или указаны некорректно;
 - нейросетевой сервер не установлен;
 - произошла ошибка при запуске нейросетевого сервера.
- Сообщение пропадает при успешном запуске детектора.

Конфигурация сервера неактуальна: очередь обновлений в данный момент переполнена

- Сообщение появляется, если очередь обновлений конфигурации сервера содержит более 500 обновлений.
- Сообщение пропадает после того, как количество обновлений в очереди снижается до 100.

Критическая загрузка CPU

- Сообщение появляется, если загрузка одного из ядер центрального процессора превышает 90%.
- Сообщение пропадает после того, как загрузка ядра, определенная серией измерений, упала ниже 90%.

Лицензия истекает в течение 24 часов

- Сообщение появляется, если срок действия лицензии на Продукт заканчивается менее чем через 24 часа.
- Сообщение пропадает после обновления файла лицензионного ключа.

Медленная обработка команд

- Сообщение появляется, если время ожидания обработки команд превышает установленное значение (по умолчанию 1 секунда). Задержка может возникнуть в результате резкого увеличения очереди команд или долгой обработки отдельных команд.
- Сообщение пропадает, если команды обрабатываются без задержек в течение 10 секунд.

Настройки Детектора пропуска пешехода и Распознавателя номеров не согласованы

- Сообщение появляется, если расхождения в количестве и/или значениях параметров настройки *Детектора пропуска пешеходов* и *Распознавателя номеров* не позволяют корректно обработать событие распознавания номера. Например, в детекторе размечено 3 полосы движения по проезжей части, а в настройках *Распознавателя номеров* — только 2.
- Сообщение пропадает, если проблема не повторяется в течение 30 минут.

Не удалось загрузить синхронизируемые файлы

- Сообщение появляется, если не удалось загрузить синхронизируемые файлы. Возможные причины:
 - файл поврежден;
 - нет доступа к файлу.
- Сообщение пропадает, если при перезагрузке сервера синхронизируемые файлы были успешно загружены.

Не удалось записать метаданные в БД видеоподсистемы

- Сообщение появляется, если не удалось произвести запись метаданных для Ретроспективного поиска в БД видеоподсистемы.
- Сообщение пропадает, если ошибка не повторяется в течение 3 минут.

Не удалось запустить Перемещаемый PostgreSQL

- Сообщение появляется, если дополнительный экземпляр PostgreSQL не может быть запущен по какой-либо причине. Например, из-за повреждения внутренних данных.
- Сообщение пропадает, если дополнительный экземпляр PostgreSQL успешно запущен.

Не удалось подключить iSCSI-диск

- Сообщение появляется, если возникли ошибки на этапе соединения, авторизации или монтирования iSCSI-диска.
- Сообщение пропадает, когда iSCSI-диск успешно смонтирован.

Не удалось получить доступ к Удаленной системе

- Сообщение появляется, если не удалось получить доступ к *Удаленной системе*. Возможные причины:
 - некорректный пароль доступа к системе;
 - доступ не настроен.
- Сообщение пропадает сразу после получения доступа к *Удаленной системе*.

Недостаточная скорость записи

- Сообщение появляется, если суммарная скорость (битрейт) записываемых потоков превышает фактическую производительность диска в режиме записи.
- Сообщение пропадает, если проблема не повторяется в течение 1 часа.

Недостаточная скорость записи в реплицированную БД

- Сообщение появляется, если время добавления в реплицированную БД очередного пакета данных, полученных из любой исходной БД, превысило 3 минуты. Добавление следующего пакета данных от этой БД будет возможно только после завершения загрузки предыдущего.
- Сообщение пропадает, если ошибка не повторяется в течение 30 минут.

Недостаточно места на системном диске

- Сообщение появляется, если на системном диске осталось меньше 10 ГБ свободного места.
- Сообщение пропадает, если свободного места на системном диске становится больше 10 ГБ.

Недостаточно памяти

- Сообщение появляется, если в течение 1 минуты используется более 80% виртуальной памяти сервера. Размер виртуальной памяти вычисляется как сумма объема оперативной памяти и максимального размера файла подкачки.
- Сообщение пропадает, если ошибка не повторяется в течение 1 минуты.

Непроанализированные дампы

- Сообщение появляется, если в системе хранятся непроанализированные дампы. В зависимости от операционной системы, дампы сохраняются в следующих директориях:
 - %ProgramData%\ISS\dumps (включая поддиректории) — в ОС Windows;
 - var/opt/securos/dumps (включая поддиректории) — в ОС Linux.
- Сообщение пропадает после удаления дампов из указанных директорий.

Внимание! Рекомендуется создать отчет при помощи утилиты **SystemInfo** (SystemInfo.exe) и отправить его в Службу технической поддержки.

Нет доступа к диску

- Сообщение появляется, если чтение или запись видео или аудио на один из дисков, заданных на закладке **Архив** объекта *Компьютер*, невозможна по одной из следующих причин:
 - нет соединения с диском;
 - ошибка оборудования/драйвера.
- Сообщение пропадает при восстановлении связи с диском.

Нет соединения с СКУД/ОПС

- Сообщение появляется, если к сторонней системе СКУД/ОПС не удалось подключиться по одной из причин:
 - с сервером СКУД/ОПС не установлено соединение;
 - некорректно указаны параметры подключения;
 - SDK для взаимодействия со сторонней системой не установлен или установлен некорректно.

Также сообщение отображается, если соединение с сервером СКУД/ОПС потеряно в процессе работы.

- Сообщение пропадает через 7 секунд после подключения или восстановления соединения с сервером.

Обнаружен поврежденный файл долговременного архива

- Сообщение появляется, если не удалось найти или прочитать файл долговременного архива при воспроизведении с помощью *Медиа Клиента* и при экспорте с помощью *Конвертера архива*.
- Сообщение пропадает, если ошибка не повторяется в течение 1 часа.

Отключен

- Сообщение появляется, если потеряно соединение с сервером.
- Сообщение пропадает через 7 секунд после восстановления соединения с сервером.

Внимание! Данное сообщение также выводится в случае, если в параметре **IP адрес** в настройках *Видеосервера* задан неправильный IP-адрес.

Очередь событий переполнена

- Сообщение появляется, если превышен максимальный размер очереди событий *Видеосервера* (больше 10000 событий). Новые события не добавляются в очередь и будут потеряны. Очередь может расти в случае отсутствия связи с *Видеосервером* или если сохраняемые события еще не записаны в БД.
- Сообщение пропадает, если ошибка не повторяется в течение 3 минут.

Ошибка записи архива

- Сообщение появляется, если запись видеоархива невозможна по какой-либо причине. Например, недостаточно места на диске, недостаточная скорость записи, нет доступа к диску и т.п.
- Сообщение пропадает, если ошибка не повторяется в течение 3 минут.

Ошибка записи аудиоархива

- Сообщение появляется, если запись аудиоархива невозможна по какой-либо причине. Например, недостаточно места на диске, недостаточная скорость записи, нет доступа к диску и т.п.
- Сообщение пропадает, если ошибка не повторяется в течение 3 минут.

Ошибка записи Тревог в БД

- Сообщение появляется, если запись тревог в БД видеоподсистемы невозможна.
- Сообщение пропадает, если в течение 3 минут после возобновления записи ошибка не повторяется.

Ошибка запуска приложения

- Сообщение появляется, если при запуске внешнего приложения произошла ошибка.
- Сообщение пропадает, если приложение успешно запущено.

Ошибка обновления конфигурации: Модули, установленные на серверах, не совпадают

- Сообщение появляется, если обнаружено несоответствие набора установленных Модулей на *Периферийном сервере* и *Сервере конфигураций*. Текущая конфигурация сервера неактуальна и будет обновлена только после установки всех недостающих Модулей на *Периферийном сервере*.
- Сообщение пропадает после обновления конфигурации.

Потеря запросов к БД - недостаточная скорость БД

- Сообщение появляется, если очередь на запись в БД достигла максимума. Новые тревоги, закладки, а также задачи для EdgeStorage не записываются в БД.
- Сообщение пропадает, если в течение 1 часа после возобновления записи ошибка не повторяется.

Перекресток: GNSS-приемник не синхронизирован

- Сообщение появляется, если при обработке нарушения время в системе не было синхронизировано через GNSS-приемник. Возможные проблемы:
 - устройство неисправно или недоступно;
 - не удастся изменить системное время.
- Сообщение пропадает через 120 минут или если при обработке нарушения время будет синхронизировано.

Перекресток: Некорректные настройки объекта Auto: Распознаватель номеров

- Сообщение появляется, если режим записи хотя бы одного из *Распознавателей номеров* отличается от "Запись видео".
- Сообщение пропадает, если режим записи всех используемых *Распознавателей номеров* принимает значение "Запись видео".

Превышены лицензионные ограничения на объекты из Удаленных систем

- Сообщение появляется, если суммарное количество *Камер* или *Распознавателей номеров*, имеющихся в *Удаленных системах*, превышает значение, разрешенное лицензией SecurOS MCC. Взаимодействие со всеми *Удаленными системами* приостановлено.
- Сообщение пропадает когда количество лицензируемых объектов в *Удаленных системах* становится меньше значения, разрешенного лицензией SecurOS MCC.

Репликатор баз данных: несоответствие копируемых данных

- Сообщение появляется, если в реплицируемой БД присутствуют поля, которых нет в реплицированной БД. Будут скопированы только те поля, которые присутствуют в обеих БД.
- Сообщение пропадает при изменении настроек объекта *Репликатор баз данных*.

Репликатор баз данных: ошибка записи в БД

- Сообщение появляется, если репликация невозможна или данные не могут быть скопированы в полном объеме по одной из следующих причин:
 - реплицированная или хотя бы одна реплицируемая база данных имеют некорректную разметку;
 - запись не может быть скопирована вследствие ее повреждения в исходной базе данных.
- Сообщение пропадает, если ошибка не повторяется в течение 10 минут.

Реплицированная БД недоступна

- Сообщение появляется, если потеряно соединение с реплицированной базой данных.
- Сообщение пропадает сразу после восстановления соединения с БД.

Сбой работы Auto: Распознавателя номеров с типом "Обработчик EdgeStorage"

- Сообщение появляется, если произошел сбой при запуске или работе одного из *Распознавателей номеров* с типом "Обработчик EdgeStorage". Полученные через *EdgeStorage* видео не будут обрабатываться проблемным *Распознавателем*.
- Сообщение пропадает, если проблемный *Распознаватель* был отключен или проработал без сбоев не менее 3 минут.

Внимание! Данное сообщение может дублироваться, если некорректно работающих обработчиков несколько.

Сервер диагностики: очередь запросов к БД на сохранение статистики переполнена

- Сообщение появляется, если превышен максимальный размер очереди запросов к БД *Сервера диагностики*. Новые запросы на сохранение статистики не добавляются в очередь и будут потеряны. Возможные причины роста очереди запросов:
 - отсутствие связи с БД;
 - недостаточная скорость записи в БД;
 - запись запросов в БД невозможна.
- Сообщение пропадает, если ошибка не повторяется в течение 3 минут.

Сервер диагностики: текущая версия PostgreSQL не поддерживается

- Сообщение появляется, если база данных *Сервера диагностики* находится под управлением несовместимой версии PostgreSQL.
- Сообщение пропадает, если *Сервер диагностики* использует базу данных под управлением PostgreSQL 12.

Сервер конфигураций недоступен

- Сообщение появляется при потере связи с *Сервером конфигураций*.
- Сообщение пропадает через 7 секунд после возобновления связи с *Сервером конфигураций*.

СКУД/ОПС: время не синхронизировано

- Сообщение появляется в следующих случаях:
 - время возникновения события в СКУД/ОПС опережает системное время на *Видеосервере* более чем на 2 секунды;
 - время возникновения текущего события в СКУД/ОПС меньше времени возникновения предыдущего события.
- Сообщение пропадает, если в течение 3 минут указанные ошибки не повторяются.

Сtereo: Детектор людей. Ошибка работы модуля

- Сообщение появляется, если произошла критическая ошибка при работе модуля. Возможные причины:
 - настройки модуля не указаны или указаны некорректно;
 - нейросетевой сервер не установлен;
 - произошла ошибка при запуске нейросетевого сервера.
- Сообщение пропадает при успешном запуске модуля.

Шлюз MCC DC: недоступен Видеосервер для шлюзования живого видео

- Сообщение появляется, если какой-либо из *Видеосерверов*, выбранных для шлюзования живого видео, не ответил на запрос *Шлюза MCC DC*. Возможные причины:
 - *Видеосервер* недоступен;
 - на *Видеосервере* установлена устаревшая версия продукта.
- Сообщение пропадает, если проблема не повторяется в течение 1 минуты.

6.6.3 Камера

Для объекта *Камера* диагностируются следующие проблемы:

- **Изображение слишком темное;**
- **Изображение слишком яркое;**
- **Камера не сфокусирована;**
- **Микрофон отключен;**
- **Нарушена целостность архива;**
- **Некорректное разрешение видео;**

- Нет сигнала от камеры;
- Обнаружен поврежденный кадр;
- Поток N отключен;
- GOP потока N больше рекомендуемого;
- GOP потока N больше критического значения;
- Edge Storage недоступен;
- Edge: архив поврежден;
- Edge: время не синхронизировано;
- Edge: истекло время ожидания ответа от Видеосервера;
- Edge: нет информации об архиве;
- Edge: отсутствуют запрашиваемые записи;
- Edge: ошибка загрузки архива.

Изображение слишком темное

- Сообщение появляется, если изображение от камеры слишком темное.
- Сообщение пропадает, когда уровень освещения нормализуется.

Изображение слишком яркое

- Сообщение появляется, если изображение от камеры слишком яркое.
- Сообщение пропадает, когда уровень освещения нормализуется.

Камера не сфокусирована

- Сообщение появляется, если камера не сфокусирована.
- Сообщение пропадает, когда камера снова сфокусирована.

Микрофон отключен

- Сообщение появляется, если нет сигнала от связанного с *Камерой Микрофона*.
- Сообщение пропадает через 7 секунд после установления соединения с *Микрофоном*.

Нарушена целостность архива

- Сообщение появляется, если не удалось найти или прочитать видео- или аудиофайл оперативного архива при воспроизведении с помощью *Медиа Клиента* или при экспорте с помощью *Конвертера архива*.

Внимание! Ситуация, в которой не найден файл, удаленный системой в штатном режиме (по срокам давности или "по кольцу") проблемной не считается.

- Сообщение пропадает, если ошибка не повторяется в течение 1 часа.

Некорректное разрешение видео

- Сообщение появляется, если ширина кадра видеопотока в пикселях не кратна 16 для черно-белого изображения. Это приводит к значительному снижению производительности и эффективности сжатия при использовании кодека MJPEG.

- Сообщение пропадает, когда с камеры начинает поступать видеопоток корректного разрешения.

Нет сигнала от камеры

- Сообщение появляется, если не удастся получить видеопоток, выбранный в параметре **Поток для записи** в настройках *Камеры*. Когда недоступен **Поток для записи**, все остальные потоки отключаются.
- Сообщение пропадает, если в течение 7 секунд с *Камеры* удастся получить заданный поток с корректным содержимым.

Обнаружен поврежденный кадр

- Сообщение появляется, если не удалось записать или воспроизвести с помощью *Медиа Клиента* кадр из оперативного или долговременного архива.
- Сообщение пропадает, если проблема не повторяется в течение 1 часа.

Поток N отключен

- Сообщение появляется, если от *Камеры* не удастся получить видеопоток или данные этого потока некорректны.
- Сообщение пропадает, если в течение 7 секунд с *Камеры* удастся получить заданный поток с корректным содержимым.

GOP потока N больше рекомендуемого

- Сообщение появляется, если размер GOP Потока N превышает рекомендуемую 1 секунду.
- Сообщение пропадает через 1 минуту, если проблема не повторяется.

GOP потока N больше критического значения

- Сообщение появляется, если размер GOP Потока N превышает рекомендуемые 2 секунды.
- Сообщение пропадает через 1 минуту, если проблема не повторяется.

Проблемы при работе с EdgeStorage Sync (см. [Локальное хранилище камеры \(Edge Storage\)](#))

Edge Storage недоступен

- Сообщение появляется, если не удалось подключиться к локальному хранилищу данных на камере. Возникает при любых ошибках подключения, кроме отсутствия связи с камерой. Например, при неудачной попытке авторизации.
- Сообщение пропадает через 3 минуты после подключения к локальному хранилищу.

Edge: архив поврежден

- Сообщение появляется, если архив камеры содержит различные записи за одно и то же время.
- Сообщение пропадает, если ошибка не повторяется в течение 3 минут.

Примечание. В большинстве случаев возникает вследствие перекрывания записей по времени, вызванного переводом времени на камере назад.

Edge: время не синхронизировано

- Сообщение появляется, если время на камере не синхронизировано со временем на *Видеосервере*.
- Сообщение пропадает, если ошибка не повторяется в течение 3 минут.

Edge: истекло время ожидания ответа от Видеосервера

- Сообщение появляется, если в течение установленного таймаута не удалось получить информацию об архиве на *Видеосервере*.
- Сообщение пропадает, если ошибка не повторяется в течение 3 минут.

Edge: нет информации об архиве

- Сообщение появляется, если не удалось получить корректной информации об архиве в локальном хранилище камеры.
- Сообщение пропадает, если ошибка не повторяется в течение 3 минут.

Edge: отсутствуют запрашиваемые записи

- Сообщение появляется, если запрашиваемые записи отсутствуют в локальном хранилище камеры. Эта часть архива не будет восстановлена.
- Сообщение пропадает, если ошибка не повторяется в течение 3 минут.

Edge: ошибка загрузки архива

- Сообщение появляется, если при копировании записи архива возникает ошибка.
- Сообщение пропадает, если ошибка не повторяется в течение 3 минут.

6.6.4 Микрофон

Для объекта *Микрофон* диагностируется следующая проблема:

Микрофон отключен

- Сообщение появляется, если нет сигнала от *Микрофона*.
- Сообщение пропадает через 7 секунд после установления соединения с *Микрофоном*.

6.6.5 Луч

Для объекта *Луч* диагностируется следующая проблема:

Луч саботирован

- Сообщение появляется, если от объекта *Луч* приходит событие SABOTAGE (см. [Руководство программиста SecurOS](#)).

- Сообщение пропадает через 7 секунд после получения события, отличного от SABOTAGE.

6.6.6 Удаленная система

Для объекта *Удаленная система* диагностируются следующие проблемы:

- **Не удалось обновить конфигурацию: некоторые объекты не поддерживаются SecurOS MCC;**
- **Отключена.**

Внимание! Проблемы диагностируются для объекта *Удаленная система* при **Прямом подключении** Центра мониторинга.

Не удалось обновить конфигурацию: некоторые объекты не поддерживаются SecurOS MCC

- Сообщение появляется, если обнаружено несоответствие набора установленных Модулей в SecurOS MCC и Удаленной системе. Взаимодействие с Удаленной системой ограничено. Текущая конфигурация неактуальна и будет обновлена только после установки всех недостающих Модулей в SecurOS MCC.
- Сообщение пропадает сразу после обновления конфигурации.

Отключена

- Сообщение появляется, если потеряно соединение с Сервером конфигураций удаленной системы или заданный в настройках сервер не является Сервером конфигураций. Взаимодействие с удаленной системой ограничено.
- Сообщение пропадает через 7 секунд после установления соединения с Сервером конфигураций.

Примечание. Проблема также поднимается в случае, если в параметре **Адрес Сервера конфигураций** объекта *Удаленная система* задан неправильный адрес.

6.7 Синхронизация файлов SecurOS

Некоторые модули, интеграции и настройки SecurOS требуют наличия дополнительных или измененных файлов на всех *Видеосерверах* и *Рабочих местах оператора*. Сервер конфигураций SecurOS синхронизирует такие файлы между всеми компьютерами в сети безопасности.

Синхронизация выполняется по следующим правилам:

- Синхронизируются следующие файлы:
 - *.dbi — только в корневой папке SecurOS;
 - *.ddi — только в корневой папке SecurOS;
 - Modules/map/*.ini;
 - Modules/Map/scripts/*.js;
 - skins/macro_icons — иконки для *Макрокоманд* (см. **Макрокоманда**);
 - skins/_common/acs/*.png;
 - acs_*.json — только в корневой папке SecurOS;
 - *.integration.json — в корневой папке SecurOS и её поддиректориях;

- Modules/auto/LPR — синхронизируются все поддиректории и файлы кроме тех, которые не используются объектами *Auto: Распознаватель номеров* и *Auto: Интерфейс оператора*.
- Файлы для синхронизации загружаются в память *Сервера конфигурации*, когда на нем запускается SecurOS. Если файлы были дополнены/изменены, необходимо перезапустить SecurOS на *Сервере конфигураций*.
- Если SecurOS на *Сервере конфигураций* был перезапущен с новыми/измененными файлами, все *Периферийные серверы* автоматически перезапустят SecurOS для обновления файлов.
- *Рабочие места оператора* загружают файлы с того *Видеосервера*, к которому подключаются. Полученные файлы хранятся:
 - в ОС Windows — в папке %ProgramData%\ISS\client;
 - в ОС Linux — в папке /var/opt/securos/client.
- Синхронизация возможна только между компьютерами, на которых установлен SecurOS одной версии.

Внимание! При работе в кластере обновление файлов на *Сервере конфигураций* необходимо выполнять в сервисном режиме кластера (см. [Конфигурирование кластера](#)).

7 Основная подсистема

Основная подсистема взаимодействует с компьютерами в распределенной сети SecurOS и установленными (такими как, например, модуль распознавания автомобильных номеров), а также другими подсистемами (например аудио- и видеоподсистемой, подсистемой телеметрии).

7.1 Принципы работы

Основная подсистема является ядром SecurOS и отслеживает состояние всех подключенных объектов, модулей и устройств.

Каждый объект SecurOS отправляет данные о своем состоянии и о событиях, возникающих в процессе его работы, основной подсистеме, которая, в свою очередь, осуществляет управление всей системой безопасности.

Компьютеры, взаимодействующие посредством основной подсистемы, являются узлами распределенной сети SecurOS. Подключение или отключение каждого узла регистрируется в файле протокола SecurOS в режиме реального времени.

Основная подсистема SecurOS позволяет подключать и отключать узлы сети безопасности, конфигурировать и синхронизировать конфигурации между узлами в сети безопасности, а также проводить мониторинг всех изменений в состоянии модулей и объектов.

При отключении узла или сегмента сети ему присваивается статус отключенного и он становится недоступным для администрирования, пока не подключится снова. При возобновлении подключения узла загружаются обновленные данные конфигурации сети, и протокол событий подключенного узла синхронизируется с файлом протокола сети SecurOS.

Обновление конфигурации позволяет постоянно просматривать видео с подключенных видеокамер, прослушивать звук, посылать команды устройствам, наблюдать за охранно-пожарными системами и управлять ими с любого рабочего места оператора сети SecurOS.

7.2 Протоколы обмена данными

Обмен данными между некоторыми модулями в сети SecurOS может осуществляться по протоколу TLS (версии 1.2).

Режим обмена данными в сети SecurOS задается в настройках объекта Система. Возможны следующие варианты соединений:

- соединения без использования TLS-протокола;
- использование TLS-протокола в соединениях для тех модулей, которые поддерживают шифрование канала передачи данных. Соединения между прочими модулями используют обычные протоколы обмена данными;
- соединения с передачей данных только по TLS-протоколу.

7.3 Описание объектов

Основная подсистема представлена следующими объектами:

- Система.
- Объект охраны.
- База данных.
- Отдел.
- Пользователь.
- Active Directory / LDAP.
- Права пользователя.
- Компьютер.
- Водяной знак.
- Фильтр событий.
- Сценарий поведения.
- SNMP агент.
- Внешнее приложение.
- Database Partitioner.
- Репликатор баз данных.

7.3.1 Система

Корневой объект всего дерева объектов, определяющий параметры всей системы. Объект нельзя удалить или отключить. Операции просмотра и редактирования параметров объекта доступны только суперпользователю (см. [Пользователи в SecurOS](#)).

Родительский объект — отсутствует (корневой объект).

Пароль суперпользователя

Новый пароль: 

Подтвердите новый пароль: 

Доступ из Центра Мониторинга и Контроля

☒ Разрешить доступ: 

☐ Запретить привилегированный доступ

Центр Мониторинга и Контроля

☒ Привилегированный доступ к Удаленным системам

Прокси-сервер для FaceX:  Не использовать 

Сохранение и восстановление конфигурации

☒ Автоматическое создание резервных копий 

Максимальное количество копий: 

Аудит

☐ Записывать данные аудита системы

Период аудита:  5 минут 

Безопасность

☐ Использовать защищённые соединения 

☒ Разрешить незащищённые подключения

☐ Принимать только TLS-подключения

Рис. 97. Окно настройки параметров объекта Система

Таблица 5. Параметры объекта Система

Параметр	Описание
Пароль суперпользователя (Для отображения вводимых символов нажмите кнопку  . Для скрытия символов нажмите кнопку  .)	
Новый пароль	Введите новый пароль суперпользователя (см. Смена пароля суперпользователя).
Подтвердите новый пароль	Подтвердите новый пароль суперпользователя.
Доступ из Центра Мониторинга и Контроля	
Разрешить доступ	Флаг управления доступом к настраиваемой системе из <i>Центра Мониторинга</i> и пароль доступа. Если не отмечен, доступ к настраиваемой системе из <i>Центра Мониторинга</i> будет запрещен. Если отмечен, доступ к настраиваемой системе из <i>Центра Мониторинга</i> будет предоставлен при совпадении заданного пароля с паролем, установленным в настройках объекта <i>Удаленная система</i> .

Параметр	Описание
Запретить привилегированный доступ	Отметьте флажок, если необходимо запретить доступ к <i>Удаленной системе</i> из <i>Центра Мониторинга</i> для проведения в ней специальных операций (подробнее см. Привилегированный доступ). Доступен, если отмечен флажок Разрешить доступ. Примечание. Настройка выполняется только на стороне <i>Удаленной системы</i>.
Центр Мониторинга и Контроля	
Привилегированный доступ к Удаленным системам	Отметьте флажок, чтобы включить возможность привилегированного доступа к <i>Удаленным системам</i> для проведения специальных операций (подробнее см. Привилегированный доступ). Внимание! Функциональность доступна только для типа SecurOS MCC PA.
Прокси-сервер для FaceX	Выберите прокси-сервер для передачи данных Модуля SecurOS FaceX между <i>Удаленной системой</i> и <i>Рабочими местами операторов Центра мониторинга</i> (см. MCC DC HTTP Proxy).
Сохранение и восстановление конфигурации	
Сохранить (кнопка)	Нажмите кнопку для сохранения конфигурации в качестве шаблона в JSON-файле. С помощью файлового менеджера выберите директорию и задайте имя сохраняемого файла. По умолчанию файл будет сохранен с именем <code>default.json</code>: • в ОС Windows — в папке <code>%ProgramData%\ISS\Sys_config</code>; • в ОС Linux — в папке <code>/var/opt/securos/Sys_config</code>. Внимание! Не рекомендуется называть файл <code>wizard.json</code>, так как данное имя используется системой для автоматического сохранения последней успешно загруженной конфигурации.
Восстановить (кнопка)	Нажмите кнопку, чтобы восстановить конфигурацию системы из файла. Файл конфигурации выбирается администратором из списка ранее сохраненных версий. Процедура восстановления конфигурации включает следующие этапы: • Восстановление конфигурации на <i>Сервере конфигураций</i>. • Обновление конфигурации на всех <i>Периферийных серверах</i> с <i>Сервера конфигураций</i>. Конфигурация <i>Периферийного сервера</i>, используемая до обновления, сохраняется в файл. При невозможности восстановить конфигурацию из файла производится откат к текущей конфигурации. Внимание! Для восстановления рекомендуется использовать ту копию файла конфигурации, которая соответствует текущей установленной версии SecurOS. При восстановлении конфигурации из файлов других версий корректная работа SecurOS не гарантируется.

Параметр	Описание
Автоматическое создание резервных копий	Флаг управления режимом автоматического создания резервных копий текущей конфигурации системы. По умолчанию отмечен. В данном режиме резервная копия: • Создается ежедневно, в 01:45 по локальному времени. • Создается только в случае изменения конфигурации системы за прошедшие сутки. • Создается на каждом <i>Видеосервере</i> даже в случае отсутствия соединения между <i>Периферийным сервером</i> и <i>Сервером конфигураций</i>. В данном случае копии конфигураций будут различаться. • Создается с именем Backup_<дата>_r<ревизия конфигурации>.json, например, Backup_2019-07-01_r0000000016.json, в следующих папках: – в ОС Windows — в папке %ProgramData%\ISS\Sys_config; – в ОС Linux — в папке /var/opt/securos/Sys_config. Значение <дата> в имени файла задается в ISO-формате. • Создается вне расписания в случае, если текущая непустая конфигурация восстанавливается из файла. Также копия создается при старте системы, если на момент старта текущая конфигурация системы отличается от последней резервной копии или резервная копия отсутствует. Примечание. При работе в конфигурации SecurOS MCC любое изменение конфигурации внешней системы приводит к изменению конфигурации SecurOS.
Максимальное количество копий	Задайте максимальное количество автоматически сохраняемых резервных копий. Диапазон возможных значений: [1 ; 30]. При достижении максимального значения автоматически созданные файлы копий конфигурации удаляются "по кольцу". Файлы конфигурации с именами, отличными от шаблонного, при этом не удаляются.
Аудит	
Записывать данные аудита системы	Отметьте флажок для проведения аудита системы и записи полученных данных. Запись ведется в специальную базу данных аудита, которая автоматически создается при установке флажка (подробнее см. Руководство пользователя SecurOS AuditTrail).

Параметр	Описание
Период аудита	Выберите из списка значение периода аудита. Под периодом аудита понимается временной интервал, используемый для фиксации длительных действий пользователя в системе. К таким действиям относятся следующие: • просмотр живого и архивного видео; • управление PTZ. Внимание! В каждом астрономическом часе содержится несколько периодов аудита. Начало первого в часе периода аудита совпадает с началом каждого астрономического часа. Заданное значение параметра влияет на формирование записей в базе данных аудита, которые можно просмотреть с помощью утилиты AuditClient. Анализ результатов работы утилиты подробно рассмотрен в разделе Примеры анализа действий пользователя.
Безопасность	
Использовать защищенные соединения	Отметьте флажок для изменения режима передачи данных в SecurOS.
Разрешить незащищенные соединения	Выберите данную опцию, чтобы использовать защищенные соединения там, где это возможно. Примечание. Модули, не поддерживающие протоколы шифрования данных, будут функционировать в обычном режиме.
Принимать только TLS-подключения	Выберите данную опцию, чтобы использовать только защищенные соединения. Примечание. Модули, не поддерживающие протоколы шифрования данных, функционировать не будут.

7.3.2 Объект охраны

Объект используется для разбиения сети SecurOS на отдельные сегменты при охране большой территории, когда необходимо независимое централизованное наблюдение за определенными участками.

Дополнительно можно организовать фильтрацию событий между *Видеосерверами* системы. Используя фильтр, можно разрешить или запретить передачу всех событий системы на выбранный *Видеосервер* (подробнее см. **Закладка Серверы для подключения**).

Для более детального разграничения доступа к объектам можно назначить права пользователям и определить уровень доступа к каждому из объектов охраны по отдельности (см. **Регистрация и настройка прав пользователей**). Например, можно ограничить доступ операторов к наблюдению территории, просмотру сигналов с определенных камер. Наблюдателю могут быть даны права на управление режимами наблюдения, включение/выключение камер, управление камерами, а главный центр охраны может составлять отчеты.

Настройки объекта позволяют распределить нагрузку на *Видеосерверы* со стороны *Рабочих мест оператора* (см. **Закладка Серверы для подключения**). В целях дополнительной защиты объект позволяет сформировать белый список IP-адресов для доступа к *Видеосерверам* (см. **Закладка Ограничение подключений**).

Используя несколько объектов охраны и настройку прав пользователей, можно делегировать привилегии администратора по управлению охраной территории, распределенной между независимыми компаниями. В этом случае сеть SecurOS делится на несколько сегментов, для каждого из которых мониторинг и администрирование будет осуществлять отдельный администратор.

Примечание. Для каждого объекта охраны применяется отдельный протокол событий.

Рекомендуется создать несколько объектов охраны в следующих случаях:

- если подсистема контроля доступа использует устройства считывания (магнитные карточки) с разными кодами пропуски на разные территории;
- если подсистема контроля доступа распределена на несколько зон с разным расписанием допуска (например, праздничные дни) и каждая зона имеет свои отделы и пользователей (например, несколько организаций в одном здании);
- если необходимо организовать отдельный протокол событий для подмножества объектов системы безопасности SecurOS.

Родительский объект — **Система**.

Окно настройки параметров содержит следующие закладки:

- Закладка **Общие**.
- Закладка **Серверы для подключения**.
- Закладка **Ограничение подключений**.
- Закладка **Управление паролями**.

7.3.2.1 Закладка Общие

Рис. 98. Окно настройки параметров объекта Объект охраны. Закладка Общие

Таблица 6. Параметры объекта Объект охраны. Закладка Общие

Параметр	Описание
Размер базы протокола (дней)	Длительность хранения сообщений о событиях в БД <i>Протокол событий</i> (дней, не более). В базе будут храниться сообщения о событиях для объектов, принадлежащих только этому объекту охраны. Возможные значения: [1; 9999]. Значение по умолчанию: 7. По истечении срока хранения сообщения удаляются автоматически. Удаление выполняется либо при старте SecurOS, либо один раз в сутки, в момент времени 02:45:00 (чч:мм:сс).
При старте запускать Макрокоманду	Выберите из списка доступных макрокоманд (объектов <i>Макрокоманда</i> , см. раздел Макрокоманда) ту, которая будет выполняться на <i>Видеосервере</i> при старте системы (см. Условия запуска Макрокоманды).
Праздничные дни	Заполните таблицу списком дат (формат ДД.ММ.ГГ), который будет использоваться для определения доступа в праздничные дни. Эти дни также используются в Расписании .

Условия запуска Макрокоманды

Макрокоманда запускается в случае, если при старте SecurOS успешно стартовали все исполнители, реализующие функциональность системы. Если установлены интеллектуальные Модули SecurOS (например, SecurOS Auto), также должны успешно стартовать исполнители этих Модулей. Если хоть один из исполнителей не стартовал, *Макрокоманда* запущена не будет.

7.3.2.2 Закладка Серверы для подключения

Рабочее место оператора является клиентским приложением и для работы должно быть подключено к серверу SecurOS. Первое подключение выполняется в ручном режиме. Оператор указывает сервер для подключения в окне **Авторизация** (см. [Запуск SecurOS на Рабочем месте оператора](#)). В дальнейшем может быть настроено автоматическое подключение (см. [Автоматическая авторизация](#)).

Внешний вид закладки представлен на рис. 99.

Закладка позволяет выбрать, к каким серверам разрешено подключение *Рабочих мест оператора*, к каким – нет, а также разделить эти серверы на группы. С помощью групп осуществляется балансировка нагрузки на серверы. Так, в случае выхода сервера из строя, произойдет попытка автоматического переподключения *Рабочего места оператора* к другому серверу из той же группы.

Примечание. Для смены группы серверов необходимо завершить сеанс пользователя и выполнить подключение к серверу из другой группы.

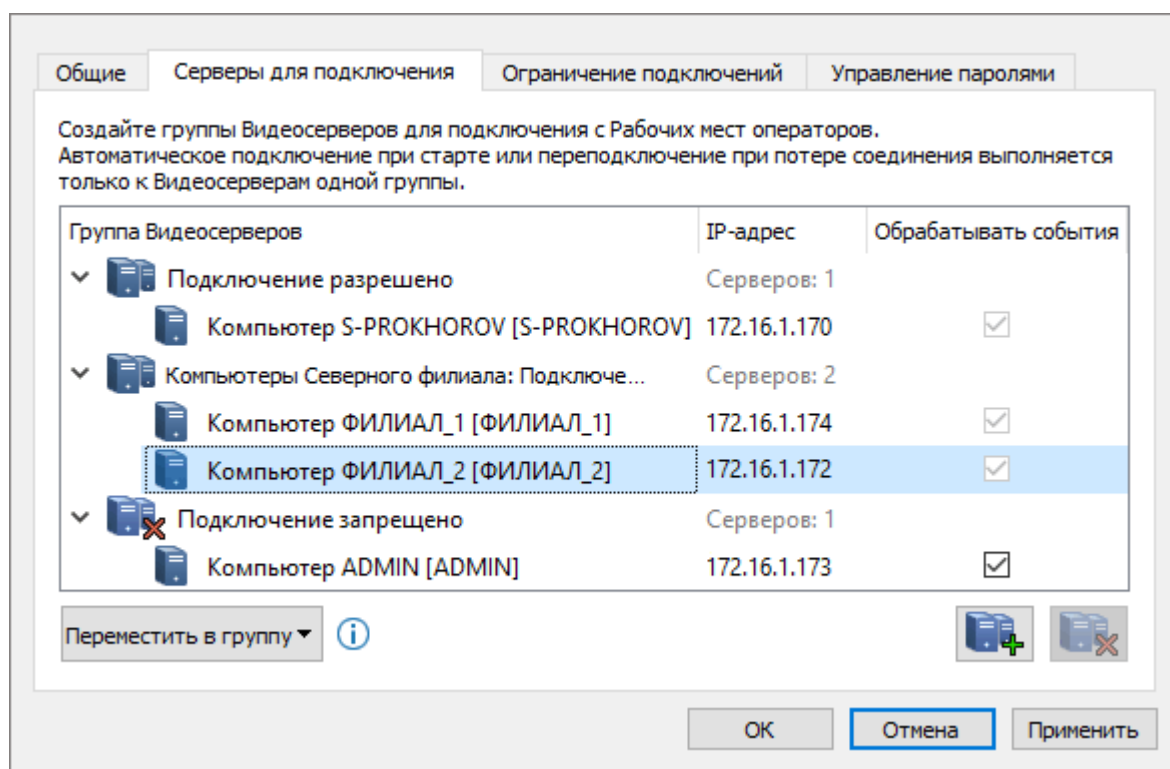


Рис. 99. Окно настройки параметров объекта Объект охраны. Закладка Серверы для подключения

Изначально список серверов содержит две системные группы – **Подключение разрешено** и **Подключение запрещено**. При этом все серверы, входящие в конфигурацию SecurOS, по умолчанию размещаются в группе **Подключение разрешено**. В эту же группу автоматически добавляются все новые *Видеосерверы*.

В зависимости от принадлежности *Видеосервера* к группе для него можно либо разрешить, либо запретить получение и обработку событий от остальных *Видеосерверов* системы. Запрет/разрешение относится ко всем событиям. При запрете обработки событий снижается нагрузка на сеть, связанная с их передачей. Если *Видеосервер* входит в группу:

1. **Подключение разрешено** — флажок **Обрабатывать события** по умолчанию отмечен и не может быть снят. Такие сервера всегда будут получать и обрабатывать все события от прочих *Видеосерверов* системы.
2. **Подключение запрещено** — флажок **Обрабатывать события** по умолчанию отмечен и может быть снят. Таким образом, для *Видеосерверов* этой группы получение и обработку всех событий от прочих *Видеосерверов* системы можно запретить.

Внимание! При подключении к серверам группы **Подключение запрещено** вход с любого компьютера может выполнить только суперпользователь (см. **Пользователи в SecurOS**). Другие пользователи могут выполнить вход только при локальном подключении клиентского приложения к этому серверу. При этом, если для таких серверов флажок **Обрабатывать события** не отмечен, состояния объектов на таких серверах будут неактуальными, т.к. события от прочих серверов системы не приходят и не обрабатываются.

При работе со списком пользователю доступны следующие операции:

1. **Создание группы** — чтобы создать новую группу серверов, нажмите кнопку  (**Создать группу**). Система автоматически создаст группу с именем N: Разрешено подключение, где N — порядковый номер группы с данным именем (если такие существуют в списке).
2. **Переименование группы** — чтобы переименовать группу, щелкните ее мышью и в поле ввода задайте новое название группы.
3. **Удаление группы** — чтобы удалить группу, выделите ее в списке, нажмите кнопку  (**Удалить группу**).

Внимание! Удалить группу, которая содержит сервера, невозможно. Для удаления такой группы сначала переместите сервера в другую группу. Также невозможно удалить системные группы **Подключение разрешено** и **Подключение запрещено**.

4. **Перемещение сервера в другую группу** — для перемещения выделите один или несколько серверов, нажмите кнопку **Переместить в группу** и выберите из списка требуемую группу. Также сервер можно переместить щелкнув его мышью, и, удерживая кнопку нажатой, перетащить его в нужную группу.

7.3.2.3 Закладка Ограничение подключений

Закладка позволяет настроить список компьютеров, которые могут подключаться к серверам из конфигурации SecurOS. Внешний вид закладки представлен на рис. 100.

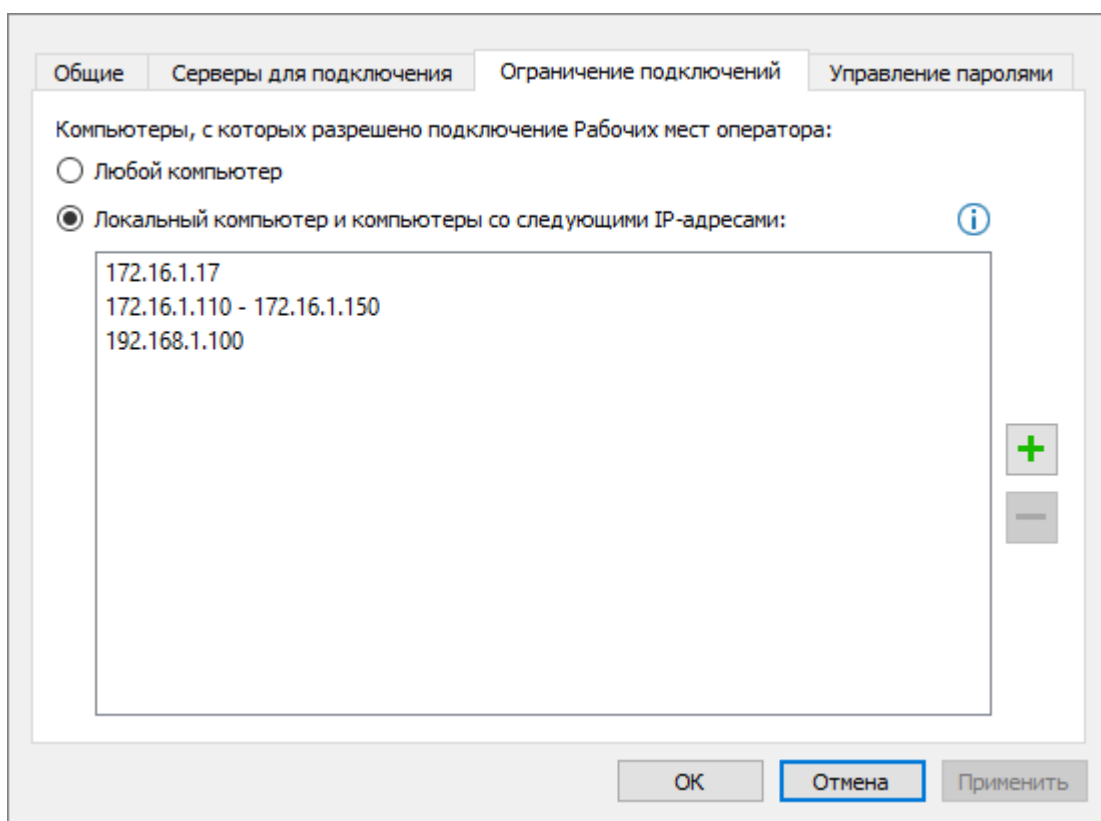


Рис. 100. Окно настройки параметров объекта Объект охраны. Закладка Ограничение подключений

Режим **Любой компьютер** выбран по умолчанию и дает возможность любому компьютеру с установленным ПО SecurOS выполнить подключение к любому серверу системы с учетом настроек на **Закладке Серверы для подключения**. Оператору достаточно знать логин и пароль пользователя SecurOS.

В качестве дополнительной меры безопасности можно ограничить список компьютеров, от которых серверы будут принимать подключение. Чтобы установить такое ограничение, выполните следующие действия:

- Для параметра **Компьютеры, с которых разрешено подключение Рабочих мест оператора** выберите вариант **Локальный компьютер и компьютеры со следующими IP-адресами**.
- Добавьте IP-адреса компьютеров в список ниже, используя кнопку . Если таких компьютеров много, и они имеют последовательные IP-адреса, удобно указать диапазон IP-адресов. Например, 172.16.1.110-172.16.1.150. IP-адреса могут быть указаны в стандарте IPv4 или IPv6.

Примечание. Если при работе в кластере (см. **Отказоустойчивый кластер**) планируется запускать интерфейс оператора на *Хостах*, необходимо добавить в список все IP-адреса *Хостов*, виртуальные IP-адреса *Нод* и виртуальный IP-адрес *Сервера конфигураций*.

7.3.2.4 Закладка Управление паролями

Закладка позволяет настроить параметры паролей (сложность, срок действия, смену/сброс пароля) для типовых пользователей SecurOS. Внешний вид закладки представлен на рис. 101.

Внимание! Параметры управления паролями не применяются к пользователям Active Directory/LDAP и суперпользователю системы (root) и пользователям, использующим автоматическую авторизацию.

Рис. 101. Окно настройки параметров объекта Объект охраны. Закладка Управление паролями

Таблица 7. Параметры объекта Объект охраны. Закладка Управление паролями

Параметр	Описание
Минимальное количество символов пароля	Параметр определяет необходимость задания пароля не менее указанного количества символов. Влияет как на задание пароля через объект Пользователь, так и на самостоятельную смену пароля пользователем (см. Смена/сброс пароля типового пользователя). Возможные значения: [6; 64]. Значение по умолчанию: 8. Примечание. Изменение значения параметра не влияет на текущие пароли типовых пользователей в системе.
Максимальный срок действия пароля (дней)	Параметр определяет срок действия пароля пользователей в днях. По истечении срока пароля, пользователь не сможет авторизоваться, используя пароль с истекшим сроком действия. Возможные значения: [1; 120]. Значение по умолчанию: 90. Примечание. При изменении значения параметра для текущих паролей, количество дней, которое прошло с момента их задания, вычитается из нового срока.

Параметр	Описание
Оповещать об окончании срока действия пароля за (дней)	Параметр определяет за сколько дней до окончания срока действия пароля необходимо начинать оповещение пользователей. Когда до окончания срока действия пароля остается указанное количество дней или меньше, у авторизованного пользователя будет появляться соответствующее информационное сообщение 1 раз в сутки. Возможные значения: [1; 30]. Значение по умолчанию: 5. Параметр становится доступен при активации флажка Максимальный срок действия пароля (дней).
Обязательное соответствие пароля требованиям к сложности	Отметьте флажок, чтобы включить следующие требования к надежности пароля при его создании/смене: • наличие строчных и прописных букв; • наличие цифр (0-9); • наличие специальных символов (~!@#\$%^&* _-+=` \(){} [] : ; " ' < > , . ? /); • длина пароля не менее 6 символов; • пароль не содержит в себе имя текущего пользователя. Примечание. Параметр не применяется к текущим паролям.
Разрешить смену пароля через Панель управления	Отметьте флажок, чтобы предоставить типовым пользователям возможность смены своих паролей после авторизации в системе. При активации параметра в меню <i>Панели управления</i> и в контекстном меню значка <i>Клиента SecurOS</i> в системном трее появляется пункт Сменить пароль (см. Смена/сброс пароля типового пользователя).
Разрешить сброс пароля через e-mail при авторизации	Отметьте флажок, чтобы предоставить типовым пользователям возможность сброса пароля из окна авторизации с помощью e-mail (см. Смена/сброс пароля типового пользователя). Для работы функциональности необходимо выбрать объект <i>Сервис почтовых сообщений</i> в параметре Сервис для отправки кодов сброса пароля (см. ниже).
Сервис для отправки кодов сброса пароля	В выпадающем списке выберите объект <i>Сервис почтовых сообщений</i>, в настройках которого активирован параметр Использовать для двухфакторной аутентификации и сброса пароля (см. Сервис почтовых сообщений). Параметр становится доступен при активации флажка Разрешить сброс пароля через e-mail при авторизации.

7.3.3 База данных

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*.

Объект используется для представления в SecurOS баз данных системы SecurOS, Модулей SecurOS и внешних баз данных.

Родительский объект — *Объект охраны\группа Базы данных*.

Рис. 102. Окно настройки параметров объекта База данных

Таблица 8. Параметры объекта База данных

Параметр	Описание
База данных	
Подключиться (опция)	Подключиться к созданной ранее Базе данных, используя заданные ниже параметры.
Создать новую (опция)	Создать новую Базу данных и учетную запись Пользователя (см. рис. 103). Внимание! Созданная с помощью этой опции База данных не может быть использована для работы следующих Модулей: SecurOS Auto, SecurOS Cargo, SecurOS Transit, SecurOS POS.

Параметр	Описание
Тип	Тип используемой базы данных. Возможные значения: • PostgreSQL — для подключения к БД PostgreSQL; • SQL Server — для подключения к БД Microsoft SQL Server. По умолчанию принимает значение PostgreSQL.
Сервер	DNS-имя или IP-адрес сервера, на котором установлена база данных, к которой осуществляется подключение. Если база данных установлена на локальном компьютере, с которого производится настройка системы, используйте значение по умолчанию.
Порт	Номер порта сервера для подключения к СУБД. По умолчанию принимает значение 5432.
Имя базы, Пользователь, Пароль	Имя базы данных, имя пользователя и пароль пользователя, заданные при установке базы данных. Внимание! При задании Пароля БД кириллические символы не допускаются. Используйте только латинские символы кодовой страницы западноевропейских языков Latin-1.
Проверка подключения (кнопка)	Для проверки соединения с заданными параметрами щелкните кнопку Проверка подключения . Если параметры заданы корректно и соединение по локальной сети возможно, слева от кнопки будет выведено подтверждение (ОК).
Опции	
Удалять записи старше	Срок хранения записей (в днях). Если принимает значение 0, записи не удаляются. Примечание. При работе с базами данных некоторых интеллектуальных Модулей SecurOS параметр игнорируется.

Рис. 103. Создание новой Базы данных и учетной записи Пользователя

Таблица 9. Параметры создания объекта База данных

Параметр	Описание
База данных	
Создать БД и Пользователя (кнопка)	Создать новую <i>Базу данных</i> для использования со сторонними системами <i>СКУД/ОПС</i> (см. Руководство пользователя SecurOS СКУД/ОПС). После задания параметров, нажмите на кнопку для создания в каталоге PostgreSQL новой базы данных и учетной записи ее пользователя. Созданная база будет размечена для хранения данных, поступающих от внешней системы <i>СКУД/ОПС</i> .
Примечание. Прочие параметры создаваемой <i>Базы данных</i> аналогичны описанным выше.	

7.3.4 Отдел

Объект используется для объединения пользователей в группы. В основном применяется в подсистеме контроля доступа и задает пользователей с определенными правами в самой сети SecurOS (см. раздел [Регистрация и настройка прав пользователей](#)).

Родительский объект — *Объект охраны\группа Пользователи и Права*.

Параметры для редактирования отсутствуют.

Примечание. Объект *Отдел* автоматически создается в дереве объектов только в том случае, если на этапе настройки системы с помощью Мастера первого запуска в системе были зарегистрированы пользователи с правами *Опытный пользователь* или *Простой пользователь*.

7.3.5 Пользователь

Объект представляет одного сотрудника (или пользователя в сети SecurOS).

Родительский объект — **Отдел**.

Внимание! Название объекта *Пользователь*, заданное в окне **Параметры создаваемого объекта**, будет использоваться далее в качестве имени пользователя при авторизации в системе. При этом авторизация возможна только на тех *Компьютерах*, которые относятся к тому же *Объекту охраны*, что и созданный *Пользователь*.

Рис. 104. Окно настройки параметров объекта Пользователь

Таблица 10. Параметры объекта Пользователь

Параметр	Описание
Пароль	Пароль пользователя. Используется для входа в систему, если данному пользователю назначены определенные права (см. Права пользователя). Обязательный параметр. Для просмотра скрытых символов пароля нажмите кнопку . Если в <i>Объекте охраны</i> настроены требования к длине и сложности пароля (см. Закладка Управление паролями), то новый пароль должен соответствовать этим требованиям. Требования к паролю перечислены во всплывающей подсказке. В случае несоответствия нового пароля заданным требованиям в окне отобразится уведомление.
Телефон	Укажите номер телефона сотрудника. Не используется системой. Может использоваться в скриптах SecurOS для отправки голосового или SMS-оповещения.

Параметр	Описание
E-mail	Укажите адрес электронной почты сотрудника. Если в системе применяется процедура двухфакторной аутентификации (см. Двухфакторная аутентификация в SecurOS), на указанный адрес будут поступать сообщения с одноразовым кодом доступа. Если в системе разрешена процедура сброса пароля с помощью e-mail (см. Смена/сброс пароля типового пользователя), на указанный адрес будут поступать сообщения с кодом для сброса пароля. Внимание! Если в Правах пользователя отмечен флажок Использовать двухфакторную аутентификацию по e-mail или для Объекта охраны отмечен флажок Разрешить сброс пароля через e-mail при авторизации (см. Закладка Управление паролями), параметр является обязательным. Указанный адрес также может использоваться в скриптах SecurOS для отправки почтового сообщения.
Требовать смену пароля при следующем входе в систему	При активации флажка пользователь будет обязан сменить установленный пароль при следующей авторизации в <i>Клиенте SecurOS</i>. Автоматический выход из текущих сессий пользователя не происходит. Внимание! Требование смены пароля не применяется при авторизации в web-приложениях SecurOS.
Дополнительная информация	Задайте любую информацию в произвольной форме, например паспортные данные сотрудника, его социальный статус. Не используется системой.

7.3.6 Active Directory / LDAP

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

В ОС **Linux** функциональность не поддерживается.

Объект предназначен для настройки домена, на который будет поступать запрос при авторизации в системе SecurOS. Для получения подробной информации см. раздел [Пример настройки прав пользователей сетевого домена](#).

Родительский объект — *Объект охраны\группа Пользователи и Права*.

Примечание. Авторизация пользователя через Active Directory возможна, если компьютер сети SecurOS состоит в домене Active Directory Windows.

Рис. 105. Окно настройки параметров объекта Active Directory / LDAP

Таблица 11. Параметры объекта Active Directory / LDAP

Параметр	Описание
Подключение	
Провайдер	Выберите тип протокола. Возможные значения: - Windows NT (локальный или доменный) — для работы только под Windows; - LDAP (доменный) — для работы под Windows и/или Linux.
Использовать шифрование	Отметьте флажок, чтобы использовать шифрование при взаимодействии с контроллером домена. Доступен в случае, если параметр Провайдер принимает значение LDAP (доменный).
Использовать контроллер домена	Отметьте флажок для использования основного домена. Внимание! Если отмечен, то следующие два параметра настройки недоступны.

Параметр	Описание
Сервер	Задайте параметры контроллера домена в зависимости от выбранного Провайдера: - Windows NT (локальный или доменный) — для авторизации пользователя с компьютера, зарегистрированного в домене, укажите короткое имя домена (например, OFFICE). Для авторизации пользователя с компьютера, не зарегистрированного в домене, но подключенного к сети, укажите полное имя домена (например, OFFICE.COMPANY). - LDAP (доменный) — для авторизации пользователя укажите IP-адрес или DNS имя контроллера домена.
Порт	<i>Необязательное поле:</i> укажите номер порта. Указывается для провайдера LDAP (доменный) или при нестандартных настройках сервера.
Пользователи	
Использовать учетную запись операционной системы	Отметьте флажок для использования при авторизации учетной записи пользователя. Внимание! Если отмечен, то следующие два параметра настройки недоступны.
Имя пользователя, Пароль	Задайте имя и пароль (учетная запись) пользователя для авторизации на сервере.

7.3.7 Права пользователя

Объект определяет права пользователей в системе (см. **Регистрация и настройка прав пользователей**).

Примечание. Все пользователи, указанные в настройках объекта *Права пользователя*, обладают одинаковым набором прав. Для присвоения других прав другой группе пользователей, необходимо создать новый объект *Права пользователя*.

Родительский объект — *Объект охраны\группа Пользователи и Права*.

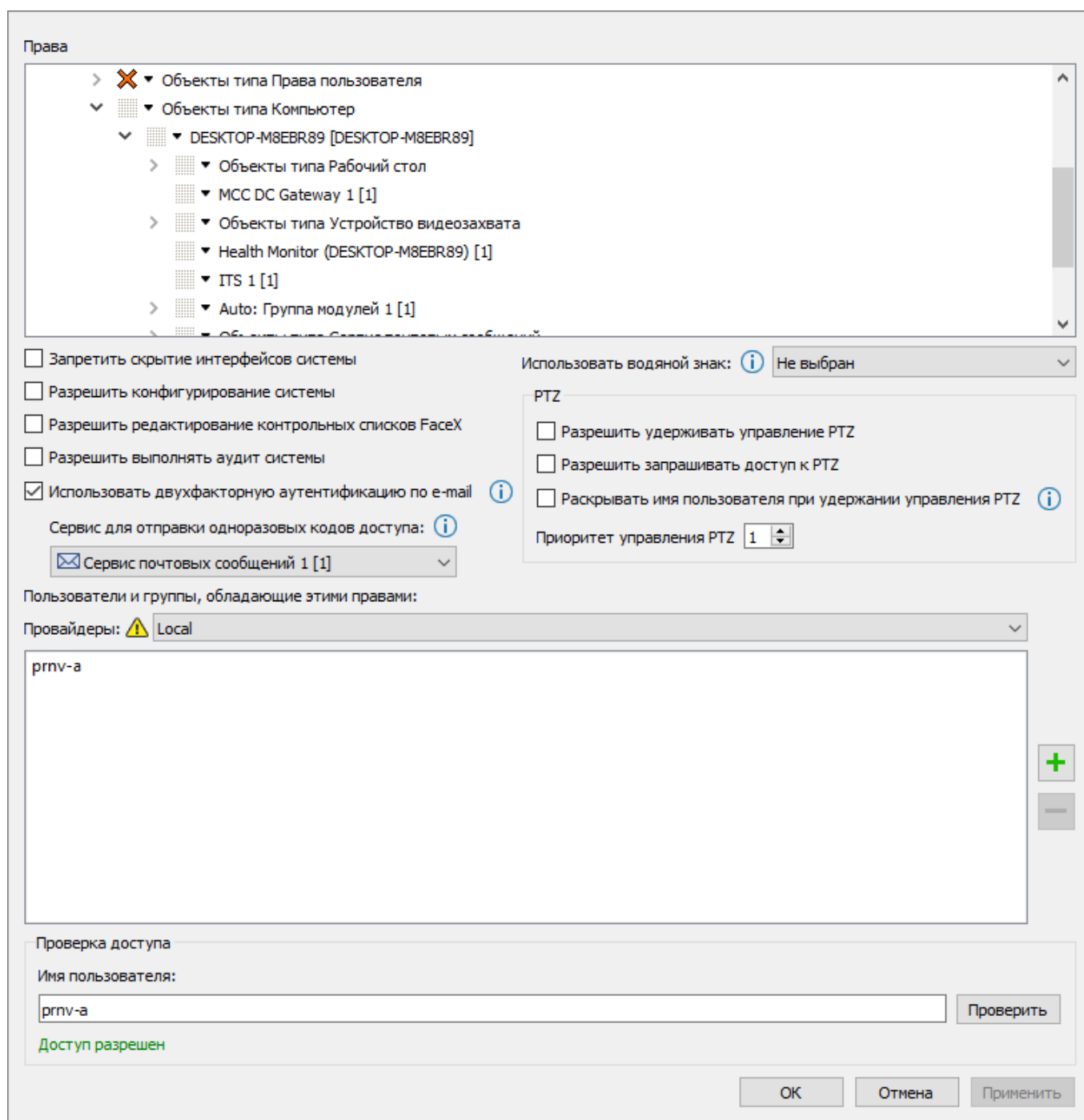


Рис. 106. Окно настройки объекта Права пользователя

Таблица 12. Параметры объекта Права пользователя

Параметр	Описание
Права	Дерево объектов, отражающее права пользователя на объекты. Чтобы определить уровень доступа пользователя к какому-либо объекту или группе (<i>Объекты типа...</i>), выберите значок этого объекта или группы. Описание значков приведено ниже.
Запретить скрывание интерфейсов системы	Отметьте флажок для запрета скрывания интерфейсов системы.

Параметр	Описание
Разрешить конфигурирование системы	Параметр определяет доступ пользователя к <i>Дереву объектов</i> SecurOS с помощью кнопки Конфигурирование системы (см. Центр администрирования). Если флажок отмечен, пользователь имеет доступ к <i>Дереву объектов</i> для просмотра и изменения параметров системы (Режим администратора, см. описание значков ниже). Если не отмечен, пользователь не имеет доступа к <i>Дереву объектов</i> для просмотра и изменения параметров системы (Режим оператора, см. описание значков ниже).
Разрешить редактирование контрольных списков FaceX	Отметьте флажок, чтобы дать пользователю возможность редактировать контрольные списки SecurOS FaceX (см. Руководство пользователя SecurOS FaceX).
Разрешить выполнять аудит системы	Отметьте флажок, чтобы разрешить пользователю выполнять аудит системы (подробнее см. Руководство пользователя SecurOS AuditTrail).
Использовать двухфакторную аутентификацию по e-mail	Отметьте флажок, чтобы включить режим двухфакторной аутентификации в SecurOS. Двухфакторная аутентификация возможна только для локальных пользователей SecurOS. Внимание! Ограничения режима описаны в разделе Двухфакторная аутентификация в SecurOS.
Сервис для отправки одноразовых кодов доступа	Выберите сервис, который будет использоваться для отправки пользователю одноразовых кодов доступа. Список содержит все объекты Сервис почтовых сообщений SecurOS, в настройках которых отмечен флажок Использовать для двухфакторной аутентификации и сброса пароля .
Использовать водяной знак	Выберите объект Водяной знак для постоянного отображения данных о <i>Пользователе</i> и/или его <i>Компьютере</i> поверх рабочей области <i>Медиа Клиента</i> (см. Наложение водяных знаков). Если установлено значение Не выбран, <i>Водяной знак</i> не используется.
PTZ	
Разрешить удерживать управление PTZ	Отметьте флажок, чтобы дать пользователю возможность удерживать управление PTZ в течение неограниченного времени (см. Раздельное управление телеметрией).
Разрешить запрашивать доступ к PTZ	Отметьте флажок, чтобы дать пользователю возможность запросить доступ к PTZ в случае, если управление удерживает пользователь с большим значением приоритета.
Раскрывать имя пользователя при удержании управления PTZ	Отметьте флажок, чтобы имя пользователя с этими правами было раскрыто для других пользователей при удержании PTZ в режиме раздельного управления (см. Раздельное управление телеметрией).

Параметр	Описание
Приоритет управления PTZ	Параметр определяет возможность пользователя перехватывать управление PTZ камеры в случае, если совместное управление телеметрией запрещено (см. Камера). Преимущественное право управления PTZ имеет пользователь с большим значением приоритета. Если пользователи имеют равный приоритет, право предоставляется тому пользователю, который первым захватил управление. Возможные значения: [1–10].
Пользователи и группы, обладающие этими правами	
Провайдеры	Выберите значение Local для назначения указанных прав доступа к выбранным объектам пользователям в списке Пользователи и Группы (см. ниже) или значение Active Directory / LDAP для назначения указанных прав пользователю/группе пользователей сетевого домена (см. раздел Active Directory / LDAP). В ОС Linux значение Active Directory / LDAP недоступно. Если отмечен флажок Использовать двухфакторную аутентификацию по e-mail, около поля выводится пиктограмма . Внимание! Для пользователей сетевого домена Active Directory/LDAP (см. Провайдеры) и суперпользователя SecurOS (см. Пользователи в SecurOS) двухфакторная аутентификация невозможна.
Список пользователей и групп	Список пользователей с определенными выше правами. Если в поле Провайдеры выбрано значение Local, для добавления пользователя нажмите кнопку . В области списка появится новая запись. Сделайте двойной щелчок по этой записи, затем выберите из выпадающего списка требуемого пользователя. Для удаления пользователя из списка выделите соответствующую запись мышью, затем нажмите кнопку  или клавишу Delete. Если в поле Провайдеры выбрано значение Active Directory / LDAP, список формируется по соответствующим правилам (см. раздел Пример настройки прав пользователей сетевого домена). В каждом случае имя сотрудника будет использовано как имя пользователя при авторизации в SecurOS. Примечание. Одного сотрудника (объект <i>Пользователь</i>) можно добавить в список только одного объекта <i>Права пользователя</i>. Внимание! При авторизации <i>Пользователя</i> в SecurOS будет использоваться пароль, заданный в настройках соответствующего объекта (см. Пользователь).

Параметр	Описание
Проверка доступа	
Имя пользователя	Задайте имя пользователя ОС или типового пользователя SecurOS, для которого необходимо проверить возможность авторизации в SecurOS.
Проверить (кнопка)	Нажмите кнопку для начала проверки. Подробное описание процедуры проверки приведено в разделе Регистрация и настройка прав пользователей .

Уровень доступа пользователя/группы пользователей к объекту/группе (блок **Права**) задается определенным значком. Значок можно изменить, нажав на него кнопкой мыши.

В системе доступны следующие значки:

-  — **доступ запрещен**. Устанавливает следующие правила поведения объекта:
 - в *Режиме администратора* — объект/группа отображается в *Дереве объектов SecurOS*. Настройка объекта и прочие операции с объектом/группой запрещены (кнопки управления на *Панели инструментов* заблокированы);
 - в *Режиме оператора* — объект/группа не отображается в интерфейсе оператора SecurOS.

Внимание! Если данный уровень доступа к объекту *Компьютер* установлен для пользователя/группы пользователей, ни один из таких пользователей не сможет авторизоваться в системе на этом компьютере.

-  — **просмотр**. Устанавливает следующие правила поведения объекта/группы:
 - в *Режиме администратора* — объект/группа отображается в *Дереве объектов SecurOS*. Настройка объекта и прочие операции с объектом/группой запрещены (кнопки управления на *Панели инструментов* заблокированы);
 - в *Режиме оператора* — объект/группа отображается в интерфейсе оператора SecurOS. Управление объектом запрещено. Например, *Камера* отображается в интерфейсе *Медиа Клиента*, но пользователь не может поставить ее на запись.
-  — **управление**. Устанавливает следующие правила поведения объекта/группы:
 - в *Режиме администратора* — аналогично уровню доступа **просмотр**.
 - в *Режиме оператора* — объект/группа отображается в интерфейсе оператора SecurOS. Управление объектом разрешено. Например, *Камера* отображается в интерфейсе *Медиа Клиента*, пользователь может поставить ее на запись, управлять телеметрией и т. д.
-  — **конфигурирование**. Устанавливает следующие правила поведения объекта/группы:
 - в *Режиме администратора* — объект/группа отображается в *Дереве объектов SecurOS*. Настройка объекта разрешена (кнопка **Настроить** на *Панели инструментов* разблокирована). Прочие операции с объектом/группой запрещены (прочие кнопки управления на *Панели инструментов* заблокированы);
 - в *Режиме оператора* — аналогично уровню доступа **управление**.
-  — **полный доступ**. Устанавливает следующие правила поведения объекта:

- в *Режиме администратора* — объект/группа отображается в *Дереве объектов SecurOS*. Настройка объекта и прочие операции с объектом/группой разрешены (все кнопки управления на *Панели инструментов* разблокированы);
- в *Режиме оператора* — аналогично уровню доступа **управление**.
-  — **наследуемые права** — права для этого объекта/группы наследуются от его родительского объекта. При создании нового объекта этот уровень доступа устанавливается по умолчанию.

7.3.7.1 Двухфакторная аутентификация в SecurOS

Внимание!

1. Для пользователей сетевого домена Active Directory/LDAP (см. **Провайдеры**) и суперпользователя SecurOS (см. **Пользователи в SecurOS**) двухфакторная аутентификация невозможна.
2. Двухфакторная аутентификация возможна для тех пользователей SecurOS, для которых включен режим автоматической авторизации (см. **Автоматическая авторизация**).
3. Опция двухфакторной аутентификации применима только к клиентам SecurOS. На процедуру авторизации в прочих Модулях системы (например, SecurOS WebConnect и пр.) не влияет.

В режиме двухфакторной аутентификации доступ к SecurOS предоставляется в два этапа:

1. Проверка логина и пароля, введенных пользователем в обычном окне авторизации (см. **Запуск SecurOS на Сервере конфигураций** и **Запуск SecurOS на Рабочем месте оператора**). Если введенные логин и пароль зарегистрированы в SecurOS, система отправит запрос на получение одноразового кода доступа. Одноразовый код доступа будет выслан на адрес электронной почты текущего пользователя с помощью заранее настроенного **Сервиса почтовых сообщений**.
2. Если проблемы функционирования SMTP-сервера отсутствуют и настройки объекта **Сервис почтовых сообщений** корректны (см. **Возможные ошибки**), система выведет окно для ввода одноразового кода доступа (см. рис. 107).

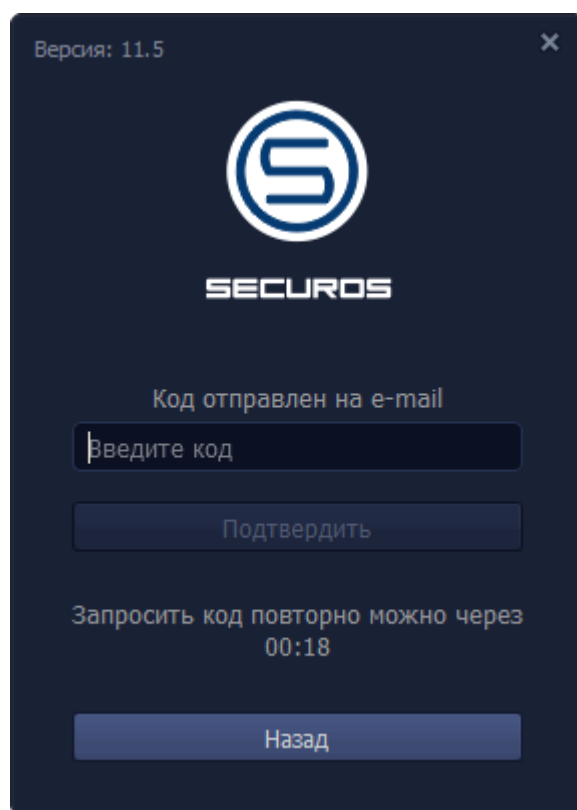


Рис. 107. Окно для ввода одноразового кода доступа

Внимание! Одноразовый код доступа валиден в течение 2-х минут после его получения.

Введите полученный код в окно подтверждения и нажмите кнопку **Подтвердить**. Если введен корректный код, будет выполнен вход в систему.

Если введен некорректный код доступа или время его действия истекло, система выведет окно с соответствующим сообщением (см. рис. 108).

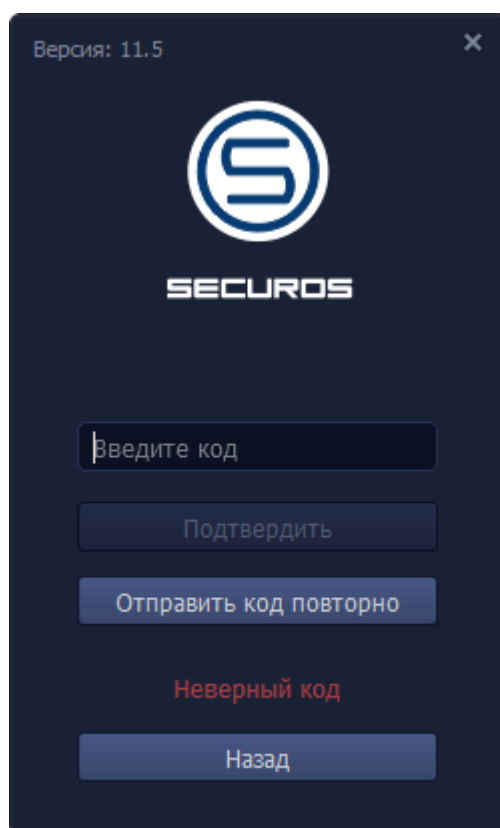


Рис. 108. Окно с сообщением о некорректном коде доступа

Нажмите кнопку **Отправить код повторно**, получите и введите полученный одноразовый код доступа.

При работе с одноразовыми кодами доступа существуют следующие ограничения:

- Запрос на повторную отправку кода доступа может быть отправлен не ранее, чем через 30 секунд после отправки предыдущего запроса (по таймеру в окне подтверждения).
- Количество попыток запроса кода доступа равно 10. Если все 10 попыток исчерпаны, нажмите кнопку **Назад** для повторной авторизации.
- Количество попыток ввода кода доступа равно 10. Если все 10 попыток исчерпаны, нажмите кнопку **Назад** для повторной авторизации.

Возможные ошибки

При возникновении проблем функционирования используемого SMTP-сервера или некорректных настройках объекта **Сервис почтовых сообщений**, система выведет окно с сообщением об ошибке (см. рис. 109).

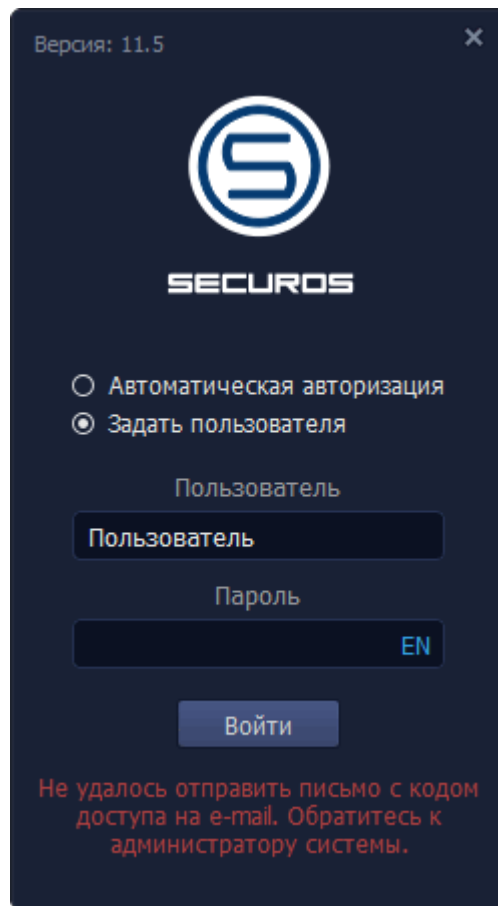


Рис. 109. Окно с сообщением об ошибке

7.3.8 Компьютер

Объект представляет определенный компьютер сети SecurOS — *Видеосервер* или *Рабочее место оператора*.

Видеосервера и *Рабочие места оператора* сети SecurOS регистрируются и отображаются в *Дереве объектов* как объекты *Компьютер*. На *Видеосерверах* запускается серверная часть SecurOS, на *Рабочих местах оператора* — клиентская. Клиентская часть также может быть запущена и на *Видеосервере*.

Видеосервера SecurOS могут посылать и принимать события от других *Видеосерверов*. Чтобы снизить нагрузку на сеть, связанную с передачей событий, избранные сервера сети можно исключить из списка рассылки событий (см. раздел [Закладка Серверы для подключения](#)).

Для обозначения роли и состояния *Компьютера* в сети SecurOS используются следующие значки *Дерева объектов* (см. рис. 110):

-  — *Сервер конфигураций* (роль компьютера *Видеосервер*);
-  — произвольный *Видеосервер*, настроенный и подключенный к сети SecurOS;
-  — произвольный *Видеосервер*, отключенный от сети SecurOS;
-  — *Нода кластера* (см. [Резервирование](#));
-  — произвольное *Рабочее место оператора* или *Профиль Рабочего места оператора* (подключение к сети SecurOS не контролируется).

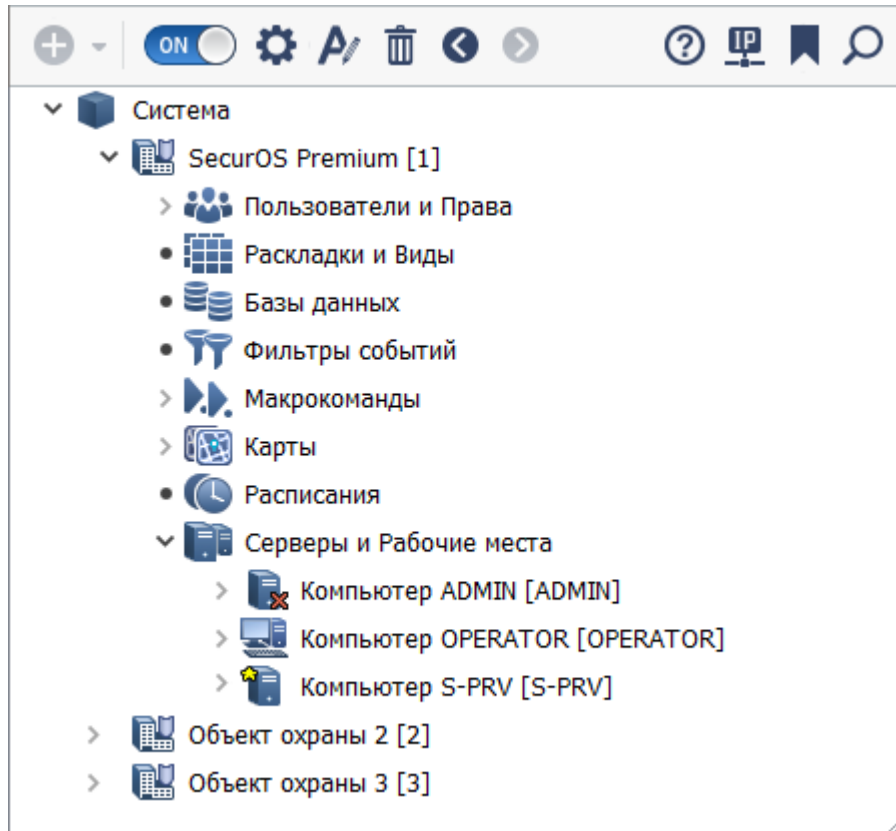


Рис. 110. Компьютеры и их состояния в Дереве объектов SecurOS

Родительский объект — *Объект охраны\группа Серверы и Рабочие места*.

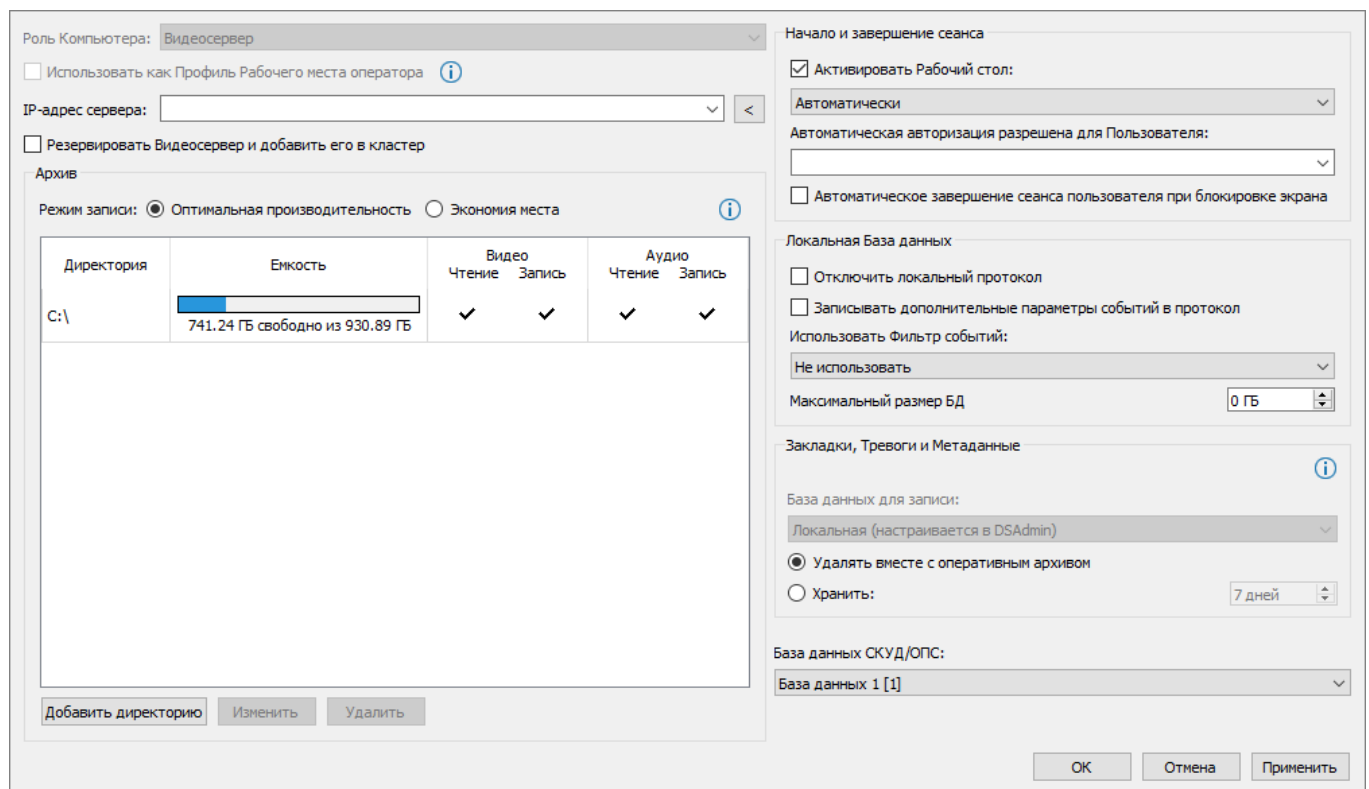


Рис. 111. Окно настройки параметров объекта Компьютер

Таблица 13. Параметры объекта Компьютер

Параметр	Описание
Роль Компьютера	Функциональный тип, который соответствует роли данного компьютера в сети. Указывается при создании объекта и не может быть изменен в дальнейшем. Возможные значения: - Рабочее место оператора — компьютер функционирует как клиент сети (даже если SecurOS установлен в другом варианте) или в качестве <i>Профиля Рабочего места оператора</i> (см. Профили Рабочих мест оператора). - Видеосервер — компьютер функционирует как сервер.
Использовать как Профиль Рабочего места оператора	Активируйте это поле, чтобы использовать объект в качестве <i>Профиля Рабочего места оператора</i> (см. Профили Рабочих мест оператора).
IP-адрес сервера	Укажите IP-адрес данного компьютера в сети TCP/IP. Используйте кнопку [<] справа от данного поля для автоматического определения IP-адреса или выберите значение из списка. Внимание! Если компьютеры находятся в различных подсетях, автоматическое определение IP-адреса невозможно. В данном случае адрес компьютера является обязательным, значение необходимо задать в ручном режиме.
Резервировать Видеосервер и добавить его в кластер	Если выбрано, объект <i>Компьютер</i> будет представлять не физический сервер, а логическую сущность — <i>Ноду</i> кластера (см. Резервирование).
Блок Архив (доступен только для <i>Компьютера</i> с ролью <i>Видеосервер</i> , см. раздел Архив).	
Начало и завершение сеанса (настройки, применяемые автоматически при запуске системы)	
Активировать Рабочий стол	Активируйте это поле, чтобы выбрать из списка объект <i>Рабочий стол</i> , который будет отображаться при запуске SecurOS на данном компьютере. При выборе значения Автоматически отобразится первый рабочий стол из списка конфигурации (с минимальным идентификационным номером). Если поле не активировано, при запуске не отобразится ни один рабочий стол.

Параметр	Описание
Автоматическая авторизация разрешена для Пользователя	Опция доступна только для компьютеров с ролью <i>Видеосервер</i> и <i>Рабочее место оператора</i>, не являющихся <i>Профилями Рабочего места оператора</i>. Выберите из списка имя зарегистрированного в системе пользователя или группы пользователей, вход которых в систему будет возможен автоматически (т.е. без задания имени пользователя и пароля в окне Авторизация). Задание значения возможно только в случае авторизации в системе с правами учетной записи суперпользователя (см. Пользователи в SecurOS). Задать значение root в поле невозможно. Примечание. Детальная информация о порядке настройки и правилах процедуры приведена в разделе Автоматическая авторизация. Группа пользователей может быть указана в случае, если в системе настроен объект Active Directory / LDAP. Имя группы указывается с префиксом @, например, @usergroup.
Автоматическое завершение сеанса пользователя при блокировке экрана	Примечание. Параметр доступен для <i>Компьютера</i> с любой ролью. В ОС Linux функциональность не поддерживается. Активируйте это поле, чтобы в момент автоматической или ручной блокировки рабочего стола происходило автоматическое завершение сеанса текущего пользователя в <i>Интерфейсе оператора</i>. Примечание. Автоматическое завершение сеанса не будет осуществляться, если в параметре Автоматическая авторизация разрешена для Пользователя указан пользователь или группа пользователей (при настроенном в системе объекте Active Directory / LDAP), и в данный момент выполнен вход под этим пользователем или группой пользователей.
Локальная база данных	
Внимание! Для Роли Компьютера <i>Рабочее место оператора</i> параметры недоступны.	
Отключить локальный протокол	Активируйте это поле для отмены сохранения текущей копии протокола событий в базе данных. Поскольку протокол синхронизирован между компьютерами и по умолчанию каждый компьютер сохраняет копию протокола в локальной базе данных, можно отменить сохранение на некоторых компьютерах без риска потери событий.

Параметр	Описание
Записывать дополнительные параметры событий в протокол	Активируйте это поле, чтобы указать о необходимости записывать параметры событий в базу данных <code>PROTOCOL_PARAMS</code>. Внимание! Данная опция используется при работе с интеллектуальными модулями. В остальных случаях ее использование может привести к снижению производительности системы, поэтому не рекомендуется активировать данное поле.
Использовать события Фильтр	Фильтр событий, который будет использован при записи событий в БД. В список возможных значений входят все объекты Фильтр событий, дочерние текущему <i>Объекту охраны</i>. Необязательный параметр. Если значение не задано, в БД будут сохраняться все системные события, если задано — только те события, которые разрешены выбранным фильтром. Внимание! Использование фильтра событий может привести к снижению производительности системы.
Максимальный размер БД	Максимальный размер базы данных для записи протокола (в ГБ), при достижении которого начнется обновление базы, при котором более старые данные будут замещаться вновь поступающими. Возможные значения: [0; 100]. Значение по умолчанию — 0 (параметр не используется).
Закладки, Тревоги и Метаданные	
Внимание! Для Роли Компьютера <i>Рабочее место оператора</i> параметры недоступны.	
В блоке задаются параметры хранения <i>Закладок, Тревог и Метаданных</i> (см. Ретроспективный поиск) в базе данных видеоподсистемы.	
База данных для записи	Выберите из списка базу данных видеоархива SecurOS (<code>fsindex</code>), которая будет использоваться для хранения <i>Закладок, Тревог и Метаданных</i>. Примечание. Параметр доступен только для <i>Ноды</i> в кластере (см. Структура кластера).
Удалять вместе с оперативным архивом	При выборе данной опции <i>Закладки, Тревоги и Метаданные</i> будут удаляться из базы данных одновременно с оперативным архивом.
Хранить	При выборе данной опции задайте длительность периода хранения закладок, тревог и метаданных в базе данных, в сутках. Для закладки отсчитывается от времени начала действия закладки, для тревоги — от времени начала тревоги. Проверка срока действия интервала выполняется каждый час или при старте SecurOS. Возможные значения: [1; 3660]. Значение по умолчанию — 7. Примечание. Максимальный срок хранения метаданных — 365 дней.

Параметр	Описание
База данных СКУД/ОПС	Выберите из списка <i>Базу данных</i> , созданную ранее для работы с Модулем СКУД/ОПС (подробнее см. Руководство пользователя SecurOS СКУД/ОПС).

7.3.8.1 Архив

Примечание. За дополнительной информацией по записи архива обращайтесь в раздел [Запись архива на диск](#).

В блоке задаются директории (носители) для работы с архивами SecurOS. Для каждой директории определяется список доступных операций.

Внешний вид блока представлен на рис. 112.

Архив

Режим записи: ☒ Оптимальная производительность ☐ Экономия места

Директория	Емкость	Видео		Аудио	
		Чтение	Запись	Чтение	Запись
D:\	460.2 ГБ свободно из 931.39 ГБ	✓	✓	✓	✓
M:\	26.89 ГБ свободно из 368.1 ГБ	✓	✓	✓	✓
S:\	25.5 ГБ свободно из 368.1 ГБ	✓	✓	✓	✓
\\s-p...HIVE\		✓	✓		

Добавить директорию Изменить Удалить

Рис. 112. Закладка Архив

В блоке доступны следующие операции:

1. **Выбор режима записи архива** — выбрать режим записи *Оперативного архива*.
2. **Добавление директории** — добавить новую директорию для работы с архивами и задать список возможных операций.
3. **Изменение директории** — изменить список возможных операций с архивом для текущей директории.
4. **Удаление директории** — удалить текущую директорию из списка.

Выбор режима записи архива

Оперативный архив может записываться в одном из двух режимов: с оптимальной производительностью или с экономией места на диске. Чтобы установить режим записи архива выберите требуемый вариант:

- **Оптимальная производительность** — позволяет увеличить скорость записи архива на диск благодаря снижению фрагментации файлов архива. Эффективность механизма зависит от объема свободного места на диске.

Примечание. Intelligent Security Systems рекомендует значение 10%. Это же значение рекомендует Microsoft Corporation для разделов NTFS. Изменить объем свободного места можно в настройках объекта **Компьютер**.

Режим рекомендуется использовать в случае записи длительных по времени фрагментов (например, при постоянной записи архива). Если архив записывается небольшими по времени фрагментами, то при использовании данного режима сократится время хранения архива и потребуется больше места на диске.

- **Экономия места** — позволяет эффективнее использовать дисковое пространство, но может привести к снижению скорости записи на диск. Рекомендуется использовать в случае, если архив записывается небольшими по времени фрагментами (например, по командам интеллектуальных Модулей).

Добавление директории

Директория для работы с архивом может быть представлена одним из следующих объектов:

- локальный жесткий диск;
- съемный накопитель;
- сетевой диск;
- сетевая папка.

Внимание! В ОС Linux возможна работа со следующими файловыми системами: ext3, ext4, cifs.

Для добавления новой директории выполните следующие действия:

1. Нажмите кнопку **Добавить директорию**.
2. В окне **Добавить новую директорию** (см. рис. 113) задайте следующие параметры:

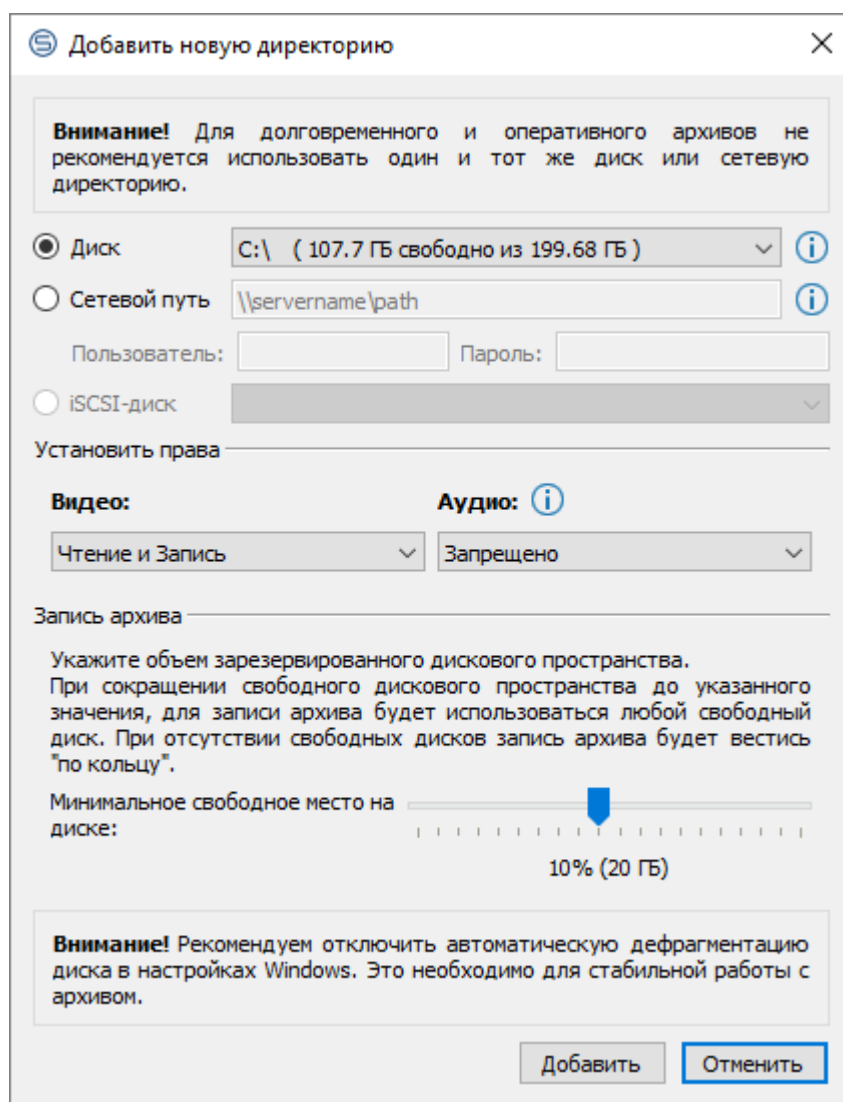


Рис. 113. Окно Добавить новую директорию

- Выберите опцию, соответствующую подключаемому носителю:

– **Диск** — с помощью данной опции подключается жесткий диск, съемный накопитель или сетевой диск.

Примечания:

1. Добавление локальных жестких дисков на *Хостах* кластера описано в разделе **Хранение видеоархива на локальных дисках Хостов**.
2. Добавление локальных жестких дисков в ОС Linux описано в разделе **Разметка и монтирование локальных дисков в ОС Linux**.
3. Для опции **Диск** некоторые сетевые диски могут отсутствовать в списке. Для подключения сетевого диска рекомендуется использовать опцию **Сетевой путь** (только для ОС Windows).
4. Для монтирования сетевого диска в ОС Linux используйте команду `sudo mount -v -t cifs с параметром actimeo=0 и опцией nobr`.

– **Сетевой путь** — с помощью данной опции подключается сетевая папка.

Примечание. Использование сетевой папки для записи архива возможно только если *Видеосервер* или *Нода* работает под управлением ОС Windows.

При необходимости задайте имя пользователя и пароль доступа к подключаемой сетевой папке.

Внимание! Одну и ту же **Директорию** для записи *Оперативного* и *Долговременного* архивов (см. [Архиватор](#)) использовать не рекомендуется.

Примечание. Если настройка выполняется для локального компьютера, в списке **Диск** отображаются буквенные обозначения доступных дисков данного компьютера. Если выполняется настройка удаленного компьютера, система выводит все буквенные обозначения дисков в алфавитном порядке.

- В блоках **Видео** и **Аудио** выберите из списка операции, которые могут быть выполнены с архивом на данном носителе:
 - Запрещено — *Видеосерверу* запрещены чтение/запись архива.
 - Чтение — *Видеосерверу* разрешено чтение архива.
 - Чтение и Запись — *Видеосерверу* разрешены чтение и запись архива.

Примечания:

1. Для сетевых папок операции с аудиоархивами недоступны.
2. В блоке **Видео** указываются права на выполнение операций с видео и соответствующим ему аудиосопровождением. В блоке **Аудио** — на выполнение операций с аудио, не привязанному к какому-либо видео.

- В блоке **Запись архива** проверьте и, при необходимости, скорректируйте значение параметра **Минимальное свободное место на диске**.

Примечания:

1. Значение параметра вычисляется и устанавливается автоматически при добавлении директории.
2. Рекомендуется выделять не менее 10% от общего объема диска. Данное значение позволяет максимально эффективно записывать архив в режиме **Оптимальная производительность**, (см. [Выбор режима записи архива](#)).

3. Нажмите кнопку **Добавить**. Выбранный носитель будет добавлен в список директорий. Операции, разрешенные для данной директории, будут отмечены символом ✓.

Внимание! На всех жестких дисках, выбранных для работы с архивом, необходимо отключить автоматическую дефрагментацию по расписанию (например, для Windows 10, **Панель управления** → **Администрирование**, подраздел **Оптимизация дисков**).

Изменение директории

Для изменения списка операций, доступных для директории, выполните следующие действия:

1. Выделите требуемую директорию и нажмите кнопку **Изменить**.
2. В окне **Изменить текущую директорию** (см. рис. 114) выберите новые значения в блоках **Видео** и **Аудио**.

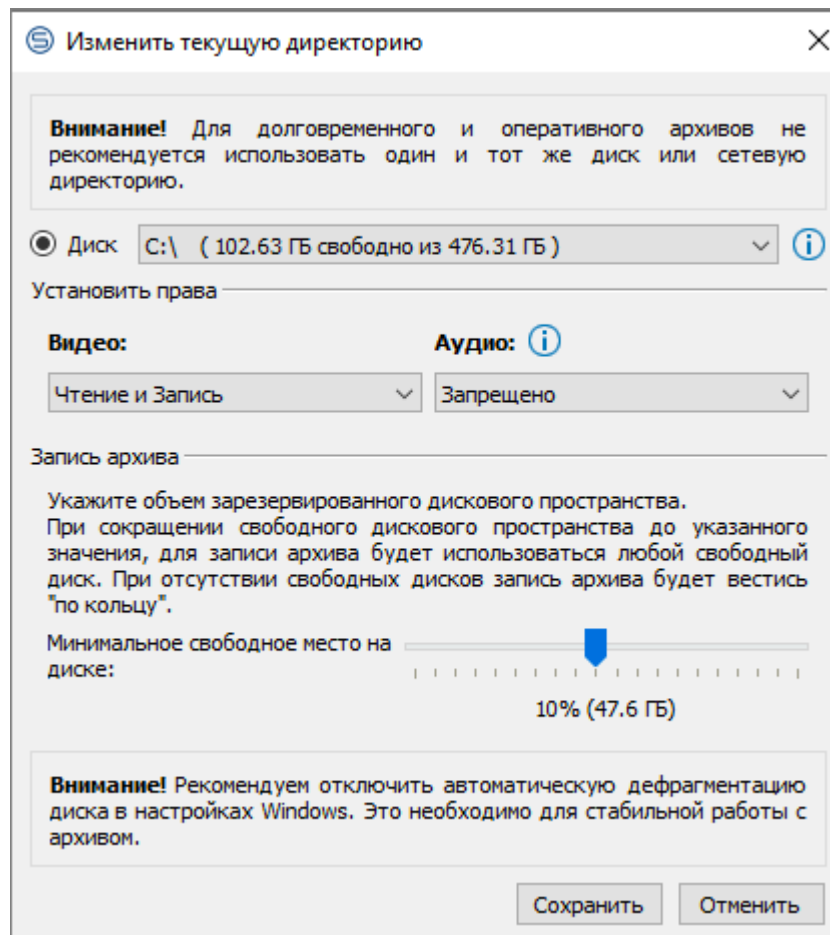


Рис. 114. Окно Изменить текущую директорию

3. Нажмите кнопку **Сохранить**.

Удаление директории

Для удаления директории выберите подключенный носитель из списка, нажмите кнопку **Удалить**. Для подтверждения удаления нажмите кнопку **Да** на панели сообщения (см. рис. 115).

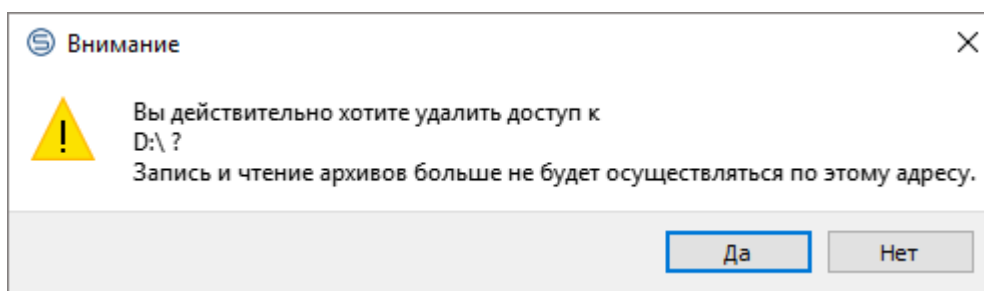


Рис. 115. Подтверждение удаления директории

7.3.8.2 Автоматическая авторизация

Автоматическая авторизация в системе возможна как для *Пользователей SecurOS*, так и для пользователей ОС Windows или Linux, зарегистрированных в домене Active Directory Windows. При совпадении учетных данных предпочтение отдается пользователям SecurOS.

Параметр **Автоматическая авторизация разрешена для Пользователя** может принимать следующие значения:

- Имя любого пользователя, зарегистрированного в текущем *Объекте охраны* сети SecurOS (*Дерево объектов* → *группа Пользователи и Права* → *Отдел* → *Пользователь*), кроме суперпользователя (см. [Пользователи в SecurOS](#)).
- Имя группы пользователей, зарегистрированной в домене Active Directory ОС. При данном значении автоматическая авторизация возможна для любого пользователя, входящего в указанную группу.
- Имя пользователя, зарегистрированного в домене Active Directory ОС. При данном значении автоматическая авторизация возможна только для указанного пользователя.

Внимание! Домен Active Directory может использоваться для аутентификации только в том случае, если в SecurOS зарегистрирован объект *Active Directory / LDAP*, который выбран в качестве провайдера объекта *Права пользователей* (см. раздел [Active Directory / LDAP](#)).

- "Не задано" (значение по умолчанию). При данном значении параметра автоматическая авторизация возможна для любого пользователя домена либо пользователя, входящего в любую группу домена Active Directory ОС, имеющих права, заданные в объекте *Права пользователя*.

7.3.9 Водяной знак

Объект предназначен для отображения водяных знаков, выводимых поверх *Рабочей области Медиа Клиента* (см. [Наложение водяных знаков](#)) и настройки их внешнего вида.

Родительский объект — *Объект охраны\группа Водяные знаки*.

Примечание. Наличие водяных знаков в *Медиа Клиенте* определяется настройками объекта [Права пользователя](#).

Внешний вид окна настройки параметров объекта представлен на рис. [116](#). В левой части окна находится список параметров (см. Таблицу [14](#)). В правой части окна расположена область предпросмотра.

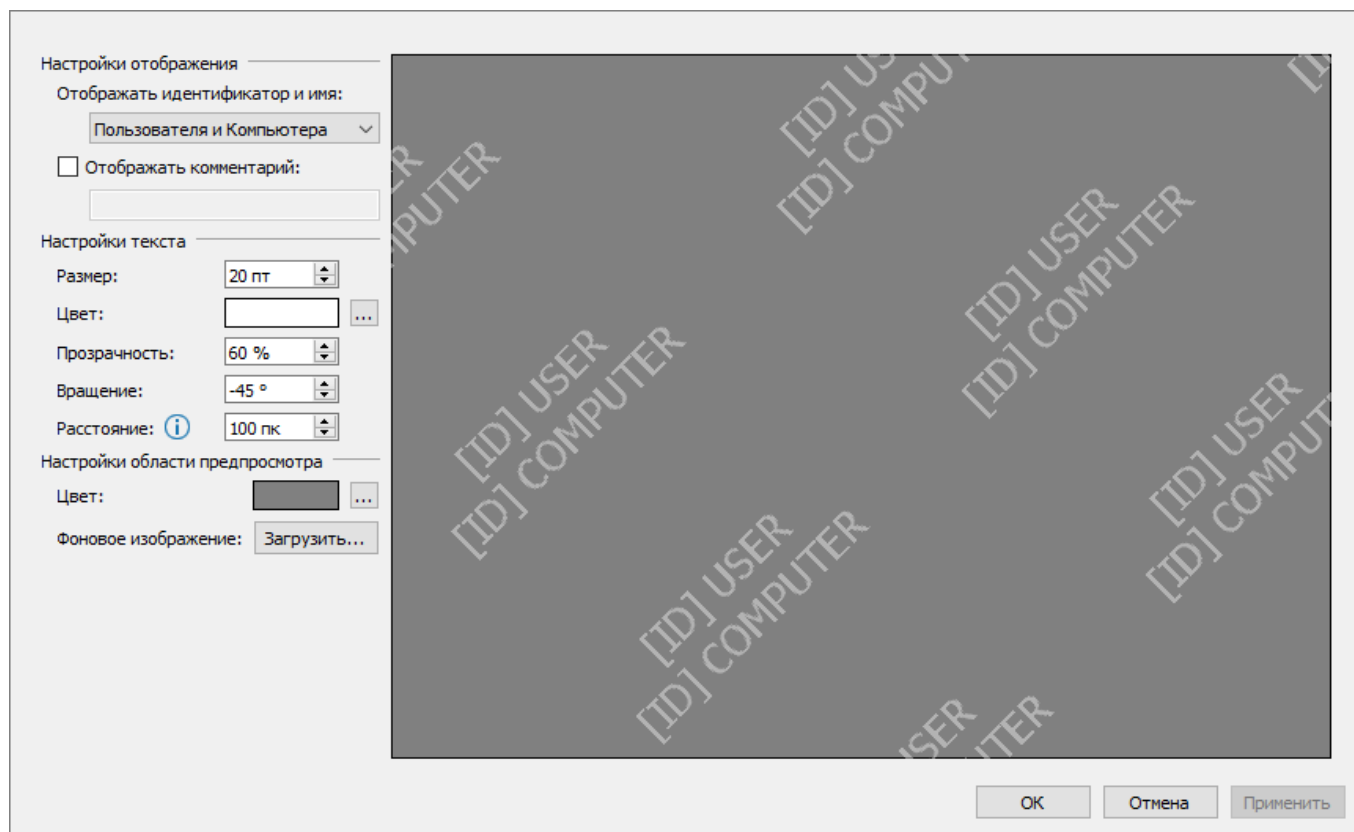


Рис. 116. Окно настройки параметров объекта Водяной знак

Таблица 14. Параметры объекта Водяной знак

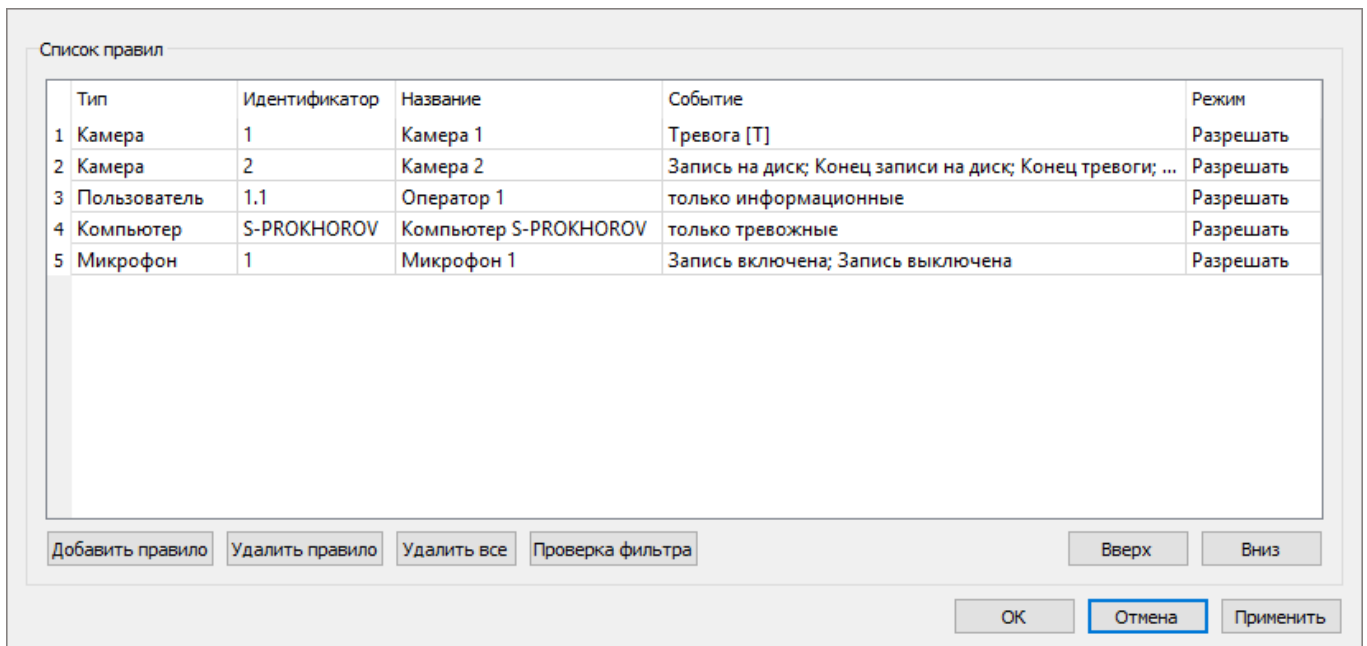
Параметр	Описание
Настройки отображения	
Отображать идентификатор и имя	Параметр определяет какие данные содержат водяные знаки. Возможные значения: - Пользователя и Компьютера (значение по умолчанию) — водяные знаки содержат данные о <i>Пользователе</i> и его <i>Компьютере</i> в формате [<i>ID</i>] Пользователя] <Имя Пользователя> и [<i>ID</i>] Компьютера] <Имя Компьютера> соответственно; - Пользователя — водяные знаки содержат данные только о <i>Пользователе</i> в формате [<i>ID</i>] Пользователя] <Имя Пользователя>; - Компьютера — водяные знаки содержат данные только о <i>Компьютере</i> в формате [<i>ID</i>] Компьютера] <Имя Компьютера>.
Отображать комментарий	Отметьте флажок, чтобы задать произвольный комментарий, который будет отображаться в составе водяного знака. Максимальное количество символов для комментария: 100.
Настройки текста	

Параметр	Описание
Размер	Размер шрифта, задается в пунктах. Значение по умолчанию: 20. Возможные значения: [1; 99].
Цвет	Нажмите на кнопку  , чтобы изменить заданный по умолчанию цвет шрифта.
Прозрачность	Прозрачность текста, задается в процентах. Значение по умолчанию: 60. Возможные значения: [0; 99].
Вращение	Угол наклона блока текста, измеряется в градусах. Значение по умолчанию: -45. Возможные значения: [-90; 90].
Расстояние	Расстояние между блоками текста, измеряется в пикселах. Отсчитывается от наиболее широкой строки. Значение по умолчанию: 100. Возможные значения: [5; 300].
Настройки области предпросмотра	
Цвет	Нажмите на кнопку  , чтобы изменить заданный по умолчанию цвет фона области предпросмотра.
Фоновое изображение	Нажмите на кнопку Загрузить , чтобы выбрать фоновое изображение для области предпросмотра. Возможные форматы файлов: PNG и JPG.

7.3.10 Фильтр событий

Объект предназначен для задания списка правил, которые могут быть использованы для фильтрации событий при выводе в окне **Протокол событий** или при записи журнала событий в базу данных.

Родительский объект — *Объект охраны\группа Фильтры событий*.



Список правил

Тип	Идентификатор	Название	Событие	Режим
1 Камера	1	Камера 1	Тревога [T]	Разрешать
2 Камера	2	Камера 2	Запись на диск; Конец записи на диск; Конец тревоги; ...	Разрешать
3 Пользователь	1.1	Оператор 1	только информационные	Разрешать
4 Компьютер	S-PROKHOROV	Компьютер S-PROKHOROV	только тревожные	Разрешать
5 Микрофон	1	Микрофон 1	Запись включена; Запись выключена	Разрешать

Добавить правило Удалить правило Удалить все Проверка фильтра Вверх Вниз ОК **Отмена** Применить

Рис. 117. Окно настройки параметров объекта Фильтр событий

Таблица 15. Параметры объекта Фильтр событий

Параметр	Описание
Список правил	
Тип	Тип системного объекта-источника события. Выберите вариант Все, чтобы учесть все возможные объекты.
Идентификатор	Идентификатор системного объекта-источника заданного типа. Оставьте список без отметок, чтобы учесть все объекты выбранного типа.
Название	<i>Информационное поле:</i> название объекта (значение поля выводится автоматически при выборе типа объекта и его идентификатора). Оставьте список без отметок, чтобы учесть все объекты выбранного типа.
Событие	Событие объекта. Список событий зависит от типа объекта. Примечания: Кроме единичных событий, списка событий или всех событий объекта в правиле может быть задана одна из следующих предопределенных групп событий: 1. Только тревожные события. 2. Только информационные события. 3. Тревожные и информационные события. • Для создания правила фильтрации одного или нескольких событий объекта отметьте флажки этих событий в списке возможных событий объекта (см. рис. 118). • Для создания правила фильтрации событий предопределенной группы отметьте флажок одной из таких групп, расположенных в верхней секции списка. • Выберите вариант Все, чтобы учесть все события объектов выбранного типа.
Режим	Результат действия правила. Может принимать следующие значения: • Запрещать — в результате применения фильтра событие будет отброшено (не будет выведено в окне Протокол событий/записано в БД). • Разрешать — в результате применения фильтра событие будет записано в протокол (выведено в окне Протокол событий/записано в БД).
Кнопки	
Добавить правило	Добавление нового правила в список правил.
Удалить правило	Удаление текущего правила из списка правил.
Удалить все	Удаление всех правил из списка.

Параметр	Описание
Проверка фильтра	Проверка нахождения правила в списке правил фильтра. Описание процедуры проверки приведено ниже.
Вверх	Кнопка ручной сортировки списка правил. Перемещение правила на одну позицию вверх.
Вниз	Кнопка ручной сортировки списка правил. Перемещение правила на одну позицию вниз.

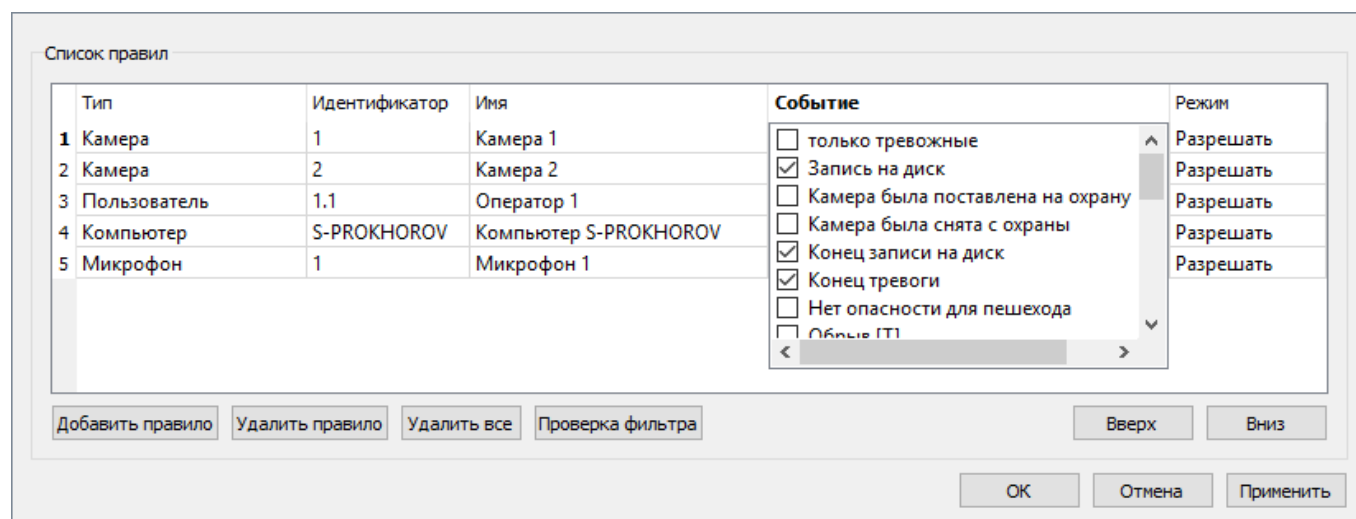


Рис. 118. Выбор множества событий для объекта

Для проверки результата обработки события, установленного правилом фильтрации, выполните следующие действия:

1. В блоке окна настройки параметров фильтра событий (см. рис. 118) нажмите кнопку **Проверка фильтра**.
2. В окне настройки параметров объекта система выведет новый блок - **События для проверки** (см. рис. 119).

Список правил

Тип	Идентификатор	Название	Событие	Режим
1 Камера	1	Камера 1	Тревога [T]	Разрешать
2 Камера	2	Камера 2	Запись на диск; Конец записи на диск; Конец тревоги; ...	Разрешать
3 Пользователь	1.1	Оператор 1	только информационные	Разрешать
4 Компьютер	S-PROKHOROV	Компьютер S-PROKHOROV	только тревожные	Разрешать
5 Микрофон	1	Микрофон 1	Запись включена; Запись выключена	Разрешать

Добавить правило Удалить правило Удалить все Скрыть проверку Вверх Вниз

События для проверки

Тип	Идентификатор	Название	Событие	Правило
1 Зона	1.0	Main_1	Конец тревоги	Нет правила фильтрации, событие запрещено
2 Камера	1	Камера 1	Тревога [T]	Событие разрешено правилом 1.

Добавить событие Удалить событие Удалить все Выполнить проверку

OK Отмена Применить

Рис. 119. Блок Событие для проверки

- В блоке **События для проверки** щелкните кнопку **Добавить событие**. Задайте событие, для которого необходимо проверить результат обработки.

Примечание. Параметры блока **События для проверки** аналогичны параметрам блока **Список правил**.

- Нажмите кнопку **Выполнить проверку**. Система выведет результат в поле **Правило**:
 - Нет правила фильтрации** – правило фильтрации заданного события отсутствует в списке правил фильтра;
 - Событие разрешено правилом N** – заданное событие разрешено правилом N;
 - Событие запрещено правилом N** – заданное событие запрещено правилом N.

Примечание. N - порядковый номер правила в списке правил фильтра.

- Для очистки списка используйте кнопки **Удалить событие/Удалить все**. Для скрытия блока **События для проверки** нажмите кнопку **Скрыть проверку**.
- Для сохранения/отмены изменений и выхода из режима администрирования нажмите кнопку **OK/Отмена**.

Фильтрация событий выполняется в соответствии со следующим алгоритмом:

- Правила применяются к событиям последовательно, в порядке перечисления в списке.
- Выполняется первое из найденных правил, соответствующих данному событию.
- Если событие явно не разрешено ни одним из правил, оно будет отброшено.

7.3.11 Сценарий поведения

Объект предназначен для загрузки сценариев поведения и для их дальнейшего применения в модулях SecurOS, использующих экспертную систему. В сценариях поведения описываются определенные правила, согласно которым экспертная система обнаруживает инциденты и генерирует события, которые могут быть отображены в *Протоколе событий*.

Родительский объект — *Объект охраны\группа Сценарии поведения*.

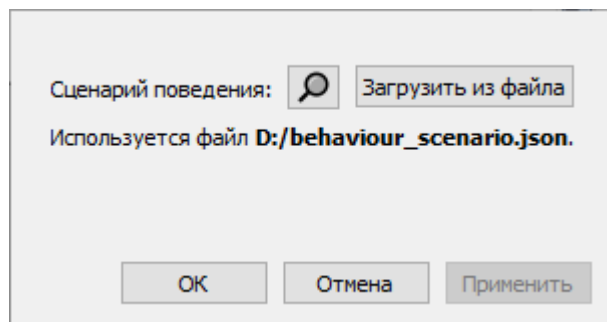


Рис. 120. Окно настройки параметров объекта Сценарий поведения

Таблица 16. Параметры объекта Сценарий поведения

Параметр	Описание
Просмотр текста сценария  (кнопка)	Открыть окно просмотра загруженного сценария поведения. Примечание. Кнопка становится активна только при загруженном сценарии.
Загрузить из файла (кнопка)	Нажмите кнопку, чтобы выбрать файл сценария в формате JSON с помощью файлового менеджера. Файл содержит набор правил для экспертной системы. Для получения сценария поведения обратитесь в Службу технической поддержки Intelligent Security Systems.

После загрузки файла сценария, объект может быть выбран в окнах настройки параметров модулей, использующих экспертную систему.

7.3.12 SNMP агент

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

В ОС **Linux** функциональность не поддерживается.

Объект предназначен для отправки событий от камер системы, а также передачи состояний камер заданным компьютерам в виде SNMP трапов. Трапы для следующих событий передаются в автоматическом режиме сразу после их возникновения в системе:

- Камера: изменила состояние;
- Камера: сфокусировалась;
- Камера: расфокусировалась;

- Камера: хорошая видимость;
- Камера: плохая видимость;
- Камера: подключение;
- Камера: обрыв.

При изменении состояний камер пересылаются их текущие состояния. Полученные трапы обрабатываются с помощью SNMP Manager'a.

Для получения таблицы *Камер* и их состояний загрузите в SNMP Manager MIB-файл SecurOS ISS-SECUIROS-MIB, расположенный по адресу <Директория_установки_SecurOS>\MIB.

Использование объекта возможно, если на компьютере установлен компонент **Management and Monitoring Tools** (см. раздел **Настройка средств управления и мониторинга Windows**).

Родительский объект — *Компьютер\группа Оповещения*.

Параметры для редактирования отсутствуют.

Примечание. В дереве объектов локального компьютера допускается наличие только одного объекта *SNMP агент*. Если объект создан, команда **Создать → SNMP агент** недоступна.

7.3.12.1 Настройка средств управления и мониторинга Windows

Для настройки отправки SNMP трапов выполните следующие действия:

1. Установите компоненты **SNMP-протокол** и **Поставщик WMI для SNMP**:
 - Запустите консольное приложение **PowerShell** от имени администратора.
 - Последовательно выполните команды:
`Add-WindowsCapability -Online -Name "SNMP.Client~~~~0.0.1.0"`
`Add-WindowsCapability -Online -Name "WMI-SNMP-Provider.Client~~~~0.0.1.0"`
2. Запустите оснастку **Службы** (**Панель управления → Администрирование → Службы**) и откройте свойства службы SNMP (**SNMP Service**).
3. На вкладке **Общие** выберите **Тип запуска: Автоматически**.
4. На вкладке **Ловушки** (см. рис. 121) задайте параметры **Имя сообщества** и **Адреса назначения ловушки**.

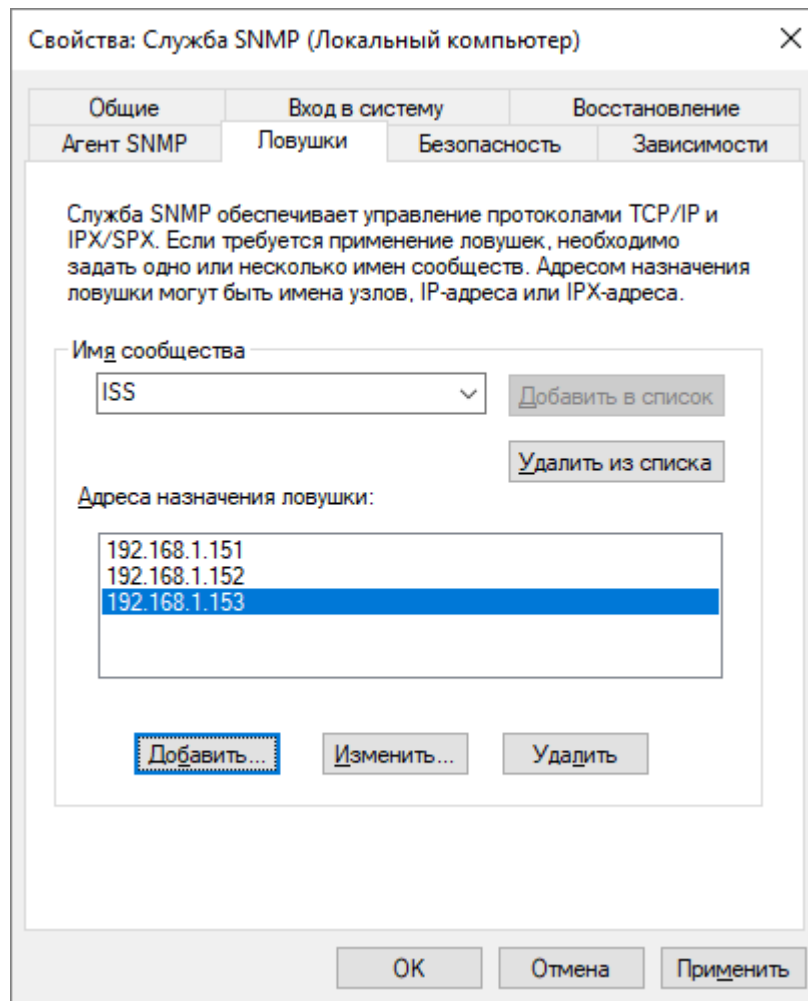


Рис. 121. Закладка Ловушки окна настроек службы SNMP Service

5. Перейдите на вкладку **Безопасность** (см. рис. 122).

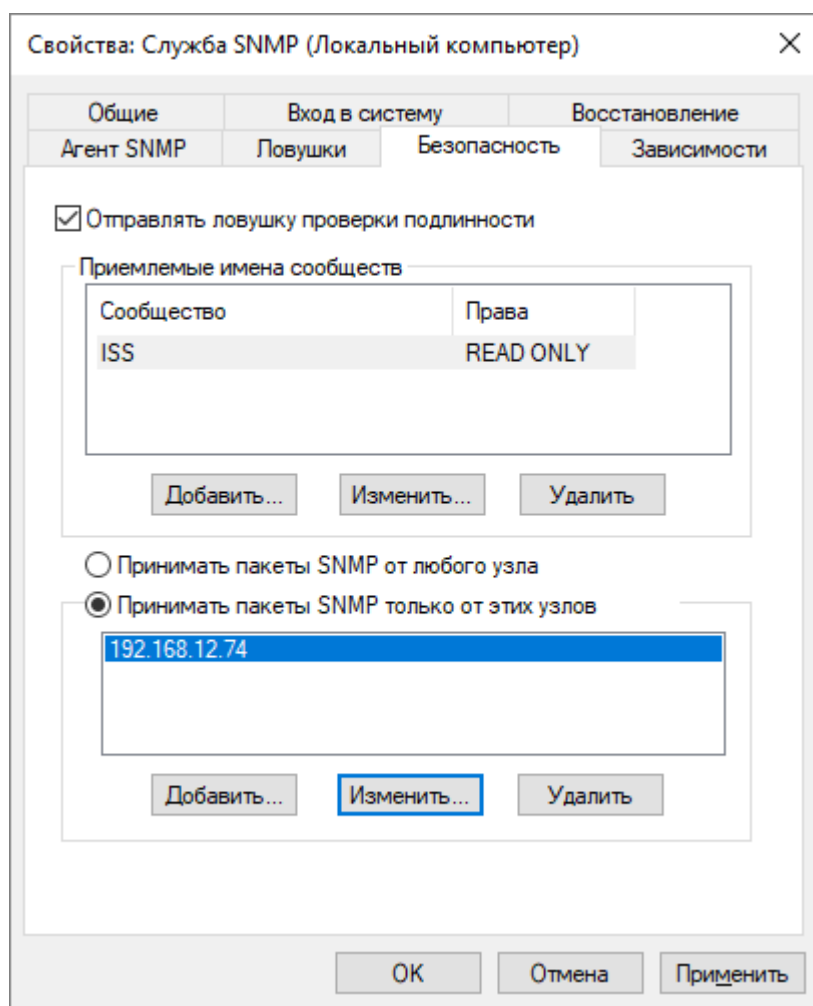


Рис. 122. Закладка Безопасность окна настроек службы SNMP Service

В блоке **Приемлемые имена** сообществ добавьте SNMP-сообщество, с которым может взаимодействовать локальный компьютер. Для добавляемого сообщества задайте следующие параметры:

- **Сообщество** — укажите имя сообщества, допустимое в сети SecurOS, например, ISS;

Примечание. В общем случае имя сообщества может быть произвольным, включая имя по умолчанию public.

- **Права** — назначьте компьютерам добавленного сообщества любые права, включающие возможность чтения MIB-файла с локального компьютера, например, READ ONLY.

Если выбрана опция **Принимать пакеты SNMP только от этих узлов**, укажите IP-адреса тех компьютеров сети SecurOS, на которых установлен SNMP-менеджер.

6. Примените новые настройки.

7. Создайте в дереве объектов SecurOS объект **SNMP агент**.

После выполнения описанных действий SecurOS будет рассылать трапы по указанным IP-адресам автоматически в режиме реального времени.

7.3.13 Внешнее приложение

Объект используется для автоматического запуска внешнего приложения из SecurOS. Приложение запускается при старте *Видеосервера* SecurOS, а также после создания или включения объекта на *Видеосервере*.

Родительский объект — *Компьютер\группа Интеграция и Автоматизация*.

Рис. 123. Окно настройки параметров объекта Внешнее приложение

Таблица 17. Параметры объекта Внешнее приложение

Параметр	Описание
Приложение	Задайте имя (исполняемый файл) приложения или имя приложения и полный путь к нему. Если задано только имя, возможность запуска приложения определяется настройками ОС на данном компьютере, например, заданными в системной переменной Path. Имя приложения может быть задано как вручную, так и с помощью кнопки Выбрать . Строка может содержать любые символы, допустимые для использования в ОС Windows или Linux.
Параметры	Задайте параметры, которые необходимо передать внешнему приложению при его запуске. Если параметров несколько, они должны перечисляться через пробел, например, 1 2 3. Опциональный параметр. Если не задан, приложение будет запущено без параметров.
Рабочая директория	Задайте или выберите с помощью диспетчера файлов рабочую директорию приложения. Опциональный параметр. Если не задан, рабочей директорией будет считаться корневая директория установки SecurOS.

Внешнее приложение, запускаемое из SecurOS, обладает следующими свойствами:

- Если внешнее приложение имеет графический интерфейс пользователя, оно запускается без загрузки этого графического интерфейса.
- При отключении/удалении объекта *Внешнее приложение* из *Дерева объектов* завершается как запущенное приложение, так и все его дочерние процессы.
- При завершении приложения (завершение с ошибкой или отключение пользователем вручную) приложение перезапускается автоматически.

При запуске/ошибке запуска/остановке внешнего приложения в SecurOS генерируются соответствующие события (см. [Руководство программиста SecurOS](#)).

7.3.14 Database Partitioner

Объект используется для оптимизации (секционирования таблиц) баз данных SecurOS Auto, что позволит ускорить работу с базами данных, содержащими большое количество записей и метаданных (см. [Руководство пользователя SecurOS Auto](#)). Окно настройки параметров объекта *Database Partitioner* представлено на рис. 124.

Родительский объект — [Компьютер](#).

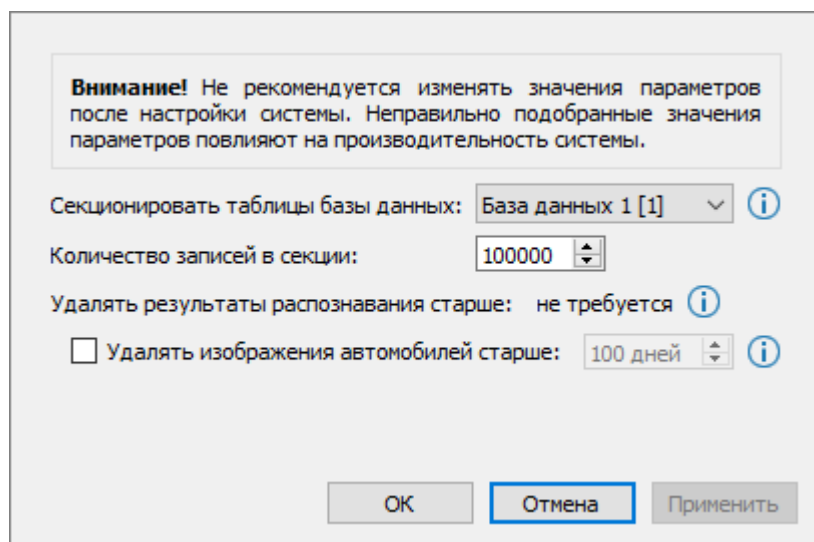


Рис. 124. Окно настройки параметров объекта Database Partitioner

Таблица 18. Параметры объекта Database Partitioner

Параметр	Описание
Секционировать таблицы базы данных	Выберите <i>Базу данных SecurOS Auto</i> для секционирования таблиц.
Количество записей в секции	Задайте требуемое количество записей в секции.
Удалять результаты распознавания старше	Данный параметр отображает срок хранения (количество дней) записей результатов распознавания в выбранной <i>Базе данных</i> (см. База данных). Если хранение бессрочно, удаление не требуется.
Удалять изображения автомобилей старше	Если флажок не отмечен, изображения автомобилей удаляются вместе с записями результатов распознавания. Отметьте флажок, чтобы изображения автомобилей удалялись раньше, чем записи результатов распознавания.

7.3.15 Репликатор баз данных

Объект используется для автоматического копирования содержимого баз данных SecurOS Auto в общую базу данных/кластер баз данных. Общая база данных/кластер баз данных могут быть использованы для поиска и просмотра всех событий SecurOS Auto (см. [Руководство пользователя SecurOS Auto](#)).

После настройки объекта начнется копирование записей выбранных баз данных. Записи копируются, начиная с самых старых. Как только все записи будут скопированы, репликация начнет осуществляться в реальном времени. Все последующие изменения исходных баз данных так же будут отражаться в реплицированной базе/кластере баз данных.

Родительский объект — [Компьютер](#).

Рис. 125. Окно настройки параметров объекта Репликатор баз данных

Таблица 19. Параметры объекта Репликатор баз данных

Параметр	Описание
Базы данных	Выберите одну или несколько исходных баз данных SecurOS Auto, записи которых необходимо реплицировать.
Фильтр	Для поиска объекта по части имени или идентификатора введите в поле требуемые символы; в дереве автоматически отобразятся только те объекты, имя или идентификатор которых соответствуют заданным условиям поиска. Для того, чтобы очистить поле, нажмите кнопку Сбросить фильтр .
Реплицировать в	
базу данных (опция)	Выберите целевую базу данных, в которую будут копироваться записи.

Параметр			Описание
кластер (опция)	баз	данных	Выберите целевой кластер баз данных, в который будут копироваться записи.

8 Подсистема интерфейса

Подсистема интерфейса предоставляет средства оператору средства визуального контроля и управления состоянием системы.

8.1 Описание объектов

Подсистема интерфейса представлена следующими объектами:

- **Рабочий стол.**
- **Карта.**
- **Карта: Интерфейс оператора.**
- **Протокол событий.**
- **Внешнее окно.**
- **HTML5 FrontEnd.**

8.1.1 Рабочий стол

Базовый объект, объединяющий объекты интерфейса пользователя. Предназначен для размещения отдельных компонентов пользовательского интерфейса.

Родительский объект — *Компьютер\группа Рабочие столы.*

Внимание! Все компоненты пользовательского интерфейса отображаются только посредством *Рабочих столов SecurOS.*

Пример. На охраняемой территории находятся две комнаты. В комнате 1 установлена купольная камера и микрофон, в комнате 2 — две видеокамеры. Администратор системы может сконфигурировать два рабочих стола: на первом *Рабочем столе* будет отображен *Медиа Клиент* для просмотра видео с купольной камеры и прослушивания звука. На второй *Рабочий стол* можно поместить *Медиа Клиент* для наблюдения за изображениями с двух видеокамер комнаты 2 и окно *Карта: Интерфейс оператора* для контроля состояний и управления всеми устройствами на охраняемой территории. Если компьютер оборудован несколькими дисплеями, вместо нескольких *Рабочих столов* можно создать один и разместить все необходимые оператору объекты на доступных дисплеях.

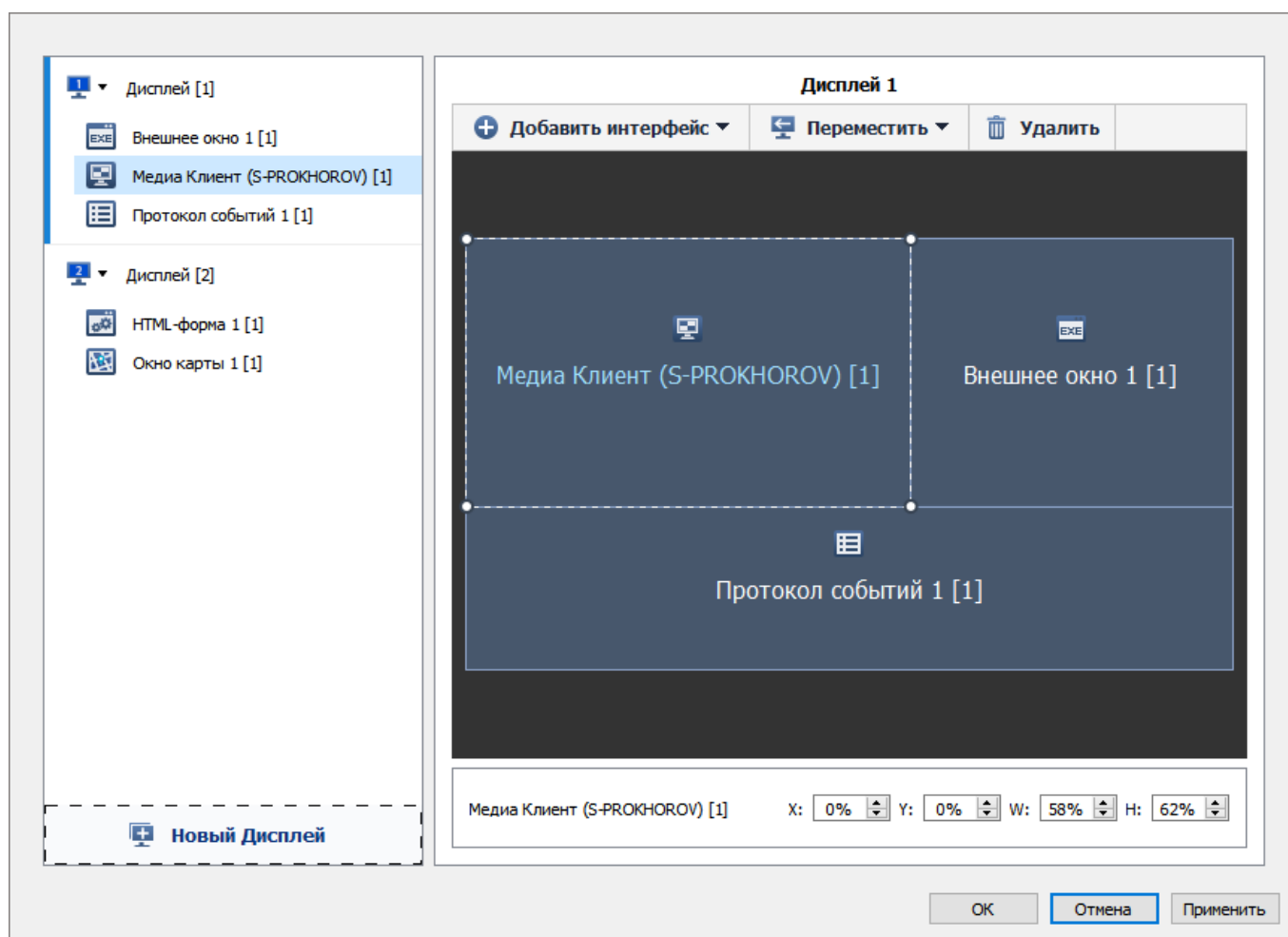


Рис. 126. Окно настройки параметров Рабочего стола

Таблица 20. Параметры объекта Рабочий стол

Параметр	Описание
Дерево объектов Рабочего стола	Располагается в левой части окна. В дереве отображаются все объекты интерфейса оператора, дочерние настраиваемому Рабочему столу. Если компьютер оператора оборудован несколькими дисплеями, эти объекты будут сгруппированы относительно Дисплея, на котором они размещены. Состояния объектов в дереве отображаются аналогично состояниям объектов в Дереве объектов SecurOS (см. Отключение/включение объекта). Внизу дерева расположено поле Новый Дисплей, которое используется для создания дисплея и размещения на нем окна объекта. Примечание. Для каждого объекта дерева доступно контекстное меню (см. Операции настройки Рабочего стола).
Область визуальной настройки	Располагается в правой части окна. Предназначена для задания положения и размеров окон объектов интерфейса оператора в графическом режиме и предпросмотра результата настройки. Содержит кнопки управления окнами интерфейсных объектов.

Блок информации о настраиваемом окне

Располагается под **Областью визуальной настройки**. В блоке отображается название выделенного окна объекта, относительные координаты его расположения и размеры.

8.1.1.1 Операции настройки Рабочего стола

Чтобы разместить окна объектов пользовательского интерфейса SecurOS или интеллектуальных Модулей SecurOS на *Рабочем столе*, необходимо задать относительные координаты расположения и размеры этих окон. Задать указанные параметры и визуально контролировать результат можно непосредственно в настройках объекта *Рабочий стол* (см. рис. 127).

Примечание. Также эти параметры можно задать и в собственных настройках каждого из интерфейсных объектов SecurOS.

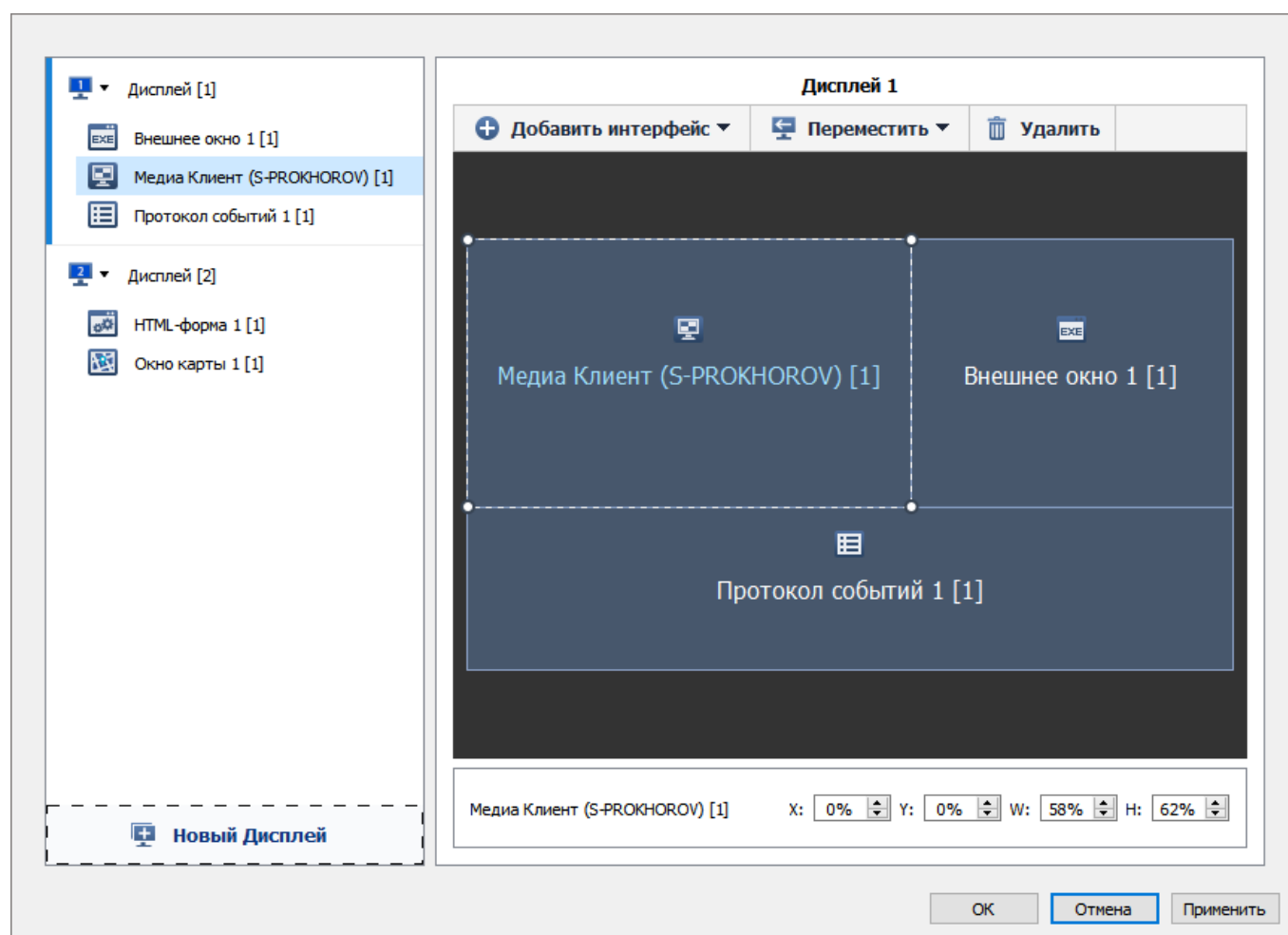


Рис. 127. Окно настройки параметров Рабочего стола

В окне настроек можно выполнять следующие операции:

- **Добавление нового объекта на дисплей.**
- **Изменение размеров и расположения окна объекта.**
- **Создание нового дисплея.**
- **Перемещение окна объекта на выбранный дисплей.**

- **Перемещение всех объектов с одного дисплея на другой.**
- **Удаление дисплея.**
- **Прочие операции с объектом.**

Детали операций с интерфейсными объектами, содержащими несколько окон (например, окно интерфейса оператора Модуля SecurOS Auto) описаны в разделе **Особенности работы с многооконными объектами**.

Добавление нового объекта на дисплей

1. В **Дереве объектов Рабочего стола** выберите объект *Дисплей*, на который необходимо добавить новый интерфейсный объект. При первоначальной настройке *Рабочего стола* в дереве объектов автоматически создается пустой дисплей.
2. В **Области визуальной настройки** нажмите кнопку **Добавить интерфейс**.
3. В выпадающем списке выберите требуемый интерфейсный объект SecurOS. Система выведет окно **Параметры создаваемого объекта** (см. рис. 128).

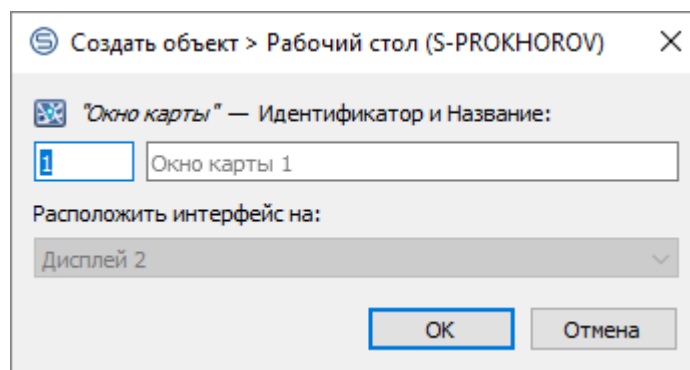


Рис. 128. Окно Параметры создаваемого объекта

4. Задайте необходимые параметры и нажмите кнопку **ОК**. Объект будет создан в *Дереве объектов SecurOS* и добавлен на выбранный дисплей.

Примечание. Операцию также можно выполнить с помощью контекстного меню объекта *Дисплей* в *Дереве объектов Рабочего стола*.

Изменение размеров и расположения окна объекта

1. В **Дереве объектов Рабочего стола** выберите объект, окно которого необходимо настроить. В **Области визуальной настройки** окно этого объекта будет выделено пунктирной линией.
2. Для изменения положения окна перетащите его в требуемом направлении.
3. Для изменения размеров окна наведите указатель мыши на вершину окна или любую из его сторон, далее растяните окно по горизонтали/вертикали.

Создание нового дисплея

Создать новый дисплей можно следующими способами:

- С помощью кнопки **Новый дисплей** в **Дереве объектов Рабочего стола**:
 1. В **Дереве объектов Рабочего стола** нажмите кнопку **Новый Дисплей**. В дереве будет создан новый дисплей, не содержащий объектов.

2. Выполните операцию **Добавление нового объекта на дисплей**, в противном случае созданный пустой дисплей будет удален из **Дерева объектов Рабочего стола**.
- Перетаскиванием объекта с существующего дисплея:
 1. В **Дереве объектов Рабочего стола** выберите объект, окно которого необходимо разместить на новом дисплее. В **Области визуальной настройки Рабочего стола** окно этого объекта будет выделено пунктирной линией.
 2. Перетащите окно из **Дерева объектов Рабочего стола** или из **Области визуальной настройки Рабочего стола** на поле **Новый Дисплей**.
- С помощью кнопки **Переместить** в **Области визуальной настройки Рабочего стола**:
 1. В **Дереве объектов Рабочего стола** выберите объект, окно которого необходимо разместить на новом дисплее. В **Области визуальной настройки Рабочего стола** окно этого объекта будет выделено пунктирной линией.
 2. В **Области визуальной настройки рабочего стола** нажмите кнопку **Переместить**.
 3. В выпадающем списке выберите **Новый Дисплей**.
- С помощью команды **Переместить** контекстного меню объекта:
 1. В **Дереве объектов Рабочего стола** выберите объект, окно которого необходимо разместить на новом дисплее.
 2. В контекстном меню объекта выберите команду **Переместить**.
 3. В выпадающем списке выберите **Новый Дисплей**.

Внимание! Количество подключенных к компьютеру оператора дисплеев автоматически не определяется и должно контролироваться администратором.

Перемещение окна объекта на выбранный дисплей

1. В **Дереве объектов Рабочего стола** выберите объект, окно которого необходимо разместить на другом дисплее. В **Области визуальной настройки** окно этого объекта будет выделено пунктирной линией.
2. Перетащите окно из **Дерева объектов Рабочего стола** или из **Области визуальной настройки** на желаемый дисплей из списка.

Примечание. Выделенное окно также можно переместить с помощью указанных выше способов, см. **Создание нового дисплея**.

Перемещение всех объектов с одного дисплея на другой

1. В **Дереве объектов Рабочего стола** нажмите кнопку  слева от дисплея, все окна которого необходимо переместить на другой дисплей.
2. В выпадающем списке выберите требуемый дисплей.

Удаление дисплея

Для удаления дисплея из **Дерева объектов Рабочего стола** достаточно переместить все расположенные на нем окна объектов на другой дисплей. Дисплей будет удален автоматически при выделении другого дисплея в **Дереве объектов Рабочего стола** или, если дисплей единственный, после применения настроек.

Прочие операции с объектом

Прочие операции выполняются с помощью контекстного меню объекта. Меню доступно как в **Дереве объектов Рабочего стола** так и в **Области визуальной настройки**. В меню доступны следующие операции:

- **Перемещение объекта** — см. **Перемещение окна объекта на выбранный дисплей**.
- **Отключение объекта** — позволяет временно отключить объект (подробнее см. **Работа с объектами**). В **Дереве объектов Рабочего стола** отключенные объекты будут отмечены так же, как и в *Дереве объектов SecurOS* (см. рис. 129).

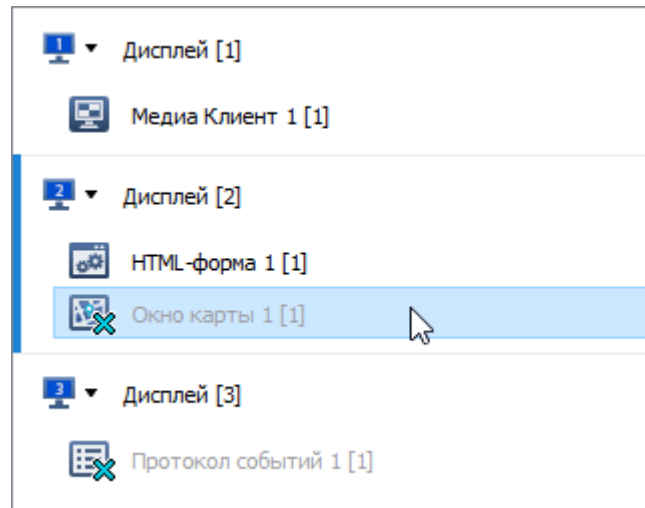


Рис. 129. Отключенный объект

- **Переименование объекта** — позволяет переименовать объект (подробнее см. **Работа с объектами**).
- **Удаление объекта** — позволяет удалить объект из *Дерева объектов SecurOS* (подробнее см. **Работа с объектами**).

Примечание. Удалить и переместить объект также можно с помощью соответствующих кнопок, расположенных в **Области визуальной настройки Рабочего стола**.

Особенности работы с многооконными объектами

При работе с многооконными интерфейсными объектами помимо перечисленных выше операций можно управлять отображением окон на экране оператора непосредственно из окна настройки параметров *Рабочего стола*. Данная операция аналогична включению/выключению режима отображения окна в собственных настройках объекта (например, *Auto: Интерфейс оператора*, см. **Руководство пользователя SecurOS Auto**). При работе с окнами таких объектов в **Блоке информации о настраиваемом окне** отметьте флажок слева от названия объекта для отображения окна (см. рис. 130) или снимите флажок, чтобы окно не выводилось на экран оператора.

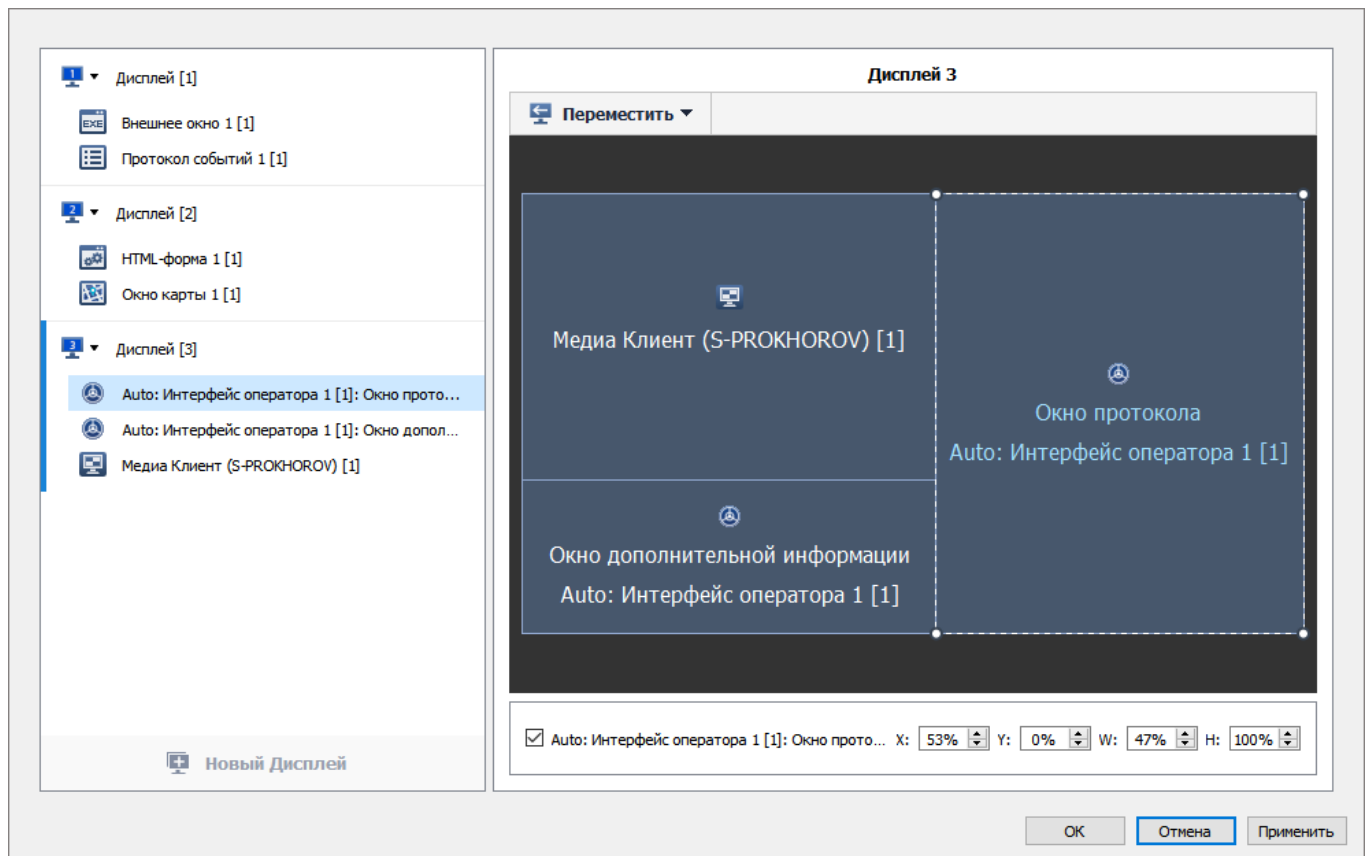


Рис. 130. Флажок управления режимом отображения окна

При работе с окнами Модуля SecurOS POS (см. [Руководство пользователя SecurOS POS](#)) окно **Информационной панели** всегда будет отображаться на том же дисплее, что и окно **Протокол событий**, независимо от его расположения в окне настроек параметров *Рабочего стола*.

8.1.2 Карта

Объект представляет многоуровневый план охраняемой территории.

Родительский объект — *Объект охраны\группа Карты*.

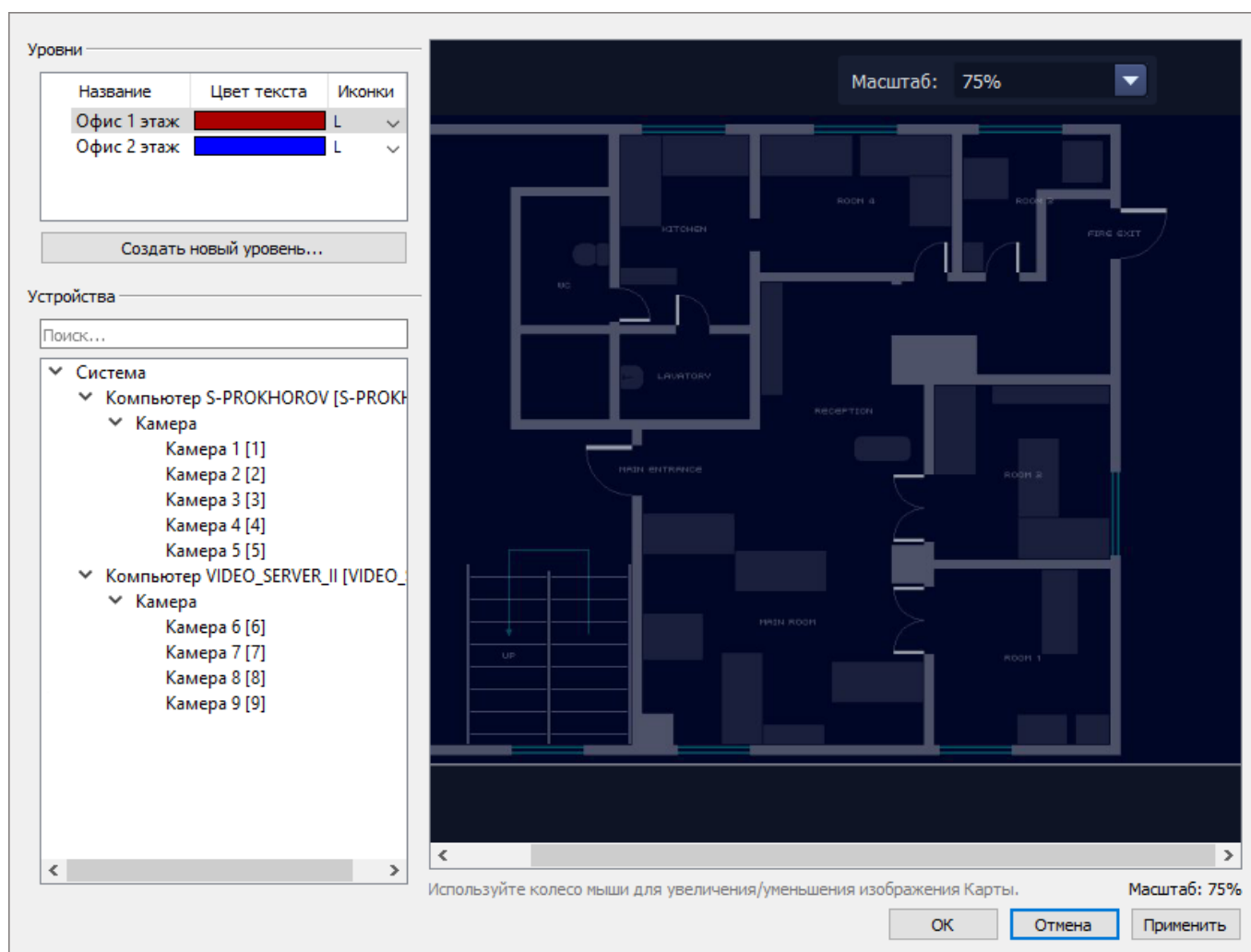


Рис. 131. Окно настройки параметров объекта Карта

Примечание. Текущие размеры блоков **Уровни**, **Устройства** и **Модель карты** можно изменять с помощью мыши.

Таблица 21. Параметры объекта Карта

Параметр	Описание
Уровни	
Название	Дерево и название уровней карты.
Цвет текста	Цвет подписей к объектам на изображении уровня карты.

Иконки	Размер иконок объектов на <i>Карте</i> и в окне Карта: Интерфейс оператора. Возможные значения: • S — маленький; • L — большой. Примечание. При масштабе от 25% до 200% будут отображаться иконки выбранного размера. При масштабе уровня карты менее 25% размер иконок будет автоматически изменен на S, при масштабе больше 200% - на L.
Устройства	
Поиск	Используется для поиска устройств (см. Работа с объектами).
Дерево устройств	В поле отображается <i>Дерево устройств</i> SecurOS, содержащее все устройства сети, которые можно добавить на карту.
Модель карты	
Масштаб	Текущий масштаб уровня карты. По умолчанию принимает значение 100%. Для изменения масштаба выберите требуемое значение из списка или наведите курсор мыши на изображение и используйте колесо прокрутки мыши. Внимание! Поле может быть перемещено в любую точку Области отображения карты. Для перемещения наведите указатель мыши на название поля, нажмите левую кнопку мыши и, не отпуская ее, переместите поле в требуемое положение.
Область отображения карты	Изображение текущего уровня карты.
Кнопки	
Создать новый уровень	Нажмите на кнопку, чтобы создать новый уровень карты (см. Работа с уровнями карты).

8.1.2.1 Принципы работы с картой

Для удобства мониторинга *Объекта охраны* рекомендуется использовать *Карту* — план охраняемой территории и расположенных на ней объектов. *Карта* может содержать несколько уровней, соответствующих, например, участкам охраняемой территории, этажам охраняемого здания или отдельным помещениям на этаже. Каждый **Уровень** карты представляет собой графическое изображение охраняемого объекта со значками элементов оборудования сети безопасности, размещенными на изображении в соответствии с их физическим расположением.

Для использования *Карт* в SecurOS необходимо выполнить следующие операции:

1. Создать объект **Карта**;
2. Создать на *Рабочем месте оператора* объект **Карта: Интерфейс оператора**;
3. Назначить оператору права доступа к данному объекту.

Примечание. Один и тот же объект *Карта* может быть использован в окне *Карта: Интерфейс оператора* на любом количестве *Рабочих мест оператора*.

После настройки оператор может использовать карты для мониторинга всей территории, а также использовать значки на карте для быстрого управления соответствующим объектом. Например, если сработала охранная сигнализация, оператор может сразу определить место срабатывания, начать запись с находящихся поблизости видеокамер, включить освещение и т. д.

8.1.2.2 Изображения уровней карты

Использование уровней карт удобно при разделении одной большой территории на несколько независимых. Уровни карты – это растровые изображения в форматах BMP, JPEG, JPG или PNG. Для создания горизонтального плана объектов можно использовать любой графический редактор, который позволяет сохранять такие изображения. Также можно использовать экспортированное растровое изображение из ПО CAD или отсканированный чертеж.

Изображения уровней могут быть любого цвета и стиля, однако необходимо учитывать следующее:

1. Все изображения должны быть в одинаковом графическом стиле для лучшего зрительного восприятия.
2. Размеры изображений (в пикселах) должны быть сопоставимы с размерами карт на экране рабочего места оператора, чтобы избежать избыточной прокрутки.
3. Цвета не должны отвлекать оператора от объектов, расположенных на карте. Не используйте яркие цвета, избегайте красных и оранжевых цветов. Чем нейтральнее фон, тем лучше.
4. Дайте название каждой охраняемой территории. Текст должен быть легко распознаваемым и читаемым.
5. Присвойте изображениям значимые имена (например, map_floor1.png, map_floor2.png, map_room123.png и т. д.).

Внимание! Не рекомендуется использовать файлы изображений размером более 4 МБ.

8.1.2.3 Работа с уровнями карты

Чтобы добавить уровень карты:

1. В окне настройки параметров объекта нажмите кнопку **Создать новый уровень**. Система выведет окно параметров уровня (см. рис. 132).

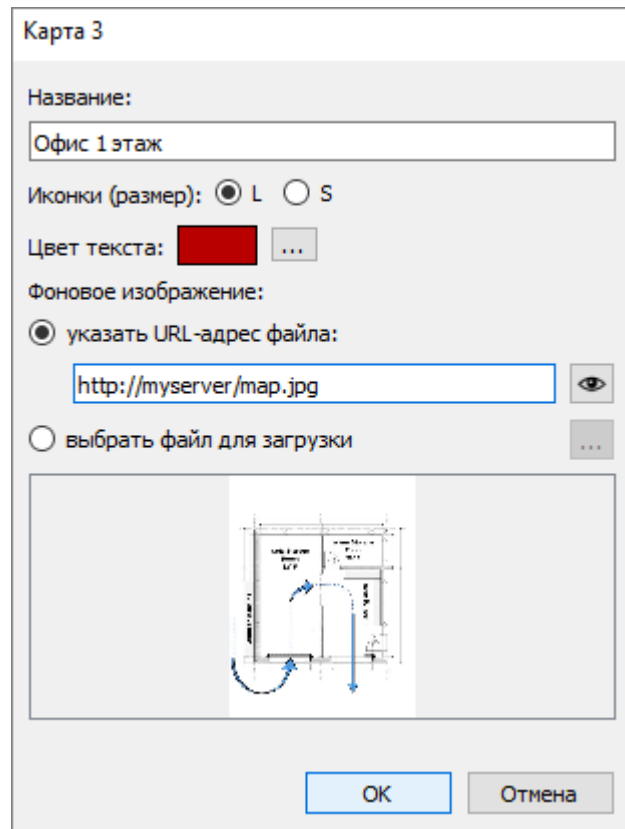


Рис. 132. Окно параметров уровня

2. Введите в поле **Название** название нового уровня.
3. Выберите размер иконок объектов:
 - S — маленький;
 - L — большой.
4. Нажмите кнопку  справа от поля **Цвет текста** и в стандартном окне выберите цвет подписей к объектам на данном уровне карты.
5. Выбрать изображение уровня можно двумя способами:
 - **указать URL-адрес файла.** В текстовом поле опции введите URL-адрес, по которому расположено изображение (адрес должен начинаться с *http* или *https*). Для предварительного просмотра запрашиваемого изображения, нажмите кнопку  справа от поля ввода URL-адреса к файлу.
 - **выбрать файл для загрузки.** Нажмите кнопку  справа от этой опции и с помощью файлового менеджера выберите файл изображения нового уровня карты.
6. Нажмите кнопку **ОК**.

Примечание. Созданный уровень размещается в списке **Название** (*Дерево уровней*) отсортированным по алфавиту.

Переход с уровня на уровень можно выполнить с помощью ссылки, представленной специальным значком, см. рис. 133 (по аналогии с гиперссылкой между страницами сайта).

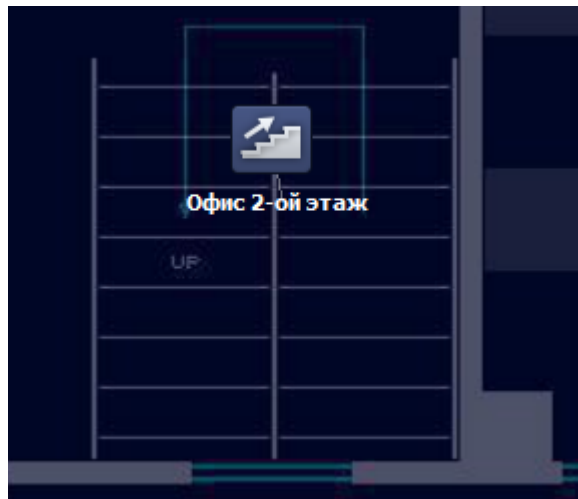


Рис. 133. Значок ссылки на уровень объекта Карты

Чтобы создать ссылку на уровень:

1. В дереве уровней выделите уровень, на котором необходимо создать ссылку на другой уровень. Изображение уровня будет выведено в **Области отображения уровней Карты**.
2. Выберите уровень, на который следует сослаться, щелкните его в списке **Название** (*Дерево уровней*) и, удерживая кнопку мыши нажатой, переместите курсор на изображение первого уровня.
3. Отпустите кнопку мыши.

После создания ссылки соответствующий значок появится на карте (см. рис. 133). Значок можно перемещать по карте, нажав на него и удерживая кнопку мыши.

Теперь можно проверить ссылку, щелкнув значок мышью: карта переключится на целевой уровень. Для упрощения навигации рекомендуется создать еще одну ссылку на этом уровне для перехода на предыдущий. Таким образом можно будет переходить по уровням в оба направления.

Значок ссылки рекомендуется размещать на плане уровня в соответствии с архитектурой охраняемого объекта. Например, если объект разделен на уровни по этажам охраняемого здания, целесообразно разместить значок ссылки на лестницах, соединяющих этажи здания, и т.д.

Прочие операции с уровнем *Карты* выполняются с помощью контекстного меню, которое вызывается щелчком правой кнопки мыши по имени уровня в списке **Название** (*Дерево уровней*). Контекстное меню содержит следующие команды (см. рис. 134):

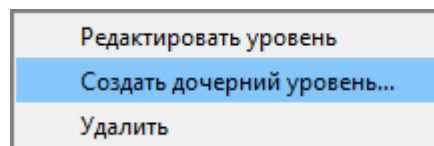


Рис. 134. Контекстное меню уровня Карты

- **Редактировать уровень** — редактирование текущего уровня;
- **Создать дочерний уровень** — создать уровень, дочерний текущему уровню в списке **Название** (*Дерево уровней*);
- **Удалить** — удаление текущего уровня.

Дочерний уровень также можно создать перетаскиванием. Щелкните мышью уровень, который необходимо сделать дочерним, и, удерживая кнопку мыши нажатой, перетащите его на родительский уровень (см. рис. 135).

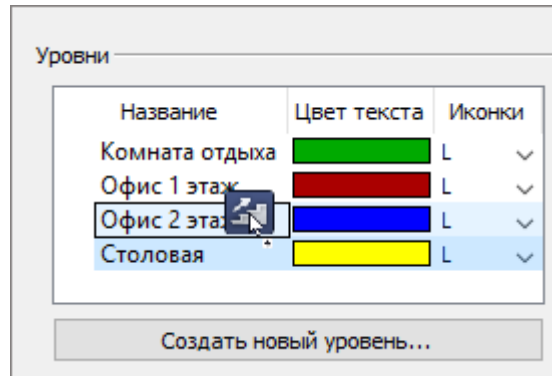


Рис. 135. Создание дочернего уровня перетаскиванием

8.1.2.4 Работа с объектами

С объектами на *Карте* возможны следующие операции:

- **Поиск объекта в Дереве устройств.**
- **Помещение объекта на уровень Карты.**
- **Изменение местоположения объекта на уровне.**
- **Ориентирование поля зрения Камеры.**
- **Позиционирование подписи к объекту.**
- **Изменение формата подписи к объекту.**
- **Удаление объекта с уровня Карты.**

Чтобы найти объект в Дереве устройств, введите в поле **Поиск** окна настройки параметров объекта любой символ (набор символов), входящий в название или идентификатор объекта. В *Дереве устройств* будут отображены все объекты, названия которых соответствуют заданному набору символов. Далее найденный объект может быть помещен на *Карту*.

Чтобы поместить объект на уровень Карты, выполните следующие действия:

1. В блоке **Уровни** выберите уровень, на который следует поместить объект. Фоновое изображение уровня будет выведено в правой части окна настройки.
2. В блоке **Устройства** выберите объект, который следует поместить на выбранный уровень.
3. Щелкните выбранный объект левой кнопкой мыши и, удерживая кнопку нажатой, переместите объект из списка в требуемое место на изображении уровня.

Чтобы изменить положение объекта в пределах уровня, выполните следующие действия:

1. В блоке **Уровни** выберите уровень, на котором располагается объект.
2. Щелкните значок объекта левой кнопкой мыши и, удерживая кнопку нажатой, перетащите его на новое место.

Чтобы повернуть значок Камеры в соответствии с реальным полем зрения Камеры, выполните следующие действия:

1. Щелкните мышью значок *Камеры*, которую надо повернуть. Справа от значка отобразится двусторонняя стрелка, см. рис. 136.

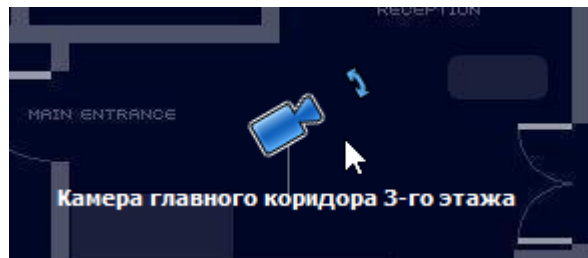


Рис. 136. Вращение значка Камеры на Карте

2. Удерживая нажатой левую кнопку мыши на этой стрелке, поверните значок вокруг своей оси в требуемом направлении в соответствии с реальным полем зрения камеры.

Чтобы переместить подпись к объекту, выполните следующие действия:

1. Наведите курсор на подпись и нажмите левую кнопку мыши. Курсор примет форму, представленную на рис. 137.

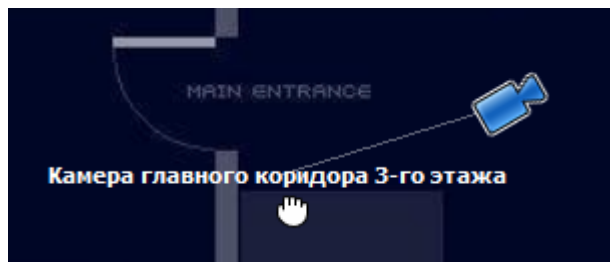


Рис. 137. Перемещение названия объекта

2. Удерживая кнопку нажатой, перетащите строку в любое место вокруг значка.

Чтобы изменить формат подписи к объекту, выполните следующие действия:

1. Нажмите иконку **A...C** справа от подписи (см. рис. 138).

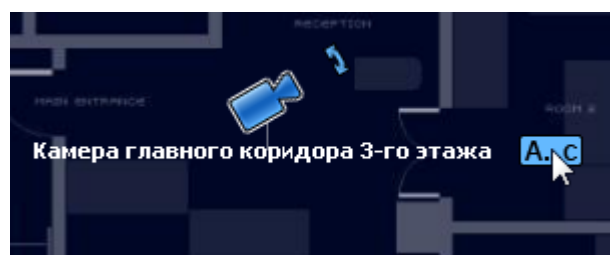


Рис. 138. Изменение отображаемого названия объекта

2. Подпись к объекту будет отображаться на *Карте* в краткой форме (см. рис. 139).

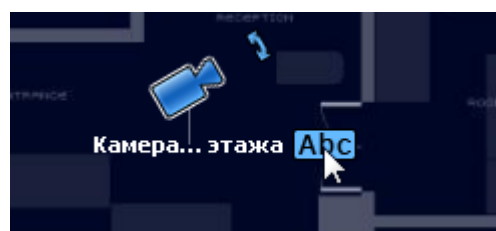


Рис. 139. Сжатое название объекта

Для возврата к полной форме подписи нажмите иконку **Abc** справа от подписи (см. рис. 139).

Чтобы удалить объект с уровня Карты, выполните следующие действия:

1. В блоке **Уровни** выберите уровень, с которого необходимо удалить объект.
2. Выделите объект щелчком мыши и нажмите клавишу **Delete**. Также объект можно удалить командой **Удалить** из контекстного меню объекта.

8.1.3 Карта: Интерфейс оператора

Объект представляет графический интерфейс для отображения **Карты**.

Родительский объект — **Рабочий стол**.

Рис. 140. Окно настройки параметров объекта Карта: Интерфейс оператора

Таблица 22. Параметры объекта Карта: Интерфейс оператора

Параметр	Описание
X, Y, W, H	Задайте координаты верхнего левого угла (X, Y) относительно верхнего левого угла дисплея, ширину и высоту (W, H) окна <i>Карта: Интерфейс оператора</i> (в процентах от размеров экрана).
Дисплей	Выберите идентификатор физического монитора, на котором будет отображаться данный объект.
Карта	Выберите из списка одну из предварительно созданных карт (см. Карта), которую необходимо отображать в данном окне.

Параметр	Описание
Показывать уровни	Признак вывода в окне объекта <i>Карта: Интерфейс оператора</i> закладки Уровни. Закладка содержит список уровней <i>Карты</i>, позволяющий выполнять переключение между уровнями. По умолчанию отмечен. Примечание. Если параметр не отмечен, переход по уровням в окне <i>Карта: Интерфейс оператора</i> возможен только с помощью ссылок на уровни (см. Работа с уровнями карты).
Показывать тревожные уровни	Признак вывода в окне объекта <i>Карта: Интерфейс оператора</i> закладки Тревоги. Закладка содержит список уровней <i>Карты</i>, на которых зафиксированы тревоги и позволяет выполнять быстрое переключение между такими уровнями. Примечание. Тревожным считается уровень, если хотя бы один из размещенных на нем объектов находится в состоянии тревоги. По умолчанию отмечен. Чек-бокс недоступен, если не отмечен чек-бокс Показывать список уровней.
Работать с Медиа Клиентом	Выберите <i>Медиа Клиент</i>, который будет использоваться для просмотра видео при переходе из окна <i>Карта: Интерфейс оператора</i>. Для перехода к просмотру видео на <i>Медиа Клиенте</i> щелкните мышью иконку одного из объектов, расположенных в окне <i>Карта: Интерфейс оператора</i>: • <i>Камера</i> — при переходе ячейка соответствующей <i>Камеры</i> будет отображаться в раскладке 1x1 в режиме живого видео; • <i>Луч</i> — при переходе будут отображаться ячейки всех <i>Камер</i>, заданных в настройках выбранного объекта <i>Луч</i>, в наиболее подходящей раскладке в режиме живого видео.
Отображать Камеры в Медиа Клиенте и фильтровать объекты СКУД/ОПС при активации Уровня	Отметьте флажок, чтобы при переходе на <i>Уровень Карты</i> отображать все <i>Камеры</i>, расположенные на этом уровне, а также все <i>Камеры</i>, связанные с прочими объектами, которые расположены на этом уровне. <i>Камеры</i> будут отображаться на <i>Медиа Клиенте</i> в наиболее подходящей раскладке. Если количество таких <i>Камер</i> превышает количество ячеек в максимально возможной раскладке, оставшиеся <i>Камеры</i> будут размещены на следующих видеостраницах <i>Медиа Клиента</i>. Внимание! Для отображения <i>Камер</i> необходимо выбрать <i>Медиа Клиент</i> в параметре Работать с Медиа Клиентом.
Фильтрация объектов в СКУД/ОПС: Интерфейсе оператора	Выберите объект <i>СКУД/ОПС: Интерфейс оператора</i>, в котором будет автоматически активирован фильтр, включающий в себя все СКУД/ОПС-объекты, расположенные на активированном <i>Уровне Карты</i>.

8.1.4 Протокол событий

Объект представляет собой визуальный протокол событий системы.

Родительский объект — **Рабочий стол**.

Рис. 141. Окно настройки параметров объекта Протокол событий

Таблица 23. Параметры объекта Протокол событий

Параметр	Описание
Х, Y, W, H	Задайте координаты верхнего левого угла (X, Y), ширину и высоту (W, H) окна (в процентах от размеров экрана).
Дисплей	Выберите идентификатор физического монитора, на котором будет отображаться данный объект.
Использовать Фильтр событий	Фильтр событий, который будет использоваться для определения событий, которые необходимо отображать в окне интерфейсного объекта Протокол событий . Необязательный параметр. Если принимает значение Не использовать, в протоколе событий будут отображаться все системные события. Если фильтр выбран, в протоколе будут отображаться только те события, которые разрешены выбранным фильтром (см. раздел Фильтр событий).

Параметр	Описание
Работать с Медиа Клиентом	Выберите Медиа Клиент, который будет использоваться для просмотра видео, соответствующего событию, занесенному в протокол. Внимание! Если <i>Медиа Клиент</i> не выбран, переход из <i>Протокола событий</i> в <i>Медиа Клиент</i> для просмотра видеофрагмента, соответствующего событию, будет невозможен.
Работа с событиями из разных часовых поясов	Активируйте данное поле, чтобы предоставить оператору доступ к инструментам <i>Протокола событий</i> , предназначенным для более удобного просмотра и поиска событий из разных часовых поясов.
Отправить Карточку в Службу реагирования	Выберите из списка объект <i>Служба реагирования</i> , который будет использоваться для создания и отправки <i>Карточки происшествия</i> (см. Служба реагирования и Взаимодействие с внешней Службой реагирования).
Реакция оператора на тревожное событие	Активируйте данное поле, чтобы разрешить оператору подтверждать тревожные события.
Время на подтверждение тревожного события оператором	Задайте время в секундах, отведенное оператору на подтверждение тревожной ситуации.

8.1.5 Внешнее окно

В ОС **Linux** функциональность не поддерживается.

Объект используется для автоматической загрузки внешнего приложения и расположения его окна на экране.

Родительский объект — **Рабочий стол**.

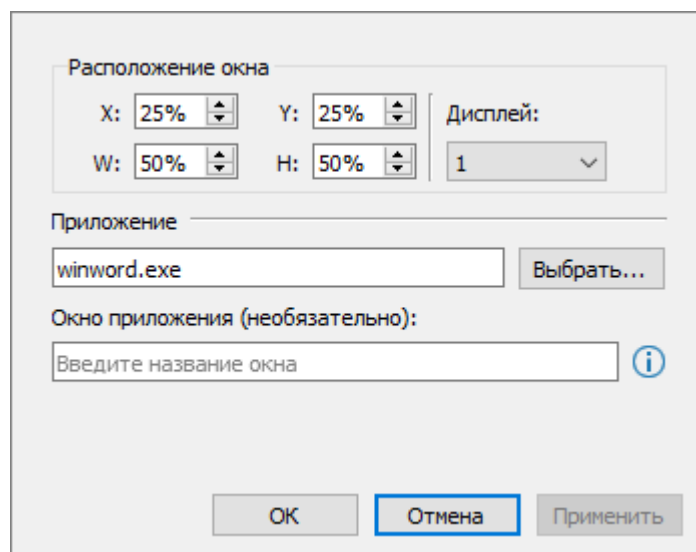


Рис. 142. Окно настройки параметров объекта Внешнее окно

Таблица 24. Параметры объекта Внешнее окно

Параметр	Описание
X, Y, W, H	Задайте координаты верхнего левого угла (X, Y), ширину и высоту (W, H) окна (в процентах от размеров экрана). Не для всех приложений возможно масштабирование их окон в других программах. Диапазон возможных значений координат (X, Y) и размеров окна (W, H) — [0; 999]. Например, если заданы значения X=150, Y=0, W=150 и H=100, то окно внешнего приложения будет размещаться на втором и третьем дисплеях (по горизонтали). Размер окна по вертикали будет равен размеру второго дисплея.
Дисплей	Выберите идентификатор физического монитора, на котором будет отображаться окно внешнего приложения.
Приложение	Укажите путь к исполняемому файлу. Можно не вводить полный путь к файлу, если он находится в каталоге, определенном в переменной среды Path.
Выбрать (кнопка)	Нажмите кнопку и, с помощью файлового менеджера, выберите исполняемый файл приложения.
Окно приложения (необязательно)	Если приложение многооконное, введите имя окна, с которым необходимо работать оператору.

8.1.6 HTML5 FrontEnd

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*.

Объект предназначен для создания на *Рабочем столе* SecurOS окна для отображения внешнего web-приложения с интерфейсом управления SecurOS. Загрузка окна выполняется при активации соответствующего *Рабочего стола*.

С помощью объекта можно интегрировать в SecurOS внешние web-приложения, поддерживающие HTML5.

Внимание! Окно объекта для отображения внешних web-приложений не является полноценным браузером и обладает ограниченной функциональностью (подробнее об ограничениях см. [Руководство программиста SecurOS](#)).

Объект позволяет:

- Задавать размеры и положение окна внешнего web-приложения на *Рабочем столе* SecurOS.
- Выбирать *Медиа Клиент* и окно *Карта: Интерфейс оператора*, с которыми может работать внешнее web-приложение.
- Отправлять дополнительные параметры из SecurOS во внешнее web-приложение.

Родительский объект — **Рабочий стол**.

Рис. 143. Окно настройки параметров объекта HTML5 FrontEnd

Таблица 25. Параметры объекта HTML5 FrontEnd

Параметр	Описание
Расположение окна	
X, Y, W, H	Задайте координаты верхнего левого угла (X, Y), ширину и высоту (W, H) окна (в процентах от размеров экрана).
Дисплей	Выберите идентификатор физического монитора, на котором будет отображаться окно внешнего web-приложения.
URL	Задайте URL HTML-страницы внешнего приложения или укажите путь к индексному файлу.
Работать с Медиа Клиентом	В выпадающем списке выберите <i>Медиа Клиент</i>, с которым будет работать web-приложение. Под работой с <i>Медиа Клиентом</i> подразумевается отправка ему <i>Событий</i> или <i>Команд</i> в формате SecurOS. Примечание. События и Команды управления Медиа Клиентом описаны в документе Руководство программиста SecurOS.
Работать с Картой: Интерфейс оператора	В выпадающем списке выберите окно <i>Карта: Интерфейс оператора</i>, с которым будет работать web-приложение. Под работой с окном <i>Карта: Интерфейс оператора</i> подразумевается отправка ему <i>Событий</i> или <i>Команд</i> в формате SecurOS. Примечание. События и Команды управления окном <i>Карта: Интерфейс оператора</i> описаны в документе Руководство программиста SecurOS.

Параметр	Описание
Дополнительно	При необходимости передавать дополнительные параметры из SecurOS во внешнее web-приложение, задайте эти параметры в данном поле. Заданные параметры будут переданы внешнему приложению в сообщении SETUP вместе с идентификаторами выбранного <i>Медиа Клиента</i> и окна <i>Карта: Интерфейс оператора</i> .

9 Видеоподсистема

Видеоподсистема используется для работы и настройки видеоустройств в сети SecurOS, обмена видеопотоками между серверами и рабочими местами и для работы с живым видео и видеоархивом на рабочих местах.

При передаче видеопотоков между устройствами и сервисами, как правило, применяют кодирование (компрессию) видео в определенные стандартные форматы. Это используется для совместимости видео с широким спектром устройств, а также для уменьшения размера файлов и экономии трафика. При получении видеопотока на клиентской стороне сначала производится декодирование (декомпрессия), а затем отображение видео. Примерами сервисов, использующих средства декомпрессии SecurOS, являются: *Медиа Клиент*, детекторы движения и расфокусировки, модули аналитики и другие. Такие сервисы, как SecurOS WebConnect и SecurOS Mobile, используют сторонние средства для декодирования видеопотоков живого и архивного видео.

Процесс кодирования представляет собой смену формата изображения. При этом происходит уменьшение объема видеoinформации с потерей качества изображения. Чем сильнее сжимается изображение, тем меньше оно занимает места и тем больше потери качества. В закодированном виде изображение на экране отобразить нельзя, его нужно предварительно декодировать. Соответственно, декодирование — это обратный процесс восстановления исходного изображения из сжатого формата. Чем больше степень сжатия, тем больше отличаются исходное изображение и полученное после цикла компрессии-декомпрессии.

В SecurOS реализованы два типа обработки изображений (компрессии/декомпрессии): программная и аппаратная.

- В случае использования программной обработки видео все вычисления проходят на центральном процессоре компьютера.
- Аппаратная обработка осуществляется с помощью интегрированного в процессор или дискретного видеоадаптера. Это позволяет существенно снизить нагрузку на процессор компьютера, ускорить обработку видео, а также снижает энергопотребление системы. Благодаря этому становится возможным обрабатывать большее количество видеопотоков в системе или использовать видеопотоки с большим разрешением без потери кадров (снижения FPS).

9.1 Аппаратная декомпрессия

В SecurOS поддерживается аппаратная декомпрессия видеопотоков в форматах H.264/H.265.

Механизм аппаратной декомпрессии реализуется по-разному в зависимости от операционной системы:

- В операционных системах семейства Microsoft Windows используется DXVA 2.0 — компонент DirectX, разработанный корпорацией Microsoft и предназначенный для обработки (в первую очередь, декодирования) битового потока видеоданных силами графических процессоров. Более подробное описание представлено в разделе [Настройка аппаратной декомпрессии для ОС Windows](#).

- В операционных системах на базе Linux интерфейс, используемый для аппаратной декомпрессии, зависит от производителя видеоадаптера компьютера и настраивается дополнительно. Более подробное описание представлено в разделе **Настройка аппаратной декомпрессии для ОС Linux**.

Внимание! Клиенты, отображающие видео от SecurOS за пределами интерфейса оператора SecurOS, могут использовать собственные средства аппаратной декомпрессии. Например, SecurOS WebConnect использует средства декомпрессии браузера.

Для обозначения технологии аппаратной декомпрессии различные производители используют независимые маркетинговые названия: Intel Quick Sync Video, NVIDIA PureVideo HD, AMD VCN. В SecurOS реализована поддержка всех перечисленных технологий. В ОС семейства Windows при наличии нескольких видеоадаптеров происходит равномерное распределение задач декодирования между всеми видеоядрами системы, включая дискретные и интегрированные, независимо от производителя видеоадаптера. В ОС семейства Linux для аппаратной декомпрессии используются только те видеоадаптеры, которые поддерживают установленный в ОС пакет API (подробнее в разделе **Настройка аппаратной декомпрессии для ОС Linux**).

Для работы SecurOS рекомендуется использование технологии Intel Quick Sync Video, которая демонстрирует лучшие показатели скорости декомпрессии среди конкурентов (NVIDIA, AMD). В SecurOS поддержка данной технологии реализована для видеоадаптеров Intel HD Graphics 2500, HD4xxx, HD5xxx (на ядрах GT3) и выше.

Во всех указанных видеоадаптерах реализована технология Intel Quick Sync Video 2.0, которая перенаправляет операции декодирования на специальный аппаратный модуль графического адаптера Intel HD Graphics – Multi-Format Codec Engine (MFX).

Все указанные видеоадаптеры являются интегрированными в CPU и поддерживают аппаратную декомпрессию независимо от модели процессора (i3, i5, i7, и т.д.):

- Для H.264 – на процессорах Intel Core 3xxx и новее.
- Для H.265 – на процессорах Intel Core 5xxx и новее.

Не все модели процессоров имеют такой интегрированный видеоадаптер (например, процессоры серии F и Xeon).

Внимание! Поддержка технологии Intel Quick Sync Video 1.0 на мобильных и десктопных видеоадаптерах Intel HD Graphics 2000 в SecurOS не реализована. Таким образом, аппаратная декомпрессия на процессорах с архитектурой Sandy Bridge не выполняется.

Основным параметром производительности чипа MFX является его пропускная способность (по сжато видео, в Гбит/с), которая ограничена не просто количеством одновременно декодируемых потоков (камер), а суммарным количеством и размером этих потоков (например, декодер Intel Quick Sync 2.0 может декодировать порядка 40 – 50 потоков размера 2 Мбит/с).

Ограничивающим фактором может быть производительность памяти. То есть, память должна успевать записывать указанное число декомпрессированных потоков, объем данных которых непосредственно зависит от разрешения. Таким образом, для достижения максимальной производительности следует комплектовать систему двухканальной памятью с частотой не менее 1600 Mhz.

9.1.1 Настройка аппаратной декомпрессии для ОС Windows

Аппаратная декомпрессия задействуется в системе автоматически.

- Если в компьютере установлен и используется только интегрированный видеоадаптер, то никаких дополнительных действий не требуется.
- Если в компьютере установлены один или несколько дискретных видеоадаптеров, а интегрированные видеоадаптеры отсутствуют, то используются все дискретные видеоадаптеры. Никаких действий не требуется.
- Если используются один или несколько дискретных видеоадаптеров, а также присутствует интегрированный в процессор видеоадаптер, то драйвер системной платы автоматически отключает встроенный видеоадаптер. Декомпрессия выполняется только на дискретных видеоадаптерах.

Для включения возможности аппаратной декомпрессии на встроенном графическом процессоре выполните следующие действия:

1. Включите поддержку интегрированного видеоадаптера в BIOS (местоположение опции зависит от поставщика и версии BIOS). После выполнения этой операции адаптер будет определяться **Диспетчером Устройств Windows**.
2. Установите совместимый драйвер встроенного видеоадаптера последней версии.

9.1.2 Настройка аппаратной декомпрессии для ОС Linux

Данный раздел содержит информацию о конфигурировании режима декомпрессии в SecurOS, который выбирается на основании дополнительно установленных пакетов Linux (см. раздел **Настройка аппаратного ускорения в ОС Linux**). Если планируется использование программной декомпрессии, то устанавливать дополнительные пакеты Linux не требуется. Конфигурирование SecurOS в этом случае тоже не требуется, поскольку режим программной декомпрессии выбран по умолчанию.

Для настройки режима декомпрессии в ОС Linux выполните следующие действия:

1. Остановите демон `vms_server` с помощью команды `sudo service vms_server stop`.
2. Откройте для редактирования файл `/etc/xdg/iss/securos.conf` и добавьте в него строку `Video\H264Decompressor=X`, где `X` — значение, определяющее режим и метод декомпрессии:
 - `ffmpeg` (значение по умолчанию) — аппаратная декомпрессия с использованием библиотеки `ffmpeg`.
 - `ffmpeg_sw` — программная декомпрессия с использованием библиотеки `ffmpeg`.
 - `ipp` — программная декомпрессия с использованием библиотеки Intel IPP.
 - `ffmpeg_vaapi` — аппаратная декомпрессия с использованием VA-API и библиотеки `ffmpeg`.
 - `ffmpeg_vdpau` — аппаратная декомпрессия с использованием VDPAU и библиотеки `ffmpeg`.
3. Запустите демон `vms_server` с помощью команды `sudo service vms_server start`.

9.2 Аппаратная компрессия

В SecurOS поддерживается аппаратная компрессия видеопотоков в формате H.264.

Механизм аппаратной компрессии реализуется по-разному в зависимости от операционной системы:

- В операционных системах семейства Microsoft Windows используется набор библиотек Intel Media SDK, которые позволяют кодировать видео в формат H.264 с использованием графических адаптеров Intel. Аппаратное кодирование поддерживается автоматически — дополнительные настройки SecurOS не требуются.
- В операционных системах на базе Linux аппаратная компрессия поддерживается с использованием VA-API, однако для этого необходимо установить дополнительные пакеты Linux (см. [Настройка аппаратного ускорения в ОС Linux](#)).

9.3 Настройка аппаратного ускорения в ОС Linux

Внимание! По умолчанию в ОС Linux используется программная декомпрессия.

В отличие от Windows, для работы аппаратной декомпрессии в ОС Linux необходима установка дополнительных пакетов API в зависимости от происхождения используемого видеоадаптера:

- Video Acceleration API (VA-API) — поддерживается Intel, AMD и NVIDIA (только драйверы Nouveau с открытым исходным кодом).
- Video Decode and Presentation API for Unix (VDPAU) — поддерживается AMD, NVIDIA (проприетарные драйверы и Nouveau). Работает только в интерфейсных приложениях. На серверных модулях (Auto, ТКЗ и т.д.) эта технология недоступна.

Внимание! На видеоадаптерах NVIDIA одновременное использование нейросетевых алгоритмов SecurOS и декомпрессии не поддерживается. Поэтому при работе с нейросетевыми алгоритмами, которые работают на видеоадаптере NVIDIA, для аппаратной декомпрессии необходимо настроить другой видеоадаптер.

9.3.1 Установка дополнительных пакетов в ОС Linux

В данном разделе представлена информация по установке дополнительных пакетов Linux для использования аппаратного ускорения. Данная инструкция подходит для большинства ОС семейства Linux, за исключением Debian. Инструкцию по установке пакетов Debian можно найти в разделе [Установка дополнительных пакетов в ОС Debian](#).

INTEL

Свободные драйверы Intel graphics поддерживают VA-API:

- Серия HD Graphics, начиная с Broadwell и новее, поддерживается `intel-media-driver`.
- GMA 4500 series и более новые GPU до Coffee Lake поддерживаются `libva-intel-driver`.
- Декодирование H.264 на GMA 4500 поддерживается `libva-intel-driver-g45-h264`.
- Гибридное декодирование VP9 на процессорах от Broadwell до Skylake, а также гибридное декодирование VP8 на процессорах от Haswell до Skylake, поддерживается `intel-hybrid-codec-driver`.
- Skylake и более новые поколения также требуют пакет с микропрограммой `linux-firmware`.

NVIDIA

Свободный драйвер Nouveau поддерживает как VA-API, так и VDPAU:

- GeForce 8 series и новее (до GeForce GTX 750) поддерживаются `libva-mesa-driver` и `mesa-udpau`.
- Необходим `nouveau-fw` — пакет с микропрограммой, которая на сегодняшний день извлекается из бинарного драйвера NVIDIA.

Проприетарный драйвер NVIDIA поддерживает следующие технологии с помощью пакета `nvidia-utils`:

- VDPAU на серии GeForce 8 и новее.
- NVDECODER на Fermi и новее.
- NVENCODER на Kepler и новее.

ATI/AMD

Свободные драйверы ATI и AMDGPU поддерживают как VA-API, так и VDPAU:

- VA-API на Radeon HD 2000 и новее поддерживается `libva-mesa-driver`.
- VDPAU на Radeon R300 и новее поддерживается `mesa-udpau`.

Проприетарный драйвер AMDGPU PRO основывается на драйвере AMDGPU и поддерживает как VA-API, так и VDPAU.

9.3.2 Установка дополнительных пакетов в ОС Debian

VA-API

- Для NVIDIA Nouveau и различных драйверов AMD достаточно установить пакет `mesa-va-drivers`.
- Пакеты с драйверами для оборудования Intel зависят от поколения графических адаптеров, а также делятся на *свободные* и *проприетарные*. Проприетарные драйверы поддерживают кодирование/декодирование видео, тогда как *свободные* — только декодирование. Для оборудования Intel поколения 8+ свободный драйвер можно установить с помощью пакета `intel-media-va-driver`. Проприетарный драйвер включен в пакет `intel-media-va-driver-non-free`.
- Для более старого оборудования Intel свободный драйвер можно установить с помощью пакета `i965-va-driver`. Проприетарный драйвер включен в пакет `i965-va-driver-shaders`.

VDPAU

- Чтобы включить поддержку VDPAU для драйверов AMD (`radeon` и `amdgpu`), а также Nouveau с открытым исходным кодом для карт NVIDIA, установите пакет `udpau-driver-all`.
- Чтобы включить поддержку VDPAU для проприетарных драйверов NVIDIA, необходимо выбрать пакет, соответствующий вашей версии драйвера. Если вы установили последние версии драйверов с помощью пакета `nvidia-driver`, то достаточно установить пакет `nvidia-udpau-driver`.

Если используется устаревший драйвер, выберите соответствующий пакет из следующих:

- `nvidia-legacy-304xx-udpau-driver`.

- nvidia-legacy-340xx-vdpau-driver.
- nvidia-legacy-390xx-vdpau-driver.

9.3.3 Проверка работы аппаратного ускорения

В большинстве случаев аппаратное ускорение будет корректно работать по умолчанию. Проверить это можно описанными ниже способами:

- **Проверка VA-API.**
- **Проверка VDPAU.**

Проверка VA-API

1. Убедитесь, что текущий пользователь, который планирует использовать SecurOS, состоит в группе render.

Примечание. Группа render является системной группой Linux. Пользователи этой группы получают доступ к использованию устройств рендеринга при аппаратном ускорении.

2. Установите пакет vainfo.
3. Проверьте настройки VA-API, выполнив команду vainfo:

```
libva info: VA-API version 0.39.4
libva info: va_getDriverName() returns 0
libva info: Trying to open /usr/lib/dri/i965_drv_video.so
libva info: Found init function __vaDriverInit_0_39
libva info: va_openDriver() returns 0
vainfo: VA-API version: 0.39 (libva 1.7.3)
vainfo: Driver version: Intel i965 driver for Intel(R) Skylake - 1.7.3
vainfo: Supported profile and entrypoints
    VAProfileMPEG2Simple : VAEntrypointVLD
    VAProfileMPEG2Simple : VAEntrypointEncSlice
    VAProfileMPEG2Main : VAEntrypointVLD
    VAProfileMPEG2Main : VAEntrypointEncSlice
    VAProfileH264ConstrainedBaseline:
    VAEntrypointVLD
    VAProfileH264ConstrainedBaseline: VAEntrypointEncSlice
    VAProfileH264ConstrainedBaseline: VAEntrypointEncSliceLP
    VAProfileH264Main : VAEntrypointVLD
    VAProfileH264Main : VAEntrypointEncSlice
    VAProfileH264Main : VAEntrypointEncSliceLP
    VAProfileH264High : VAEntrypointVLD
    VAProfileH264High : VAEntrypointEncSlice
    VAProfileH264High : VAEntrypointEncSliceLP
    VAProfileH264MultiviewHigh : VAEntrypointVLD
    VAProfileH264MultiviewHigh : VAEntrypointEncSlice
    VAProfileH264StereoHigh : VAEntrypointVLD
    VAProfileH264StereoHigh : VAEntrypointEncSlice
    VAProfileVC1Simple : VAEntrypointVLD
    VAProfileVC1Main : VAEntrypointVLD
    VAProfileVC1Advanced : VAEntrypointVLD
    VAProfileNone : VAEntrypointVideoProc
    VAProfileJPEGBaseline : VAEntrypointVLD
    VAProfileJPEGBaseline : VAEntrypointEncPicture
    VAProfileVP8Version0_3 : VAEntrypointVLD
    VAProfileVP8Version0_3 : VAEntrypointEncSlice
    VAProfileHEVCMail : VAEntrypointVLD
```

VAProfileHEVCMain : VAEntrypointEncSlice

VAEntrypointVLD означает, что видеоадаптер способен декомпрессировать данный формат, а VAEntrypointEncSlice означает, что данный формат можно компрессировать.

В данном примере используется драйвер i965:

```
libva info: Trying to open /usr/lib/dri/i965_drv_video.so
```

Если при выполнении vainfo отображается следующая ошибка:

```
libva info: va_openDriver() returns -1
vaInitialize failed with error code -1 (unknown libva error),exit
```

Необходимо задать корректный драйвер, см. [Настройка VA-API](#).

Проверка VDPAU

1. Установите пакет vdpauinfo.
2. Получите полный отчёт о конфигурации драйвера VDPAU и убедитесь, что он загружен корректно:

```
$ vdpauinfo
display: :0      screen: 0
API version: 1
Information string: G3DVL VDPAU Driver Shared Library version 1.0
```

Video surface:

name	width	height	types
420	16384	16384	NV12 YV12
422	16384	16384	UYVY YUYV
444	16384	16384	Y8U8V8A8 V8U8Y8A8

Decoder capabilities:

name	level	macbs	width	height
MPEG1	--- not supported ---			
MPEG2_SIMPLE	3	9216	2048	1152
MPEG2_MAIN	3	9216	2048	1152
H264_BASELINE	41	9216	2048	1152
H264_MAIN	41	9216	2048	1152
H264_HIGH	41	9216	2048	1152
VC1_SIMPLE	1	9216	2048	1152
VC1_MAIN	2	9216	2048	1152
VC1_ADVANCED	4	9216	2048	1152

..

9.3.4 Решение типовых проблем аппаратного ускорения

Несмотря на то, что видеодрайвер должен автоматически активировать поддержку аппаратного ускорения видео с помощью VA-API и VDPAU, в некоторых случаях может потребоваться настроить VA-API/VDPAU вручную. Перед тем, как продолжать чтение данного раздела, просмотрите раздел [Проверка работы аппаратного ускорения](#).

Названия драйверов по умолчанию определяются автоматически системой, если отсутствуют какие-либо другие настройки. Однако они часто не совпадают и не работают. Предполагаемые значения можно просмотреть, выполнив следующую команду:

```
$ grep -iE 'vdpaу | dri driver' /var/log/Xorg.0.log
```

Результат выполнения команды:

```
(II) RADEON(0): [DRI2] DRI driver: radeonsi
(II) RADEON(0): [DRI2] VDPAU driver: radeonsi
```

В данном случае по умолчанию используется драйвер `radeonsi` для VA-API и VDPAU.

Внимание! Если используется GDM, выполните вместо этого команду `journalctl -b | grep -iE 'vdpaу | dri driver'`.

Настройка VA-API

Драйвер VA-API можно переопределить с помощью переменной окружения `LIBVA_DRIVER_NAME`:

- Intel graphics:
 - Укажите `i965`, если используется `libva-intel-driver` (`i965-va-driver` для Debian).
 - Укажите `iHD`, если используется `intel-media-driver` (`intel-media-va-driver` для Debian).
- NVIDIA:
 - Укажите `nouveau`, если используется Nouveau.
 - Укажите `vdpaу`, если используется NVIDIA.
- ATI/AMD:
 - Укажите `radeonsi`, если используется AMDGPU.

Обратите внимание на то, что:

- Установленные драйверы находятся в `/usr/lib/dri/` и используются как `/usr/lib/dri/${LIBVA_DRIVER_NAME}_drv_video.so`.
- Некоторые драйверы устанавливаются несколько раз под разными именами в целях совместимости. Их список можно увидеть, выполнив команду `shasum /usr/lib/dri/* | sort`.
- `LIBVA_DRIVERS_PATH` может использоваться для переопределения расположения драйверов VA-API.
- Начиная с версии 12.0.1, `libva-mesa-driver` предоставляет `radeonsi` вместо `gallium`.

Настройка VDPAU

Драйвер VDPAU можно переопределить с помощью переменной окружения `VDPAU_DRIVER`.

Корректное название драйвера зависит от конфигурации:

- Если используется Intel Graphics или AMD Catalyst, необходимо задать значение `va_gl`.
- Если используется свободный драйвер AMD/ATI, задайте соответствующую версию драйвера в зависимости от видеокарты (см. [Проверка VDPAU](#) в разделе [Проверка работы аппаратного ускорения](#)).

- Если используется свободный драйвер Nouveau, задайте nouveau.
- Если используется проприетарный драйвер NVIDIA, задайте nvidia.

Обратите внимание на то, что:

- Установленные драйверы находятся в `/usr/lib/vdpau/` и используются как `/usr/lib/vdpau/libvdpau_${VDPAU_DRIVER}.so`.
- Некоторые драйверы устанавливаются несколько раз под разными именами в целях совместимости. Их список можно увидеть, выполнив команду `shasum /usr/lib/vdpau/*`.
- В случае с конфигурацией с гибридной графикой (как с NVIDIA, так и с AMD), может потребоваться задать переменную окружения `DRI_PRIME=1`.

9.4 Многопоточность

Большое количество современных камер оснащены функцией поддержки нескольких потоков видеосигнала — многопоточностью. Потоки могут иметь различные наборы настроек (разрешение, частоту кадров, компрессию и т.п.) и использоваться для различных целей. Такие наборы настроек могут быть встроенными и определяться уникальным именем потока, либо задаваться *Профилем камеры*, который создается и редактируется администратором с помощью web-интерфейса *Камеры*.

Необходимость в широком потоке (с высоким качеством, разрешением, fps) возникает при отображении *Камеры* в ячейке *Медиа Клиента* большого размера, цифровом масштабировании, при записи видеоархива. Узкие потоки (с низким битрейтом) используются для передачи видеосигнала по каналам с низкой пропускной способностью (например, при передаче видео по каналу 3g на мобильные устройства), для записи облегченного архива (при необходимости длительного хранения видеоархивов в хранилищах небольшой вместимости), при просмотре видео на *Медиа Клиенте*, содержащем большое количество ячеек камер, или на дисплее с небольшим разрешением.

Использование камер с поддержкой многопоточности позволяет осуществлять сбалансированную настройку системы и решать следующие задачи:

1. Отображать видео с одной и той же камеры в разном качестве на разных *Медиа Клиентах*. Например, в одном из *Медиа Клиентов* камера отображается в небольшой ячейке. В этом случае нет необходимости увеличивать нагрузку на сеть, используя широкий поток. При этом есть возможность просматривать этот же поток в лучшем качестве (например, с большим разрешением или fps) на другом *Медиа Клиенте*, где нагрузка на сеть не является критичной или где необходимо отображать видео в высоком разрешении.
2. Отображать и записывать видео с одной и той же *Камеры* в разном качестве. В случае, если *Видеосервер* соединен с *Рабочими местами операторов* каналом со слабой пропускной способностью, становится возможным записывать видеоархив в высоком качестве, и, не перегружая сеть, передавать поток со сниженным битрейтом для просмотра видео оператором в режиме реального времени.
3. Использовать потоки с различным качеством для отображения и для анализа различными детекторами.

В SecurOS реализована поддержка одновременного использования трех потоков от *Камеры*, любой из которых может быть выбран для записи. Описанные выше задачи решаются путем распределения потоков по типам на уровне настройки *Камеры*.

9.5 Прореживание видеопотока

При любом значении параметра **FPS**, заданном в настройках объектов *Медиа Клиент*, *Камера*, *Зона* (закладка **Настройка зон**) или *Архиватор*, будет осуществляться прореживание исходного видеопотока по ключевым кадрам. Процедура прореживания выполняется в две стадии:

- На первом этапе видео прореживается до частоты опорных кадров видеопотока (I-frame или intra coded picture), определяемой как отношение собственной частоты видеопотока и значения параметра **GOP length** (**GOV length**, **Intra-Period** или **Intra-Refresh Period**) в настройках IP-камеры. Например, если собственная частота камеры 30 к/с, и при этом параметр **GOP length** принимает значение 10, то полученная в результате прореживания частота видео будет составлять 3 к/с.
- На втором этапе полученная частота сравнивается со значением параметра **FPS**, заданного в настройках объектов *Медиа Клиент*, *Камера* или *Зона*, при этом:
 - Если значение параметра **FPS** больше частоты, полученной при первичном прореживании, дальнейшее прореживание не выполняется;
 - Если значение параметра меньше, то частота итогового видео приводится к значению параметра (выполняется дальнейшее прореживание опорных кадров). Например, если частота опорных кадров видео составляет 16 к/с, а значение параметра **FPS** равно 8 к/с, в итоговом видео будет прорежен каждый второй опорный кадр.

9.6 Принципы работы зон обнаружения движения

В системе SecurOS можно определить многозонный детектор движения для разделения области охвата камеры на несколько независимых областей (зон) с разными параметрами обнаружения движения (сигнала тревоги или уровня порога обнаружения объектов).

Каждой зоне обнаружения движения соответствует объект *Зона* (см. раздел *Зона*). Зоны делятся на два типа:

- *Тревожная зона* — предназначена для подачи сигнала тревог и перевода камеры в тревожное состояние при обнаружении движения.
- *Информационная зона* — предназначена для генерации сигнала "движение обнаружено", который можно обрабатывать в скриптах для настройки дальнейшего поведения системы. При этом камера не будет переходить в тревожное состояние.

Пример. Требуется установить видеонаблюдение над территорией, внутри которой установлены ворота, а также виден ряд окон здания поверх ворот. Задача состоит в том, чтобы не подавать сигнал тревоги при использовании ворот, но подавать его, если движение обнаружено в области окон. В данном случае рекомендуется настроить два объекта *Зона*: для области возле ворот и для области вокруг окон. При этом зону для окон следует настроить как тревожную зону, а зону ворот — как информационную. Если у окон в силу условий окружающей среды различное освещение, можно создать отдельный объект *Зона* для каждого из окон и настроить параметры обнаружения индивидуально (задать разный уровень контрастности обнаруживаемого объекта).

Чтобы в зонах обнаруживалось движение, они должны быть поставлены на охрану оператором через интерфейс камеры. Можно настроить отдельные зоны так, чтобы они стояли на охране всегда (см. раздел *Зона*). В этом случае оператор не сможет снять такие зоны с охраны.

9.6.1 Создание зон

Рекомендуется создать зоны для каждого охраняемого участка в поле зрения камеры, отдельные от зоны Main.

9.7 Архивы SecurOS

В SecurOS существует два типа видеоархивов:

- *Оперативный* — архив с ограниченным сроком хранения. Такой архив создается автоматически, например, при постановке камеры на запись. По умолчанию хранится в директории ISS_MEDIA на диске, заданном в настройках объекта **Компьютер**.
- *Долговременный* — архив длительного хранения, полученный конвертацией файлов оперативного архива. По умолчанию хранится в директории ARCHIVE\ISS_MEDIA на дисках, заданных в настройках объекта **Архиватор**.

Функциональность создания и работы с Долговременным архивом доступна в редакциях SecurOS Monitoring & Control Center, SecurOS Enterprise, SecurOS Premium.

В ОС Linux функциональность создания и работы с Долговременным архивом не поддерживается.

Оперативный архив доступен по умолчанию, возможность работы с *Долговременным архивом* настраивается дополнительно (см. ниже).

Копирование *Оперативного архива* в *Долговременный* выполняется с помощью объекта **Архиватор**. Процедура запускается автоматически или с помощью объектов подсистемы автоматизации (см. **Архиватор**).

Для просмотра архива любого типа используется **Медиа Клиент**. Просмотр *Оперативного архива* доступен по умолчанию. Для просмотра *Долговременного архива* в настройках **Медиа Клиента** необходимо включить опцию **Доступ к Долговременному архиву** (см. **Закладка Экспорт и архив**).

Архив любого типа может быть экспортирован из формата SecurOS в файл стандартного формата AVI/ASF или в файл специального формата Evidence. В последнем случае файл можно зашифровать и защитить паролем (см. **Конвертер архива**). Для экспорта используется **Медиа Клиент**, в настройках которого необходимо выбрать объект **Конвертер архива** или включить возможность использования **Профилей экспорта архива** (см. **Закладка Экспорт и архив**). Конвертация может быть выполнена в том числе с использованием цифровой подписи (см. **Цифровая подпись**).

Примечание. Альтернативным образом экспортировать архив в файл стандартного формата можно с помощью утилиты **Media Export Utility** (backup.exe).

Смотри также:

- **Настройка дисков для записи.**

9.8 Локальное хранилище камеры (Edge Storage)

Edge Storage – технология, позволяющая IP-камерам записывать видеоархив в собственное хранилище. Таким хранилищем может быть встроенный модуль памяти, съемный носитель (например, SD-карта) или сетевая папка.

Для использования этой технологии в SecurOS существует два решения:

- **EdgeStorage Sync**, обеспечивающая непрерывную запись оперативного архива даже в случаях временного отсутствия связи между *Камерой* и *Видеосервером* и предназначенная для заполнения разрывов в оперативных архивах *Видеосерверов* соответствующими фрагментами локальных архивов *Камер*.

Основные варианты использования технологии **EdgeStorage Sync** в SecurOS:

- При сбоях в сети передачи данных и проблемах с оборудованием, не связанных с самой камерой (например, с картой памяти). В этом случае после восстановления работоспособности системы отсутствующие на *Видеосервере* фрагменты архива будут скопированы из хранилища камеры.
- В случаях, когда камера установлена на передвижных объектах (автобусах и т.п.), и постоянная связь с ней отсутствует. Архив копируется из локального хранилища камеры в оперативный архив SecurOS после установления связи между камерой и *Видеосервером*.
- **EdgeStorage Gate**, предназначенная для прямого доступа к архиву, расположенному в локальном хранилище камеры. Это решение используется, когда хранить архив на жестком диске невозможно. Для экспорта архива из локального хранилища *Камеры*, просматриваемого с помощью **EdgeStorage Gate**, существует ряд ограничений (см. **Ограничения экспорта архива Камеры, просматриваемого через EdgeStorage Gate**).

При возникновении ошибок, связанных с **Edge Storage**, SecurOS сообщит о них с помощью *Health Monitor* (см. **Модуль самодиагностики Health Monitor**).

9.8.1 Требования к системе

В этом разделе описаны следующие требования к системе для работы с **Edge Storage**:

- **Требования к оборудованию;**
- **Синхронизация времени;**
- **Требования к локальному хранилищу камеры.**

Требования к оборудованию

SecurOS поддерживает работу с локальным хранилищем в камерах следующих брендов:

- Axis;
- Bosch;
- Dahua;
- HikVision;
- Hanwha (Samsung);
- SecurOS Motus;
- Прочих камер и устройств, поддерживающих спецификацию ONVIF.

Для некоторых камер функционал **Edge Storage** доступен в SecurOS в том числе при работе по протоколу HTTPS.

Синхронизация времени

Для работы с **Edge Storage** требуется, чтобы время на *Видеосервере* SecurOS и камере было синхронизировано средствами NTP-сервера. На NTP-сервер накладываются ограничения:

- Ручной перевод времени не допускается.
- Переход на зимнее/летнее время не поддерживается.

В настройках камеры и компьютера должен быть выбран одинаковый часовой пояс.

Требования к локальному хранилищу камеры

Большинство камер в качестве локального хранилища используют съемные носители, такие как SD- и microSD-карты. Допустимо использование только тех карт памяти, которые рекомендованы производителем камер.

9.8.2 Настройка системы для работы с Edge Storage

Для подготовки системы к использованию функциональности локального хранилища данных выполните следующие операции:

- **настройте SecurOS;**
- **настройте камеру.**

Настройка SecurOS

Выполните следующие действия:

1. В *Дереве объектов* создайте *Устройство видеозахвата* с **Типом** и **Моделью**, соответствующими внешнему устройству.
2. В поле **IP-адрес** настроек объекта укажите IP-адрес внешнего устройства, где расположен архив, с которым необходимо работать.
3. Создайте объект *Камера*, дочерний созданному *Устройству видеозахвата*.
4. В настройках объекта *Камера* на закладке **Запись** (см. рис. 144):
 - для использования **EdgeStorage Gate** отметьте флажок **Просмотр архива, хранящегося на удаленном устройстве (EdgeStorage Gate)**;
 - для использования **EdgeStorage Sync** отметьте флажок **Восстанавливать архив из локального хранилища Камеры (EdgeStorage Sync)**.

Примечание. Параметры, необходимые для более гибкой настройки взаимодействия с **Edge Storage**, описаны в подразделе **Закладка Запись** раздела **Камера**.

Общие Поток **Запись** Аудио Детекторы PTZ Дополнительные

Режим записи: По команде и детектору движения

Длительность пред-записи: 0 с

Длительность пост-записи: 0 с

☐ Прореживание, макс. FPS: 1

☒ Полный FPS во время тревоги

Пред-запись Тревога Пост-запись t

Архив

☐ Хранить не менее: 1 дней

☐ Удалять спустя: 1 дней

Edge Storage

☐ Просмотр архива, хранящегося на удаленном устройстве (EdgeStorage Gate)

☒ Не корректировать время кадров при ускоренном воспроизведении

☐ Восстанавливать архив из локального хранилища Камеры (EdgeStorage Sync)

Не восстанавливать последние, мин: 10

Номер профиля потока: Все доступные

ОК Отмена Применить

Рис. 144. Закладка Запись (на примере камеры Axis)

Настройка камеры

Настройка записи в локальное хранилище выполняется с помощью web-интерфейса камеры.

Для настройки локальной записи выполните следующие действия (на примере одноканального сетевого видеосервера AXIS Q7411):

Внимание! Камеры некоторых брендов могут потребовать дополнительных шагов для корректной работы SecurOS с Edge Storage (см. [Особенности настройки отдельных камер](#)).

1. Откройте web-браузер и введите в адресной строке IP-адрес, присвоенный камере при подключении к сети. Для получения доступа к web-интерфейсу в окне авторизации введите логин/пароль администратора. В окне приложения откройте группу настроек **Setup** (см. рис. 145).

Рис. 145. Закладка настройки записи на встроенный носитель

2. В группе настроек выберите **Recordings** → **Continuous**.
3. На закладке **Continuous Recording**:
 - выберите канал устройства, транслирующий видео, которое необходимо записывать, для чего активируйте чек бокс **Enable**.
 - для записи на карту памяти в списке **Disk** выберите значение **SD card**.
 - в списке **Stream profile** выберите профиль потока, который необходимо записывать.

Примечания:

1. Список содержит предопределенное количество профилей потоков. Используемые по умолчанию параметры профилей могут быть изменены администратором на закладке **Video & Audio**.
2. Для обеспечения плавного проигрывания восстановленного оперативного архива и работы аналитических модулей рекомендуется, чтобы профиль потока, записываемого на камере, соответствовал профилю потока, записываемого в SecurOS.

4. Для сохранения настроек нажмите кнопку **Save**.

Особенности настройки отдельных камер**Камеры Hanwha (Samsung)**

Для корректной работы **EdgeStorage Sync** в камерах Hanwha (Samsung) выполните следующие действия:

1. Установите тип записи в значение **SD Normal**.
2. Отключите запись на карту по событиям (таким как **AlarmInput**, **MotionDetection**, **NetworkDisconnect** и другим).

Внимание! Во время настройки камер Hanwha (Samsung) будьте внимательны при изменении кодека для записи видео в локальное хранилище. Видео, сохраненное с другим кодеком, не будет восстановлено в оперативный архив SecurOS.

9.8.3 Ограничения экспорта архива Камеры, просматриваемого через EdgeStorage Gate

При экспорте локального архива *Камеры*, просматриваемого с помощью **EdgeStorage Gate**, существуют следующие ограничения:

- Экспорт звукового сопровождения невозможен.
- Факт экспорта архива из локального хранилища *Камеры* не будет учтен для последующего аудита действий пользователя SecurOS.
- При плохом соединении с *Камерой* целостность экспортируемого архива не гарантируется.
- Независимо от настроек источника в *Конверторе архива*, при экспорте фрагмента архива из локального хранилища *Камеры*, дополнить экспортируемый фрагмент из других источников (*Оперативного* или *Долговременного* архива) невозможно.
- В режиме *Привилегированного доступа* (см. **Привилегированный доступ**) экспорт из локального хранилища *Камеры* с помощью *Медиа Клиента* невозможен.

9.9 Ретроспективный поиск

Функциональность доступна в редакциях *SecurOS Enterprise*, *SecurOS Premium*.

Ретроспективный поиск в видеоархиве основан на использовании метаданных, сопровождающих видеопоток. Метаданные — это данные о том, что происходит в кадре (например, информация о движущихся объектах и их треки, скорость, атрибуты классификации, данные о качестве видеопотока и неисправностях камеры и пр.). Метаданные формируются детекторами видеоаналитики и записываются и хранятся в SecurOS в исходном виде, т. е. до обработки их алгоритмами таких детекторов. В качестве параметра ретроспективного поиска может быть использован любой из атрибутов объекта, сохраненный в метаданных.

В SecurOS метаданные формируются и сохраняются серверными видеоаналитическими детекторами (см. **Компьютерное зрение**).

Для использования функциональности в системе необходимо настроить следующие объекты:

- Если используется **Компьютерное зрение**, включите видеоаналитический детектор (см. **Настройка встроенных видеоаналитических детекторов**) и сохранение метаданных для *Камеры* в плагине Tracking Kit III (см. **Настройка плагина Tracking Kit III. Закладка Ретроспективный поиск**). Если сохранение метаданных не включено, выполнить ретроспективный поиск будет невозможно, даже если ранее метаданные сохранялись.

Внимание!

1. Сохранение метаданных выполняется только во время записи видеоархива.
2. Если запись видеоархива ведется не постоянно (например, по тревоге), для корректной работы ретроспективного поиска необходимо установить в настройках *Камеры* ненулевую **Длительность пред-записи** (см. **Закладка Запись**).

Ретроспективный поиск выполняется с помощью *Медиа Клиента* (см. **Краткое руководство пользователя SecurOS**).

9.10 Наложение водяных знаков

Чтобы предотвратить несанкционированную съемку содержимого *Медиа Клиента*, в SecurOS используются водяные знаки.

Водяной знак представляет собой надпись, которая позволяет выявить с какого именно экрана было снято видео.

Для водяных знаков можно настроить цвет и размер шрифта, его прозрачность, угол наклона блоков текста и расстояние между ними. Подробнее о создании и настройке водяных знаков см. **Водяной знак**. После создания, объект *Водяной знак* можно использовать для определенных групп *Пользователей* (см. **Права пользователя**).

Внимание!

1. Водяные знаки отображаются только поверх *Рабочей области Медиа Клиента* (см. **Краткое руководство пользователя SecurOS**).
2. Отображаемые водяные знаки не сохраняются в экспортированных из *Медиа Клиента* архивах или кадрах.
3. Для суперпользователя SecurOS с учетной записью `root` отображение водяных знаков не поддерживается.

9.11 Специальные настройки элементов видеоподсистемы

В данном разделе рассматриваются особенности настройки объектов видеоподсистемы.

9.11.1 Настройки изображения

Администратор может настраивать изображение двумя способами:

1. В окне настройки параметров объекта *Камера* (см. раздел **Камера**);
2. Через интерфейс камеры в режиме оператора (см. **Краткое руководство пользователя SecurOS**). Если объекты *Устройство видеозахвата* и *Камера* уже созданы, то администратор должен создать объекты *Рабочий стол* и *Медиа Клиент* для отображения соответствующих камер.

9.11.2 Запись архива на диск

В данном разделе рассматриваются особенности операции записи архива на жесткий диск и ее настройки:

- **Настройка дисков для записи.**
- **Горячая замена диска.**

9.11.2.1 Настройка дисков для записи

В данном разделе представлена информация о следующих настройках:

- **Минимальный объем свободного места на диске.**
- **Предоставление необходимых прав для записи архива в ОС Linux.**

Минимальный объем свободного места на диске

Чтобы избежать ситуации, когда при постоянной записи видеоархива в формате SecurOS с камер наблюдения (оперативного видеоархива) свободного места на диске не остается, рекомендуется предварительно задать обязательный размер свободного места на диске.

Это значение задается в настройках объекта *Компьютер* (см. [Архив](#)) и, по умолчанию, составляет 10% от объема диска.

Если размер свободного места диска достиг указанного предела, то система продолжает запись оперативного видеоархива на другой диск, доступный для записи. При отсутствии других свободных дисков ведется запись "по кольцу" (при этом удаление начинается с самых старых файлов).

Внимание! Для записи архивов могут быть использованы сетевые папки, размеченные как сетевые диски. В этом случае каждая сетевая папка должна использоваться только одним *Видеосервером* сети.

Предоставление необходимых прав для записи архива в ОС Linux

Для записи архива в ОС Linux определите директорию. Рекомендуется использовать для этого жесткий диск, отличный от системного, или создать отдельный логический раздел на системном диске. Предоставьте системному пользователю `securos` права на чтение и запись для выбранной директории. Для этого используйте следующие команды:

```
sudo chown securos -R <директория_для_записи_архива>
sudo chmod 744 -R <директория_для_записи_архива>
```

При необходимости в выбранную директорию для записи архива может быть примонтирован диск. Процесс разметки и монтирования дисков подробно описан в разделе [Разметка и монтирование локальных дисков в ОС Linux](#).

9.11.2.1.1 Разметка и монтирование локальных дисков в ОС Linux

Монтирование дисков в ОС Linux — это подключение диска к корневому каталогу файловой системы. Это позволяет операционной системе обращаться к файлам и папкам, хранящимся на диске, а также читать и записывать данные на него. [Разметка и форматирование](#) диска, а затем [монтирование](#) его в определенный каталог (с нужными [правами](#)) позволяет SecurOS использовать такой диск для хранения видеоархива. В данном разделе описаны разметка и монтирование дисков с помощью утилиты **GParted**.

Все описанные команды, включая запуск утилиты **GParted**, выполняются с правами суперпользователя.

Если утилита **GParted** не установлена, то для ее установки достаточно выполнить команду в терминале:

```
sudo apt install gparted
```

После установки утилиты, пиктограмма **GParted** будет отображаться в списке доступных приложений.

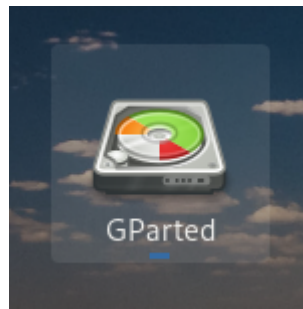


Рис. 146. Иконка утилиты GParted

Разметка и форматирование диска

Для разметки нового диска выполните следующие шаги:

1. Выберите в списке нужное устройство — диск, который будет использоваться для записи архива (в данном примере используется `/dev/sdb`).

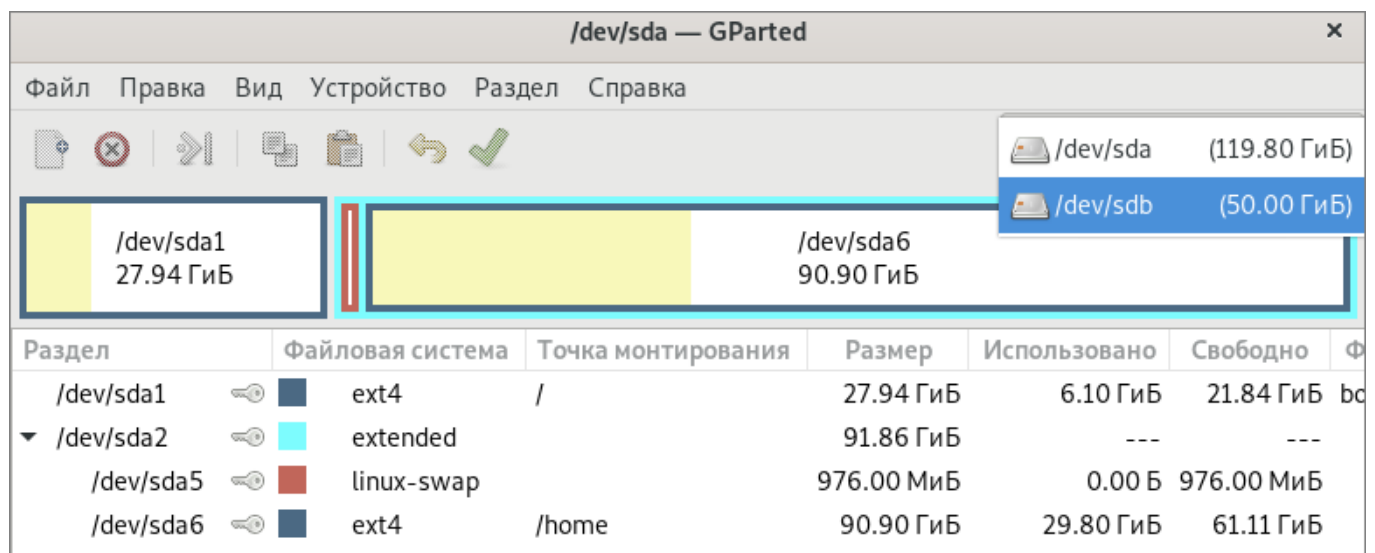


Рис. 147. Меню выбора накопительных устройств

2. После выбора нужного устройства в пункте меню **Устройство** выберите опцию **Создать таблицу разделов**.

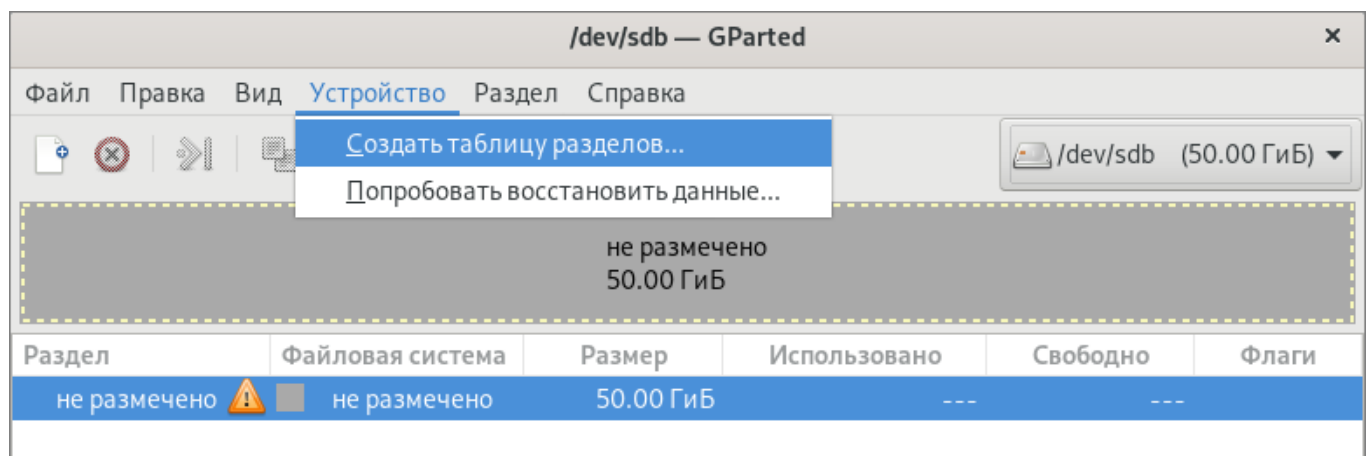


Рис. 148. Опция "Создать таблицу разделов" в пункте меню "Устройство"

3. Из предложенных типов таблиц разделов выберите `gpt` и примените изменения.

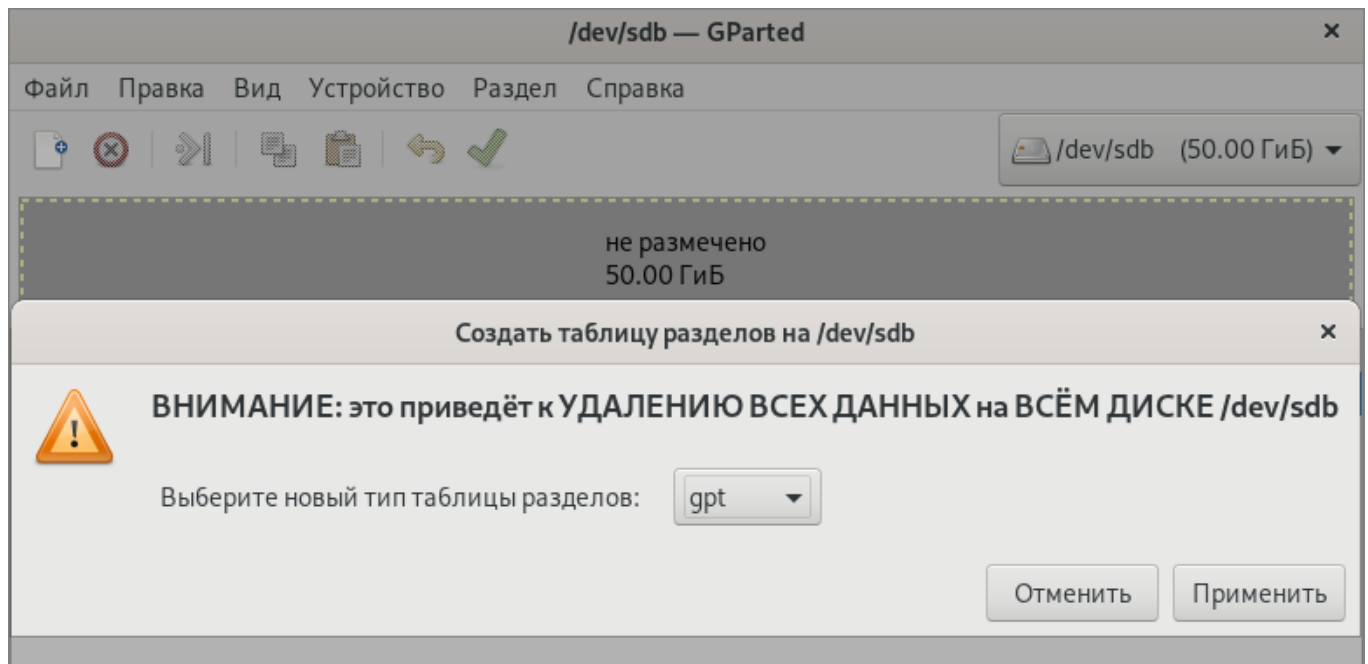


Рис. 149. Окно выбора типа таблицы разделов

4. В пункте меню Раздел выберите опцию Новый.

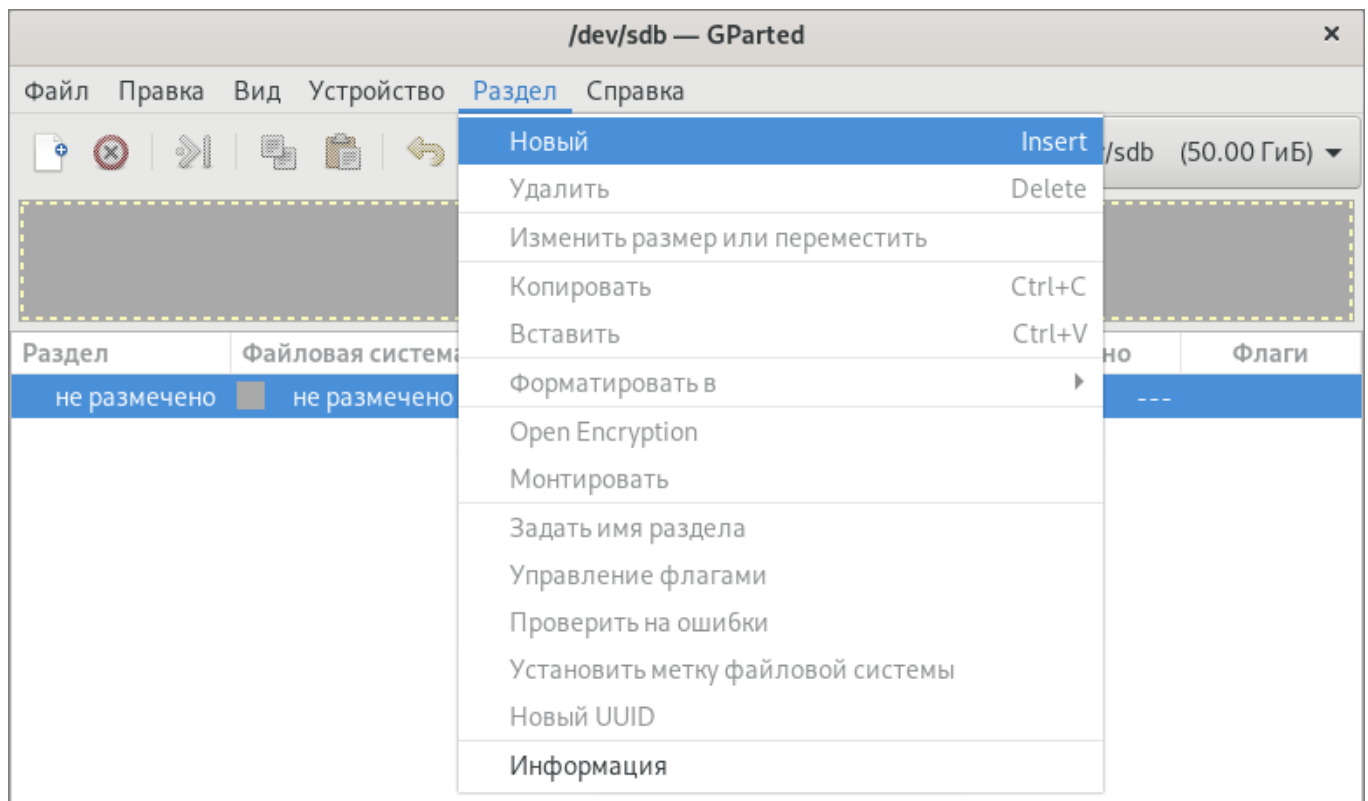


Рис. 150. Опция "Новый" в пункте меню "Раздел"

5. Укажите размер нового раздела (по умолчанию будет использовано все свободное место на диске), файловую систему и нажмите кнопку Добавить.

Внимание! В ОС Linux возможна работа со следующими файловыми системами: ext3, ext4, cifs.

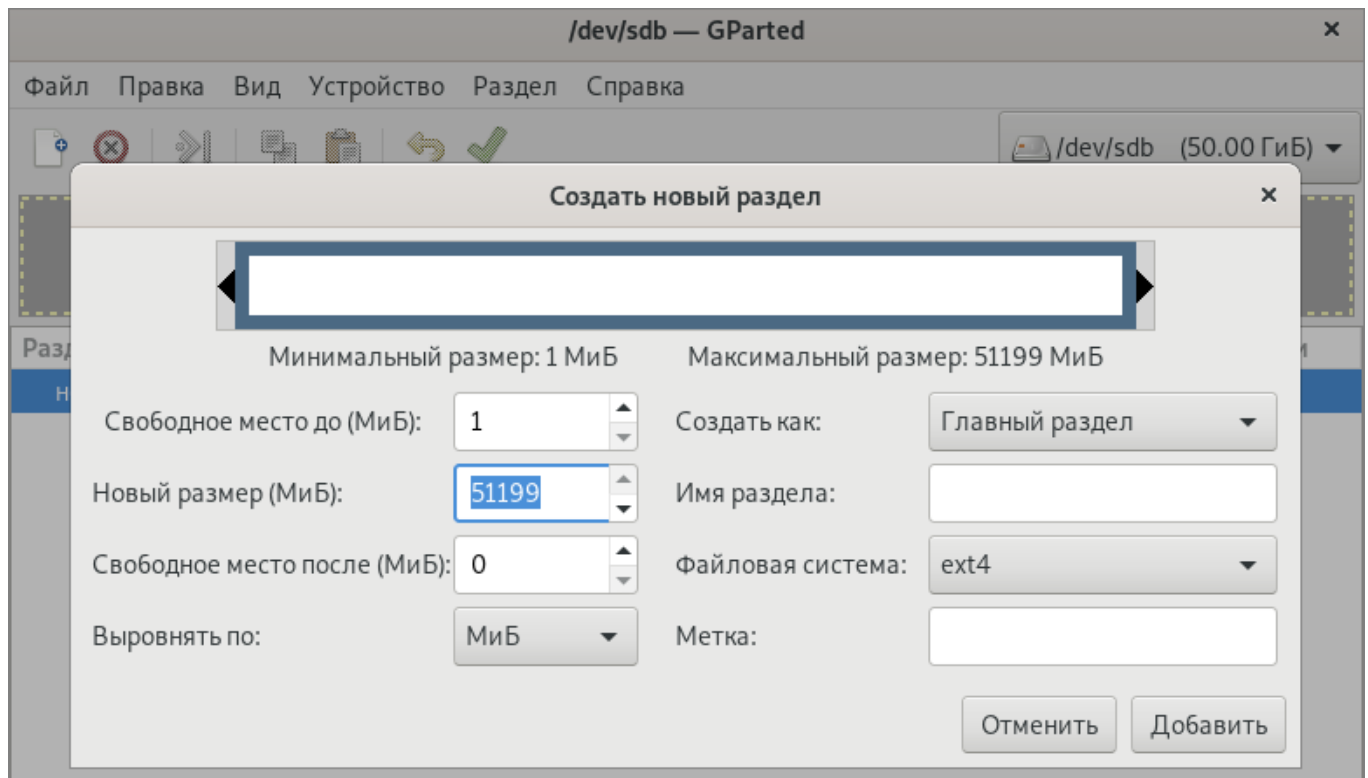


Рис. 151. Окно создания нового раздела

6. Нажмите на кнопку Применить все операции (зеленая галочка) для применения всех ранее выполненных операций.

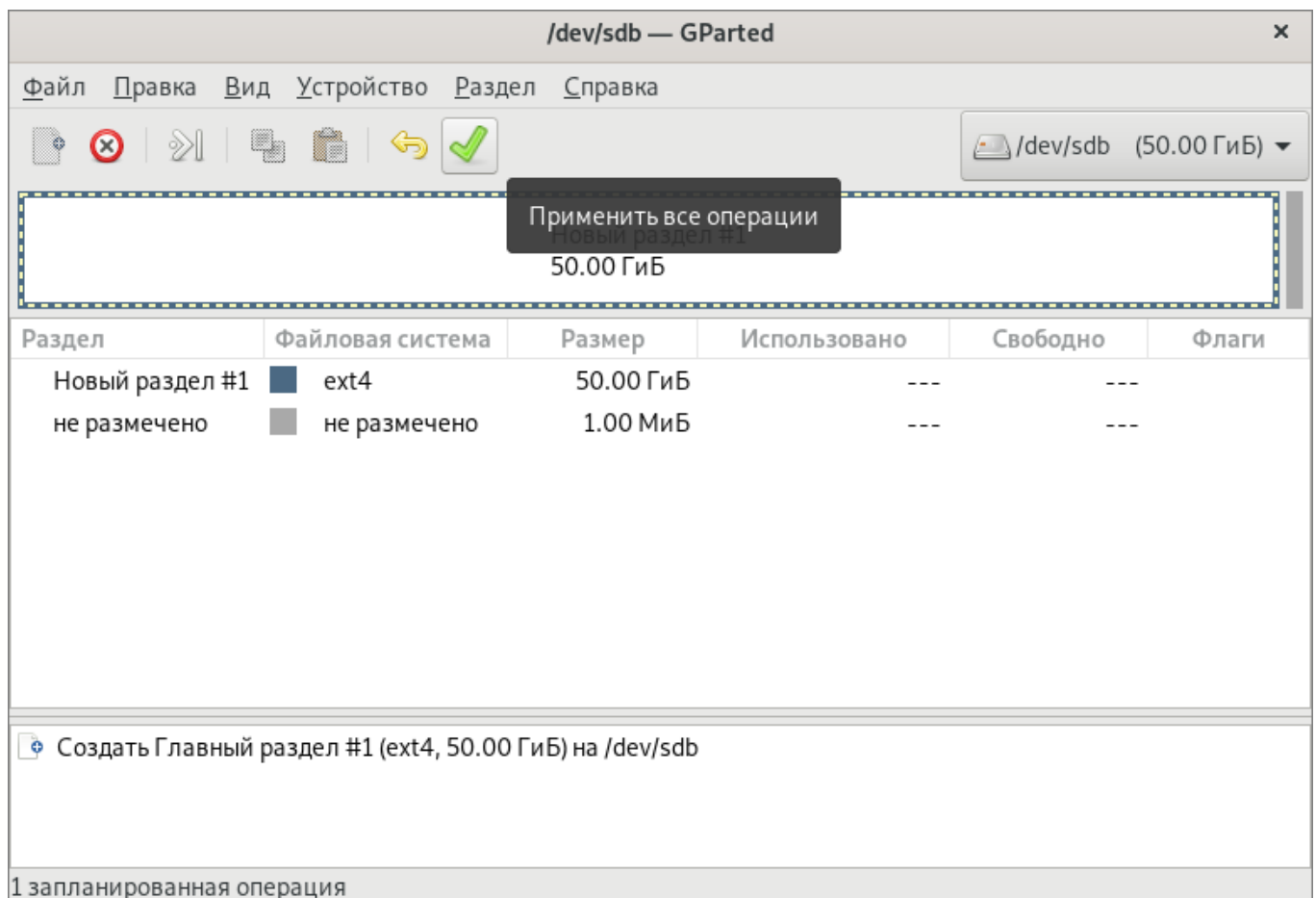


Рис. 152. Опция "Применить все операции"

После того как все выбранные операции будут проделаны, в случае успеха будет выведено сообщение об успешном выполнении данных операций (см. рис. 153).

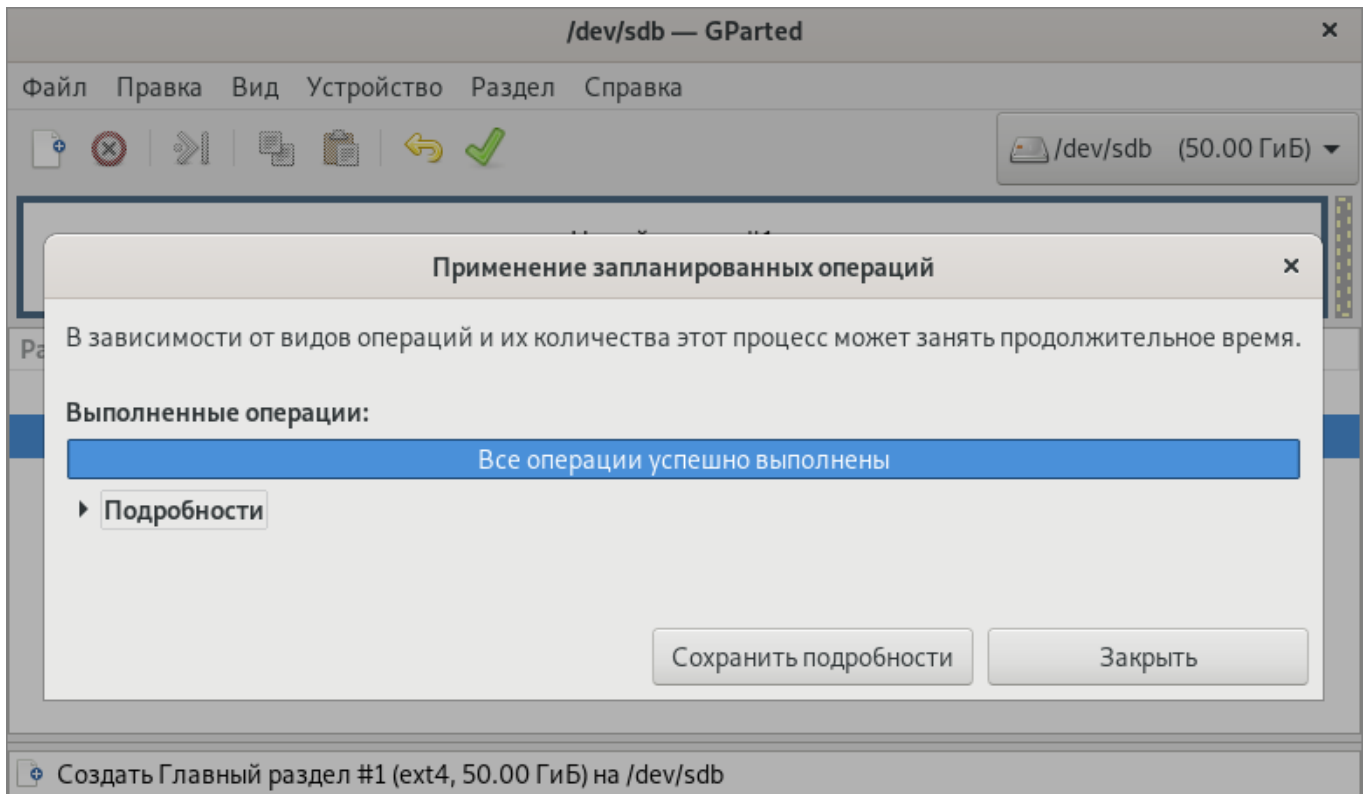


Рис. 153. Сообщение об успешном выполнении всех операций

В окне Применение запланированных операций нажмите на кнопку Закрыть и в столбце Раздел запомните название с номером созданного раздела – они пригодятся в процессе монтирования диска (см. рис. 154).

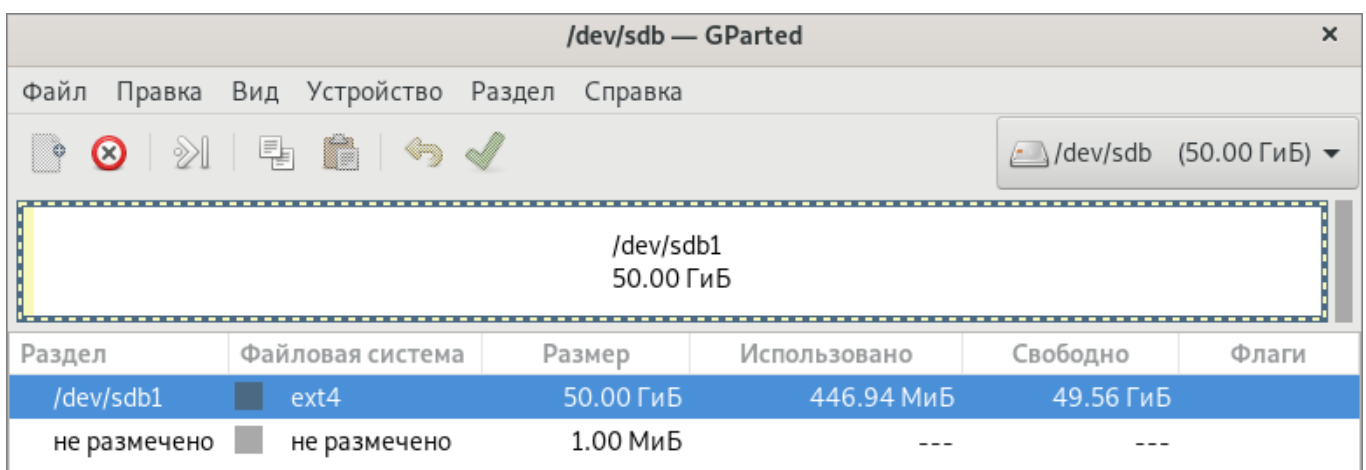


Рис. 154. Название и номер созданного раздела

Монтирование диска

После успешной разметки диска, нужно примонтировать его в директорию, в которую планируется записывать архив. Если директория не была предварительно создана, воспользуйтесь командой `mkdir`. Например:

```
sudo mkdir /home/video/
```

Чтобы примонтировать диск к выбранной директории, выполните следующие шаги:

1. В текстовом редакторе откройте файл `fstab` с правами суперпользователя. Например, с помощью редактора `nano` и команды:

```
sudo nano /etc/fstab
```

2. Добавьте в файл новую запись в следующем формате:

```
/dev/<имя и номер раздела> <путь до папки для записи видео> ext4 defaults 0 0
```

Например:

```
/dev/sdb1 /home/video ext4 defaults 0 0
```

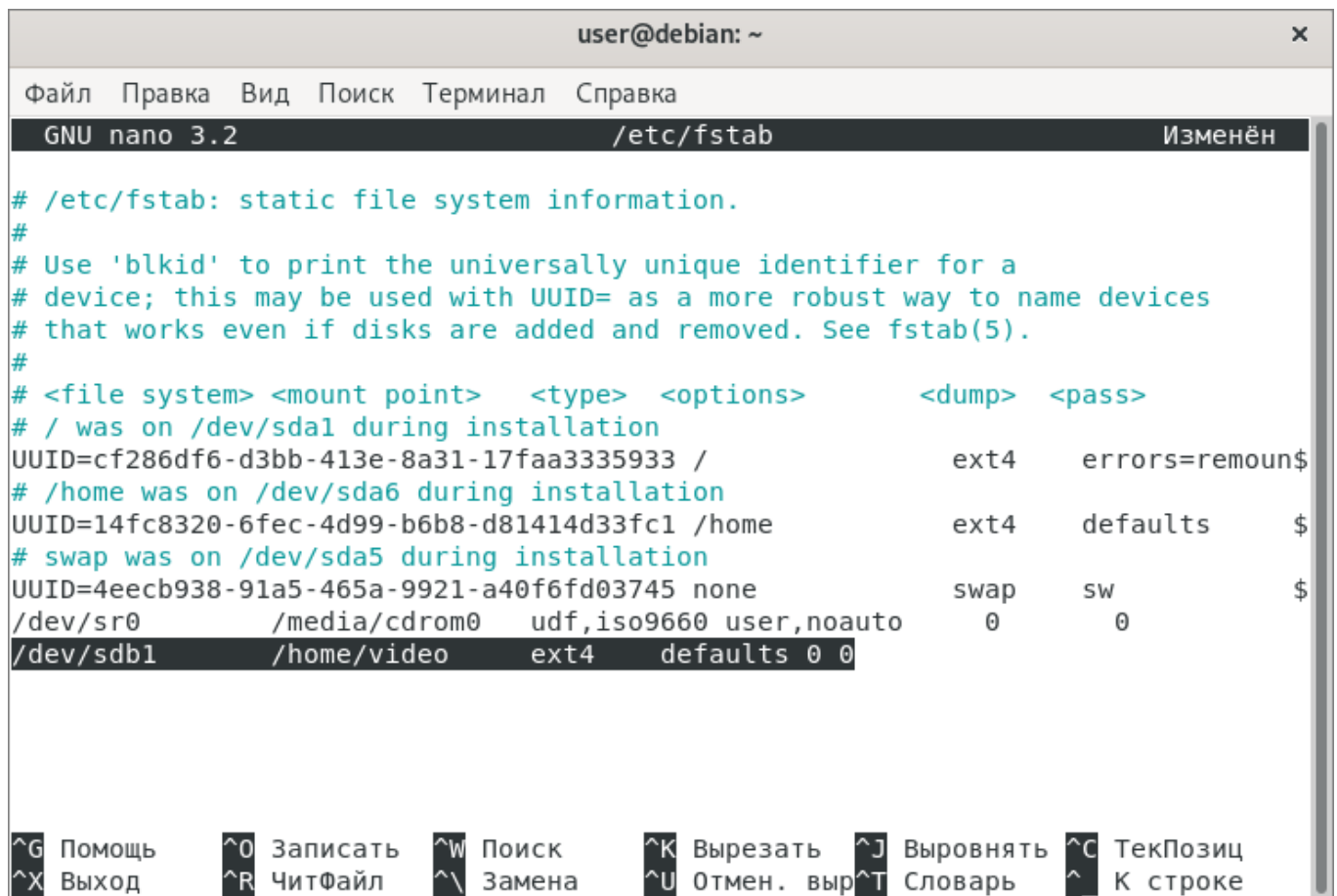


Рис. 155. Новая запись в файле `fstab`

3. Сохраните изменения (**Ctrl+O** для редактора `nano`).
4. Выполните команду:

```
mount /dev/<имя и номер раздела>
```

Например:

```
sudo mount /dev/sdb1
```

Предоставление прав

Предоставьте системному пользователю `securos` права на чтение и запись для выбранной директории (подробнее см. [Предоставление необходимых прав для записи архива в ОС Linux](#)).

Если все шаги были выполнены успешно, то в SecurOS появится новый раздел для записи (см. рис. 156).

Добавить новую директорию [X]

Внимание! Для долговременного и оперативного архивов не рекомендуется использовать один и тот же диск или сетевую директорию.

☒ Диск / (20.43 ГБ свободно из 27.33 ГБ) ⓘ

☐ Сетевой путь /home/video/ (46.4 ГБ свободно из 48.91 ГБ)

Пользователь: Пароль:

☐ iSCSI-диск

Установить права

Видео: Чтение и Запись **Аудио:** ⓘ Запрещено

Запись архива

Укажите объем зарезервированного дискового пространства. При сокращении свободного дискового пространства до указанного значения, для записи архива будет использоваться любой свободный диск. При отсутствии свободных дисков запись архива будет вестись "по кольцу".

Минимальное свободное место на диске: 10% (2.7 ГБ)

Рис. 156. Окно добавления новой директории в SecurOS

Примечание. После выполнения всех операций рекомендуется закрыть утилиту **GParted**.

9.11.2.2 Горячая замена диска

Горячая замена диска — это процесс отключения директории (носителя) для работы с архивом с одним физическим диском и подключение ее обратно под тем же именем, но с другим физическим диском. Например, отключается внешний жесткий диск и подключается другой с таким же буквенным обозначением или монтируется другой диск в уже ранее созданную точку монтирования.

Ниже представлена информация о следующих операциях по горячей замене диска:

- **Горячая замена диска Оперативного архива.**
- **Горячая замена диска Долговременного архива.**
- **Горячая замена диска в кластере.**

Горячая замена диска Оперативного архива

Для горячей замены диска *Оперативного архива* выполните следующие действия:

1. Замените физический диск.
2. В *Дереве объектов SecurOS* выберите необходимый объект *Компьютер*.
3. Удалите директорию с замененным диском (подробнее см. подраздел **Удаление директории** раздела **Архив**).
4. Нажмите кнопку **Применить**.
5. Заново добавьте этот диск (подробнее см. подраздел **Добавление директории** раздела **Архив**).
6. Нажмите кнопку **Применить**.

Горячая замена диска Долговременного архива

Для горячей замены диска *Долговременного архива* выполните следующие действия:

1. Замените физический диск.
2. В *Дереве объектов SecurOS* выберите необходимый объект *Архиватор*.
3. Удалите директорию с замененным диском (подробнее см. подраздел **Удаление директории для записи архива** раздела **Архиватор**).
4. Нажмите кнопку **Применить**.
5. Заново добавьте этот диск (подробнее см. подраздел **Добавление директории для записи архива** раздела **Архиватор**).
6. Нажмите кнопку **Применить**.

Горячая замена диска в кластере

Для горячей замены локального диска в кластере выполните следующие действия:

1. Замените физический диск.
2. Запустите утилиту **Server Manager**.
3. Выберите *Хост* кластера в списке, нажмите кнопку **Расширенные настройки** и выберите пункт **Настройки локальных дисков** (см. подраздел **Настройка / просмотр локальных дисков для хранения архива** раздела **Расширенные настройки кластера**).
4. В открывшемся окне **Хранить архив на локальных дисках** снимите флажок с требуемого диска и нажмите кнопку **ОК**.
5. Повторно откройте окно **Хранить архив на локальных дисках**, отметьте флажок для требуемого диска и нажмите кнопку **ОК**.

9.12 Описание объектов

Видеоподсистема представлена следующими классами объектов:

- **Системные объекты.**
- **Объекты пользовательского интерфейса.**

9.12.1 Системные объекты

К системным относятся следующие объекты видеоподсистемы:

- Устройство видеозахвата.
- Камера.
- Детектор расфокусировки.
- Раскладка.
- Вид.
- Зона.
- Световой детектор.
- Конвертер архива.
- Профиль экспорта архива.
- Архиватор.
- Image Processor.
- RTSP-сервер.
- ONVIF-сервер.

9.12.1.1 Устройство видеозахвата

Объект представляет IP-камеру, включенную в сеть TCP/IP.

Родительский объект — *Компьютер\группа Устройства (Камеры и Микрофоны)*.

Окно настройки параметров, в зависимости от **Типа** и **Модели** устройства, может содержать следующие закладки:

- Закладка **Подключение**.
- Закладка **Прошивка**.

9.12.1.1.1 Закладка Подключение

В таблице 26 представлены типовые параметры *Устройств видеозахвата*.

Рис. 157. Окно настройки параметров объекта Устройство видеозахвата.
Закладка Подключение

Примечание. На рис. 157 представлены параметры, доступные для устройства Samsung SNB-C7478. Отображение таких параметров как **Протокол**, **PCI канал** и **Формат** зависит от интеграции в SecurOS выбранного **Типа** и **Модели** устройства.

Таблица 26. Параметры объекта Устройство видеозахвата. Закладка Подключение

Параметр	Описание
Тип	Выберите значение, соответствующее марке устройства.
	Внимание! В ОС Linux тип устройства Player AVI не поддерживается.
	Примечание. Тип Virtual устанавливается для эмуляции камер, используется при тестировании настроек системы.
Модель	Выберите модель <i>Устройства видеозахвата</i> заданного Типа (если доступно).
Протокол	Выберите версию протокола передачи данных, которую использует подключаемая камера.
	Примечание. Параметр отображается в случае, если в SecurOS поддерживается несколько версий интеграции камеры заданного Типа и Модели , соответствующих различным протоколам передачи данных и API.

PCI канал	Выберите уникальный номер PCI-канала для Типа Virtual или Player AVI.
Формат	Выберите из списка формат видеосигнала в зависимости от типа устройства: H.264, MPEG4, MJPEG, PAL, SECAM и т.д.

IP-адрес

Укажите `<host>[:<port>]` из полного URL устройства.

Значение `<host>` допускается указывать в виде:

- IP-адреса, например, `172.16.1.12` — для устройств любого **Типа**, кроме `Virtual`.
- полного доменного имени, например, `axis.network.iss` — для устройств с **Типом** `Axis` и `Generic RTSP`.
- краткого доменного имени, например, `axis` — для устройств с **Типом** `Axis` и `Generic RTSP`.

Значение `[:<port>]` является опциональным и зависит от протокола соединения с камерой, который задается в настройках самой камеры с помощью web-интерфейса.

Если в настройках камеры задан протокол **HTTP**, номер порта может быть задан в виде:

`[:<http_port>][:<rtsp_port>]`, где:

- `[:<http_port>]` — номер HTTP-порта;
- `[:<rtsp_port>]` — номер RTSP-порта для получения видео по RTSP.

Например:

- `127.0.0.1:8080:554` — указан HTTP-порт 8080 и RTSP-порт 554.
- `127.0.0.1::554` — HTTP-порт не указан, указан RTSP-порт 554.

Если в настройках камеры задан протокол **RTSP**, номер порта может быть задан в виде:

`[:<rtsp_port>]`, где:

- `[:<rtsp_port>]` — номер RTSP-порта для получения видео по RTSP.

Например:

- `127.0.0.1:554` — указан RTSP-порт 554.

Для устройства с типом `Generic RTSP` в поле также допускается указывать:

- полный URL устройства — `<host>[:<port>]/<URL path>[?<параметры>]`.

	• только значение <host>[:<port>] из полного URL устройства. В этом случае прочие компоненты URL (/<URL path>[?<параметры>]) должны быть указаны в настройках <i>Камеры</i> (см. Закладка Поток, параметр Путь). Разделитель (/) может быть указан как в параметре IP-адрес, так и в параметре Путь в настройках <i>Камеры</i>.
Пользователь	Укажите имя пользователя для соединения с IP-камерой. Используйте стандартное значение securos или укажите имя для доступа к IP-камере с заданным адресом.
Пароль	Оставьте значение поля по умолчанию или введите пароль для доступа к IP-камере с заданным адресом. Внимание! Пароль виден при вводе, но при повторном открытии окна настройки параметров в поле отображаются символы "*" (количество символов не равно количеству букв в пароле).
Просмотр	Ссылка, размещенная справа, позволяет быстро открыть web-страницу настроек сетевой камеры в браузере Internet Explorer. Если на заданы параметры IP-адрес, Пользователь и Пароль, ссылка неактивна. Примечание. Поля окна авторизации браузера IE автоматически заполняются значениями Пользователь и Пароль, заданными в настройках данного <i>Устройства видеозахвата</i>.
Использовать безопасное соединение (HTTPS)	С помощью данного параметра задается тип соединения с камерой. Чтобы использовать защищенное соединение с камерой: • отметьте флажок; • с помощью web-интерфейса в собственных настройках камеры выберите для пользователя HTTPS-протокол и установите доверенный сертификат шифрования. Внимание! Если не выполнено одно из условий, защищенное сетевое соединение с камерой установлено не будет. Примечания: 1. Параметр доступен в зависимости от выбранного Типа устройства. За список поддерживаемых устройств обращайтесь в Службу технической поддержки компании Intelligent Security Systems. 2. Если отмечен, то для передачи видеопотока в настройках объекта <i>Камера</i> для параметра Протокол необходимо выбрать значение RTSP поверх HTTPS (см. Закладка Поток). 3. Если отмечен, соединение с камерой всегда будет осуществляться по протоколу TCP, независимо от флага RTP поверх RTSP (TCP), см. Закладка Поток.

9.12.1.1.2 Закладка Прошивка

На данной закладке (см. рис. 158) предоставлена возможность обновления встроенного программного обеспечения устройства (прошивки).

Примечание. Возможность обновления прошивки средствами SecurOS предусмотрена только для устройств типа ONVIF.

Внимание! Обновление прошивки может привести к неисправности устройства. За дополнительной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems (см. раздел [Обращение за технической поддержкой](#)).

Рис. 158. Окно настройки параметров объекта Устройство видеозахвата. Закладка Прошивка

Таблица 27. Параметры объекта Устройство видеозахвата. Закладка Прошивка

Параметр	Описание
Прошивка	Нажмите кнопку Определить для вывода в данном поле информации о текущей версии прошивки.
Обновление прошивки	
Файл прошивки	Укажите путь к файлу прошивки. Для запуска процесса обновления прошивки нажмите кнопку Обновить. Рекомендуется подождать завершения процесса перед закрытием этого окна, чтобы убедиться, что обновление прошивки прошло успешно. Обновление прошивки доступно только в случае, если системе удалось получить информацию о ее текущей версии (см. Прошивка).

9.12.1.1.3 Active Camera Recorder (AC Recorder)

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*.

В ОС **Linux** функциональность не поддерживается.

Устройство видеозахвата типа Active Camera Recorder (далее AC Recorder) предназначено для получения **Потока для записи** активной Камеры одного из Компьютеров сети безопасности. Полученный видеопоток отображается в стандартной ячейке дочерней Камеры в режиме реального времени и может быть записан в архив.

Для настройки AC Recorder'a выполните следующие действия:

1. Войдите в режим администрирования.
2. В *Дереве объектов* выберите объект *Компьютер*, с которым будет связано добавляемое устройство.
3. В группе *Устройства* (Камеры и Микрофоны) создайте дочерний объект *Устройство видеозахвата*.
4. В окне **Параметры создаваемого объекта** в поле **Тип** выберите значение AC Recorder.
5. В поле **Компьютер** окна настройки параметров созданного объекта задайте IP-адрес или DNS-имя Компьютера, с которого необходимо получать поток активной камеры.
6. Создайте объект *Камера*, дочерний созданному *Устройству видеозахвата*.
7. Если *Медиа Клиент* данного Компьютера находится в режиме **Работать только с указанными Камерами**, добавьте созданную *Камеру* в список указанных камер. Если *Медиа Клиент* находится в режиме **Работы со всеми камерами**, созданная *Камера* добавится автоматически.

9.12.1.2 Камера

Объект представляет физическую видеокамеру или другой видеоисточник.

Родительский объект — **Устройство видеозахвата**.

Окно настройки параметров, в зависимости от **Типа** и **Модели** камеры, может содержать следующие закладки:

- Закладка **Общие**.
- Закладка **Поток**.
- Закладка **Запись**.
- Закладка **Аудио**.
- Закладка **Детекторы**.
- Закладка **PTZ**.
- Закладка **Дополнительные**.

Для каждой из закладок в соответствующих разделах описаны общие для всех Камер параметры, не зависящие от **Типа** и **Модели** устройства.

Кроме общих параметров, интегрированные в SecurOS камеры могут иметь собственные настройки. Эти настройки зависят от **Типа** и **Модели** камеры и управляют дополнительными функциональными возможностями камер. Описание таких параметров для каждой закладки можно найти в конце соответствующего раздела.

Примечание. В данном документе описаны наиболее важные из дополнительных параметров. Краткое описание прочих дополнительных параметров выводится во всплывающей подсказке в окне настройки параметров *Камеры*.

9.12.1.2.1 Закладка Общие

В таблице 28 представлены типовые параметры камер. Параметры, зависящие от **Типа** и **Модели** камеры, описаны в таблице 29.

Рис. 159. Параметры объекта Камера. Закладка Общие

Таблица 28. Параметры объекта Камера. Закладка Общие

Параметр	Описание
Координаты	Задайте координаты камеры (GPS, ГЛОНАСС и т. д.) в любом формате. Например, 55.792461, 37.637515.
	Примечание. Координаты камеры будут передаваться наряду с прочими параметрами настройки объекта при их запросе из внешней системы с помощью интерфейса REST API . Данные будут переданы в том виде, в каком они заданы в настройках объекта.
Канал	Выберите из списка номер канала камеры.

Поворотное устройство	Параметр определяет возможность управления нативной телеметрией данной <i>Камеры</i> (см. Настройка телеметрии). Выберите одно из следующих значений: • Использовать — позволяет оператору управлять телеметрией в окне <i>Медиа Клиента</i>. • Не использовать — отключает возможность управления телеметрией. Параметр принимает это значение по умолчанию. • Управлять только зумом — используется, если камера оснащена моторизированным объективом.
Дворник	Если камера оснащена устройством дистанционной очистки стекла, выберите объект, с помощью которого осуществляется управление <i>Дворником</i>. Примечание. Подробнее см. раздел Настройка системы для работы с Дворниками и Омывающими устройствами. По умолчанию принимает значение Не использовать, отключающее возможность управления дворником. Если камера оснащена встроенным дворником, выберите значение Встроенный. При этом параметр Поворотное устройство автоматически примет значение Использовать, которое нельзя будет изменить. Примечание. Чтобы оператор мог использовать данную функциональность, требуется наличие прав пользователя на соответствующую камеру не ниже уровня Управление.
Отображение	Параметр определяет формат отображения видео в ячейке <i>Камеры</i> во всех <i>Медиа Клиентах</i> системы безопасности SecurOS. При этом для каждого <i>Медиа Клиента</i> формат отображения видео для выбранной <i>Камеры</i> может быть изменен локально с помощью элементов управления ячейки данной <i>Камеры</i> (см. Краткое руководство пользователя SecurOS). Возможные значения: • Сохранять пропорции — при отображении видео будет использоваться исходный формат кадра. Является значением по умолчанию. • Во всю ячейку — при отображении видео изображение занимает всю ячейку <i>Медиа Клиента</i>. • Привести к 4:3 — при отображении видео будет масштабироваться до соотношения сторон 4:3.

Размер буфера	Задайте размер буфера видео- и аудиокадров при работе в режиме буферизации живого видео, в мс. Буферизация позволяет сгладить неровности воспроизведения видео при недостаточной скорости передачи видеок кадров по сети и циклические запаздывания сопровождающего аудио (полученного от связанных <i>Микрофонов</i>) или его обрывы при воспроизведении в <i>Медиа Клиенте</i>. Однако, при включенной буферизации, живое видео в <i>Медиа Клиенте</i> будет воспроизводиться с временной задержкой не менее заданного размера буфера. Диапазон возможных значений: [0; 5000]. Внимание! После задания параметра включите режим буферизации видео в настройках требуемого <i>Медиа Клиента</i> (см. Закладка Камеры).

Таблица 29. Опциональные параметры закладки Общие

Параметр	Описание
Использовать только дайджест-аутентификацию	Отметьте флажок, чтобы использовать шифрование при отправке параметров авторизации.
Омывающее устройство	Если камера оснащена омывающим устройством, выберите объект, с помощью которого осуществляется управление <i>Омывающим устройством</i>. Примечание. Подробнее см. раздел Настройка системы для работы с Дворниками и Омывающими устройствами. По умолчанию принимает значение Не использовать, отключающее возможность управления омывающим устройством. Если камера оснащена встроенным омывающим устройством, выберите значение Встроенное. Примечания: 1. Функциональность доступна только для некоторых моделей камер. За списком поддерживаемых устройств обращайтесь в Службу технической поддержки компании Intelligent Security Systems. 2. Чтобы оператор мог использовать данную функциональность, требуется наличие прав пользователя на соответствующую камеру не ниже уровня Управление. 3. Параметры процедуры мойки определяются собственными настройками камеры, выполняемыми через web-интерфейс устройства.

Освещение

Если камера оснащена встроенной лампой освещения, выберите из выпадающего списка значение **Встроенное** чтобы включить возможность управления такой лампой. При этом параметр **Поворотное устройство** автоматически примет значение **Использовать**, которое нельзя будет изменить.

По умолчанию принимает значение **Не использовать**, отключающее возможность управления встроенной лампой.

Некоторые камеры позволяют задавать интенсивность освещения. Чтобы задать интенсивность, выберите требуемое значение из списка:

- Включить 1 LED группу.
- Включить 2 LED группу.
- Включить все LED группы.

При выборе определенного значения для освещения будут использоваться только 1-ая, 2-ая или все группы светодиодов одновременно.

Примечание. Чтобы оператор мог использовать данную функциональность, требуется наличие прав пользователя на соответствующую камеру не ниже уровня **Управление**.

9.12.1.2.2 Закладка Поток

В таблице 30 описаны типовые параметры камер. Параметры, зависящие от **Типа** и **Модели** камеры, описаны в таблице 31.

Общие Поток Запись Аудио Детекторы PTZ Дополнительные

Камера **Virtual default** поддерживает работу с несколькими видеопотоками. Доступные настройки Потоков соответствуют значениям в Веб-интерфейсе настроек камеры.

☒ Поток 1
☐ Поток 2
☐ Поток 3

Использование потоков

Для записи видео: Поток 1

Для детектора движения: Поток 1

Для отображения видео

Низкое разрешение: Поток 1

Базовый: Поток 1

Высокое разрешение: Поток 1

OK Отмена Применить

Рис. 160. Параметры объекта Камера. Закладка Поток

Внимание!

1. На закладке представлены типовые параметры настройки камеры, поддерживающей многопоточность.
2. Для камер, не поддерживающих многопоточность, набор параметров закладки определяется типом родительского *Устройства видеозахвата* или закладка отсутствует.

Таблица 30. Параметры объекта Камера. Закладка Поток

Параметр	Описание
Поток 1 (блок активации режима настройки и использования Потока 1). По умолчанию активирован.	
<i>Примечание.</i> Настройки блоков Поток 1 , Поток 2 и Поток 3 одинаковы и зависят от типа и модели <i>Устройства видеозахвата</i> .	
Поток 2 (блок активации режима настройки и использования Потока 2). Отметьте флажок для возможности выбора данного потока в блоке Использование потоков .	
Поток 3 (блок активации режима настройки и использования Потока 3). Доступен в случае, если активирован параметр Поток 2 . Отметьте флажок для возможности выбора данного потока в блоке Использование потоков .	
Использование потоков	
Для записи видео	Выберите из выпадающего списка поток для записи видеoarхива.
Для детектора движения	Выберите из выпадающего списка поток, который будет анализироваться детектором движения.
Для отображения видео	
Низкое разрешение	Выберите из выпадающего списка поток низкого разрешения.
Базовый	Выберите из выпадающего списка базовый поток.
Высокое разрешение	Выберите из выпадающего списка поток высокого разрешения.

Внимание! Для подключаемых IP-камер и видеосерверов не рекомендуется использовать значения параметра **GOP (GOV)**, превышающие 32 кадра или 2 секунды. Настройка параметра возможна через web-интерфейс IP-камер. Для некоторых типов *Устройств видеозахвата* данная настройка доступна на закладке **Поток** окна настройки параметров объекта *Камера*.

Ниже приведены некоторые рекомендации по выбору потоков.

1. В качестве **Потока высокого разрешения** рекомендуется указать поток, имеющий наибольшее разрешение, например, для отображения видео на *Медиа Клиенте* в ячейках большого размера (например, в раскладках 1*1 или 2*2), либо для отображения на *Мониторе видеостены*.

2. В качестве **Потока низкого разрешения** рекомендуется указать поток с наименьшим разрешением, которое допускается требованиями к системе безопасности. Такой поток можно использовать для отображения на *Медиа Клиенте* в ячейках раскладок 5*5 и выше.
3. В качестве **Базового потока** рекомендуется указать поток с разрешением, достаточным для отображения видео в ячейках среднего размера. Например, в раскладках 3*3, 4*4 на *Медиа Клиентах Рабочих мест операторов*, или в раскладках 4*4, 5*5 на *Мониторах видеостены*.
4. При указании **Потока для записи** выберите поток, который отвечает требованиям к качеству архивного видео в системе безопасности. При выборе потока необходимо учитывать, что чем шире поток, тем больше места на диске занимает архив.

Внимание! В текущей реализации все *Программные детекторы* и *Интеллектуальные Модули* (SecurOS Auto, SecurOS Transit, SecurOS FaceX) работают с **Потоком для записи**. Таким образом, при выборе **Потока для записи** необходимо учитывать требования и рекомендации к настройке видео, предъявляемые теми Модулями и Детекторами, совместно с которыми предполагается использование данной *Камеры*.

В случае, если возникает необходимость записи потока высокого качества, а *Видеосервер* соединен с *Рабочими местами операторов* каналом с низкой пропускной способностью, не указывайте поток, выбранный в качестве **Потока для записи** ни в одном из типов **Потоков для отображения**. В этом случае поток высокого качества не будет передаваться за пределы *Видеосервера* в режиме реального времени (только при просмотре архивов), что значительно снизит нагрузку на канал связи.

Таблица 31. Опциональные параметры закладки Поток

Параметр	Описание
Опции работы с потоками (см. рис. 161).	
Использовать настройки камеры	При включенной опции потоку <i>Камеры</i> будет сопоставлен поток, соответствующий текущим настройкам камеры в web-интерфейсе. По умолчанию включена.
Профиль	С помощью этого поля каждому из потоков <i>Камеры</i> можно сопоставить один из потоков, настроенных на камере с помощью web-интерфейса. Выберите из списка или введите вручную название профиля, соответствующее потоку, настроенному в web-интерфейсе камеры. Для <i>Устройств видеозахвата</i> с типом Thermal (тепловизор) параметр может принимать следующие значения: • Термометрический — поток необработанных данных, полученных от тепловизора камеры. В ячейке камеры выводится термограмма объекта. Данный поток используется для дальнейшей обработки модулями видеоаналитики SecurOS. • Оптический — опциональный (не термометрический) поток камеры, без данных тепловизора. • Визуально-информационный — термометрический поток, дополненный вспомогательными данными.

Параметр	Описание
Поток	У некоторых моделей камер флажок Поток (см. таб. 30) дополнен полем Поток. С помощью этого поля каждому из потоков <i>Камеры</i> можно сопоставить один из следующих исходных потоков, настроенных на камере с помощью web-интерфейса: • Поток (1) – Поток (4). • MJPEG. Внимание! Для камер с типом <i>Устройства видеозахвата</i> Panasonic RTSP Stream при выборе значения MJPEG потоку <i>Камеры</i> будет сопоставлен первый из JPEG-потоков, настроенных на камере с помощью web-интерфейса.
Путь	Укажите компоненты <URL path>[?<параметры>] из полного URL устройства для получения RTSP-потока. Например, если полный URL имеет вид 172.16.16.250/axis-media/media.amp?camera=1 то в поле Путь следует задать значение /axis-media/media.amp?camera=1 Внимание! Только для устройства с Типом Generic RTSP. См. также Устройство видеозахвата, параметр IP-адрес.
Идентификатор Камеры во внешнем устройстве	Задайте идентификатор, присвоенный <i>Камере</i> в настройках внешнего устройства. Используется для просмотра архивного видео камер внешнего устройства в SecurOS с помощью <i>EdgeStorage Gate</i>.
Режим совместимости диапазонов	Параметр влияет на низкоуровневые механизмы SecurOS. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.
Протокол	Параметр определяет тип соединения с камерой. Возможные значения: • RTP поверх UDP — для взаимодействия с камерой будет использоваться протокол UDP. • RTP поверх TCP — для взаимодействия с камерой будет использоваться протокол TCP. • RTSP поверх HTTP/HTTPS — для взаимодействия с камерой будет использоваться незащищенное/защищенное TCP-соединение с туннелированием. Внимание! RTSP поверх HTTPS-соединение будет установлено только в том случае, если помощью web-интерфейса в собственных настройках камеры установлен доверенный сертификат шифрования и для пользователя выбрано соединение по HTTPS. В настройках <i>Устройства видеозахвата</i> должен быть установлен флаг Использовать безопасное соединение (HTTPS).

Параметр	Описание
Использовать поток по запросу	Отметьте флажок для передачи потока живого видео в систему только при наличии в системе потребителя этого потока. Потребитель потока существует в системе при просмотре живого видео, записи видеоархива, при работе детекторов сервисной аналитики (детектор движения, расфокусировки, засвечивания и т. п.) или видеоаналитических детекторов. Параметр предназначен для управления видеопотоком при работе в сетях с низкой пропускной способностью.
Мультикаст, группа параметров (подробнее см. раздел Мультикаст)	
Включить мультикаст	Отметьте флажок, чтобы включить возможность многоадресной рассылки видео с данной <i>Камеры</i> .
Адрес (IPv4) для Мультикастной группы	IP-адрес, на который будет транслироваться видеопоток с данной <i>Камеры</i> (группа рассылки, для которой будет вестись вещание). Значение должно принадлежать диапазону IP-адресов класса D , зарезервированных для многоадресной рассылки.
Порт для Мультикастной группы	Номер порта, на который будет рассылаться видеопоток.
RTP поверх RTSP (TCP)	Отметьте флажок, если камера работает в загруженной сети, сети с низкой пропускной способностью, или в сети с фильтрацией пакетов RTP. Видеопоток будет передаваться по протоколу TCP.
Латентность сети, мс	Время, выделяемое на сборку кадра при текущей пропускной способности сети (в миллисекундах). Если реальная латентность сети известна, рекомендуется установить соответствующее значение. В противном случае используйте значение по умолчанию. Примечание. Параметр отображается на форме лишь для некоторых <i>Устройств видеозахвата</i>. Если не отображается, используется значение 0,5 с.

Общие Поток Запись Аудио Детекторы PTZ Дополнительные

Камера **Axis VAPIX3** поддерживает работу с несколькими видеопотоками. Доступные настройки Потоков соответствуют значениям в Веб-интерфейсе настроек камеры.

Поток 1

☒ Использовать настройки камеры

☐ Профиль: Quality

☐ RTP поверх RTSP (TCP)

Латентность сети, мс: 500

☐ Поток 2

Рис. 161. Закладка Поток многопоточной камеры Axis

9.12.1.2.3 Закладка Запись

В таблице 32 представлены типовые параметры камер. Параметры, зависящие от **Типа** и **Модели** камеры, описаны в таблице 33.

Общие Поток Запись Аудио Детекторы PTZ Дополнительные

Режим записи: По команде и детектору движения

Длительность пред-записи: 0 с

Длительность пост-записи: 0 с

☐ Прореживание, макс. FPS: 1

☒ Полный FPS во время тревоги

Пред-запись Тревога Пост-запись t

Архив

☐ Хранить не менее: 1 дней

☐ Удалять спустя: 1 дней

Edge Storage

☐ Просмотр архива, хранящегося на удаленном устройстве (EdgeStorage Gate)

☒ Не корректировать время кадров при ускоренном воспроизведении

☐ Восстанавливать архив из локального хранилища Камеры (EdgeStorage Sync)

Не восстанавливать последние, мин: 10

Номер профиля потока: Все доступные

OK Отмена Применить

Рис. 162. Параметры объекта Камера. Закладка Запись

Таблица 32. Параметры объекта Камера. Закладка Запись

Параметр	Описание
Режим записи	Выберите из списка режим записи камеры: По команде — запись видео будет осуществляться по команде оператора или с помощью подсистемы автоматизации (см. Подсистема автоматизации); По команде и детектору движения — возможно осуществлять запись видео автоматически при срабатывании детектора движения камеры и автоматически останавливать запись при отсутствии движения; Непрерывный — запись видео будет осуществляться непрерывно. Примечание. Запись видео можно остановить только изменив настройку <i>Камеры</i>. Непрерывный с переменным потоком — в данном режиме запись ведется постоянно. При этом: • При нормальных условиях записывается поток Низкого разрешения. (см. Закладка Поток). • При срабатывании <i>Детектора движения</i>, либо по команде оператора или по команде из скрипта, начинается запись потока Для записи видео (см. Закладка Поток). При переключении на поток Для записи видео к записи добавляется пред-запись видео высокого разрешения, сделанная в соответствии с настройками <i>Камеры</i> (см. Длительность пред-записи). • По окончании тревоги, либо по команде оператора или команде из скрипта, камера возвращается к записи потока Низкого разрешения. Запретить запись — в данном режиме поставить камеру на запись невозможно ни одним из доступных в SecurOS способом (например, из <i>Медиа Клиента</i>, программно либо с помощью <i>Макроса</i>, с <i>Карты</i> и т.д.).
Длительность записи	пред- Задайте длительность предзаписи в секундах. Чем дольше идет запись, тем больше оперативной памяти используется для хранения видео. Диапазон возможных значений: [0; 999]. Если задано значение 0, предзапись не ведется.
Длительность пост-записи	Задайте длительность постзаписи в секундах. Диапазон возможных значений: [0; 999]. Если задано значение 0, постзапись не ведется.

Параметр	Описание
Прореживание, макс. FPS	Признак прореживания и значение максимальной частоты кадров. Диапазон возможных значений: [1; 99]. Механизм прореживания подробно описан в разделе Прореживание видеопотока .
Полный FPS во время тревоги	Признак сохранения исходной частоты кадров видео, получаемого с камеры, при записи видео во время тревоги. Доступен только для режима записи По команде и детектору движения при активном параметре Прореживание, макс. FPS. Если отмечен: • во время тревоги запись ведется с исходным FPS. • предзапись и постзапись ведется с прореживанием.
Архив	
Хранить не менее	Задайте минимальное время хранения видеоархива в сутках. Примечание. За начало срока хранения архива принимается значение часа создания архива, например, 15:00 01.07.2015. Проверка необходимости удаления файлов архива выполняется при старте системы и, далее, по истечении каждого часа. При этом архив, срок хранения которого еще не истек, будет автоматически удален, если на доступных для записи дисках недостаточно места. Удаление начинается с наиболее старых записей, при этом запись архива приостанавливается до высвобождения места. При удалении такого архива генерируется соответствующее сообщение (см. Модуль самодиагностики Health Monitor). Диапазон возможных значений: [1; 9999].
Удалять спустя	Задайте максимальное время хранения видеоархива в сутках. Проверка необходимости удаления файлов архива выполняется при старте системы и, далее, по истечении каждого часа. Если заданное значение достигнуто, удаляются все записи архива в часовом интервале, с учетом параметра Хранить не менее (если задан). Если значение поля не указано, то архив будет храниться, пока на жестком диске будет оставаться свободное место для новых кадров архива. Диапазон возможных значений: [1; 9999].

Таблица 33. Опциональные параметры закладки Запись

Параметр	Описание

Просмотр архива, хранящегося на удаленном устройстве (EdgeStorage Gate)	Отметьте флажок для работы с архивом, который хранится на удаленном устройстве (см. Локальное хранилище камеры (Edge Storage)). Внимание! Запись видео с <i>Камер</i>, работающих с удаленным архивом, в SecurOS невозможна.
Не корректировать время кадров при ускоренном воспроизведении	Используется при ускоренном просмотре архива, хранящегося на удаленном устройстве. Отметьте флажок, если скорость смещения указателя позиции архива не соответствует скорости воспроизведения. Доступен, если отмечен параметр Просмотр архива, хранящегося на удаленном устройстве.
Восстанавливать архив из локального хранилища Камеры (EdgeStorage Sync)	Отметьте флажок для восстановления архива <i>Видеосервера</i> из локального архива <i>Камеры</i> при использовании технологии Edge Storage (см. Локальное хранилище камеры (Edge Storage)).
Не восстанавливать последние, мин	Задайте временной сдвиг для записи архива. При восстановлении архива <i>Видеосервера</i> из локального хранилища камеры будут скопированы фрагменты до момента времени $T_{\text{тек}} - N$, где: • $T_{\text{тек}}$ — текущее время; • N — заданное значение параметра. Оставшаяся часть архива будет записана с временной задержкой, равной заданному значению параметра. Настройка рекомендуется к использованию на камерах, пишущих на локальные носители информации видефрагменты большого размера. Установите значение параметра равное или превышающее длительность записи самого большого файла в локальном хранилище камеры. Например, заданное значение параметра равно 10 минутам. Связь с камерой пропадает на 15 минут, а затем восстанавливается. После восстановления связи из локального хранилища камеры будут загружены первые 5 минут архива от момента потери связи. Оставшийся пробел продолжительностью в 10 минут будет закрываться по частям в течение следующих 10 минут. Установка такого ограничения позволяет избежать ложных сообщений об ошибках, возникающих из-за невозможности загрузить с камеры архив прежде чем он будет фактически сохранен в локальном хранилище. Диапазон возможных значений: $[0; 60]$. Значение по умолчанию – 10.

Скорость загрузки относительно FPS	Установите скорость загрузки архива из локального хранилища камеры Edge Storage относительно FPS живого видеопотока. Большая скорость позволяет быстрее закрывать пробелы в архиве, но повышает нагрузку на сеть. Возможные значения: x1, x2, x4, x8, x16, x20. Значение по умолчанию – x1. При таком значении время закрытия пробела в архиве равно его продолжительности.
Номер профиля потока	Выберите номер профиля потока, заданного в настройках камеры с помощью web-интерфейса, который будет использоваться как для закрытия пробелов в архиве камеры в SecurOS (с помощью EdgeStorage Sync), так и при просмотре архива непосредственно с локального хранилища камеры (с помощью EdgeStorage Gate). Примечание. Указание номера профиля потока может привести к ошибке в работе некоторых устройств. В этом случае выберите значение Не использовать.

9.12.1.2.4 Закладка Аудио

The screenshot displays the 'Аудио' (Audio) configuration tab within the SecurOS interface. At the top, there are several tabs: 'Общие' (General), 'Поток' (Stream), 'Запись' (Recording), 'Аудио' (Audio), 'Детекторы' (Detectors), 'PTZ', and 'Дополнительные' (Additional). The 'Аудио' tab is currently selected.

The settings are organized into two main sections:

- Microphone Section:**
 - ☒ **Микрофон:** (Microphone) with an information icon (i). The dropdown menu is set to 'Встроенный' (Built-in).
 - Частота:** (Frequency) dropdown menu set to '8000'.
 - Сигнал:** (Signal) dropdown menu set to '-60 дБ'.
 - Усиление:** (Gain) slider set to '0дБ'.
- Speaker Section:**
 - ☐ **Динамик:** (Speaker) dropdown menu set to 'Внешний' (External).
 - Тип:** (Type) dropdown menu set to 'Axis'.
 - Модель:** (Model) dropdown menu set to 'Axis Network Speaker'.
 - IP-адрес:** (IP address) text field containing '0.0.0.0'.
 - Пользователь:** (User) text field.
 - Пароль:** (Password) text field.

At the bottom right of the window, there are three buttons: 'ОК' (OK), 'Отмена' (Cancel), and 'Применить' (Apply). The 'Отмена' button is highlighted with a blue border.

Рис. 163. Параметры объекта Камера. Закладка Аудио

Таблица 34. Параметры объекта Камера. Закладка Аудио

Параметр	Описание
Микрофон	Параметр определяет возможность воспроизведения звука в живом и архивном видео. Отметьте флажок и выберите Встроенный или внешний <i>Микрофон</i>, чтобы просматривать видео со звуком, если это возможно. Примечания: 1. Поддержка встроенного микрофона определяется техническими характеристиками камеры. 2. Для воспроизведения звука в <i>Медиа Клиенте</i> параметр Работать со звуком должен быть активен (см. Закладка Аудио).
Частота	Выберите частоту встроенного <i>Микрофона</i> .
Сигнал	Информационное поле: индикатор текущего уровня шума. Используется для проверки микрофона в режиме реального времени.
Усиление	Задайте усиление встроенного <i>Микрофона</i> .
Динамик	Отметьте флажок и выберите тип динамика камеры, на который будет осуществляться трансляция. Возможные значения: Встроенный — будет использоваться интегрированный динамик камеры. Является значением по умолчанию, если камера оснащена встроенным динамиком. При выборе данного значения указанные ниже параметры недоступны. Внешний — будет использоваться внешний сетевой динамик/громкоговоритель. Примечания: 1. Встроенный динамик поддерживается только некоторыми моделями камер Axis и Beward B. 2. Внешний динамик типа Axis может быть подключен к <i>Камере</i> любого Типа и Модели.
Тип	Выберите тип внешнего динамика.
Модель	Выберите модель внешнего динамика.
IP-адрес	Задайте IP-адрес внешнего динамика.
Пользователь, Пароль	Задайте имя пользователя и пароль для работы с внешним динамиком.

9.12.1.2.5 Закладка Детекторы

Общие Поток Запись Аудио **Детекторы** PTZ Дополнительные

☒ Детекция засвечивания

Размер: 0 100%

Контраст: мин макс

Работать согласно выбранному Расписанию: Всегда (Расписание не выбрано)

OK Отмена Применить

Рис. 164. Параметры объекта Камера. Закладка Детекторы

Таблица 35. Параметры объекта Камера. Закладка Детекторы

Параметр	Описание
Детекция засвечивания	Активируйте поле, чтобы система генерировала специальные события при засвечивании объектива камеры. Эти события могут быть использованы в макрокомандах или скриптах.
Размер	Передвигая ползунок, настройте чувствительность камеры. Возможные значения: • 0% — объектив камеры всегда засвечен; • 50% — объектив камеры будет засвечен, если размер области с низкой контрастностью занимает 50% кадра; • 100% — детектор срабатывает только при полном засвечивании объектива (камера с низкой контрастностью).
Контраст	Передвигая ползунок, настройте чувствительность контраста. Граничные значения: • мин — области с минимальным контрастом (например, лист бумаги); • макс — области с максимальным контрастом.
Работать согласно выбранному Расписанию	Выберите Расписание , в соответствии с которым будет работать детектор засвечивания.

9.12.1.2.6 Закладка PTZ

Рис. 165. Параметры объекта Камера. Закладка PTZ

Таблица 36. Параметры объекта Камера. Закладка PTZ

Параметр	Описание
Протокол PTZ	Выберите из списка протокол управления PTZ, доступный для данной модели <i>Камеры</i>. Примечание. Параметр доступен в зависимости от типа родительского <i>Устройства видеозахвата</i>.
Канал PTZ	Выберите канал управления телеметрией.
Запретить совместное управление	Выберите режим управления телеметрией (см. Совместное управление телеметрией и Раздельное управление телеметрией).

Параметр	Описание
Тип тура	Выберите из списка тип туров, которые будут доступны при работе с данной <i>Камерой</i>. Возможные значения: - По препозициям — туры, которые предопределены в настройках камеры с помощью web-интерфейса. - Записанный — туры, которые записаны пользователем на камере с помощью web-интерфейса. Примечание. Параметр доступен в зависимости от типа родительского <i>Устройства видеозахвата</i>.
Отображать только выбранные препозиции	Отметьте флажок, чтобы ограничить список препозиций <i>Камеры</i>. По умолчанию флажок не отмечен. В этом случае операторам будут доступны все препозиции <i>Камеры</i>. Примечание. Параметры по управлению отображением препозиций недоступны для <i>Камер</i> с родительским типом <i>Устройств видеозахвата</i> ISS Video Concentrator.
Фильтр	Для поиска препозиции по части имени или идентификатора введите в поле требуемые символы; в списке автоматически отобразятся только те препозиции, имя или идентификатор которых соответствуют заданным условиям поиска. Для того, чтобы очистить поле, нажмите кнопку Сбросить фильтр.
Список препозиций	Чтобы получить список доступных препозиций <i>Камеры</i> нажмите кнопку Получить препозиции (см. ниже). Для отображения препозиции в <i>Медиа Клиенте</i> (и других модулях SecurOS, работающих с препозициями <i>Камер</i>) отметьте соответствующий флажок слева от нее.
Получить препозиции (кнопка)	Нажмите кнопку, чтобы отправить запрос к <i>Камере</i> для получения списка препозиций. После выполнения запроса справа от кнопки отобразится его статус. Примечание. Если список препозиций успешно получен, но он пустой, т. е. для <i>Камеры</i> не создано ни одной препозиции, то в окне будет отображаться текст Для камеры не созданы препозиции.

9.12.1.2.7 Закладка Дополнительные

Общие Поток Запись Аудио Детекторы PTZ **Дополнительные**

☐ Использовать альтернативный способ синхронизации звука для встроенного микрофона

☒ Ручная настройка изображения

Яркость: 0

Контраст: 0

☐ Цветность

Насыщенность: 0

☐ Используется панорамный объектив: ImmerVision A0**V

Расположение камеры: потолок

Протокол оmyивающего устройства / дворника: Axis

OK **Отмена** Применить

Рис. 166. Параметры объекта Камера. Закладка Дополнительные

Примечание. На рис. 166 представлен набор параметров камеры Axis M3204.

В зависимости от модели *Камеры* список доступных параметров может отличаться. В этом разделе описаны следующие наборы параметров:

- **Дополнительные параметры Камеры ONVIF (Устройство видеозахвата с Типом ONVIF).**
- **Дополнительные параметры Камеры SecurOS Motus (Устройство видеозахвата с Типом SecurOS Motus).**
- **Дополнительные параметры виртуальной Камеры (Устройство видеозахвата с Типом Virtual).**
- **Дополнительные параметры Камеры Generic RTSP (Устройство видеозахвата с Типом Generic RTSP).**
- **Другие дополнительные параметры.**

Таблица 37. Дополнительные параметры Камеры ONVIF (Устройство видеозахвата с Типом ONVIF)

Параметр	Описание
Немедленно перезапускать поток при разрыве	Параметр позволяет повысить стабильность соединения для камер, связь с которыми часто нарушается на небольшой промежуток времени по причине разрыва соединения или ошибки.
Включить передачу необработанных событий	Отметьте флажок, чтобы разрешить передачу всех событий Камеры в ядро SecurOS. Используется для передачи событий встроенной аналитики Камеры получателю без их предварительной обработки.
Ручная настройка экспозиции	Отметьте флажок, чтобы вручную настроить параметры экспозиции для камеры. Примечание. Если эта опция включена, настройка диафрагмы из интерфейса оператора SecurOS невозможна.
Время экспозиции	Доступен только при выбранной опции Ручная настройка экспозиции . Возможные значения: [0; 100]. Значение по умолчанию: 50.
Усиление	Доступен только при выбранной опции Ручная настройка экспозиции . Возможные значения: [0; 100]. Значение по умолчанию: 50.
Диафрагма	Доступен только при выбранной опции Ручная настройка экспозиции . Возможные значения: [0; 100]. Значение по умолчанию: 50.
Яркость	Отметьте флажок, чтобы вручную настроить яркость изображения. Возможные значения: [0; 100]. Значение по умолчанию: 50.
Насыщенность	Отметьте флажок, чтобы вручную настроить насыщенность изображения. Возможные значения: [0; 100]. Значение по умолчанию: 50.
Резкость	Отметьте флажок, чтобы вручную настроить резкость изображения. Возможные значения: [0; 100]. Значение по умолчанию: 50.
Контраст	Отметьте флажок, чтобы вручную настроить контраст изображения. Возможные значения: [0; 100]. Значение по умолчанию: 50.
Баланс белого	Отметьте флажок, чтобы вручную настроить баланс белого в кадре.
Rgain	Доступен только при выбранной опции Баланс белого . Регулирует количество красного цвета в изображении. Чем выше значение, тем интенсивнее красный цвет. Возможные значения: [0; 100]. Значение по умолчанию: 50.

Параметр	Описание
Bgain	Доступен только при выбранной опции Баланс белого . Регулирует количество синего цвета в изображении. Чем выше значение, тем интенсивнее синий цвет. Возможные значения: [0; 100]. Значение по умолчанию: 50.
Компенсация засветки	Отметьте флажок, чтобы задействовать алгоритм компенсации засветки изображения.
Уровень	Доступен только при выбранной опции Компенсация засветки. Определяет насколько сильной будет влияние компенсации засветки. Возможные значения: [0; 100]. Значение по умолчанию: 50. Примечание. В случае, если камера не поддерживает настройку уровня, компенсация засветки будет осуществляться согласно механизмам, предусмотренных производителем.
Режим WDR	Отметьте флажок, чтобы задействовать технологию WDR. Примечание. Технология WDR (Wide Dynamic Range – широкий динамический диапазон) позволяет получать высокое качество изображения при перепаде уровней освещённости.
Уровень	Доступен только при выбранной опции Режим WDR. Определяет насколько сильным будет влияние WDR. Возможные значения: [0; 100]. Значение по умолчанию: 50. Примечание. В случае, если камера не поддерживает настройку уровня, WDR будет работать согласно механизмам, предусмотренных производителем.
Режим работы ИК-фильтра	Отметьте флажок, чтобы определить режим работы ИК-фильтра. Возможные значения: • автоматическое вкл/выкл (значение по умолчанию); • всегда включен; • всегда отключен.
Нестандартные команды управления дворником	Отметьте флажок, если для управления дворником ONVIF-устройства требуется использование нестандартных команд: Запуск дворника — введите команду для запуска дворника. Остановка дворника — введите команду для остановки дворника. Примечание. Если параметр активен, но команда не задана, то соответствующая команда (в том числе стандартная) не будет отправляться на ONVIF-устройство.

Параметр	Описание
Нестандартные команды управления омывающим устройством	Отметьте флажок, если для управления омывающим устройством ONVIF-устройства требуется использование нестандартных команд: Запуск омывающего устройства – введите команду для запуска омывающего устройства. Остановка омывающего устройства – введите команду для остановки омывающего устройства. Примечание. Если параметр активен, но команда не задана, то соответствующая команда (в том числе стандартная) не будет отправляться на ONVIF-устройство.
Центрирование кадра по выбранной точке	Активация данного параметра позволяет использовать функциональность центрирования кадра по выбранной точке (см. Краткое руководство пользователя SecurOS , раздел Управление с помощью мыши).
Масштабирование выделенной области кадра	Активация данного параметра позволяет использовать функциональность масштабирования выделенной области кадра (см. Краткое руководство пользователя SecurOS , раздел Управление с помощью мыши).
H264/H265: Использовать маркеры RTP	Параметр влияет на низкоуровневые механизмы протокола связи с камерой. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.
H265: Игнорировать бит начала FU в заголовке	Параметр влияет на низкоуровневые механизмы протокола связи с камерой. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.
H265: Игнорировать бит конца FU в заголовке	Параметр влияет на низкоуровневые механизмы протокола связи с камерой. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.
H265: Игнорировать тип FU в заголовке	Параметр влияет на низкоуровневые механизмы протокола связи с камерой. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.
H265: Игнорировать тип полезной нагрузки в заголовке FU	Параметр влияет на низкоуровневые механизмы протокола связи с камерой. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.
Записывать состояние PTZ в метаданные видеокадра	Параметр влияет на низкоуровневые механизмы протокола связи с камерой. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.

Таблица 38. Дополнительные параметры Камеры SecurOS Motus (Устройство видеозахвата с Типом SecurOS Motus)

Параметр	Описание
Использовать встроенный контроллер SecurOS Motus	Отметьте флажок, чтобы управлять подсветкой камеры, масштабированием и фокусным расстоянием камеры. Примечание. Если не отмечен, все указанные ниже параметры недоступны. Внимание! Для управления камерой с помощью контроллера Motus в настройках объекта <i>Камера</i> необходимо задать значение Использовать для параметра Поворотное устройство (см. Закладка Общие). В противном случае управлять камерой будет невозможно.
IP-адрес управляющего устройства	Задайте IP-адрес контроллера Motus, который будет использоваться для управления подсветкой, масштабированием и фокусным расстоянием камеры.
Пользователь/Пароль	Задайте имя и пароль пользователя для доступа к управлению подсветкой, масштабированием и фокусным расстоянием камеры.
Режим работы подсветки	Задайте режим работы подсветки. Возможные значения: • всегда включена (значение по умолчанию) — при выборе данного значения все зоны постоянно подсвечиваются с заданной интенсивностью; • всегда выключена — при выборе данного значения подсветка всех зон постоянно отключена; • автоматическое вкл/выкл — при выборе данного значения подсветка включается/выключается автоматически в зависимости от уровня фактической освещенности (определяется датчиком камеры). Если фактическая освещенность ниже уровня, заданного параметром Уровень переключения режима день/ночь, подсветка включается для всех зон с указанной для каждой зоны интенсивностью, и наоборот.
Подсветка ближней/средней/дальней зоны	Задайте уровень освещения для каждой зоны (в %, в диапазоне, настроенном в контроллере). Например, если в контроллере задан диапазон интенсивности [15; 75], а значение параметра задано равным 40, то фактическая интенсивность освещения будет равна 39.
Уровень переключения режима день/ночь	Задайте порог автоматического включения/выключения подсветки для режима автоматическое вкл/выкл.

Параметр	Описание
Принудительное переключение камеры в ночной режим	Внимание! Только для камер с ИК-подсветкой. Флаг управления ИК-фильтром камеры. Если отмечен (значение по умолчанию), ИК-фильтр камеры отключается, если уровень освещения ниже или равен значению, заданному в параметре Уровень переключения режима день/ночь.
Настройки подсветки для Модели SMT-LT357-IR (с ИК-подсветкой)	
Управление освещением	Отметьте флажок, чтобы управлять ИК-подсветкой камеры. Открывает доступ к параметрам, перечисленным ниже.
Режим день/ночь	Определяет режим работы источников света. Возможные значения: • автоматическое вкл/выкл (значение по умолчанию); • день; • ночь.
Чувствительность	Настройка доступна только при выбранном Режиме день-ночь Автоматическое вкл/выкл. Определяет чувствительность к свету для переключения режима день/ночь. Чем выше значение, тем раньше камера переключится в ночной режим при наступлении сумерек. Возможные значения: [0; 9]. Значение по умолчанию: 7.
Управление интенсивностью подсветки	Выберите режим, согласно которому будет определяться интенсивность подсветки. Возможные значения: • автоматическое; • ручное.
Подсветка ближней зоны/Подсветка дальней зоны	Настройка доступна только для варианта Управление интенсивностью подсветки Ручное. Определяет интенсивность работы источников света в ближней/дальней зоне. Возможные значения: [0; 1000]. Значение по умолчанию: 500. Примечание. На некоторых моделях камер возможность управления интенсивностью подсветки в разных зонах может быть частично или полностью недоступна.
Настройки подсветки для Модели SMT-LT556-WL (с белым светом)	
Управление освещением	Отметьте флажок, чтобы управлять источником белого света камеры. Открывает доступ к параметрам, перечисленным ниже.
Режим работы подсветки	Определяет режим работы источников света. Возможные значения: • автоматическое вкл/выкл (значение по умолчанию); • всегда включена; • всегда выключена.

Параметр	Описание
Чувствительность	Настройка доступна только при выбранном Режиме работы подсветки Автоматическое вкл/выкл. Определяет чувствительность к свету для переключения режима работы подсветки. Чем выше значение, тем раньше камера включит подсветку при наступлении сумерек. Возможные значения: [0; 9]. Значение по умолчанию: 7.
Подсветка ближней зоны/Подсветка дальней зоны	Определяет интенсивность работы источников света в ближней/дальней зоне. Возможные значения: [0; 1000]. Значение по умолчанию: 500. Примечание. На некоторых моделях камер возможность управления интенсивностью подсветки в разных зонах может быть частично или полностью недоступна.

Таблица 39. Дополнительные параметры виртуальной Камеры (Устройство видеозахвата с Типом Virtual)

Параметр	Описание
Разрешить воспроизведение кадров BinaryPack	Отметьте флажок, если видеопоток содержит кадры в формате BinaryPack.
Включить синхронизацию потоков	Отметьте флажок для синхронизации всех видеопотоков всех <i>Камер</i> , дочерних данному <i>Устройству видеозахвата</i> . После применения настройки все потоки объединяются в единую группу синхронизации. Для данной группы ищется общий временной интервал, после чего видео с каждой <i>Камеры</i> проигрывается синхронно по кругу в пределах такого интервала. Если общий интервал не найден, видео не синхронизируется.
Использовать межкадровые задержки из файла	Отметьте флажок, чтобы проигрывать видеоархив с теми же межкадровыми интервалами, с какими этот архив был записан. Исходные межкадровые интервалы будут в точности воспроизводиться при каждом произвольном проигрывании архива. Данный режим используется для демонстрации изменений в работе алгоритмов видеоаналитики при их совершенствовании. Если флажок снят, межкадровые интервалы будут рассчитываться <i>Устройством видеозахвата</i> автоматически и будут отличаться для каждого отдельного проигрывания архива.

Таблица 40. Дополнительные параметры Камеры Generic RTSP (Устройство видеозахвата с Типом Generic RTSP)

Параметр	Описание
Добавить данные авторизации в URL	Отметьте флажок для передачи данных авторизации (пользователь, пароль) в строке URL. Данная опция предназначена для подключения к камерам, не поддерживающим подключение с данными авторизации в зашифрованном виде. По умолчанию не отмечен.
Использовать совместимое форматирование URL в методе SETUP	Параметр влияет на низкоуровневые механизмы протокола связи с камерой. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.
Игнорировать RTP SSRC	Параметр влияет на низкоуровневые механизмы протокола связи с камерой. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.
Игнорировать тип полезной нагрузки RTP	Параметр влияет на низкоуровневые механизмы протокола связи с камерой. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.
Игнорировать номер последовательности в заголовке RTP (только для RTP/TCP)	Параметр влияет на низкоуровневые механизмы протокола связи с камерой. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.
Отключить NAT hole punching	Параметр влияет на низкоуровневые механизмы протокола связи с камерой. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.
Немедленно перезапускать поток при разрыве	Параметр позволяет повысить стабильность соединения для камер, связь с которыми часто нарушается на небольшой промежуток времени по причине разрыва соединения или ошибки.
H264/H265: Использовать маркеры RTP	Параметр влияет на низкоуровневые механизмы протокола связи с камерой. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.
H265: Игнорировать бит начала FU в заголовке	Параметр влияет на низкоуровневые механизмы протокола связи с камерой. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.
H265: Игнорировать бит конца FU в заголовке	Параметр влияет на низкоуровневые механизмы протокола связи с камерой. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.

Параметр	Описание
H265: Игнорировать тип FU в заголовке	Параметр влияет на низкоуровневые механизмы протокола связи с камерой. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.
H265: Игнорировать тип полезной нагрузки в заголовке FU	Параметр влияет на низкоуровневые механизмы протокола связи с камерой. Использование параметра возможно только по указанию Службы технической поддержки Intelligent Security Systems.

Таблица 41. Другие дополнительные параметры

Параметр	Описание
Использовать альтернативный способ синхронизации звука для встроенного микрофона	В некоторых случаях параметр позволяет решить возможные неполадки со звуком при использовании камеры со встроенным микрофоном.
Используется паноморфный объектив	Если на камере установлен паноморфный объектив, отметьте флажок и выберите модель объектива. Подробнее см. раздел Настройка панорамных камер .
Расположение камеры	Выберите из списка место расположения камеры с паноморфным объективом.
Протокол омывающего устройства / дворника	Настройка позволяет задать протокол взаимодействия с омывающим устройством или дворником для некоторых устройств Axis. Отметьте флажок и выберите из списка требуемый протокол.
Игнорировать параметр qop (Quality of protection) со значением auth при дайджест-аутентификации	Флажок определяет ответ сервера на запрос при дайджест-аутентификации: • если отмечен, ответ вычисляется по алгоритму MD5 (HA1 : nonce : HA2); • если не отмечен, и в запросе указана директива qop="auth", ответ вычисляется по алгоритму MD5 (HA1 : nonce : nonceCount : clientNonce : qop : HA2). Примечание. Директива qop="auth" в запросе на авторизацию указывается автоматически RTSP-сервером.
Формат данных пиксельных	Выберите из списка формат пиксельных данных несжатого видео, который поддерживается данной моделью Камеры. В случае, если выбранное значение не поддерживается, видеопоток с данной Камеры получен не будет. Внимание! Полный список поддерживаемых значений приводится в Руководстве пользователя для выбранной модели Камеры.

Параметр	Описание
Серийный номер камеры	Для получения в SecurOS видеопотока от конкретной <i>Камеры</i> , задайте ее серийный номер. Параметр используется в случае, если к одному <i>Компьютеру</i> по интерфейсу USB 3.0 подключено несколько устройств.
Автоматический баланс белого	Внимание! Параметр предназначен для использования только с теми моделями камер Basler Pylon GigE (Area Scan Camera) и Basler Pylon USB 3.0, в собственных настройках которых поддерживается автобаланс белого. В противном случае использование параметра может привести к неработоспособности <i>Камеры</i> в SecurOS. Настройка позволяет компенсировать отличия в цвете, возникающие при работе камеры в условиях различной освещенности. Отметьте флажок и выберите из списка один из режимов регулировки баланса белого: • Выключен — автоматическая корректировка баланса белого отключена. • Зафиксирован при съемке — при выборе данного значения баланс белого будет автоматически корректироваться до тех пор, пока не будет получено оптимальное значение в условиях текущей освещенности. После достижения такого значения будет автоматически установлен режим Выключен, а полученное значение будет использоваться постоянно для всех следующих кадров. • Автоматический — баланс белого будет автоматически корректироваться для каждого кадра до тех пор, пока не будет выбран режим Выключен или Зафиксирован при съемке. • Предустановка 3200K. • Предустановка 5000K. • Предустановка 6500K. • Предустановка 7500K.

Параметр	Описание
Автоматическое усиление	Отметьте флажок и выберите один из режимов регулировки усиления: - Выключен — автоматическая регулировка усиления отключена. Значение усиления задается вручную с помощью перемещения ползунка. - Зафиксирован при съемке — при выборе данного значения камера автоматически отрегулирует усиление только один раз. После этого будет автоматически установлен режим Выключен, а полученное значение будет использоваться постоянно для всех следующих кадров. - Автоматический — при выборе данного значения камера переходит в режим автоматической регулировки усиления. В этом режиме усиление будет автоматически регулироваться для каждого кадра до тех пор, пока не будет выбран режим Выключен или Зафиксирован при съемке.
Усиление	Задайте значение усиления выходного сигнала камеры.
Минимальное усиление	Задайте минимальное значение усиления (см. параметр Автоматическое усиление). Возможные значения: [100; 12599]. Значение по умолчанию: 100.
Максимальное усиление	Задайте максимальное значение усиления (см. параметр Автоматическое усиление). Возможные значения: [100; 12600]. Значение по умолчанию: 100.
Ширина кадра, пк	Задайте ширину кадра (в пикселях), если не требуется использовать максимально возможное разрешение матрицы по горизонтали.
Высота кадра, пк	Задайте высоту кадра (в пикселях), если не требуется использовать максимально возможное разрешение матрицы по вертикали.
Время экспозиции, мкс	Задайте максимальное время экспозиции кадра (в микросекундах). Параметр регулирует яркость кадра: чем больше значение, тем ярче будет изображение.
Автоматическое центрирование по горизонтали	Отметьте флажок для автоматического центрирования кадра по горизонтали. По умолчанию не отмечен.
Сдвиг по горизонтали, пк	Задайте сдвиг кадра по горизонтали (в пикселях). Параметр задает смещение левого верхнего угла кадра относительно левого верхнего угла матрицы в случае, если размер кадра по горизонтали меньше максимально допустимого (см. параметр Ширина кадра).

Параметр	Описание
Автоматическое центрирование вертикали	Отметьте флажок для автоматического центрирования кадра по вертикали. По умолчанию не отмечен.
Сдвиг по вертикали, пк	Задайте сдвиг кадра по вертикали (в пикселях). Параметр задает смещение левого верхнего угла кадра относительно левого верхнего угла матрицы в случае, если размер кадра по вертикали меньше максимально допустимого (см. параметр Высота кадра).
Кодек	Выберите кодек, соответствующий требуемому видеопотоку камеры.
Кодек для записи видеоархива	Выберите кодек, который будет использоваться для сохранения видео в архив.
HDR преобразование	В некоторых случаях HDR преобразование делает изображение более пригодным для видеоаналитики. Опция требует дополнительных вычислительных ресурсов.
Режим ожидания	Отметьте флажок, чтобы во время отсутствия автомобиля над UVSS платформой для камеры применялись другие настройки экспонирования.

9.12.1.2.8 Мультикаст

Видео от камеры наблюдения может передаваться на рабочие места операторов в двух режимах:

- юникаст-трансляция — поток транслируется по маршруту **Камера → Видеосервер → Рабочее место оператора**. В этом режиме от *Видеосервера* к *Рабочим местам оператора* передается столько одинаковых потоков видео, сколько операторов наблюдают за камерой.
- мультикаст-трансляция — в этом режиме от камеры в сеть передается единственный поток видео. Далее этот поток средствами сетевого оборудования передается на *Видеосервер* и неограниченное число *Рабочих мест оператора*.

Преимущества использования мультикаст-трансляции

При большом количестве операторов видеонаблюдения использование мультикаст-трансляции дает следующие преимущества:

- значительно снижаются затраты на приобретение и эксплуатацию необходимого сетевого оборудования;
- снижается нагрузка на видеосервер.

Например, в сети SecurOS есть несколько *Видеосерверов*, к каждому из которых подключено по 100 *Камер*. Поток видео, транслируемого каждой *Камерой*, равен 5 Мбит/с. В сети создано 40 *Рабочих мест оператора*, на каждом из которых ведется наблюдение за 20 *Камерами*.

Рассмотрим наихудший случай, когда все 40 операторов одновременно наблюдают за *Камерами*, подключенными к одному *Видеосерверу*. В этом случае получаем:

- **Юникаст-режим**

- Суммарный видеопоток на входе *Видеосервера* будет составлять $100 \times 5 = 500$ Мбит/с. Для работы с таким видеопотоком достаточно одного сетевого интерфейса (сетевой платы) со скоростью передачи данных 1 Гбит/с.
 - Суммарный видеопоток на выходе *Видеосервера* будет составлять $20 \times 40 \times 5 = 4000$ Мбит/с. Для работы с таким видеопотоком уже требуется 10 Гбит/с интерфейс на сервере и такой же 10 Гбит/с интерфейс на сетевом оборудовании. В настоящее время такое оборудование существенно дороже, чем широко распространенное 1 Гбит/с.
 - Для передачи такого видеопотока в сеть *Видеосервер* должен обладать достаточным запасом производительности CPU.
- **Мультикаст-режим**
 - Суммарный видеопоток на входе *Видеосервера* остается прежним (500 Мбит/с). Для работы с таким видеопотоком достаточно одного сетевого интерфейса (сетевой платы) со скоростью передачи данных 1 Гбит/с.
 - Видеопоток на выходе *Видеосервера* отсутствует. Таким образом, достаточно уже имеющегося 1 Гбит/с сетевого интерфейса и такого же 1 Гбит/с интерфейса на сетевом оборудовании.
 - Дополнительной мощности CPU *Видеосервера* для передачи видеопотока в сеть не требуется.

Условия использования мультикаст-трансляции

Мультикаст-трансляцию целесообразно использовать при выполнении следующих условий:

- сетевое оборудование поддерживает протокол IGMP Version 3;
- сетевое оборудование настроено для мультикаст-трансляции и обеспечивает доставку видео любому клиенту, подключенному к сети SecurOS;
- пропускная способность любого из сегментов сети исключает потерю UDP-пакетов при передаче видео.

Дополнительная информация

Потеря UDP-пакетов приводит к значительному прореживанию видеопотока, что будет проявляться в виде "скачков" и "рывков" изображения при воспроизведении видео.

В противном случае использование мультикаст-трансляции не оправдано и не приведет к ожидаемому результату.

Настройка Камеры

Внимание! В текущем релизе мультикаст-трансляция поддерживается только для протокола ONVIF.

Для использования мультикаст-трансляции, задайте следующие параметры на закладке **Поток** в окне настройки *Камеры* (см. рис. 167):

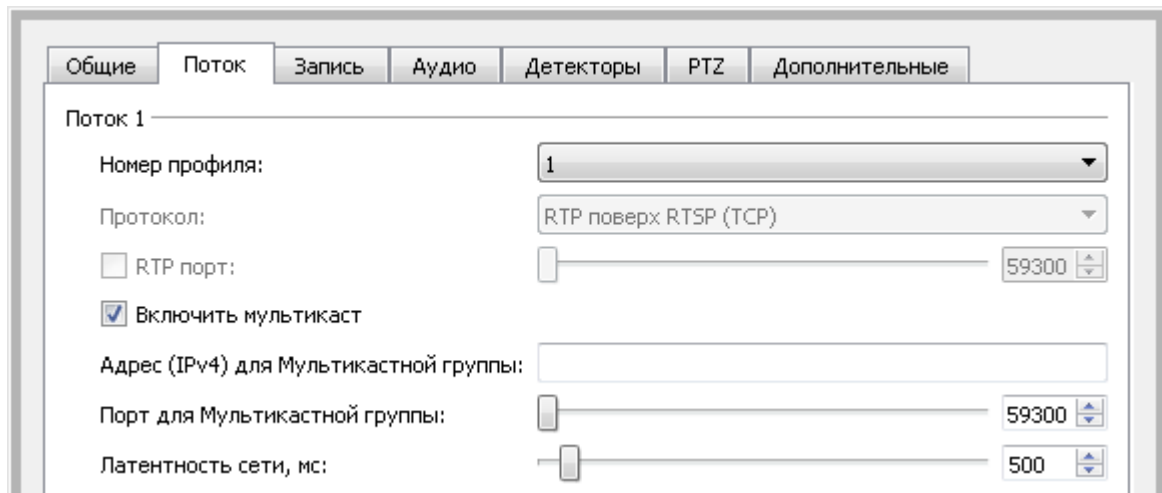


Рис. 167. Настройка режима мультикаст-трансляции

1. **Включить мультикаст.**
2. **Адрес (IPv4) и Порт** для мультикаст-группы трансляции.

Внимание! Каждая пара значений **Адрес (IPv4)/Порт** должна быть уникальна. Проверка уникальности заданных значений выполняется администратором системы.

9.12.1.2.9 Настройка панорамных камер

Исходное круговое изображение панорамной камеры может быть "развернуто" и приведено к виду, удобному для восприятия оператором. Для такой "развертки" используются различные алгоритмы, соответствующие **Типу** и **Модели** камеры. Настройка панорамных камер выполняется для выбора корректного алгоритма, позволяющего просматривать "развернутое" изображение от камер, оборудованных различными типами объективов.

Настройка панорамных камер выполняется на закладке **Дополнительные** (см. рис. 168). В зависимости от **Типа** и **Модели** камеры возможны следующие варианты настройки:

- **Настройка камер, оборудованных паноморфным объективом с поддержкой технологии ImmerVision;**
- **Настройка прочих камер, оборудованных панорамным объективом.**

Возможность управления поддерживаемыми панорамными камерами с помощью электронного PTZ включается автоматически после выполнения операций настройки.

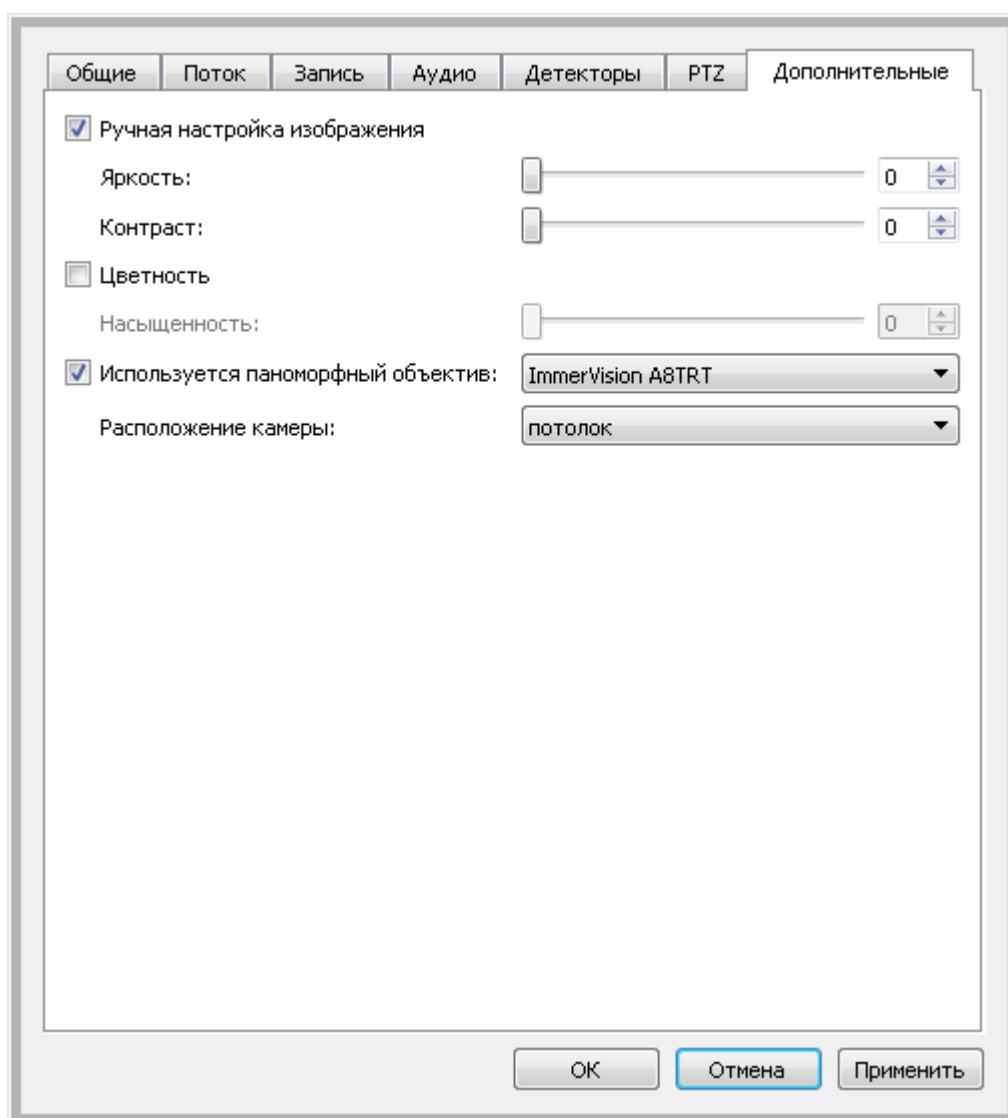


Рис. 168. Закладка Дополнительные для камер с панорамными объективами

Настройка камер, оборудованных панорамным объективом с поддержкой технологии ImmerVision

Для настройки камеры выполните следующие действия:

1. Отметьте флажок **Используется панорамный объектив**, в списке справа выберите модель используемого объектива.
2. В списке **Расположение камеры** выберите место установки камеры.

Настройка прочих камер, оборудованных панорамным объективом

Для настройки камеры в списке **Расположение камеры** выберите место установки камеры.

9.12.1.3 Детектор расфокусировки

Объект предназначен для настройки параметров, используемых в алгоритме определения расфокусированности *Камеры*.

Родительский объект — **Камера**.

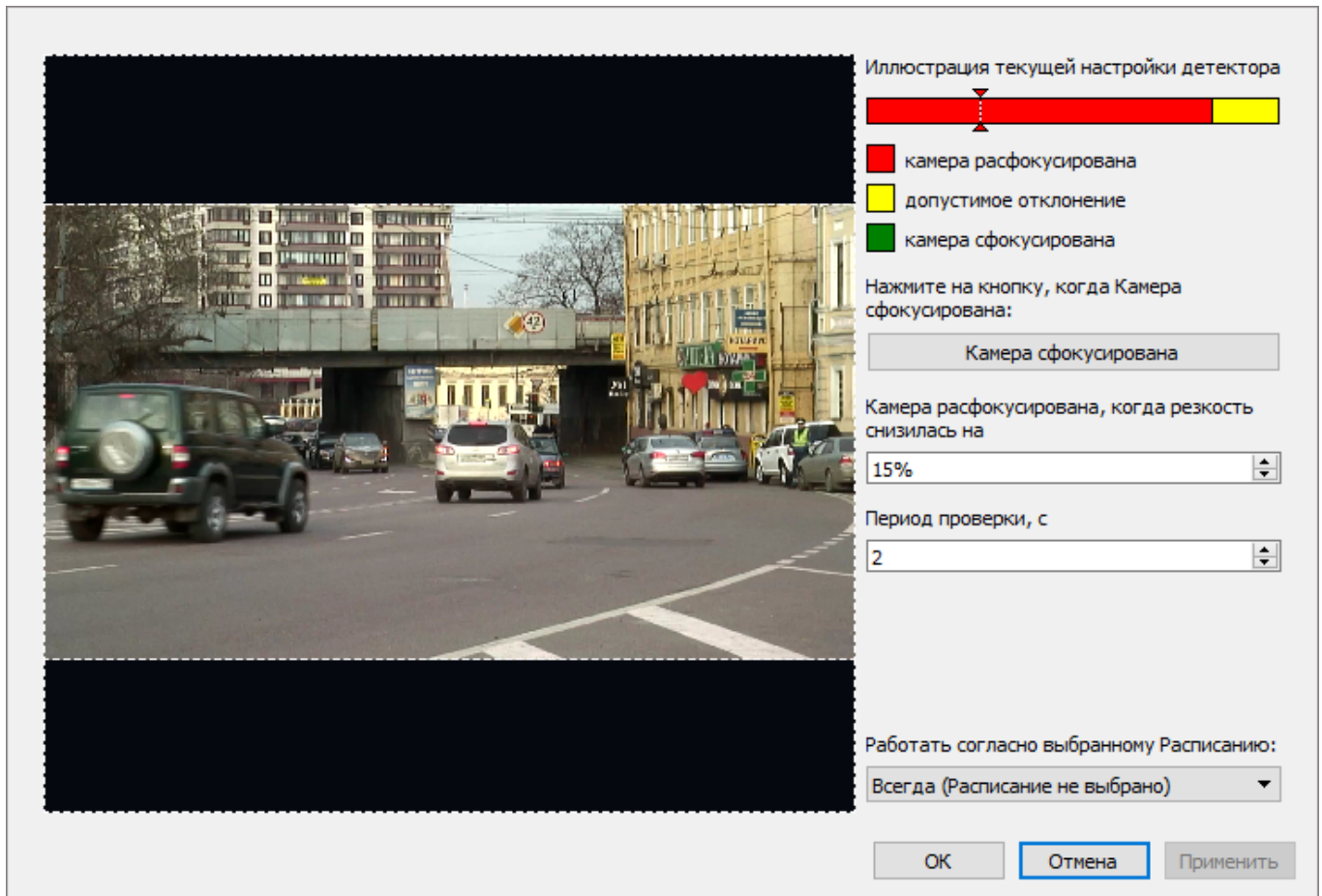


Рис. 169. Окно настройки параметров объекта Детектор расфокусировки

Таблица 42. Параметры объекта Детектор расфокусировки

Параметр	Описание
Область детектирования	Расположена в левой части окна настройки параметров. Представляет собой прямоугольную область, ограниченную белой пунктирной линией, внутри которой видеопоток отображается без искажений. Четкость изображения в области детектирования принимается за эталонную. Для изменения размеров области захватите мышью любую сторону рамки, и, не отпуская кнопку, переместите курсор в требуемом направлении. Для перемещения области детектирования щелкните мышью внутри рамки, и, не отпуская кнопку, переместите рамку в требуемом направлении. По умолчанию устанавливается равной размеру кадра отображаемого видеопотока.
Камера сфокусирована (кнопка)	После настройки параметров детектирования, нажмите кнопку для сохранения эталонного изображения.
Камера расфокусирована, когда резкость снизилась на	Отклонение четкости текущего изображения в области детекции от эталонного, в процентах, при превышении которого камера будет считаться расфокусированной. Сопровождается генерацией соответствующего события (см. Руководство программиста SecurOS).

Параметр	Описание
Период проверки	Период проверки фокусировки камеры, в секундах. Диапазон возможных значений: [1; 120].
Работать согласно выбранному Расписанию	Выберите из списка Расписание , в соответствии с которым будет выполняться проверка расфокусированности камеры. Если не отмечен, проверка выполняется всегда.

Рекомендации по выбору области детектирования и настройке остальных параметров детектора приведены ниже (см. раздел **Рекомендации по настройке**).

9.12.1.3.1 Рекомендации по настройке

При задании области детектирования рекомендуется учитывать следующие требования:

1. Изображение в области детектирования должно быть по возможности статичным.
2. Изображение в области детектирования должно содержать максимально возможное количество небольших по размеру объектов с четко распознаваемыми границами.
3. Затеняемость изображения в области детектирования прочими объектами должна быть минимизирована.

При выборе **Периода проверки** для областей, в которых затеняемость изображения охраняемого объекта в нормальных условиях не предусмотрена, рекомендуется задавать небольшой период проверки. Это позволит, например, зафиксировать кратковременные заслонения области при саботаже.

При выборе **Расписания** рекомендуется использовать временные периоды, на всем протяжении которых изменение освещенности в области детектирования незначительно.

При правильном выборе зоны детектирования и других параметров индикатор текущей настройки детектора будет выглядеть следующим образом (см. рис. 170):

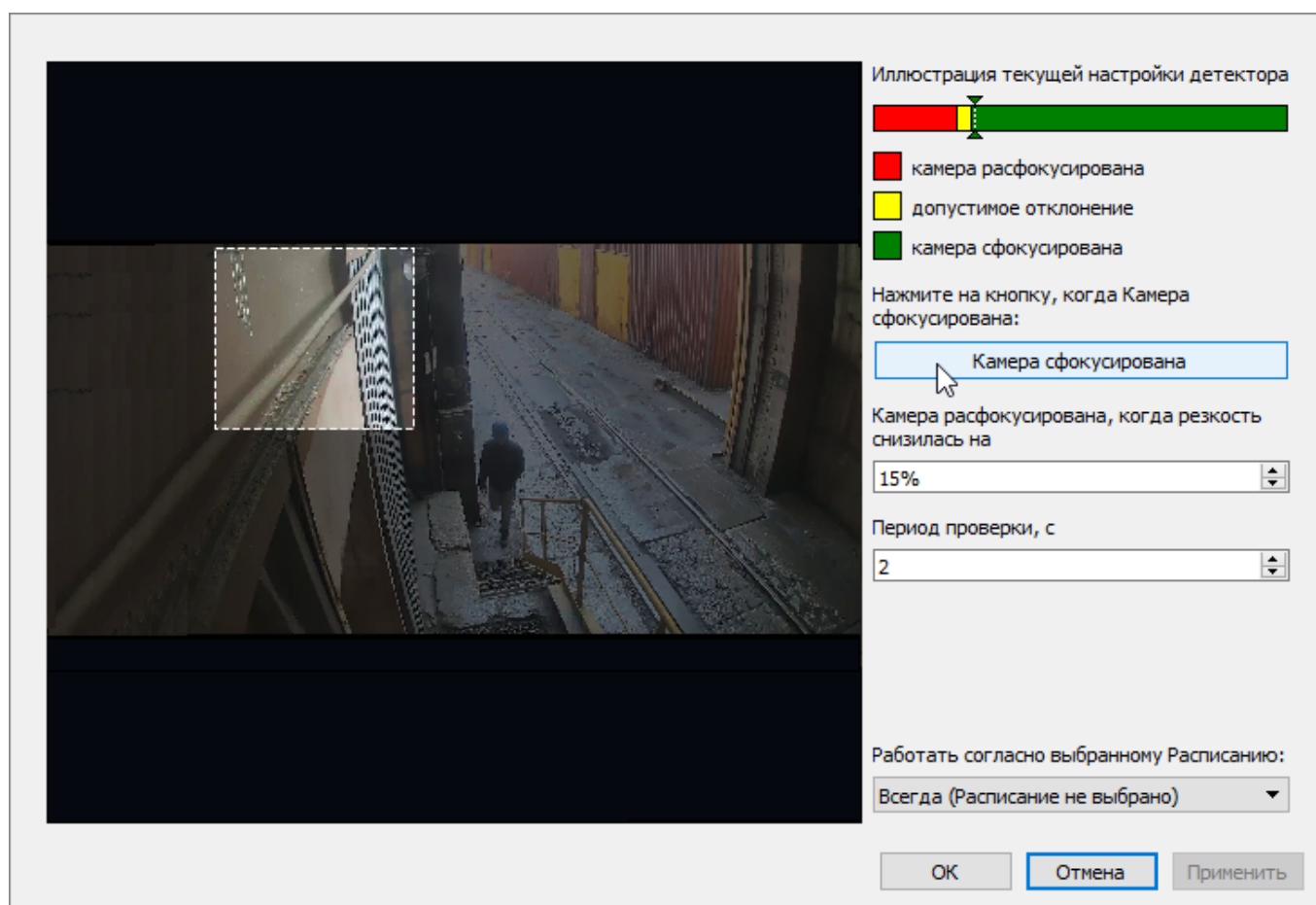


Рис. 170. Настройка детектора расфокусировки

9.12.1.4 Раскладка

Объект используется для создания макета видеостраницы *Медиа Клиента* — формы, размеров и взаимного расположения ячеек для вывода изображения с *Камер*. Для использования созданных пользовательских раскладок активируйте желаемые раскладки на закладке **Раскладки** (см. раздел **Медиа Клиент**). Аналогично системным раскладкам, при использовании пользовательской раскладки допускается перемещение произвольной камеры в произвольную ячейку раскладки.

Родительский объект — *Объект охраны\группа Раскладки и Видеы*.

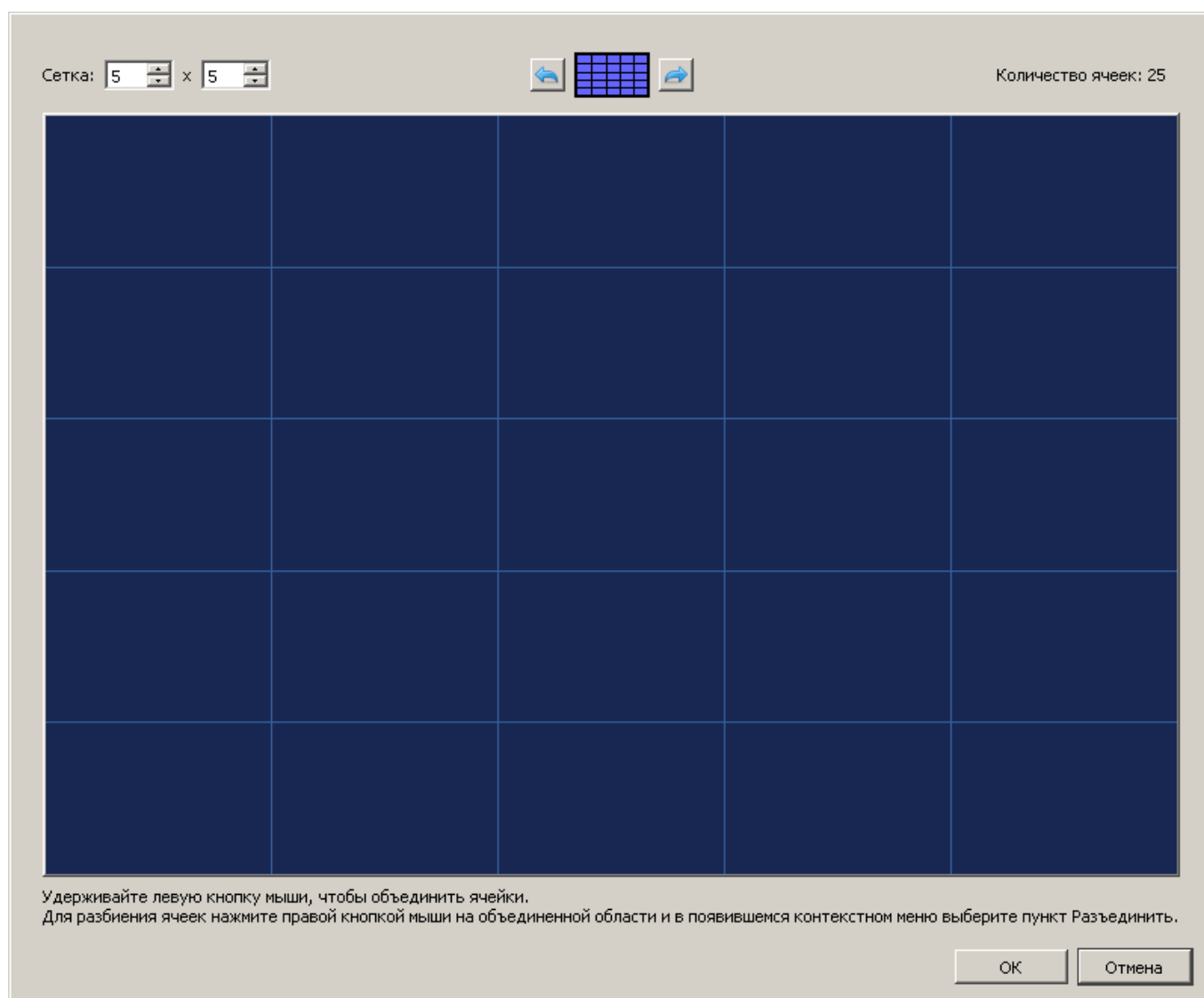


Рис. 171. Окно настройки параметров объекта Раскладка

Таблица 43. Параметры объекта Раскладка

Параметр	Описание
Сетка	Сетка определяет базовый макет рабочей области <i>Медиа Клиента (Раскладку)</i> , содержащий заданное количество ячеек по вертикали и горизонтали, соответственно. При создании/редактировании раскладки любое количество смежных базовых ячеек может быть объединено в ячейку увеличенного размера. Ячейка увеличенного размера может быть разъединена на соответствующее количество базовых ячеек.
Количество ячеек	Информационная строка. Отображает общее количество ячеек отображаемой раскладки. Обновляется автоматически при изменении макета раскладки. Максимальное количество ячеек раскладки — 250.
Кнопки	

Параметр	Описание
	Кнопки просмотра (Предыдущий вид, Следующий вид) рабочих вариантов макета раскладки. Примечание. При создании/редактировании макета раскладки в рамках одной сессии работы в окне настроек объекта промежуточные варианты раскладки сохраняются в оперативной памяти SecurOS и доступны пользователю.
ОК (Отмена)	Сохранение текущей раскладки и выход из окна настройки (закрытие окна без сохранения изменений).

9.12.1.5 Вид

Вид представляет собой совокупность нескольких *Камер*, *Микрофонов* или *Камер* и *Микрофонов* одновременно, сгруппированных в единый объект, управление которым осуществляется с помощью *Медиа Клиента*. Визуально *Вид* включает в себя *Рабочую область Медиа Клиента*, на которой выводится изображение от *Камер*, и *Панели микрофонов*. Каждый *Вид* является отдельным объектом *Медиа Клиента*, что позволяет обеспечить быстрый доступ оператора к интересующей информации, получаемой заранее определенным постоянным набором видео - и аудиоисточников.

Родительский объект — *Объект охраны\группа Раскладки и Виды*.

Параметры для редактирования отсутствуют.

Настройка *Видов* для использования на *Рабочем месте оператора* выполняется администратором системы с помощью *Медиа Клиента* (см. **О Видах**).

Настройка *Медиа Клиента* для работы с *Видами* выполняется на закладке **Виды**.

9.12.1.6 Зона

Объект представляет определенную зону детектора движения (см. **Принципы работы зон обнаружения движения**). Главная зона Main создается по умолчанию при создании объекта *Камера* и занимает всю область изображения *Камеры*.

При настройке объекта *Зона* рекомендуется обратить внимание на следующие параметры:

- **Контраст** — минимум контраста объекта по отношению к окружению. Если ползунок находится в крайней верхней позиции, то как движущиеся будут восприниматься только те объекты, которые значительно отличаются от окружения. Нижнее положение ползунка означает, что даже слабо выделяющиеся среди окружения объекты будут восприниматься как движущиеся.
- **Размер** — минимум размера объекта. Верхнее положение ползунка означает, что *Зона* будет реагировать только на большие объекты; при нижнем положении ползунка *Зона* реагирует и на маленькие, и на большие объекты.

Примечание. Значения параметров **Контраст** и **Размер** подбираются экспериментально.

- Поле **Тревожная** следует активировать, если камера должна переходить в тревожное состояние в случае обнаружения движения в зоне. Если это поле не активировано, зона считается информационной.
- Поле **Всегда на охране** следует активировать, если зона всегда должна быть на охране, независимо от состояния остальных зон данной камеры.
- Поле **Сохранять координаты движения (для Умного поиска)** следует активировать, если необходимо записывать в БД координаты объектов, которые вызвали тревогу.

Примечание. Объекты *Зона*, относящиеся к одному и тому же родительскому объекту, объединяются в логическую группу **Зоны изображения** в дереве объектов.

Родительский объект — *Камера\группа Зоны изображения*.

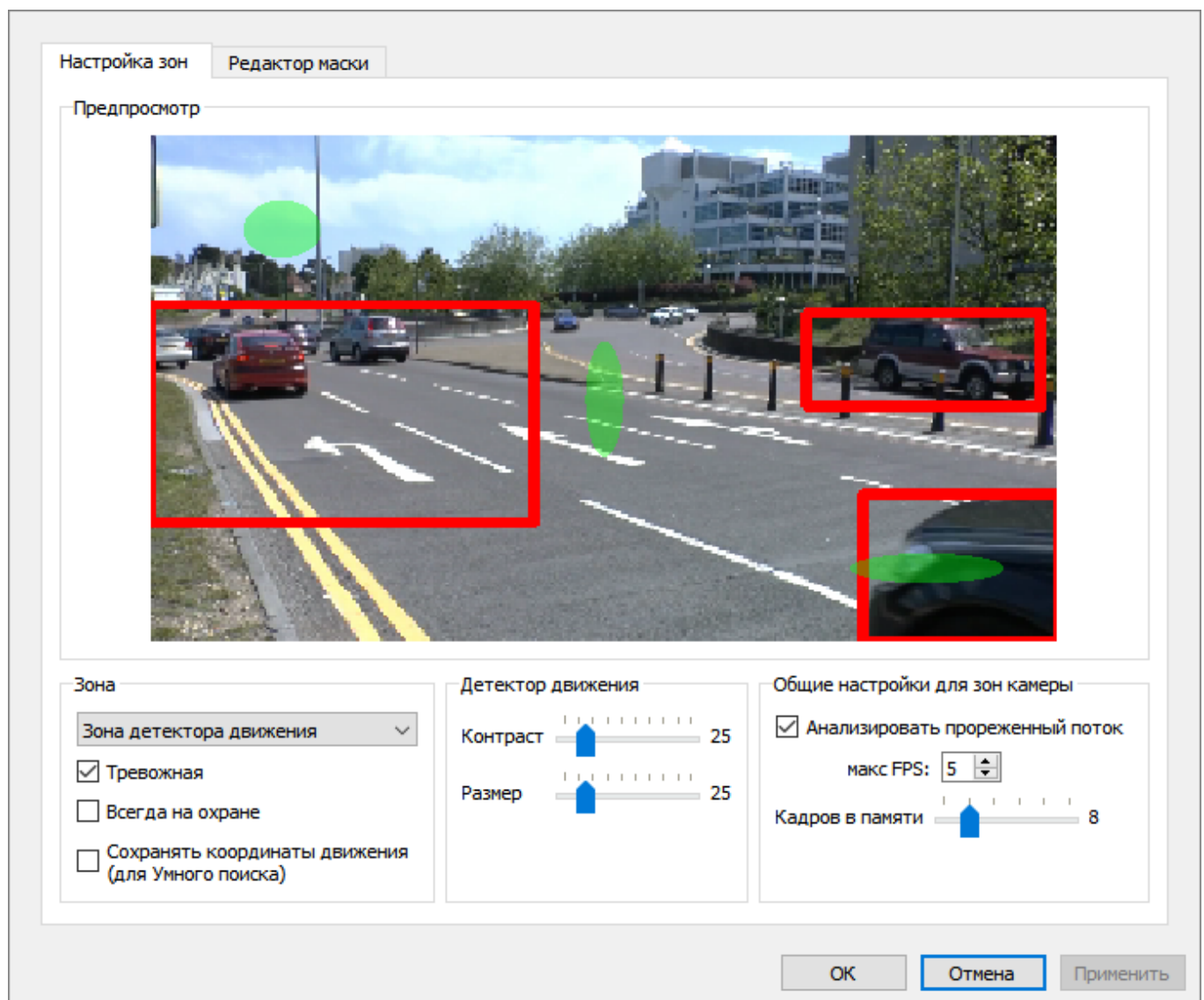


Рис. 172. Окно настройки параметров объекта *Зона*

Таблица 44. Параметры объекта Зона

Параметр	Описание
Вкладка Настройка зон	
Зона	
Типы зон (выпадающий список)	Зона может быть представлена одним из следующих типов: • Зона детектора движения — предназначена для обнаружения движения в выделенной области изображения <i>Камеры</i>. • Зона конфиденциальности — предназначена для скрытия части области изображения <i>Камеры</i>. • Зона общего назначения — предназначена для хранения информации о геометрии зоны.
Тревожная	Активируйте поле, чтобы детектор движения при срабатывании (обнаружении движения) генерировал наступление тревожной ситуации (камера перейдет в режим тревоги, автоматически начнется запись и т. д.). Если поле активировано, поле Сохранять координаты движения (для Умного поиска) будет доступно. Если поле деактивировано, данная зона будет восприниматься как "информационная": никакие действия не предписаны, объект <i>Зона</i> генерирует события при срабатывании детектора движения (эти события можно обрабатывать в макрокомандах).
Всегда на охране	Активируйте поле, чтобы камера постоянно находилась в режиме охраны. Оператору будет запрещено снимать зону с охраны.
Сохранять координаты движения (для Умного поиска)	Активируйте поле, чтобы записывать в БД SecurOS координаты объектов, вызвавших тревогу. Если поле активировано, координаты объектов будут записываться в БД <i>fsindex</i> (детекция <i>Тревог</i> производится при постановке камеры на охрану), что в свою очередь в дальнейшем позволяет выполнять расширенный поиск <i>Тревог</i> по определенным критериям. Внимание! Записи моментов времени начала и конца <i>Тревог</i> в микросекундах заносятся в базу данных SecurOS только в случае использования СУБД PostgreSQL. В случае использования других СУБД время <i>Тревоги</i> не записывается и поиск по архиву будет невозможен. Примечание. Записи времени тревог производятся независимо от того, был ли архив за этот период времени. Подразумевается, что запись с камеры идет постоянно или по обычному детектору движения.
Детектор движения	

Параметр	Описание
Контраст	Передвигая ползунок, настройте контрастность объекта, на который срабатывает детектор. Граничные значения: • 10 — детектор будет срабатывать даже на объекты с низкой контрастностью. • 99 — детектор будет срабатывать только на объекты с высокой контрастностью.
Размер	Передвигая ползунок, задайте размер объекта, на который срабатывает детектор. Граничные значения: • 10 — детектор будет срабатывать даже на маленькие объекты. • 99 — детектор будет срабатывать только на крупные объекты.
Общие настройки для зон камеры	
Анализировать прореженный поток, макс FPS	Отметьте чек-бокс Анализировать прореженный поток, если при детекции движения допускается использовать видеопоток со сниженным FPS. При необходимости укажите максимальное число кадров в секунду, достаточное для детекции движения (спин бокс макс FPS). Примечание. Прореживание осуществляется по опорным кадрам. Если значение, заданное в параметре макс FPS, ниже частоты, полученной таким образом, то выполняется прореживание опорных кадров. По умолчанию чек-бокс не активирован, параметр макс FPS недоступен. При активации диапазон возможных значений параметра макс FPS — [1; 30].
Кадров в памяти	Задайте используемое при анализе движения количество последних поступивших с камеры кадров. Если кадров не достаточно, то процедура детекции движения не начинается (подразумевается начало детекции после старта системы). Допустимые значения от 4 до 128 (кадров). Значение по умолчанию — 8.
Вкладка Редактор маски (см. рис. 173)	
Видео	Область отображения маски на кадре.
Заполнить все	Нажмите кнопку, чтобы маска покрывала весь кадр.
Очистить	Нажмите кнопку, чтобы снять маску с кадра.
Показывать все зоны	Нажмите кнопку для отображения всех зон, дочерних к этой камере.

Параметр	Описание
ОК (Отмена)	Кнопки для завершения настройки с (без) сохранения.

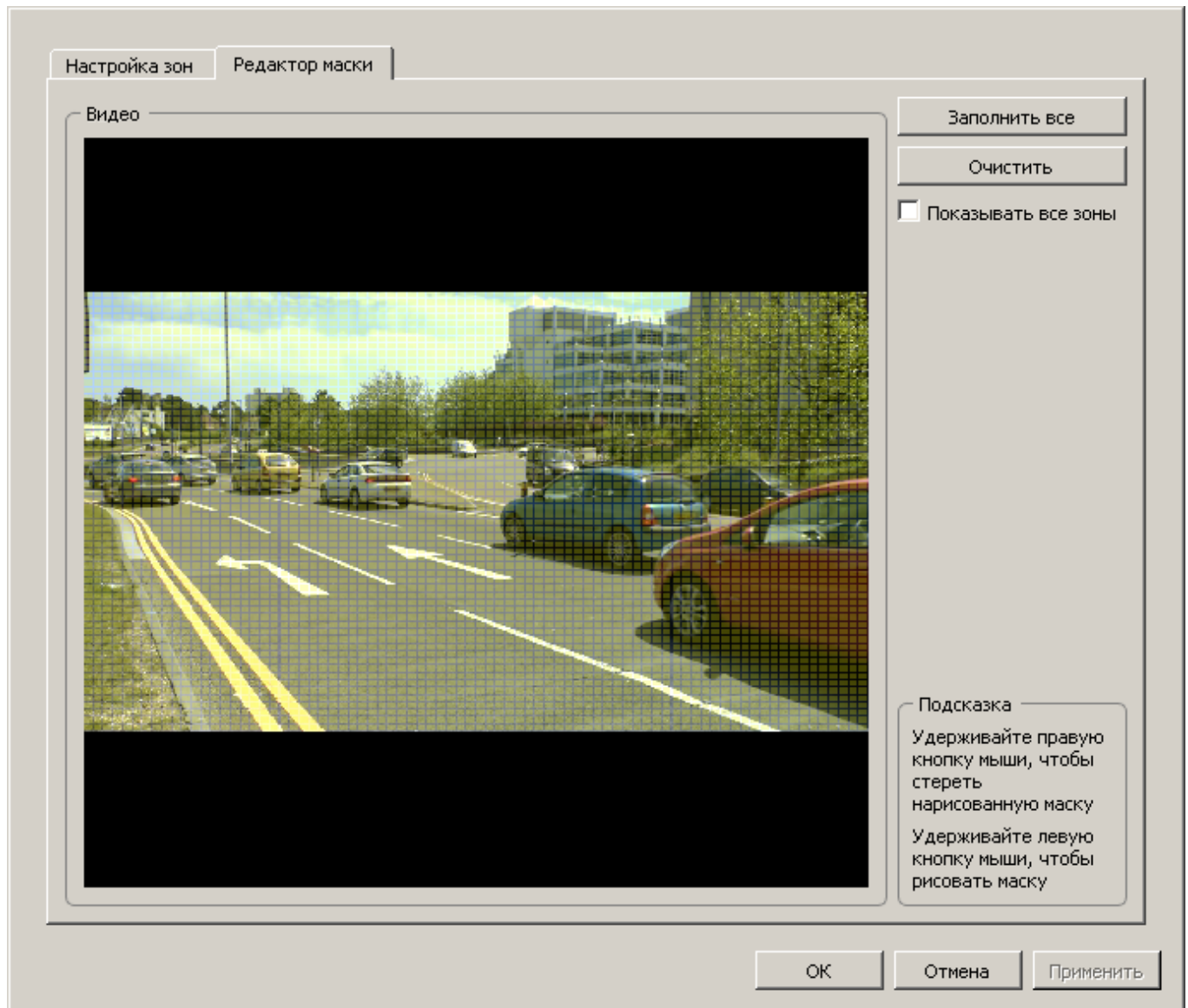


Рис. 173. Окно настройки параметров объекта Зона. Редактор маски

Чтобы отредактировать маску созданной зоны:

1. Перейдите на вкладку **Редактор маски** окна настроек объекта *Зона*.
2. Нажмите правую кнопку мыши и, не отпуская ее, нарисуйте один или несколько прямоугольников внутри ячейки камеры. Эта область будет исключена из зоны обнаружения движения.
3. Нажмите левую кнопку мыши и, не отпуская ее, нарисуйте один или несколько прямоугольников внутри ячейки камеры. Эта область будет добавлена в зону обнаружения движения.

9.12.1.7 Световой детектор

Объект представляет детектор разности освещенности внешней и внутренней зон.

Родительский объект — **Камера**.

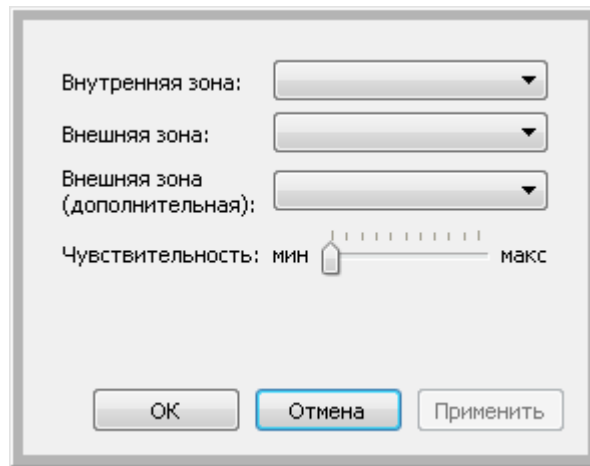


Рис. 174. Окно настройки параметров объекта Световой детектор

Таблица 45. Параметры объекта Световой детектор

Параметр	Описание
Внутренняя зона	Выберите из списка объект <i>Зона</i> , соответствующий внутренней зоне.
Внешняя зона	Выберите из списка объект <i>Зона</i> , соответствующий внешней зоне.
Внешняя зона (дополнительная)	При необходимости проверки уровня освещенности по двум независимым зонам, выберите из списка объект <i>Зона</i> , соответствующий дополнительной (тестовой) внешней зоне.
Чувствительность	Передвигая ползунок, настройте разницу освещенности внутренней и внешней зон, при которой срабатывает детектор. Граничные значения: Мин— детектор срабатывает даже на незначительное изменение освещенности; Макс— детектор срабатывает на значительное изменение освещенности.

9.12.1.8 Конвертер архива

Объект используется для получения архива со всех видеосерверов системы и конвертации его в форматы ASF, AVI, MOV, Evidence и Устаревший формат.

Внимание!

1. В случае, если начало периода конвертации не совпадает со временем ключевого кадра (с точностью до миллисекунд), фактическое начало периода конвертации сместится до времени первого ключевого кадра справа.
2. На системном диске компьютера, где выполняется конвертация, необходимо зарезервировать достаточно свободного места для хранения временных файлов видеоархива.

Примечание. Для просмотра видео, полученного в результате **быстрой конвертации**, рекомендуется использовать медиа-проигрыватель VLC.

Родительский объект — **Компьютер**.

В зависимости от формата, в котором будет сохранен конвертируемый файл, окно настройки параметров объекта будет отличаться (см. рис. 175 и рис. 176).

Тип файла: Evidence

☐ Приложить SecurOS Evidence Manager

Экспортировать в: C:\export

Шаблон имени: {CAMID} ({EXPORT_START_TIME} - {EXPORT_STOP_TIME})

Приоритет архивов: Экспортировать из оперативного, дополнять из долговременного

Алгоритм шифрования: AES-128

Видео

☐ Экспортировать видео со звуком

☐ Прореживание видео

Делитель частоты кадров: 2

☐ Прореживать на сервере

OK Отмена Применить

Рис. 175. Окно настройки параметров объекта Конвертер архива. Тип файла - Evidence

Тип файла: AVI

☐ Разделять на файлы размером: 2000 Мб

Экспортировать в: c:\export

Шаблон имени: {CAMID} {EXPORT_START_TIME} - {EXPORT_STOP_TIME}

Приоритет архивов: Экспортировать из оперативного, дополнять из долговременного

Видео

☐ Быстрый экспорт

☐ Экспортировать видео со звуком

Кодек: MPEG4

Качество: Высокое

☐ Прореживание видео

Делитель частоты кадров: 2

☐ Прореживать на сервере

Аудио

Кодек: MP3

Наложение логотипа

 Логотип не выбран

Выбрать

Расположение: левый верхний угол

OK Отмена Применить

Рис. 176. Окно настройки параметров объекта Конвертер архива. Тип файла - AVI/ASF/MOV

Таблица 46. Параметры объекта Конвертер архива

Параметр	Описание
Тип файла	Выберите формат, в котором будет записываться конвертируемый файл: ASF, AVI, MOV, Evidence или Устаревший формат. Значение по умолчанию - ASF. Примечания: 1. Формат Evidence используется для экспорта в специальный контейнер ISS. Просмотр сконвертированного видео возможен только с помощью проигрывателя SecurOS Evidence Manager. 2. При экспорте в формат Evidence в один файл можно записать архив сразу нескольких <i>Камер</i>.
Приложить SecurOS Evidence Manager	Отметьте флажок, чтобы приложить к создаваемому архиву проигрыватель SecurOS Evidence Manager (см. Руководство пользователя SecurOS Evidence Manager).
Разделять на файлы размером	Максимальный размер каждого из файлов, составляющих архив. По умолчанию принимает значение 2000 МБ. Максимальное значение — 10000 МБ. Внимание! Некоторые медиа-проигрыватели не поддерживают AVI-файлы размером более 2 ГБ. При экспорте в форматы AVI и ASF возможно разбиение архива на несколько файлов вне зависимости от заданного значения параметра. Разбиение осуществляется автоматически, если: • Видеоархив содержит кадры с различным разрешением. При смене разрешения будет записан новый файл; • Выполняется быстрый экспорт видеоархива (см. Быстрый экспорт) и происходит смена кодека видео; • Выполняется экспорт как из <i>Оперативного</i>, так и из <i>Долговременного архивов</i>. При этом создается два отдельных файла: один для всех записей <i>Оперативного архива</i>, другой - для всех записей <i>Долговременного</i>.
Экспортировать в	Директория для сохранения файлов сконвертированного архива. Допустимые значения: любая доступная директория на жестких дисках локального компьютера. Необязательный параметр. Если не задан, файл сохраняется в директорию с: \export. Примечание. При указании имени директории допускается использование макрокоманд шаблона имени файла (см. описание параметра Шаблон имени).

Параметр	Описание
Шаблон имени	Маска имен создаваемых файлов. Может формироваться из любой комбинации <i>допустимых символов</i> и <i>макроподстановок</i>. Необязательный параметр. По умолчанию принимает значение {CAMID} ({EXPORT_START_TIME} – {EXPORT_STOP_TIME}) Допускается использовать любые символы, разрешенные ОС для использования в именах файлов. Для задания имен файлов в системе определены следующие макроподстановки (наличие фигурных скобок обязательно): • {SID} — порядковый номер сессии экспорта. Сбрасывается на 0 при перезапуске SecurOS; • {CAMID} — идентификатор камеры при экспорте видео или идентификатор свободного микрофона при экспорте только аудио-файла; • {CAMNAME} — имя камеры при экспорте видео или имя свободного микрофона при экспорте только аудио-файла; • {COMPID} — идентификатор компьютера (видеосервера); Внимание! При конвертации в формат Evidence архива сразу нескольких <i>Камер</i> макроподстановки CAMID, CAMNAME и COMPID игнорируются.
	• {SOURCE_TYPE} — тип объекта, с помощью которого был получен исходный архивный файл. Может принимать следующие значения: – video — архив был записан <i>Камерой</i>; – audio — архив был записан <i>Микрофоном</i>. • {COMMENT} — комментарий инициатора экспорта, используется при запуске экспорта из программы или при экспорте закладки; • {CUR_YEAR} — текущий год в формате "YYYY"; • {CUR_MONTH} — текущий месяц в формате "MM". При выводе в имени файла незначащий ноль отрезается; • {CUR_DAY} — текущий день в формате "DD". При выводе в имени файла незначащий ноль отрезается; • {CUR_HOUR} — текущий час в формате "HH". При выводе в имени файла незначащий ноль отрезается; • {CUR_MINUTE} — текущая минута в формате "MM". При выводе в имени файла незначащий ноль отрезается; • {CUR_SEC} — текущая секунда в формате "SS". При выводе в имени файла незначащий ноль отрезается;

Параметр	Описание
	• {CUR_FRAC} — текущая миллисекунда в формате "SSS". При выводе в имени файла незначащий ноль отрезается; • {CUR_DATE} — текущая дата в формате "YYYY-MM-DD" (например, "2011-12-31"); • {CUR_TIME} — текущее время в формате "HH'MM'SS" (например, "23'05'06"); • {EXPORT_START_TIME} — начало временного интервала периода конвертации в формате "YYYY-MM-DD HH'MM'SS" (например, "2011-12-31 23'02'06"); • {EXPORT_START_YEAR} — год начала периода конвертации; • {EXPORT_START_MONTH} — месяц начала периода конвертации (число); • {EXPORT_START_MONTH_STR} — месяц начала периода конвертации (строка); • {EXPORT_START_DAY} — день начала периода конвертации; • {EXPORT_START_HOUR} — час начала периода конвертации; • {EXPORT_START_MINUTE} — минута начала периода конвертации; • {EXPORT_START_SEC} — секунда начала периода конвертации; • {EXPORT_START_FRAC} — миллисекунда начала периода конвертации; • {EXPORT_STOP_TIME} — конец временного интервала периода конвертации в формате "YYYY-MM-DD HH'MM'SS" (например, "2011-12-31 23'02'06"); • {EXPORT_STOP_YEAR} — год окончания периода конвертации; • {EXPORT_STOP_MONTH} — месяц окончания периода конвертации (число); • {EXPORT_STOP_MONTH_STR} — месяц окончания периода конвертации (строка); • {EXPORT_STOP_DAY} — день окончания периода конвертации; • {EXPORT_STOP_HOUR} — час окончания периода конвертации;

Параметр	Описание
	• {EXPORT_STOP_MINUTE} — минута окончания периода конвертации; • {EXPORT_STOP_SEC} — секунда окончания периода конвертации; • {EXPORT_STOP_FRAC} — миллисекунда окончания периода конвертации.
Приоритет архивов	Выберите последовательность просмотра архивов при экспорте из них требуемых фрагментов. Возможные значения: • Экспортировать из оперативного, дополнять из долговременного — при экспорте фрагмента сначала будет просматриваться <i>Оперативный архив</i>. При отсутствии в нем требуемого фрагмента будет просматриваться <i>Долговременный архив</i>; • Экспортировать из долговременного, дополнять из оперативного — при экспорте фрагмента сначала будет просматриваться <i>Долговременный архив</i>. При отсутствии в нем требуемого фрагмента будет просматриваться <i>Оперативный архив</i>. Примечание. Если выбрано значение Экспортировать из долговременного, дополнять из оперативного, будет экспортировано только то сопровождающее аудио, которое записано в <i>Долговременном архиве</i>.
Алгоритм шифрования	Выберите алгоритм шифрования данных при конвертации видео в формат Evidence. Возможные значения: • AES-128; • AES-192; • AES-256. Внимание! Файл будет зашифрован только в том случае, если в параметрах задачи на экспорт будет задан пароль для защиты файла от несанкционированного доступа (см. Краткое руководство пользователя SecurOS, раздел Экспорт архива).
Видео (параметры конвертации видео)	

Параметр	Описание
Быстрый экспорт	Конвертация с сохранением исходного кодека и качества видео. Позволяет существенно повысить скорость конвертации и снизить нагрузку на центральный процессор. Сохранение исходного кодека и качества возможно для видео форматов H.263, H.264, H.265, MJPEG, MPEG-4. Примечание. При обычном экспорте (флажок Быстрый экспорт снят) выполняется перекодировка видеоданных, которая осуществляется на одном ядре процессора, что требует дополнительных вычислительных мощностей и может занять много времени.
Экспортировать видео со звуком	Конвертация с сохранением звукового сопровождения при его наличии. Примечание. Экспорт видео со звуком недоступен для формата Устаревший формат.
Кодек	Видео кодек, который будет использоваться при конвертации архива. Возможные значения: • MJPEG; • MPEG-4.
Качество	Выберите качество видео, получаемого в результате конвертации архива.
Прореживание видео (использовать прореживание при конвертации). Отметьте флажок для задания параметров прореживания	
Делитель частоты кадров	Коэффициент прореживания кадров архива при конвертации. Диапазон возможных значений: [2; 100].
Прореживать на сервере	Режим прореживания только по ключевым кадрам (см. Прореживание видеопотока). Архив будет предварительно прорежен на том <i>Видеосервере</i>, на котором он хранится.
Аудио (параметры конвертации аудио)	
Кодек	Аудио кодек, который будет использоваться при конвертации архива. Возможные значения: • PCM; • WMA (для контейнера ASF); • MP3 (для контейнера AVI).
Наложение логотипа (добавлять логотип на видео)	
Внимание! При быстром экспорте (см. Быстрый экспорт) логотип не накладывается.	

Параметр	Описание
Выбрать (кнопка)	Нажмите кнопку и используйте диспетчер файлов чтобы выбрать файл с изображением логотипа. Файл с логотипом должен удовлетворять следующим требованиям: • формат файла — PNG; • максимальный размер изображения — 500×500 пикселей; • максимальный размер файла — 500 КВ. В случае удачной загрузки файла блок будет выглядеть как показано на рис. 177. Для просмотра загруженного логотипа нажмите кнопку  (Просмотреть логотип). Чтобы изменить масштаб изображения используйте колесо прокрутки мыши. Чтобы удалить загруженный логотип, нажмите кнопку Удалить.
Расположение	Расположение логотипа в кадре. Возможные значения: • левый верхний угол; • правый верхний угол; • правый нижний угол; • левый нижний угол.

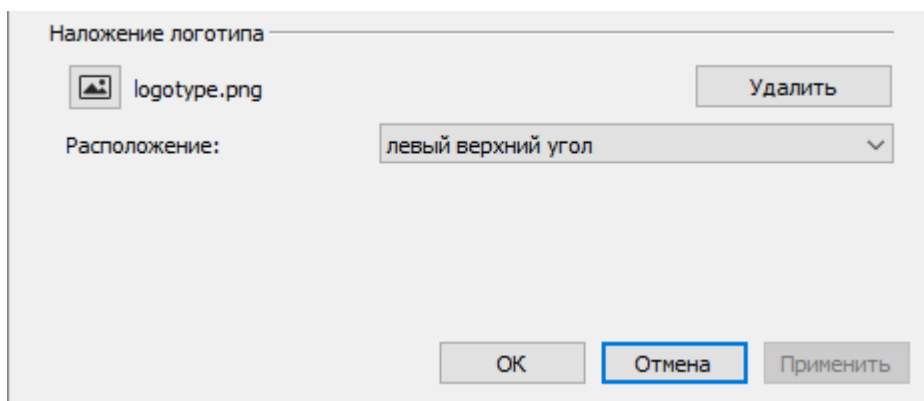


Рис. 177. Внешний вид блока Наложение логотипа после загрузки файла логотипа

9.12.1.8.1 Цифровая подпись

В ОС **Linux** функциональность не поддерживается.

Цифровая подпись с помощью сертификата гарантирует, что подписанный файл не был подменен или отредактирован после создания. В SecurOS подпись файлов осуществляется с применением стандарта **PKCS#7 Signed data detached signature**.

Возможность подписывать файлы с помощью сертификата доступна на *Компьютерах* с любой ролью (см. **Компьютер**).

- Цифровая подпись на *Видеосервере* возможна в случае, если для экспорта выбран *Конвертер архива*, настроенный в любом из **Профилей рабочего места оператора**;
- Цифровая подпись на *Рабочем месте оператора* возможна в случае, если для экспорта выбран *Конвертер архива*, настроенный на этом **Рабочем месте оператора**, или в любом из **Профилей рабочего места оператора**.

После включения функциональности цифровой подписи *Конвертер архива* будет автоматически подписывать аудио- и видеофайлы с помощью выбранного сертификата.

Включение функциональности выполняется непосредственно на *Рабочем месте оператора* или *Видеосервере*. Предварительно администратор должен установить на компьютере сертификат, удовлетворяющий следующим требованиям:

- Сертификат имеет свойство **Key usage** с установленным битом **Digital Signature**;
- Сертификат имеет свойство **Enhanced key** с атрибутом **Code signing**.

Процедура включения функциональности и **Утилита проверки цифровой подписи** подробно описаны в **Кратком руководстве пользователя SecurOS**.

Примечание. Для проверки и демонстрации работы цифровой подписи можно использовать самоподписанный сертификат, созданный с помощью утилиты **Certificate Generator**.

9.12.1.8.2 Отображение субтитров в экспортированном видео

Субтитры могут быть наложены на кадр живого видео следующими способами:

- с помощью *Модуля SecurOS POS* (см. **Руководство пользователя SecurOS POS**);
- из **Скрипта Node.js** с помощью команды `ADD_SUBTITLES` (см. **Руководство программиста SecurOS**).

Наложенные субтитры сохраняются в *Оперативном* и *Долговременном* архивах.

При экспорте в форматы AVI/ASF/MOV или Evidence наложенные субтитры сохраняются в архиве только в том случае, если выполняется экспорт с перекодировкой исходного видеопотока (опция **Быстрый экспорт** не выбрана). Если опция **Быстрый экспорт** выбрана, субтитры в экспортированном файле не сохраняются. Субтитры в экспортированном видео являются частью кадра и не могут быть скрыты.

Независимо от наличия в кадре субтитров, наложенных одним из указанных выше способов, на экспортированное видео автоматически накладываются следующие данные:

- Идентификатор камеры — накладывается в левом нижнем углу кадра.
- Дата и время кадра — накладывается в правом нижнем углу кадра.

9.12.1.9 Профиль экспорта архива

Профиль экспорта архива — специальный объект, который предназначен для быстрой настройки функциональности экспорта архива на любом *Рабочем месте оператора* сети SecurOS. Настройки объекта полностью аналогичны настройкам объекта **Конвертер архива**, за исключением параметра **Экспортировать в**.

При использовании *Профиля экспорта архива* для создания задачи на экспорт и выполнения процедуры экспорта используется только *Медиа Клиент*.

Так же, как и при использовании *Конвертера архива*, файл архива также может быть подписан с помощью сертификата (см. [Цифровая подпись](#)). При этом подписать файл можно на любых *Компьютерах* без дополнительных ограничений.

Родительский объект — [Объект охраны](#).

9.12.1.10 Архиватор

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

В ОС **Linux** функциональность не поддерживается.

Объект используется для копирования записей указанных камер из *Оперативного архива* в *Долговременный архив* в формате SecurOS (см. [Архивы SecurOS](#)) и просмотра файлов долговременного архива в *Медиа Клиенте*.

Родительский объект — [Компьютер](#).

Режим архивирования

По команде ⓘ Расписание: Не выбрано

Хранение архива:

Директория	Емкость	Видео Чтение	Видео Запись
C:\	105.12 ГБ свободно из 237.92 ГБ	✓	✓

Добавить директорию Изменить Удалить

Камеры:

Фильтровать по названию и идентификатору Сбросить фильтр

Название	Макс. FPS	Удалять спустя
✓ SecurOS Premium [1]		
✓ Компьютер VIDEO SERVER [VIDEO SERVER]		
✓ Камера 1 [1]	30	183 дня
□ Камера 2 [2]	-	-
□ Камера 3 [3]	-	-

Камера 3 [3] задана в настройках Архиватор 2 [2]

☐ Архивировать сопровождающее аудио

ОК Отмена Применить

Рис. 178. Окно настройки параметров объекта Архиватор

Таблица 47. Параметры объекта Архиватор

Параметр	Описание
Режим архивирования	
Режим архивирования	Выберите из списка режим, в котором будет выполняться копирование файлов <i>Оперативного архива</i>: - По команде — в данном режиме копирование начнется только при выполнении <i>Макрокоманды</i> или вызове метода, заданного в <i>Скрипте Node.js</i>. Скопированы будут только те записи, которые соответствуют параметрам команды (подробнее см. Руководство программиста SecurOS, команда ADD_TASK). Внимание! При обновлении версии SecurOS 9.5 (и более ранних) на версию 9.6 (и более поздние) необходимо отредактировать все используемые в системе Макрокоманды и Скрипты Node.js, относящиеся к созданию <i>Долговременного архива</i>. - Постоянный — в данном режиме непрерывно копируются все имеющиеся на данный момент архивы всех <i>Камер</i>, выбранных в настройках объекта. - По расписанию — аналогично Постоянному режиму, но копирование выполняется только во время действия выбранного временного интервала (см. параметр Расписание ниже). Примечание. Копирование по расписанию позволяет выбрать для выполнения операции такой период, когда общая загрузка системы минимальна. Например, ночной период.
Расписание	Определяет расписание для копирования оперативного архива. Доступен, если параметр Режим архивирования принимает значение По расписанию.
Хранение архива (таблица)	
Директория	Список дисков, доступных для записи и/или чтения архива данным <i>Архиватором</i>. Примечание. При первом запуске таблица не содержит записей.
Емкость	Информация о свободном месте на диске.
Видео	Доступный режим работы с заданной директорией. Возможные значения: - Чтение — директория доступна только для чтения видео и сопровождающего аудио. - Чтение + Запись — директория доступна для чтения и записи видео и сопровождающего аудио.
Кнопки	

Параметр	Описание
Добавить директорию	Нажмите кнопку, чтобы добавить новую директорию для хранения долговременного архива. Подробнее см. Добавление директории для записи архива .
Изменить	Нажмите кнопку, чтобы изменить параметры директории, выделенной в таблице. Подробнее см. Изменение директории для записи архива .
Удалить	Нажмите кнопку, чтобы удалить директорию, выделенную в таблице. Подробнее см. Удаление директории для записи архива .
Камеры	
Фильтр	Для поиска <i>Камеры</i> по части имени или идентификатора введите в поле требуемые символы; в дереве автоматически отобразятся только те <i>Камеры</i> , имя или идентификатор которых соответствуют заданным условиям поиска. Для того, чтобы очистить поле, нажмите кнопку Сбросить фильтр .
Список камер (таблица)	
Название	Для добавления камеры в список <i>Камер</i>, с которыми будет работать данный <i>Архиватор</i>, отметьте соответствующий флажок слева от объекта <i>Камера</i>. Примечания: - Камеры, выбранные для работы с другим <i>Архиватором</i>, нельзя добавить в список текущего <i>Архиватора</i>. Флажки таких камер недоступны для выбора. При выделении такой камеры система выведет подсказку с указанием имени <i>Архиватора</i>, в настройках которого выбрана данная <i>Камера</i>. - Камеры, работающие с удаленным архивом с помощью <i>EdgeStorage Gate</i>, в списке <i>Камер</i> не отображаются.
Макс. FPS	Задайте максимальную частоту кадров (от 1 до 60) для записи <i>Долговременного архива</i> (см. Прореживание видеопотока). Если значение не задано, частота кадров видео <i>Долговременного архива</i> будет равна частоте кадров видео <i>Оперативного архива</i> .

Параметр	Описание
Удалять спустя	Задайте максимальный срок хранения фрагмента в <i>Долговременном архиве</i> (в днях). Внимание! Срок хранения отсчитывается не от момента размещения фрагмента в <i>Долговременном архиве</i>, а от момента записи фрагмента в <i>Оперативном архиве</i>. Например: фрагмент был записан в <i>Оперативный архив</i> 10 апреля, а помещен в <i>Долговременный архив</i> 15 апреля. Если значение параметра Удалять спустя равно 15, то фрагмент будет удален из <i>Долговременного архива</i> 25 апреля (т.е. через 10 дней после его копирования). Примечание. Если свободного места на дисках недостаточно для записи долговременного архива, архив будет удален ранее указанного срока хранения для освобождения места для записи новых файлов. Если значение не задано, долговременный архив будет перезаписываться в режиме "по кольцу" (старые файлы удаляются, на их место записываются новые).
Архивировать сопровождающее аудио	Отметьте флажок для копирования сопровождающего аудио из <i>Оперативного архива</i> в <i>Долговременный</i> (при его наличии). По умолчанию не отмечен. Примечание. Источником сопровождающего аудио является <i>Микрофон</i>, связанный с выбранной для архивации <i>Камерой</i> (см. параметр Название). Внимание! Если в <i>Удаленной системе</i> не поддерживается запись сопровождающего аудио в <i>Долговременный архив</i> (версия SecurOS, установленная в <i>Удаленной системе</i>, ниже 11.8), <i>Архиватор Центра Мониторинга</i> не сможет получить доступ к соответствующим аудиофайлам.

Добавление директории для записи архива

Чтобы добавить директорию для записи долговременного архива:

1. В окне настройки параметров объекта (см. рис. 178) нажмите кнопку **Добавить директорию**.
2. Система выведет окно **Добавить новую директорию** (см. рис. 179).

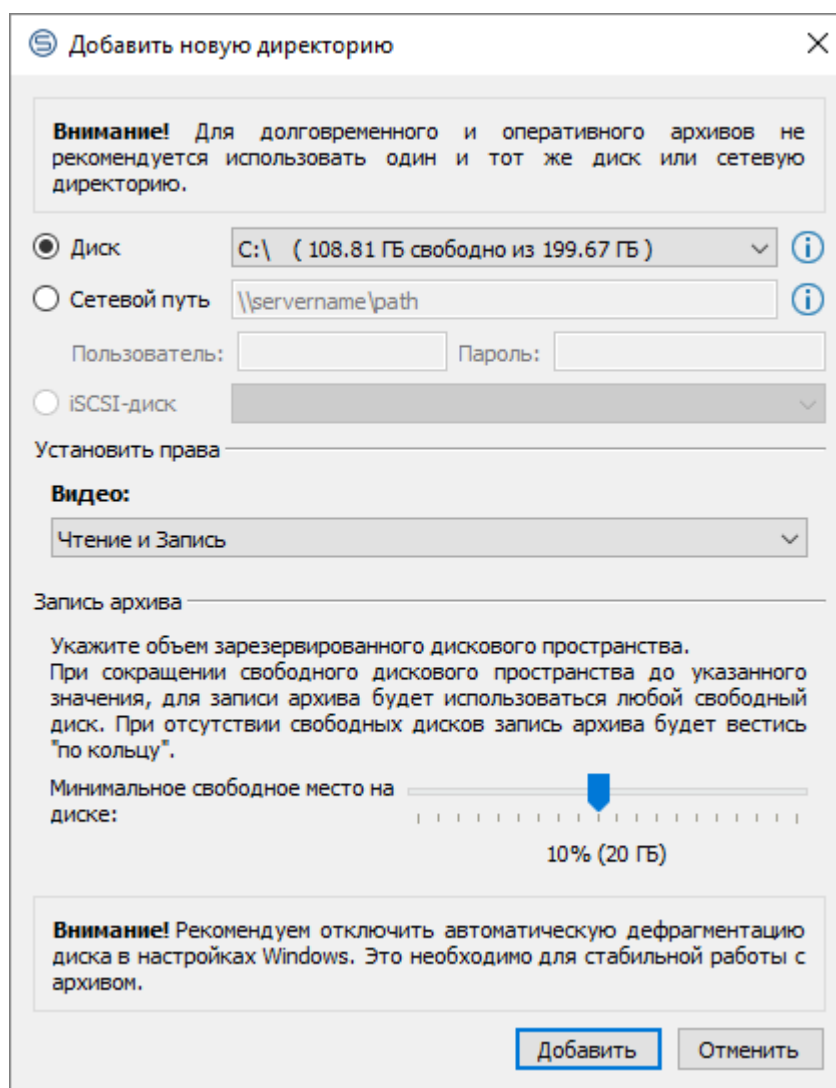


Рис. 179. Окно Добавить новую директорию

3. Выберите опцию для сохранения архива (**Диск/Сетевой путь**) и выберите в списке жесткий диск или укажите путь к сетевой папке (имя пользователя и пароль указываются опционально).

Примечания:

1. В списке опции **Диск** автоматически отображаются все жесткие диски, доступные на данном *Видеосервере*.
2. При отсутствии связи с *Видеосервером* в списке будут отображены все буквы алфавита от A до Z.
3. Некоторые сетевые диски могут отсутствовать в списке опции **Диск**. Для подключения сетевого диска рекомендуется использовать опцию **Сетевой путь**.
4. Использование сетевой папки для записи архива возможно только если *Видеосервер* или *Нода* работает под управлением ОС Windows.

Внимание! Одну и ту же **Директорию** для записи *Оперативного* (см. **Архив** в настройках объекта *Компьютер*) и *Долговременного* архивов использовать не рекомендуется.

4. В поле **Видео** (блок **Установить права**) задайте права доступа к директории. Возможные значения:
 - Чтение — директория будет доступна только для чтения.
 - Чтение и Запись — директория будет доступна для чтения и записи.

5. В блоке **Запись архива** проверьте и, при необходимости, скорректируйте значение параметра **Минимальное свободное место на диске**.

Примечания:

1. Значение параметра вычисляется и устанавливается автоматически при добавлении директории.
2. Рекомендуется выделять не менее 10% от общего объема диска. Данное значение позволяет записывать архив максимально эффективно.

6. Для сохранения изменений нажмите кнопку **Добавить**.

Изменение директории для записи архива

Чтобы изменить параметры директории для записи *Долговременного архива*:

1. Выберите требуемую запись в таблице **Хранение архива** (см. рис. 178), нажмите кнопку **Изменить**.
2. Система выведет окно **Изменить текущую директорию** (см. рис. 180).

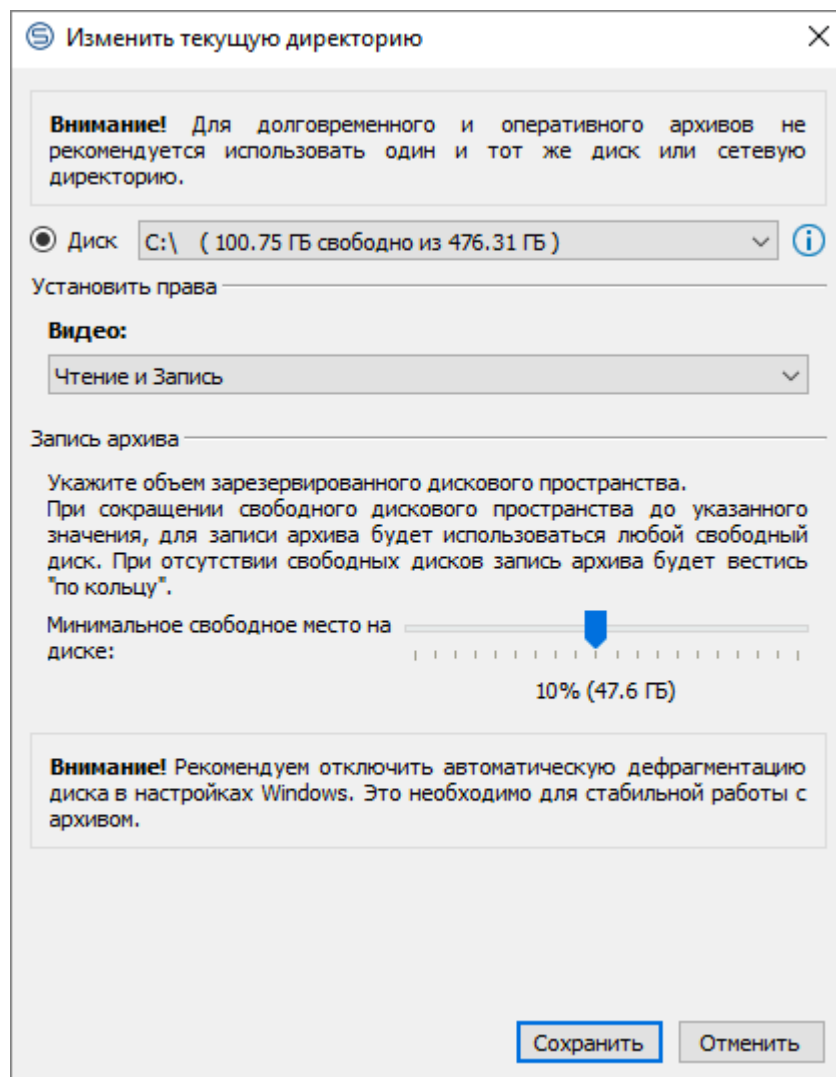


Рис. 180. Окно Изменить текущую директорию

3. Измените текущие параметры директории.

Внимание! Одну и ту же **Директорию** для записи *Оперативного* (см. **Архив** в настройках объекта *Компьютер*) и *Долговременного* архивов использовать не рекомендуется.

4. В поле **Видео** (блок **Установить права**) измените права доступа к архиву. Возможные значения:
- Чтение — архив будет доступен только для чтения.
 - Чтение и Запись — архив будет доступен для чтения и записи.
5. В блоке **Запись архива** проверьте и, при необходимости, скорректируйте значение параметра **Минимальное свободное место на диске**.

Примечания:

1. Значение параметра вычисляется и устанавливается автоматически при добавлении директории.
 2. Рекомендуется выделять не менее 10% от общего объема диска. Данное значение позволяет записывать архив максимально эффективно.
-

6. Для сохранения изменений нажмите кнопку **Сохранить**.

Удаление директории для записи архива

Чтобы удалить директорию, выберите требуемую запись в таблице **Хранение архива** (см. рис. 178), нажмите кнопку **Удалить**. Для подтверждения удаления нажмите кнопку **Да** на панели сообщения (см. рис. 181).

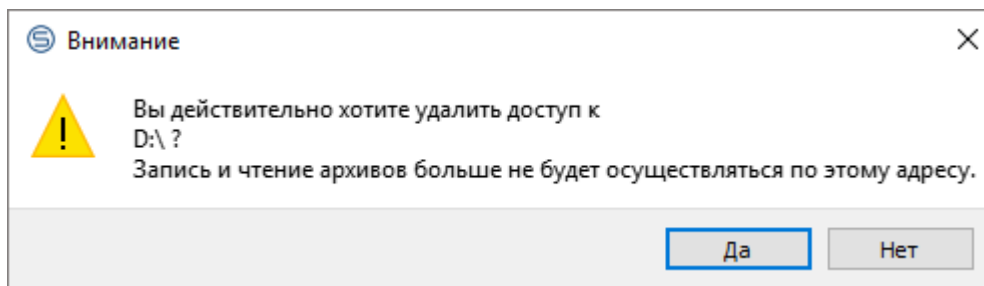


Рис. 181. Подтверждение удаления директории

9.12.1.11 Image Processor

Объект используется для обработки и последующего экспорта изображения (кадра) в файл или базу данных.

Родительский объект — **Компьютер**.

Параметры для редактирования отсутствуют.

При обработке изображения возможно выполнение следующих операций:

- обрезка исходного изображения с указанием относительного размера и положения результирующей области;
- нанесение на изображение незакрашенных прямоугольников заданного цвета, толщины линии и положения.

При экспорте изображения в файл кадр сохраняется на жестком диске родительского *Компьютера*, а при экспорте в базу данных может быть сохранен в любой *Базе данных*, настроенной как объект в дереве объектов SecurOS.

Для обработки и экспорта кадров используется команда EXPORT, которая определяется с помощью объекта **Скрипт Node.js**. Синтаксис команды экспорта описан в **Руководстве программиста SecurOS**.

Дополнительные параметры процедуры экспорта

Помимо параметров, задаваемых в команде, процедура экспорта регулируется следующими дополнительными параметрами:

- `deltaArchive` — временное смещение, в секундах, от заданного в команде времени экспорта (Т). Используется для задания интервала, в котором будет осуществляться поиск кадра в архиве: $[T - \text{deltaArchive}; T + \text{deltaArchive}]$. По умолчанию принимает значение 600;
- `downloadTimeout` — время ожидания поступления кадра в архив, в секундах. Используется при экспорте кадров в режиме реального времени. По умолчанию принимает значение 20.

Настройка дополнительных параметров возможна в ОС Windows и ОС Linux. Порядок настройки для каждой ОС описан ниже:

- **Настройка для ОС Windows.**
- **Настройка для ОС Linux.**

Настройка для ОС Windows

1. Остановите службу Video Management System Server.
2. Откройте раздел `\HKLM\SOFTWARE\ISS\SecurOS\NISS400\ImageProcessor`, и установите для параметров `deltaArchive` и `downloadTimeout` требуемые значения.
3. Запустите службу Video Management System Server.

Настройка для ОС Linux

1. Остановите демон `vms_server` с помощью команды `sudo service vms_server stop`.
2. Откройте для редактирования файл `/etc/xdg/iss/securos.conf` и добавьте в него строки `ImageProcessor\deltaArchive=X` и `ImageProcessor\downloadTimeout=X`, где X — требуемые значения.
3. Запустите демон `vms_server` с помощью команды `sudo service vms_server start`.

9.12.1.12 RTSP-сервер

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

Объект предназначен для передачи живого или архивного видео формата H.264 с *Видеосерверов SecurOS* на внешние системы по протоколу RTSP/RTP. Видеопоток может передаваться как по протоколу UDP, который используется *RTSP-сервером* по умолчанию, так и по протоколу TCP. Тип используемого транспортного протокола определяется настройками внешнего приложения.

При передаче видео с *RTSP-сервера* действуют следующие ограничения:

- общее количество *Камер*, подключаемых к одному объекту *RTSP-сервер* — не более 1000;
- количество потребителей живого или архивного видео на каждую *Камеру* — не более 800.

Внимание!

1. Поддерживается передача любого видеопотока многопоточной камеры.
2. Передача синхронного аудио не поддерживается.

Родительский объект — *Компьютер\группа Интеграция и Автоматизация*.

Порт RTSP: 554 Порт HTTP: 81

RTSP спецификация: RFC 2326

Кодек: H.264

☐ Запрашивать аутентификацию

Камеры:

Фильтровать по имени или идентификатору Сбросить фильтр

- SecurOS Premium [1]
 - Компьютер DESKTOP-M8EBR89 [DESKTOP-M8EBR89]
 - ☒ Камера 1 [1]
 - ☐ Камера 2 [2]
 - ☒ Камера 3 [3]
 - ☐ Камера 4 [4]
 - Компьютер REMOTE_SERVER [REMOTE_SERVER]
 - ☒ Камера 5 [5]
 - ☒ Камера 6 [6]
 - ☐ Камера 7 [7]
 - ☒ Камера 8 [8]

Доступно: неограниченно, выбрано: 5

OK Отмена Применить

Рис. 182. Параметры объекта RTSP-сервер

Таблица 48. Параметры объекта RTSP-сервер

Параметр	Описание
Порт RTSP	Номер порта SecurOS для взаимодействия с внешней системой по протоколу RTSP. Используется для получения живого и архивного видео с помощью внешнего приложения (медиаплеера). Диапазон возможных значений: [1; 32768]. По умолчанию принимает значение 554.
Порт HTTP	Номер порта SecurOS для взаимодействия с внешней системой по протоколу HTTP. Используется для получения списка архивных видео записей через web-браузер. Диапазон возможных значений: [1; 32768]. По умолчанию принимает значение 81. Внимание! Для определения свободного порта при изменении значения по умолчанию рекомендуется выполнить в командной строке запрос <code>netstat -aon more</code>.

Параметр	Описание
RTSP спецификация	Протокол передачи архивного видео. Возможные значения: • RFC 2326 — значение по умолчанию. Рекомендуется для использования в большинстве случаев; • UDC — выберите данное значение, если проигрывание запрошенного архивного видео в обратном направлении по протоколу RFC 2326 происходит с ошибками.
Кодек	Кодек для передачи видео. Значение должно совпадать с исходным кодеком потока. Возможные значения: • Все — выберите данное значение, чтобы работать со всеми нижеперечисленными кодеками. Имеются ограничения. За дополнительной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems; • H.264 — значение по умолчанию; Внимание! Если выбрано значение H.264, а исходный видеопоток имеет другой кодек, то будет выполняться транскодирование. Транскодирование поддерживается только на графических процессорах Intel. Использование транскодирования создает дополнительную нагрузку на <i>Видеосервер</i>. • H.265; • MPEG4; • MJPEG.
Запрашивать аутентификацию	Отметьте флажок, чтобы к <i>RTSP-серверу</i> могли подключаться только авторизованные пользователи SecurOS. Внимание! Работа с пользователями домена Windows Active Directory не поддерживается. Если отмечен, перед соединением будут проверяться права доступа <i>Пользователя</i> SecurOS к <i>Камерам</i>, с которых запрашивается видео. Для получения видео уровень доступа авторизованного пользователя к <i>Камерам</i> должен быть не ниже, чем  (Просмотр). Если в системе есть <i>Пользователи</i>, настройки которых должны быть изменены для работы с <i>RTSP-сервером</i> после обновления на версию 10.8, в окне будет выведен значок . Подробнее о таких <i>Пользователях</i> см. Обновление версии 10.7 и более ранних. Настройки <i>Пользователей</i>, созданных после обновления на версию 10.8, изменять не требуется.
Камеры	

Параметр	Описание
Дерево объектов	Список камер SecurOS, с которых возможна передача живого и архивного видео на внешнюю систему по протоколу RTSP. Структура дерева аналогична структуре <i>Дерева объектов</i> SecurOS. Для выбора <i>Камеры</i> отметьте соответствующий чек-бокс слева от объекта. Для выбора всех <i>Камер</i> компьютера отметьте чек-бокс слева от соответствующего <i>Компьютера</i>. Для выбора всех <i>Камер</i> всех <i>Компьютеров</i> объекта охраны, отметьте чек-бокс слева от <i>Объекта охраны</i>. Примечание. Временно отключенные <i>Камеры</i> (см. Отключение объекта) выделяются в дереве объектов серым (см. рис. 182, Камера 1). Внимание! Количество камер, с которых возможна одновременная передача видео, является лицензируемым параметром. При превышении заданного в лицензии параметра кнопка ОК блокируется.
Кнопки	
ОК (Отмена)	Сохранение заданных значений и выход из окна настройки (заккрытие окна без сохранения изменений).

За более подробной информацией об использовании *RTSP-сервера* обращайтесь к вашему региональному представителю Intelligent Security Systems.

9.12.1.13 ONVIF-сервер

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

Объект предназначен для передачи живого видео и архивного видео различных форматов с *Видеосерверов* SecurOS на внешние системы по протоколу RTSP и управления телеметрией камер SecurOS из внешней системы по протоколу ONVIF. При использовании встроенного RTSP-сервера возможна юникаст/мультикаст трансляция с выбранных камер без использования отдельного объекта SecurOS **RTSP-сервер**.

Родительский объект — *Компьютер\группа Интеграция и Автоматизация*.

Окно настройки параметров содержит следующие закладки:

- Закладка **Общие**.
- Закладка **Встроенный RTSP-сервер**.

За более подробной информацией об использовании *ONVIF-сервера* обращайтесь к вашему региональному представителю Intelligent Security Systems.

9.12.1.13.1 Закладка Общие

Общие Встроенный RTSP-сервер

RTSP-сервер: RTSP-сервер 1

Протокол: HTTPS Порт: 8088

☒ Запрашивать аутентификацию

Сетевой интерфейс: Любой

Подключение возможно по любому IP-адресу из списка доступных Сетевых интерфейсов.

Сертификат и ключ

Сертификат выбран
Ключ сертификата выбран

Выбрать сертификат Выбрать ключ

Пароль сертификата:

OK **Отмена** Применить

Рис. 183. Окно настройки параметров объекта ONVIF-сервер. Закладка Общие

Таблица 49. Параметры объекта ONVIF-сервер. Закладка Общие

Параметр	Описание
RTSP-сервер	Выберите из списка RTSP-сервер, параметры которого будут использоваться при формировании RTSP-запроса на передачу видео из SecurOS. Если выбрано значение Встроенный, закладка Встроенный RTSP-сервер становится активной. Все ее параметры становятся доступными для редактирования.

Параметр	Описание
Протокол	Выберите протокол взаимодействия с <i>ONVIF-сервером</i>. Возможные значения: • HTTP — для незащищенного соединения. • HTTPS — для защищенного соединения с использованием сертификата (рекомендуется).
Порт	Номер порта SecurOS для взаимодействия с внешней системой по протоколу ONVIF. Используется для управления PTZ камерами SecurOS из внешней системы. Диапазон возможных значений: [1; 65535]. По умолчанию принимает значение 8088.
Запрашивать аутентификацию	Отметьте флажок, чтобы к <i>ONVIF-серверу</i> могли подключаться только авторизованные пользователи SecurOS. Также будут проверяться права пользователя на доступ к <i>Камерам</i>, выбранным на закладке Встроенный RTSP-сервер: •  (Доступ запрещен) — пользователю запрещены любые операции с <i>Камерами</i> через <i>ONVIF-сервер</i>, в т. ч. просмотр видео. •  (Просмотр) — пользователю разрешено просматривать живое видео и архив <i>Камер</i>. •  (Управление) и выше — пользователю разрешено управлять поворотными устройствами (PTZ) <i>Камер</i>. Внимание! Работа с пользователями домена Windows Active Directory не поддерживается. Примечание. Если отмечен и в поле RTSP-сервер выбран конкретный сервер, флаг будет влиять только на подключение к <i>ONVIF-серверу</i>. Возможность передачи видео будет определяться правами доступа к <i>Камерам</i>, выбранным в настройках объекта RTSP-сервер (см. Запрашивать аутентификацию).
Сетевой интерфейс	Список поля содержит все доступные сетевые интерфейсы, которые могут использоваться для подключения к <i>ONVIF-серверу</i>. Возможные значения: • Любой — для подключения может использоваться любой из IP-адресов, указанных в списке доступных. • Список доступных IP-адресов — выберите требуемый IP-адрес из списка. Подключение к <i>ONVIF-серверу</i> будет выполняться только по выбранному IP-адресу.
Сертификат и ключ	В поле отображается информация о сертификате и ключе. Поле доступно, если выбран протокол HTTPS.
Выбрать сертификат (кнопка)	Выберите доверенный сертификат, который будет использован для обеспечения безопасного соединения. SecurOS поддерживает сертификаты в формате .pem. Кнопка доступна, если выбран протокол HTTPS.

Параметр	Описание
Выбрать ключ (кнопка)	Выберите файл ключа, если он хранится отдельно от сертификата. Кнопка доступна, если выбран протокол HTTPS.
Пароль сертификата	Если сертификат защищен паролем, введите пароль в это поле. Поле доступно, если выбран протокол HTTPS.

9.12.1.13.2 Закладка Встроенный RTSP-сервер

Внимание! Закладка и все ее параметры становятся доступны для редактирования, если в параметре **RTSP-сервер** выбрано значение **Встроенный** (см. [Закладка Общие](#)).

Использование встроенного RTSP-сервера позволяет осуществлять трансляцию видео с *Камер SecurOS* с помощью *ONVIF-сервера*, без использования отдельного объекта SecurOS **RTSP-сервер**. Трансляция может осуществляться как в юникаст, так и в мультикаст режиме.

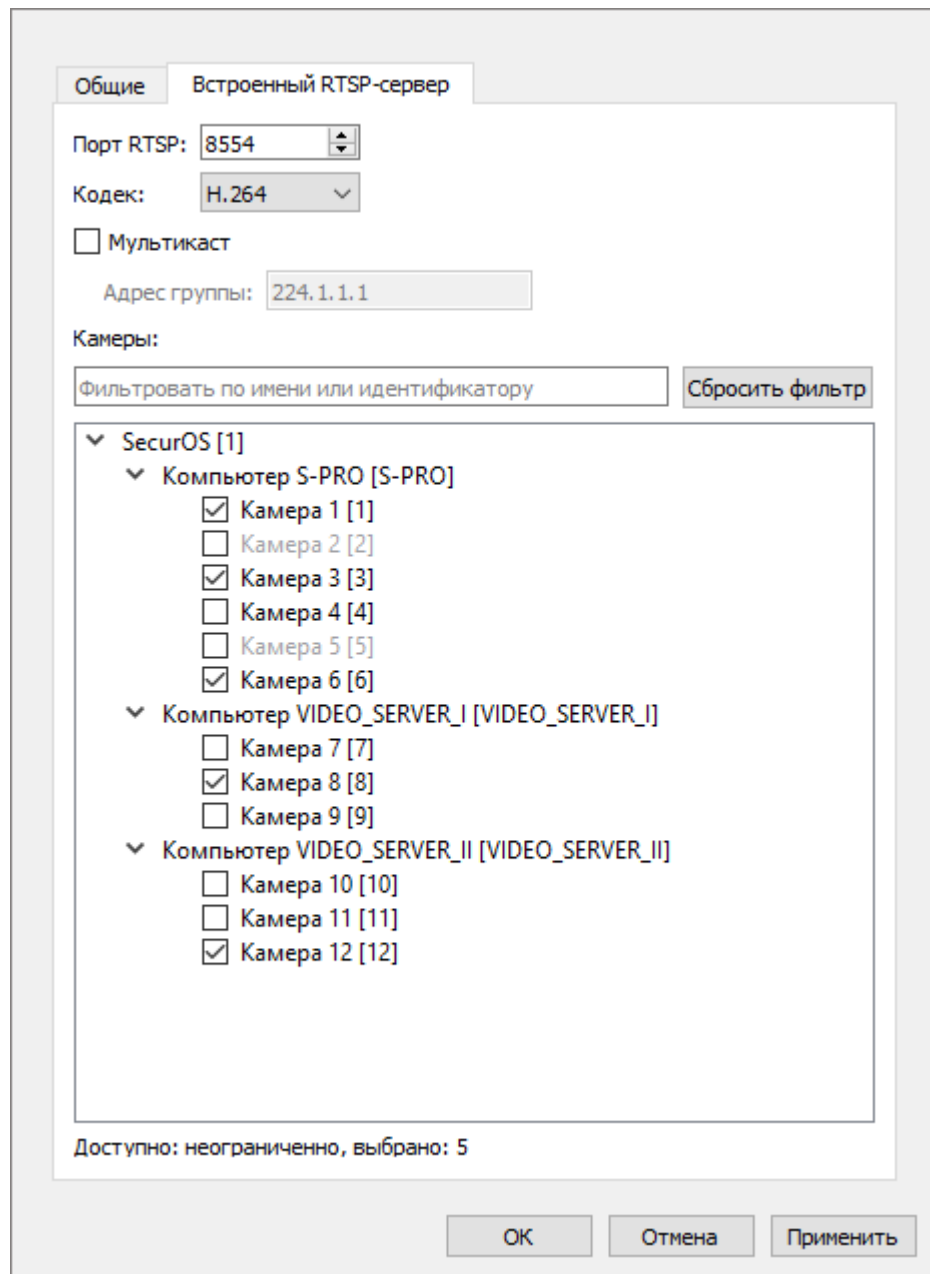


Рис. 184. Окно настройки параметров объекта ONVIF-сервер. Закладка Встроенный RTSP-сервер

Таблица 50. Параметры объекта ONVIF-сервер. Закладка Встроенный RTSP-сервер

Параметр	Описание
Порт RTSP	Номер порта SecurOS для взаимодействия с внешней системой по протоколу RTSP. Используется для просмотра живого и архивного видео с помощью внешнего приложения. Диапазон возможных значений: [1 ; 32768]. По умолчанию принимает значение 8554.

Параметр	Описание
Кодек	Выберите кодек для передачи видео. Возможные значения: • Все — трансляция видео возможна с любым кодеком. • H.264 — видео будет транслироваться с кодеком H.264. Значение по умолчанию.
	Примечание. Если исходный кодек видео отличается от H.264, будет выполнено транскодирование.
	• H.265. • MPEG4. • MJPEG.
Мультикаст	Отметьте флажок для трансляции видео в режиме мультикаст. Иначе трансляция будет вестись в режиме юникаст.
Адрес группы	Задайте IP-адрес группы мультикаст трансляции в формате IPv4, который будет использоваться по умолчанию. Если не отмечен флажок Мультикаст параметр недоступен.
Камеры	
Фильтр	Для поиска объекта по части имени или идентификатора введите в поле требуемые символы; в дереве автоматически отобразятся только те объекты, имя или идентификатор которых соответствуют заданным условиям поиска. Для того, чтобы очистить поле, нажмите кнопку Сбросить фильтр .
Дерево объектов	Список камер SecurOS, с которых возможна передача живого и архивного видео на внешнюю систему по протоколу RTSP. Структура дерева аналогична структуре <i>Дерева объектов</i> SecurOS. Для выбора <i>Камеры</i> отметьте соответствующий чек-бокс слева от объекта. Для выбора всех <i>Камер</i> компьютера отметьте чек-бокс слева от соответствующего <i>Компьютера</i>. Для выбора всех <i>Камер</i> всех <i>Компьютеров</i> объекта охраны, отметьте чек-бокс слева от <i>Объекта охраны</i>. Примечание. Временно отключенные <i>Камеры</i> (см. Отключение объекта) выделяются в дереве объектов серым (см. рис. 184). Внимание! Количество камер, с которых возможна одновременная передача видео, является лицензируемым параметром. При превышении заданного в лицензии параметра кнопка ОК блокируется.

9.12.2 Объекты пользовательского интерфейса

К объектам пользовательского интерфейса видеоподсистемы относится **Медиа Клиент**.

9.12.2.1 Медиа Клиент

В ОС **Linux** функциональность ограничена.

Объект представляет собой графический интерфейс пользователя для работы с *Камерами* и *Микрофонами*. *Медиа Клиент* предоставляет возможность обработки каждого из потоков, формируемых многопоточной камерой в режиме реального времени (см. раздел **Многопоточность**) и указывать типы отображаемых потоков в зависимости от размера ячеек (см. рис. 186 и Таблицу 52).

При использовании режима цифрового масштабирования в *Медиа Клиенте* возможно автоматическое переключение на поток лучшего качества для многопоточных камер (см. ниже).

Медиа Клиент может работать в двух режимах — с указанным списком *Камер* или со всеми *Камерами* системы. По умолчанию *Медиа Клиент* содержит все включенные *Камеры* системы, которые добавляются в *Список камер* автоматически, при создании объекта *Медиа Клиент*. При создании нового объекта *Камера* она автоматически добавляется в список (только в режиме работы со всеми *Камерами*).

Родительский объект — **Рабочий стол**.

Окно настройки параметров содержит следующие закладки:

- Закладка **Отображение**.
- Закладка **Раскладки**.
- Закладка **Виды**.
- Закладка **Камеры**.
- Закладка **Экспорт и архив**.
- Закладка **Аудио**.
- Закладка **Дополнительные**.

9.12.2.1.1 Закладка Отображение

Отображение Раскладки Виды Камеры Экспорт и архив Аудио Дополнительные

Режим работы: Обычный

Расположение окна

X: 30% Y: 29% Дисплей: 1
W: 54% H: 60%

Дополнительные панели

☒ Список Устройств
☐ Группировать Камеры и Микрофоны по имени
☒ Панель управления поворотным устройством

Элементы управления в ячейке Камеры

☒ Управление записью
☒ Управление тревожным режимом Камеры
☒ Цифровое масштабирование
☒ Одна Камера с переключением потоков
☐ Любое количество Камер, без переключения потоков
☒ Управление поворотным устройством с помощью мыши
☒ Сохранение кадров ☐ Добавить колонтитул
c:\export
☐ Печать кадров

Общие настройки

☒ Отображать идентификатор Медиа Клиента
☐ Отображать идентификатор Камеры
Время отображения страницы при автолистании 5 с

OK Отмена Применить

Рис. 185. Окно настройки параметров объекта Медиа Клиент. Закладка Отображение

Таблица 51. Параметры объекта Медиа Клиент. Закладка Отображение

Параметр	Описание
Режим работы (выберите режим работы <i>Медиа Клиента</i>)	

Параметр	Описание
Обычный	Нормальный режим работы. Доступность стандартных средств управления <i>Медиа Клиента</i> и вспомогательных элементов определяется текущими настройками. Элементы управления в ячейке камеры и рамка ячейки отображаются. Устанавливается по умолчанию.
Только онлайн	Режим работы только с живым видео или звуком — перевод объектов в режим архива оператором невозможен. В данном режиме все доступные оператору стандартные и дополнительные элементы управления архивом скрываются (например, панель Экспорт, кнопка Онлайн/Архив в ячейке <i>Камеры</i> или на <i>Панели микрофонов</i>, команды управления архивом контекстного меню).
Тревожный	Режим отображения только тревожных камер (камер, на которых зафиксировано движение). В данном режиме стандартные (<i>Панель раскладок</i>, <i>Панель управления камерами</i>) и вспомогательные (<i>Список Устройств</i>, <i>PTZ-панель</i> и пр.) средства управления <i>Медиа Клиентом</i> недоступны оператору. Из ячейки камеры доступны команды <i>Цифрового масштабирования</i> и <i>Сохранения кадра</i>. Камера отображается на <i>Медиа Клиенте</i> только в случае обнаружения движения в зоне детектирования. При окончании тревоги камера скрывается в соответствии с параметром После завершения тревоги не скрывать Камеру (см. ниже).
Активный	Работа с активной камерой в раскладке 1x1. Стандартные средства управления <i>Медиа Клиента</i> и <i>Список Устройств</i> скрываются. Элементы управления в ячейке камеры и рамка ячейки отображаются.

Параметр	Описание
Только просмотр	В данном режиме стандартные средства управления <i>Медиа Клиента</i> недоступны оператору. При переходе в режим просмотра все вспомогательные элементы управления <i>Медиа Клиентом</i> (<i>Панель камер</i>, <i>Панель раскладки</i> и пр.), а также элементы управления в ячейке <i>Камеры</i> и рамка ячейки <i>Камеры</i>, отображаемые в нормальном режиме, скрываются. Если настройка применяется к существующему объекту <i>Медиа Клиент</i>, все камеры переводятся в режим просмотра живого видео, раскладка рабочей области и отображаемая видеостраница не изменяются. В режиме просмотра управление <i>Медиа Клиентом</i> осуществляется извне, например, с помощью Скриптов Node.js. Поддерживаются следующие типы команд: • Переключение раскладки; • Перемещение <i>Камеры</i> в заданную ячейку; • Переключение в режим просмотра архива и обратно; • Команды управления архивом.
Настройки тревожного режима	
После завершения тревоги не скрывать Камеру	Задайте время, в течение которого <i>Камера</i> будет отображаться на <i>Медиа Клиенте</i> после окончания тревоги (в секундах).
Расположение окна	
X, Y	Задайте координаты верхнего левого угла (X, Y), относительно верхнего левого угла монитора компьютера. Возможные значения: [0; 70], в процентах от размера экрана.
W, H	Задайте ширину и высоту (W, H) окна. Возможные значения: [30; 100], в процентах от размера экрана. Примечания: 1. В случае, если заданные значения параметров приводят к соотношениям $(X+W) > 100$ или $(Y+H) > 100$, и при этом параметр Режим просмотра отключен, то система автоматически уменьшает заданные значения до выполнения соотношений $(X+W) = 100$ или $(Y+H) = 100$. 2. В случае, если заданные значения параметров приводят к соотношениям $(X+W) > 100$ или $(Y+H) > 100$, и при этом параметр Режим просмотра включен, то система отобразит окно <i>Медиа Клиента</i> на нескольких физических дисплеях, учитывая их взаимное расположение (системная настройка).

Параметр	Описание
Дисплей	Выберите номер физического дисплея на котором должно располагаться окно <i>Медиа Клиента</i> . Возможные значения: [1; 16]. По умолчанию принимает значение 1.
Дополнительные панели	
Список Устройств	Снимите флажок для скрытия <i>Списка Устройств</i> в интерфейсе пользователя на данном <i>Медиа Клиенте</i> . По умолчанию отмечен.
Группировать Камеры и Микрофоны по имени	Отметьте флажок для группировки <i>Камер</i> и <i>Микрофонов</i> по имени в случае, если Название <i>Камеры/Микрофона</i> содержит разделитель (-и) ":" (см. Добавление камеры в систему). Разделители могут использоваться, например, для точного указания местоположения камеры/микрофона в сегменте сети безопасности. Пример Названия <i>Камеры</i>: Завод:Цех:Участок:Камера1. В системе поддерживается до 10-ти уровней вложенности имени устройства. Примечания: 1. Группы (уровни вложенности) отображаются в <i>Списке Устройств</i> в алфавитном порядке, сортировка <i>Камер/Микрофонов</i> внутри уровня также осуществляется в алфавитном порядке. 2. <i>Камеры/Микрофоны</i>, в Названии которых отсутствует разделитель ":", не принадлежат ни к одному уровню и объединяются в соответствующую системную группу. Не сгруппированы в начале списка.
Панель управления поворотным устройством	Снимите флажок для того, чтобы скрыть Панель управления поворотным устройством . По умолчанию отмечен.
Элементы управления в ячейке Камеры	
Управление записью	Снимите флажок, чтобы запретить оператору управлять записью. По умолчанию отмечен.
Управление тревожным режимом Камеры	Снимите флажок, чтобы запретить оператору управлять тревожным режимом камеры. По умолчанию отмечен.
Цифровое масштабирование	Снимите флажок, чтобы запретить оператору использовать цифровое масштабирование. По умолчанию отмечен.

Параметр	Описание
Одна Камера с переключением потоков	Если выбрана данная опция, только одна <i>Камера</i> может одновременно находиться в режиме цифрового масштабирования. При включении режима цифрового масштабирования система автоматически переключит камеру на отображение потока наилучшего качества. Рекомендуется для использования, если камеры системы поддерживают и настроены на работу с многопоточностью. Опция доступна в случае, если отмечен параметр Цифровое масштабирование, и является значением по умолчанию.
Любое количество Камер, без переключения потоков	Если выбрана данная опция, в режиме цифрового масштабирования могут одновременно находиться несколько <i>Камер</i>. При включении режима цифрового масштабирования автоматического переключения на поток наилучшего качества не происходит. Опция доступна в случае, если отмечен параметр Цифровое масштабирование.
Управление поворотным устройством с помощью мыши	Снимите флажок для того, чтобы запретить управление PTZ при помощи мыши (см. Краткое руководство пользователя SecurOS). По умолчанию отмечен.
Сохранение кадров	Снимите флажок, чтобы запретить оператору сохранять кадры из <i>Медиа Клиента</i> . По умолчанию отмечен. При выбранной опции кадр можно сохранить в указанную директорию.
Добавить колонтитул	Отметьте флажок, чтобы добавлять на сохраняемый кадр дополнительную информацию. Дополнительная информация будет выводиться в нижнем колонтитуле кадра в следующем формате: <Дата кадра в формате ОС> <Время кадра в формате ОС, с миллисекундами> [<ID Камеры>] <Название Камеры>
Печать кадров	Отметьте флажок, чтобы разрешить оператору печать кадров из <i>Медиа Клиента</i> .
Общие настройки	
Отображать идентификатор Медиа Клиента	Отметьте флажок для отображения идентификатора <i>Медиа Клиента</i> на верхней панели <i>Медиа Клиента</i> . По умолчанию не отмечен. Параметр доступен в режимах Обычный и Только онлайн.
Отображать идентификатор Камеры	Отметьте флажок для отображения идентификатора <i>Камеры</i> в заголовке ячейки камеры. Если флажок отмечен, имя <i>Камеры</i> в заголовке будет отображаться в формате [<Идентификатор камеры>] <Название камеры>. По умолчанию не отмечен.
Время отображения страницы автолистания при автолистании	Время отображения видеостраницы на экране в режиме автолистания (в секундах).

9.12.2.1.2 Закладка Раскладки

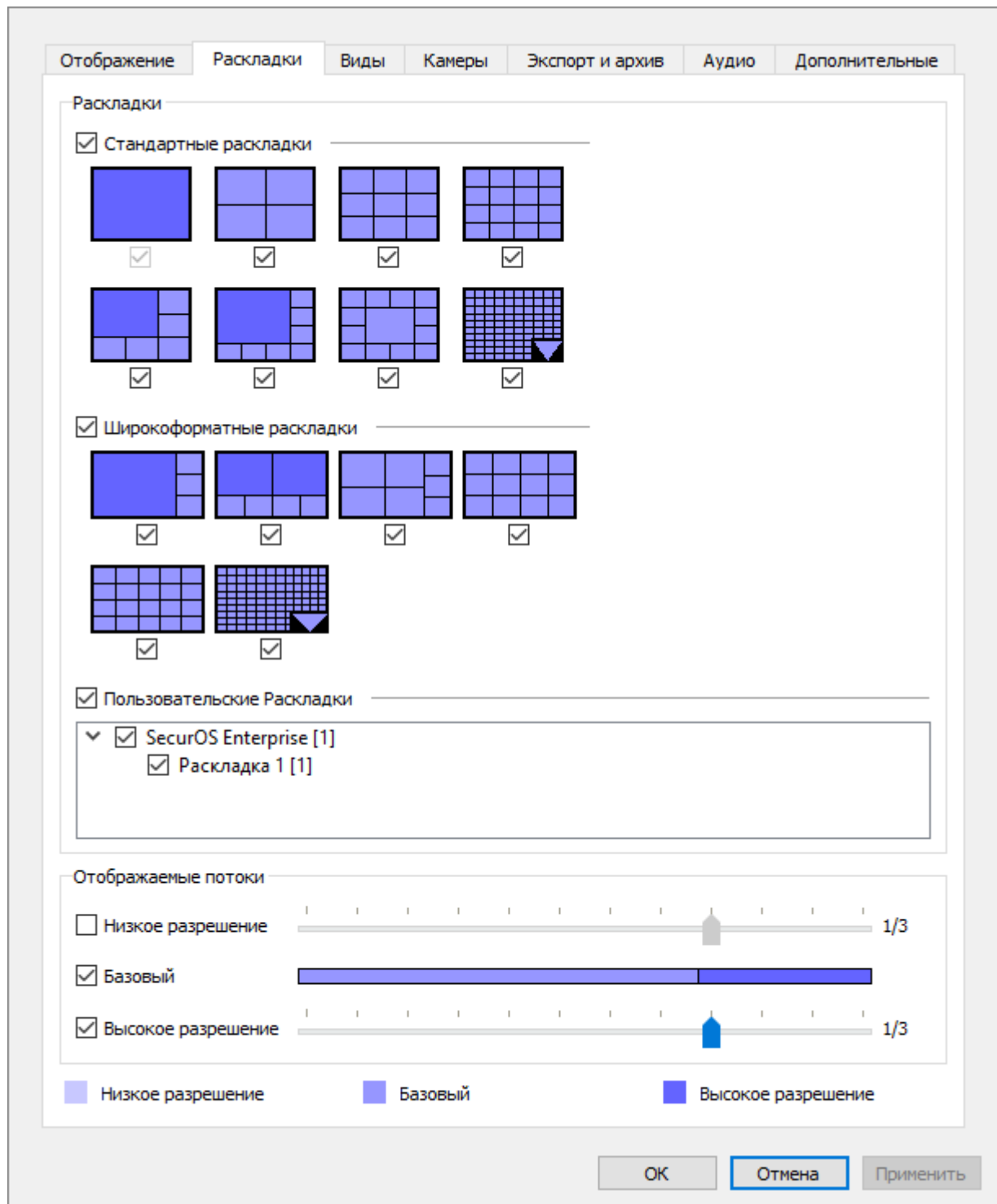


Рис. 186. Окно настройки параметров объекта Медиа Клиент. Закладка Раскладки

Таблица 52. Параметры объекта Медиа Клиент. Закладка Раскладки

Параметр	Описание
Количество ячеек для определения раскладки	

Параметр	Описание
Минимум, Максимум	Внимание! Параметры блока отображаются только при выборе режима Тревожный. Задайте значения Минимум и Максимум для определения минимального и максимального количества ячеек в раскладке, которая может быть использована. Автоматически будут выбраны только те раскладки, типы которых предопределены заранее (см. Раскладки) и ячейки которых имеют одинаковый размер. Если отображается максимально возможное количество камер, прочие тревожные камеры помещаются в очередь. Камеры из очереди будут выводиться последовательно, при окончании тревоги на какой-либо текущей отображаемой камере. Если тревога окончена, камера удаляется из очереди.
	Пример. При работе в Тревожном режиме выбранные раскладки сменяются автоматически, в зависимости от числа тревожных камер. Например, параметр Минимум равен 4, а параметр Максимум — 9. Это означает, что могут быть использованы раскладки 2x2 и 3x3. Если количество тревожных камер меньше или равно 4, будет использоваться раскладка 2x2, а если количество тревожных камер больше 4, <i>Медиа Клиент</i> автоматически переключится на раскладку 3x3. Раскладка 1x1 доступна всегда.
Раскладки (для выделения/деактивации всех раскладок группы отметьте/снимите соответствующий флажок слева от имени группы)	
Стандартные раскладки	Выберите стандартные раскладки, которые будут доступны оператору на панели раскладок <i>Медиа Клиента</i>, для чего отметьте флажок соответствующей раскладки. Внимание! Раскладка 1*1 является обязательной, отмечена по умолчанию и не может быть деактивирована.
Широкоформатные раскладки	Выберите широкоформатные раскладки, которые будут доступны оператору на панели раскладок <i>Медиа Клиента</i>, для чего отметьте флажок соответствующей раскладки.
Пользовательские Раскладки	Выберите пользовательские раскладки (см. Раскладка), которые будут доступны оператору на панели раскладок <i>Медиа Клиента</i>, для чего отметьте флажок соответствующей раскладки.
Отображаемые потоки	

Параметр	Описание
Низкое разрешение, Базовый, Высокое разрешение	Для использования потока отметьте соответствующий ему флажок. Для задания размера ячеек (в долях от рабочей области <i>Медиа Клиента</i>), в которых будет отображаться выбранный поток, используйте соответствующий ползунок. При задании размера ячеек для нескольких используемых потоков, на закладке (см. рис. 186) будет графически представлено соотношение поток/размер ячеек. Внимание! По умолчанию отмечен Базовый поток, который будет отображаться в ячейках размером меньше 1 / 3 рабочей области <i>Медиа Клиента</i>, и Поток высокого разрешения, который будет отображаться в ячейках с размером 1 / 3 и более.

Например, как представлено на рис. 186, если для отображения выбраны все три потока камеры, то при указанных настройках **Поток высокого разрешения** будет отображаться в любых ячейках с размером не менее 1/2 рабочей области, **Поток низкого разрешения** будет отображаться во всех ячейках с размером не более 1/4 рабочей области. При этом, **Базовый поток** будет отображаться в ячейках промежуточного размера.

9.12.2.1.3 Закладка Виды

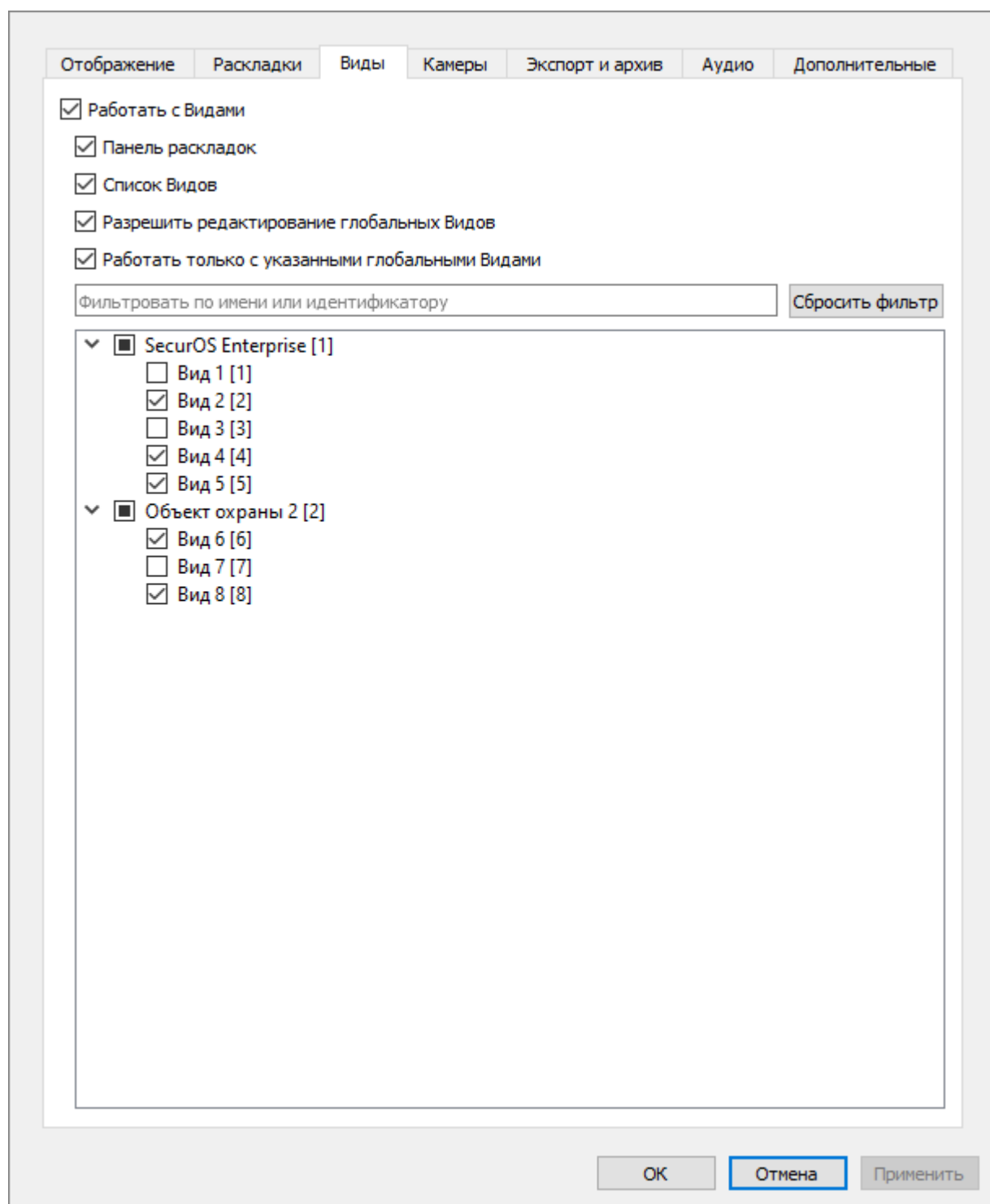


Рис. 187. Окно настройки параметров объекта Медиа Клиент. Закладка Виды

Таблица 53. Параметры объекта Медиа Клиент. Закладка Виды

Параметр	Описание
Работать с Видами	Отметьте флажок для работы с <i>Видами</i>. По умолчанию не отмечен. Примечание. Перечисленные ниже параметры доступны в случае, если данный флажок отмечен. Описание операций с <i>Видами</i> приведено в разделе Операции с Видами.
Панель раскладок	Снимите флажок для скрытия <i>Панели раскладок</i> . По умолчанию отмечен.
Список Видов	Снимите флажок для скрытия <i>Списка видов</i> . По умолчанию отмечен.
Разрешить редактирование глобальных Видов	Отметьте флажок для возможности редактирования глобальных <i>Видов</i> оператором. По умолчанию не отмечен.
Работать только с указанными глобальными Видами	Отметьте флажок для перехода в режим ручного управления <i>Списком видов</i> данного <i>Медиа Клиента</i>. Если не отмечен, <i>Список видов</i> формируется автоматически и содержит все <i>Виды</i>, созданные в системе. По умолчанию не отмечен. Примечание. Перечисленные ниже параметры доступны в случае, если данный флажок отмечен.
Фильтр	Для поиска объекта по части имени или идентификатора введите в поле требуемые символы; в дереве автоматически отобразятся только те объекты, имя или идентификатор которых соответствуют заданным условиям поиска. Для того, чтобы очистить поле, нажмите кнопку Сбросить фильтр .
Дерево объектов	Дерево <i>Объектов охраны</i> в сети системы безопасности SecurOS со всеми дочерними глобальными <i>Видами</i>, сгруппированными по этим <i>Объектам охраны</i>. Для добавления <i>Вида</i> в <i>Список Видов Медиа Клиента</i> отметьте соответствующий флажок слева от объекта <i>Вид</i>. Примечание. По умолчанию объекты дерева отсортированы по возрастанию, по имени и идентификатору объекта.

9.12.2.1.4 Закладка Камеры

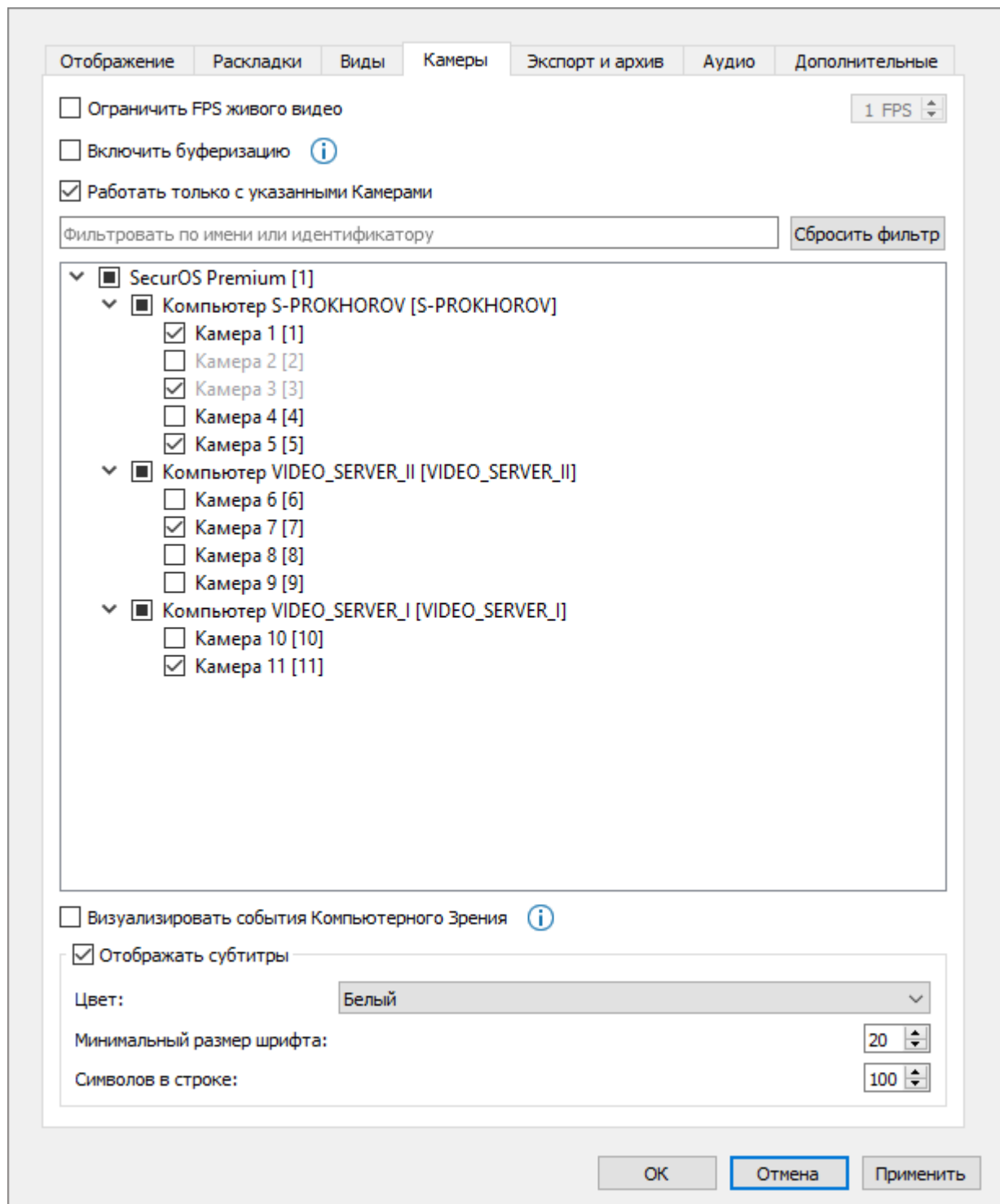


Рис. 188. Окно настройки параметров объекта Медиа Клиент. Закладка Камеры

Таблица 54. Параметры объекта Медиа Клиент. Зкладка Камеры

Параметр	Описание
Ограничить FPS живого видео	Отметьте флажок, если необходимо ограничить количество кадров живого видео в секунду и задайте требуемое значение. При заданном значении для прореживания используется алгоритм, описанный в разделе Прореживание видеопотока. Примечания: 1. Заданное значение применяется ко всем <i>Камерам</i>, выбранным для работы с данным <i>Медиа Клиентом</i>. 2. Если на одном <i>Рабочем столе</i> настроено более одного <i>Медиа Клиента</i>, каждый из которых работает с данной <i>Камерой</i>, то FPS этой <i>Камеры</i> будет равен максимальному значению из заданных на всех <i>Медиа Клиентах</i>.
Включить буферизацию	Отметьте флажок, чтобы включить буферизацию живого видео и сопровождающего аудио на каждой камере, с которой работает <i>Медиа Клиент</i>. Буферизация видео позволяет устранить неравномерное ("рваное") воспроизведение видео, цикличное запаздывание или обрывы воспроизведения сопровождающего аудио. При включенном флажке для каждой <i>Камеры</i> активируется собственный буфер видео- и аудиокадров, размер которого (в мс) определяется в ее настройках (см. раздел Закладка Общие). Внимание! При включенном режиме буферизации: 1. Видео будет отображаться с задержкой, минимальное значение которой равно заданному размеру буфера. 2. Индикаторы тревог и записи будут соответствовать реальному времени кадра, т.е. будут рассинхронизированы по времени с отображаемыми кадрами. 3. При управлении PTZ режим буферизации будет отключен автоматически до момента освобождения управления PTZ. Режим буферизации будет включен автоматически через 10 секунд после отправки последней команды, при этом проигрывание видео будет приостановлено для набора буфера.
Работать только с указанными Камерами	Отметьте флажок для перехода в режим ручного управления <i>Списком камер</i> данного <i>Медиа Клиента</i>. Если не отмечен, <i>Список камер</i> формируется автоматически, не может быть изменен и содержит все <i>Камеры</i>, подключенные к системе. По умолчанию не отмечен.
Фильтр	Для поиска объекта по части имени или идентификатора введите в поле требуемые символы; в дереве автоматически отобразятся только те объекты, имя или идентификатор которых соответствуют заданным условиям поиска. Для того, чтобы очистить поле, нажмите кнопку Сбросить фильтр.

Параметр	Описание
Дерево объектов	Дерево <i>Компьютеров</i> с ролью <i>Видеосервер</i>, существующих в сети SecurOS. При развертывании узла каждого <i>Видеосервера</i> отображается список созданных на нем <i>Камер</i>. Для добавления камеры в <i>Список камер Медиа Клиента</i> отметьте соответствующий флажок слева от объекта <i>Камера</i>.
Визуализировать события Компьютерного Зрения	Отметьте флажок, чтобы визуализировать события, зарегистрированные видеоаналитическими детекторами плагина Tracking Kit III (см. Настройка встроенных видеоаналитических детекторов). Визуализация событий возможна при просмотре живого видео. Подробнее о визуализации событий на <i>Медиа Клиенте</i> см. раздел Представление результатов работы видеоаналитического детектора. Флажок отображается, если в <i>Дереве объектов</i> существует хотя бы один объект <i>Компьютерное зрение</i>.
Отображать субтитры (отметьте флажок для вывода субтитров с заданными параметрами). Если отмечен, субтитры выводятся как в режиме Онлайн, так и в режиме Архив. Субтитры добавляются на изображение извне, с помощью команды ADD_SUBTITLES (см. Руководство программиста SecurOS).	
Внимание! Если параметры субтитров заданы в команде добавления субтитров ADD_SUBTITLES, указанные ниже значения игнорируются.	
Цвет	Выберите из списка цвет субтитров.
Минимальный размер шрифта	Параметр задает минимально возможный размер шрифта субтитров. Диапазон возможных значений: [1; 50]. Фактический размер шрифта вычисляется автоматически в зависимости от текущего размера кадра и значения параметра Символов в строке. Вычисленное значение Y всегда будет удовлетворять условию $X_{min} \leq Y \leq 50$, где X_{min} — заданное значение параметра. При изменении размера кадра вычисленное значение изменяется пропорционально.

Параметр	Описание
Символов в строке	Параметр задает такой минимальный размер шрифта, при котором указанное количество символов текста гарантированно не будет перенесено на следующую строку в ячейке <i>Камеры</i>. Диапазон возможных значений: [1; 200]. Количество символов в строке будет неизменным до тех пор, пока вычисленный размер шрифта больше заданного Минимального размера шрифта для данного размера кадра. Если вычисленный размер меньше чем Минимальный размер шрифта, то размер символов будет равен Минимальному размеру шрифта. При этом в строке может помещаться меньше символов, чем это задано параметром Символов в строке. Если длина текста субтитров превышает размеры кадра, субтитры переносятся на следующую строку "по словам". Подробнее об управлении субтитрами см. Руководство программиста SecurOS, раздел Работа с субтитрами.

9.12.2.1.5 Закладка Экспорт и архив

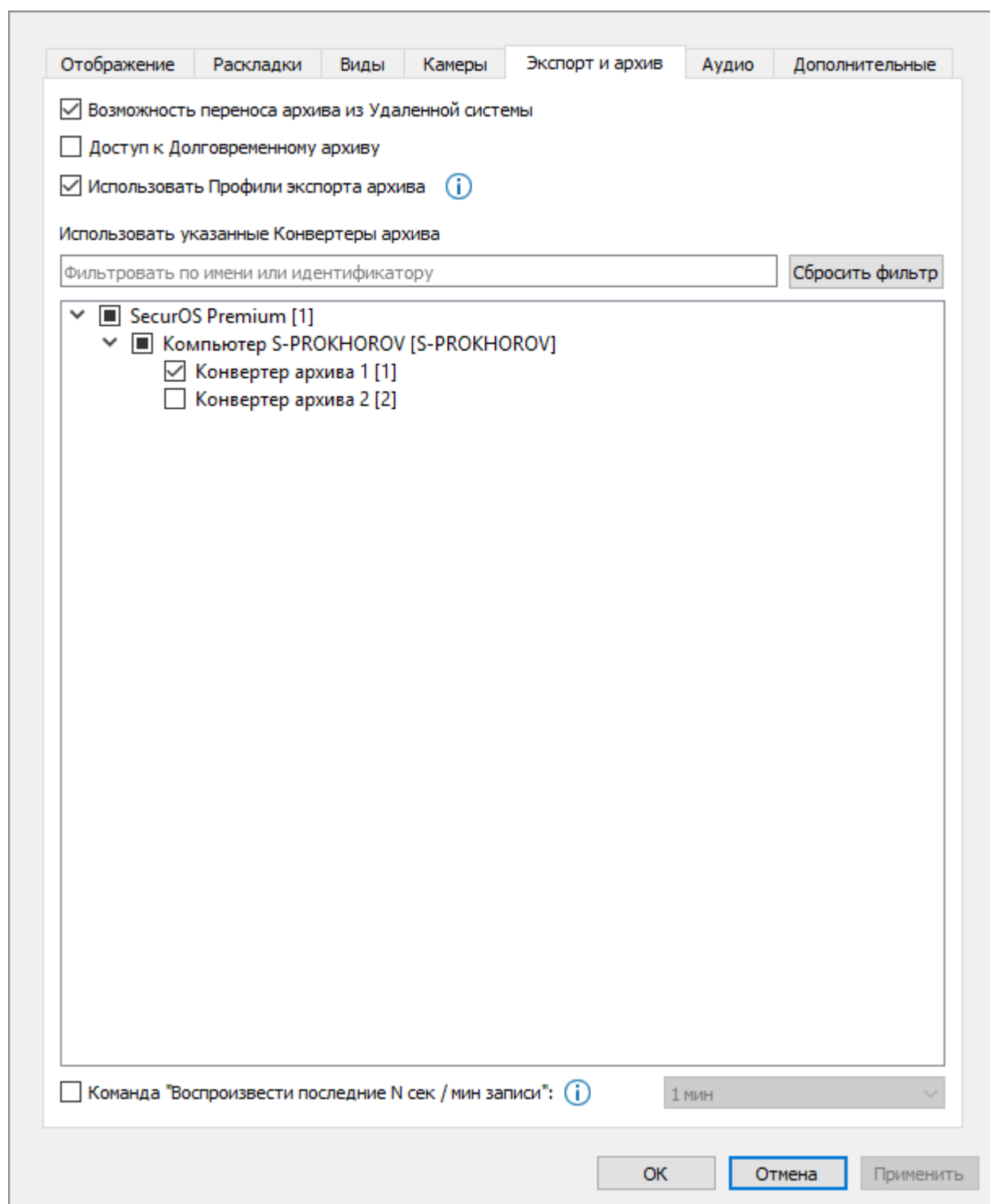


Рис. 189. Окно настройки параметров объекта Медиа Клиент. Закладка Экспорт и архив

Таблица 55. Параметры объекта Медиа Клиент. Закладка Экспорт и архив

Параметр	Описание
Возможность переноса архива из Удаленной системы	Отметьте флажок, чтобы разрешить перенос архива между Удаленной системой и Центром Мониторинга (см. Перенос архива между Удаленной системой и Центром Мониторинга). Примечание. Флажок отображается на закладке только в том случае, если в настройках объекта Система отмечен флажок Привилегированный доступ к Удаленным системам. Внимание! Опция доступна только в режимах работы Обычный и Активный (см. параметр Режим работы).
Доступ к Долговременному архиву	Отметьте флажок, чтобы разрешить оператору работу как с Оперативным, так и Долговременным архивом. Если отмечен, в ячейке камеры Медиа Клиента появляются дополнительные элементы управления (см. Краткое руководство пользователя SecurOS). Внимание! Опция доступна только в режимах работы Обычный и Активный (см. параметр Режим работы).
Использовать Профили экспорта архива	Отметьте флажок для использования Профилей экспорта архива для экспорта архива с помощью данного Медиа Клиента (см. Экспорт с помощью Профиля экспорта архива).
Использовать указанные Конвертеры архива	
Фильтр	Для поиска объекта по части имени или идентификатора введите в поле требуемые символы; в дереве автоматически отобразятся только те объекты, имя или идентификатор которых соответствуют заданным условиям поиска. Для того, чтобы очистить поле, нажмите кнопку Сбросить фильтр.
Дерево объектов	Дерево Видеосерверов, Рабочих мест оператора или Профилей Рабочих мест оператора, существующих в сети SecurOS, у которых есть дочерние объекты Конвертер архива. При разворачивании узла каждого объекта отображается список созданных на нем Конвертеров архива. Для выбора Конвертера архива, который будет использоваться данным Медиа Клиентом, отметьте соответствующий флажок слева от объекта Конвертер архива (см. Экспорт с помощью Конвертера архива). Внимание! Конвертеры архива, созданные на Видеосерверах, доступны на любом Компьютере. Конвертеры архива, созданные на Рабочих местах оператора или Профилях Рабочих мест оператора, доступны для выбора только на данных Компьютерах.

Параметр	Описание
Команда "Воспроизвести последние N сек / мин записи"	Отметьте флажок, чтобы добавить команду Воспроизвести последние N сек / мин записи в контекстное меню ячейки <i>Камеры</i> на <i>Медиа Клиенте</i> и задайте значение параметра. Подробнее об использовании команды и особенностях воспроизведения см. Краткое руководство пользователя SecurOS. Внимание! Опция доступна только в режимах работы Обычный и Активный (см. параметр Режим работы).

Внимание! Для экспорта архива уровень доступа пользователя к объектам *Профиль экспорта архива* и *Конвертер архива* должен быть не ниже, чем  (**просмотр**), см. [Права пользователя](#). При наличии доступа возможность использования объектов определяется параметрами данной закладки.

Экспорт с помощью Профиля экспорта архива

При использовании *Профиля экспорта архива*:

- **Задача на экспорт** создается средствами *Медиа Клиента*.
- **Операция экспорта** выполняется также средствами *Медиа Клиента*.

Экспорт с помощью Конвертера архива

При использовании *Конвертера архива*:

- **Задача на экспорт** создается средствами *Медиа Клиента*.
- **Операция экспорта** выполняется с помощью *Конвертера архива*.

9.12.2.1.6 Закладка Аудио

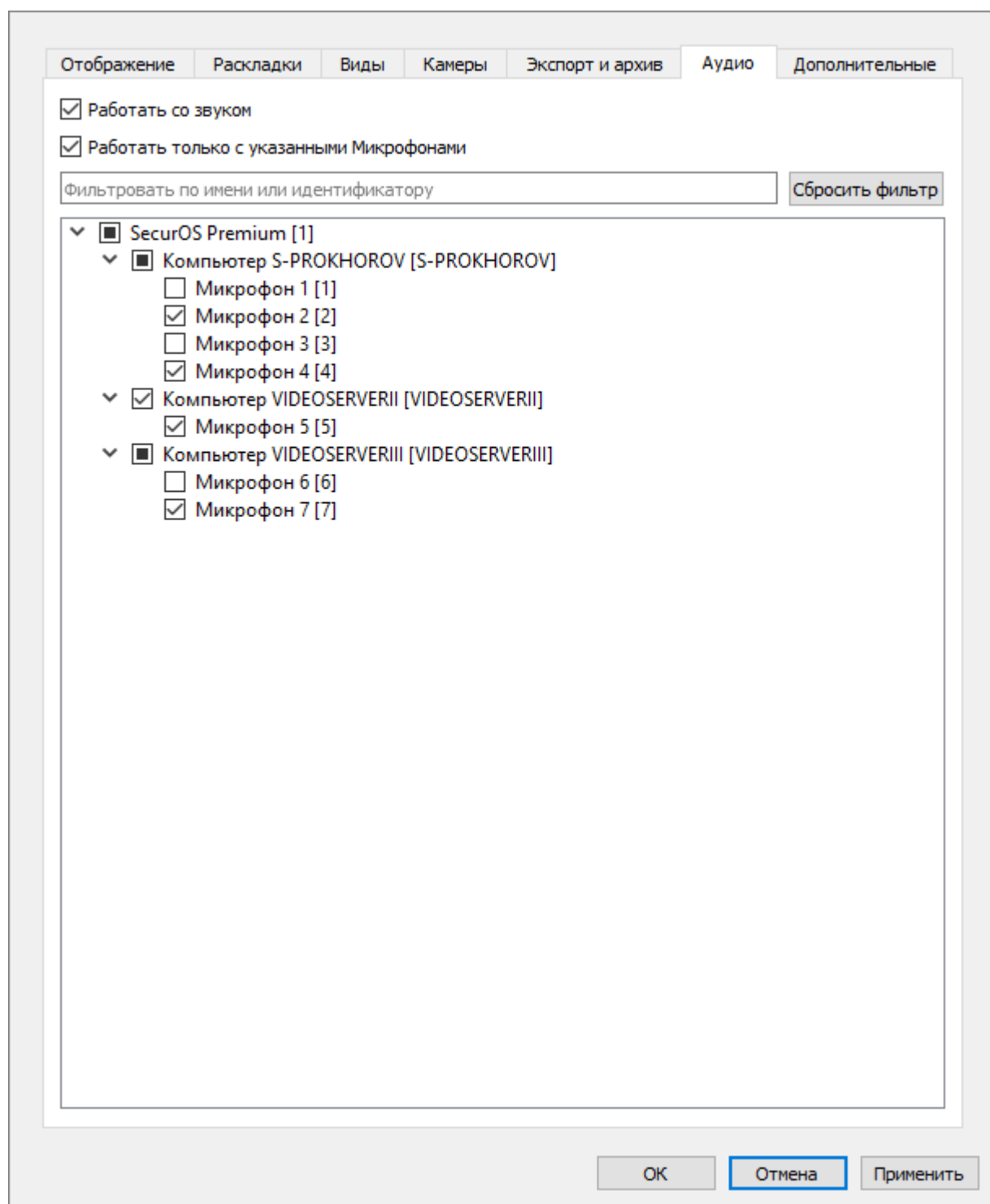


Рис. 190. Окно настройки параметров объекта Медиа Клиент. Закладка Аудио

Таблица 56. Параметры объекта Медиа Клиент. Закладка Аудио

Параметр	Описание
Работать со звуком	Отметьте флажок для возможности прослушивания живого и архивного звука при работе с данным <i>Медиа Клиентом</i>. Параметр влияет на воспроизведение звука от любых <i>Микрофонов</i>. Примечания: 1. Данный параметр не влияет на запись архивного звука. 2. Перечисленные ниже параметры доступны в случае, если данный флажок отмечен.
Работать только с указанными Микрофонами	Отметьте флажок для перехода в режим ручного управления <i>Списком свободных микрофонов</i> данного <i>Медиа Клиента</i>. Примечания: 1. Под <i>Свободным микрофоном</i> понимается микрофон, не связанный ни с одной <i>Камерой</i> системы. 2. Данная настройка не влияет на работу с <i>Микрофонами</i>, связанными с <i>Камерами</i> (см. Закладка Аудио). Если не отмечен, <i>Список свободных микрофонов</i> формируется автоматически, не может быть изменен и содержит все свободные <i>Микрофоны</i>, существующие в сети SecurOS.
Фильтр	Для поиска объекта по части имени или идентификатора введите в поле требуемые символы; в дереве автоматически отобразятся только те объекты, имя или идентификатор которых соответствуют заданным условиям поиска. Для того, чтобы очистить поле, нажмите кнопку Сбросить фильтр.
Дерево объектов	Дерево свободных <i>Микрофонов</i>, существующих в сети SecurOS. При разворачивании узла каждого <i>Видеосервера</i> отображается список созданных на нем свободных <i>Микрофонов</i>. Для добавления свободного <i>Микрофона</i> в <i>Список свободных микрофонов Медиа Клиента</i> отметьте соответствующий флажок слева от объекта <i>Микрофон</i>.

9.12.2.1.7 Закладка Дополнительные

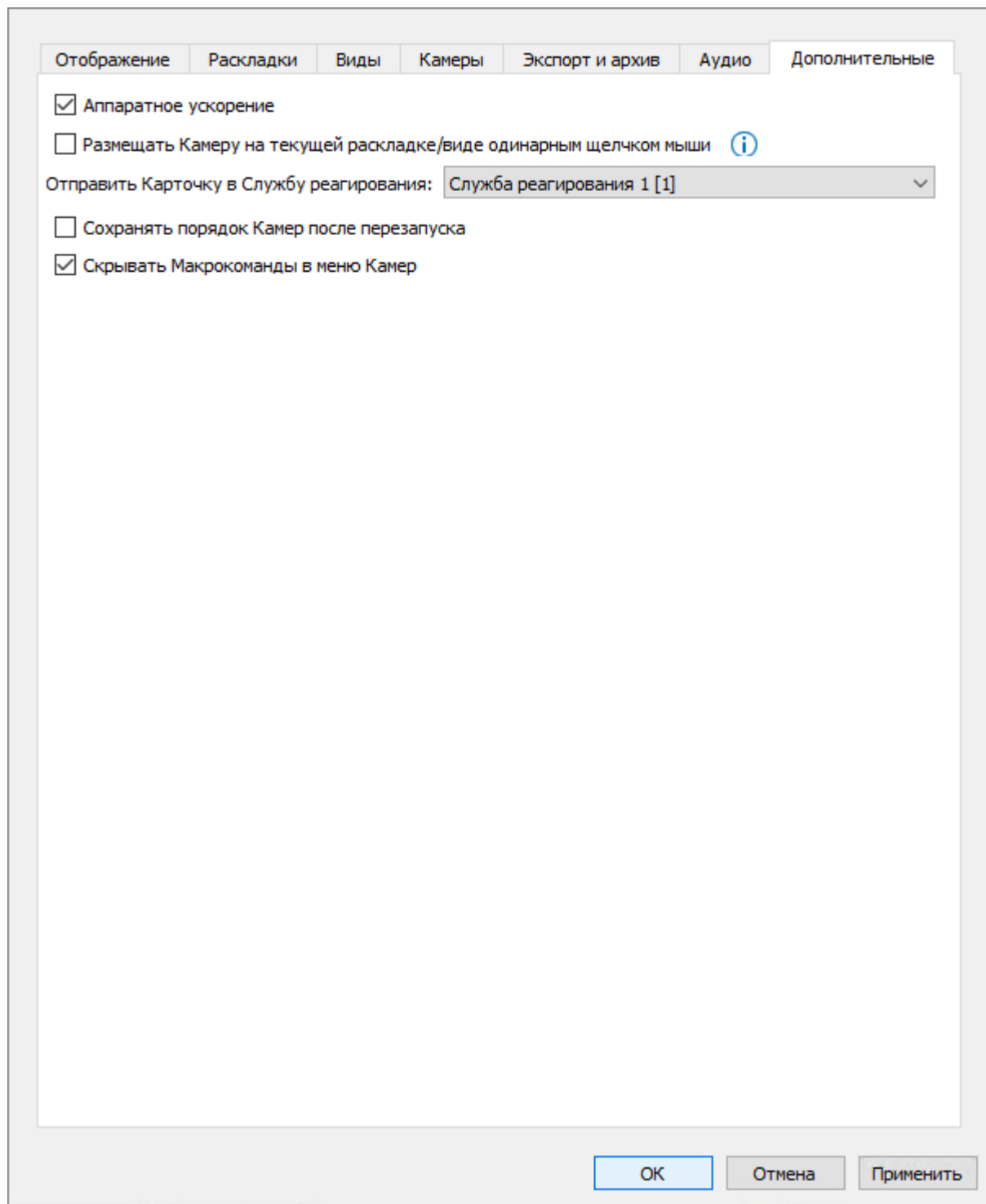


Рис. 191. Окно настройки параметров объекта Медиа Клиент. Закладка Дополнительные

Таблица 57. Параметры объекта Медиа Клиент. Закладка Дополнительные

Параметр	Описание
Аппаратное ускорение	Отметьте флажок для использования технологии Direct3D для отображения видео. Примечание. При отмеченном флажке оператор получает возможность настройки параметров изображения в ячейке камеры на <i>Медиа Клиенте</i> (см. Краткое руководство пользователя SecurOS). Если флажок не отмечен, будет использоваться программный режим отображения.
Размещать Камеру на текущей раскладке/виде одинарным щелчком мыши	Данный флажок позволяет настроить поведение <i>Медиа Клиента</i> при выборе <i>Камеры</i> в <i>Списке Устройств</i> в случае нажатия на нее одинарным/двойным щелчком мыши. При снятом флажке одинарный/двойной щелчок мыши по <i>Камере</i> в <i>Списке Устройств</i> обрабатывается следующим образом: • Если выбранная <i>Камера</i> присутствует на текущей <i>Раскладке</i>, эта <i>Камера</i> становится активной. • Если выбранная <i>Камера</i> отсутствует на текущей видеостранице, то <i>Медиа Клиент</i> переходит к видеостранице, на которой находится требуемая <i>Камера</i>. Выбранная <i>Камера</i> становится активной. Размерность <i>Раскладки</i> не изменится. При установленном флажке одинарный щелчок мыши по <i>Камере</i> в <i>Списке Устройств</i> позволяет добавлять <i>Камеры</i> на текущую видеостраницу. Это происходит согласно следующим правилам: • Если на текущей <i>Раскладке</i> есть активная <i>Камера</i>, то она заменяется на выбранную пользователем в <i>Списке Устройств</i>. • Если на текущей <i>Раскладке</i> нет активной <i>Камеры</i>, каждая выбранная <i>Камера</i> последовательно занимает ячейку, начиная с левого верхнего угла. • В обоих случаях уже находящиеся на <i>Раскладке</i> <i>Камеры</i> не меняют своего положения. Поведение двойного щелчка мыши соответствует поведению при снятом флажке. Аналогичные правила действуют при работе с <i>Видами</i>.
Отправить Карточку в Службу реагирования	Выберите из списка объект <i>Служба реагирования</i>, который будет использоваться для создания и отправки <i>Карточки происшествия</i> (см. Служба реагирования и Взаимодействие с внешней Службой реагирования).

Параметр	Описание
Сохранять порядок Камер после перезапуска	Отметьте флажок, чтобы сохранять текущие пользовательские настройки <i>Медиа Клиента</i> при его перезапуске. Под пользовательскими настройками понимается текущая раскладка <i>Медиа Клиента</i> и порядок расположения <i>Камер</i> в ней для каждого оператора SecurOS или <i>Профиля рабочего места оператора</i>. При перезапуске <i>Медиа Клиента</i> при снятом флажке: • Сохраняется последняя используемая раскладка. Если эта раскладка была удалена во время перезапуска <i>Медиа Клиента</i>, будет выведена раскладка 1×1. • Последний порядок расположения <i>Камер</i> в ячейках <i>Медиа Клиента</i> будет сброшен. Будет использоваться порядок по умолчанию (слева-направо и сверху-вниз в алфавитном порядке). При перезапуске <i>Медиа Клиента</i> при установленном флажке: • Сохраняется последняя используемая раскладка. Если эта раскладка была удалена во время перезапуска <i>Медиа Клиента</i>, будет выведена раскладка 1×1. • Будет сохранен последний порядок расположения <i>Камер</i> в ячейках <i>Раскладки</i>. • В случае изменения набора <i>Раскладок</i> или отображаемых <i>Камер</i> во время перезапуска <i>Медиа Клиента</i>, восстановление порядка <i>Камер</i> в <i>Раскладке</i> не гарантируется. Примечание. Если ранее установленный флажок будет снят во время работы <i>Медиа Клиента</i>, все сохраненные пользовательские настройки будут сброшены.
Скрывать Макрокоманды в меню Камер	Отметьте флажок, чтобы <i>Макрокоманды</i> не отображались в контекстном меню <i>Камер</i> данного <i>Медиа Клиента</i> .

9.12.2.1.8 О Видах

Виды позволяют группировать *Камеры* и *Микрофоны* и располагать их требуемым образом в *Медиа Клиенте*.

На рис. 192 показан пример *Вида*.

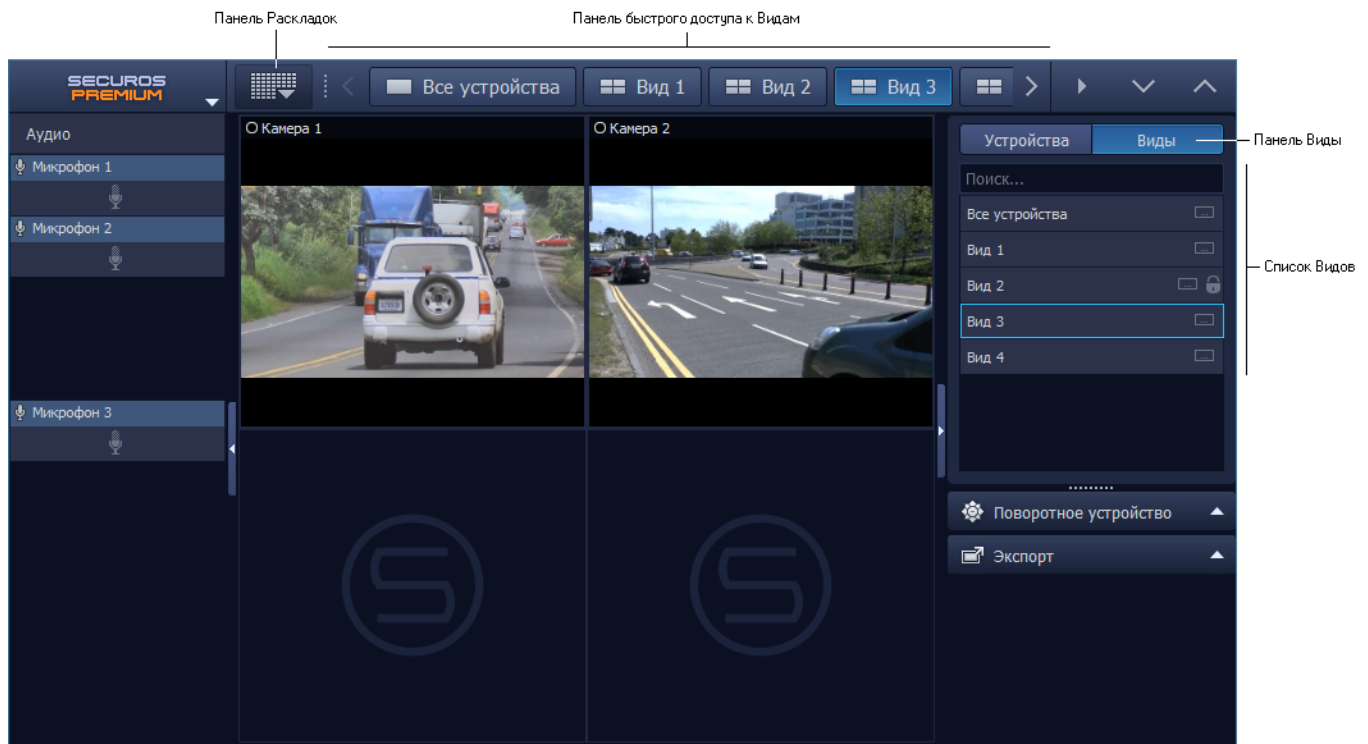


Рис. 192. Пример Вида

Все *Виды*, за исключением *Вида* с именем **Все устройства**, являются одностраничными, то есть *Камеры Видов* невозможно листать. Многостраничный *Вид Все устройства* существует всегда и включает в себя все доступные *Камеры* и *Микрофоны*.

На рис. 192 показаны:

- *Панель раскладок* (на рис. 192 свернута) содержит все *Раскладки*, которые могут быть использованы при работе с *Видами*;
- *Панель быстрого доступа к Видам*, на которую можно перетянуть часто используемые *Виды*. Текущий *Вид* выделяется голубым фоном;
- *Панель Видов* содержит *Список Видов* и поле поиска *Видов*;
- *Список Видов* содержит все доступные *Виды*. Текущий *Вид* выделяется голубой рамкой.

Администратор может скрыть *Список Видов*, *Панель раскладок*, а также выбрать *Виды* для отображения в *Медиа Клиенте* с помощью настроек на закладке **Виды**.

Примечание. Если *Список Видов* скрыт, то *Виды* отображаются на *Панели быстрого доступа к Видам*.

О том, как переключать *Виды*, работать с *Панелью быстрого доступа к Видам*, вносить временные изменения в *Виды* см. **Краткое руководство пользователя SecurOS**.

9.12.2.1.9 Операции с Видами

Чтобы иметь возможность выполнять операции по созданию, удалению и изменению *Видов*, отметьте флажок **Разрешить редактирование глобальных Видов** на закладке **Виды** *Медиа Клиента*.

Затем перейдите в *Редактор Видов*, для чего нажмите кнопку  в левом верхнем углу *Медиа Клиента* (см. рис. 193) и выберите **Открыть редактор Видов**.

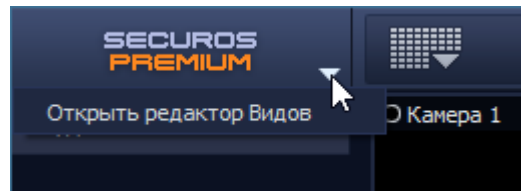


Рис. 193. Переход в Редактор Видов

В *Редакторе Видов* можно выполнить следующие операции:

- **Создание Вида.**
- **Редактирование Вида.**
- **Переименование Вида.**
- **Удаление Вида.**

Эти операции выполняются с помощью кнопок на *Панели редактирования Видов* (см. рис. 194).

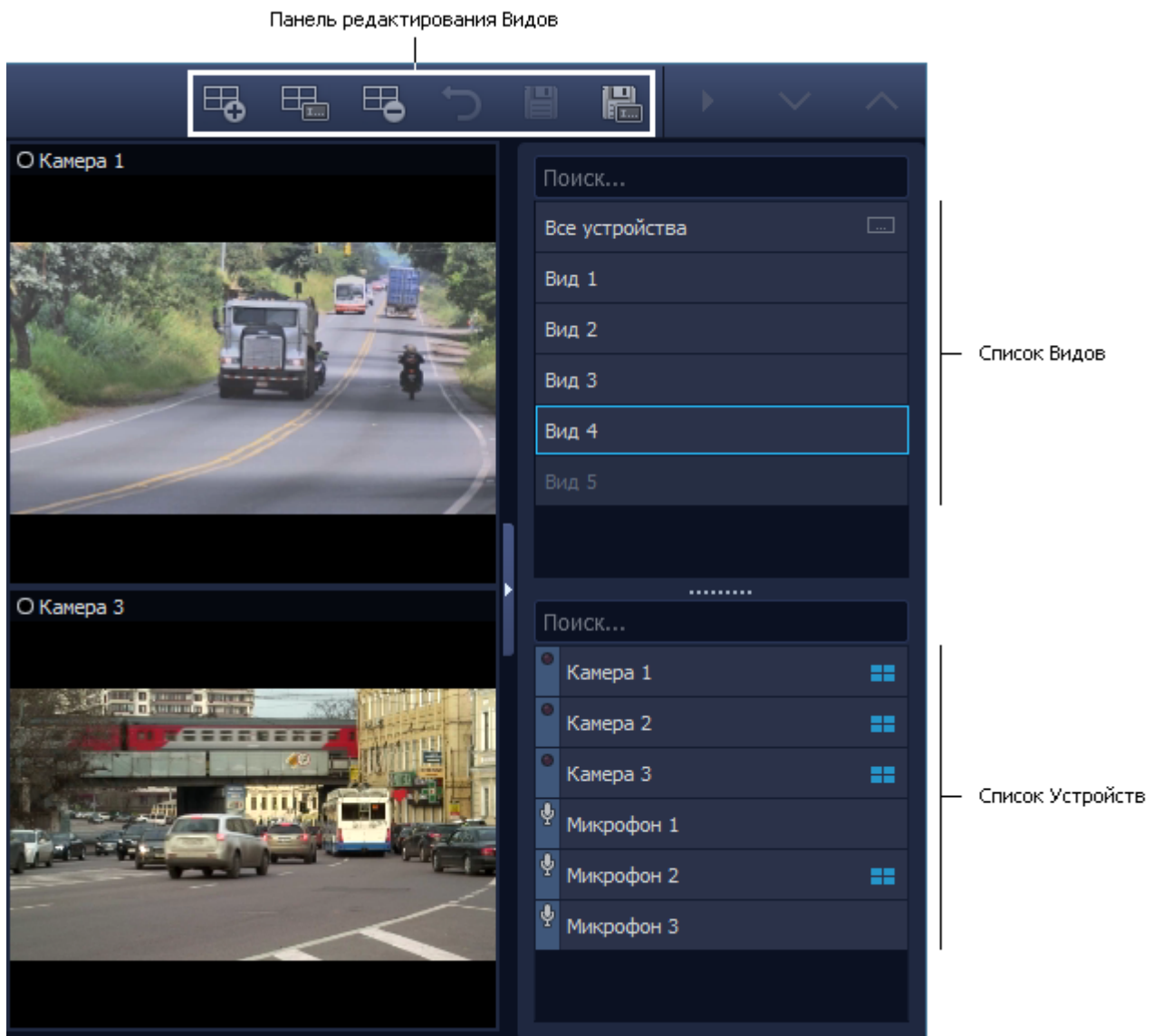


Рис. 194. Редактор Видов

Обратите внимание, что в *Редакторе Видов* *Список устройств* располагается под *Списком Видов*. В *Списке Видов* серым фоном выделяются те *Виды*, которые не содержат устройства (на рис. 194 — *Вид 5*).

Для выхода из *Редактора Видов* нажмите кнопку  в левом верхнем углу *Медиа Клиента* (см. рис. 193) и выберите **Заккрыть редактор Видов**.

9.12.2.1.9.1 Создание Вида

Примечание. В настоящем разделе приведена информация по созданию *Вида* с *Камерами*. Создание *Вида*, содержащего *Микрофоны*, осуществляется аналогичным образом.

Для создания **Вида** в *Редакторе Видов* выполните следующие действия:

1. На *Панели редактирования Видов* нажмите кнопку  (**Создать новый**). Появится окно создания *Вида* (см. рис. 195).

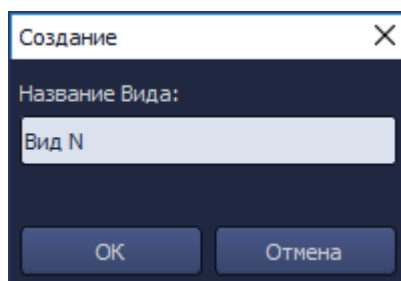


Рис. 195. Окно создания Вида

2. Введите новое имя *Вида* в поле **Название Вида** и нажмите кнопку **ОК**.
3. По умолчанию в *Рабочей области Медиа Клиента* выбрана *Раскладка 2x2*. Для **изменения раскладки** выберите требуемую раскладку в *Панели Раскладок*.
4. Для **добавления Камеры** выберите ее в *Списке Устройств* и перетащите в требуемую ячейку *Медиа Клиента*.
5. Для **удаления Камеры** выберите ее в ячейке *Медиа Клиента* и перетащите в *Список Устройств*.
6. Для **изменения положения Камеры** выберите ее и перетащите в требуемую ячейку *Раскладки*.

7. Для сохранения изменений нажмите кнопку  (**Сохранить**) на *Панели редактирования Видов*. Для отмены изменений нажмите кнопку  (**Отменить внесенные изменения**) на *Панели редактирования Видов*.

Примечание. *Виды* с несохраненными изменениями выделяются в *Списке Видов* курсивом.

9.12.2.1.9.2 Редактирование Вида

Редактирование Вида возможно путем добавления или удаления *Камер* и/или *Микрофонов*, изменения положения *Камер* и/или *Микрофонов* в ячейках *Медиа Клиента*, изменения *Раскладки Рабочей области Медиа Клиента*. О том, как выполнить эти действия, см. раздел **Создание Вида**.

Для сохранения *Вида* с тем же именем нажмите кнопку  (**Сохранить**), с новым именем — кнопку  (**Сохранить как**).

Примечания:

1. При сохранении изменения *Вида* применяются для всех *Медиа Клиентов*, использующих этот *Вид*.
 2. *Вид* с устройствами, доступ к которым запрещен (*Вид* со значком  в *Списке Видов*), не может быть сохранен с прежним именем. В сохраненном с новым именем *Виде* ячейки *Медиа Клиента* с такими устройствами будут пустыми.
-

9.12.2.1.9.3 Переименование Вида

Для переименования *Вида* в *Редакторе Видов* выполните следующие действия:

1. В *Списке Видов* выберите требуемый *Вид*.
2. На *Панели редактирования Видов* нажмите кнопку  (**Переименовать**). Появится окно **Переименование** (см. рис. 196).

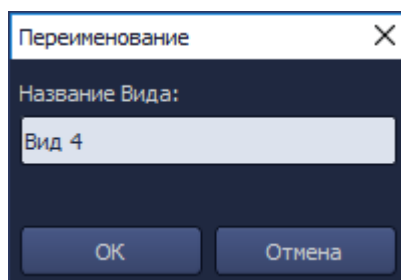


Рис. 196. Окно Переименование

3. Введите новое имя *Вида* в поле **Название Вида** и нажмите кнопку **ОК**.

Дополнительная информация

Переименовать *Вид* также можно с помощью *Дерева объектов SecurOS* (см. раздел [Работа с объектами](#)).

Примечание. *Вид* с устройствами, доступ к которым запрещен (*Вид* со значком  в *Списке Видов*), не может быть переименован.

9.12.2.1.9.4 Удаление Вида

Для удаления *Вида* в *Редакторе Видов* выполните следующие действия:

1. В *Списке Видов* выберите требуемый *Вид*.
2. На *Панели редактирования Видов* нажмите кнопку  (**Удалить**).

Дополнительная информация

Удалить *Вид* также можно с помощью *Дерева объектов SecurOS* (см. раздел [Работа с объектами](#)).

Примечание. Вид с устройствами, доступ к которым запрещен (Вид со значком  в Списке Видов), не может быть удален.

9.13 Примеры настройки

В данном разделе приведены примеры настройки типовых конфигураций.

9.13.1 Одиночная конфигурация

Постановка задачи: один компьютер и две подключенные к локальной сети видеокамеры. Компьютер получает и записывает видеопоток и осуществляет мониторинг камер.

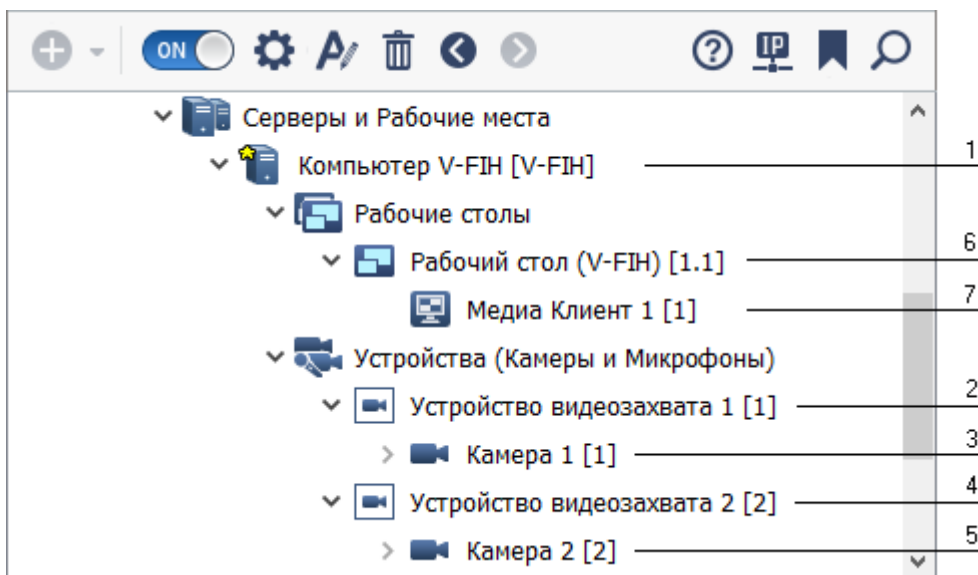


Рис. 197. Дерево объектов при одиночной конфигурации

Решение (см. рис. 197):

Перейдите в режим администрирования (см. [Администрирование SecurOS](#)) и выполните следующие действия:

1. Откройте окно настройки параметров объекта *Компьютер* (см. [Изменение параметров объекта](#)). В блоке **Архив** укажите значение Чтение и Запись для параметра **Видео** хотя бы для одной директории (например, для диска C : \).
2. В дереве объектов перейдите к ветви *Компьютер* → *Устройства (Камеры и Микрофоны)* и создайте объект *Устройство видеозахвата*.

Укажите следующие значения параметров объекта:

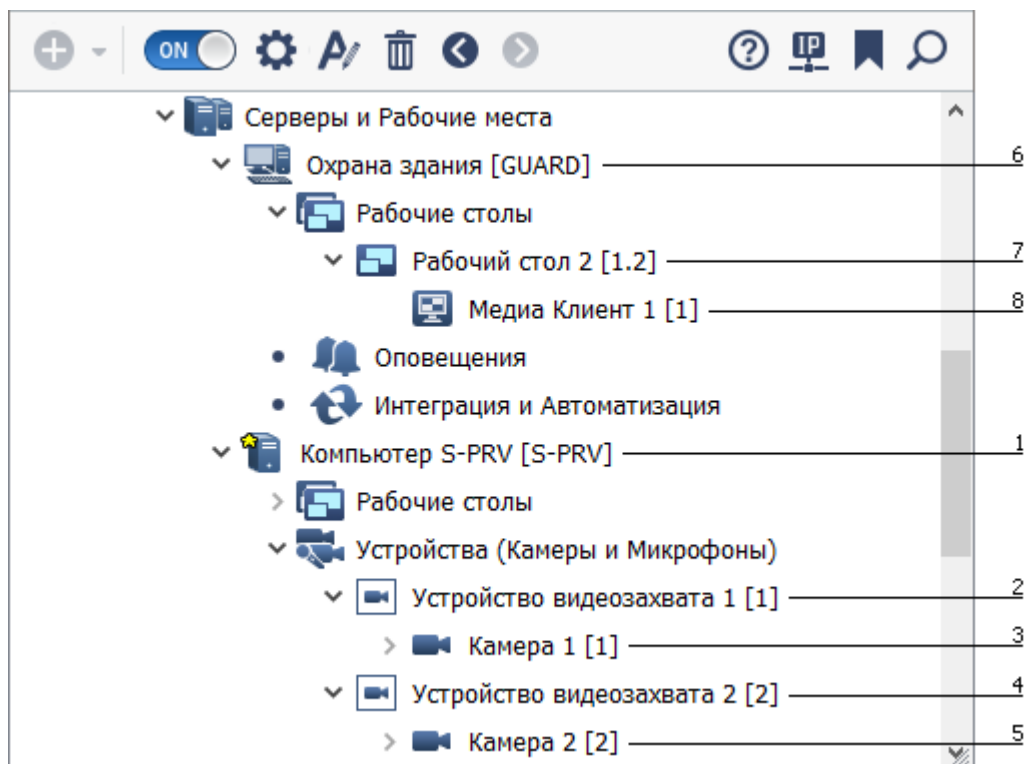
- **Тип:** производитель камеры;
- **Модель:** модель камеры выбранного производителя или, в некоторых случаях, протокол связи с камерой;
- **Протокол:** версия протокола связи с камерой. Для некоторых моделей параметр может отсутствовать;
- **IP-адрес:** адрес камеры в сети TCP/IP;
- **Пользователь и Пароль:** логин и пароль пользователя, имеющего доступ к видеопотоку камеры (задается в веб-интерфейсе самой камеры).

3. Создайте объект *Камера*, дочерний созданному *Устройству видеозахвата*.
4. Создайте второй объект *Устройство видеозахвата* и аналогичным образом выполните его настройку.
5. Создайте объект *Камера*, дочерний второму *Устройству видеозахвата*.
6. В дереве объектов перейдите к ветви *Компьютер* → *Рабочие столы* и создайте объект *Рабочий стол*.
7. Создайте объект *Медиа Клиент*, дочерний созданному объекту *Рабочий стол*.
8. Выйдите из режима администрирования.

На полноэкранном *Медиа Клиенте* будет отображаться видео с двух камер.

9.13.2 Видеосервер и Рабочие места оператора

Постановка задачи: видеосервер и две подключенные к локальной сети видеокамеры. Мониторинг может выполняться с одного или нескольких рабочих мест оператора. Для них будет создан пользовательский интерфейс – *Профиль Рабочего места оператора* (см. **Профили Рабочих мест оператора**), который может быть использован на всех компьютерах.



Решение (см. рис. 198):

Перейдите в режим администрирования (см. **Администрирование SecurOS**) и выполните следующие действия:

1. Откройте окно настройки параметров объекта *Компьютер*, соответствующего видеосерверу (см. **Изменение параметров объекта**). В блоке **Архив** укажите значение **Чтение** и **Запись** для параметра **Видео** хотя бы для одной директории (например, для диска C:\).
2. В дереве объектов перейдите к ветви *Компьютер* → *Устройства (Камеры и Микрофоны)* и создайте объект *Устройство видеозахвата*.

Укажите следующие значения параметров объекта:

- **Тип:** производитель камеры;
 - **Модель:** модель камеры выбранного производителя или, в некоторых случаях, протокол связи с камерой;
 - **Протокол:** версия протокола связи с камерой. Для некоторых моделей параметр может отсутствовать;
 - **IP-адрес:** адрес камеры в сети TCP/IP;
 - **Пользователь и Пароль:** логин и пароль пользователя, имеющего доступ к видеопотоку камеры (задается в веб-интерфейсе самой камеры).
3. Создайте объект *Камера*, дочерний созданному *Устройству видеозахвата*.
 4. Создайте второй объект *Устройство видеозахвата* и аналогичным образом выполните его настройку.
 5. Создайте объект *Камера*, дочерний второму *Устройству видеозахвата*.
 6. Создайте объект *Компьютер* с любыми идентификатором и именем, соответствующими его назначению, и ролью *Рабочее место оператора*.
 7. В настройках созданного объекта *Компьютер* отметьте флаг **Использовать как Профиль Рабочего места оператора**.
 8. Создайте дочерний объект *Рабочий стол* в группе *Рабочие столы*.
 9. Создайте объект *Медиа Клиент*, дочерний созданному объекту *Рабочий стол*.
 10. Запустите интерфейс оператора SecurOS на компьютере, который будет использоваться как *Рабочее место оператора*. Укажите IP-адрес или DNS/WINS-имя видеосервера.

Загрузится интерфейс оператора с *Рабочим окружением*, соответствующим созданному профилю. Появится *Медиа Клиент*, на котором будет отображаться видео с двух камер.

9.13.3 Настройка камеры

Процедура настройка камеры включает следующие операции:

1. **Добавление устройства видеозахвата в систему.**
2. **Добавление камеры в систему.**
3. **Выбор камеры для работы с Медиа Клиентом.**
4. **Добавление прав пользователя.**
5. **Настройка RTZ-устройства.**

9.13.3.1 Добавление устройства видеозахвата в систему

Для добавления *Устройства видеозахвата* выполните следующие действия:

1. Войдите в режим администрирования.
2. В *Дереве объектов* выберите объект *Компьютер*, с которым будет связано добавляемое устройство.
3. В группе *Устройства* (*Камеры и Микрофоны*) создайте дочерний объект *Устройство видеозахвата*.
4. В окне **Параметры создаваемого объекта** задайте требуемые значения.

5. В окне настройки параметров созданного объекта (см. рис. 199) задайте требуемые значения.

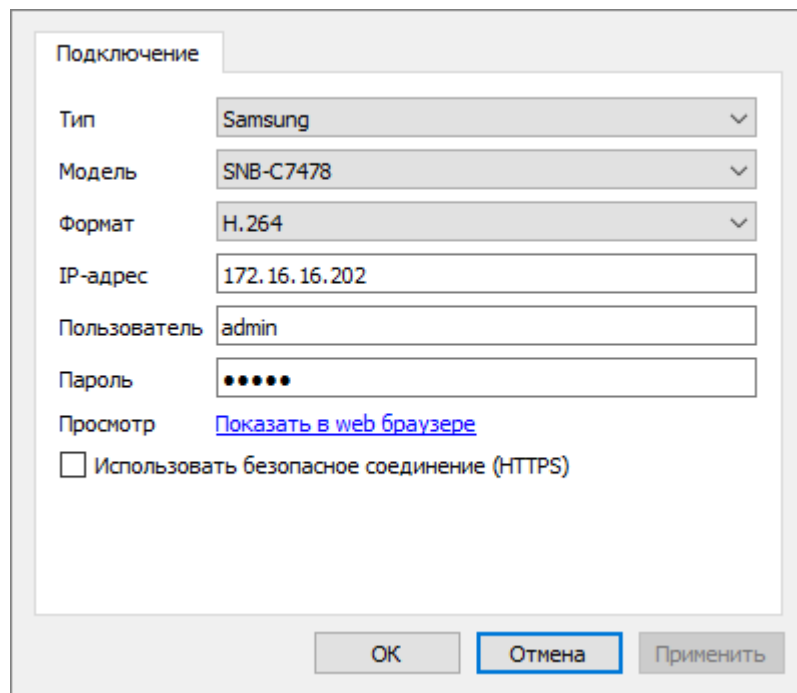


Рис. 199. Окно настройки параметров устройства видеозахвата

6. Примените новые настройки.

9.13.3.2 Добавление камеры в систему

Для добавления *Камеры* выполните следующие действия:

1. Войдите в режим администрирования.
2. Выберите в *Дереве объектов* созданное *Устройство видеозахвата*.
3. Создайте дочерний объект *Камера*.
4. В окне **Параметры создаваемого объекта** задайте требуемые значения.

Примечание. Используйте разделители ":" в **Названии** объекта, чтобы определить уровень вложенности *Камеры* в *Списке Устройств* (например, Завод:Цех:Участок:Камера1). Для отображения заданных таким образом групп параметр **Группировать Камеры и Микрофоны по имени** должен быть включен (см. [Закладка Отображение](#)).

5. В окне настройки параметров созданного объекта (см. рис. 200) задайте требуемые значения.

Примечание. На данном этапе возможна настройка PTZ-устройства управления камерой. Последовательность настройки описана в разделе [Настройка телеметрии](#). Операция также может быть выполнена отдельно.

Общие | Запись | Аудио | Детекторы | PTZ | Дополнительные

Координаты: Географические координаты (GPS, ГЛОНАСС и т. д.) в любом формате

Канал: 1

Поворотное устройство: Не использовать

Дворник: Не использовать

Отображение: Сохранять пропорции

Размер буфера: 0 мс

OK Отмена Применить

Рис. 200. Окно настройки параметров камеры

6. Примените новые настройки.

9.13.3.3 Выбор камеры для работы с Медиа Клиентом

По умолчанию, на каждом вновь созданном *Медиа Клиенте* будет выводиться изображение со всех камер, подключенных к системе.

Для вывода на *Медиа Клиенте* изображения только от требуемых *Камер* выполните следующие действия:

1. Войдите в режим администрирования.
2. В *Дереве объектов* выберите *Медиа Клиент*, для которого необходимо настроить список *Камер* (**Объект охраны** → *группа Серверы и Рабочие места* → **Компьютер** → *группа Рабочие столы* → **Рабочий стол** → **Медиа Клиент**).
3. Войдите в режим редактирования настроек *Медиа Клиента*. На закладке **Камеры** (см. рис. 201) выполните следующие действия:

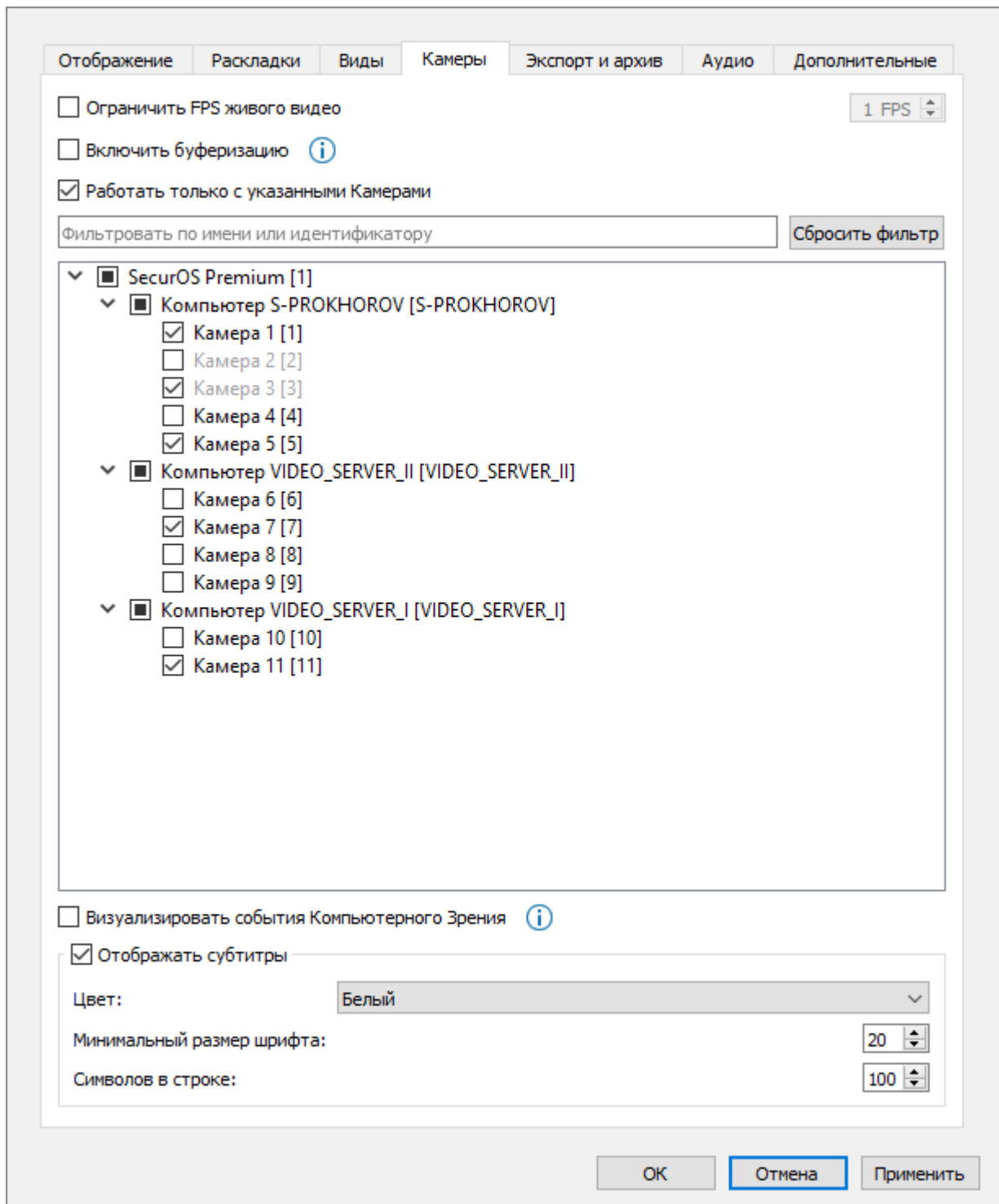


Рис. 201. Выбор камер для отображения на Медиа Клиенте

- отметьте флажок **Работать только с указанными Камерами**.
- в *Дереве объектов* отметьте флажки слева от тех *Камер*, изображение с которых необходимо выводить на *Медиа Клиенте*.

4. Примените новые настройки.

9.13.3.4 Добавление прав пользователя

Для пользователей, созданных системой по умолчанию, права на дочерние объекты наследуются от родительского. В случае, если наследуемых по умолчанию прав недостаточно для управления вновь созданным объектом, такие права необходимо назначить. Для добавления пользователю прав на вновь созданный объект выполните следующие действия:

1. Войдите в режим администрирования.
2. В *Дереве объектов SecurOS* выберите объект *Права пользователя*, в котором определен пользователь или группа, которым необходимо предоставить право управления созданной *Камерой*.
3. В окне настройки прав (см. рис. 202) выберите созданный объект *Камера*, для которого задайте требуемый уровень доступа (значок слева от объекта дерева).

Рис. 202. Окно настройки параметров объекта Права пользователя

Примечание. Детальное описание уровней доступа и соответствующих им значков приведено в разделе [Права пользователя](#).

- По умолчанию пользователю доступен захват управления PTZ с автоматическим освобождением. Если необходимо предоставить пользователю право удерживать управление PTZ в течение неограниченного времени, отметьте флажок **Разрешить удерживать управление PTZ** (подробнее о режимах раздельного управления см. **Раздельное управление телеметрией**).
- Если необходимо ограничить порядок доступа пользователей к управлению PTZ (см. **Совместное управление телеметрией** и **Раздельное управление телеметрией**), задайте требуемое значение в поле **Приоритет управления PTZ**.

Примечание. Заданный приоритет пользователя распространяется на все *Камеры* системы, управляемые данным пользователем.

- Примените новые настройки.

9.13.3.5 Настройка телеметрии

Настройка телеметрии выполняется на закладках **Общие** и **PTZ** в окне настройки параметров *Камеры*.

После выполнения любой из процедур настройки поворотного устройства, при активации ячейки каждой управляемой камеры, расположенной на *Медиа Клиенте*, будет отображаться кнопка управления **PTZ**.

При активации управляемой камеры на *Медиа Клиенте* оператора будет активирована *PTZ-панель*.

9.13.3.5.1 Настройка телеметрии для IP-устройств

Для настройки нативной телеметрии IP-устройства выполните следующие действия:

- Войдите в режим администрирования.
- В *Дереве объектов SecurOS* выберите объект *Камера* (см. раздел **Настройка камеры**), для которой необходимо настроить телеметрию.
- На закладке **Общие** (см. рис. 203) в выпадающем списке параметра **Поворотное устройство** выберите значение **Использовать**.

Рис. 203. Закладка **Общие** окна настройки параметров объекта *Камера*

4. На закладке **PTZ** (см. рис. 204) задайте значения соответствующих параметров.

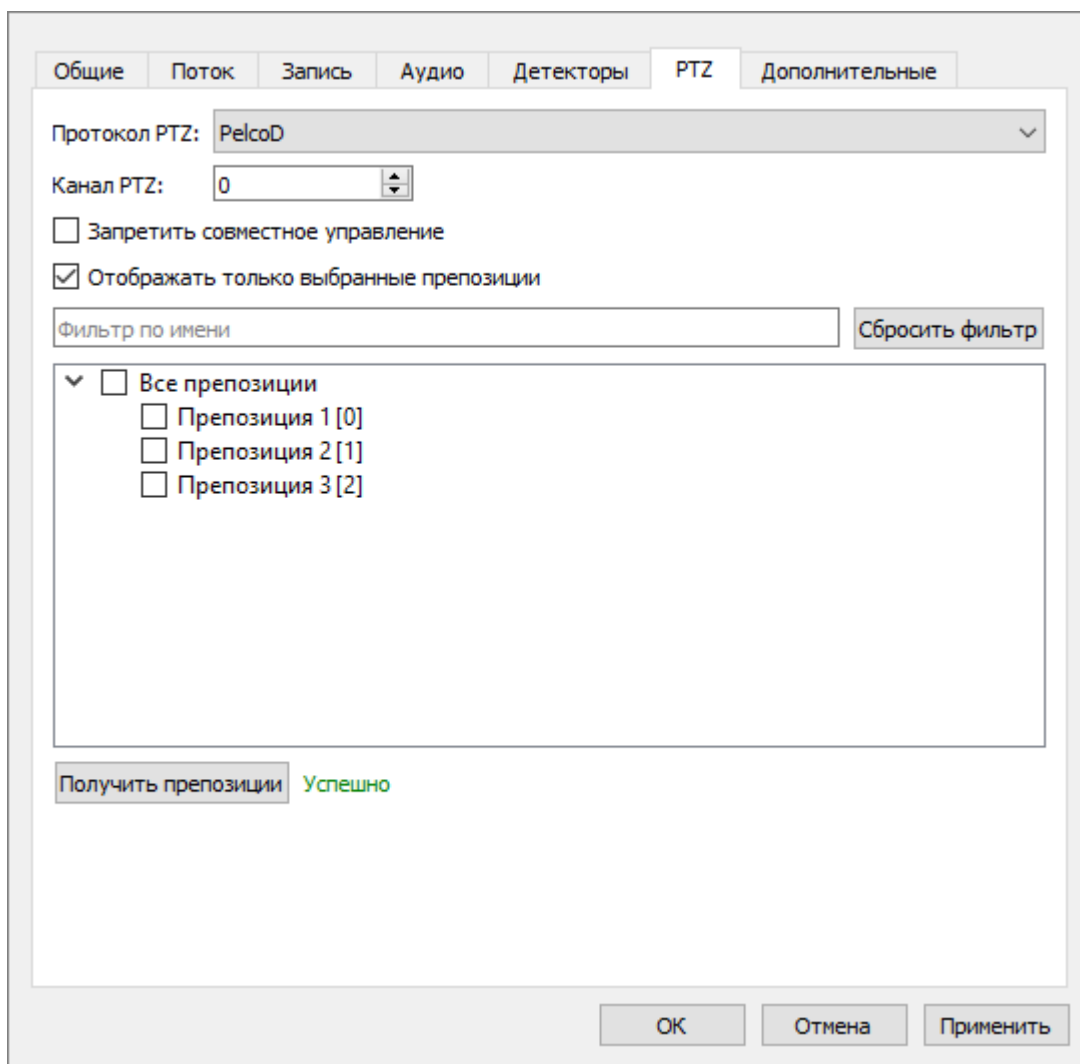


Рис. 204. Закладка PTZ окна настройки параметров объекта Камера

5. Выберите режим управления телеметрией:
- Совместное управление — для выбора режима используйте значение по умолчанию (флажок **Запретить совместное управление** не отмечен). Подробнее о режиме совместного управления см. раздел **Совместное управление телеметрией**;
 - Раздельное управление — для выбора режима отметьте флажок **Запретить совместное управление**. Подробнее о режиме раздельного управления см. раздел **Раздельное управление телеметрией**.
6. Если выбран режим Раздельное управление, задайте приоритет управления телеметрией для каждого пользователя системы (см. **Права пользователя**).
7. Для включения возможности длительного удержания управления оператором отметьте флажок **Разрешить удерживать управление PTZ** в настройках объекта **Права пользователя**.
8. Для отображения **Панели PTZ** на **Медиа Клиенте** отметьте флажок **Панель управления поворотным устройством** на закладке **Отображение** окна настроек параметра **Медиа Клиента**.

9. Для отображения кнопки **PTZ** в ячейке *Камеры* отметьте флажок **Управление поворотным устройством с помощью мыши** на закладке **Отображение** окна настроек параметра **Медиа Клиента**.
10. Примените новые настройки.

9.13.3.5.1.1 Совместное управление телеметрией

В режиме совместного управления телеметрией выполняются все поступившие команды. Команды выполняются в том порядке, в каком они были отправлены операторами. Каждая новая команда начинает выполняться сразу после ее получения. Например, первый оператор запустил патрулирование, а второй, через малый промежуток времени, стал поворачивать камеру с помощью джойстика. В этом случае патрулирование будет прервано, начнется поворот камеры.

При работе в режиме совместного управления:

- приоритет отправителя команды не анализируется;
- блокировка управления телеметрией не осуществляется;
- команды управления, посланные с помощью *Макрокоманд* или *Скриптов Node.js* исполняются в порядке общей очереди.

9.13.3.5.1.2 Раздельное управление телеметрией

Внимание! Режим раздельного управления телеметрией применим только к камерам, оборудованным встроенным поворотным устройством.

В режиме раздельного управления телеметрией возможны 2 варианта работы оператора:

1. **Захват управления с автоматическим освобождением.**
2. **Захват управления на длительное время с освобождением по команде оператора (длительное удержание).**

Захват управления с автоматическим освобождением доступен по умолчанию. Возможность захвата и длительного удержания управления настраивается дополнительно администратором (см. **Права пользователя**, параметр **Разрешить удерживать управление PTZ**). Если эта возможность настроена, оператор может выбрать один из двух вариантов работы.

Для каждого из вариантов управления:

- анализируется приоритет отправителя команды;
- при захвате управления доступ к управлению блокируется для всех пользователей с равным или низшим приоритетом;
- команды управления, посланные с помощью *Макрокоманд* или *Скриптов Node.js* исполняются в зависимости от их приоритета.

Захват управления с автоматическим освобождением

Если выбран вариант управления с автоматическим освобождением, система функционирует следующим образом:

1. Оператор отправляет команду управления PTZ.
2. На время выполнения команды система передает управление этому оператору и анализирует все прочие поступающие команды. При этом:

- если команду отправил пользователь, приоритет которого ниже или равен приоритету текущего оператора, команда игнорируется.
 - если команду отправил пользователь, приоритет которого выше приоритета текущего оператора, выполнение текущей команды прекращается, начинается выполнение новой команды.
3. После выполнения текущей команды система в течение 5 секунд ожидает новую команду от этого же оператора.
 4. Если такая команда не была отправлена, система автоматически освобождает управления для любого оператора сети.

Захват управления на длительное время с освобождением по команде оператора (длительное удержание)

Если выбран вариант с длительным удержанием управления, система функционирует следующим образом:

Примечание. Если возможность длительного удержания настроена администратором, в ячейке камеры отображаются дополнительные элементы управления (см. [Краткое руководство пользователя SecurOS](#)).

1. Оператор включает длительное удержание телеметрии и отправляет команду управления PTZ.
2. Система передает управление этому оператору на неограниченное время и анализирует все прочие поступающие команды. При этом:
 - если команду отправил пользователь, приоритет которого ниже или равен приоритету текущего оператора, команда игнорируется.
 - если команду отправил пользователь, приоритет которого выше приоритета текущего оператора, управление передается этому пользователю. При этом возможны два варианта поведения системы:
 - команда отправлена в режиме управления с автоматическим освобождением (без включения длительного удержания) — после выполнения команды система в течение 5 секунд ожидает новую команду от этого же оператора. Если такая команда не была отправлена, система автоматически освобождает управление для любого оператора сети.
 - команда отправлена после включения длительного захвата управления — см. п. 2. По окончании работы управление освобождается оператором вручную или может быть освобождено оператором с более высоким приоритетом. Суперпользователь (см. [Пользователи в SecurOS](#)) может снять блокировку любого другого пользователя, включая собственную блокировку на другом *Компьютере*.

Командам управления телеметрией, посланным с помощью *Макрокоманд* и *Скриптов Node.js*, может быть присвоен собственный приоритет (параметр `priority`, см. [Руководство программиста SecurOS](#)). Если такой приоритет выше, чем приоритет *Пользователя*, захватившего управление, то управление PTZ будет осуществляться из *Макрокоманды* или *Скрипта Node.js*.

При работе в режиме раздельного управления Панель управления PTZ *Медиа Клиента* и кнопка управления PTZ в ячейке *Камеры* блокируются для всех остальных пользователей системы, кроме захватившего управление и пользователей с более высоким приоритетом (подробнее см. [Краткое руководство пользователя SecurOS](#)).

9.13.4 Настройка джойстика

Для использования джойстика при управлении с *Медиа Клиента Камерами*, оснащенными поворотным устройством (см. [Краткое руководство пользователя SecurOS](#)), необходимо выполнить процедуру подключения и настройки.

Чтобы настроить джойстик:

1. Подключите джойстик к компьютеру рабочего места оператора. Устройство определится автоматически, или будет необходимо установить драйверы.
2. Найдите в списке устройств (**Панель управления** → **Игровые устройства**) установленный джойстик и запишите его название в точности так, как в списке (например, Joystick_Name).
3. Сохраните конфигурационный файл джойстика default.xml, находящийся в папке \Joy_config корневой директории SecurOS, в файл Joystick_Name.xml в этой же папке (или, в качестве альтернативы, скопируйте файл default.xml в ту же папку и соответствующим образом переименуйте его).
4. Нажмите в списке игровых устройств кнопку **Свойства** и в появившемся окне вкладку **Калибровка**. Проведите калибровку управления ручками и кнопками установленного джойстика.

Внимание! Процедура калибровки необходима, иначе устройство не будет функционировать в SecurOS!

10 Аудиоподсистема

Аудиоподсистема используется для работы и настройки аудиоустройств (звуковых плат, микрофонов) в сети SecurOS, обмена аудиопотоками между серверами и рабочими местами, а также для работы с живым звуком и аудиоархивом на рабочих местах.

10.1 Режимы работы

Работа с аудиопотоком может осуществляться в одном из двух режимов:

1. **Синхронная запись и воспроизведение аудио- и видеопотока;**
2. **Независимая запись и воспроизведение произвольного аудиопотока.**

Возможности использования системных объектов для записи и дальнейшего воспроизведения аудиопотока в каждом из режимов имеют принципиальные отличия и определяются их настройками. Детальное описание особенностей каждого режима приведено ниже.

10.1.1 Синхронная запись и воспроизведение аудио- и видеопотока

В данном режиме видеопоток записывается совместно со звуковым сопровождением, что позволяет при последующем воспроизведении архивных записей анализировать не только видео, но и аудиоинформацию.

Синхронная запись аудио- и видеопотока осуществляется с использованием микрофона, ассоциированного с камерой. Если *Камера* использует Встроенный микрофон, никаких дополнительных объектов не требуется. Если *Камера* использует внешний *Микрофон*, его необходимо создать в *Дереве объектов* (см. **Микрофон**). Задать встроенный или внешний микрофон можно в настройках объекта *Камера* (см. **Камера**).

Управление режимом синхронной записи и воспроизведения осуществляется с помощью элементов управления ячейки *Медиа Клиента* (см. **Медиа Клиент**), в которую выводится изображение с *Камеры*, с которой связан соответствующий *Микрофон*.

Внимание! *Микрофон*, ассоциированный с *Камерой*, ни при каких условиях не может быть использован отдельно от *Камеры* для независимой записи произвольного аудиопотока.

Описание операций настройки системы для обеспечения режима синхронной записи аудио- и видеопотока приведено в разделе **Пример настройки для синхронного прослушивания, записи и воспроизведения аудио- и видеопотока**.

10.1.2 Независимая запись и воспроизведение произвольного аудиопотока

Запись произвольного аудиопотока, не привязанного к видеопотоку, осуществляется с помощью объекта *Микрофон*, не ассоциированного с объектом *Камера*.

Управление режимом независимой записи и воспроизведения осуществляется с помощью объекта *Медиа Клиент*.

10.2 Описание объектов

Аудиоподсистема представлена следующими объектами:

- **Устройство аудиозахвата.**
- **Микрофон.**

10.2.1 Устройство аудиозахвата

Объект предназначен для настройки и инициализации в сети SecurOS следующих типовых аудиоисточников:

- IP-устройств;
- физических устройств аудиозахвата, установленных на компьютере сети, включая:
 - звуковые платы;
 - подключенные к аудиовходам компьютера микрофоны.

Родительский объект — *Компьютер\группа Устройства (Камеры и Микрофоны).*

Рис. 205. Окно настройки параметров объекта Устройство аудиозахвата

Примечание. Внешний вид окна зависит от **Типа** и **Модели** устройства.

Таблица 58. Параметры объекта Устройство аудиозахвата

Параметр	Описание
Основные	

Параметр	Описание
Тип	Выберите тип аудиоисточника. Обязательный параметр. Внимание! В ОС Linux тип аудиоисточника SoundBlaster не поддерживается.
Модель	Выберите модель аудиоисточника. Обязательный параметр. Внимание! Если в SecurOS поддерживается только одна модель устройства выбранного Типа, поле недоступно для изменения.
Протокол	Выберите протокол, по которому будет работать аудиоисточник. Внимание! Если выбранная Модель устройства поддерживает только один протокол, поле недоступно для изменения.
Частота	Выберите частоту для аудиоисточника (Гц). Обязательный параметр. Примечание. Чем выше частота, тем выше качество звука архива, однако более высокая частота дискретизации требует больше свободного места на сервере для хранения аудиоархива. Внимание! Поле доступно для изменения только при выборе устройства Типа SoundBlaster.
Дополнительные	
IP-адрес	IP-адрес устройства.
Пользователь	Имя пользователя для доступа к IP-устройству. Задается с помощью интерфейсов настройки устройства (см. документацию производителя устройства).
Пароль	Пароль пользователя для доступа к IP-устройству. Задается с помощью интерфейсов настройки устройства (см. документацию производителя устройства).
Использовать безопасное соединение (HTTPS)	С помощью данного параметра задается тип соединения с устройством. Чтобы использовать защищенное соединение с устройством: • отметьте флажок; • с помощью web-интерфейса в собственных настройках устройства выберите для пользователя HTTPS-протокол и установите доверенный сертификат шифрования. Внимание! Если не выполнено одно из условий, защищенное сетевое соединение с устройством установлено не будет. Примечание. Возможность использования безопасного соединения зависит от Типа и Модели устройства.

Параметр	Описание
PCI-канал	Задайте номер PCI-канала для подключения устройств платы аудио- или видеозахвата. Обязательный параметр. Диапазон возможных значений: [1; 64]. Значение параметра уникально для каждого объекта <i>Устройство аудиозахвата</i>, дочернего системному объекту <i>Компьютер</i>. Значение по умолчанию — минимальное из диапазона возможных, исключая присвоенные другим <i>Устройствам аудиозахвата</i>. Примечание. Система позволяет использовать только один микрофон из нескольких, подключенных к звуковой плате.

10.2.2 Микрофон

Объект представляет один канал для подключения микрофона.

Родительский объект — **Устройство аудиозахвата**.

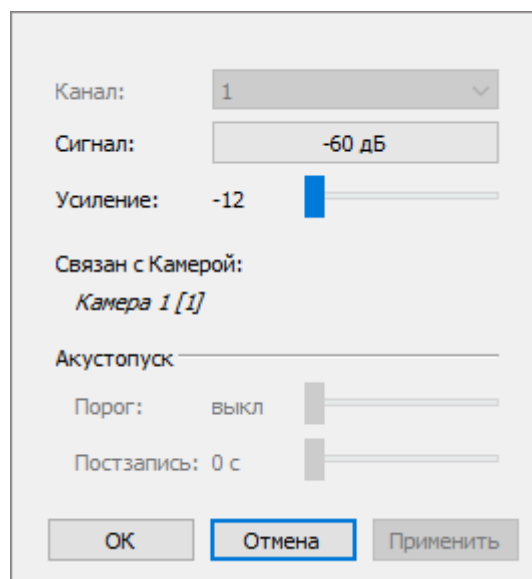


Рис. 206. Окно настройки параметров объекта Микрофон

Таблица 59. Параметры объекта Микрофон

Параметр	Описание
Канал	Выберите из списка аудиоканал для подключения микрофона.
Сигнал	Информационное поле: индикатор текущего уровня шума. Используется для проверки микрофона в режиме реального времени.
Усиление	Передвигая ползунок, измените уровень усиления сигнала (от – 12 дВ до 12 дВ). Повысьте уровень, если аудиоисточник слабый. Для визуальной настройки используйте индикатор Сигнал .

Параметр	Описание
Связан с Камерой	Если <i>Микрофон</i> привязан к <i>Камере</i> (см. Закладка Аудио), в поле выводится Название и Идентификатор соответствующей <i>Камеры</i> . В противном случае (свободный <i>Микрофон</i>) в поле выводится нет .
Акустопуск (параметры автоматической записи звука при достижении определенного порогового уровня).	
Примечание. Данная группа параметров используется только в режиме независимой записи аудиопотока (см. раздел Независимая запись и воспроизведение произвольного аудиопотока)	
Внимание! Для срабатывания акустопуска <i>Микрофон</i> необходимо поставить на охрану с помощью Макрокоманды или Скрипта Node.js , либо поставить на запись с помощью <i>Медиа Клиента</i> .	
Порог	Передвигая ползунок, установите пороговое значение уровня звука (от -60 до 0 dB), при достижении которого автоматически начинается запись. Для визуальной оценки уровня звука используйте индикатор Сигнал . При значении Off акустопуск отключен.
Постзапись	Задайте время постзаписи (в секундах) аудиоролика в случае начала записи в режиме акустопуска.

10.3 Пример настройки для синхронного прослушивания, записи и воспроизведения аудио- и видеопотока

Для настройки режима выполните следующие действия:

Если будет использоваться встроенный Микрофон

1. Для того, чтобы использовать встроенный микрофон, выберите в настройках соответствующего объекта *Камера* значение **Встроенный** в списке параметра **Микрофон** (см. раздел [Камера](#)). Теперь просмотр живого видео будет сопровождаться звуком, запись видео- и аудио- архива также будет вестись синхронно.
2. В группе *Рабочие столы* соответствующего *Компьютера* создайте объект *Рабочий стол*.
3. Создайте объект *Медиа Клиент*, дочерний созданному *Рабочему столу*, на котором разместите *Камеру* со *Встроенным Микрофоном*.

Если будет использоваться внешний Микрофон

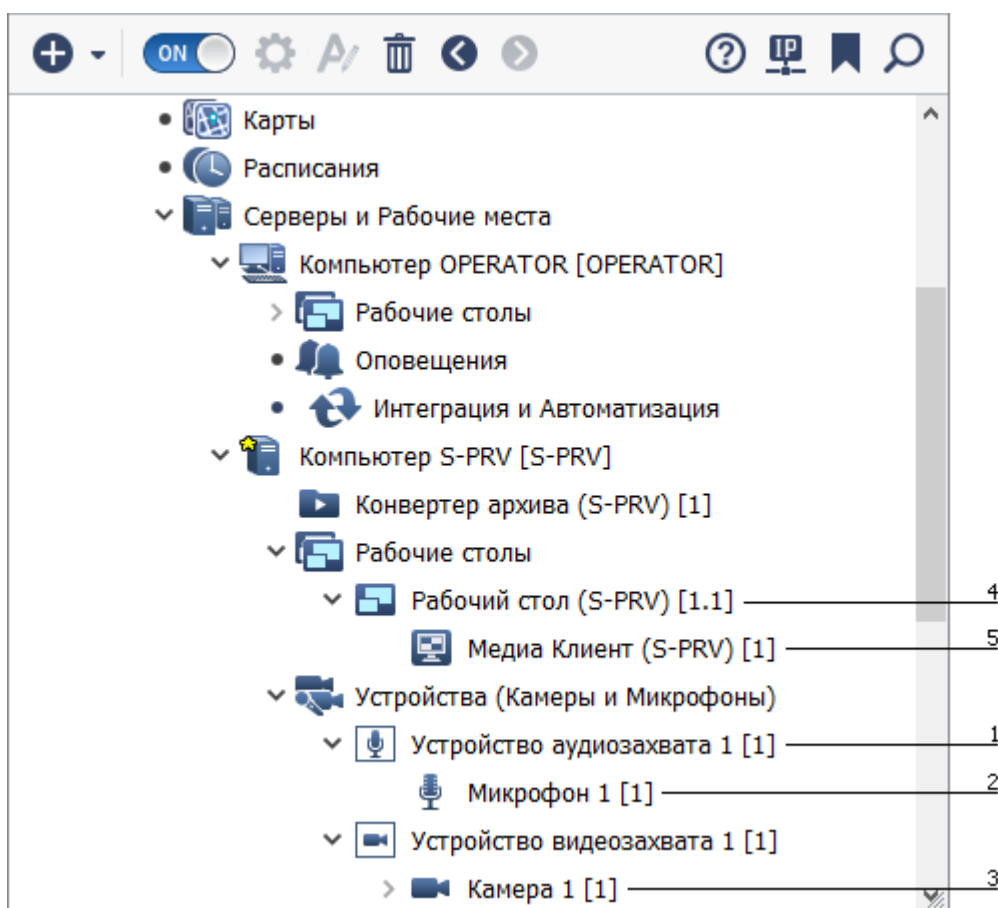


Рис. 207. Дерево объектов для рабочей станции с конфигурацией синхронной записи аудио- и видеопотока

1. В *Дереве объектов* (см. рис. 207) выберите объект *Компьютер*, на котором установлено или к которому подключено соответствующее оборудование, в дочерней группе *Устройства (Камеры и Микрофоны)* создайте объект *Устройство аудиозахвата* (см. раздел **Устройство аудиозахвата**). Настройте устройство, для чего задайте значения параметров, характерных для выбранного типа устройства.
2. Для созданного *Устройства аудиозахвата* создайте дочерний объект *Микрофон* (см. раздел **Микрофон**). Настройки, выставляемые по умолчанию, как правило, достаточны для записи звука.
3. Для того, чтобы "привязать" микрофон к определенной камере, выберите в настройках соответствующего объекта *Камера* нужный микрофон в списке параметра **Микрофон** (см. раздел **Камера**). Теперь просмотр живого видео будет сопровождаться звуком, запись видео- и аудио- архива также будет вестись синхронно.
4. В группе *Рабочие столы* соответствующего *Компьютера* создайте объект *Рабочий стол*.
5. Создайте объект *Медиа Клиент*, дочерний созданному *Рабочему столу*, на котором разместите *Камеру* с "привязанным" *Микрофоном*.

Внимание! При неравномерном воспроизведении видео, наличии циклического запаздывания или обрывов в воспроизведении сопровождающего аудио включите режим буферизации. Для включения режима в настройках *Камеры* задайте значение параметра **Размер буфера** (см. **Закладка Общие**) и отметьте флажок **Включить буферизацию** в настройках *Медиа Клиента* (см. **Закладка Камеры**).

11 Подсистема ввода/вывода

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*, *SecurOS Xpress*.

Подсистема ввода/вывода используется для управления и настройки универсальных устройств ввода/вывода (лучи и реле) в сети SecurOS.

Примечание. Универсальные устройства ввода/вывода подключаются к поддерживаемым IP-устройствам.

11.1 Описание объектов

Подсистема ввода/вывода представлена следующими объектами:

- **Луч.**
- **Реле.**
- **CCTV Клавиатура или джойстик.**

11.1.1 Луч

Объект представляет физическое сенсорное устройство или последовательную структуру датчиков (шлейф охранной сигнализации).

При срабатывании датчика *Луча* это событие фиксируется в *Протоколе событий*, из которого можно перейти на *Медиа Клиент* для просмотра видео. Если к *Лучу* привязано несколько *Камер*, при таком переходе на *Медиа Клиенте* отобразятся все эти *Камеры*. Данная функциональность позволяет синхронно просматривать видео из различных контролируемых зон, соответствующее моменту срабатывания датчика.

Родительский объект — **Устройство видеозахвата.**

Рис. 208. Окно настройки параметров объекта Луч

Таблица 60. Параметры объекта Луч

Параметр	Описание
Канал	Задайте номер канала, к которому подключен датчик.
Условие срабатывания	Выберите тип перехода в состояние тревоги. Возможные значения: • на замыкание — срабатывание при замыкании контактов; • на размыкание — срабатывание при размыкании контактов.
Тип	Выберите тип датчика (этот параметр влияет только на отображающийся на <i>Карте</i> значок устройства).
Объект в области видимости Камер(ы):	
Фильтр	Для поиска объекта по части имени или идентификатора введите в поле требуемые символы; в дереве автоматически отобразятся только те объекты, имя или идентификатор которых соответствуют заданным условиям поиска. Для того, чтобы очистить поле, нажмите кнопку Сбросить фильтр .

Параметр	Описание
Дерево объектов	Дерево <i>Компьютеров</i> с ролью <i>Видеосервер</i>, существующих в сети SecurOS. При развертывании узла каждого <i>Видеосервера</i> отображается список созданных на нем <i>Камер</i>. Отметьте флажками <i>Камеры</i>, видео с которых необходимо просматривать при срабатывании датчика <i>Луча</i>.

11.1.2 Реле

Объект представляет физический исполнительный блок (например, реле), который управляет каким-либо устройством.

Родительский объект — **Устройство видеозахвата**.

Рис. 209. Окно настройки параметров объекта Реле

Таблица 61. Параметры объекта Реле

Параметр	Описание
Номер реле	Выберите номер канала, на котором работает реле.
Тип устройства	Выберите тип управляемого устройства (параметр влияет на отображающийся значок на карте). Возможные значения: Замок, Сирена, Свет, Дворник.
Внешнее устройство	
Протокол	Выберите протокол для связи с управляемым устройством (параметр используется для управления Дворником).
Канал	Выберите канал для связи с управляемым устройством (параметр используется для управления Дворником).

11.1.3 CCTV Клавиатура или джойстик

CCTV-клавиатуры предназначены для управления объектами пользовательского интерфейса (например, *Медиа Клиентом*), *Камерами* и их режимами, выполнения операций с раскладками, операций записи изображения и т. д.

Внимание! Работа клавиатур с *Камерами Удаленных систем* не поддерживается.

Примечание. При работе с клавиатурой *Права пользователя* на управление *Камерами* учитываются так же, как при работе с *Медиа Клиентом* (см. [Права пользователя](#)).

В SecurOS поддерживаются следующие типы клавиатур:

- Клавиатуры, настраиваемые с помощью объекта *CCTV Клавиатура или джойстик*.
- Клавиатуры, работающие по принципу Plug and Play и не требующие дополнительной настройки.

Родительский объект — [Компьютер](#).

С помощью объекта можно настраивать следующие клавиатуры:

- [Bosch IntuiKey](#).
- [Hikvision DS-1100KI](#).
- [Hikvision DS-1200KI/DS-1600KI\(B\)](#).
- [Panasonic WV-CU950](#).
- [Pelco KBD300A](#).

Примечание. При указании IP-адреса устройства в настройках объекта *CCTV Клавиатура или Джойстик* необходимо учитывать маршрутизацию в сети. В некоторых случаях требуется указать внешний IP-адрес, с которого осуществляется работа с устройством. Например, при использовании VPN.

К клавиатурам, не требующим дополнительной настройки, относятся:

- AXIS T8310.
- AXIS TU9001.
- Bosch KBD-Universal XF.
- Hanwha SPC-7000.

Примечание. Принципы работы с перечисленными клавиатурами описаны в [Руководстве пользователя SecurOS](#).

Выбор **Типа устройства** осуществляется в окне настройки параметров объекта.

Внимание! Полный перечень USB-джойстиков, поддерживаемых системой, приведен в `DevicesIntegrationList`.

11.1.3.1 Bosch IntuiKey

Внимание! Для работы клавиатуры требуется, чтобы чипсет COM-порта (PL-2303) поддерживался используемой операционной системой. Проверить поддержку можно на сайте производителя http://www.prolific.com.tw/US/ShowProduct.aspx?p_id=225&pcid=41.

Рис. 210. Тип устройства Bosch IntuiKey

Внимание! Кодовая страница, используемая при передаче текстовых данных от SecurOS на клавиатуру, задается параметром **Формат** (Панель управления → Часы, язык и регион → Язык и региональные стандарты → Формат).

Таблица 62. Параметры подключения устройства Bosch IntuiKey

Параметр	Описание
COM порт	COM порт для физического подключения устройства.
Проверка (кнопка)	Проверка доступности устройства при подключении через указанный COM порт (см. Проверка связи с клавиатурой).

Параметр	Описание
Главное меню	Программируемые кнопки устройства и назначенное действие. Список возможных действий представлен командами SecurOS, которые поддерживаются устройством.
	Примечание. Значение Остальные команды включает список команд, неопределенных в Главном меню .
Инвертировать направление движения камеры (вверх/вниз)	Отметьте флажок, чтобы инвертировать перемещение камеры по вертикали при перемещении ручки джойстика вверх-вниз.

Проверка связи с клавиатурой

Для проверки связи с клавиатурой выполните следующие действия:

1. Выберите соответствующий **СОМ порт**, далее нажмите кнопку **Проверка**. Система выведет окно **Проверка связи с клавиатурой** (см. рис. 211).

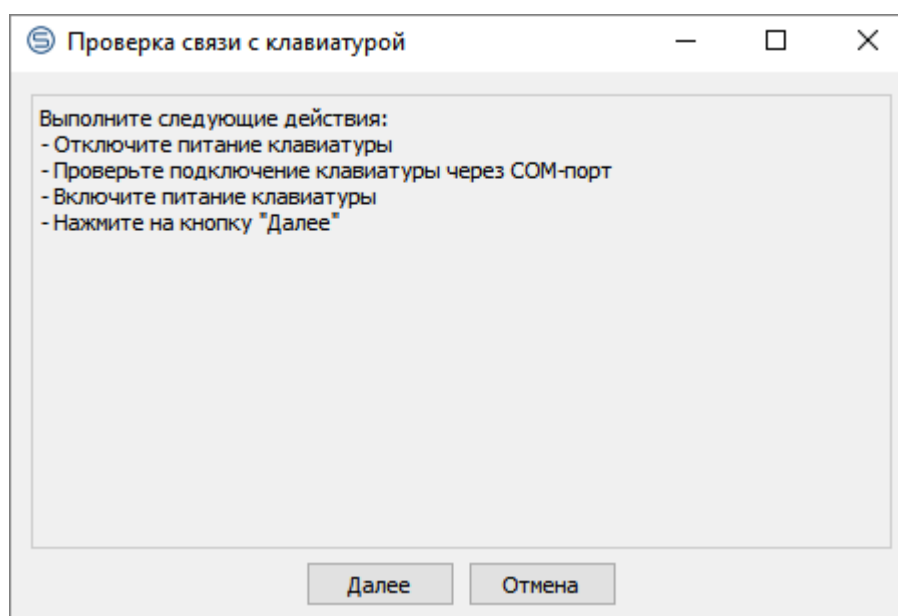


Рис. 211. Окно Проверка связи с клавиатурой

2. Последовательно выполните операции, перечисленные в окне. Нажмите кнопку **Далее**.
3. Следуйте дальнейшим указаниям, выводимым в окне.

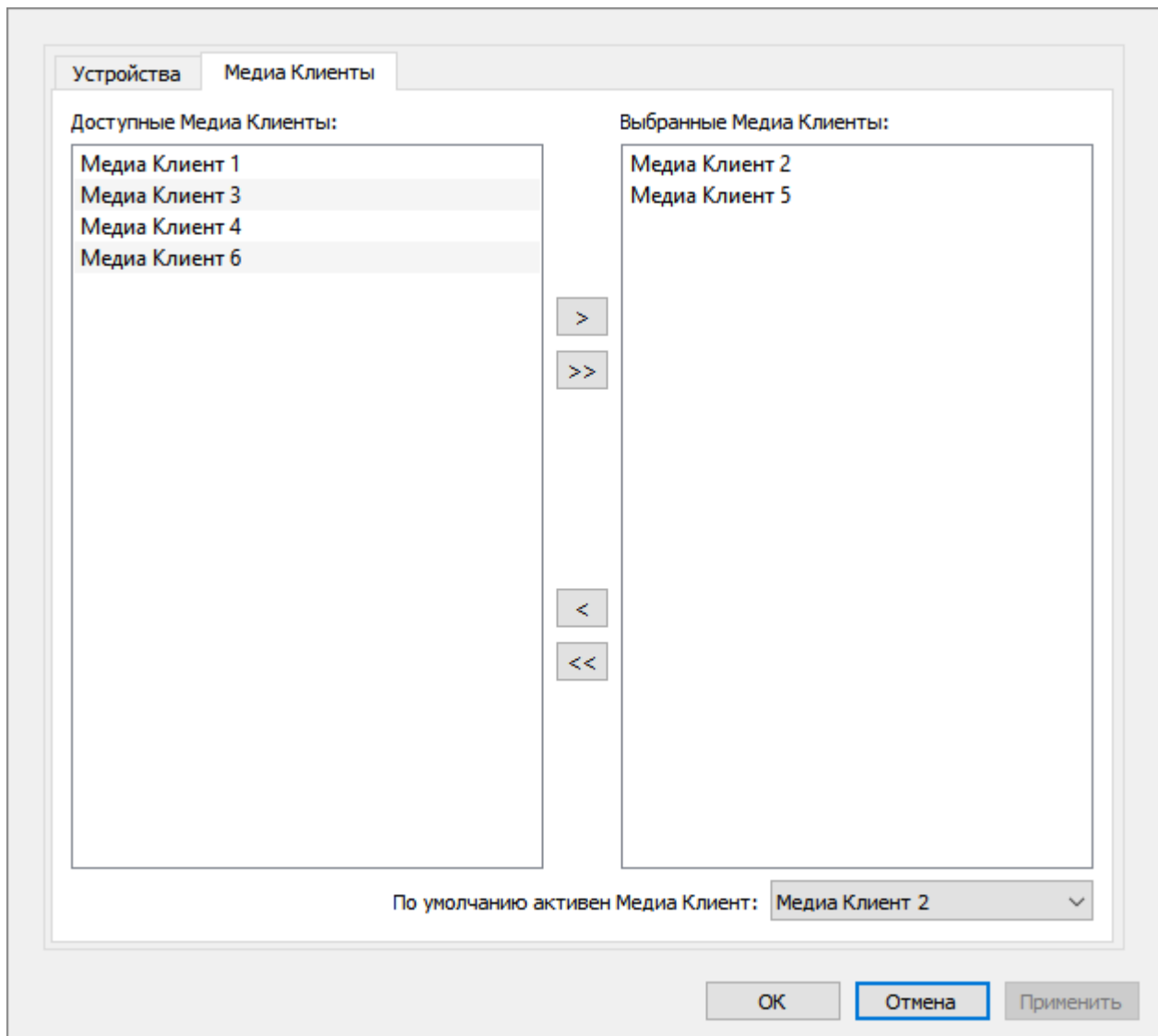


Рис. 212. Окно настройки параметров устройства. Закладка Медиа Клиенты

Закладка **Медиа Клиенты** предназначена для задания списка *Медиа Клиентов*, которыми можно будет управлять с помощью настраиваемого устройства.

Примечание. В каждый текущий момент времени с помощью объекта *CCTV Клавиатура* или джойстик можно управлять только одним *Медиа Клиентом*.

Таблица 63. Закладка Медиа Клиенты

Параметр	Описание
Доступные Медиа Клиенты	Список всех <i>Медиа Клиентов</i> , дочерних тому же объекту <i>Компьютер</i> , что и настраиваемый объект. Для возможности управления выберите требуемый <i>Медиа Клиент</i> и нажмите кнопку > .
Выбранные Медиа Клиенты	Список <i>Медиа Клиентов</i> системы, для которых определена возможность управления с помощью настраиваемого объекта <i>CCTV Клавиатура</i> или джойстик.

Параметр	Описание
По умолчанию активен Медиа Клиент	<i>Медиа Клиент</i>, который будет выбран для управления с помощью CCTV-клавиатуры по умолчанию при старте SecurOS. Возможные значения: любой <i>Медиа Клиент</i> из списка Выбранные Медиа Клиенты. Примечание. Для того, чтобы сменить управляемый <i>Медиа Клиент</i> в процессе работы с системой, задайте на устройстве его идентификатор или выберите из списка имя <i>Медиа Клиента</i> (см. Руководство пользователя соответствующей CCTV-клавиатуры).

11.1.3.2 Hikvision DS-1100KI

Устройства Медиа Клиенты

Тип устройства: Hikvision DS-1100KI

 IP-адрес: 192.168.0.210

Порт: 25

☐ Инвертировать направление движения камеры (вверх/вниз)

ОК Отмена Применить

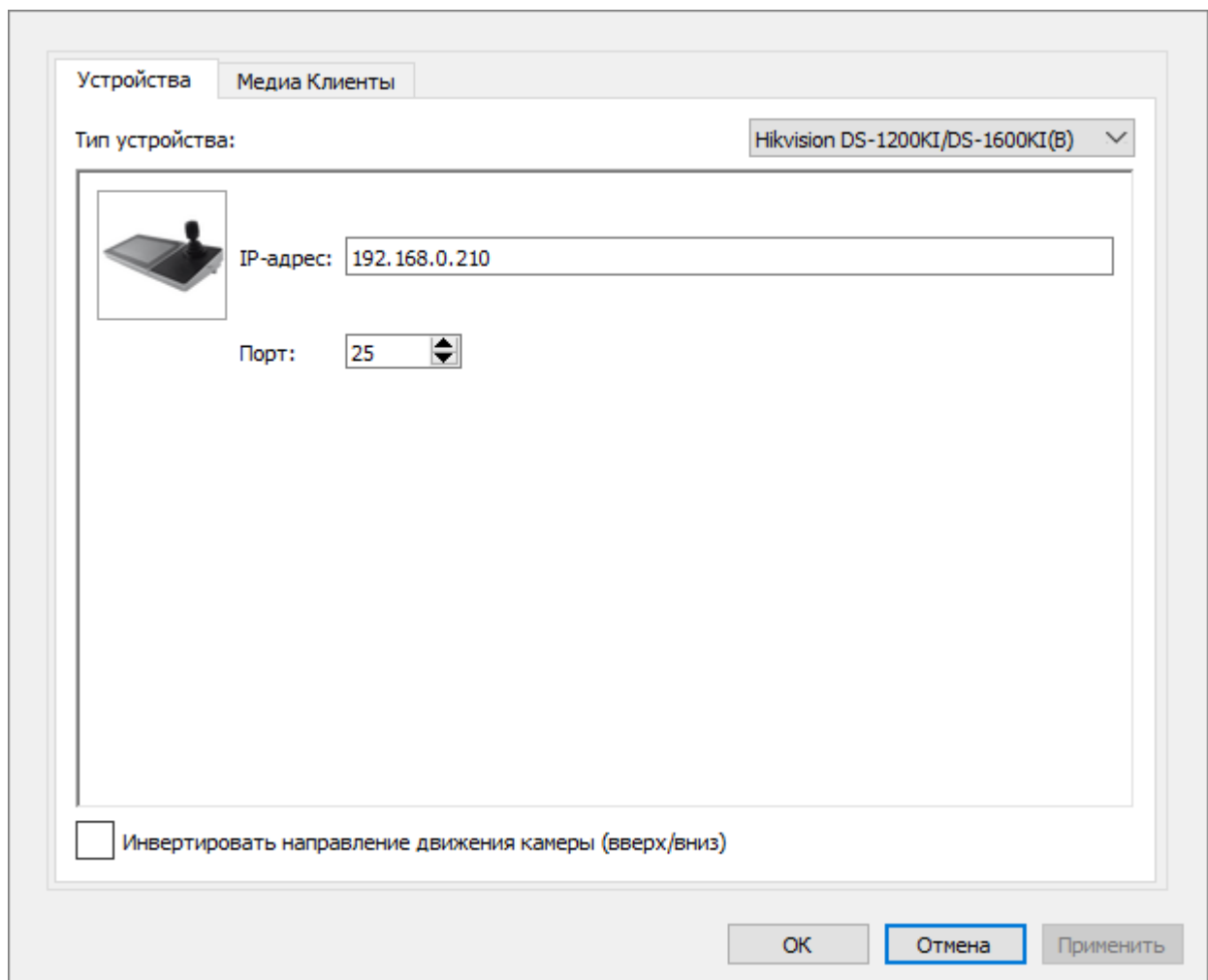
Рис. 213. Тип устройства Hikvision DS-1100KI

Таблица 64. Параметры подключения устройства Hikvision DS-1100KI

Параметр	Описание
IP-адрес	IP-адрес подключения устройства.
Порт	Сетевой порт, по которому происходит взаимодействие с клавиатурой.
Инвертировать направление движения камеры (вверх/вниз)	Отметьте флажок, чтобы инвертировать перемещение камеры по вертикали при перемещении ручки джойстика вверх-вниз.

Закладка **Медиа Клиенты** и выполняемые с ее помощью действия описаны в разделе **Bosch IntuiKey**.

11.1.3.3 Hikvision DS-1200KI/DS-1600KI(B)



Устройства Медиа Клиенты

Тип устройства: Hikvision DS-1200KI/DS-1600KI(B) ▼

 IP-адрес: 192.168.0.210

Порт: 25

☐ Инвертировать направление движения камеры (вверх/вниз)

OK Отмена Применить

Рис. 214. Тип устройства Hikvision DS-1200KI/Hikvision DS-1600KI(B)**Таблица 65.** Параметры подключения устройства Hikvision DS-1200KI/DS-1600KI(B)

Параметр	Описание
IP-адрес	IP-адрес подключения устройства.

Параметр	Описание
Порт	Сетевой порт, по которому происходит взаимодействие с клавиатурой.
Инвертировать направление движения камеры (вверх/вниз)	Отметьте флажок, чтобы инвертировать перемещение камеры по вертикали при перемещении ручки джойстика вверх-вниз.

Закладка **Медиа Клиенты** и выполняемые с ее помощью действия описаны в разделе **Bosch IntuiKey**.

11.1.3.4 Panasonic WV-CU950

Устройства Медиа Клиенты

Тип устройства: Panasonic WV-CU950

IP-адрес: 192.168.0.210

Функциональные кнопки

F1	<ничего не делать>	Shift-F1	<ничего не делать>
F2	<ничего не делать>	Shift-F2	<ничего не делать>
F3	<ничего не делать>	Shift-F3	<ничего не делать>
F4	<ничего не делать>	Shift-F4	<ничего не делать>

Кнопки джойстика

A	<ничего не делать>	B	<ничего не делать>

☐ Инвертировать направление движения камеры (вверх/вниз)

OK **Отмена** Применить

Рис. 215. Тип устройства Panasonic WV-CU950

Таблица 66. Параметры подключения устройства Panasonic WV-CU950

Параметр	Описание
IP-адрес	IP-адрес подключения устройства.

Параметр	Описание
Функциональные кнопки	Программируемые кнопки устройства и назначенное действие. Список возможных действий представлен командами SecurOS, которые поддерживаются устройством.
Кнопки джойстика	Программируемые кнопки джойстика устройства и назначенное действие. Список возможных действий представлен командами SecurOS, которые поддерживаются устройством.
Инвертировать направление движения камеры (вверх/вниз)	Отметьте флажок, чтобы инвертировать перемещение камеры по вертикали при перемещении ручки джойстика вверх-вниз.

Закладка **Медиа Клиенты** и выполняемые с ее помощью действия описаны в разделе **Bosch IntuiKey**.

11.1.3.5 Pelco KBD300A

Устройства Медиа Клиенты

Тип устройства: Pelco KBD300A

COM порт: COM1 Проверка

Программирование клавиш

ACK	<ничего не делать>
Shift-F1	<ничего не делать>
Shift-F2	<ничего не делать>
Shift-F3	<ничего не делать>
Shift-F4	<ничего не делать>
Shift-F5	<ничего не делать>

Примечание. Клавиатура будет работать только если выбран протокол Pelco ASCII. Для этого установите на задней панели клавиатуры джампер 7 в нижнее положение. Все остальные джамперы должны быть установлены в верхнее положение.

☐ Инвертировать направление движения камеры (вверх/вниз)

ОК Отмена Применить

Рис. 216. Тип устройства Pelco KBD300A

Таблица 67. Параметры подключения устройства Pelco KBD300A

Параметр	Описание
COM порт	COM порт для физического подключения устройства.
Проверка (кнопка)	Проверка доступности устройства при подключении через указанный порт.
Программирование клавиш	Программируемые кнопки устройства и назначенное действие. Список возможных действий представлен командами SecurOS, которые поддерживаются устройством.
Инвертировать направление движения камеры (вверх/вниз)	Отметьте флажок, чтобы инвертировать перемещение камеры по вертикали при перемещении ручки джойстика вверх-вниз.

Закладка **Медиа Клиенты** и выполняемые с ее помощью действия описаны в разделе **Bosch IntuiKey**.

11.2 Настройка системы для работы с Дворниками и Омывающими устройствами

Дворники и омывающие устройства устанавливаются на камеру видеонаблюдения и предназначены для дистанционной очистки стекла.

Возможность поддержки устройства и параметры его настройки указываются в сопроводительном листе видеокамеры.

Настройка и управление *Дворником/Омывающим устройством* осуществляется с помощью следующих объектов SecurOS:

- *Реле* — используется для настройки параметров управления *Дворником/Омывающим устройством*. Не требуется для камер со встроенным дворником/омывающим устройством.
- *Камера* — в настройках объекта задается устройство *Реле*, используемое для управления *Дворником/Омывающим устройством* данной камеры.

Для настройки *Дворника/Омывающего устройства* для вновь устанавливаемых камер выполните следующие действия:

1. В дереве объектов SecurOS создайте объект **Устройство видеозахвата** с дочерним объектом **Камера**, соответствующие устанавливаемой камере.
2. Создайте объект **Реле**, дочерний созданному *Устройству видеозахвата*.
3. В окне настроек объекта *Реле* выберите **Тип устройства** — Дворник (в т. ч. и для *Омывающего устройства*). При необходимости задайте параметры его управления **Протокол** и **Канал**.
4. В окне настроек созданного объекта *Камера* на закладке **Общие** в поле **Дворник** (или **Омывающее устройство** для *Омывающего устройства*) выберите созданный объект *Реле* или вариант *Встроенный*.
5. Если *Медиа Клиент* работает со списком камер, добавьте созданную *Камеру* в список **Работать только с указанными камерами**. Чтобы опция управления *Дворником/Омывающим устройством* () отображалась в ячейке *Камеры* в *Медиа Клиенте*, у пользователя должны быть установлены права на эту *Камеру* не ниже уровня **Управление**.

12 Подсистема оповещения

Подсистема оповещения информирует о событиях в сети безопасности с помощью электронных сообщений, коротких сообщений и звуковых сигналов. Оповещения о событиях объектов можно настраивать с помощью *Макрокоманд* или *Скриптов Node.js* (см. [Руководство программиста SecurOS](#)).

12.1 Описание объектов

Подсистема оповещения представлена следующими объектами:

- [Всплывающее окно HTML5](#).
- [Сервис почтовых сообщений](#).
- [Почтовое сообщение](#).
- [Сервис коротких сообщений](#).
- [Короткое сообщение](#).
- [Сервис звукового оповещения](#).
- [Служба реагирования](#).
- [Интеграция с SIP-устройствами](#).

12.1.1 Всплывающее окно HTML5

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

Объект используется для создания всплывающих окон HTML5, которые отображаются на мониторе в течение некоторого времени в ответ на какое-либо внешнее событие или поведение системы. Например, диалог может быть активирован с помощью *Скрипта Node.js* при обработке событий. Всплывающие окна могут быть закрыты вручную или автоматически системой (а также с помощью скриптов). Всплывающее окно HTML5 может представлять собой, например, интерфейс управления или простое информационное сообщение.

Внимание! Окно объекта не является полноценным браузером и обладает ограниченной функциональностью. Подробнее об особенностях работы со всплывающими окнами HTML5 и их ограничениях см. [Руководство программиста SecurOS](#).

Объект позволяет:

- Задавать размеры и положение всплывающего окна внешнего web-приложения на экране монитора.
- Отправлять дополнительные параметры из SecurOS во внешнее web-приложение.

Внимание! Всплывающее окно HTML5 всегда выводится поверх всех прочих окон, расположенных на рабочем столе Windows.

Родительский объект — *Компьютер\группа Оповещения*.

Рис. 217. Окно настройки параметров объекта Всплывающее окно HTML5

Таблица 68. Параметры объекта Всплывающее окно HTML5

Параметр	Описание
Расположение окна	
X, Y, W, H	Задайте координаты верхнего левого угла (X , Y), ширину и высоту (W , H) всплывающего окна (в процентах от размеров экрана).
Дисплей	Выберите идентификатор физического монитора, на котором будет отображаться всплывающее окно внешнего web-приложения.
URL	Задайте URL HTML-страницы внешнего приложения. Примечания: - Для указания пути с помощью файлового менеджера нажмите кнопку . - Указание пути с помощью файлового менеджера при удаленной настройке невозможно.
Дополнительно	При необходимости передавать дополнительные параметры из SecurOS во внешнее web-приложение, задайте эти параметры в данном поле. Заданные параметры будут переданы внешнему приложению в сообщении SETUP.

12.1.2 Сервис почтовых сообщений

Объект представляет SMTP-сервер, используемый для отправки уведомлений по электронной почте.

Примечание. При отправке сообщений с помощью *Скриптов Node.js* (подробнее см. [Руководство программиста SecurOS](#)) или по протоколу IIDK (см. [Руководство программиста SecurOS IIDK](#), не входит в общий комплект документации и предоставляется по запросу) возможно использование формата HTML в теле сообщения.

Родительский объект — *Компьютер\группа Оповещения*.

Рис. 218. Окно настройки параметров объекта Сервис почтовых сообщений

Внимание! Допустимые значения параметров объекта зависят от настроек используемого SMTP-сервера.

Таблица 69. Параметры объекта Сервис почтовых сообщений

Параметр	Описание
SMTP сервер	Укажите IP-адрес или DNS/WINS-имя SMTP-сервера. Можно использовать внутренние или внешние SMTP-серверы или установить службу SMTP-сервера на локальном компьютере (см. Установка и настройка почтового SMTP-сервера). Обязательный параметр.
Порт	Укажите порт SMTP-сервера. Значение по умолчанию — 25.
Требуется аутентификация	Отметьте флажок, если на сервере необходима SMTP-аутентификация. Внимание! Если флажок отмечен, то следующие два параметра настройки активны.
Имя пользователя, Пароль	Укажите системное имя и пароль для SMTP-аутентификации.

Параметр	Описание
Шифрование	Выберите из списка протокол шифрования. Возможные значения: Отключено — шифрование не используется (значение по умолчанию). SSL/TLS — подключение по протоколу SSL/TLS. STARTTLS — подключение по протоколу STARTTLS.
Использовать для двухфакторной аутентификации и сброса пароля	Отметьте флажок, чтобы использовать сервис почтовых сообщений в процедуре двухфакторной аутентификации (см. Двухфакторная аутентификация в SecurOS) или сброса пароля типовых пользователей через e-mail в окне авторизации (см. Смена/сброс пароля типового пользователя). По умолчанию не отмечен. Примечание. Если отмечен, данный <i>Сервис почтовых сообщений</i> будет доступен для выбора в списке сервисов для отправки одноразовых кодов доступа в Правах пользователя и в Закладке Управление паролями для сброса паролей через e-mail. Если отмечен, сообщения будут отправляться с адреса электронной почты, указанного в параметре Отправитель.
Отправитель	Задайте адрес электронной почты отправителя, от имени которого будут отправляться почтовые сообщения с одноразовыми кодами доступа и кодами для сброса пароля. Внимание! Отправитель задается в формате <имя_пользователя>@<домен>. Например, user@organization.com. В противном случае настройка не будет применена. Заданный адрес будет использоваться только для отправки сообщений с одноразовыми кодами доступа или для сброса пароля через e-mail. Для всех прочих сообщений будут использоваться адреса, заданные в собственных параметрах Почтового сообщения. Поле недоступно, если не отмечен флажок Использовать для двухфакторной аутентификации и сброса пароля. Если флажок отмечен, поле обязательно для заполнения. Примечание. Сообщения будут отправляться на адрес электронной почты, который задан в настройках текущего Пользователя SecurOS.

12.1.3 Почтовое сообщение

Объект представляет сообщение электронной почты (или шаблон сообщения). Почтовые сообщения отправляются с помощью *Макрокоманд* и *Скриптов Node.js*.

Родительский объект — [Сервис почтовых сообщений](#).

Рис. 219. Окно настройки параметров объекта Почтовое сообщение

Таблица 70. Параметры объекта Почтовое сообщение

Параметр	Описание
Кому	Задайте электронный адрес получателя. Можно задать несколько адресов, используя в качестве разделителя символ ";". Например: admin@domain.com; security@domain.com.
От кого	Задайте электронный адрес отправителя. Можно задать несколько адресов, используя в качестве разделителя символ ";".
Копия	Задайте электронный адрес получателя копии сообщения. Можно задать несколько адресов, используя в качестве разделителя символ ";".
Тема	Задайте тему сообщения. Можно указать переменные параметры в формате #param_name#. Реальное значение параметра будет автоматически подставлено при отправке сообщения. Параметры используются в скриптах.
Сообщение	Наберите сообщение. Можно указать переменные параметры (как в теме сообщения).

Параметр	Описание
Вложения	Выберите присоединяемые файлы. Формат: строка с названиями файлов, максимальная длина — 250 символов. Можно либо ввести абсолютный путь к файлу, либо указать только имя файла. В последнем случае, система будет искать файл в директории установки продукта. Нажмите кнопку  для выбора одного файла. Чтобы присоединить несколько файлов, укажите путь к ним вручную, используя в качестве разделителя символ "," (например: C:\temp\image.jpg, C:\temp\log.txt).
Архивировать	Необязательное действие: выберите архиватор для упаковки всех присоединенных файлов в архивы. Каждый из файлов, указанный в приложении, будет упакован в свой архив. Возможные значения: нет сжатия, 7Z, GZIP, ZIP.

12.1.4 Сервис коротких сообщений

Объект представляет телефон или подобное устройство, подключенное к компьютеру через последовательный порт (COM-порт) или через USB-порт и используемое для отправки SMS-сообщений.

Родительский объект — *Компьютер\группа Оповещения*.

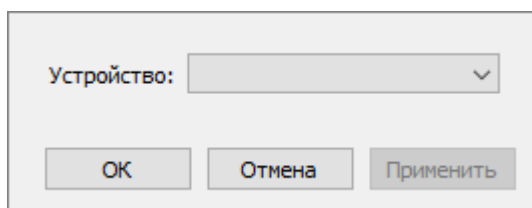


Рис. 220. Окно настройки параметров объекта Сервис коротких сообщений

Таблица 71. Параметры объекта Сервис коротких сообщений

Параметр	Описание
Устройство	Выберите из списка устройство для отправки SMS-сообщений. Для отображения устройства в списке необходимо наличие установленного драйвера от производителя. Совместимы любые устройства, которые могут работать как GSM-модем в PDU-режиме. Экран блокировки устройства должен быть отключен. На устройствах, начиная с Android 10, требуется включить АТ-команды (см. инструкцию устройства). Примечание. Если устройство не поддерживает работу в PDU-режиме, будет использован альтернативный способ отправки коротких сообщений. В таком случае сообщение должно состоять только из латинских букв и иметь длину не более 70 символов.

12.1.5 Короткое сообщение

Объект представляет отдельное SMS-сообщение. Короткие сообщения отправляются с помощью *Макрокоманд* и *Скриптов Node.js*.

Родительский объект — **Сервис коротких сообщений**.

Рис. 221. Окно настройки параметров объекта
Короткое сообщение

Таблица 72. Параметры объекта Короткое сообщение

Параметр	Описание
Телефон	Задайте номер телефона, на который отправляется сообщение. Номер может быть задан в международных стандартах E.163 и E.164.
Сообщение	Наберите сообщение. Можно использовать как символы ASCII-кода (латинские), так и кириллические символы. Максимальная длина сообщения — 70 символов.

12.1.6 Сервис звукового оповещения

Объект представляет звуковую плату, которая воспроизводит звуки, определенные для каждого события. Соответствие звука событию объекта можно посмотреть и при необходимости изменить через утилиту **Редактор регистрационных файлов (DDI)**. Аудиофайлы должны находиться в папке `\wav` корневой директории SecurOS.

Родительский объект — *Компьютер\группа Оповещения*.

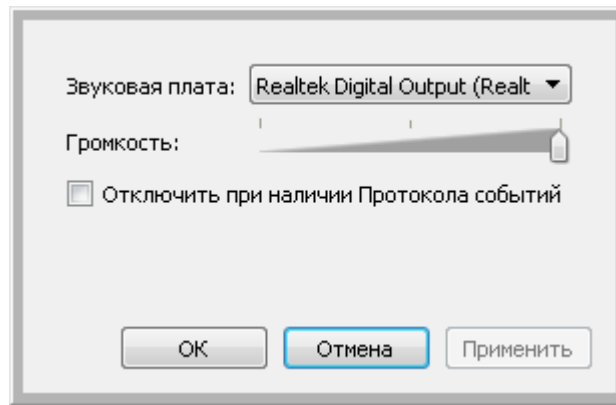


Рис. 222. Окно настройки параметров объекта Сервис звукового оповещения

Таблица 73. Параметры объекта Сервис звукового оповещения

Параметр	Описание
Звуковая плата	Выберите из списка звуковую плату.
Громкость	Передвигая ползунок, установите громкость сигнала звукового оповещения.
Отключить при наличии Протокола событий	Активируйте поле при необходимости отключения звукового оповещения о событиях при наличии <i>Протокола событий</i> . Опция работает при наличии включенного объекта <i>Протокол событий</i> на том же компьютере, где работает объект <i>Сервис звукового оповещения</i> .

12.1.7 Служба реагирования

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

В ОС **Linux** функциональность не поддерживается.

Объект предназначен для отправки в Службу реагирования карточки, в которой содержится информация о происшествии. Подробности настройки SecurOS и описание принципов взаимодействия со Службой реагирования приведены в разделе **Взаимодействие с внешней Службой реагирования**.

Родительский объект — **Компьютер**.

HTTP адрес Службы реагирования:

Настройки подключения

☒ **WebView**
 Сервер: Порт:
 Пользователь:
 Пароль:
 WebView Монитор:

☒ **RTSP-сервер**
 Сервер: Порт:

Камеры

☒ **SecurOS Premium [1]**
☒ **Компьютер S-PROKHOROV [S-PR...**
☒ Камера 1 [1]
☒ **Камера 2 [2]**
☐ Камера 3 [3]
☒ Камера 5 [5]

☐ **Удаленная система: SecurOS Premium [4#1]**
☐ **Удаленная система: Компьютер SERV...**
 Удаленная система: Камера 1 [4#1]
 Удаленная система: Камера 2 [4#2]
 Удаленная система: Камера 5 [4#5]

Физический адрес Камеры

Город:

Район:

Улица:

Тип улицы:

Номер дома:

Подъезд:

Дорога:

Километр дороги:

Типы происшествий

Задайте Типы происшествий

Рис. 223. Окно настройки параметров объекта Служба реагирования

Таблица 74. Параметры объекта Служба реагирования

Параметр	Описание
HTTP адрес Службы реагирования	Задайте http-адрес, на который будет отправляться <i>Карточка происшествия</i> и ссылка на видео.
Настройки подключения (параметры блока используются для формирования ссылок на видео, соответствующее происшествию)	

Параметр	Описание
WebView	Отметьте флажок для формирования ссылки на видео, которое может быть получено с помощью WebView по протоколу http.
Сервер, Порт	Задайте IP-адрес и номер порта сервера WebView, через который будет осуществляться взаимодействие с внешней системой.
Пользователь/Пароль	Введите имя и пароль пользователя, зарегистрированного в SecurOS, для которого настроены права работы с Модулем SecurOS WebView.
WebView Монитор	Выберите из списка объект <i>WebView Монитор</i> , который будет использоваться для отображения видео с <i>Камер</i> .
RTSP-сервер	Отметьте флажок для формирования ссылки на видео, которое может быть получено с помощью RTSP-сервера по протоколу rtsp.
Сервер/Порт	Задайте IP-адрес и номер порта RTSP-сервера, через который будет осуществляться взаимодействие с внешней системой.
Камеры	
Дерево Камер	Выберите <i>Камеры</i>, для которых будет возможно формировать <i>Карточку происшествия</i> и отправлять ее в Службу реагирования. Для выбора отметьте флажок слева от требуемой <i>Камеры</i>. При работе в конфигурации <i>Центра мониторинга</i> (см. Центр Мониторинга и Контроля) в <i>Дереве Камер</i> дополнительно отображаются <i>Камеры Удаленных систем</i>, которые выбраны в настройках объектов <i>Служба реагирования</i> в <i>Удаленных системах</i>.
Физический адрес Камеры	
Город, Район, Улица, Тип улицы, Номер дома, Подъезд, Дорога, Километр дороги	Для задания адреса установки отметьте флажок слева от требуемой камеры. Заполните необходимые поля. Физический адрес места установки камеры будет передан в <i>Карточке происшествия</i>. Примечание. Физические адреса мест установки камер <i>Удаленной системы</i> отображаются в случае, если они заданы в настройках объекта <i>Служба реагирования</i> в <i>Удаленной системе</i>. Такие адреса не могут быть изменены из <i>Центра Мониторинга</i>.
Типы происшествий	
Список типов происшествий	В поле отображается текущий список типов происшествий, который используется при формировании и отправке <i>Карточки происшествия</i>. Внимание! Если список типов происшествий не загружен, отправка <i>Карточки происшествия</i> во внешнюю Службу реагирования будет невозможна.

Параметр	Описание
Загрузить из файла (кнопка)	Нажмите кнопку для загрузки списка происшествий из файла. При успешном или неудачном выполнении операции система выведет соответствующее сообщение (например, см. рис. 224).
Сохранить в файл (кнопка)	Нажмите кнопку для сохранения текущего списка происшествий в файл. При успешном или неудачном выполнении операции система выведет соответствующее сообщение (например, см. рис. 225).

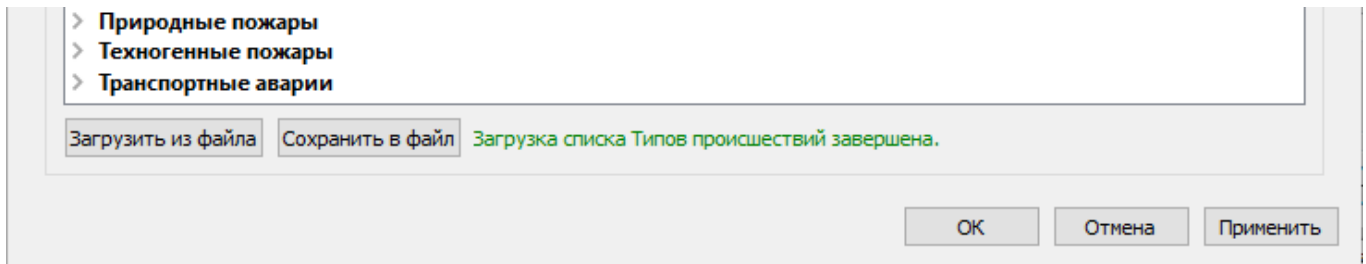


Рис. 224. Сообщение об успешной загрузке файла

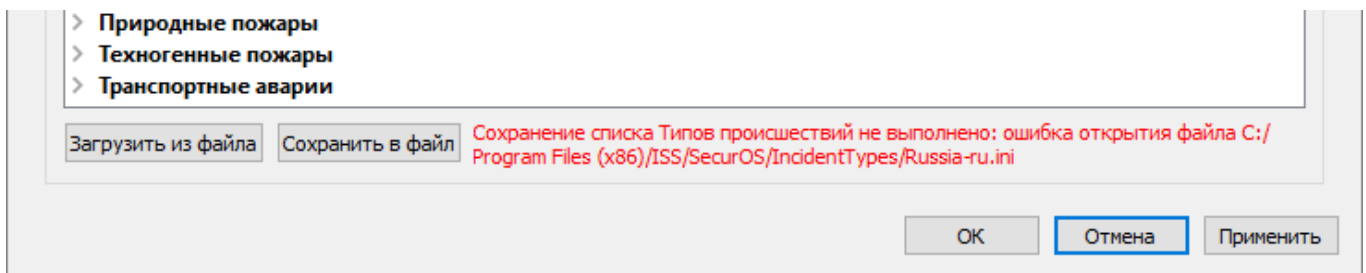


Рис. 225. Сообщение о невозможности записи в файл

12.1.7.1 Список типов происшествий. Формат файла

В соответствии с требованиями служб экстренного реагирования при формировании Карточки происшествия необходимо использовать код и описание происшествия в стандартном формате. Для загрузки таких данных в SecurOS используется файл списка типов происшествий.

Примечание. При установке SecurOS такие файлы автоматически создаются в папке \IncidentTypes корневой директории установки продукта.

Пользовательский список происшествий может быть создан и загружен в систему в виде ini-файла в любой локальной кодировке или кодировке UTF-16 LE с BOM. Формат файла представлен в Листинге 2:

Листинг 2. Формат файла списка типов происшествий

```
[section1]
Name=<Название категории типов происшествий>
<Код происшествия>=<Название Типа происшествия>
<Код происшествия>=<Название Типа происшествия>
...
[section2]
Name=<Название категории Типа происшествий>
```

```
<Код происшествия>=<Название Типа происшествия>  
<Код происшествия>=<Название Типа происшествия>  
...
```

где:

- **[sectionN]** — уникальное название секции. В названии секции допускается использовать только латинские символы и/или цифры.
- **Name=<Название категории типов происшествий>** — уникальное название категории происшествий. В названии категории допускается использовать символы в любой кодировке. Длина строки: [1; 255] символов.

Внимание! Перенос строки названия категории типа происшествия запрещен.

- **<Код происшествия>** — уникальный код происшествия. В коде допускается использовать только латинские символы и/или цифры. Длина строки: [1; 16] символов.
- **<Название Типа происшествия>** — название типа происшествия. Допускается использовать символы в любой кодировке. Длина строки: [1; 255] символов.

Внимание! Перенос строки названия типа происшествия запрещен.

Пример файла с типами происшествий представлен в Листинге 3.

Листинг 3. Пример файла со списком типов происшествий

```
[S1]  
Name=Техногенные пожары  
S101=пожары в зданиях, на коммуникациях и пр.  
S102=пожары на транспорте  
S103=пожары в метрополитене  
S104=пожары в зданиях и сооружениях жилого и прочего назначения  
S100=иные техногенные пожары  
  
[S2]  
Name=Природные пожары  
S201=лесные пожары  
S202=пожары степных и хлебных массивов  
S200=иные природные пожары  
  
[S3]  
Name=Дорожно-транспортные происшествия  
S301=столкновение ТС  
S302=опрокидывание ТС  
S303=наезд на стоящее ТС  
S304=наезд на пешехода  
S305=наезд на велосипедиста  
S306=наезд на препятствие  
S307=наезд на животных  
S300=иные ДТП  
  
. . . .  
  
[S7]  
Name=Геологические / гидрологические опасные явления
```

```
S701=обвалы, осыпи
S702=просадка (провал) земной поверхности, дороги
S703=высокие уровни воды / наводнения
S700=иные геологически / гидрологические опасные явления

[S8]
Name=Иные происшествия
S801=скопление людей
S802=праздношатание
S803=вандализм
S804=драка, нападение
S805=проход в запрещенную зону / пересечение периметра
S806=оставленные предметы
S807=обнаружение автомобиля из черного списка или находящегося в розыске
S808=обнаружение человека из черного списка или находящегося в розыске
S809=необходима медицинская помощь
S800=иные происшествия
```

12.1.8 Интеграция с SIP-устройствами

В ОС **Linux** функциональность не поддерживается.

SecurOS позволяет интегрировать в свою конфигурацию устройства, работающие по *протоколу установления сеанса (SIP)*, такие как колонны экстренного вызова и их аналоги. Операторы SecurOS имеют двухстороннюю связь с такими устройствами и средства для наблюдения за местами расположения этих устройств, чтобы оперативно реагировать на инциденты.

Для обеспечения работы SecurOS с SIP-устройствами, создайте и настройте следующие объекты:

- **Подсистема SIP;**
- **SIP-устройство;**
- **SIP: Интерфейс оператора.**

12.1.8.1 Подсистема SIP

Объект позволяет указать контакт для входящих звонков, настроить взаимодействие с автоматической телефонной станцией (АТС) и сетевые параметры. *Подсистема SIP* также является родительским объектом для всех *SIP-устройств* (см. **SIP-устройство**), связанных с сервером, где она создана.

Родительский объект — **Компьютер**.

Рис. 226. Окно настройки параметров объекта
Подсистема SIP

Таблица 75. Параметры объекта Подсистема SIP

Параметр	Описание
Контакт	Контакт, который будут использовать дочерние <i>SIP-устройства</i> для установления связи с операторами. В зависимости от конфигурации, в качестве контакта может выступать IP-адрес сервера SecurOS, на котором создан объект, или уникальный идентификатор, определяемый настройками АТС. Максимальная длина 256 символов. Примечание. При использовании АТС формат контакта определяется ее настройками и другими требованиями текущей конфигурации.
Работать с АТС	Установите этот флаг, если ваша конфигурация предусматривает использование АТС для осуществления связи с <i>SIP-устройствами</i> . Если флаг установлен, становятся доступны настройки АТС.
IP-адрес	IP-адрес для подключения к АТС или серверу, на котором находится программная АТС.
Порт	Сетевой порт для подключения к АТС. Значение по умолчанию: 5060.
Пользователь	Логин пользователя, от имени которого родительский <i>Компьютер</i> данной Подсистемы SIP будет подключаться к АТС.
Пароль	Пароль пользователя.
Сетевые порты	
Порт TCP	Сетевой порт для установления TCP-соединений. Значение по умолчанию: 5060.

Параметр	Описание
Порт UDP	Сетевой порт для установления UDP-соединений. Значение по умолчанию: 5060.
	Примечание. Каждый активный разговор требует открыть два UDP-порта, начиная с заданного значения. Учитывайте это при настройке брандмауэра. Например, чтобы поддерживать 10 активных разговоров одновременно, потребуются UDP-порты с 5060 до 5079.

12.1.8.2 SIP-устройство

Внимание! Раздел описывает только настройку объекта SecurOS. За инструкцией по настройке оборудования вы можете обратиться к его производителю.

Объект представляет устройство, работающее по протоколу SIP, с которого будут поступать звонки, и на которое оператор сможет совершать вызовы. Для работы с созданными *SIP-устройствами* используется окно **SIP: Интерфейс оператора**. Возможности по взаимодействию с ними определяются правами пользователя (см. **Доступ к SIP-устройствам**). Кроме этого, *SIP-устройством* можно управлять из окна **Карта: Интерфейс оператора** (если *SIP-устройство* размещено на **Карте** и настроен **SIP: Интерфейс оператора**), или с помощью контекстного меню ячейки **Камеры Медиа Клиента** (если с *SIP-устройством* связана хотя бы одна **Камера**).

Родительский объект — **Подсистема SIP**.

Рис. 227. Окно настройки параметров объекта SIP-устройство

Таблица 76. Параметры объекта SIP-устройство

Параметр	Описание
Контакт	Контакт, который будет использован для установления связи с этим <i>SIP-устройством</i>. В зависимости от конфигурации, в качестве контакта может выступать IP-адрес <i>SIP-устройства</i> или уникальный идентификатор, определяемый настройками АТС. Максимальная длина 256 символов. Примечание. При использовании АТС формат контакта определяется ее настройками и другими требованиями текущей конфигурации.
Камеры	
Фильтр	Для поиска <i>Камеры</i> по части имени или идентификатора, введите в поле требуемые символы; в дереве автоматически отобразятся только те <i>Камеры</i> , имя или идентификатор которых соответствуют заданным условиям поиска. Для того, чтобы очистить поле, нажмите кнопку Сбросить фильтр .
Список камер (таблица)	
Название	Отметьте флажок слева от <i>Камеры</i> , чтобы связать с ней данное <i>SIP-устройство</i> . Это позволит быстро показать нужные камеры в <i>Медиа Клиенте</i> во время разговора, а также совершать вызовы на это устройство из ячейки <i>Камеры</i> .
Препопозиция	Укажите идентификатор препопозиции, в которой данное <i>SIP-устройство</i> находится в поле зрения поворотной <i>Камеры</i>. Примечание. Идентификатор препопозиции можно посмотреть в <i>Медиа Клиенте</i> на панели PTZ, выбрав нужную <i>Камеру</i> (см. Краткое руководство пользователя SecurOS). <i>Камера</i> будет переходить в указанную препопозицию при поступлении звонков с этого <i>SIP-устройства</i>, исходящих вызовах на него или вручную при помощи кнопки Перейти к камерам в окне <i>SIP: Интерфейс оператора</i>.
Основная камера	<i>Камера</i> , которая является основной (имеет лучший обзор) для данного <i>SIP-устройства</i> . Основная <i>Камера</i> всегда выводится в верхнем левом углу <i>Медиа Клиента</i> при совершении звонков.
Описание	Краткое описание данного <i>SIP-устройства</i> (например, местонахождение). Описание выводится в окне <i>SIP: Интерфейс оператора</i> при выборе этого устройства в списке.

Доступ к SIP-устройствам

Доступ к *SIP-устройствам* регулируется *Правами пользователя* (см. **Права пользователя**). Возможны следующие уровни доступа:

- **Доступ запрещен** (✗). Оператор не видит устройство в окне *SIP: Интерфейс оператора* и не получает звонков от него.
- **Просмотр** (👁). Оператор видит устройство в окне *SIP: Интерфейс оператора* и может принимать звонки от него. Исходящие вызовы недоступны.

- *Управление* (🖱️) и выше. Оператор видит устройство в окне *SIP: Интерфейс оператора* и может принимать звонки от него. Он также может совершать исходящие вызовы.

12.1.8.3 SIP: Интерфейс оператора

Объект представляет графический интерфейс для принятия звонков от *SIP-устройств* и совершения вызовов на них.

Родительский объект — **Рабочий стол**.

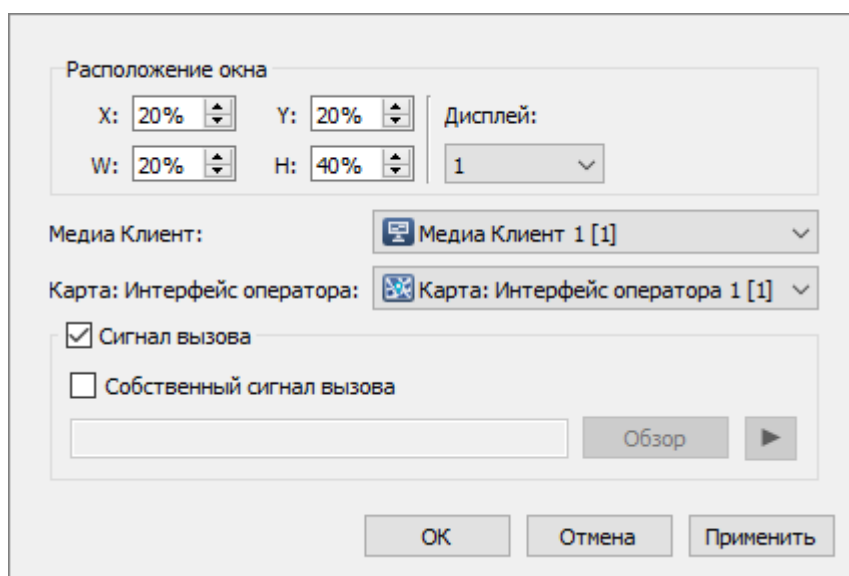


Рис. 228. Окно настройки параметров объекта SIP: Интерфейс оператора

Таблица 77. Параметры объекта SIP: Интерфейс оператора

Параметр	Описание
X, Y, W, H	Задайте координаты верхнего левого угла (X , Y) относительно верхнего левого угла дисплея, ширину и высоту (W , H) окна <i>SIP: Интерфейс оператора</i> (в процентах от размеров экрана).
Дисплей	Выберите идентификатор физического монитора, на котором будет отображаться данный объект.
Медиа Клиент	Выберите <i>Медиа Клиент</i> , с которым будет взаимодействовать окно <i>SIP: Интерфейс оператора</i> . Этот <i>Медиа Клиент</i> будет использован, чтобы отобразить <i>Камеры</i> , связанные с интересующим оператора <i>SIP-устройством</i> .

Параметр	Описание
Карта: Интерфейс оператора	Выберите окно <i>Карта: Интерфейс оператора</i>, с которым будет взаимодействовать окно <i>SIP: Интерфейс оператора</i>. Внимание! Выбранное окно <i>Карта: Интерфейс оператора</i> должно находиться на том же <i>Рабочем столе</i>, что и окно <i>SIP: Интерфейс оператора</i>. Если окно <i>Карта: Интерфейс оператора</i> выбрано: • оператор SecurOS сможет звонить на <i>SIP-устройство</i> из окна <i>Карта: Интерфейс оператора</i>; • оператор SecurOS сможет переходить из окна <i>Карта: Интерфейс оператора</i> на <i>Медиа Клиент</i> для просмотра видео с <i>Камер</i>, связанных с <i>SIP-устройством</i>; • при любом взаимодействии с <i>SIP-устройством</i> из окна <i>SIP: Интерфейс оператора</i>, карта будет автоматически отцентрирована относительно данного <i>SIP-устройства</i> (если это возможно). Подробнее см. Краткое руководство пользователя SecurOS.
Сигнал вызова	Установите этот флаг, чтобы при поступлении входящего вызова воспроизводился звуковой сигнал.
Собственный сигнал вызова	Установите этот флаг, чтобы выбрать собственный сигнал входящего вызова.
Имя файла и кнопка Обзор	Кнопка Обзор позволяет выбрать аудиофайл, который будет использоваться в качестве сигнала входящего вызова. Действуют следующие ограничения: • Поддерживаемые расширения файлов: mp3, wav. • Максимальный размер файла: 1 МВ. После выбора файла его имя будет отображаться в поле слева от кнопки.
Кнопка Воспроизвести	Позволяет прослушать выбранный сигнал вызова.

13 Подсистема автоматизации

Подсистема автоматизации предоставляет средства для фильтрации и обработки действий и событий в сети SecurOS, создавая таким образом логику целой сети безопасности.

13.1 Описание объектов

Подсистема автоматизации представлена следующими объектами:

- **Расписание.**
- **Макрокоманда.**
- **Скрипт Node.js.**
- **Интерфейс IIDK.**
- **HTTP Event Gate.**
- **REST API.**

13.1.1 Расписание

Объект *Расписание* позволяет настроить расписание для срабатывания *Макрокоманд* и *Скриптов Node.js*. Для каждого *Расписания* укажите временные интервалы, дни недели, отдельные даты и периоды, в течение которых будут использоваться правила, определенные макрокомандами. В эти дни будут действовать правила *Расписания*.

Пример. Если в *Расписании* указан временной интервал с 08:00:00 до 22:00:00 и дни недели Понедельник и Среда, то правила будут действовать с 08:00:00 до 22:00:00 по понедельникам и средам.

Родительский объект — *Объект охраны\группа Расписания*.

Рис. 229. Окно настройки параметров объекта Расписание

Таблица 78. Параметры объекта Расписание

Параметр	Описание
Список временных интервалов (располагается в левой части окна)	
Временные интервалы	Нумерованный список заданных временных интервалов и периодов их действия. Чтобы отредактировать параметры заданного временного интервала, щелкните требуемый интервал мышью, в блоке настройки задайте новые значения параметров.
Добавить (кнопка)	Нажмите кнопку чтобы добавить в список новый временной интервал.
Удалить (кнопка)	Нажмите кнопку чтобы удалить из списка выбранный временной интервал.
Блок настройки временного интервала (располагается в правой части окна)	

Параметр	Описание
От, До	В полях От и До задайте время начала и окончания интервала. При задании значений допускается ситуация, когда начало временного интервала (От) больше его окончания (До). В этом случае в системе фактически создается два временных интервала, действующих в течение одних суток: • от 00:00:00 до времени окончания (До); • от времени начала (От) до 23:59:59. Примечание. Дни или периоды действия такого интервала задаются по общим правилам (см. ниже). Например, если задан интервал 15:00:00 – 11:00:00 и день недели Понедельник, то такой интервал будет действовать от 00:00:00 до 11:00:00 и от 15:00:00 до 23:59:59 каждого понедельника. Если необходимо задать непрерывный временной период, начало которого приходится на одни сутки, а окончание - на следующие, то в этом случае необходимо задать 2 временных интервала, первый из которых заканчивается, а второй начинается в полночь. Например, требуется задать интервал, непрерывно действующий с 18:00:00 вечера понедельника до 02:00:00 утра вторника. В этом случае следует задать следующие временные интервалы: • от 18:00:00 до 23:59:59 с периодом действия Пн; • от 00:00:00 до 02:00:00 с периодом действия Вт.
Действие временного интервала	
По дням недели	Выберите данную опцию, чтобы задать область действия временного интервала в привязке к дням недели и/или праздничным дням: • Отметьте флажки, соответствующие Дням недели, для которых будет действовать временной интервал; • При необходимости, для срабатывания временного интервала в праздничные дни, отметьте флажок Праздничные дни. Примечание. Список Праздничных дней задается в настройках Объекта охраны.

Параметр	Описание
Дата, с повторением	Выберите данную опцию, чтобы задать область действия временного интервала в привязке к календарным датам: - В поле Дата выберите календарную дату действия временного интервала. - При необходимости повторного срабатывания временного интервала отметьте флажок Повторять каждые. Задайте промежуток срабатывания (в днях) от заданной даты.

13.1.2 Макрокоманда

Объект используется для определения поведения системы SecurOS посредством установления связи события одного объекта и реакции другого объекта на это событие.

При наступлении события, описанного в макрокоманде, в системе автоматически выполняется предопределенное в команде действие или набор действий. Макрокоманда также может быть запущена оператором в ручном режиме. Каждый объект системы имеет свои события, список которых определяется его свойствами.

Отображение и возможность использования макрокоманд регулируется *Правами пользователя* (см. [Права пользователя](#)). Возможны следующие уровни доступа:

- Доступ запрещен (✗). Макрокоманды не отображаются в панели управления и меню *Камер* в *Медиа Клиенте*.
- Просмотр (👁) и выше. Макрокоманды отображаются в панели управления и меню *Камер* в *Медиа Клиенте* и их можно использовать.

Дополнительную информацию по настройке макрокоманд см. в разделе [Настройка макрокоманд](#).

Родительский объект — *Объект охраны\группа Макрокоманды*.

Действия:  ☐ Выполнять локально

Тип	Идентификатор	Название	Действие	Параметры
Камера	2	Камера 2	Поставить на о...	

Автоматический запуск действий по событиям:

Тип	Идентификатор	Название	Событие
Камера	2	Камера 2	Тревога

Ручной запуск действий:

☐ Скрыть кнопку запуска Макрокоманды на Панели управления

Отображать Макрокоманду в Медиа Клиенте в меню выбранных Камер:

Фильтровать по имени или ID

☒ SecurOS [1]

- ☒ Компьютер
 - ☐ Камера 1 [1]
 - ☒ Камера 2 [2]
 - ☐ Камера 3 [3]
 - ☐ Камера 4 [4]

Иконка:  Позиция в меню: 2 Выбрано Камер: 1

Рис. 230. Окно настройки параметров объекта Макрокоманда

Таблица 79. Параметры объекта Макрокоманда

Параметр	Описание
Выполнять локально	Активация данного поля запретит пересылку события MACRO (X) RUN на другие компьютеры сети. Таким образом, если макрокоманда запускается в ручном режиме, то результат ее действий не может затронуть другие компьютеры сети. В случае, если макрокоманда запускается каким-либо событием, то макрокоманда будет выполнена локально на всех компьютерах сети, получивших данное событие. Если макрокоманда запущена системой при старте, то система обрабатывает ее также как и при ручном запуске макрокоманды, т. е. локально, на том компьютере, который был запущен. Если поле деактивировано, то макрокоманда будет выполняться на всех компьютерах сети.
Действия (какие действия необходимо выполнить при наступлении события или по команде оператора)	

Параметр	Описание
Тип	Выберите тип объекта.
Идентификатор	Выберите идентификатор объекта. Значение Все эквивалентно выбору всех объектов данного типа.
Название	<i>Информационное поле:</i> название объекта (появляется автоматически после выбора типа объекта и его номера).
Действие	Выберите команду, которую должен выполнить объект. Список действий зависит от типа объекта. Внимание! Выбрать два одинаковых Действия для одного и того же объекта невозможно даже в том случае, если эти Действия имеют различный набор Параметров. При необходимости отправить несколько одинаковых команд одному и тому же объекту создайте несколько объектов <i>Макрокоманда</i>.
Параметры	Параметры выполнения действия. Задаются в виде строки, максимальная длина — 255 символов. Формат строки: param1<value1>,param2<value2>. Например, file<\wav\sound1.wav>, color<green>.
Автоматический запуск действий по событиям (макрокоманда выполняется при возникновении любого из перечисленных событий)	
Тип	Выберите тип объекта-источника.
Идентификатор	Выберите идентификатор объекта-источника. Значение Все эквивалентно выбору всех объектов данного типа.
Название	<i>Информационное поле:</i> название объекта (появляется автоматически после выбора типа объекта и его номера).
Событие	Выберите событие объекта-источника. Список событий зависит от типа объекта.
Ручной запуск действий (позволяет оператору выполнять макрокоманды из <i>Медиа Клиента</i>)	
Скрыть кнопку запуска Макрокоманды на Панели управления	Отметьте флажок, чтобы кнопка запуска <i>Макрокоманды</i> не отображалась на <i>Панели управления</i> .
Отображать Макрокоманду в Медиа Клиенте в меню выбранных Камер	Выберите <i>Камеры</i> , через контекстное меню которых можно будет вызвать <i>Макрокоманду</i> в <i>Медиа Клиенте</i> . Если нужно, чтобы <i>Макрокоманда</i> была доступна только в некоторых <i>Медиа Клиентах</i> , скройте <i>Макрокоманду</i> с помощью параметра Скрывать Макрокоманды в меню Камер на закладке Дополнительные в настройках конкретного <i>Медиа Клиента</i> (см. Закладка Дополнительные).

Параметр	Описание
Иконка	Выберите иконку для <i>Макрокоманды</i> из выпадающего списка. Помимо стандартных иконок в список можно добавить пользовательские иконки. Пользовательские иконки необходимо положить на <i>Сервер конфигураций</i>, после чего они будут автоматически перенесены на все компьютеры конфигурации (см. Синхронизация файлов SecurOS). Для этого создайте папку custom в папке со стандартными иконками <директория установки SecurOS>\skins\macro_icons и сохраните иконку в ней. Иконка должна соответствовать следующим требованиям: • формат изображения: PNG; • размер: 16x16 пк; • имя файла оканчивается на: – _dark_0.png (темная иконка для параметра Иконки в окне настроек параметров <i>Макрокоманд</i>. Рекомендуется внутренний отступ 2 пк от каждого края изображения); – _light_0.png (светлая иконка для контекстного меню <i>Медиа Клиента</i>); – _dark_1.png (темная иконка для <i>Панели управления</i>).
Позиция в меню	Выберите позицию, которую <i>Макрокоманда</i> будет занимать в контекстном меню <i>Камеры</i>.

13.1.3 Скрипт Node.js

Данный объект представляет собой среду для разработки и отладки сценариев Node.js в ОС Windows и Linux. Позволяет обрабатывать *События*, управлять *Объектами SecurOS*, вести журнал выполнения скрипта и т.д. Подробнее о работе с Модулем см. [Руководство программиста SecurOS](#).

Родительский объект — *Компьютер\группа Интеграция и Автоматизация\Скрипты Node.js*.

Внешний вид окна представлен на рис. [231](#).

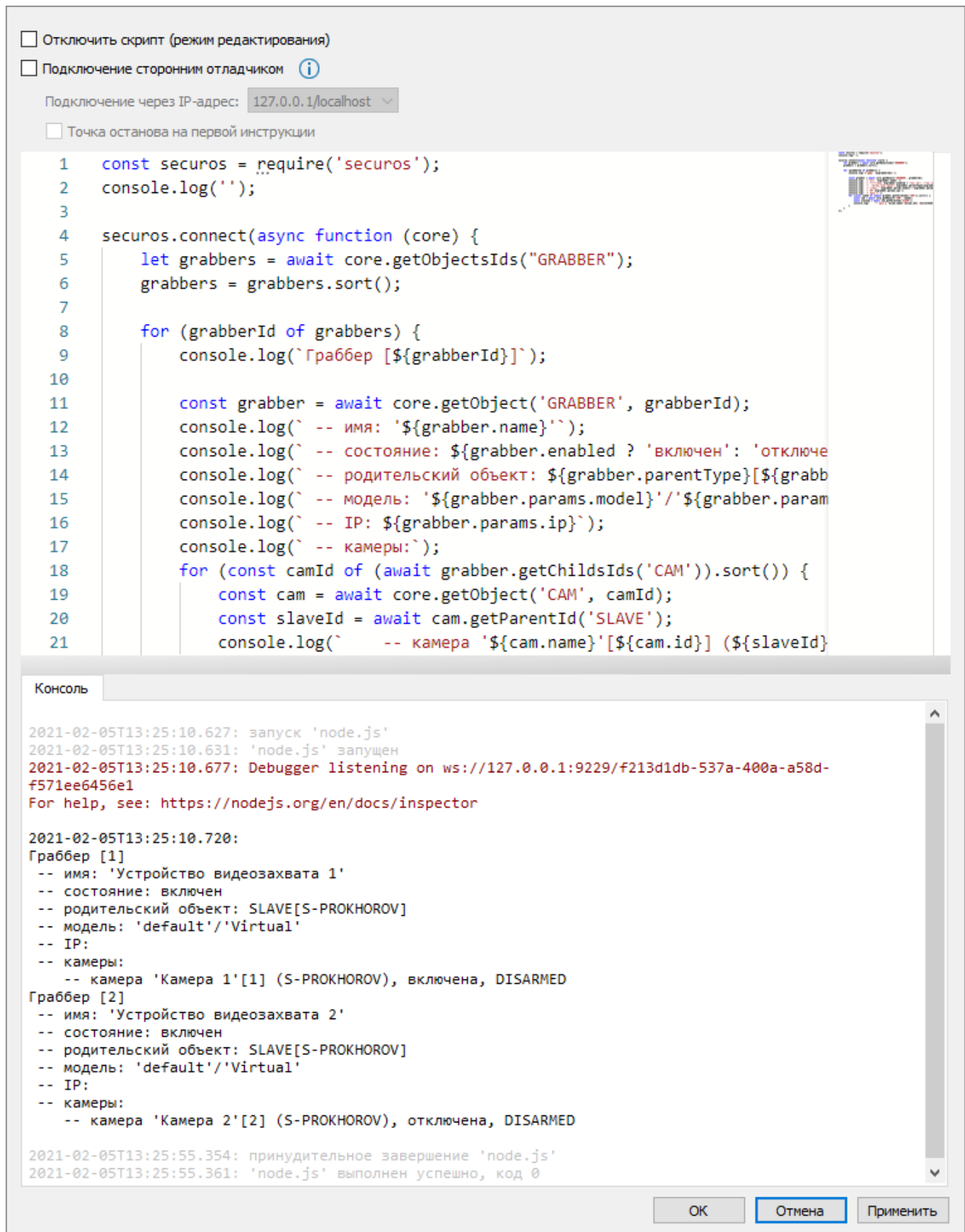


Рис. 231. Окно настройки параметров объекта Скрипт Node.js

Для создания и настройки объекта *Скрипт Node.js* выполните следующие действия:

1. В дереве объектов SecurOS выберите или создайте объект *Скрипты Node.js*, для которого создайте дочерний объект *Скрипт Node.js*.

- В окне **Параметры создаваемого объекта** (здесь и далее не приводится) задайте требуемые значения.
- В окне настройки объекта задайте значения параметров (см. ниже).

Таблица 80. Параметры объекта Node.js Script

Параметр	Описание
Отключить скрипт (режим редактирования)	Флаг включения режима редактирования скрипта. В данном режиме скрипт выполняться не будет. По умолчанию не отмечен.
Подключение сторонним отладчиком	Флаг возможности подключения произвольного внешнего отладчика. По умолчанию не отмечен. Параметр недоступен в следующих случаях: - если отмечен флаг Отключить скрипт (режим редактирования); - не удалось получить список IP-адресов для подключения (см. параметр Подключение через IP-адрес).
Подключение через IP-адрес	Содержит список внешних IP-адресов того сервера, на котором расположен тестируемый скрипт (объект <i>Скрипт Node.js</i>). Для подключения внешним отладчиком возможно использовать любой из IP-адресов списка. Если в списке выбрано какое-либо значение, это же значение необходимо указать в настройках отладчика при его запуске. Примечание. Если выбрано значение <code>localhost</code>, подключение внешним отладчиком возможно только с того <i>Компьютера</i>, где создан скрипт. Параметр недоступен, если выполняется хотя бы одно из следующих условий: - отмечен флаг Отключить скрипт (режим редактирования); - не отмечен флаг Подключение сторонним отладчиком; - не удалось получить список IP-адресов для подключения (например, при отсутствии соединения).
Точка останова на первой инструкции	Флаг ожидания подключения отладчиком. Доступен в случае, если отмечен флаг Подключение сторонним отладчиком . Если не отмечен, скрипт будет выполняться непрерывно.
Окно сценария	Текстовое поле, содержащее код скрипта. Подробнее см. Руководство программиста SecurOS .
Окно результата выполнения сценария (Консоль)	Содержит данные стандартных потоков <code>stdout</code> и <code>stderr</code> , соответствующие примененному, а не отредактированному скрипту. Результат работы скрипта или детальное сообщение об ошибке будут выводиться в окне при работе скрипта.

4. Создайте сценарий.
5. Проверьте синтаксис созданного сценария.
6. Для сохранения и контрольного запуска созданного сценария нажмите кнопку **Применить**.

13.1.4 Интерфейс IIDK

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

SecurOS поддерживает обмен данными с другими компьютерами. Обмен данными происходит посредством специального протокола IIDK (ISS Integration Development Kit). С его помощью другой компьютер может быть подключен к сети SecurOS для передачи событий сети и управления объектами SecurOS.

Объект *Интерфейс IIDK* представляет собой сервис для внешнего соединения с SecurOS по протоколу IIDK. Создайте этот объект на одном или нескольких компьютерах, выполняющих роль IIDK сервера (см. **Руководство программиста SecurOS IIDK**).

Примечание. Руководство программиста SecurOS IIDK не входит в общий комплект документации и предоставляется по запросу.

Права пользователя при подключении к SecurOS по интерфейсу IIDK игнорируются.

Родительский объект — *Компьютер\группа Интеграция и Автоматизация*.

Компьютеры, с которых разрешено подключение к сети:

☐ Локальный компьютер

☒ Компьютеры со следующими IP-адресами: ⓘ

172.16.1.93
172.16.1.110 - 172.16.11.150

+

-

ОК Отмена Применить

Рис. 232. Параметры объекта Интерфейс IIDK

Таблица 81. Параметры объекта Интерфейс IIDK

Параметр	Описание
Компьютеры, с которых разрешено подключение к сети	Выберите один из вариантов, который определит, какие компьютеры могут подключаться к данному IIDK серверу: • Локальный компьютер. Возможно только локальное подключение. • Компьютеры со следующими IP-адресами. Могут подключаться компьютеры, IP-адреса которых указаны в списке ниже.
Список IP-адресов	Укажите IP-адреса компьютеров, которые могут подключаться к данному IIDK серверу. IP-адреса могут быть указаны в стандарте IPv4 или IPv6. Допустимо указание диапазонов адресов через тире (например, 172.16.1.110 – 172.16.1.150).

13.1.5 HTTP Event Gate

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

В ОС **Linux** функциональность не поддерживается.

Объект предназначен для передачи в SecurOS данных, отправляемых внешней системой посредством GET/POST-запросов HTTP.

Родительский объект — *Компьютер\группа Интеграция и Автоматизация*.

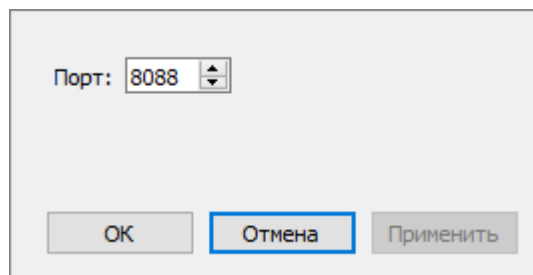


Рис. 233. Окно настройки параметров объекта HTTP Event Gate

Таблица 82. Параметры объекта HTTP Event Gate

Параметр	Описание
Порт	Номер порта HTTP-сервера SecurOS, на который поступают запросы от внешней системы.

Для передачи данных в SecurOS внешняя система должна отправить запрос на указанный номер порта HTTP-сервера.

За более подробной информацией об использовании *HTTP Event Gate* обращайтесь к вашему региональному представителю Intelligent Security Systems.

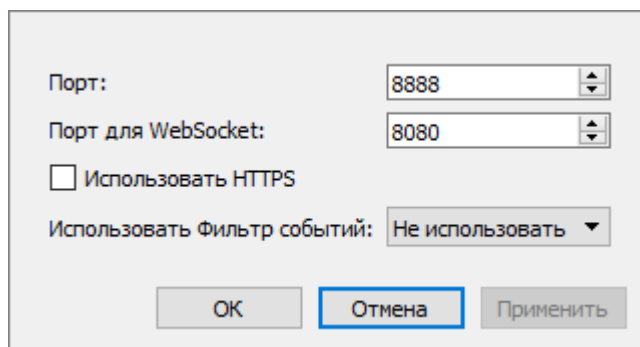
13.1.6 REST API

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

Объект реализует программный интерфейс взаимодействия SecurOS с внешними системами по протоколам HTTP/HTTPS или WebSocket. При помощи интерфейса можно:

1. Частично конфигурировать SecurOS.
2. Получать информацию об объектах SecurOS, SecurOS FaceX и их состояниях.
3. Подписываться на оповещения о событиях и изменении состояний объектов SecurOS.
4. Фильтровать события, пересылаемые из SecurOS во внешнюю систему.
5. Управлять записью на *Камере*.
6. Получать фрагменты видеоархива и отдельные кадры.
7. Получать из *Протокола событий* список зарегистрированных событий объекта *Камера*.
8. Создавать, редактировать параметры и удалять *Пользователей* SecurOS.
9. Управлять телеметрией.
10. Получать *Карты*, сконфигурированные в SecurOS.
11. Запускать *Макрокоманды*.

Родительский объект — *Компьютер\группа Интеграция и Автоматизация*.



Порт: 8888

Порт для WebSocket: 8080

☐ Использовать HTTPS

Использовать Фильтр событий: Не использовать

ОК Отмена Применить

Рис. 234. Параметры объекта REST API

Таблица 83. Параметры объекта REST API

Параметр	Описание
Порт	Номер порта SecurOS для взаимодействия с внешней системой по протоколу HTTP/HTTPS. Диапазон возможных значений: [1; 65535]. По умолчанию принимает значение 8888.
Порт WebSocket для	Номер порта SecurOS для взаимодействия с внешней системой по протоколу WebSocket. Диапазон возможных значений: [1; 65535]. По умолчанию принимает значение 8080.
Использовать HTTPS	Отметьте флажок, если необходимо взаимодействовать с SecurOS по протоколу HTTPS.
Использовать Фильтр событий	Выберите из списка один из существующих в системе <i>Фильтров событий</i> для фильтрации событий, пересылаемых из SecurOS во внешнюю систему.

Детальная информация о порядке настройки системы и использовании *REST API* приведена в документе **Руководство программиста REST API**.

Примечание. Руководство программиста REST API не входит в общий комплект документации и предоставляется по запросу.

13.2 Настройка макрокоманд и скриптов

Данный раздел содержит описание особенностей операций настройки и использования *Макрокоманд* и *Скриптов Node.js*.

13.2.1 Настройка макрокоманд

Макрокоманды используются для определения связей между событиями и реакциями системы на такие события.

Примечания:

1. Описание объекта *Макрокоманда* см. в разделе **Макрокоманда**.
 2. Детальное описание макрокоманд приведено в документе **Руководство программиста SecurOS**.
-

Для настройки *Макрокоманды* выполните следующие действия:

1. В *Дереве объектов SecurOS* в группе *Макрокоманды*, дочерней *Объекту охраны*, создайте объект *Макрокоманда*.
2. В окне **Параметры создаваемого объекта** задайте требуемые значения.
3. В окне настройки параметров объекта (см. рис. 235) создайте описание макрокоманды.

Действия:  ☐ Выполнять локально

Тип	Идентификатор	Название	Действие	Параметры
Камера	2	Камера 2	Поставить на о...	

Автоматический запуск действий по событиям:

Тип	Идентификатор	Название	Событие
Камера	2	Камера 2	Тревога

Ручной запуск действий:

☐ Скрыть кнопку запуска Макрокоманды на Панели управления

Отображать Макрокоманду в Медиа Клиенте в меню выбранных Камер:

Фильтровать по имени или ID

☒ SecurOS [1]

- ☒ Компьютер
 - ☐ Камера 1 [1]
 - ☒ Камера 2 [2]
 - ☐ Камера 3 [3]
 - ☐ Камера 4 [4]

Иконка:  ▼ Позиция в меню: 2 ▼ Выбрано Камер: 1

Рис. 235. Окно настройки параметров объекта

4. Примените новые настройки.

Доступные к запуску *Макрокоманды* выводятся на *Панель управления* (см. рис. 236).



Рис. 236. Панель управления. Доступные Макрокоманды

13.2.2 Настройка скриптов Node.js

Скрипты Node.js используются для более гибкого, по сравнению с *Макрокомандами*, описания логики обработки событий и соответствующей реакции системы.

Примечание. Детальное описание скриптов Node.js приведено в документе [Руководство программиста SecurOS](#).

Для создания *Скрипта Node.js* выполните следующие действия:

1. В *Дереве объектов SecurOS* выберите объект *Компьютер*, в дочерней группе *Интеграция и Автоматизация* создайте дочернюю группу *Скрипты Node.js*.
2. В группе *Скрипты Node.js* создайте объект *Скрипт Node.js*.
3. В окне **Параметры создаваемого объекта** задайте необходимые значения.
4. В окне настройки параметров объекта *Скрипт Node.js* создайте программный код.
5. Проверьте синтаксис программного кода, исправьте обнаруженные ошибки.
6. Примените новые настройки.

14 Компьютерное зрение

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

Подсистема компьютерного зрения SecurOS позволяет привлекать внимание оператора к потенциально опасным ситуациям, таким как пересечение человеком или автомобилем границы запрещенной области, подозрительное поведение человека вблизи припаркованных автомобилей, скопление людей около охраняемых объектов или административных зданий и т.д.

В SecurOS подсистема представлена объектом *Компьютерное зрение*, в состав которого входят как плагины со встроенными видеоаналитическими детекторами, так и независимые видеоаналитические детекторы.

Родительский объект — **Компьютер**.

Примечание. Создание нескольких объектов типа *Компьютерное зрение* с различным набором видеоаналитических детекторов может быть целесообразным при необходимости оптимизировать производительность мультипроцессорных систем с NUMA-архитектурой (см. [Оптимизация производительности NUMA-систем](#)).

Внешний вид окна представлен на рис. 237.

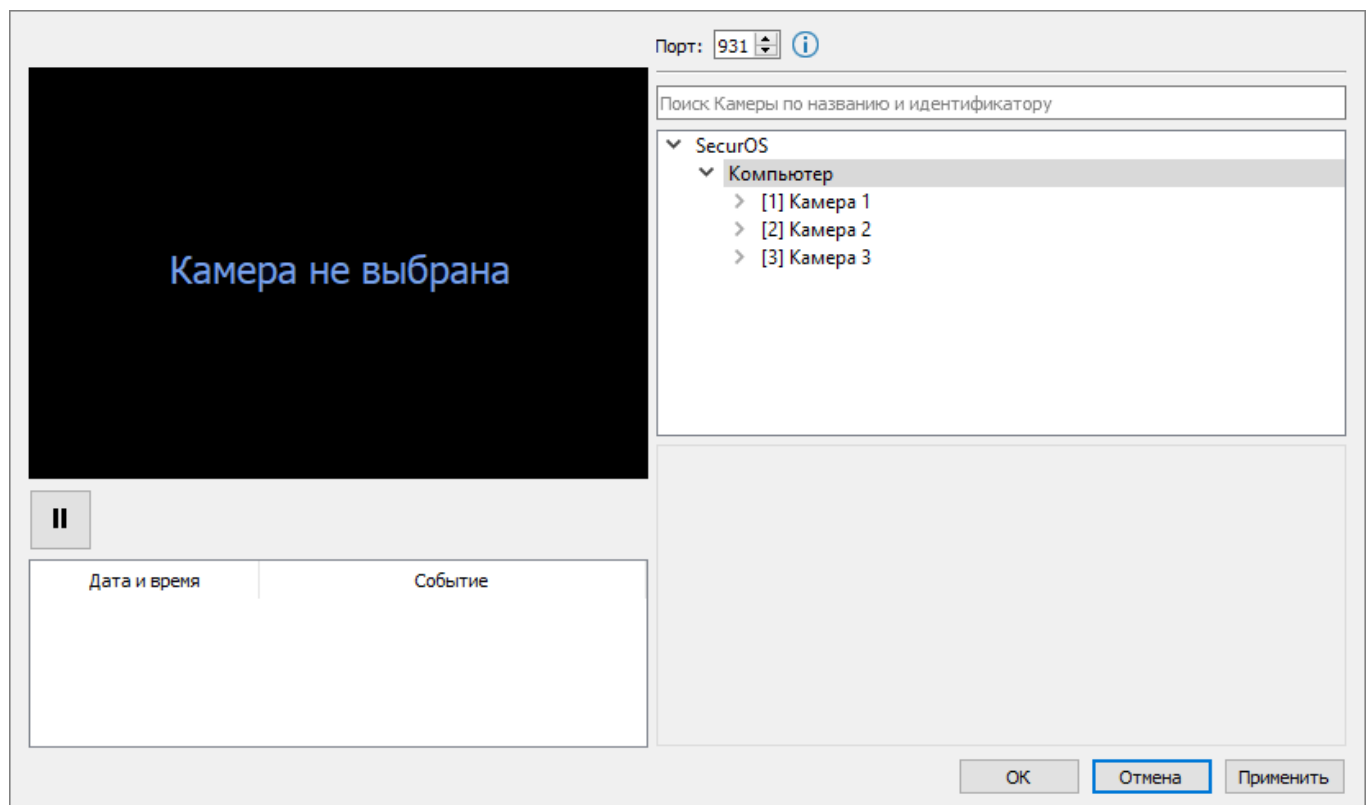


Рис. 237. Окно настройки объекта Компьютерное зрение

Таблица 84. Параметры объекта Компьютерное зрение

Параметр	Описание
Порт	Номер порта для взаимодействия с компонентами SecurOS. Диапазон возможных значений: [930; 939]. По умолчанию принимает значение 930.
	Примечание. При создании каждого нового объекта <i>Компьютерное зрение</i> система автоматически устанавливает уникальное значение параметра Порт .

Параметры, связанные непосредственно с настройкой работы видеоаналитических детекторов, подробно описаны в соответствующих разделах (см. [Настройка системы](#)).

14.1 Общие рекомендации по настройке и расположению камер

Ниже перечислены основные требования и рекомендации к содержанию сцены, расположению камер и источников освещения при решении задач видеоаналитики, основанных на алгоритмах трекинга движущихся объектов. Несоблюдение указанных требований в большинстве случаев влечет за собой возникновение ложных срабатываний видеоаналитических детекторов или пропуск событий.

1. Минимальное разрешение кадров составляет 320×240 пикселей. Максимальное разрешение в целом не ограничено, поскольку входной кадр, как правило, приводится к одному из стандартных размеров: CIF или D1 (задается в общих настройках трекера).
2. Минимальное значение FPS: 15 к/с. FPS потока должен быть стабилен, в противном случае корректная работа детекторов не гарантируется.
3. Линейные размеры отслеживаемых объектов должны составлять не менее 5–10% от размеров кадра. Например, при размере кадра 640×480 размеры человека должны составлять ~24×32 пикселей.
4. Максимально допустимые линейные размеры отслеживаемых объектов — не более 40% от размеров кадра.
5. Наилучшее качество работы видеоаналитических детекторов достигается в том случае, когда сцена хорошо и равномерно освещена. Иными словами, совокупность параметров чувствительности камеры, источников освещения, свойств отражающих поверхностей элементов фона, а также положение камеры относительно источников освещения (как естественных, так и искусственных) и тенеобразующих препятствий должны обеспечивать равномерную освещенность всей наблюдаемой сцены при минимальном уровне шума на видеоизображении. Если работа видеоаналитического детектора предполагается также и в темное время суток, то необходимо обеспечить должный уровень искусственного освещения, а также избегать таких ракурсов и/или зон видеоанализа, в которых возможно появление существенных бликов от фар транспортных средств, световых рекламных табло и т.п.
6. При монтаже камер следует избегать ракурсов, вызывающих перекрытие одних движущихся объектов (людей, транспортных средств и т.д.) другими движущимися объектами либо неподвижными препятствиями (архитектурными объектами, деревьями и т.д.).
7. Следует избегать размещения камер напротив источников света (следует избегать контрового света). При несоблюдении данного требования, регистрируемые камерой видеонаблюдения изображения в большинстве случаев оказываются непригодными как для визуального анализа человеком, так и для обработки видеоаналитическими детекторами.

8. Следует избегать наличия сильных теней. В противном случае необходимо минимизировать их наличие путем установки дополнительного освещения.
9. По возможности следует избегать наличия в кадре деревьев и прочей растительности, а также водных поверхностей, либо убедиться в возможности маскирования таких зон видеокadra с целью игнорирования их системой видеоаналитики.
10. Камера должна быть прочно и жестко закреплена. Следует избегать наличия колебаний и вибраций либо минимизировать их амплитуду.
11. Алгоритмы видеоаналитики, как правило, предназначены для работы с фиксированными камерами видеонаблюдения. Работа с PTZ-камерами возможна только в одной конкретной препозиции, для которой была произведена настройка видеоаналитического детектора. При переходе камеры из рабочей препозиции в иное положение (при повороте/масштабировании изображения оператором или при переходе в другую препозицию) возможно появление ложных срабатываний детектора.
12. В настройках камер видеонаблюдения (в особенности для сложных и нестабильных сцен) рекомендуется отключать функции автоматического баланса белого, автоматической регулировки диафрагмы и автоматической регулировки усиления. В противном случае возможно появление сильных изменений изображения в моменты подстройки камеры под текущую сцену, что будет вызывать ложные срабатывания видеоаналитических детекторов.

14.2 Настройка системы

В подсистеме компьютерного зрения SecurOS используются как встроенные детекторы, входящие в состав плагина Tracking Kit III, так и независимые от него детекторы, для работы которых плагин не требуется. Как встроенные, так и независимые детекторы используют один и тот же видеопоток, настроенный на родительском для этих детекторов объекте *Камера*.

Выберите *Камеру*, видеопоток которой требуется анализировать (см. **Выбор видеопотока для аналитики**), после чего выполните настройку требуемого детектора:

- **Настройка плагина Tracking Kit III и встроенных видеоаналитических детекторов.**
- **Настройка независимых видеоаналитических детекторов.**

Для работы ряда детекторов потребуется установить программное обеспечение, которое задействует нейросетевые алгоритмы (см. **Установка программного обеспечения для работы нейросетевых алгоритмов**).

Детекторы, использующие нейросетевые алгоритмы в обязательном порядке:

- **Детектор людей без касок.**
- **Нейросетевой детектор драк.**
- **Нейросетевой детектор дыма и огня.**
- **Нейросетевой детектор празднотатания.**
- **Нейросетевой детектор уклонения от оплаты.**
- **Нейросетевой детектор упавших людей.**
- **Нейросетевой счетчик людей.**

Детекторы, использующие нейросетевые алгоритмы только при включении некоторых опций:

- **Детектор бега.**
- **Детектор движения в запрещенном направлении.**

- Детектор пересечения линии.
- Детектор праздношатания.
- Детектор проникновения в запрещенную зону.

14.2.1 Выбор видеопотока для аналитики

Все детекторы (встроенные и независимые), дочерние любой *Камере* из *Дерева камер*, будут использовать для анализа один и тот же видеопоток, поступающий от этой *Камеры*. Если *Камера* является многопоточной, поток для анализа можно выбрать в ее настройках (см. рис. 238).

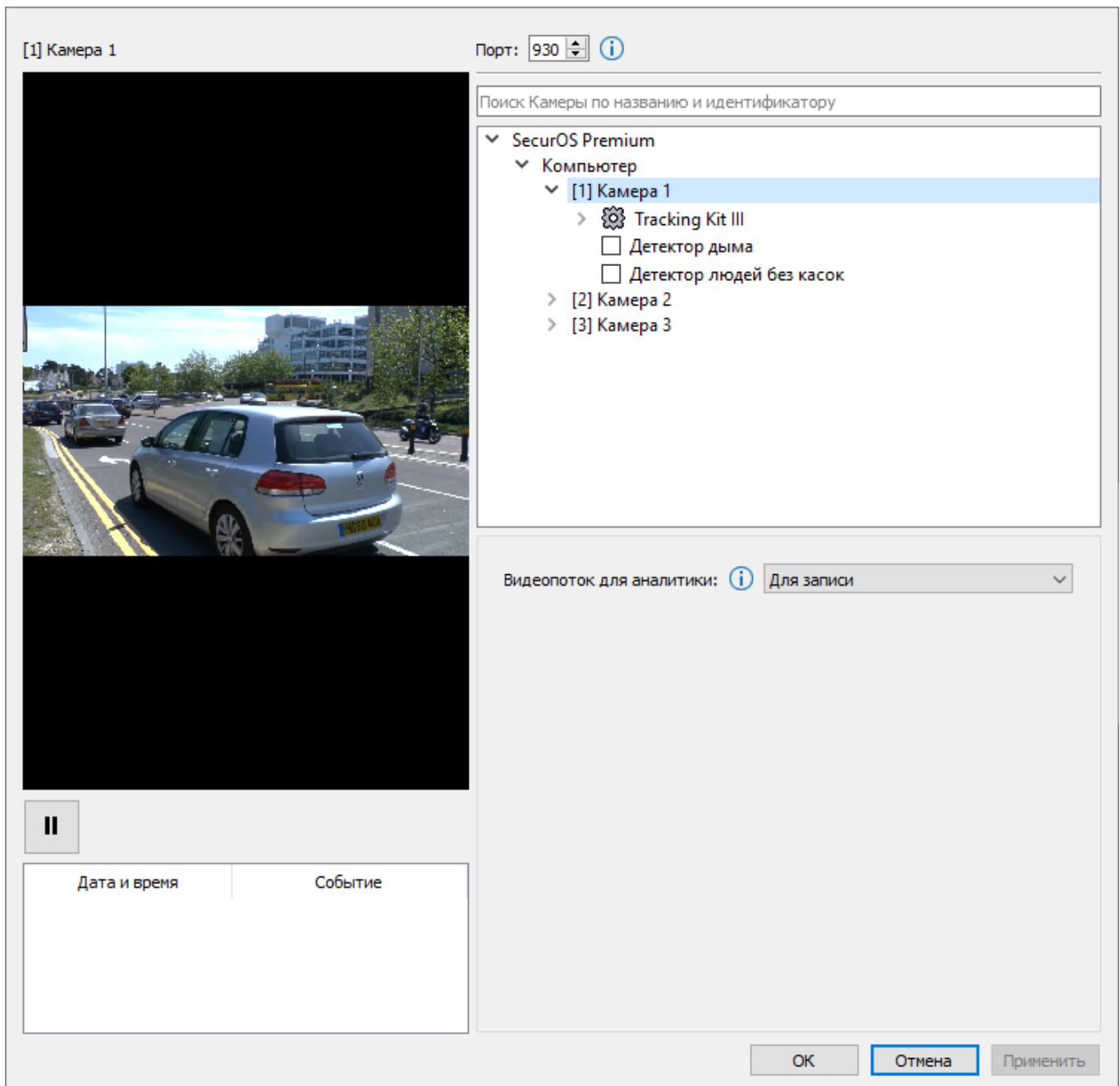


Рис. 238. Окно выбора видеопотока для аналитики

Для выбора видеопотока:

1. В *Дереве камер* двойным щелчком мыши выберите *Камеру*, для которой надо задать общие настройки анализа изображения. В левом верхнем углу окна будет выведено изображение с выбранной камеры, ее идентификатор и название.

Примечание. Если дерево содержит большое количество *Камер*, для поиска требуемой *Камеры* задайте в поле **Поиск Камеры по названию и идентификатору** часть ее названия или идентификатора. В дереве будут автоматически отображены только те *Камеры*, названия или идентификаторы которых удовлетворяют заданным условиям.

2. В правом нижнем углу окна, в блоке настроек параметров *Камеры*, задайте значение параметра **Видеопоток для аналитики**.

Параметр **Видеопоток для аналитики** каждой *Камеры* содержит следующие значения:

- Для записи;
- Для детектора движения;
- Низкое разрешение;
- Базовый;
- Высокое разрешение.

Каждый из доступных видеопотоков может быть выбран, если он определен в настройках объекта *Камера* (см. раздел **Закладка Поток**). Наличие множества потоков позволяет выбрать поток, оптимально отвечающий тем задачам видеоаналитики, которые решаются с помощью детекторов, использующих данную *Камеру*.

Примечание. Если камера не поддерживает многопоточность, детекторы плагина будут использовать единственный доступный видеопоток независимо от значения, выбранного в параметре **Видеопоток для аналитики**.

14.2.2 Настройка плагина Tracking Kit III и встроенных видеоаналитических детекторов

Плагин Tracking Kit III представляет собой интегрированный в SecurOS контейнер, содержащий следующие видеоаналитические детекторы:

- **Детектор бега** — предназначен для обнаружения людей,двигающихся со скоростью, превышающей установленное значение.
- **Детектор движения в запрещенном направлении** — предназначен для обнаружения движения в запрещенном направлении.
- **Детектор оставленных и унесенных предметов** — предназначен для обнаружения оставленных и унесенных предметов.
- **Детектор пересечения линии** — предназначен для подсчета объектов, пересекающих линию контроля.
- **Детектор праздношатания** — предназначен для обнаружения людей, перемещающихся в контролируемой зоне в течение длительного времени.
- **Детектор пребывания в зоне** — предназначен для предоставления статистических данных о длительном/кратковременном пребывании людей в определенном месте.

- **Детектор проникновения в запрещенную зону** — предназначен для обнаружения объектов, пересекающих границу запрещенной зоны.
- **Детектор скопления людей** — предназначен для обнаружения потенциально опасных групп людей.
- **Счетчик объектов** — предназначен для подсчета объектов, пересекающих линию контроля в противоположных направлениях.

Настройки плагина и входящих в его состав детекторов описаны в следующих разделах:

- **Настройка плагина Tracking Kit III.**
- **Настройка встроенных видеоаналитических детекторов.**

14.2.2.1 Настройка плагина Tracking Kit III

В SecurOS каждой *Камере* соответствует отдельный экземпляр плагина Tracking Kit III, который настраивается независимо. При настройке задаются общие параметры детектирования, влияющие на работу каждого видеоаналитического детектора, входящего в состав плагина.

Для настройки плагина выполните следующие действия:

1. Щелкните мышью объект *Tracking Kit III*, дочерний настраиваемой *Камере*. В правом нижнем углу окна отобразится блок настроек параметров плагина (см. рис. 239).

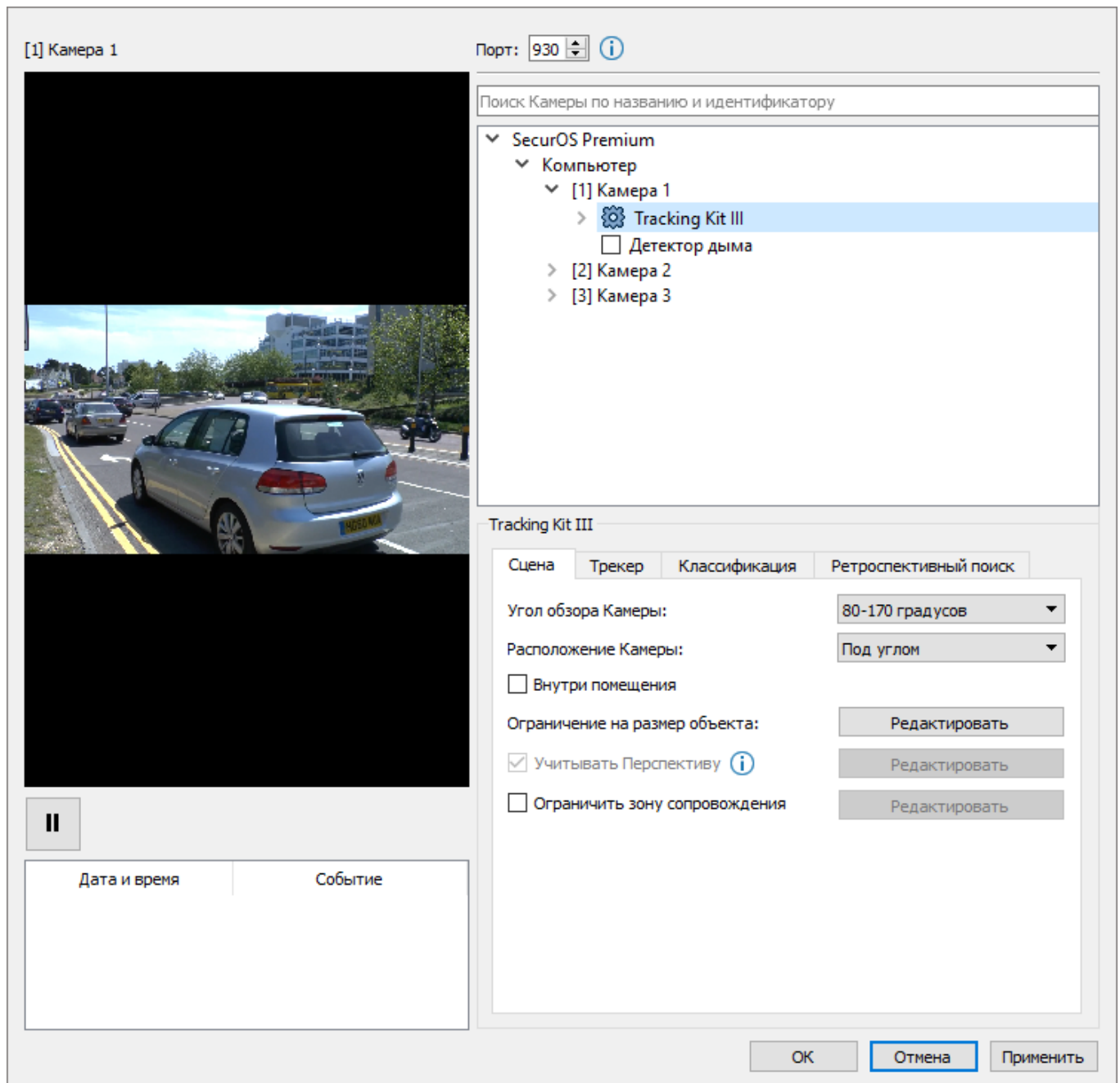


Рис. 239. Окно настройки плагина. Блок Tracking Kit III

- На закладках **Сцена**, **Трекер**, **Классификация** и **Ретроспективный поиск** задайте требуемые значения параметров.
- Для применения настроек нажмите кнопку **Применить** или кнопку **OK**.

Примечание. Таблица событий, расположенная в нижнем левом углу окна, является информационной. Данные в таблице выводятся только в том случае, если один или несколько детекторов выбраны для работы с *Камерой* (см. **Настройка встроенных видеоаналитических детекторов**).

14.2.2.1.1 Закладка Сцена

Закладка предназначена для настройки параметров кадра, который будет анализироваться.

Внешний вид закладки представлен на рис. 240.

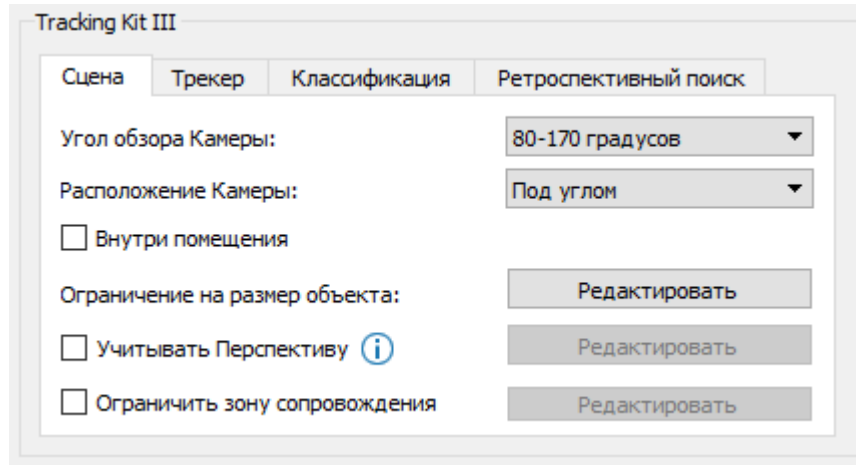


Рис. 240. Плагин Tracking Kit III. Закладка Сцена

Для настройки параметров сцены задайте значения следующих параметров:

- **Угол обзора Камеры, Расположение Камеры, Внутри помещения** — параметры влияют на работу алгоритма детектирования и точность классификации обнаруженных объектов.

Внимание! При использовании PTZ-камеры корректная работа алгоритма возможна только в той препозиции, для которой были произведены настройки детектора.

- **Ограничение на размер объекта** — параметр задает диапазон размеров движущихся в кадре объектов, которые будут отслеживаться трекером. Чем точнее заданные значения соответствуют реальным размерам объектов, тем выше качество трекинга. Для задания граничных размеров нажмите кнопку **Редактировать**, укажите требуемые размеры с помощью мыши (см. рис. 241).



Рис. 241. Задание размеров объектов

- **Учитывать перспективу** — параметр позволяет моделировать трехмерную сцену на основе "плоского" кадра и размеров объектов. В зависимости от значений параметров **Угол обзора Камеры** и **Расположение Камеры** учет перспективы ведется двумя различными способами:
 - с помощью задания двух размеров объекта;
 - с помощью задания одного размера объекта.

Учет перспективы с помощью задания двух размеров объекта — вблизи *Камеры* и на удалении от нее — являлся единственным методом вплоть до релиза 11.8.

Учет перспективы с помощью задания одного размера объекта может быть использован начиная с релиза 11.8. При обновлении SecurOS этот метод становится обязательным для использования в некоторых детекторах, что требует корректировки настроек после обновления. При этом старые настройки перспективы будут сохранены в базе данных независимо от новых.

Внимание! Оптимальный метод учета перспективы выбирается автоматически в зависимости от значений параметров **Угол обзора Камеры** и **Расположение Камеры**.

Настройка перспективы **обязательна** для следующих встроенных детекторов:

- *Детектор бега* (см. **Настройка перспективы для Детектора бега**).
- *Детектор скопления людей* (см. **Настройка перспективы для Детектора скопления людей**).

Примечание. В зависимости от прочих параметров настройка перспективы для *Детектора скопления людей* может быть либо обязательной, либо рекомендуемой.

Для следующих встроенных детекторов использование перспективы **рекомендуется**, но не является обязательным:

- *Детектор скопления людей* (см. **Настройка перспективы для Детектора скопления людей**).

- Детектор движения в запрещенном направлении (см. [Настройка перспективы для Детектора движения в запрещенном направлении](#)).
- Счетчик объектов (см. [Настройка перспективы для Счетчика объектов](#)).

Для учета перспективы отметьте флажок, нажмите кнопку **Редактировать**, с помощью мыши укажите размер (-ы) объекта. На рис. 242 приведен пример настройки перспективы с помощью указания двух размеров объекта — вблизи Камеры и на удалении от нее.

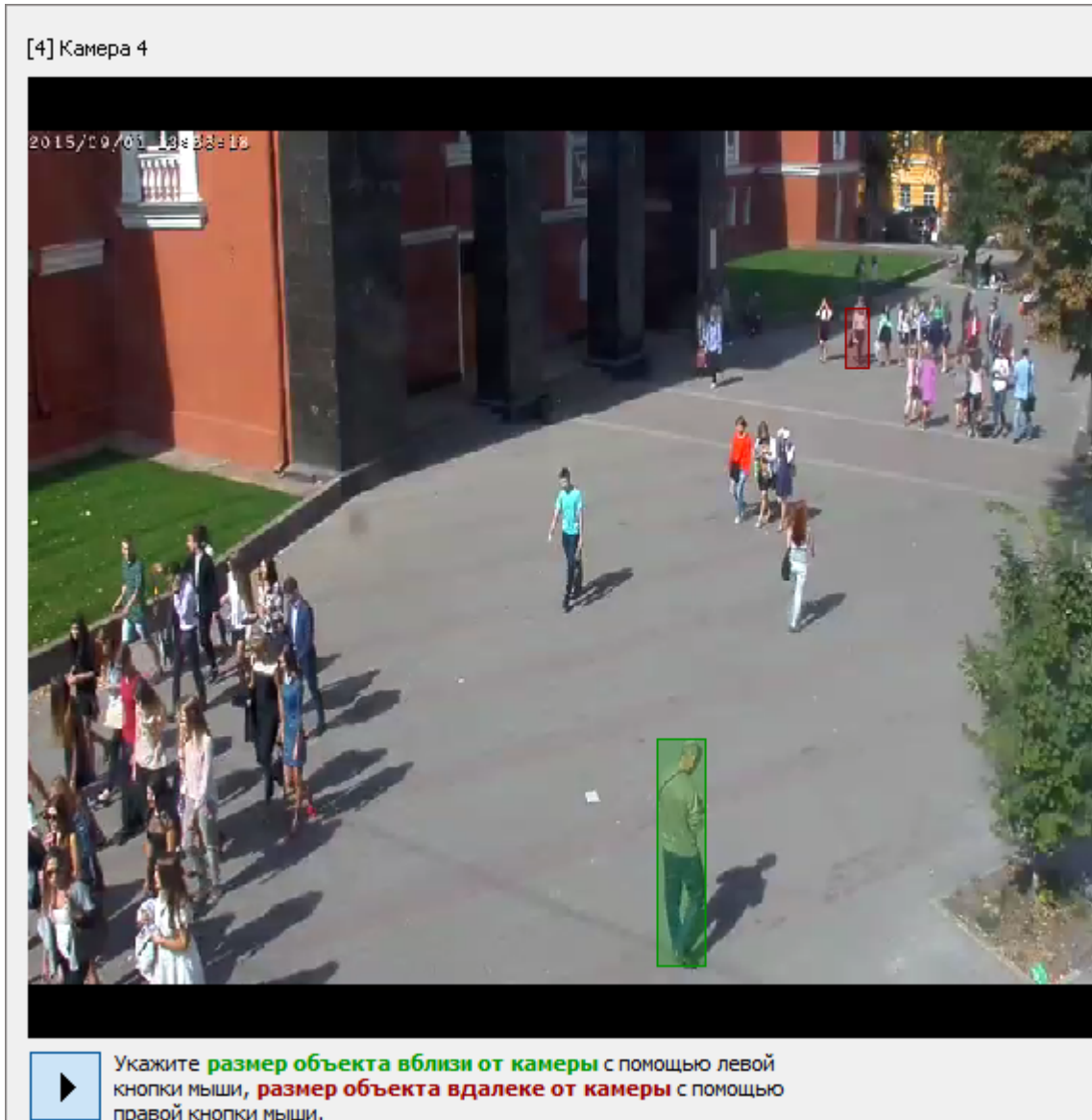


Рис. 242. Задание перспективы

- **Ограничить зону сопровождения** — параметр позволяет ограничить область сопровождения (трекинга) объектов в кадре. Ограничение области сопровождения может существенно снизить вычислительную нагрузку на систему, однако уменьшать размеры области следует с особым вниманием и ответственностью. Для ограничения области трекинга отметьте флажок, с помощью мыши задайте область, в пределах которой будет осуществляться сопровождение (см. рис. 243). После применения настроек контролируемая область кадра будет сужена. В окне настроек детектора область игнорирования (область, в которой сопровождение объектов не осуществляется) будет затемнена (см. рис. 244).

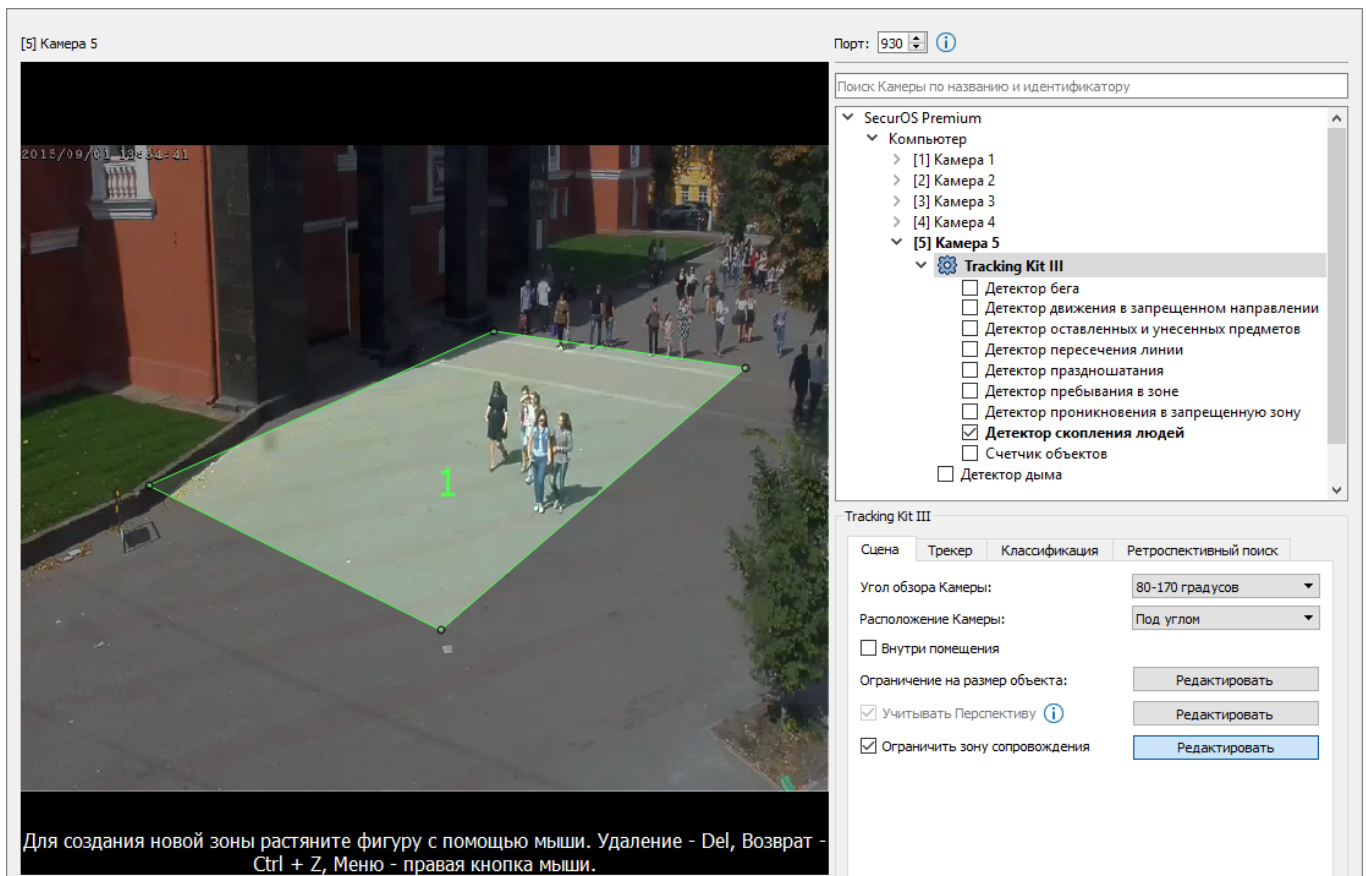


Рис. 243. Ограничение контролируемой зоны в настройках плагина

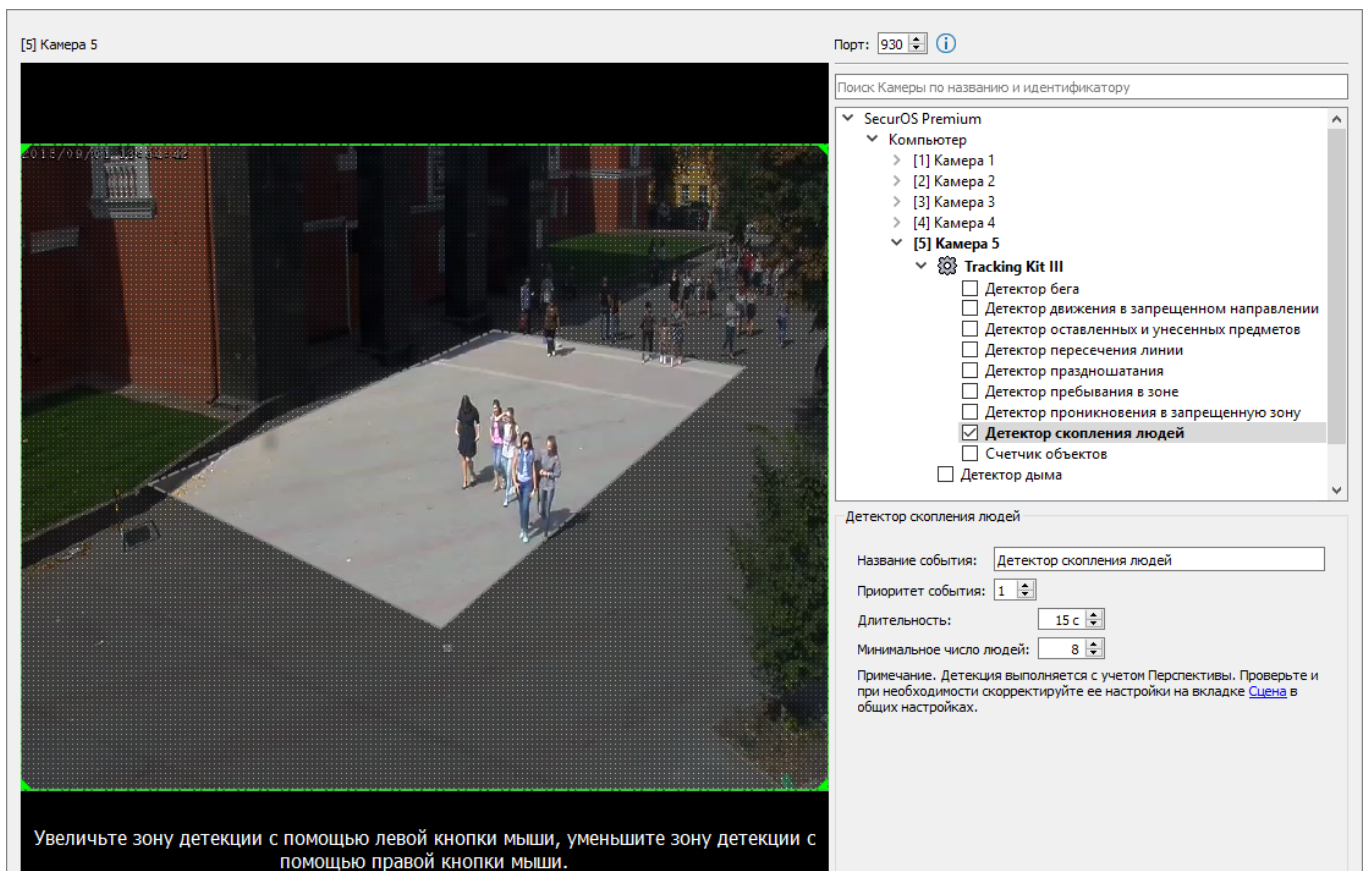


Рис. 244. Отображение ограниченной контролируемой зоны в настройках детектора

14.2.2.1.2 Закладка Трекер

Закладка предназначена для настройки параметров трекера, используемого для анализа кадра.

Внешний вид закладки представлен на рис. 245.

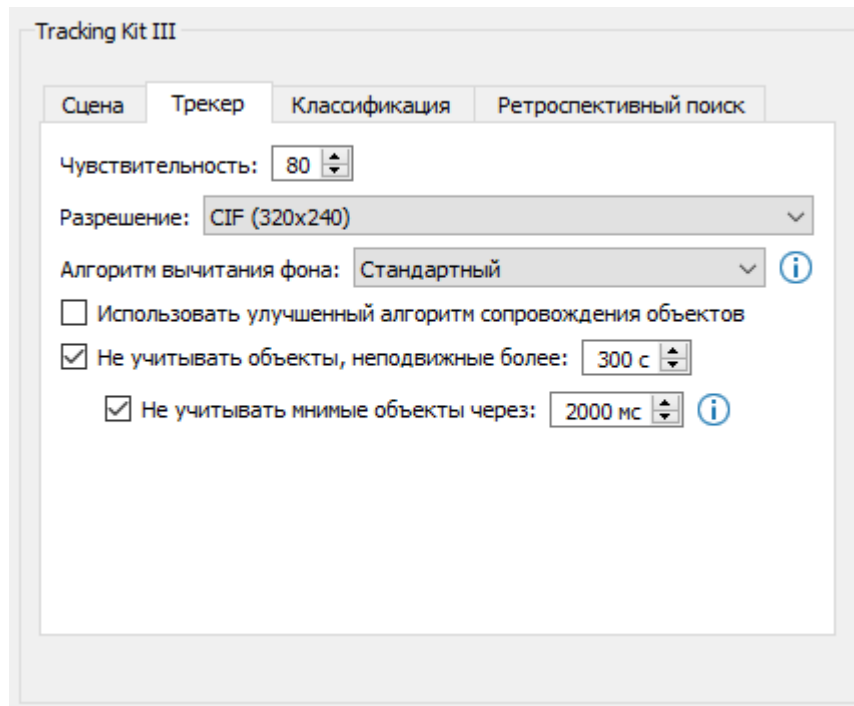


Рис. 245. Плагин Tracking Kit III. Закладка Трекер

Для настройки трекера задайте значения следующих параметров:

- **Чувствительность** — параметр задает чувствительность алгоритма обнаружения движения. При увеличении чувствительности минимальный размер обнаруживаемого объекта снижается, количество обнаруживаемых объектов возрастает. При уменьшении чувствительности минимальный размер обнаруживаемого объекта возрастает, количество обнаруживаемых объектов снижается.

Примечание. В большинстве случаев рекомендуется использовать значение по умолчанию.

- **Разрешение** — параметр задает разрешение анализируемого кадра, к которому будет приведено исходное разрешение видеопотока. В общем случае, чем больше разрешение, тем большее количество объектов малых размеров может быть обнаружено. При этом увеличение разрешения может снижать производительность системы в целом. Рекомендуемое значение — 320×240, которое является минимально достаточным для применения алгоритмов детектирования. При выборе такого значения рекомендуется также использовать улучшенные алгоритмы вычитания фона и сопровождения объектов (параметры **Алгоритм вычитания фона** и **Использовать улучшенный алгоритм сопровождения объектов**). Значение 320×240 также является оптимальным при соблюдении требований, приведенных в разделе **Общие рекомендации по настройке и расположению камер**.

Дополнительная информация

Например, разрешение 640×480 (без включения улучшенных алгоритмов) может быть использовано при необходимости обнаружения объектов малых размеров. По производительности такая конфигурация настройки сравнима с конфигурацией, использующей разрешение 320×240 в сочетании с улучшенными алгоритмами вычитания фона и сопровождения объектов.

- **Алгоритм вычитания фона** — выберите один из предложенных алгоритмов вычитания фона для обнаружения движущегося объекта:
 - Стандартный — самый быстрый режим. Рекомендуется использовать на стабильных сценах с минимальными колебаниями освещенности и отсутствием бликов.
 - Улучшенный — оптимальный режим для обнаружения движущегося объекта в условиях небольших световых и визуальных помех.
 - Максимальный — самый точный режим. Позволяет работать на сложных сценах, автоматически регулирует **Чувствительность**. Использование данного алгоритма рекомендуется только при высокой вычислительной мощности компьютера (процессора).
- **Использовать улучшенный алгоритм сопровождения объектов** — отметьте флажок для использования улучшенного алгоритма сопровождения объектов. Использование улучшенного алгоритма позволяет повысить точность разделения движущихся объектов и снизить вероятность ошибки трекара при пересечении траектории объектов и их взаимном заслонении. Рекомендуется использовать, если заданное значение **Разрешения** равно 320x240.
- **Не учитывать объекты, неподвижные более** — отметьте флажок для исключения из обработки объектов, неподвижных в течение заданного времени. По истечении заданного времени все сущности, ранее определенные как объекты, будут считаться фоном и не будут обрабатываться алгоритмами обнаружения и сопровождения.
- **Не учитывать мнимые объекты через** — отметьте флажок для исключения из обработки мнимых объектов. Под мнимым объектом подразумевается сущность, которая не может быть классифицирована ни как объект, ни как фон. Например, остановившийся автомобиль, ранее определенный как объект, через некоторое время покинул место стоянки. В результате на анализируемом кадре детектируется "пустая" область, которая и представляет собой мнимый объект. Параметр недоступен, если не отмечен флажок **Не учитывать объекты, неподвижные более**.

Примечание. Для корректной работы *Детектора оставленных и унесенных предметов* параметр **Не учитывать мнимые объекты через** рекомендуется отключить.

14.2.2.1.3 Закладка Классификация

Закладка предназначена для настройки общих параметров алгоритма классификации, которые будут применены ко всем *классам* детектируемых объектов. Класс объекта определяется совокупностью его специфических характеристик, которые задаются внутри алгоритма классификации. Детекторы SecurOS могут работать со следующими классами объектов и их комбинациями:

- Автомобиль;
- Животное;
- Человек;
- Автомобиль и человек.

Включить режим классификации и выбрать класс объекта можно для каждого детектора индивидуально в его настройках. Если класс выбран, то детектор будет отслеживать только объекты данного класса, что позволяет снизить нагрузку на детектор и повысить качество детектирования.

Внимание! Максимальный и минимальный размеры объекта должны лежать внутри диапазона размеров детектируемых объектов, заданных на закладке **Сцена**.

Внешний вид закладки представлен на рис. 246.

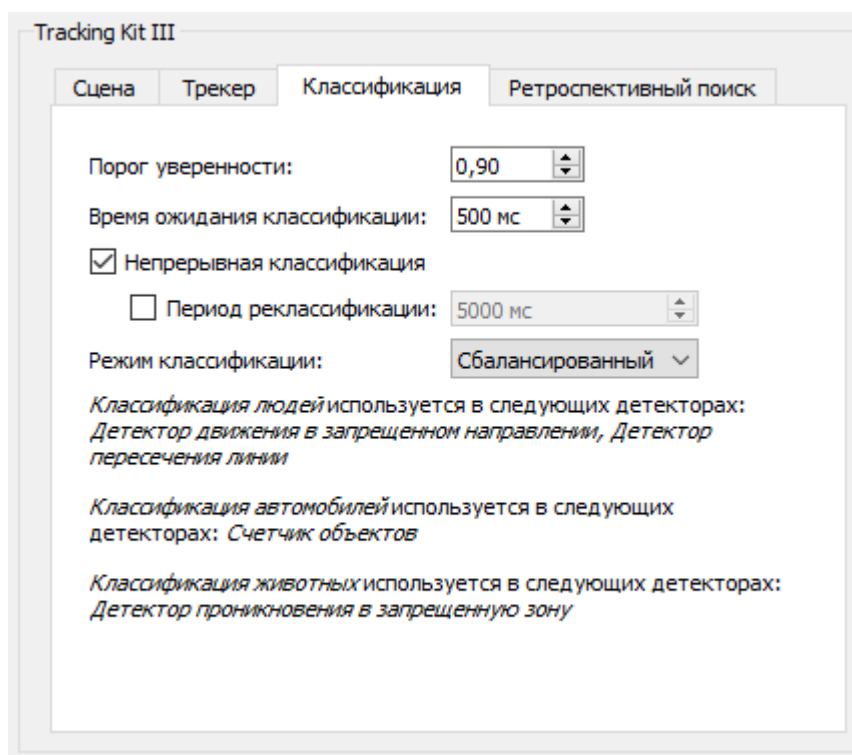


Рис. 246. Плагин Tracking Kit III. Закладка Классификация

Задайте параметры процедуры классификации объектов:

- **Порог уверенности** — порог вероятности определения класса, при превышении которого считается, что объект гарантированно принадлежит определенному классу. Диапазон возможных значений: $[0.01; 0.99]$. Чем ниже заданное значение, тем выше будет скорость классификации объекта и, одновременно, вероятность ошибки классификации, и наоборот.
- **Время ожидания классификации** — максимальное время ожидания определения класса объекта после срабатывания детектора для генерации события. Если в течение заданного времени после срабатывания детектора класс объекта не определен, событие не генерируется. Если класс объекта определен, событие генерируется со временем срабатывания детектора. Диапазон возможных значений (в миллисекундах): $[0; 10000]$.
- **Непрерывная классификация** — отметьте флажок, если необходимо периодически уточнять определенный класс объекта (Человек, Автомобиль, Животное) в течение всего времени нахождения объекта в кадре. Алгоритм позволяет повысить качество трекинга за счет снижения количества ошибок определения класса, но требует больших вычислительных ресурсов.
- **Период реклассификации** — отметьте флажок, если необходимо принудительно сбрасывать ранее определенный класс объекта, если в течение указанного времени алгоритму не удастся достоверно подтвердить этот класс. Диапазон возможных значений (в миллисекундах): $[1000; 60000]$.
- **Режим классификации** — режим, определяющий качество и скорость классификации объектов. По умолчанию принимает значение Сбалансированный. Если значение по умолчанию не обеспечивает необходимую скорость работы и требования к точности классификации невысоки, выберите значение Высокая скорость. Если точность классификации недостаточна, а вычислительные ресурсы комплекса высоки, выберите значение Высокая точность.

Примечание. Значение по умолчанию изменять не рекомендуется.

Ниже на вкладке приводится справочная информация об алгоритмах классификации, используемых различными детекторами, см. рис. 246.

14.2.2.1.4 Закладка Ретроспективный поиск

Закладка предназначена для управления записью метаданных в БД видеоархива SecurOS (fsindex). Подробнее про поиск в видеоархиве с использованием метаданных см. [Ретроспективный поиск](#).

Внешний вид закладки представлен на рис. 247.

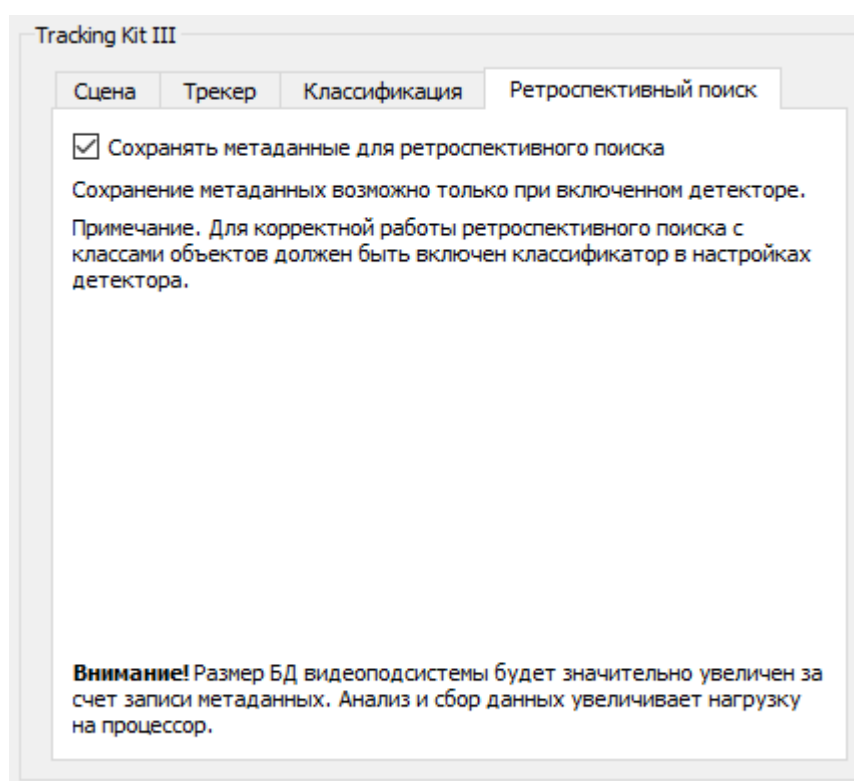


Рис. 247. Плагин Tracking Kit III. Закладка Ретроспективный поиск

Для записи метаданных в БД отметьте флажок **Сохранять метаданные для ретроспективного поиска** (по умолчанию снят).

Примечание. Флажок доступен в том случае, если для работы с *Камерой* выбран хотя бы один детектор.

14.2.2.2 Настройка встроенных видеоаналитических детекторов

В данном разделе приводится описание параметров и особенностей настройки видеоаналитических детекторов, входящих в состав плагина Tracking Kit III.

Для настройки параметров детектора в *Дереве камер* выберите *Камеру*, отметьте флажок слева от названия требуемого детектора. В окне настройки будет выведено изображение с данной *Камеры* и параметры настройки выбранного детектора (см. рис. 248).

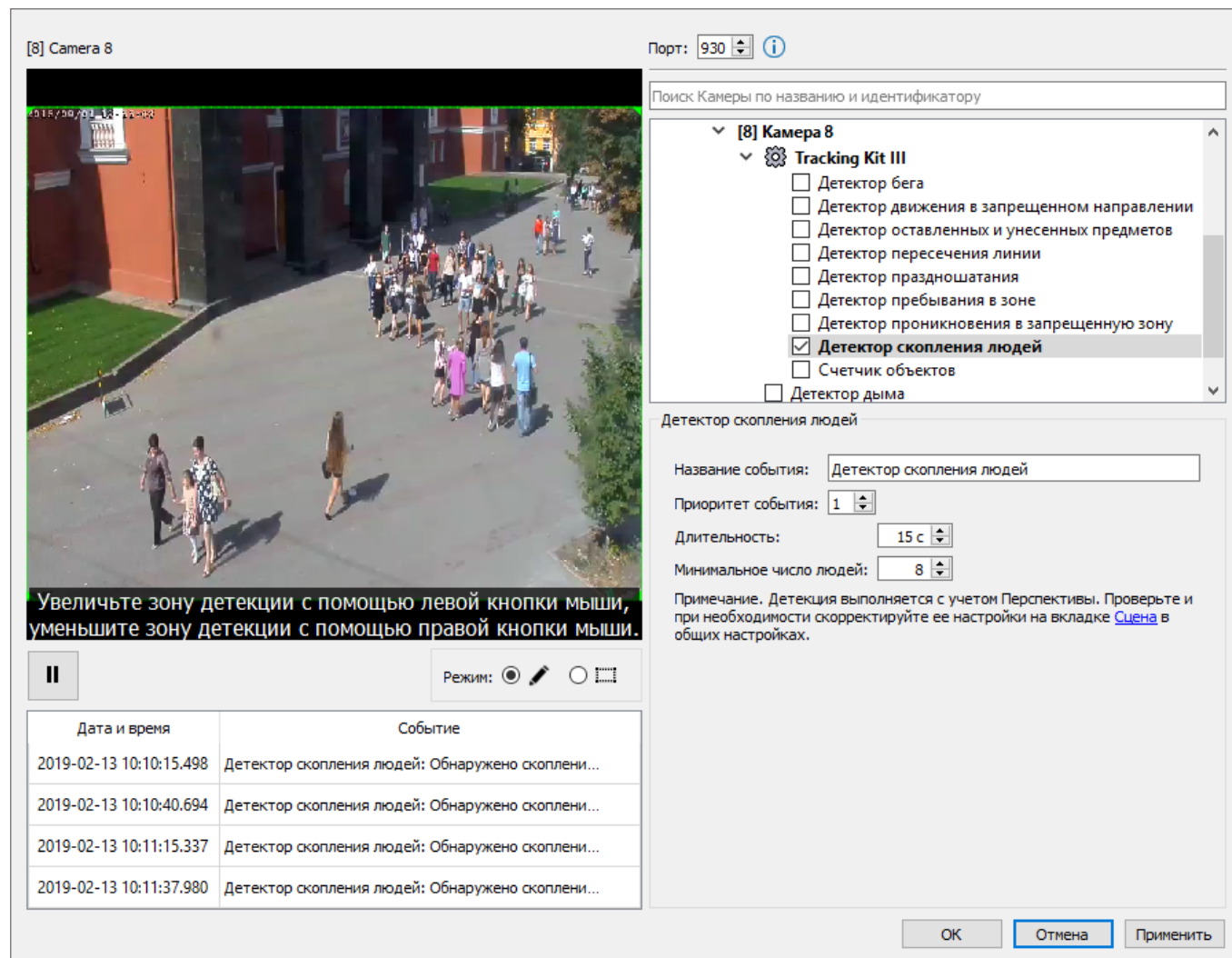


Рис. 248. Окно настройки параметров детектора

Примечание. Камеры, для которых выбран хотя бы один детектор, выделяются в *Дереве камер* **жирным** шрифтом.

Корректность заданных параметров детектора можно проверить сразу после его настройки. Для этого используется *Таблица событий*, расположенная в левом нижнем углу окна (см. рис. 248). Проверка корректности настроек выполняется следующим образом:

1. Задаются и применяются все необходимые параметры детектора, зоны и линии детектирования.

Примечание. Зоны и линии детектирования удобнее наносить на статичном кадре. Для остановки видеопотока нажмите кнопку , нанесите требуемые зоны и линии контроля. Для воспроизведения видеопотока нажмите кнопку .

2. Просматривая изображение с *Камеры*, оператор визуально фиксирует ситуацию, которая, в соответствии с настройками, должна быть обработана детектором (например, объект пересек границу запрещенной зоны).
3. Если при возникновении такой ситуации в *Таблицу событий* каждый раз заносится новая запись о событии, настройки детектора считаются корректными. В противном случае настройки считаются неудовлетворительными и должны быть изменены.

Внимание! На работу детектора влияют как собственные настройки детектора, так и общие настройки плагина (см. **Настройка плагина Tracking Kit III**). Если собственные настройки детектора не позволяют добиться корректных результатов работы, необходимо изменить общие настройки плагина.

14.2.2.2.1 Настройка контролируемой зоны

При работе видеоаналитического детектора объекты наблюдения и условия срабатывания детектора контролируются в некоторой зоне, заданной в кадре. Такая зона представляет собой "прозрачную" для детектора область кадра.

Для обеспечения работы детектора в системе используются следующие контролируемые зоны:

- *Зона сопровождения объектов* (далее *Зона трекинга*) — в этой зоне выполняется только сопровождение объектов. Данная зона является общей для всех видеоаналитических детекторов и задается в настройках плагина **Tracking Kit III** на закладке **Сцена**.
- *Зона детектирования событий* (далее *Зона детектирования*) — в этой зоне выполняется анализ условий срабатывания детектора и генерация событий. Данная зона задается независимо для каждого детектора в его собственных настройках.

Контролируемая зона может быть образована с помощью прямоугольников либо полигонов. В кадре можно задать одну единую зону, состоящую из множества прямоугольников и/или их комбинаций, и не более 9 независимых зон, образованных полигонами.

Способы задания зон описаны в следующих разделах:

- **Задание прямоугольной зоны.**
- **Задание полигональной зоны.**

Примечания:

1. В настройках плагина можно создать не более 9 полигональных зон.
 2. В настройках детектора можно создать не более 9 полигональных зон или 1 прямоугольную зону.
 3. При переключении режимов в настройках детектора ранее созданные зоны удаляются.
-

Задание прямоугольной зоны

По умолчанию, при первоначальной настройке системы, площадь контролируемой зоны равна всей площади кадра (см. рис. 249).

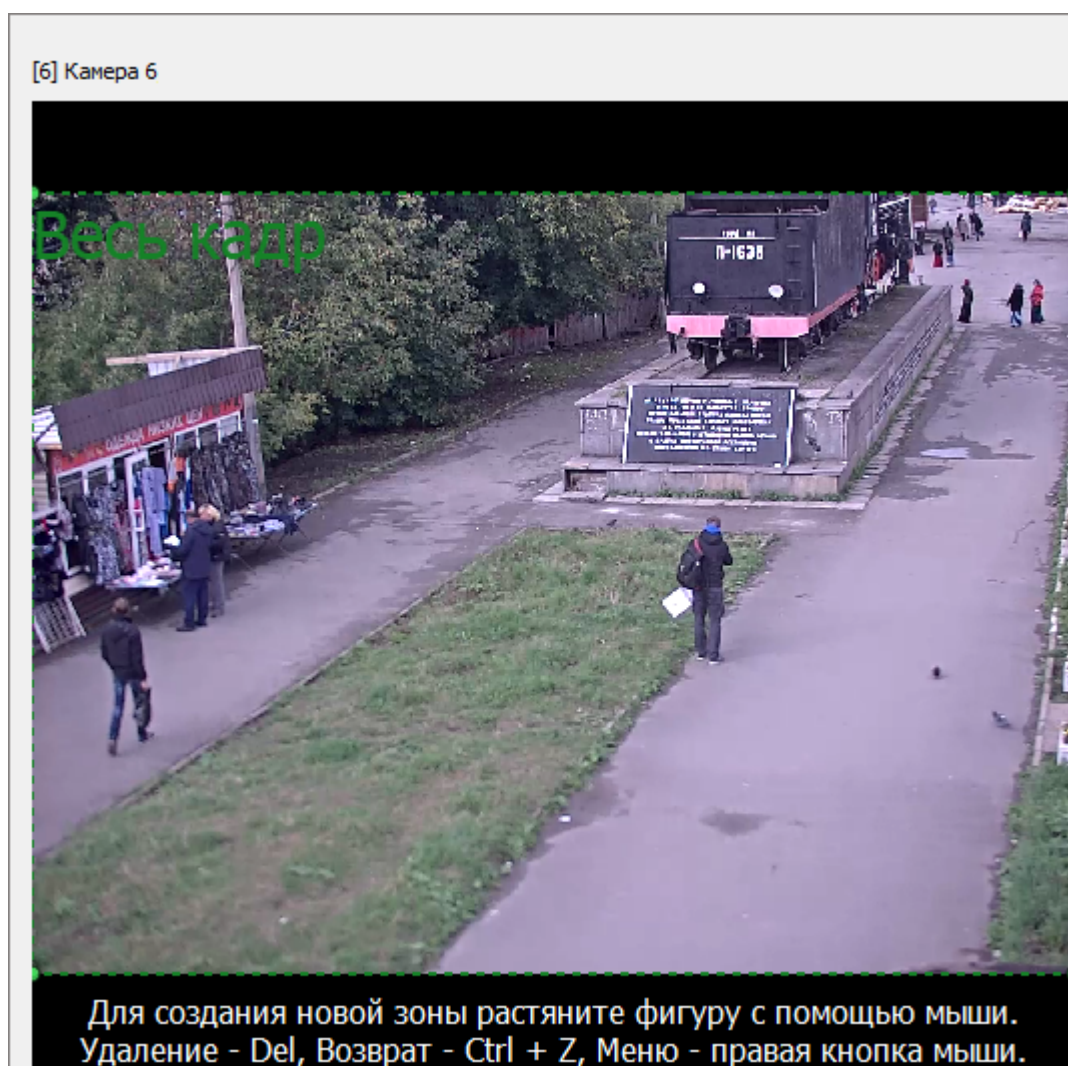


Рис. 249. Размер зоны по умолчанию

Для уменьшения размеров зоны нажмите левую кнопку мыши и, удерживая ее, нарисуйте в кадре один или несколько прямоугольников или их комбинаций (см. рис. 250).

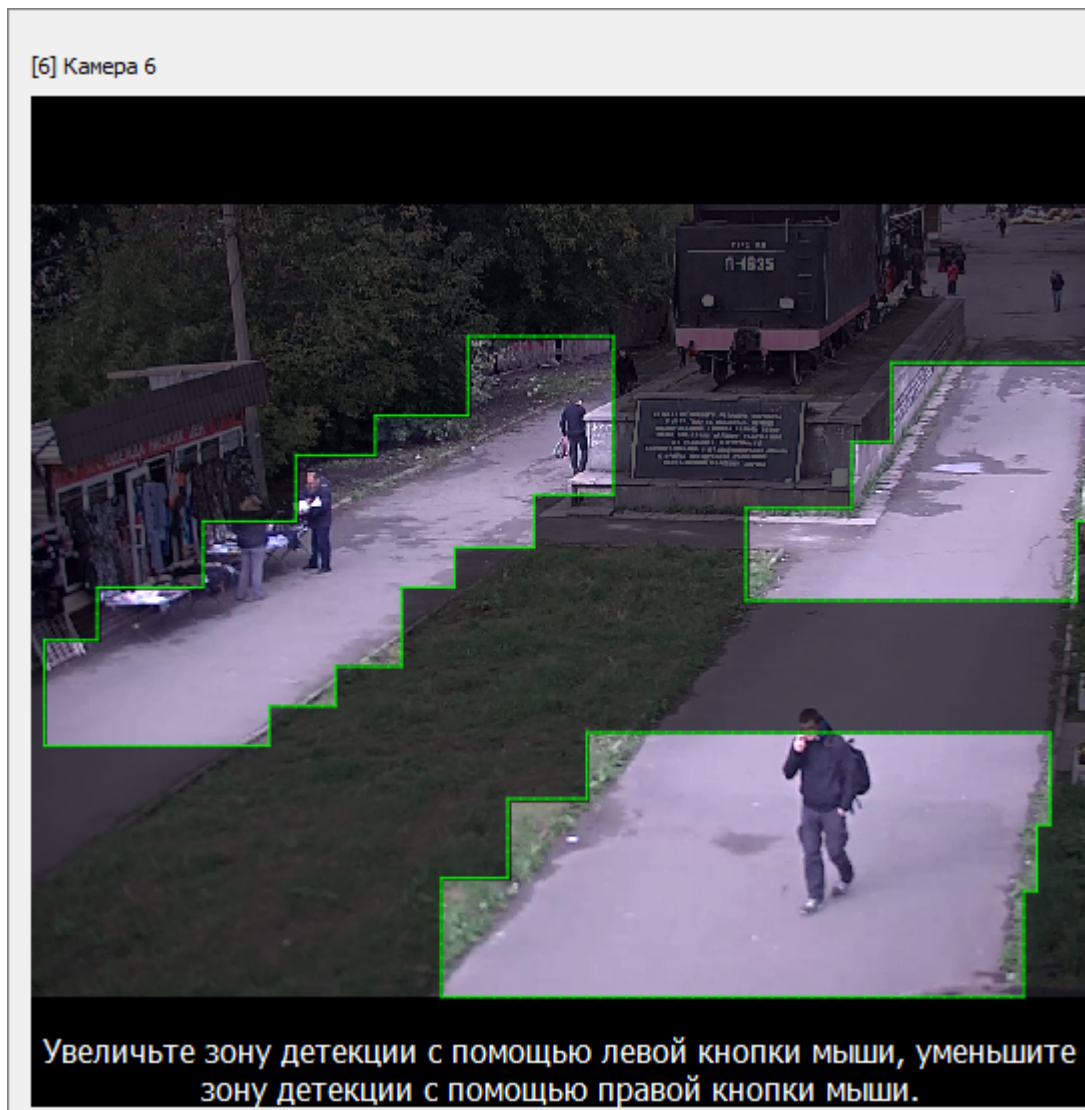


Рис. 250. Прямоугольная зона, образованная несколькими фигурами

Прямоугольники могут перекрываться или располагаться в кадре отдельно. Количество простых и сложных фигур при этом неограничено.

Внимание! Все прямоугольники, заданные в кадре, составляют одну единственную контролируемую зону, независимо от их количества и комбинации.

Задание полигональной зоны

Аналогично прямоугольной зоне, полигональная зона по умолчанию устанавливается равной всей площади кадра (см. рис. 249). Для уменьшения размеров зоны в контекстном меню кадра выберите режим работы с полигонами (см. рис. 251).

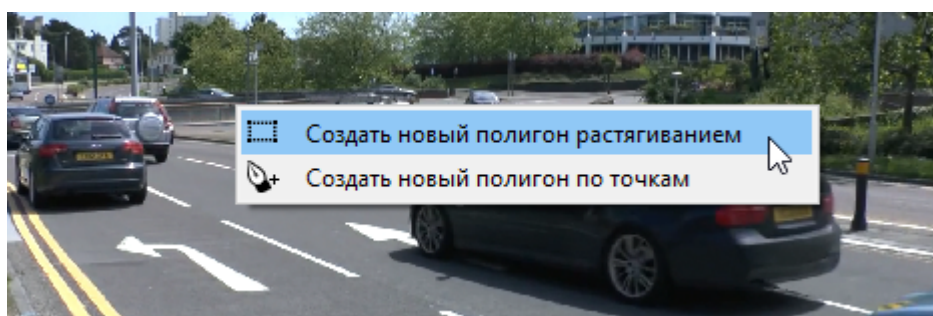


Рис. 251. Выбор режима работы с полигонами

Примечания:

1. В настройках детектора переключение режимов рисования (Прямоугольник/Полигон) выполняется с помощью опций   (Прямоугольник) и   (Полигон).
2. По умолчанию, при первоначальной настройке, для рисования полигонов установлен режим **Растягивания**.

В режиме создания полигона **Растягиванием** наведите указатель мыши на какую-либо из сторон или вершин исходного прямоугольника (см. рис. 252).

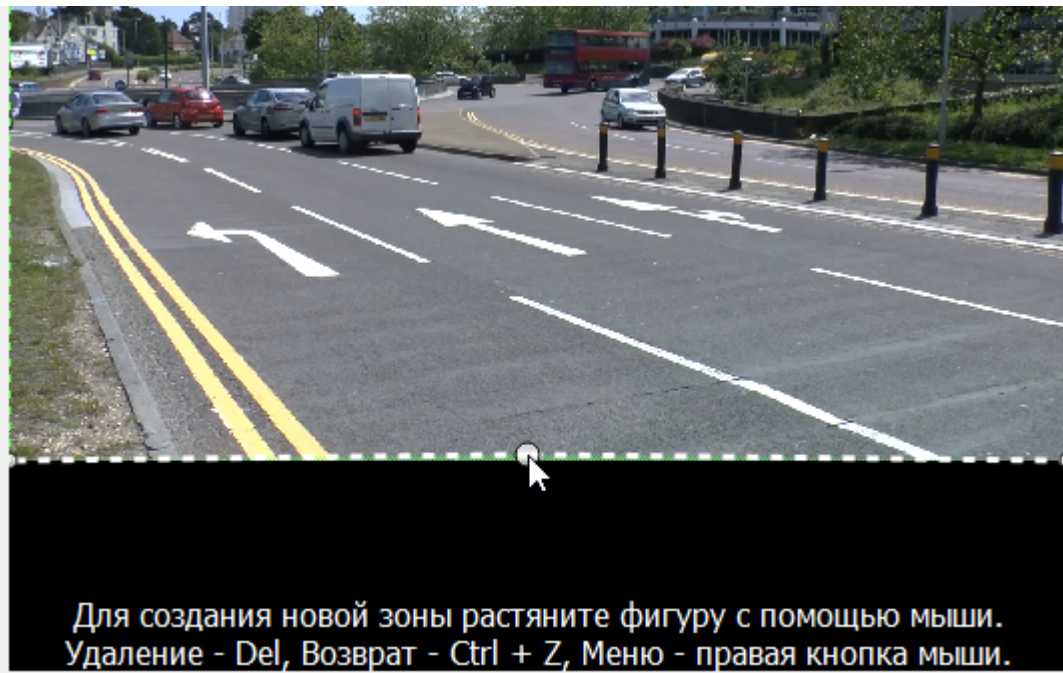


Рис. 252. Точка растягивания зоны

Переместите точку в требуемом направлении. Последовательно выбирая точки на периметре или вершинах фигуры, сформируйте требуемую форму зоны (например, см. рис. 253).

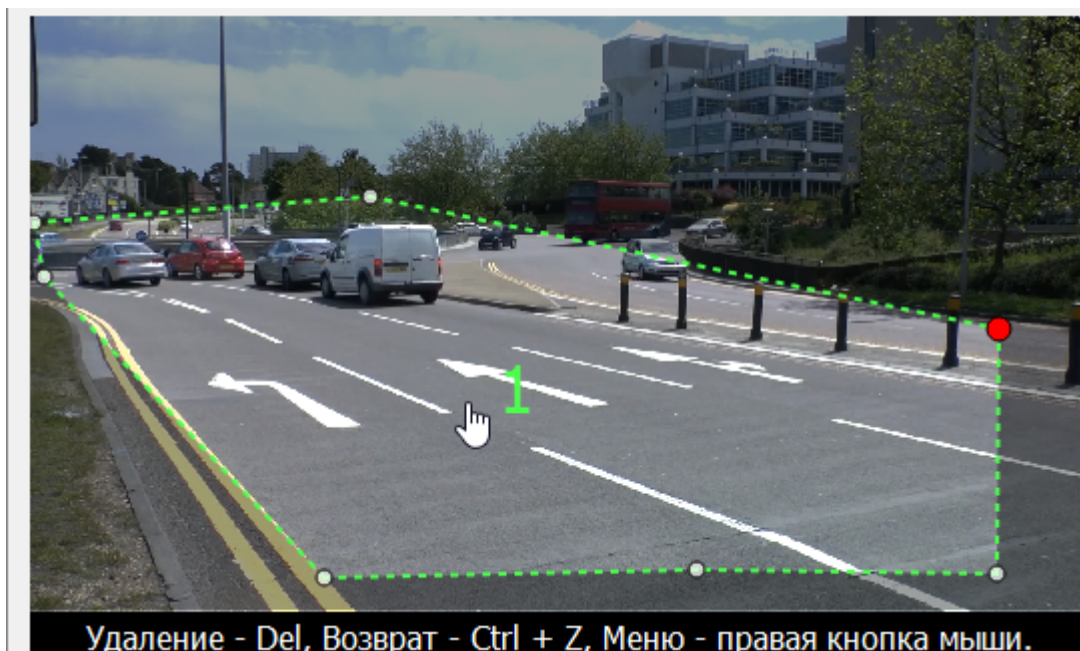


Рис. 253. Полигональная зона (растягивание)

В режиме создания полигона **По точкам**, указатель мыши принимает форму, показанную на рис. 254.

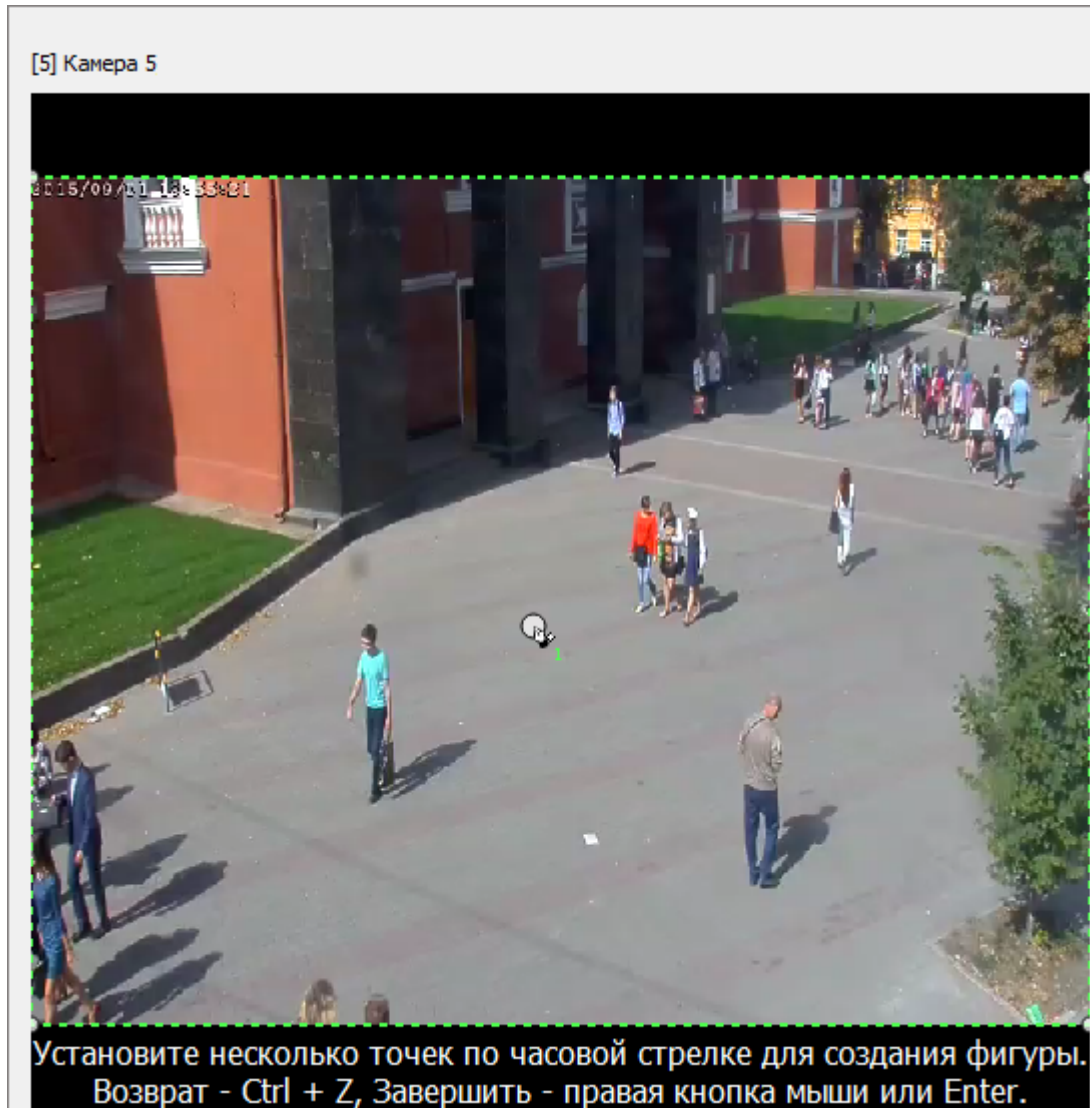


Рис. 254. Режим задания полигональной зоны по точкам

Переместите указатель в требуемом направлении и нажмите левую кнопку мыши. На кадре будет отмечена первая из вершин полигона. Чтобы задать зону требуемой формы, последовательно выполните указанную операцию несколько раз (см. рис. 255).

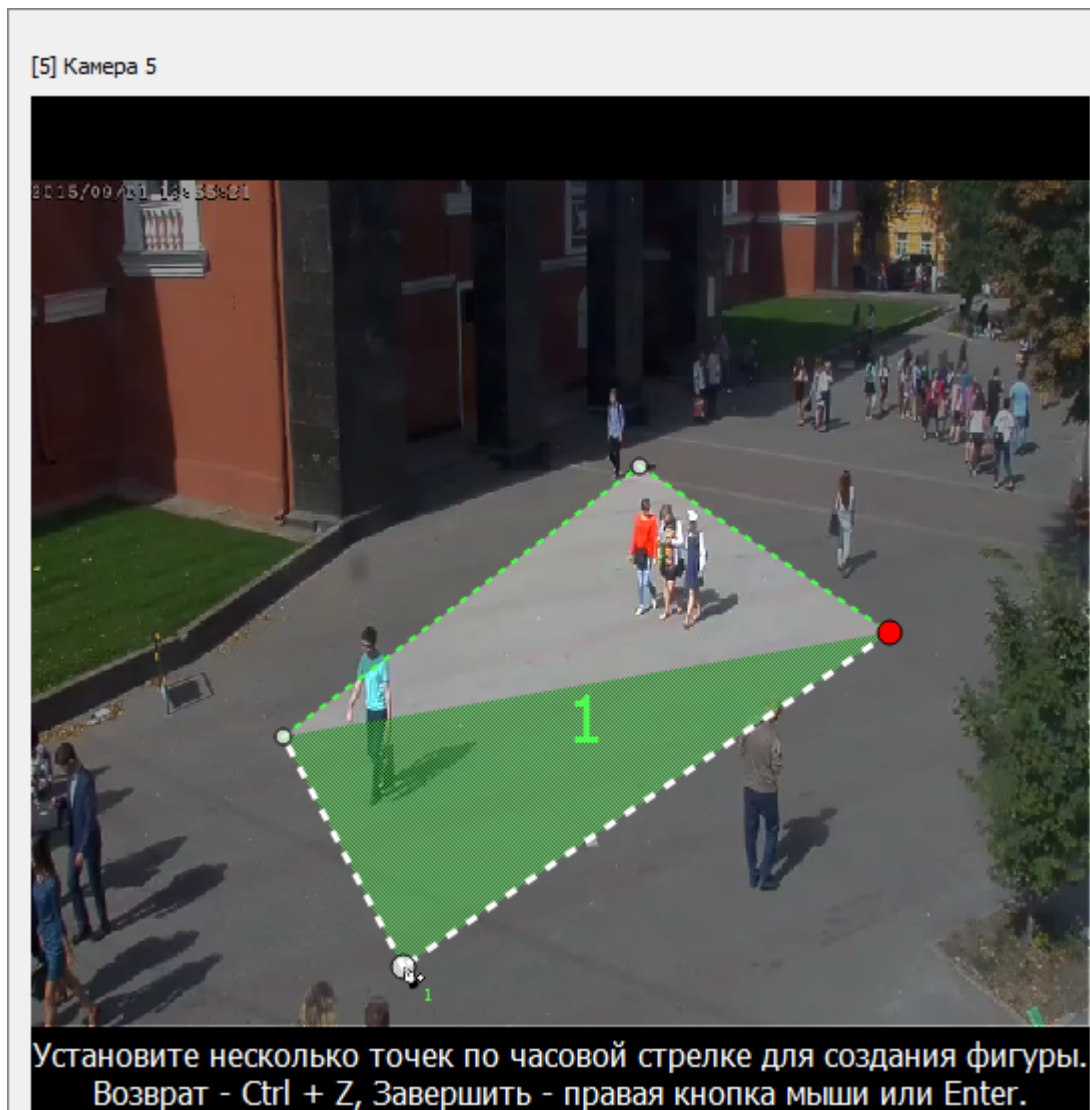


Рис. 255. Полигональная зона (создание по точкам)

Чтобы завершить работу с зоной, дважды нажмите левую кнопку мыши в последней заданной точке.

Внимание! В кадре можно задать до 9 полигонов, каждый из которых будет считаться отдельной зоной. Для удобства работы такие зоны будут пронумерованы.

С помощью контекстного меню каждой полигональной зоне можно назначить приоритет (см. рис. 256). Приоритет зоны добавляется в комментарий к событию (см. [Представление результатов работы видеоаналитического детектора](#)). Дальнейшая обработка события может выполняться в соответствии с приоритетом события и/или приоритетом зоны. Зона с приоритетом 1 отмечается зеленым цветом, зона с приоритетом 10 — красным. Прочие зоны окрашиваются в промежуточные цвета в соответствии с их приоритетом.

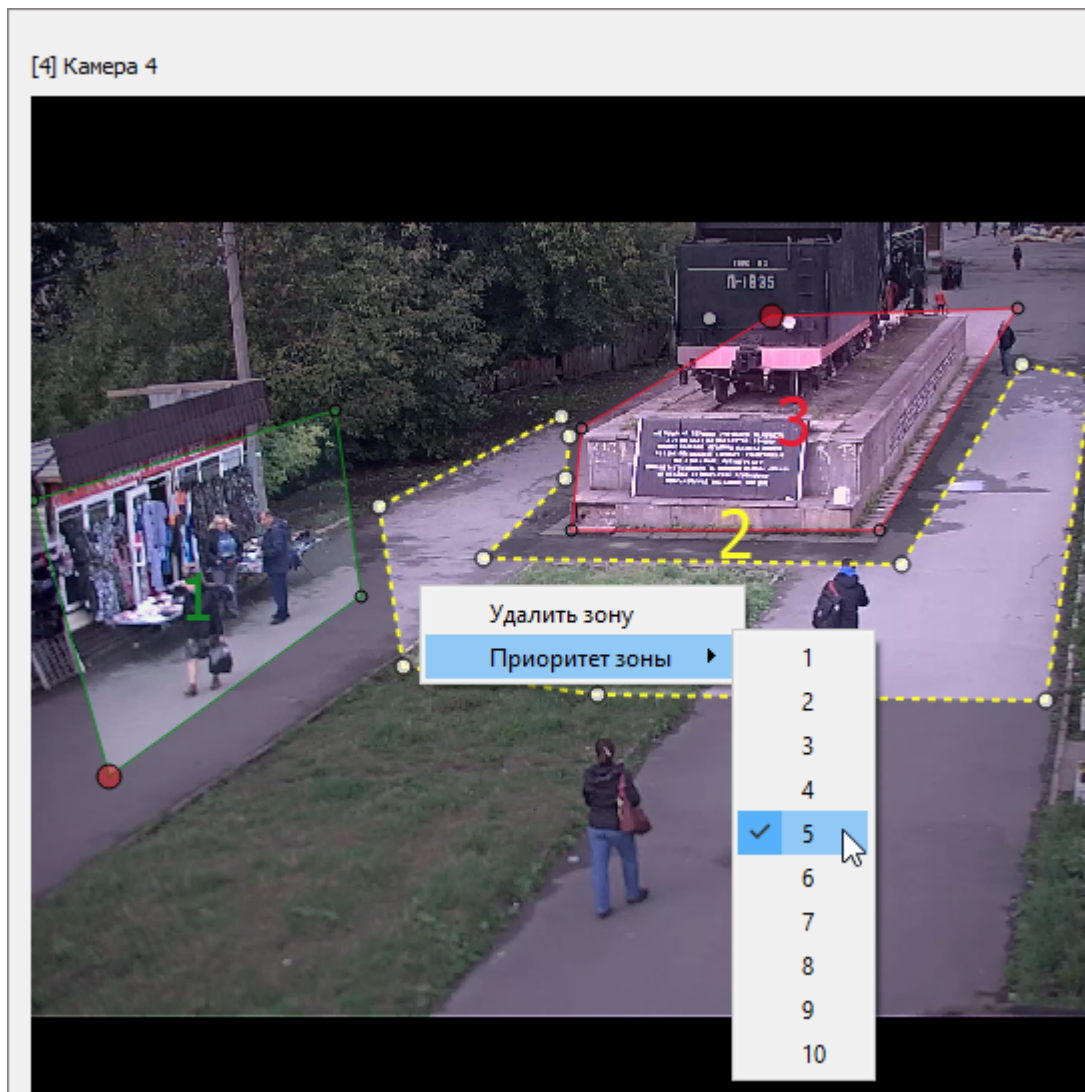


Рис. 256. Задание приоритета зоны

14.2.2.2 Детектор бега

Под бегом понимается движение человека в контролируемой зоне со скоростью, превышающей пороговую, которая вычисляется, используя средний размер человека в данной точке с учетом перспективы. Контролируемая зона и пороговое значение скорости являются настраиваемыми параметрами детектора.

Необходимо задать граничные размеры объектов. Для достижения наилучших показателей работы данного детектора рекомендуется использование ракурса "под углом". Для минимизации ложных срабатываний требуется визуальная делимость движущихся в кадре объектов (люди не должны перекрывать друг друга либо двигаться в плотном потоке).

Детектор работает только с классом объектов Человек, который устанавливается автоматически и не может быть отключен.

Окно настройки параметров *Детектора бега* представлено на рис. 257.

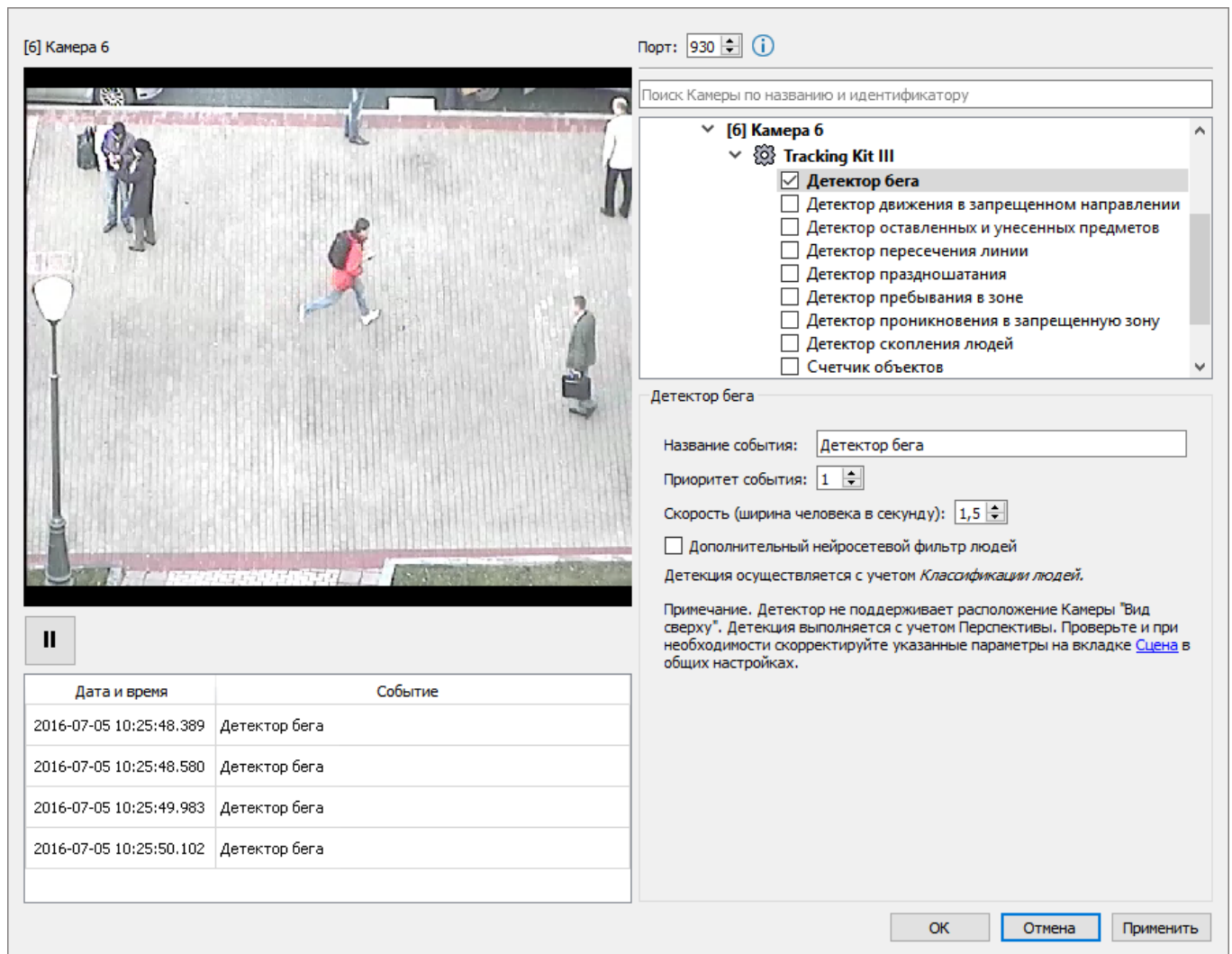


Рис. 257. Окно настройки параметров Детектора бега

Таблица 85. Параметры Детектора бега

Параметр	Описание
Название события	Задайте название события, которое будет отправляться в <i>Протокол событий</i> , если скорость человека внутри контролируемой зоны больше установленного значения.
Приоритет события	Задайте приоритет события данного детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения.

Параметр	Описание
Скорость (ширина человека в секунду)	Задайте скорость движения (в относительных единицах), при превышении которой человек будет считаться бегущим. Примечание. Скорость движения задается относительно ширины объекта, вычисленной на момент его захвата детектором (далее эталонная ширина). Если длина траектории, которую преодолевает человек за 1 секунду, превышает значение эталонной ширины в Скорость раз, человек считается бегущим. При этом, в зависимости от траектории движения, эталонная ширина изменяется с учетом перспективы.
Дополнительный нейросетевой фильтр людей	Отметьте флажок, чтобы использовать дополнительный нейросетевой фильтр. Применение фильтра снижает количество ложных срабатываний детектора, но приводит к повышению вычислительной нагрузки. Примечание. Для работы фильтра необходимо дополнительно установить OpenVINO Server. За подробной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems.

Внимание! Для работы детектора необходимо настроить перспективу (см. [Закладка Сцена](#)).

14.2.2.2.1 Настройка перспективы для Детектора бега

Настройка перспективы для *Детектора бега* является обязательной.

Внимание! Детектор не будет работать, если параметр **Расположение камеры** принимает значение Вид сверху. При прочих значениях параметра **Расположение Камеры** перспектива будет учитываться автоматически.

В Таблице 86 приведены возможные методы настройки перспективы в зависимости от значений параметров **Угол обзора Камеры** и **Расположение Камеры**.

Таблица 86. Методы настройки перспективы для Детектора бега

Параметр Угол обзора Камеры	Параметр Расположение Камеры	Метод настройки перспективы
80–170 градусов	Под углом	По двум размерам объекта — вблизи и на удалении от камеры
	Горизонтальное	По одному размеру объекта
360 градусов	Под углом	По двум размерам объекта — вблизи и на удалении от камеры
	Горизонтальное	По одному размеру объекта

14.2.2.2.3 Детектор движения в запрещенном направлении

Детектор предназначен для обнаружения движения в запрещенном направлении.

Для успешного срабатывания детектора необходимо точное определение траектории объекта. Объект должен непрерывно распознаваться на протяжении некоторого отрезка времени.

Наибольшая точность подсчета достигается при достижении хорошего контраста объекта и фона. В плохую погоду при наличии воды на асфальте могут возникать локальные помехи мешающие детектированию объектов, вследствие чего срабатывание детектора может не произойти.

Окно настройки параметров Детектора движения в запрещенном направлении представлено на рис. 258.

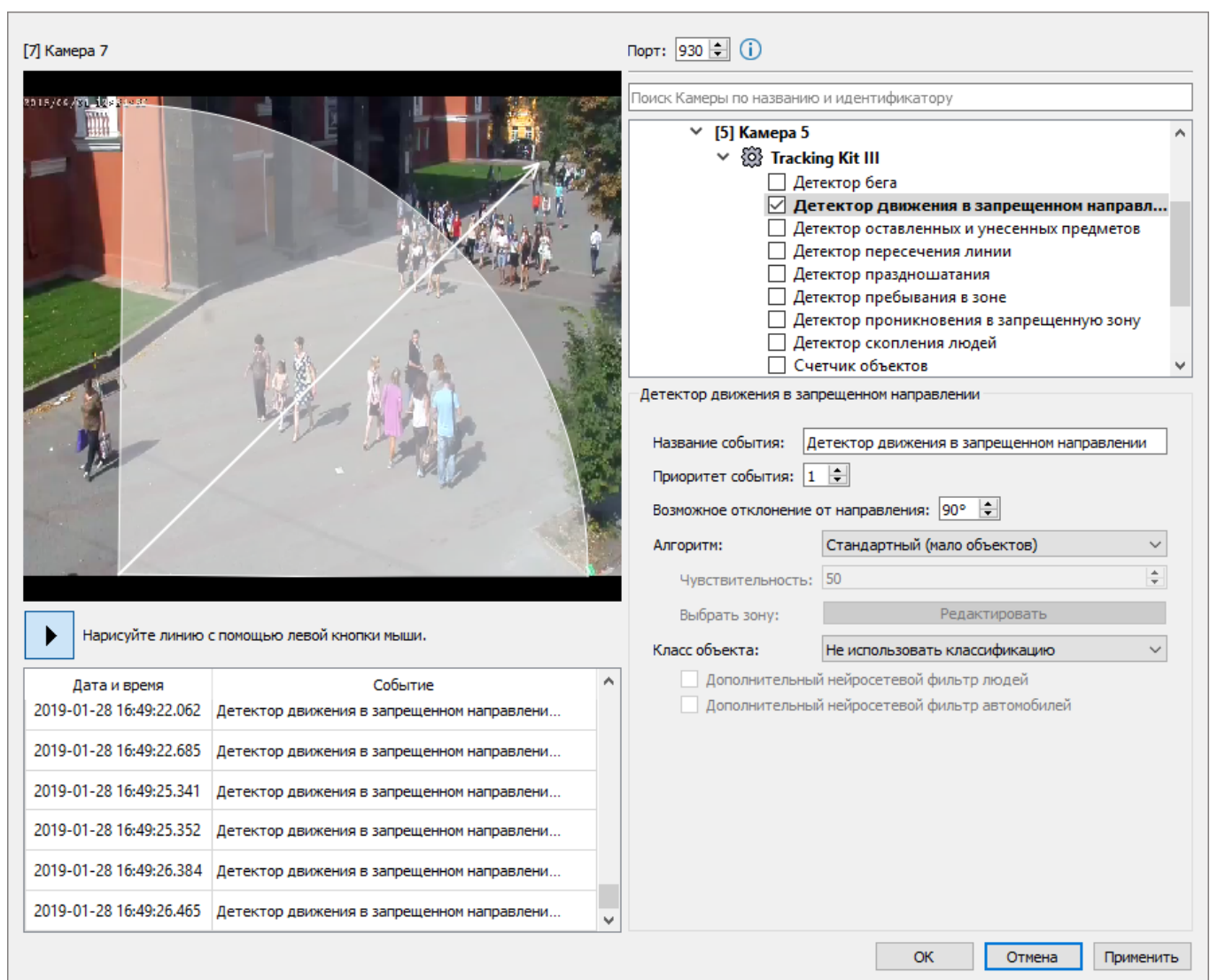


Рис. 258. Окно настройки параметров Детектора движения в запрещенном направлении

Таблица 87. Параметры Детектора движения в запрещенном направлении

Параметр	Описание
Название события	Задайте название события, которое будет отправляться в <i>Протокол событий</i> при обнаружении объекта, движущегося в запрещенном направлении.
Приоритет события	Задайте приоритет события данного детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения.
Возможное отклонение от направления	Задайте сектор отклонения (в градусах) от заданного вектора запрещенного направления, в пределах которого будет считаться, что объект также движется в запрещенном направлении.
Алгоритм	В зависимости от контролируемой сцены выберите требуемый алгоритм детектирования. Возможные значения: - Стандартный (мало объектов) — количество объектов в кадре мало. Объекты визуально разделимы; - Продвинутый (толпа) — количество объектов в кадре велико. Объекты визуально неразделимы.
Класс объекта	Выберите из списка класс контролируемого объекта. Возможные значения: - Не использовать классификацию — анализироваться будут все объекты; - Автомобиль — анализироваться будут только объекты, классифицированные как "автомобиль"; - Человек — анализироваться будут только объекты, классифицированные как "человек"; - Автомобиль и человек — анализироваться будут только объекты, классифицированные как "автомобиль" или "человек".
Дополнительный нейросетевой фильтр людей	Отметьте флажок, чтобы использовать дополнительный нейросетевой фильтр. Применение фильтра снижает количество ложных срабатываний детектора, но приводит к повышению вычислительной нагрузки. Доступен в случае, если параметр Класс объекта принимает значение Человек или Автомобиль и человек. Примечание. Для работы фильтра необходимо дополнительно установить OpenVINOServer. За подробной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems.

Параметр	Описание
Дополнительный нейросетевой фильтр автомобилей	Отметьте флажок, чтобы использовать дополнительный нейросетевой фильтр. Применение фильтра снижает количество ложных срабатываний детектора, но приводит к повышению вычислительной нагрузки.
	Доступен в случае, если параметр Класс объекта принимает значение Автомобиль или Автомобиль и человек. Примечание. Для работы фильтра необходимо дополнительно установить OpenVINOServer. За подробной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems.
Указанные ниже параметры доступны только для Алгоритма Продвинутой толпы	
Чувствительность	Задайте чувствительность алгоритма детектирования. При этом, если заданное значение параметра: • лежит в нижней области диапазона — количество ложных срабатываний детектора минимально, но при этом повышается вероятность пропуска событий детектирования; • лежит в средней области диапазона (значение по умолчанию 50) — детектор работает в оптимальном режиме, при котором количество ложных срабатываний детектора сбалансировано с вероятностью пропуска событий детектирования; • лежит в верхней области диапазона — количество пропущенных событий детектирования минимально, но при этом повышается вероятность ложных срабатываний детектора.
Выбрать зону	Задайте в кадре <i>Зону контроля</i> , внутри которой будет применен алгоритм детектирования Продвинутой толпы . Описание порядка настройки зоны приведено в разделе Настройка контролируемой зоны .

Для настройки детектора необходимо задать вектор запрещенного направления движения и угол допустимого отклонения, в пределах которого направление движения также будет считаться запрещенным. Угол отображается автоматически, в зависимости от заданного значения параметра **Возможное отклонение от направления** (см. рис. 258).

Чтобы задать запрещенное направление движения, поместите указатель мыши в требуемую точку кадра и нажмите левую кнопку. Удерживая кнопку нажатой, проведите линию в требуемом направлении. На кадр будет нанесена линия со стрелкой, указывающей запрещенное направление движения, и угол допустимого отклонения от него. Информация об объектах, движущихся в заданном направлении, будет выводиться в поле **Комментарий Протокола событий**.

14.2.2.2.3.1 Настройка перспективы для Детектора движения в запрещенном направлении

Если в настройках детектора параметр **Алгоритм** принимает значение **Продвинутый (толпа)**, настройка перспективы для *Детектора движения в запрещенном направлении* является рекомендуемой.

В Таблице 88 приведены возможные методы рекомендуемой настройки перспективы.

Таблица 88. Методы настройки перспективы для Детектора движения в запрещенном направлении. Рекомендуемая настройка

Параметр Угол обзора Камеры	Параметр Расположение Камеры	Метод настройки перспективы
80–170 градусов	Под углом	По двум размерам объекта — вблизи и на удалении от камеры
	Вид сверху	По одному размеру объекта
	Горизонтальное	По одному размеру объекта
360 градусов	Под углом	По двум размерам объекта — вблизи и на удалении от камеры
	Вид сверху	По двум размерам объекта — вблизи и на удалении от камеры
	Горизонтальное	По одному размеру объекта

14.2.2.2.4 Детектор оставленных и унесенных предметов

Детектор предназначен для выявления предметов, оставленных в поле зрения камеры или унесенных из нее. Под оставленным предметом понимается объект, который отделился от какого-либо из отслеживаемых трекером движущихся объектов и после этого оставался в контролируемой зоне неподвижным. Под унесенным предметом понимается объект, исчезнувший из поля зрения камеры. При этом подразумевается, что до момента исчезновения данный предмет считался фоном контролируемой зоны. Контролируемая зона и режим работы детектора являются настраиваемыми параметрами детектора.

Примечание. Объект считается находящимся в контролируемой зоне, если площадь пересечения объекта и контролируемой зоны составляет не менее 50% от вычисленной площади обнаруженного объекта.

Линейные размеры оставленного/унесенного предмета должны составлять не менее 5% от размеров кадра. Для достижения наилучших показателей работы данного детектора необходимо обеспечить такой ракурс, при котором возможность взаимных перекрытий объектов будет минимальна (движущиеся объекты не должны заслонять оставленный предмет). Таким образом, оптимальным является ракурс "вид сверху". Вид в перспективе (под углом) также допускается при установке камеры на достаточно большой высоте и направленности ее оптической оси вниз под достаточно острым углом. Однако при ракурсе "под углом" наиболее надежным окажется обнаружение оставленных/унесенных предметов в ближней зоне видеонаблюдения, в то время как в дальней зоне уже будут иметь место существенные взаимные перекрытия отслеживаемых объектов.

Существенным условием для надежной работы детектора является стабильное хорошее освещение, что достижимо в первую очередь внутри помещений. В условиях уличного видеонаблюдения возможно увеличение количества ложных срабатываний.

Окно настройки параметров *Детектора оставленных и унесенных предметов* представлено на рис. 259.

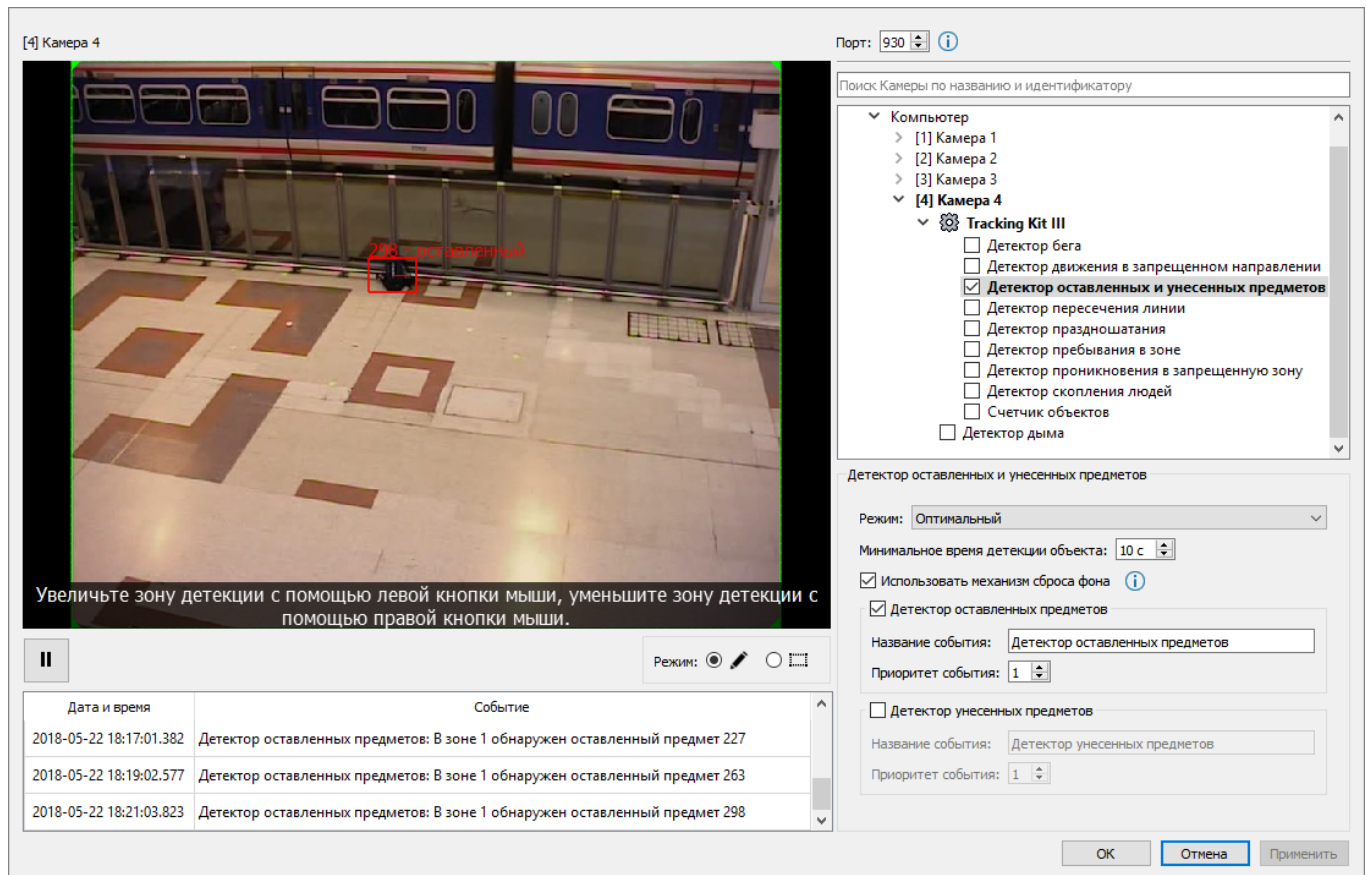


Рис. 259. Окно настройки параметров Детектора оставленных и унесенных предметов

Таблица 89. Параметры Детектора оставленных и унесенных предметов

Параметр	Описание
Режим	Выберите требуемый режим работы детектора: - Оптимальный — оптимальный режим, при котором количество ложных срабатываний детектора сбалансировано с вероятностью пропуска событий детектирования; - Минимизация ложных срабатываний — количество ложных срабатываний детектора минимально, но при этом повышается вероятность пропуска событий детектирования; - Минимизация пропущенных событий — количество пропущенных событий детектирования минимально, но при этом повышается вероятность ложных срабатываний детектора.

Параметр	Описание
Минимальное время детекции объекта	Задайте длительность периода (в секундах), при превышении которого предмет будет считаться оставленным/унесенным: - для оставленных предметов — время нахождения объекта в контролируемой зоне с момента его появления. При этом объект должен оставаться неподвижным в течение указанного времени; - для унесенных предметов — время, прошедшее после исчезновения объекта из контролируемой зоны. При этом считается, что до момента исчезновения объект являлся частью фона. Внимание! Если заданное значение параметра превышает значение параметра Не учитывать объекты, неподвижные более (см. Закладка Трекер), объект не будет определяться как оставленный.
Использовать механизм сброса фона	Отметьте флажок, чтобы избежать ложных срабатываний детектора на рябящих поверхностях (песок, листья и т.д.).
Детектор оставленных предметов	Отметьте флажок, чтобы выявлять предметы, оставленные в контролируемой зоне.
Название события	Задайте название события, которое будет фиксироваться в <i>Протоколе событий</i> , если предмет находится в контролируемой зоне дольше установленного времени.
Приоритет события	Задайте приоритет события данного детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения.
Детектор унесенных предметов	Отметьте флажок, чтобы выявлять предметы, унесенные из контролируемой зоны. По умолчанию снят.
Название события	Задайте название события, которое будет фиксироваться в <i>Протоколе событий</i> , если предмет исчезает из поля зрения камеры.
Приоритет события	Задайте приоритет события данного детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения.

14.2.2.2.5 Детектор пересечения линии

Детектор предназначен для подсчета объектов, пересекающих линию контроля. Подсчитывается общее количество пересечений линии независимо от направления движения объекта. Поддерживается работа с несколькими линиями контроля. В этом случае подсчет ведется как отдельно, для каждой линии, так и суммарно, для всех линий детектора.

Наибольшая точность подсчета достигается при хорошем контрасте объекта и фона. В плохую погоду при наличии воды на асфальте могут возникать локальные помехи, мешающие детектированию объектов, вследствие чего срабатывание детектора может не произойти.

Окно настройки параметров *Детектора пересечения линии* представлено на рис. 260.

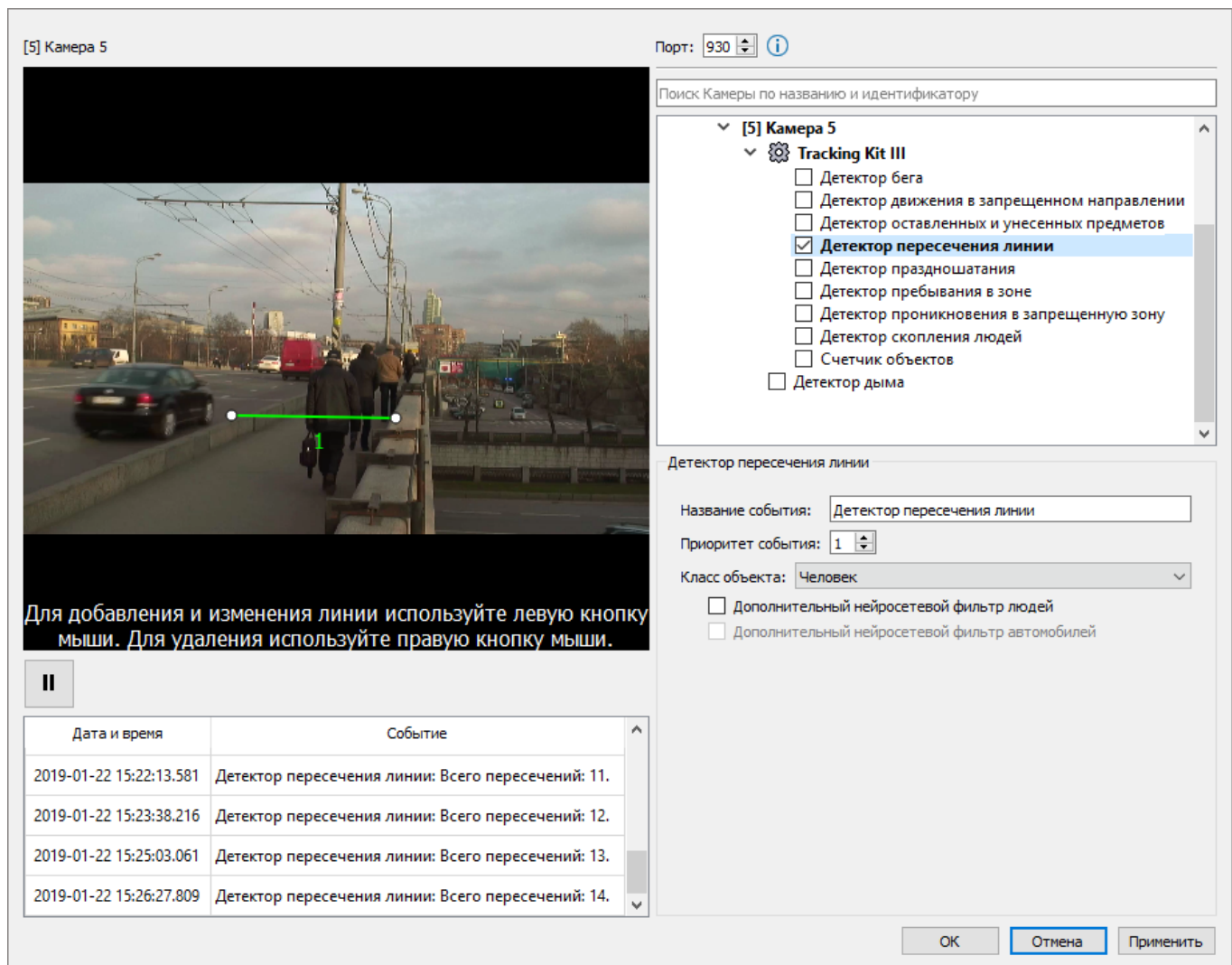


Рис. 260. Окно настройки параметров Детектора пересечения линии

Таблица 90. Параметры Детектора пересечения линии

Параметр	Описание
Название события	Задайте название события, которое будет отправляться в <i>Протокол событий</i> при пересечении объектом линии контроля.

Параметр	Описание
Приоритет события	Задайте приоритет события данного детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения.
Класс объекта	Выберите из списка класс контролируемого объекта. Возможные значения: • Не использовать классификацию — анализироваться будут все объекты; • Автомобиль — анализироваться будут только объекты, классифицированные как "автомобиль"; • Человек — анализироваться будут только объекты, классифицированные как "человек"; • Автомобиль и человек — анализироваться будут только объекты, классифицированные как "автомобиль" или "человек".
Дополнительный нейросетевой фильтр людей	Отметьте флажок, чтобы использовать дополнительный нейросетевой фильтр. Применение фильтра снижает количество ложных срабатываний детектора, но приводит к повышению вычислительной нагрузки. Доступен в случае, если параметр Класс объекта принимает значение Человек или Автомобиль и человек. Примечание. Для работы фильтра необходимо дополнительно установить OpenVINOServer. За подробной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems.
Дополнительный нейросетевой фильтр автомобилей	Отметьте флажок, чтобы использовать дополнительный нейросетевой фильтр. Применение фильтра снижает количество ложных срабатываний детектора, но приводит к повышению вычислительной нагрузки. Доступен в случае, если параметр Класс объекта принимает значение Автомобиль или Автомобиль и человек. Примечание. Для работы фильтра необходимо дополнительно установить OpenVINOServer. За подробной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems.

Для настройки счетчика необходимо задать одну или несколько *Линий контроля*. При этом определяться будут объекты заданного класса, которые пересекают заданную *Линию контроля* и размер которых лежит в пределах, указанных в глобальных настройках плагина (см. [Закладка Сцена](#)).

Внимание! Максимальное количество *Линий контроля* ограничено.

Чтобы нанести *Линию контроля* на изображение, поместите курсор мыши в требуемую точку кадра и нажмите левую кнопку. Удерживая кнопку нажатой, проведите линию в требуемом направлении. Линия будет нанесена на кадр. Информация о суммарном количестве объектов будет выводиться в поле **Комментарий Протокола событий**.

Для удаления линии щелкните линию правой кнопкой мыши, в контекстном меню выберите команду **Удалить линию**.

Примечание. Последнюю оставшуюся в кадре линию удалить невозможно.

14.2.2.2.6 Детектор праздношатания

Под праздношатанием понимается нахождение объекта внутри контролируемой зоны в течение заданного времени. Контролируемая зона и пороговое значение времени являются настраиваемыми параметрами детектора. Объекты, отвечающие условиям детектирования, будут отмечены рамкой красного цвета.

Необходимо задать граничные размеры объектов и обеспечить отсутствие в зоне контроля предметов, которые могут загораживать детектируемые объекты. Для достижения наилучших показателей работы данного детектора (в особенности для сложных сцен, где возможно одновременное нахождение большого числа объектов) требуется использование ракурса "вид сверху". Для сцен с заведомо небольшим количеством объектов также допускается использование вида в перспективе (под углом), но только при установке камеры на достаточно большой высоте и направленности ее оптической оси вниз под достаточно острым углом.

Окно настройки параметров *Детектора праздношатания* представлено на рис. 261.

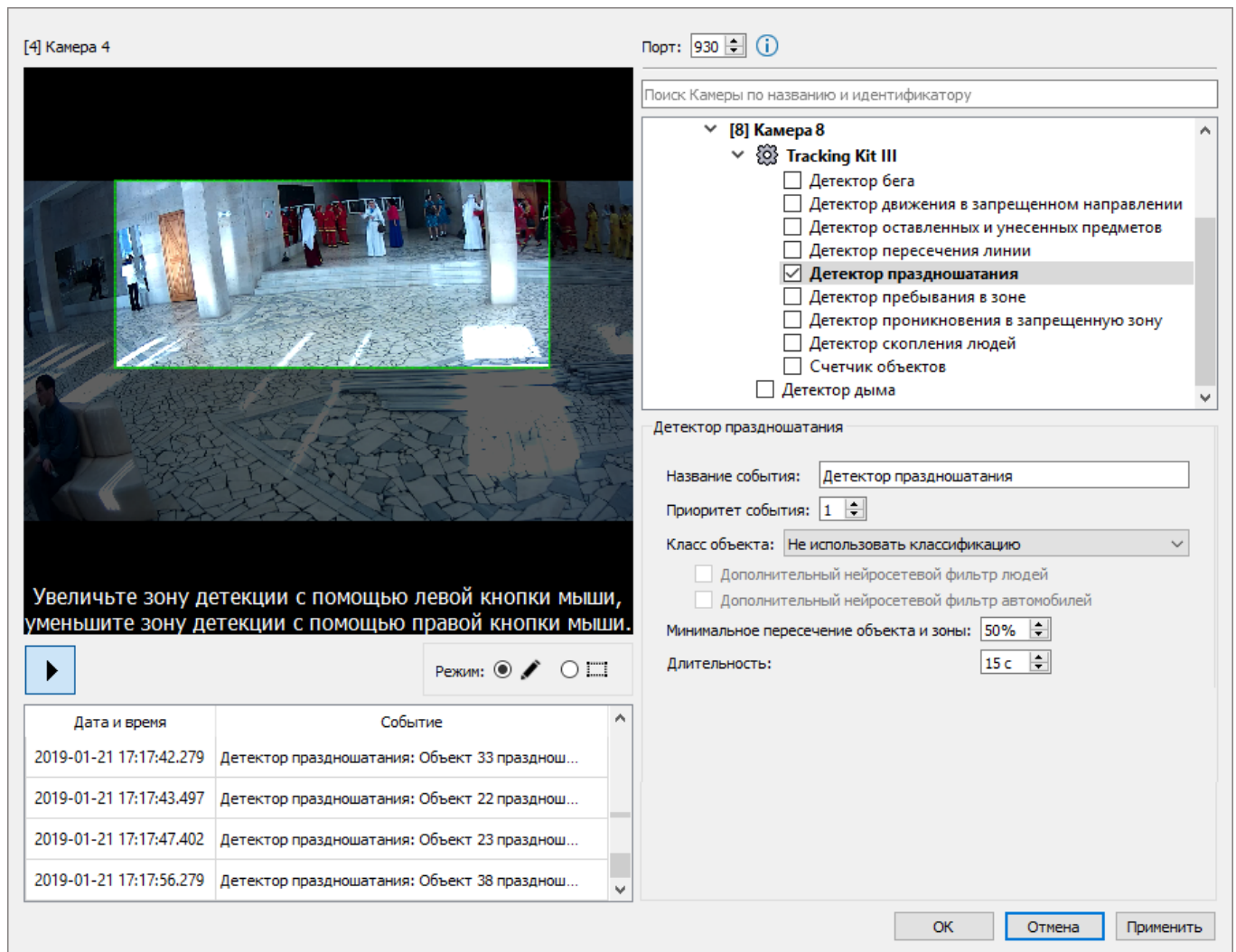


Рис. 261. Окно настройки параметров Детектора празднования

Таблица 91. Параметры Детектора празднования

Параметр	Описание
Название события	Задайте название события, которое будет отправляться в <i>Протокол событий</i> , если объект находится внутри контролируемой зоны в течение заданного времени.
Приоритет события	Задайте приоритет события данного детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения.

Параметр	Описание
Класс объекта	Выберите из списка класс контролируемого объекта. Возможные значения: • Не использовать классификацию — анализироваться будут все объекты; • Автомобиль — анализироваться будут только объекты, классифицированные как "автомобиль"; • Человек — анализироваться будут только объекты, классифицированные как "человек"; • Автомобиль и человек — анализироваться будут только объекты, классифицированные как "автомобиль" или "человек".
Дополнительный нейросетевой фильтр людей	Отметьте флажок, чтобы использовать дополнительный нейросетевой фильтр. Применение фильтра снижает количество ложных срабатываний детектора, но приводит к повышению вычислительной нагрузки. Доступен в случае, если параметр Класс объекта принимает значение Человек или Автомобиль и человек. Примечание. Для работы фильтра необходимо дополнительно установить OpenVINOServer. За подробной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems.
Дополнительный нейросетевой фильтр автомобилей	Отметьте флажок, чтобы использовать дополнительный нейросетевой фильтр. Применение фильтра снижает количество ложных срабатываний детектора, но приводит к повышению вычислительной нагрузки. Доступен в случае, если параметр Класс объекта принимает значение Автомобиль или Автомобиль и человек. Примечание. Для работы фильтра необходимо дополнительно установить OpenVINOServer. За подробной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems.
Минимальное пересечение объекта и зоны	Задайте площадь пересечения объекта и контролируемой зоны (в процентах от вычисленной площади обнаруженного объекта), при превышении которой объект будет считаться находящимся в контролируемой зоне.
Длительность	Задайте время нахождения объекта внутри контролируемой зоны (в секундах), при превышении которого объект будет считаться праздношатающимся.

14.2.2.2.7 Детектор пребывания в зоне

Детектор предназначен для предоставления статистических данных о длительном/кратковременном пребывании людей в определенном месте. Контролируемая зона и порог кратковременного/длительного пребывания в зоне являются настраиваемыми параметрами детектора. Поддерживается работа с одной прямоугольной или несколькими полигональными зонами (подробнее см. раздел [Настройка контролируемой зоны](#)).

Объект должен непрерывно распознаваться на протяжении всего времени пребывания в зоне.

Необходимо задать граничные размеры объектов или обеспечить отсутствие останавливающихся транспортных средств в зоне контроля. Для достижения наилучших показателей работы данного детектора (в особенности для сложных сцен, где возможно одновременное нахождение большого числа людей) требуется использование ракурса "вид сверху". Количество ложных срабатываний может возрастать при наличии сильных (и в особенности длинных) теней, а также в темное время суток при наличии световых бликов (например, от фар автомобилей).

Наибольшая точность подсчета достигается при достижении хорошего контраста объекта и фона. В плохую погоду при наличии воды на асфальте могут возникать локальные помехи мешающие детектированию объектов, вследствие чего срабатывание детектора может не произойти.

Окно настройки параметров *Детектора пребывания в зоне* представлено на рис. 262.

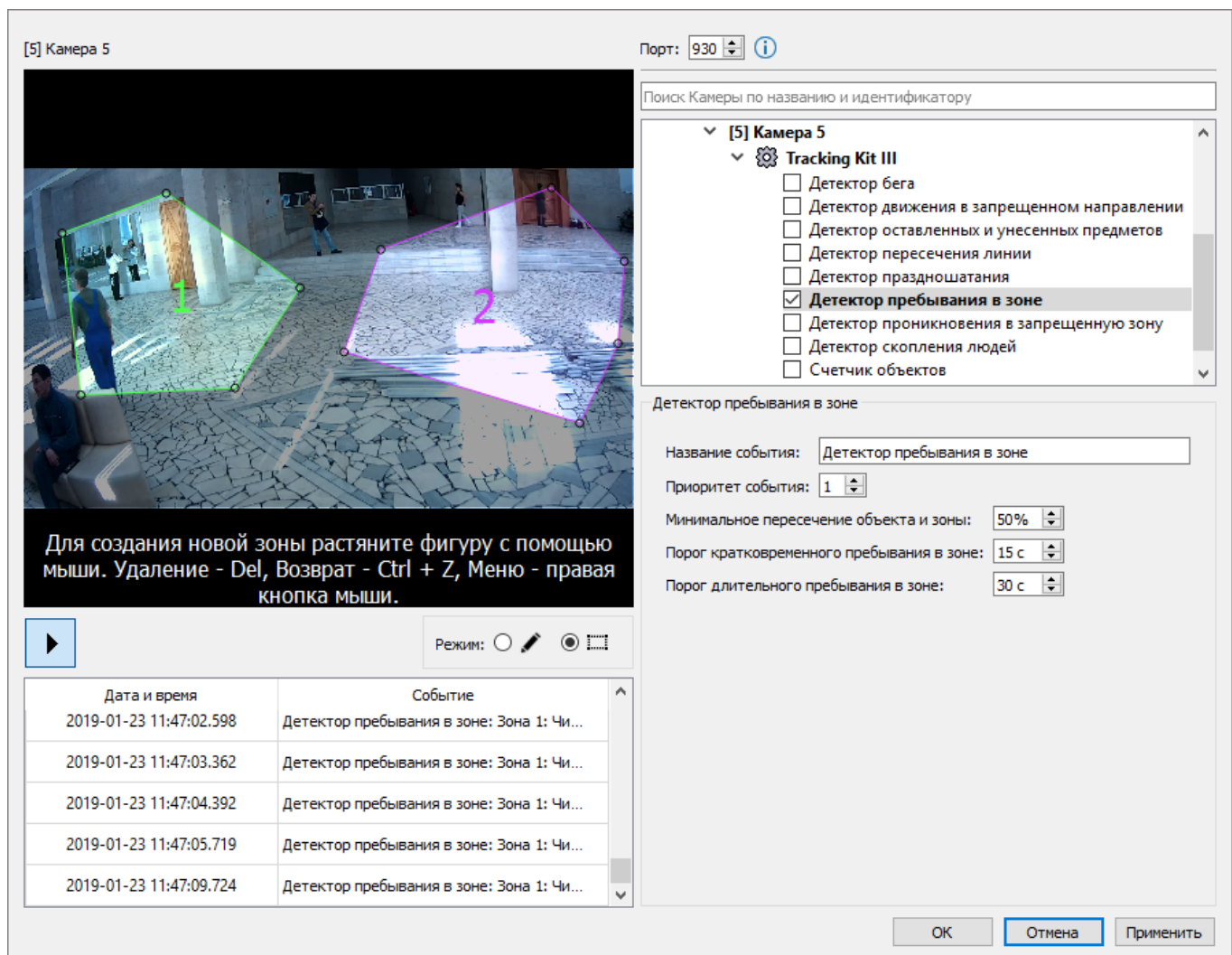


Рис. 262. Окно настройки параметров Детектора пребывания в зоне

Таблица 92. Параметры Детектора пребывания в зоне

Параметр	Описание
Название события	Задайте название события, которое будет отправляться в <i>Протокол событий</i> при превышении порогов пребывания в зоне.
Приоритет события	Задайте приоритет события данного детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения.
Минимальное пересечение объекта и зоны	Задайте площадь пересечения объекта и контролируемой зоны (в процентах от вычисленной площади обнаруженного объекта), при превышении которой объект будет считаться находящимся в контролируемой зоне.
Порог кратковременного пребывания в зоне	Задайте длительность нахождения объекта в зоне (в секундах), при превышении которой пребывание объекта в зоне будет считаться <i>Кратковременным</i> .
Порог длительного пребывания в зоне	Задайте длительность нахождения объекта в зоне (в секундах), при превышении которой пребывание объекта в зоне будет считаться <i>Длительным</i> .

Для настройки детектора необходимо задать одну или несколько *Зон контроля*. Выбирать большие по площади зоны не рекомендуется. Если задано несколько зон контроля, подсчет количества объектов ведется независимо для каждой из зон.

В результате работы детектора в протокол выводится следующая информация:

- Количество объектов, находящихся в зоне в течение короткого периода времени на момент события.
- Общее количество объектов, находившихся в зоне в течение короткого периода времени с начала работы детектора.
- Количество объектов, находящихся в зоне в течение длительного периода времени на момент события.
- Общее количество объектов, находившихся в зоне в течение длительного периода времени с начала работы детектора.

14.2.2.2.8 Детектор проникновения в запрещенную зону

Под проникновением в запрещенную зону понимается перемещение (проезд, проход) отслеживаемого объекта внутрь контролируемой зоны. Контролируемая зона и класс вызывающего тревогу объекта (человек, транспортное средство, животное) являются настраиваемыми параметрами детектора.

Для достижения наилучших показателей работы данного детектора рекомендуется использование ракурса "вид сверху" либо "под углом" (но при установке камеры на достаточно большой высоте и направленности ее оптической оси вниз под достаточно острым углом). Иными словами, необходимо обеспечить такой ракурс, при котором объекты переднего плана не будут закрывать собой контролируруемую зону.

Количество ложных срабатываний может возрастать при наличии сильных (и в особенности длинных) теней, а также в темное время суток при наличии световых бликов (например, от фар автомобилей).

Окно настройки параметров *Детектора проникновения в запрещенную зону* представлено на рис. 263.

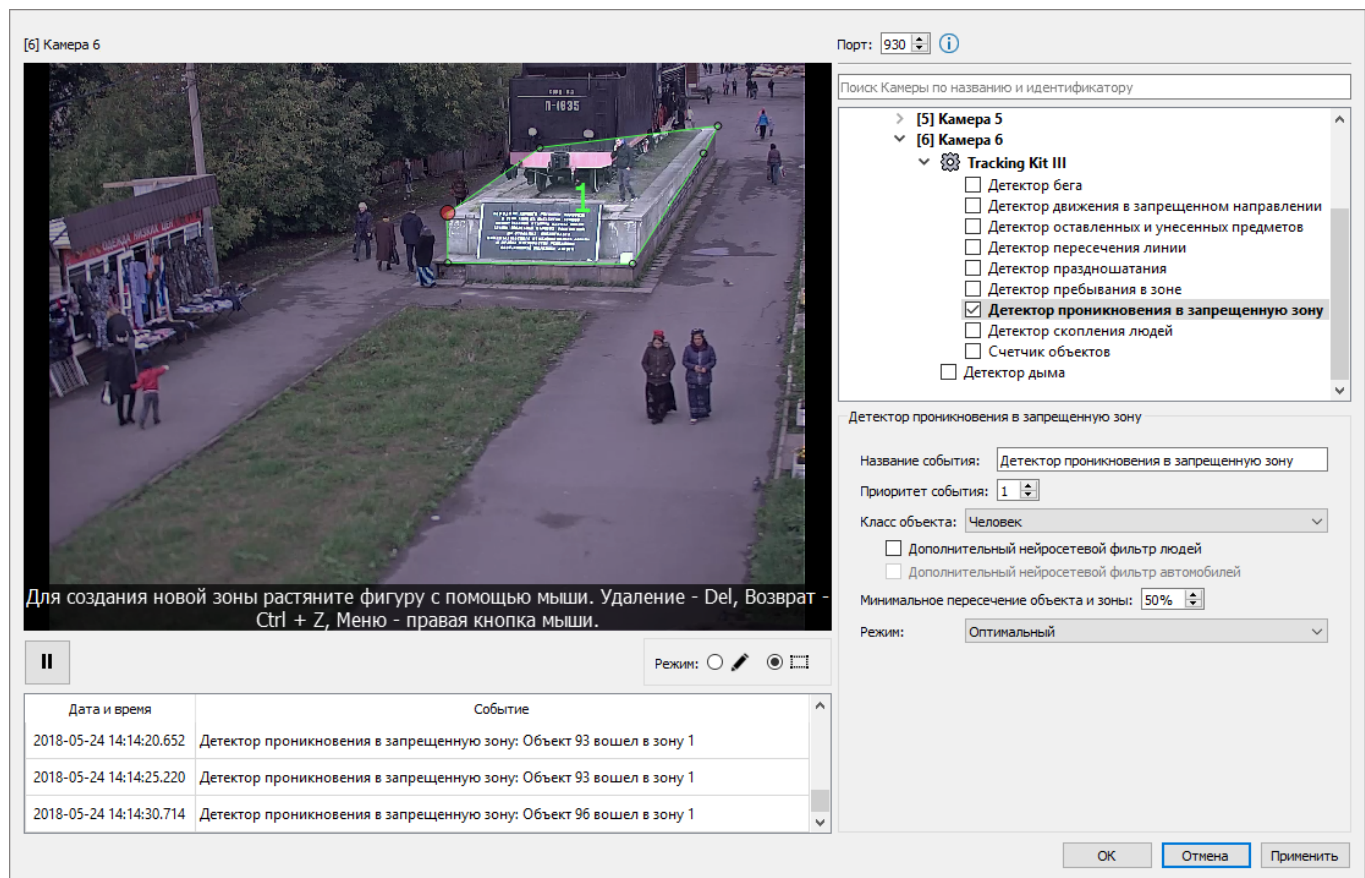


Рис. 263. Окно настройки параметров Детектора проникновения в запрещенную зону

Таблица 93. Параметры Детектора проникновения в запрещенную зону

Параметр	Описание
Название события	Задайте название события, которое будет фиксироваться в <i>Протоколе событий</i> , если объект выбранного класса пересек границу запрещенной зоны.
Приоритет события	Задайте приоритет события данного детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения.

Параметр	Описание
Класс объекта	Выберите из списка класс контролируемого объекта. Возможные значения: • Не использовать классификацию — анализироваться будут все объекты; • Автомобиль — анализироваться будут только объекты, классифицированные как "автомобиль"; • Человек — анализироваться будут только объекты, классифицированные как "человек"; • Автомобиль и человек — анализироваться будут только объекты, классифицированные как "автомобиль" или "человек"; • Животное — анализироваться будут только объекты, классифицированные как "животное".
Дополнительный нейросетевой фильтр людей	Отметьте флажок, чтобы использовать дополнительный нейросетевой фильтр. Применение фильтра снижает количество ложных срабатываний детектора, но приводит к повышению вычислительной нагрузки. Доступен в случае, если параметр Класс объекта принимает значение Человек или Автомобиль и человек. Примечание. Для работы фильтра необходимо дополнительно установить OpenVINOServer. За подробной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems.
Дополнительный нейросетевой фильтр автомобилей	Отметьте флажок, чтобы использовать дополнительный нейросетевой фильтр. Применение фильтра снижает количество ложных срабатываний детектора, но приводит к повышению вычислительной нагрузки. Доступен в случае, если параметр Класс объекта принимает значение Автомобиль или Автомобиль и человек. Примечание. Для работы фильтра необходимо дополнительно установить OpenVINOServer. За подробной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems.
Минимальное пересечение объекта и зоны	Задайте площадь пересечения объекта и контролируемой зоны (в процентах от вычисленной площади обнаруженного объекта), при превышении которой объект будет считаться находящимся в контролируемой зоне.

Параметр	Описание
Режим	Выберите требуемый режим работы детектора: • Оптимальный — оптимальный режим, при котором количество ложных срабатываний детектора сбалансировано с вероятностью пропуска событий детектирования; • Минимизация ложных срабатываний — количество ложных срабатываний детектора минимально, но при этом повышается вероятность пропуска событий детектирования; • Минимизация пропущенных событий — количество пропущенных событий детектирования минимально, но при этом повышается вероятность ложных срабатываний детектора.

14.2.2.2.9 Детектор скопления людей

Под скоплением людей понимается одновременное нахождение в зоне определенного количества людей в течение фиксированного интервала времени. При этом геометрия зоны, пороговое число людей и временной интервал являются настраиваемыми параметрами детектора.

В контролируемой зоне крайне нежелательно перемещение транспортных средств. Наиболее высокое качество работы детектора достигается если камера установлена сверху контролируемой зоны (ракурс камеры "вид сверху"). Вид в перспективе (под углом) допускается, но только при установке камеры на достаточно большой высоте и направленности ее оптической оси вниз под достаточно острым углом.

Окно настройки параметров *Детектора скопления людей* представлено на рис. 264.

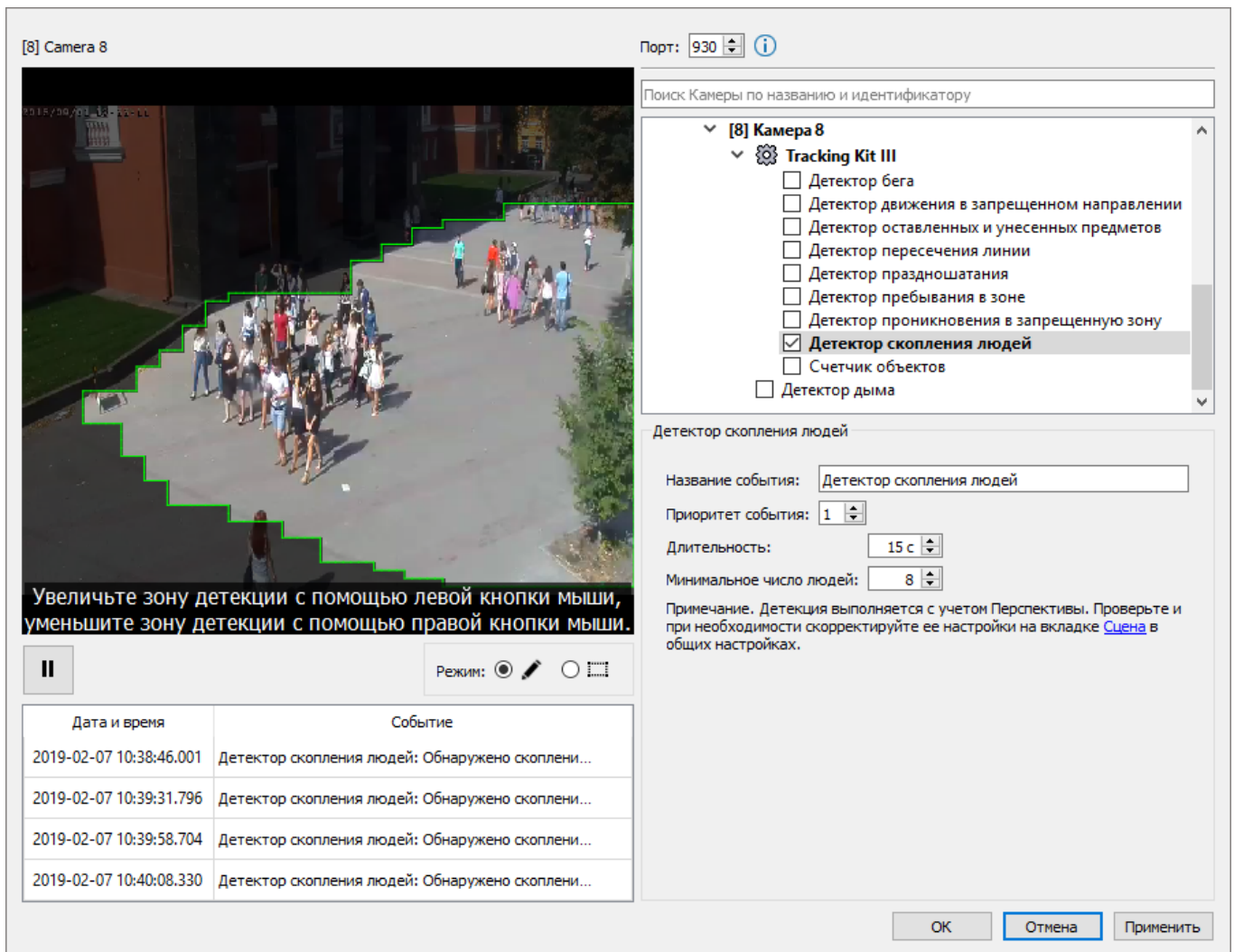


Рис. 264. Окно настройки параметров Детектора скопления людей

Таблица 94. Параметры детектора скопления людей

Параметр	Описание
Название события	Задайте название события, которое будет фиксироваться в <i>Протоколе событий</i> , если обнаружено скопление людей, находящихся в контролируемой зоне дольше установленного времени.
Приоритет события	Задайте приоритет события данного детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения.
Длительность	Задайте время нахождения группы людей в контролируемой зоне (в секундах), при превышении которого произойдет срабатывание детектора.
Минимальное число людей	Задайте минимальное количество людей в группе, при превышении которого данная группа будет считаться скоплением.

Внимание! Для работы детектора необходимо настроить перспективу (см. [Закладка Сцена](#)).

14.2.2.2.9.1 Настройка перспективы для Детектора скопления людей

В зависимости от значения параметров **Угол обзора Камеры** и **Расположение Камеры** настройка перспективы для *Детектора скопления людей* является обязательной либо рекомендуемой.

В Таблице 95 приведены возможные методы обязательной настройки перспективы.

Внимание! Для указанных значений параметров перспектива будет учитываться автоматически (флажок **Учитывать перспективу** автоматически отмечается и блокируется).

Таблица 95. Методы настройки перспективы для Детектора скопления людей. Обязательная настройка

Параметр Угол обзора Камеры	Параметр Расположение Камеры	Метод настройки перспективы
80–170 градусов	Под углом	По двум размерам объекта — вблизи и на удалении от камеры
	Горизонтальное	По одному размеру объекта
360 градусов	Под углом	По двум размерам объекта — вблизи и на удалении от камеры
	Вид сверху	По двум размерам объекта — вблизи и на удалении от камеры
	Горизонтальное	По одному размеру объекта

В Таблице 96 приведены возможные методы рекомендуемой настройки перспективы.

Таблица 96. Методы настройки перспективы для Детектора скопления людей. Рекомендуемая настройка

Параметр Угол обзора Камеры	Параметр Расположение Камеры	Метод настройки перспективы
80–170 градусов	Вид сверху	По одному размеру объекта

14.2.2.2.10 Счетчик объектов

Детектор предназначен для подсчета объектов, пересекающих линию контроля. Подсчет производится отдельно для объектов, пересекающих линию контроля в противоположных направлениях. Поддерживается работа с несколькими линиями контроля. В этом случае подсчет ведется как отдельно, для каждой линии, так и суммарно, для всех линий детектора.

Наибольшая точность подсчета достигается при использовании ракурса камеры "вид сверху". Вид в перспективе (под углом) допускается, но только при установке камеры на достаточно большой высоте и направленности ее оптической оси вниз под достаточно острым углом. Подсчет количества объектов будет корректным только в случае визуальной разделимости движущихся в кадре объектов. Иными словами, объекты не должны перекрывать друг друга либо двигаться в плотном потоке.

Окно настройки параметров *Счетчика объектов* представлено на рис. 265.

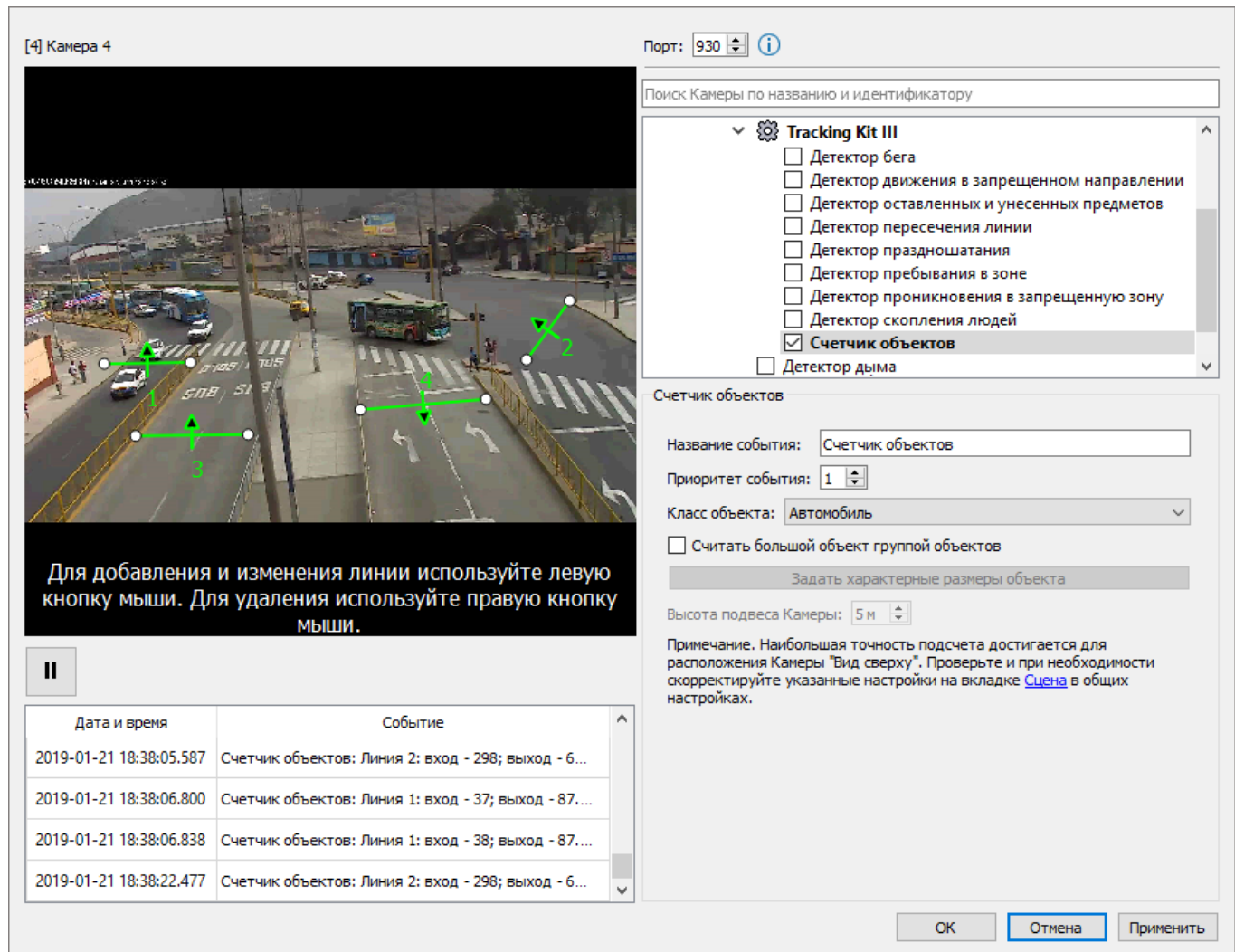


Рис. 265. Окно настройки параметров Счетчика объектов

Таблица 97. Параметры Счетчика объектов

Параметр	Описание
Название события	Задайте название события, которое будет отправляться в <i>Протокол событий</i> при пересечении объектом линии контроля.
Приоритет события	Задайте приоритет события данного детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения.

Параметр	Описание
Класс объекта	Выберите из списка класс контролируемого объекта. Возможные значения: • Не использовать классификацию — анализироваться будут все объекты; • Автомобиль — анализироваться будут только объекты, классифицированные как "автомобиль"; • Человек — анализироваться будут только объекты, классифицированные как "человек"; • Автомобиль и человек — анализироваться будут только объекты, классифицированные как "автомобиль" или "человек". Внимание! Если отмечен флажок Считать большой объект группой объектов (см. ниже) параметр не отображается.
Считать большой объект группой объектов	Отметьте данный флажок, если объекты в кадре нельзя разделить визуально. Если флажок отмечен, при подсчете количества объектов будет применен алгоритм деления большого объекта на отдельные.
Указанные ниже параметры доступны в случае, если отмечен флажок Считать большой объект группой объектов .	
Задать характерные размеры объекта	Нажмите на кнопку, чтобы задать характерные размеры объекта в кадре. Характерные размеры позволяют детектору отделять "большие" объекты от прочих отслеживаемых в кадре объектов. Если размер объекта в кадре будет превышать верхнюю границу заданного диапазона, такой объект будет считаться "большим". Метод задания характерных размеров объекта полностью аналогичен методу задания размеров отслеживаемых в кадре объектов (см. раздел Закладка Сцена, параметр Ограничение на размер объекта). Диапазон характерных размеров объекта должен лежать внутри диапазона размеров детектируемых объектов.
Высота подвеса Камеры	Укажите высоту подвеса <i>Камеры</i> над контролируемой сценой.

Для настройки счетчика необходимо задать одну или несколько *Линий контроля*. При этом определяться будут объекты заданного класса, которые пересекают заданную *Линию контроля* и размер которых лежит в пределах, указанных в глобальных настройках плагина (см. [Закладка Сцена](#)).

Внимание! Максимальное количество *Линий контроля* ограничено.

Чтобы нанести *Линию контроля* на изображение, поместите курсор мыши в требуемую точку кадра и нажмите левую кнопку. Удерживая кнопку нажатой, проведите линию в требуемом направлении. Линия будет нанесена на кадр. Входящее направление будет обозначено направленными стрелками. Объекты, пересекающие линию в данном направлении будут считаться "входящими", в обратном направлении - "исходящими". Подсчет "входящих" и "исходящих" объектов выполняется отдельно. Информация о количестве объектов каждого типа будет выводиться в поле **Комментарий Протокола событий**.

Примечание. Положение стрелок указания направления зависит от порядка нанесения линии контроля (слева-направо или справа-налево).

Для удаления линии щелкните линию правой кнопкой мыши, в контекстном меню выберите команду **Удалить линию**.

Примечание. Последнюю оставшуюся в кадре линию удалить невозможно.

14.2.2.2.10.1 Настройка перспективы для Счетчика объектов

Если в настройках детектора отмечен флажок **Считать большой объект группой объектов**, настройка перспективы для *Счетчика объектов* является рекомендуемой.

В Таблице 98 приведены возможные методы рекомендуемой настройки перспективы.

Таблица 98. Методы настройки перспективы для Счетчика объектов. Рекомендуемая настройка

Параметр Угол обзора Камеры	Параметр Расположение Камеры	Метод настройки перспективы
80–170 градусов	Под углом	По двум размерам объекта — вблизи и на удалении от камеры
	Вид сверху	По одному размеру объекта
	Горизонтальное	По одному размеру объекта
360 градусов	Под углом	По двум размерам объекта — вблизи и на удалении от камеры
	Вид сверху	По двум размерам объекта — вблизи и на удалении от камеры
	Горизонтальное	По одному размеру объекта

14.2.3 Настройка независимых видеоаналитических детекторов

В данном разделе приводится описание параметров и особенностей настройки независимых видеоаналитических детекторов.

14.2.3.1 Детектор дыма

Детектор предназначен для обнаружения дыма. Контролируемая зона и чувствительность являются настраиваемыми параметрами детектора.

В SecurOS каждой *Камере* соответствует отдельный экземпляр *Детектора дыма*, который настраивается независимо от плагина Tracking Kit III и его детекторов. Чтобы настроить детектор, отметьте флажок **Детектор дыма** в списке дочерних объектов настраиваемой камеры. Система активирует окно настройки параметров детектора (см. рис. 266).

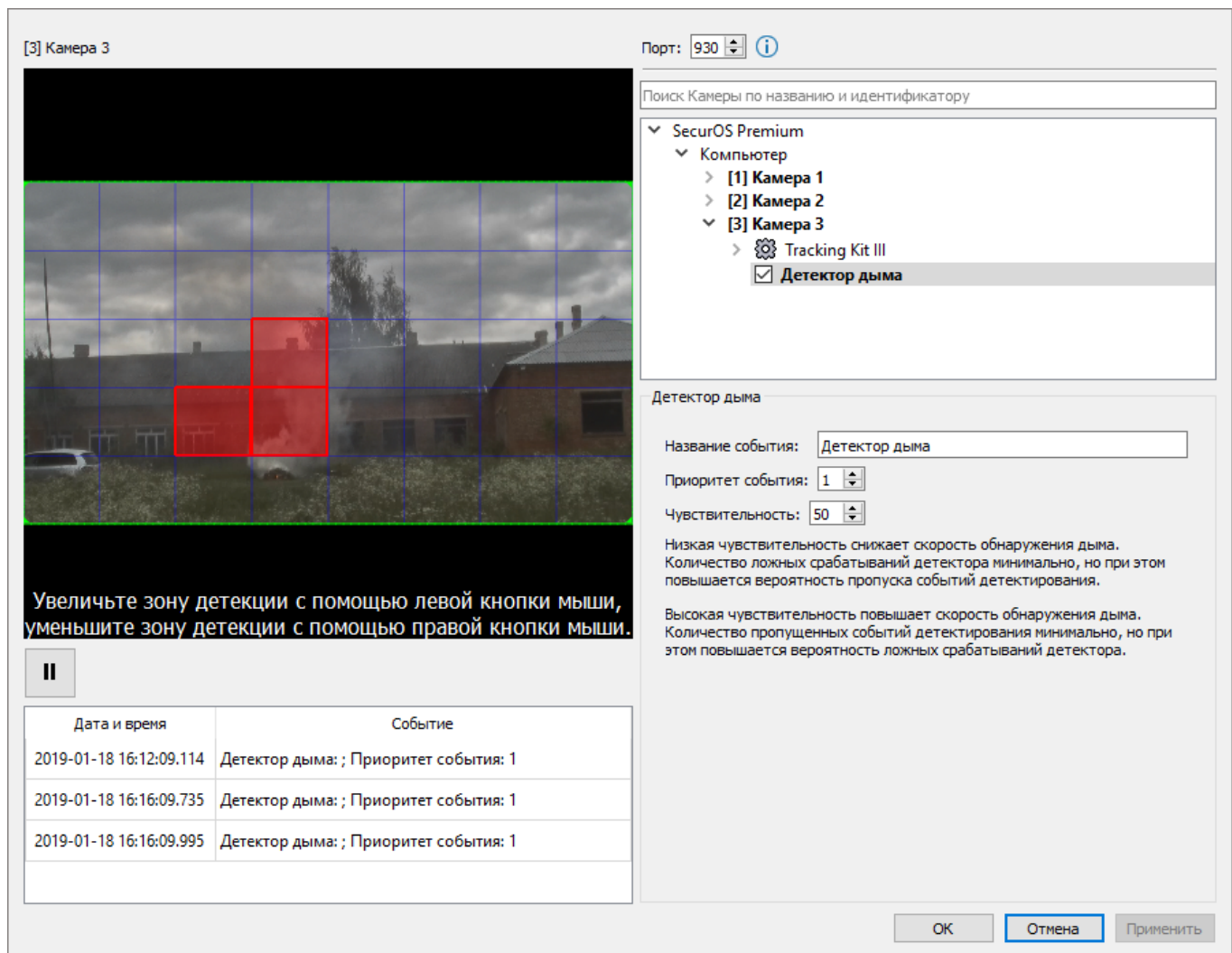


Рис. 266. Окно настройки параметров Детектора дыма

Таблица 99. Параметры Детектора дыма

Параметр	Описание
Название события	Задайте название события, которое будет отправляться в <i>Протокол событий</i> , если в контролируемой зоне обнаружен дым.
Приоритет события	Задайте приоритет события данного детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения.

Параметр	Описание
Чувствительность	Задайте чувствительность детектора (в относительных единицах). Чувствительность влияет на скорость срабатывания детектора при наступлении события обнаружения. Подробное описание алгоритма работы детектора в зависимости от заданного значения приведено на закладке настройки параметров.

Область детектирования может быть ограничена. Порядок настройки области описан в разделе **Настройка контролируемой зоны**.

14.2.3.1.1 Рекомендации по настройке камер для Детектора дыма

Ниже перечислены дополнительные требования и рекомендации к содержанию сцены, расположению камер и источников освещения при решении задачи обнаружения дыма. Несоблюдение указанных требований в большинстве случаев влечет за собой возникновение ложных срабатываний видеоаналитических детекторов или пропуск событий.

1. Минимальное разрешение кадров составляет 640x480 пикселей. Максимальное разрешение в целом не ограничено.
2. Минимальное значение FPS: 5 к/с. FPS потока должен быть стабилен, в противном случае корректная работа детекторов не гарантируется.
3. Минимальный размер области задымления должен составлять не менее 10% от линейных размеров кадра.

Прочие рекомендации по настройке и расположению камер см. в разделе **Общие рекомендации по настройке и расположению камер**.

14.2.3.2 Детектор людей без касок

Детектор предназначен для обнаружения людей без касок.

Поддерживается работа с одной прямоугольной зоной (подробнее см. раздел **Настройка контролируемой зоны**). Для корректной работы детектора объект должен непрерывно распознаваться на протяжении всего времени пребывания в *Зоне детекции*.

Внимание! Для работы детектора требуется дискретная видеокарта NVIDIA. В противном случае работа детектора невозможна.

В SecurOS каждой *Камере* соответствует отдельный экземпляр *Детектора людей без касок*, который настраивается независимо от плагина Tracking Kit III и его детекторов. Чтобы настроить детектор, отметьте флажок **Детектор людей без касок** в списке дочерних объектов настраиваемой камеры. Система активирует окно настройки параметров детектора (см. рис. 267).

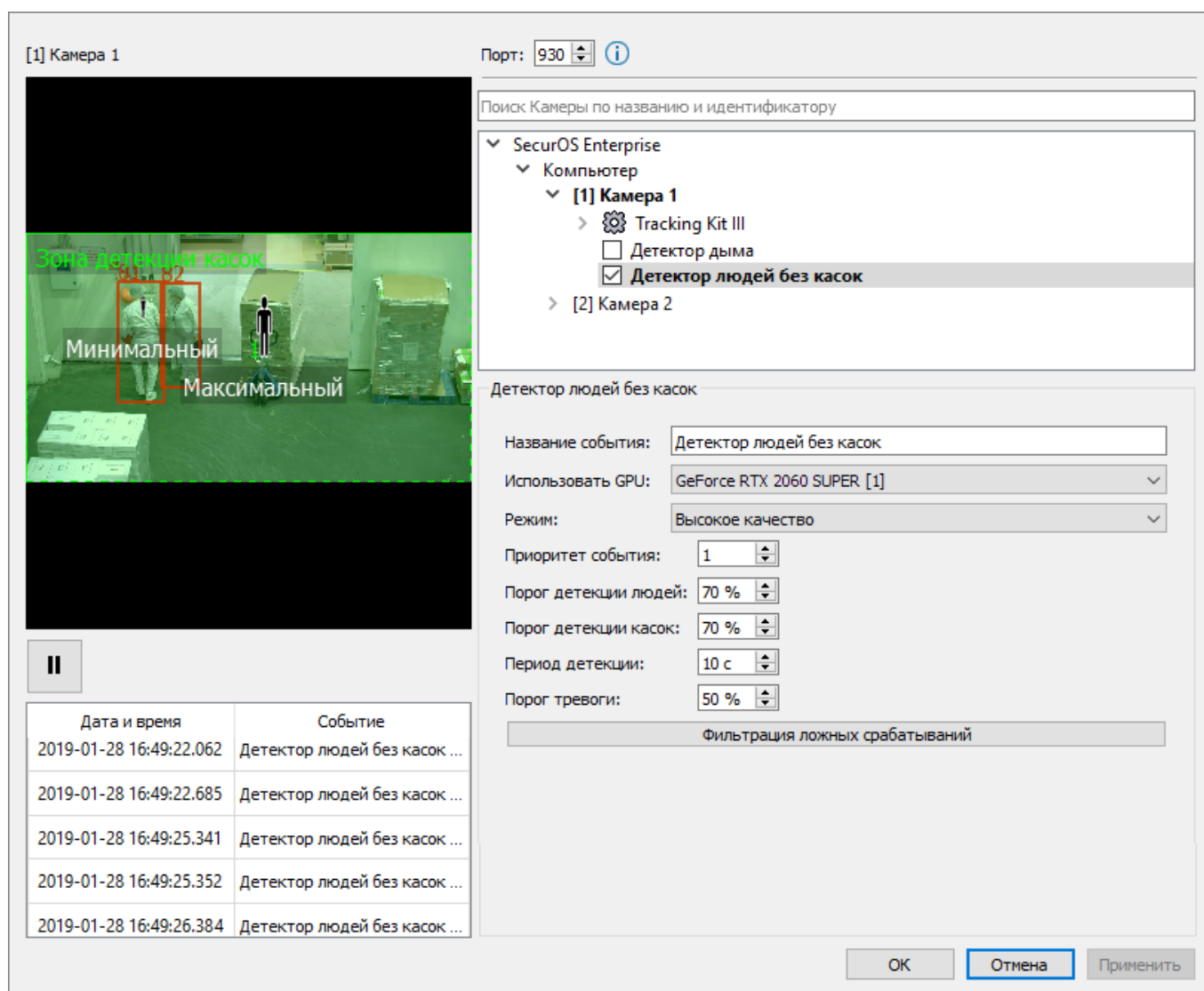


Рис. 267. Окно настройки параметров Детектора людей без касок

Таблица 100. Параметры Детектора людей без касок

Параметр	Описание
Название события	Задайте название события, которое будет отправляться в <i>Протокол событий</i> , если в контролируемой зоне обнаружен человек без каски.
Использовать GPU	Выберите из списка графический процессор, который будет использоваться для определения отсутствия касок с помощью нейросетевых алгоритмов.
Режим	Выберите режим определения отсутствия касок. Возможные значения: - Высокое качество; - Высокая скорость.

Параметр	Описание
Приоритет события	Задайте приоритет события данного детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения.
Порог детекции людей	Задайте минимальный коэффициент уверенности в том, что обнаруженный в кадре объект классифицируется как Человек. Если фактическая уверенность превысит заданное значение, будет достоверно считаться, что обнаруженный в кадре объект является Человеком. Диапазон возможных значений (в процентах): [1; 100]. По умолчанию принимает значение 70.
Порог детекции касок	Задайте минимальный коэффициент уверенности в том, что на обнаруженном в кадре человеке надета каска. Если фактическая уверенность превысит заданное значение, будет достоверно считаться, что обнаруженный в кадре объект Человек носит каску. Диапазон возможных значений (в процентах): [1; 100]. По умолчанию принимает значение 70.
Период детекции	Задайте длительность периода анализа наличия/отсутствия каски. На основании результата анализа этого периода будет приниматься решение о тревоге (см. описание параметра Порог тревоги). Примечание. Фактически алгоритм будет рассматривать то количество кадров, которое соответствует заданному временному промежутку. Диапазон возможных значений (в секундах): [1; 100]. По умолчанию принимает значение 10.
Порог тревоги	Доля кадров в анализируемом периоде (см. описание параметра Период детекции), на которых человек должен быть в каске. Если фактическое значение ниже заданного, детектор генерирует сообщение о тревоге. Диапазон возможных значений (в процентах): [1; 100]. По умолчанию принимает значение 50.

Параметр	Описание
Фильтрация ложных срабатываний (кнопка)	Нажмите кнопку и задайте одну или несколько зон, в которых будет выполняться фильтрация ложных срабатываний детектора. Примечание. Зоны фильтрации ложных срабатываний необходимо задавать в случае, если в области детектирования касок находится много статичных предметов (например, огнетушители или ящики с песком), на которые может реагировать детектор. Для каждого из таких предметов следует задать отдельную зону фильтрации.

Область детектирования может быть ограничена. Порядок настройки области описан в разделе **Настройка контролируемой зоны**. Для работы детектора также необходимо задать **Минимальный** и **Максимальный** размеры людей в *Зоне детекции*. Чем больше диапазон значений, и меньше **Минимальный** размер, тем больше вычислительных ресурсов требуется детектору.

В результате работы детектора в протокол выводится следующая информация:

- Тип нарушения.
- Дата и время нарушения.

14.2.3.2.1 Рекомендации по настройке камер для Детектора людей без касок

Ниже перечислены дополнительные требования и рекомендации к содержанию сцены, расположению камер и источников освещения при решении задачи обнаружения людей без касок. Несоблюдение указанных требований в большинстве случаев влечет за собой возникновение ложных срабатываний видеоаналитических детекторов или пропуск событий.

1. Минимальное разрешение кадров составляет 1920×1080 пикселей. Максимальное разрешение в целом не ограничено.
2. Минимальное значение FPS: 12 к/с. FPS потока должен быть стабилен, в противном случае корректная работа детектора не гарантируется.
3. Угол подвеса камеры: 30 — 70°.
4. Минимальный размер человека должен составлять не менее 10% по высоте от размера кадра.

Прочие рекомендации по настройке и расположению камер см. в разделе **Общие рекомендации по настройке и расположению камер**.

14.2.3.3 Нейросетевой детектор драк

Детектор предназначен для обнаружения драк.

Внимание! Для работы данного детектора необходимо установить OpenVINO Server. За подробной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems.

Чтобы настроить детектор, отметьте флажок **Нейросетевой детектор драк** в списке дочерних объектов *Камеры* (см. рис. 268). По умолчанию зона контроля размечена на весь кадр, но также поддерживается работа с несколькими зонами на кадре (см. **Настройка контролируемой зоны**).

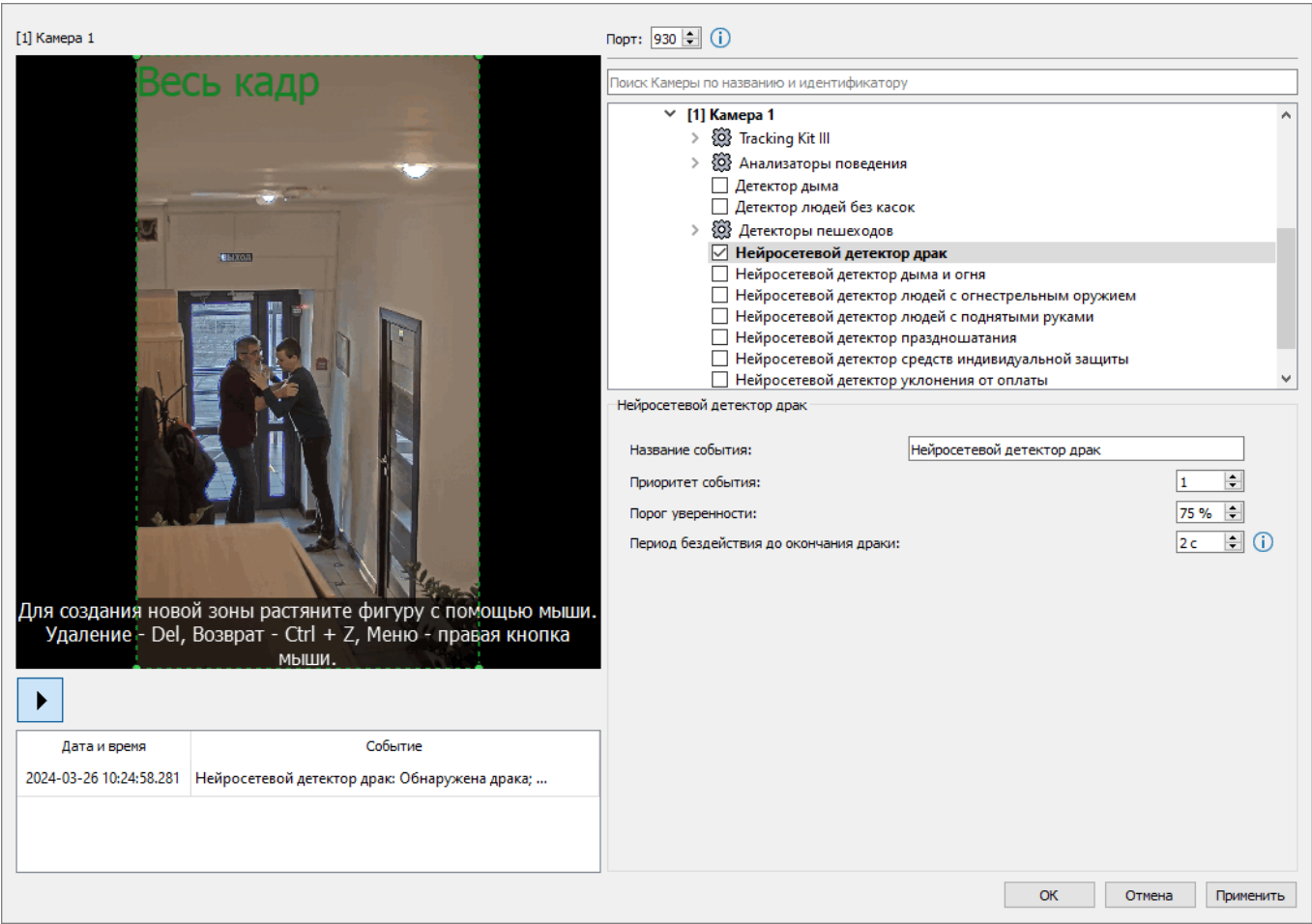


Рис. 268. Окно настройки параметров Нейросетевого детектора драк

Таблица 101. Параметры Нейросетевого детектора драк

Параметр	Описание
Название события	Задайте название события, которое будет отправляться в <i>Протокол событий</i>, если в контролируемой зоне обнаружена драка/завершение драки. Примечание. В параметре задается общая часть названия, к которой будет добавлено соответствующее уточнение (Обнаружена драка/Драка закончилась).
Приоритет события	Задайте приоритет события этого детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения. Диапазон возможных значений: [1 ; 10]. По умолчанию принимает значение 1.

Параметр	Описание
Порог уверенности	Задайте минимальный коэффициент уверенности в том, что обнаруженный в кадре объект классифицируется как дерущийся человек. Диапазон возможных значений: [1; 100]. По умолчанию принимает значение 75. Чем ниже заданное значение, тем выше будет скорость обнаружения и выше вероятность ошибки в определении драк, и наоборот.
Период бездействия до окончания драки	Если после начала драки в течение заданного промежутка времени ее участники не совершают агрессивных действий, драка будет считаться завершенной. Возобновление агрессивного поведения повлечет создание нового события. Диапазон возможных значений: [1; 300]. По умолчанию принимает значение 10 секунд.

14.2.3.3.1 Рекомендации по настройке камер для Нейросетевого детектора драк

Ниже перечислены дополнительные требования и рекомендации к содержанию сцены, расположению камер и источников освещения при решении задачи обнаружения драк. Несоблюдение указанных требований в большинстве случаев влечет за собой возникновение ложных срабатываний видеоаналитических детекторов или пропуск событий.

1. Минимальное разрешение кадров составляет 640×480 пикселей. Максимальное разрешение в целом не ограничено.
2. Минимальное значение FPS: 10 к/с. FPS потока должен быть стабилен, в противном случае корректная работа детекторов не гарантируется.
3. Высота подвеса камеры: 2–3 м.
4. Угол подвеса камеры (относительно потолка): 15 – 60°.
5. Минимальный размер человека в кадре должен составлять не менее 20% высоты кадра, а также должен быть не менее 100 пикселей.

Прочие рекомендации по настройке и расположению камер см. в разделе **Общие рекомендации по настройке и расположению камер**.

14.2.3.4 Нейросетевой детектор дыма и огня

Детектор предназначен для обнаружения дыма и огня. При срабатывании детектора соответствующее событие отправляется в *Протокол событий*.

Внимание! Для работы данного детектора необходимо установить OpenVINO Server. За подробной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems.

Чтобы настроить детектор, отметьте флажок **Нейросетевой детектор дыма и огня** в списке дочерних объектов *Камеры* (см. рис. 269). По умолчанию зона контроля размечена на весь кадр, но также поддерживается работа с несколькими зонами на кадре (см. **Настройка контролируемой зоны**).

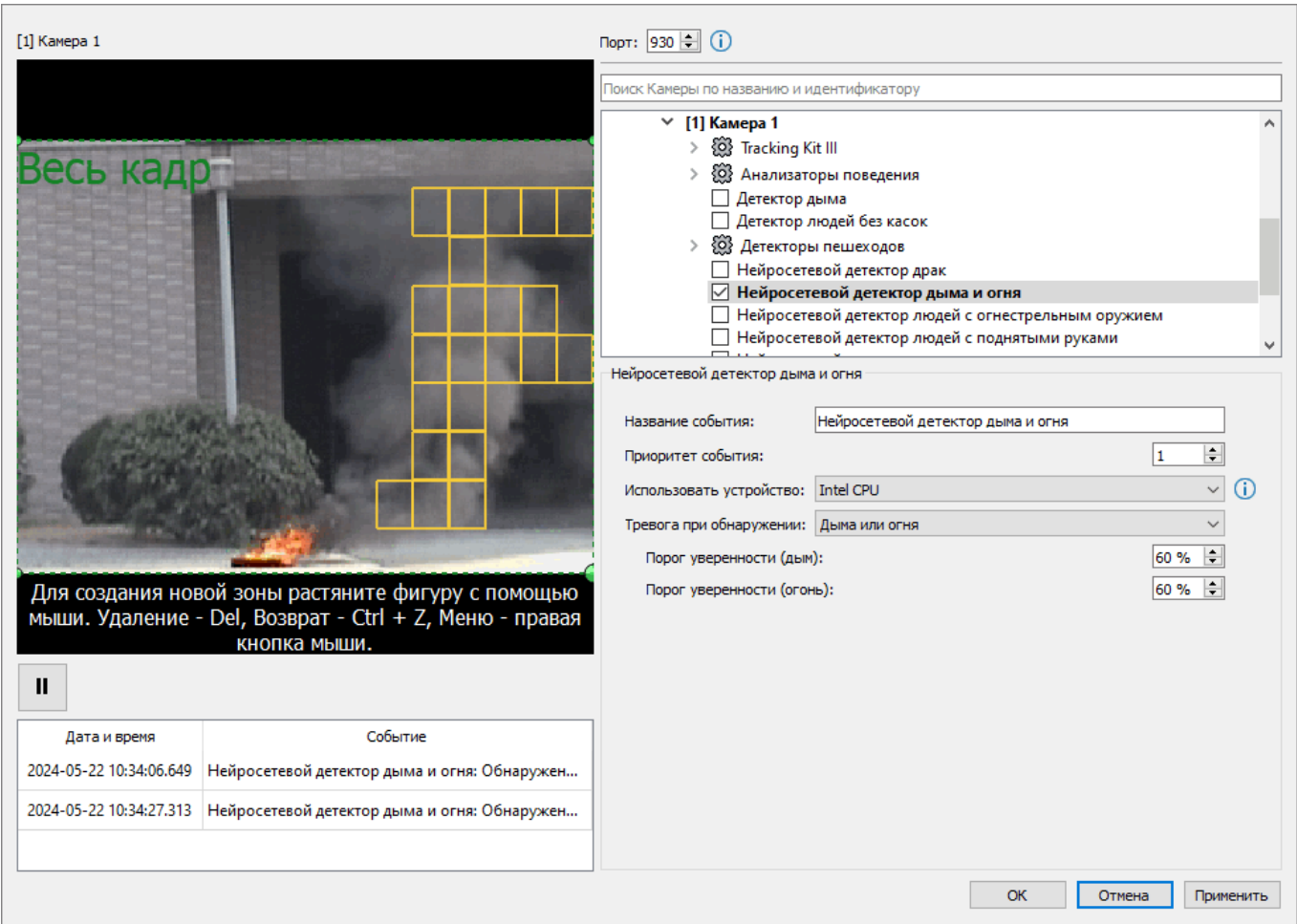


Рис. 269. Окно настройки параметров Нейросетевого детектора дыма и огня

Таблица 102. Параметры Нейросетевого детектора дыма и огня

Параметр	Описание
Название события	Задайте название события, которое будет отправляться в <i>Протокол событий</i>, если в контролируемой зоне обнаружен дым или огонь. Примечание. В параметре задается общая часть названия, к которой при обнаружении огня или дыма будет добавлено соответствующее уточнение (Обнаружено задымление/Обнаружено возгорание).
Приоритет события	Задайте приоритет события данного детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения. Диапазон возможных значений: [1 ; 10]. По умолчанию принимает значение 1.
Использовать устройство	Выберите из списка процессорное устройство, которое будет использоваться для определения дыма или огня с помощью нейросетевых алгоритмов.

Тревога при обнаружении	Выберите явление, при обнаружении которого в кадре будет генерироваться событие определенного типа. Может принимать следующие значения: • Дыма или огня — событие будет генерироваться, если в кадре обнаружен дым или огонь. Является значением по умолчанию. • Дыма — событие будет генерироваться, если в кадре обнаружен дым. Наличие огня в кадре будет игнорироваться. • Огня — событие будет генерироваться, если в кадре обнаружен огонь. Наличие дыма в кадре будет игнорироваться.
Порог уверенности (дым)	Задайте минимальный коэффициент уверенности в том, что в кадре присутствует дым. Если фактическая уверенность превысит заданное значение, будет достоверно считаться, что в кадре обнаружен дым. Диапазон возможных значений: [1; 100]. По умолчанию принимает значение 60. Недоступен, если параметр Тревога при обнаружении принимает значение Огня.
Порог уверенности (огонь)	Задайте минимальный коэффициент уверенности в том, что в кадре присутствует огонь. Если фактическая уверенность превысит заданное значение, будет достоверно считаться, что в кадре обнаружен огонь. Диапазон возможных значений: [1; 100]. По умолчанию принимает значение 60. Недоступен, если параметр Тревога при обнаружении принимает значение Дыма.

14.2.3.4.1 Рекомендации по настройке камер для Нейросетевого детектора дыма и огня

Ниже перечислены дополнительные требования и рекомендации к содержанию сцены и расположению камер при решении задачи обнаружения дыма и огня. Несоблюдение указанных требований в большинстве случаев влечет за собой возникновение ложных срабатываний видеоаналитических детекторов или пропуск событий.

1. Минимальное разрешение кадров составляет 416×416 пикселей. Максимальное разрешение в целом не ограничено.
2. Минимальное значение FPS: 5 к/с. FPS потока должен быть стабилен, в противном случае корректная работа детектора не гарантируется.
3. Минимальный размер области задымления должен составлять не менее 8% от линейных размеров кадра.

4. Высота подвеса камеры: значение ограничивается требованием к минимальному размеру области задымления (см. п. 3).
5. Угол подвеса камеры: значение ограничивается требованием к минимальному размеру области задымления (см. п. 3).

Прочие рекомендации по настройке и расположению камер см. в разделе **Общие рекомендации по настройке и расположению камер**.

14.2.3.5 Нейросетевой детектор праздношатания

Нейросетевой детектор праздношатания предназначен для определения людей, находящихся в контролируемой зоне в течение заданного времени. При обнаружении праздношатающегося человека соответствующее событие отправляется в *Протокол событий*.

Внимание! Для работы данного детектора необходимо установить OpenVINO Server. За подробной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems.

Чтобы настроить детектор, отметьте флажок **Нейросетевой детектор праздношатания** в списке дочерних объектов *Камеры* (см. рис. 270). По умолчанию зона контроля размечена на весь кадр, но также поддерживается работа с несколькими зонами на кадре (см. **Настройка контролируемой зоны**).

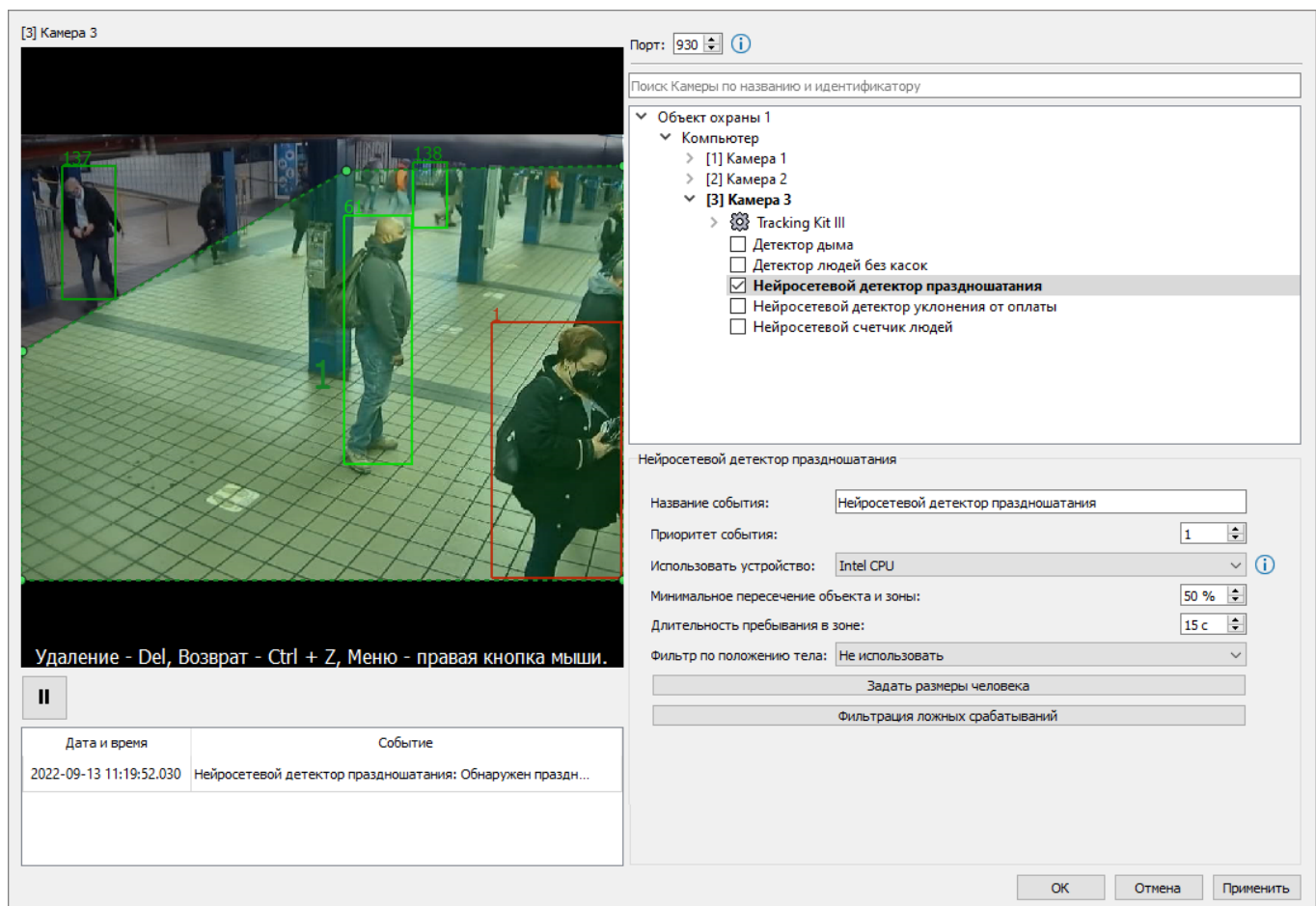


Рис. 270. Окно настройки параметров Нейросетевого детектора праздношатания

Таблица 103. Параметры Нейросетевого детектора празднования

Параметр	Описание
Название события	Задайте название события, которое будет отправляться в <i>Протокол событий</i> , если человек находится внутри контролируемой зоны в течение заданного времени.
Приоритет события	Задайте приоритет события данного детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения.
Использовать устройство	Выберите из списка процессорное устройство, которое будет использоваться для определения количества людей с помощью нейросетевых алгоритмов.
Минимальное пересечение объекта и зоны	Задайте площадь пересечения объекта и контролируемой зоны (в процентах от вычисленной площади обнаруженного объекта), при превышении которой объект будет считаться находящимся в контролируемой зоне.
Длительность пребывания в зоне	Задайте время нахождения объекта в контролируемой зоне (в секундах), при превышении которого произойдет срабатывание детектора.
Фильтр по положению тела	Выберите положение тела человека, при котором произойдет срабатывание детектора, если время непрерывного пребывания в данном положении не менее заданного значения (см. Длительность пребывания в зоне). Возможные значения: • Не использовать — празднующими будут считаться люди, которые находятся в любом положении. • Только положение сидя — празднующими будут считаться только те люди, которые находятся в положении сидя. • Только положение стоя — празднующими будут считаться те люди, которые находятся в положении стоя.
Задать размеры человека	Нажмите кнопку и задайте минимальный и максимальный размеры человека в области воспроизведения видео. Если размеры объекта не входят в данный диапазон, то он не будет классифицироваться как человек.
Фильтрация ложных срабатываний	Нажмите кнопку и задайте одну или несколько зон, в которых будет выполняться фильтрация ложных срабатываний детектора.

14.2.3.5.1 Рекомендации по настройке камер для Нейросетевого детектора праздноташатания

Ниже перечислены дополнительные требования и рекомендации к содержанию сцены, расположению камер и источников освещения при решении задачи обнаружения праздноташающихся людей. Несоблюдение указанных требований в большинстве случаев влечет за собой возникновение ложных срабатываний видеоаналитических детекторов или пропуск событий.

1. Минимальное разрешение кадров составляет 640×480 пикселей. Максимальное разрешение в целом не ограничено.
2. Минимальное значение FPS: 10 к/с. FPS потока должен быть стабилен, в противном случае корректная работа детектора не гарантируется.
3. Угол подвеса камеры: 30 — 70°.
4. Минимальный размер человека должен составлять не менее 40 пикселей.

Прочие рекомендации по настройке и расположению камер см. в разделе **Общие рекомендации по настройке и расположению камер**.

14.2.3.6 Нейросетевой детектор уклонения от оплаты

Нейросетевой детектор уклонения от оплаты предназначен для определения фактов несанкционированного доступа к пространству за турникетом. К таким фактам относятся: проползание под преграждающим элементом (штанги турникета), перешагивание и обхождение его по краю. При выявлении нарушений соответствующие события отправляются в *Протокол событий*.

Для корректной работы детектора необходимо, чтобы камера была обращена навстречу потоку людей, совершающих оплату за проход через турникет. Поведение людей, проходящих через турникет со стороны камеры, не анализируется.

Внимание! Для работы данного детектора необходимо установить OpenVINO Server. За подробной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems.

Чтобы настроить детектор, отметьте флажок **Нейросетевой детектор уклонения от оплаты** в списке дочерних объектов *Камеры* (см. рис. 271). При разметке зоны контроля для каждого из турникетов необходимо разметить отдельную полигональную зону.

Чтобы настроить полигональную зону, выполните следующие действия:

1. Щелкните правой кнопкой мыши по области воспроизведения видео и выберите пункт **Добавить полигон**.
2. Переместите созданный полигон в область турникета и измените его размер так, чтобы он покрывал область прохода через турникет.
3. Отрегулируйте положение и высоту границ среднего синего полигона так, чтобы он совпадал с положением штанги турникета.
4. Уменьшите размеры верхнего и нижнего желтых полигонов так, чтобы между ними и синим полигоном оставалось свободное пространство. При этом желательно, чтобы проползающие под штангой турникета люди не задевали нижний желтый полигон.

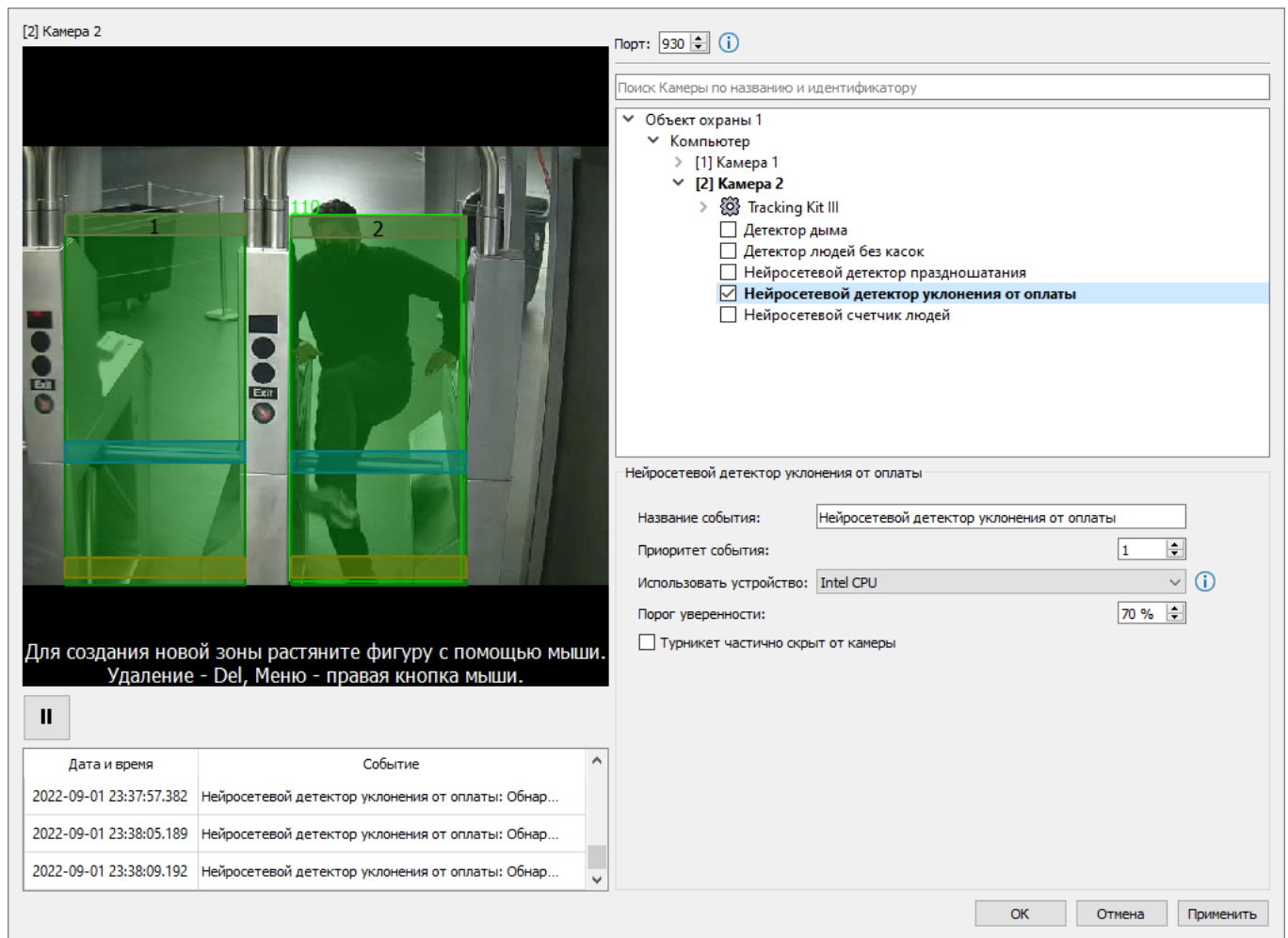


Рис. 271. Окно настройки параметров Нейросетевого детектора уклонения от оплаты

Таблица 104. Параметры Нейросетевого детектора уклонения от оплаты

Параметр	Описание
Название события	Задайте название события, которое будет отправляться в <i>Протокол событий</i> , если в контролируемой зоне обнаружено нарушение.
Приоритет события	Задайте приоритет события данного детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения.
Использовать устройство	Выберите из списка процессорное устройство, которое будет использоваться для определения нарушений с помощью нейросетевых алгоритмов.

Параметр	Описание
Порог уверенности	Задайте минимальный коэффициент уверенности в том, что обнаруженный в кадре объект классифицируется как человек. Если фактическая уверенность превысит заданное значение, будет достоверно считаться, что обнаруженный в кадре объект является человеком. Диапазон возможных значений: [1; 100]. По умолчанию принимает значение 50.
Турникет частично скрыт от камеры	Отметьте данный флажок в случае, если турникет частично скрыт от камеры. Если параметр активен, для определения нарушений будет использоваться альтернативный алгоритм работы, позволяющий снизить количество ложных срабатываний при работе в таких условиях.

14.2.3.6.1 Рекомендации по настройке камер для Нейросетевого детектора уклонения от оплаты

Ниже перечислены дополнительные требования и рекомендации к содержанию сцены, расположению камер и источников освещения при решении задачи обнаружения уклонения от оплаты. Несоблюдение указанных требований в большинстве случаев влечет за собой возникновение ложных срабатываний видеоаналитических детекторов или пропуск событий.

1. Минимальное разрешение кадров составляет 640×480 пикселей. Максимальное разрешение в целом не ограничено.
2. Минимальное значение FPS: 15 к/с. FPS потока должен быть стабилен, в противном случае корректная работа детектора не гарантируется.
3. Угол подвеса камеры: 80 — 90°.
4. Минимальный размер человека должен составлять не менее 100 пикселей.

Прочие рекомендации по настройке и расположению камер см. в разделе **Общие рекомендации по настройке и расположению камер**.

14.2.3.7 Нейросетевой детектор упавших людей

Нейросетевой детектор упавших людей предназначен для обнаружения людей, находящихся в лежачем положении в течение заданного времени. Детектор предназначен для использования в помещениях с невысоким (до 3 метров) потолком, например, в коридорах, на станциях и т. п. Ниже приведены некоторые сценарии, в которых может быть использован детектор:

- мониторинг перемещения людей на каталках в медицинских учреждениях;
- помощь лицам, потерявшим сознание, упавшим вследствие удара, полученной травмы или нарушений двигательных функций;
- выявление людей, намеренно занявших лежачее положение в местах, где это запрещено.

Внимание! Для работы данного детектора необходимо установить OpenVINO Server. За подробной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems.

Чтобы настроить детектор, отметьте флажок **Нейросетевой детектор упавших людей** в списке дочерних объектов *Камеры* (см. рис. 272). По умолчанию зона контроля размечена на весь кадр, но также поддерживается работа с несколькими зонами на кадре (см. **Настройка контролируемой зоны**).

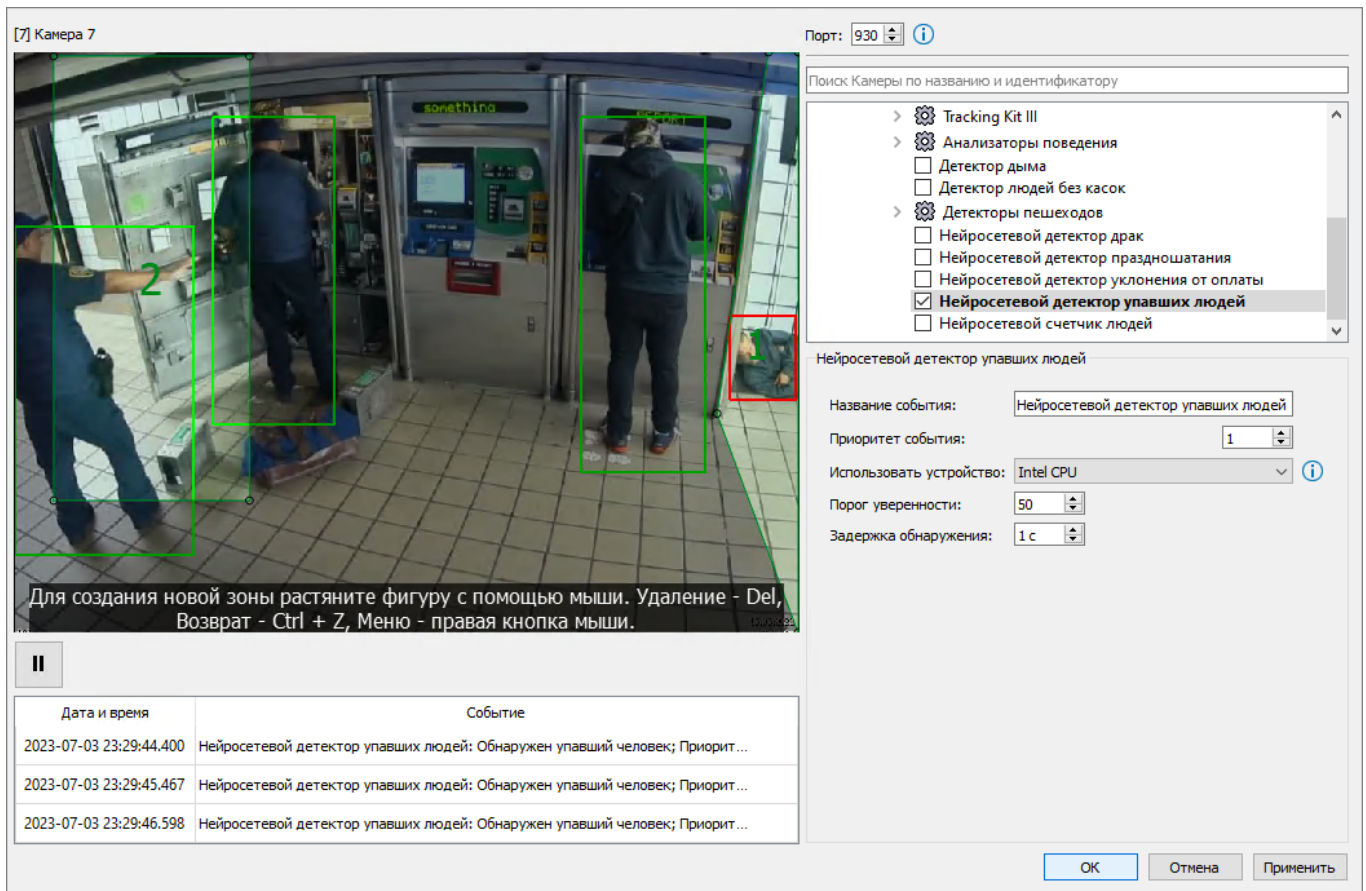


Рис. 272. Окно настройки параметров Нейросетевого детектора упавших людей

Таблица 105. Параметры Нейросетевого детектора упавших людей

Параметр	Описание
Название события	Задайте название события, которое будет отправляться в <i>Протокол событий</i> , если в контролируемой зоне обнаружен человек в лежачем положении.
Приоритет события	Задайте приоритет события этого детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения. Диапазон возможных значений: [1 ; 10].
Использовать устройство	Выберите из списка процессорное устройство, которое будет использоваться для определения нарушений с помощью нейросетевых алгоритмов.

Параметр	Описание
Порог уверенности	Задайте минимальный коэффициент уверенности в том, что обнаруженный в кадре объект классифицируется как упавший человек. Диапазон возможных значений: [1; 100]. По умолчанию принимает значение 75. Чем ниже заданное значение, тем выше будет скорость обнаружения и выше вероятность ошибки в определении упавших людей, и наоборот.
Задержка обнаружения	Задайте время, в течение которого человек должен находиться в лежащем положении, прежде чем будет сгенерировано тревожное событие. Диапазон возможных значений: [1; 99]. По умолчанию принимает значение 1 секунда.

14.2.3.7.1 Рекомендации по настройке камер для Нейросетевого детектора упавших людей

Ниже перечислены дополнительные требования и рекомендации к содержанию сцены, расположению камер и источников освещения при решении задачи обнаружения упавших людей. Несоблюдение указанных требований в большинстве случаев влечет за собой возникновение ложных срабатываний видеоаналитических детекторов или пропуск событий.

1. Минимальное разрешение кадров составляет 544×320 пикселей. Максимальное разрешение в целом не ограничено.
2. Минимальное значение FPS: 1 к/с. FPS потока должен быть стабилен, в противном случае корректная работа детектора не гарантируется.
3. Высота подвеса камеры: 2–3 м.
4. Угол подвеса камеры: 30–80°.
5. Минимальный размер человека стоя/лежа должен составлять не менее 18×36/38×18 пикселей при разрешении 544×320 пикселей.

Прочие рекомендации по настройке и расположению камер см. в разделе **Общие рекомендации по настройке и расположению камер**.

14.2.3.8 Нейросетевой счетчик людей

Нейросетевой счетчик людей предназначен для использования в местах больших скоплений людей, например, на станциях метро. Позволяет определять количество людей, одновременно находящихся в контролируемой области и отображать соответствующую информацию в *Протоколе событий*. При этом события генерируются с заданной периодичностью. Если количество людей превышает предельно допустимое, то события помечаются как тревожные.

Внимание! Для работы данного детектора необходимо установить OpenVINO Server. За подробной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems.

Чтобы настроить детектор, отметьте флажок **Нейросетевой счетчик людей** в списке дочерних объектов *Камеры* (см. рис. 273). По умолчанию зона контроля размечена на весь кадр, но также поддерживается работа с несколькими зонами на кадре (см. **Настройка контролируемой зоны**).

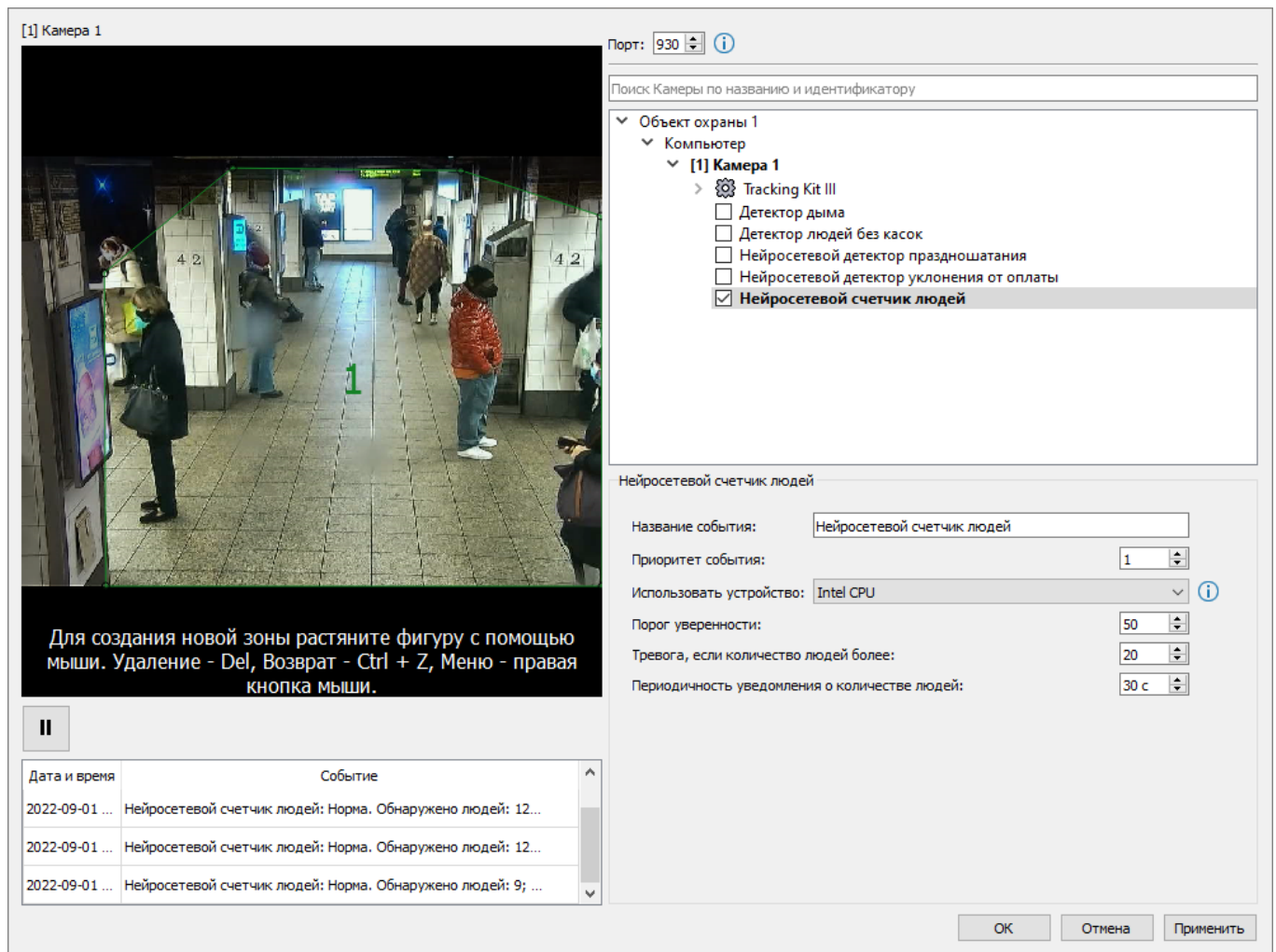


Рис. 273. Окно настройки параметров Нейросетевого счетчика людей

Таблица 106. Параметры Нейросетевого счетчика людей

Параметр	Описание
Название события	Задайте название события, которое будет отправляться в <i>Протокол событий</i> при подсчете количества людей в контролируемой зоне.
Приоритет события	Задайте приоритет события данного детектора. Приоритет определяет степень важности зарегистрированного детектором события и может быть использован при дальнейшей обработке события VCA_EVENT (см. Руководство программиста SecurOS) с помощью внешнего приложения.
Использовать устройство	Выберите из списка процессорное устройство, которое будет использоваться для определения количества людей с помощью нейросетевых алгоритмов.

Порог уверенности	Задайте минимальный коэффициент уверенности в том, что обнаруженный в кадре объект классифицируется как человек. Если фактическая уверенность превысит заданное значение, будет достоверно считаться, что обнаруженный в кадре объект является человеком. Диапазон возможных значений: [1; 100]. По умолчанию принимает значение 50.
Тревога, если количество людей более	Задайте максимальное количество людей, которые могут одновременно находиться в контролируемой зоне. При достижении или превышении заданного значения в <i>Протоколе событий</i> будет сгенерировано тревожное событие.
Периодичность уведомления о количестве людей	Задайте временной интервал (в секундах) для генерации событий в <i>Протоколе событий</i>.

14.2.3.8.1 Рекомендации по настройке камер для Нейросетевого счетчика людей

Ниже перечислены дополнительные требования и рекомендации к содержанию сцены, расположению камер и источников освещения при решении задачи обнаружения скоплений людей. Несоблюдение указанных требований в большинстве случаев влечет за собой возникновение ложных срабатываний видеоаналитических детекторов или пропуск событий.

1. Минимальное разрешение кадров составляет 640×480 пикселей. Максимальное разрешение в целом не ограничено.
2. Минимальное значение FPS: 1 к/с. FPS потока должен быть стабилен, в противном случае корректная работа детектора не гарантируется.
3. Угол подвеса камеры: 80°.
4. Минимальный размер головы человека должен составлять не менее 14×14 пикселей.

Прочие рекомендации по настройке и расположению камер см. в разделе **Общие рекомендации по настройке и расположению камер**.

14.2.4 Оптимизация производительности NUMA-систем

В целях повышения производительности для решения задач видеоаналитики на серверах могут использоваться мультипроцессорные системы с NUMA-архитектурой. Однако операционная система не всегда распределяет процессы между несколькими физическими процессорами достаточно эффективно, что может привести к снижению производительности. Для оптимизации производительности NUMA-систем в SecurOS предусмотрена возможность ручного распределения процессов между узлами NUMA.

Ручное распределение процессов между узлами NUMA

Для осуществления ручной настройки выполните следующие действия:

1. Остановите службу Video Management System Server. Для ОС семейства Windows используйте утилиту **Server Control Agent**. Для ОС семейства Linux используйте команду:

```
sudo service vms_server stop
```


2. В корневой директории SecurOS откройте файл `numa_settings.sample`.
3. Отредактируйте файл, чтобы его содержимое представляло собой набор строк следующего формата:

```
[path/]trackingkit3,object_id,numa_node
```

Где:

- `[path/]trackingkit3` — путь к исполняемому файлу и название исполняемого файла, запускающего процесс (указывается без расширения `.exe`).
- `object_id` — идентификатор объекта *Компьютерное зрение* в *Дереве Объектов SecurOS*.
- `numa_node` — номер предпочтительного узла NUMA, на котором должен запускаться процесс.

Например:

```
modules/trackingkit3/trackingkit3,1,0  
modules/trackingkit3/trackingkit3,2,1
```

В указанном выше примере настроена работа объекта *Компьютерное зрение* с идентификатором 1 на узле NUMA с индексом 0 (т. е. на первом физическом процессоре) и объекта *Компьютерное зрение* с идентификатором 2 на узле NUMA с индексом 1 (т. е. на втором физическом процессоре).

Примечание. Каждый процесс, соответствующий объекту *Компьютерное зрение*, должен быть представлен отдельной строкой в файле.

4. Измените расширение файла на `.txt`.
5. Запустите службу Video Management System Server. Для ОС семейства Windows используйте утилиту **Server Control Agent**. Для ОС семейства Linux используйте команду:

```
sudo service vms_server start
```

14.3 Представление результатов работы видеоаналитического детектора

При срабатывании видеоаналитического детектора в SecurOS формируется событие, которое может быть обработано с помощью *Скрипта Node.js* с учетом его приоритета (см. **Руководство программиста SecurOS**) или отслежено оператором в *Протоколе событий*. Событие формируется объектом *Камера*, для которой создан видеоаналитический детектор, и имеет название **Событие видеоаналитики** (`VCA_EVENT`) вне зависимости от используемого детектора. При этом в *Протоколе событий* будет отображаться то название, которое задано в настройках детектора (параметр **Название события**). При отображении в *Протоколе событий* события могут быть отфильтрованы по типу детектора.

Примечание. Если параметр не задан в настройках детектора, используется значение по умолчанию, совпадающее с названием детектора.

При необходимости оператор может реагировать на событие детектирования. Например, перейти из *Протокола событий* к видеозаписи события в *Медиа Клиенте* или отправить *Карточку происшествия* в *Службу реагирования* (см. [Краткое руководство пользователя SecurOS](#)).

В *Медиа Клиенте* возможна визуализации событий детекторов плагина Tracking Kit III. При визуализации в ячейке *Камеры* каждое событие будет выделяться графически. Например, при работе с *Детектором бега* будут выделяться бегущие объекты и их треки, при работе с *Детектором оставленных и унесенных предметов* будут выделяться все оставленные предметы, или места, где находились унесенные предметы, и т.д.

Внимание! Визуализация событий в *Медиа Клиенте* возможна только для детекторов плагина Tracking Kit III (см. [Настройка плагина Tracking Kit III и встроенных видеоаналитических детекторов](#)) при просмотре только живого видео.

Для визуализации событий отметьте флажок [Визуализировать события Компьютерного Зрения](#) в настройках *Медиа Клиента* (см. [Закладка Камеры](#)).

15 Центр Мониторинга и Контроля

Функциональность доступна в редакции *SecurOS Monitoring & Control Center*.

В ОС **Linux** функциональность ограничена.

Редакция *SecurOS Monitoring & Control Center* позволяет организовать единый региональный *Центр Мониторинга и Контроля* множества территориально разделенных систем безопасности.

Примечание. Далее по тексту для обозначения *SecurOS Monitoring & Control Center* будет использоваться краткое название *Центр Мониторинга* или *SecurOS MCC*.

В SecurOS существует два типа *Центра Мониторинга*, отличающихся по функциональным возможностям:

- SecurOS MCC DC (Direct Connect) — прямое подключение. Данный тип *Центра Мониторинга* является основным и используется для работы с *Удаленными системами* в большинстве случаев. Подробнее о данном типе см. **Прямое подключение**.
- SecurOS MCC PA (Privileged Access) — прямое подключение с возможностью *привилегированного доступа*. Данный тип *Центра Мониторинга* используется для проведения специальных операций в *Удаленных системах*. Подробнее о данном типе см. **Привилегированный доступ**.

Внимание! Корректная работа SecurOS MCC гарантируется в случае, если номер версии SecurOS, установленного в *Удаленной системе*, равен или меньше номера версии SecurOS MCC. При этом совместимость версий ограничена. За подробной информацией обращайтесь в Службу технической поддержки Intelligent Security Systems.

Работать с удаленными объектами можно после загрузки конфигурации *Удаленных систем* в SecurOS MCC. Особенности загрузки конфигурации, общие для каждого типа *Центра Мониторинга*, приведены в разделе **Прямое подключение**.

15.1 Прямое подключение

При прямом подключении *Центр Мониторинга* может быть настроен для работы:

- с архивами, хранящимися в *Удаленной системе* (*Оперативным* и *Долговременным*) — при наличии связи с *Удаленной системой*;
- с *Оперативным архивом* *Удаленной системы*, ранее сконвертированным в *Долговременный* и сохраненным вне *Удаленной системы* с помощью объекта **Архиватор** — при отсутствии связи с *Удаленной системой*.

15.1.1 Ограничения

Для обеспечения корректной работы *Центра Мониторинга* при прямом подключении вводятся следующие ограничения:

1. Версии SecurOS MCC и редакций SecurOS *Удаленных систем*, должны быть не ниже 9.1.
2. Региональные настройки операционной системы на серверах SecurOS MCC и серверах SecurOS *Удаленных систем* должны совпадать.
3. Интеллектуальные Модули, установленные в *Удаленной системе*, должны быть также установлены в SecurOS MCC.

15.1.2 Настройка Прямого подключения

Для настройки прямого подключения *Центра Мониторинга* выполните следующие действия:

Примечание. Конфигурирование может выполняться на любом компьютере с установленным SecurOS MCC.

1. В конфигурации *Удаленной системы* в настройках объекта **Система** отметьте флаг **Разрешить доступ** и задайте пароль доступа к этой *Удаленной системе* из *Центра Мониторинга*.
2. В конфигурации SecurOS MCC в *Дереве объектов* создайте и настройте объект **Удаленная система**, включая пароль для подключения к *Удаленной системе*.
3. В настройках объекта **Права пользователя** задайте для операторов *Центра Мониторинга* требуемые права доступа к *Камерам Удаленной системы*.

Примечание. По умолчанию, после загрузки конфигурации в *Центр Мониторинга*, доступ оператора к объекту *Удаленная система* и всем дочерним запрещен.

После загрузки конфигурации на сервере *Центра Мониторинга* для каждой подключенной *Удаленной системы* создается отдельное *Дерево видимости объектов*. Такое дерево находится на том же уровне иерархии, что и объект *Система* *Центра Мониторинга* (см. рис. 274). В *Дереве видимости* отображаются только следующие объекты *Удаленной системы*:

1. Базы данных;
2. Компьютеры;
3. Камеры;
4. Микрофоны;
5. Зоны;
6. Лучи;
7. Реле;
8. Архиваторы;
9. Службы реагирования;
10. SIP-устройства;
11. Компьютерные зрения;
12. Объекты СКУД/ОПС.

Примечание. "Видимость" объектов *Удаленной системы* в SecurOS MCC означает возможность прямого взаимодействия с этими объектами. При этом доступ оператора к настройкам и прочим операциям с этими объектами в *Дереве объектов* (Отключение/Переименование/Удаление) запрещен.

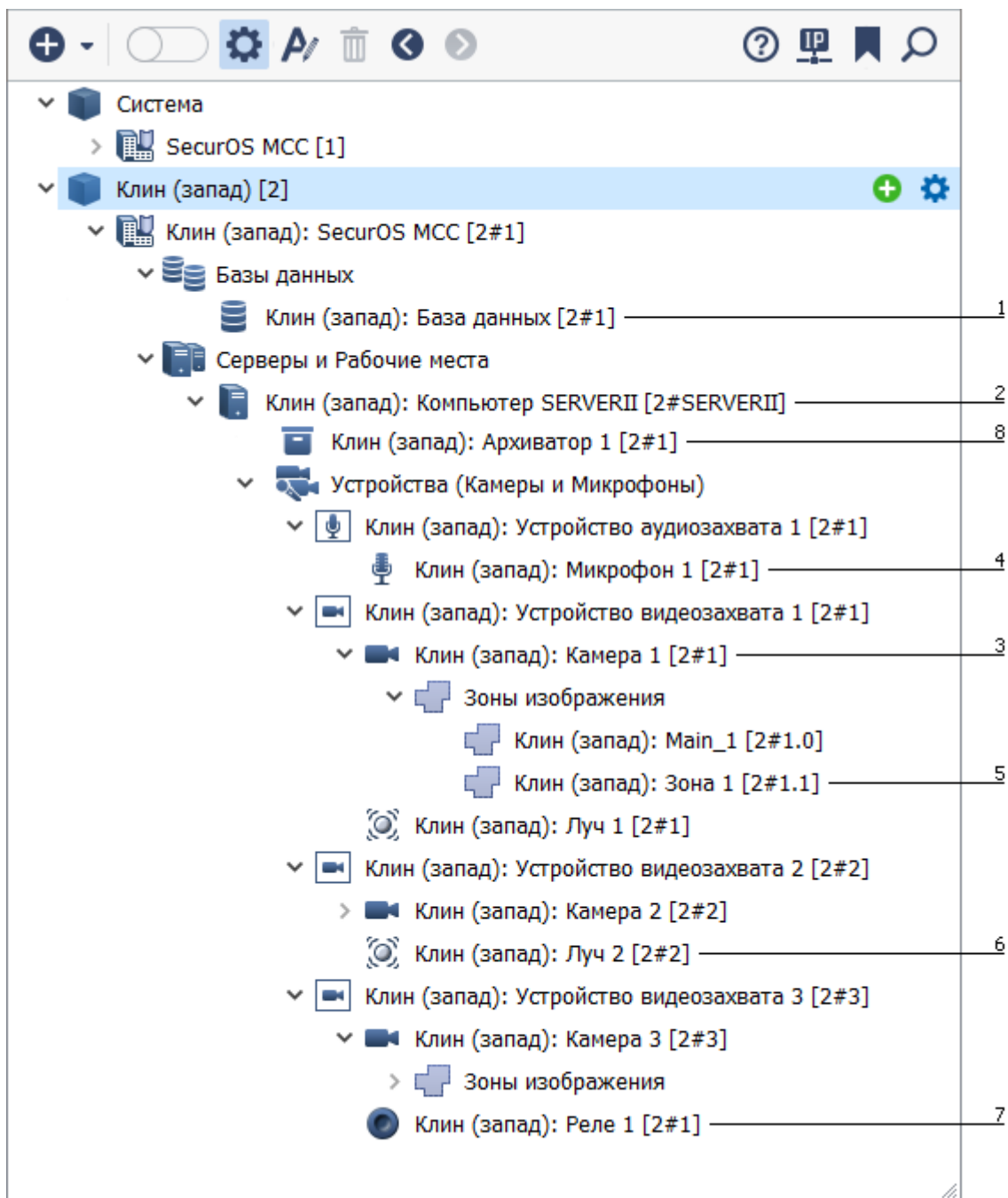


Рис. 274. Конфигурация Удаленной системы, отображаемая в Дереве объектов Центра мониторинга

Расположение и названия объектов Удаленной системы

Удаленная система создается в *Дереве объектов* на том же уровне иерархии, что и объект *Система* Центра Мониторинга. **Название** и **Идентификатор**, которые присваиваются ей при создании, несут, как правило, полезную информацию. Например, о местоположении этой *Удаленной системы*. После загрузки конфигурации объектам *Удаленной системы* присваиваются **Названия** и **Идентификаторы** в следующем формате:

- **Название объекта:** <Название удаленной системы>:<пробел><Название объекта в удаленной системе>
- **Идентификатор объекта:** <Идентификатор удаленной системы>#<Идентификатор объекта в удаленной системе>

15.1.2.1 Шлюз MCC DC

Объект предназначен для назначения нескольким *Видеосерверам* SecurOS роли шлюзов *Удаленной системы*, которые будут использоваться для передачи только живого видео. При шлюзовании из *Удаленной системы* будет поступать единственный поток, независимо от количества потребителей этого потока в SecurOS MCC. Таким образом, использование шлюзования позволяет существенно снизить сетевой трафик. При этом использование нескольких *Видеосерверов* в роли шлюзов позволяет динамически распределять нагрузку между выделенными серверами при передаче в SecurOS данных, отправляемых удаленной системой.

Родительский объект — *Компьютер*.

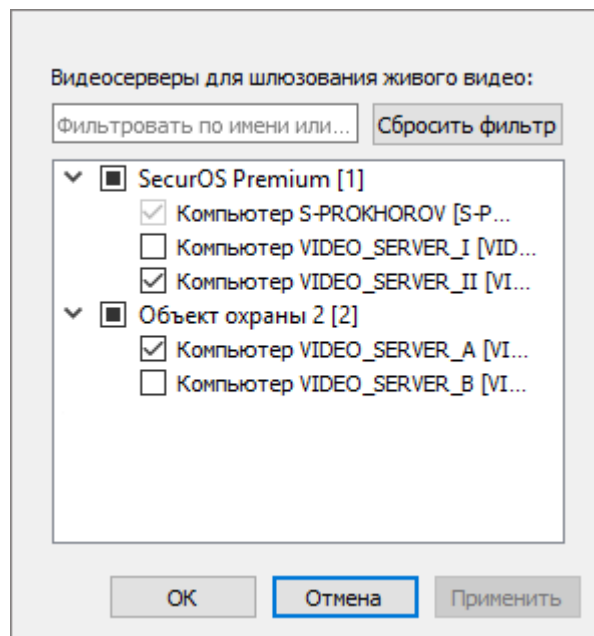


Рис. 275. Окно настройки параметров объекта Шлюз MCC DC

Таблица 107. Параметры объекта Шлюз MCC DC

Параметр	Описание
Фильтр	Для поиска объекта по части имени или идентификатора введите в поле требуемые символы; в дереве автоматически отобразятся только те объекты, имя или идентификатор которых соответствуют заданным условиям поиска. Для того, чтобы очистить поле, нажмите кнопку Сбросить фильтр .

Параметр	Описание
Дерево объектов	Дерево <i>Компьютеров</i> с ролью <i>Видеосервер</i> , существующих в сети SecurOS. Все существующие в системе <i>Видеосерверы</i> сгруппированы по отношению к <i>Объектам охраны</i> .
	Для добавления <i>Видеосервера</i> в список шлюзов отметьте соответствующий флажок слева от объекта <i>Видеосервер</i> .
	Примечание. <i>Видеосервер</i> , который является родительским для настраиваемого объекта <i>Шлюз MCC DC</i> , выделен в списке серым. Такой <i>Видеосервер</i> нельзя исключить из списка шлюзов.

Для распределения нагрузки модуль запрашивает у каждого из указанных *Видеосерверов* текущую загрузку. Далее, на основании полученной информации, подключает клиента, который запрашивает видео, к наименее загруженному *Видеосерверу*.

15.1.2.2 MCC DC HTTP Proxy

Объект позволяет использовать *Видеосервер* SecurOS в качестве прокси-сервера для обмена данными между *Удаленной системой* и *Рабочими местами операторов* Центра Мониторинга в случаях, если прямое соединение между ними невозможно или является нестабильным. Для использования прокси-сервера необходимо выбрать соответствующий объект *MCC DC HTTP Proxy* в настройках объекта *Удаленная система*.

Примечание. Для работы с Модулем SecurOS *FaceX* через прокси-сервер необходимо выбрать соответствующий объект *MCC DC HTTP Proxy* в настройках объекта *Система*.

Родительский объект — *Компьютер*.

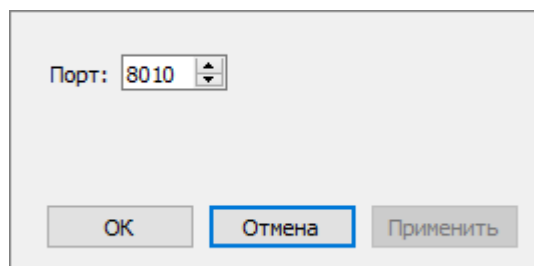


Рис. 276. Окно настройки параметров объекта MCC DC HTTP Proxy

Таблица 108. Параметры объекта MCC DC HTTP Proxy

Параметр	Описание
Порт	Задайте TCP-порт для сетевого взаимодействия с прокси-сервером. По умолчанию принимает значение 8010.

15.1.2.3 Удаленная система

Объект обеспечивает подключение *Центра Мониторинга* к *Удаленной системе*. Дополнительно объект обеспечивает шлюзование потока живого видео, доступ к данным через прокси-сервер и преобразование IP-адресов объектов *Удаленной системы*.

Внимание! Создание и настройка объекта *Удаленная система* выполняется только суперпользователем SecurOS MCC (см. [Пользователи в SecurOS](#)).

Окно настройки параметров содержит следующие закладки:

- Закладка **Общие**.
- Закладка **Шлюз и прокси**.

Подключение к Удаленной системе

Для подключения к *Удаленной системе* выполните следующие действия:

1. Для создания объекта в *Дереве объектов SecurOS MCC* выберите объект **Система**, нажмите кнопку **Создать**, выберите пункт **Удаленная система**.
2. Откройте окно настройки параметров *Удаленной системы* (см. [Закладка Общие](#)).
3. В поле **Адрес Сервера конфигураций** задайте IP-адрес **Сервера конфигурации** *Удаленной системы*.
4. В поле **Пароль доступа** задайте пароль доступа к *Удаленной системе* из *Центра Мониторинга*. Заданный пароль должен совпадать с паролем, указанным в настройках объекта **Система** в конфигурации *Удаленной системы*.
5. При необходимости заполните таблицу **Преобразование адресов**.

Шлюзование живого видео

В SecurOS MCC доступно шлюзование живого видео, поступающего из *Удаленной системы*.

Для шлюзования видео выполните следующие действия:

1. В *Дереве объектов SecurOS MCC* выберите произвольный **Компьютер** с ролью *Видеосервер*.
2. Для выбранного *Видеосервера* создайте и настройте дочерний объект **Шлюз MCC DC**.
3. Выберите созданный шлюз в настройках объекта *Удаленная система* (см. [Закладка Шлюз и прокси](#)).

Доступ к архивному видео и другим данным через прокси-сервер

В SecurOS MCC доступ к архивному видео и другим данным *Удаленной системы* может быть обеспечен через прокси-сервер.

Для обеспечения доступа к архивному видео и другим данным через прокси-сервер выполните следующие действия:

1. В *Дереве объектов SecurOS MCC* выберите произвольный **Компьютер** с ролью *Видеосервер*.
2. Для выбранного *Видеосервера* создайте и настройте дочерний объект **MCC DC HTTP Proxy**.
3. Выберите созданный прокси-сервер в настройках объекта *Удаленная система* (см. [Закладка Шлюз и прокси](#)).

15.1.2.3.1 Закладка Общие

Общие Шлюз и прокси

Настройки подключения к Удаленной системе

Адрес Сервера конфигураций: 172.16.1.203

Пароль доступа:

Соединение установлено

Преобразование адресов:

Название	Адрес	Доступность
REMOTE SYSTEM: Компьютер SERVERII	172.16.1.207	Недоступен
REMOTE SYSTEM: Компьютер V-BOIKO		Доступен
REMOTE SYSTEM: Компьютер V-FIH	172.16.1.93	Доступен
REMOTE SYSTEM: База данных 1		

Фильтр событий: Фильтр событий 1 [1]

ОК Отмена Применить

Рис. 277. Окно настройки параметров объекта Удаленная система. Закладка Общие

Таблица 109. Параметры объекта Удаленная система. Закладка Общие

Параметр	Описание
Адрес конфигураций Сервера	Задайте IP-адрес Сервера конфигураций Удаленной системы SecurOS.
Пароль доступа	Задайте пароль доступа к Удаленной системе из Центра Мониторинга. Для установления соединения заданный пароль должен совпадать с паролем, заданным в настройках объекта Система на стороне Удаленной системы. Примечание. Если доступ к Удаленной системе предоставляется без пароля, параметр необязателен.

Параметр	Описание
Преобразование адресов	Таблица соответствия между именами <i>Компьютеров</i> и <i>Баз данных Удаленной системы</i> и их публичными IP-адресами. Задается в случае необходимости, например, если между <i>Центром Мониторинга</i> и <i>Удаленной системой</i> установлено VPN-соединение, они находятся в сетях разных провайдеров и т.п. Проверка доступности <i>Компьютера</i> автоматически выполняется при указании IP-адреса. Примечания: 1. Если соединение с <i>Удаленной системой</i> не установлено, проверка доступности не выполняется. 2. Проверка доступности выполняется только для <i>Компьютеров</i>.
Фильтр событий	Выберите один из Фильтров событий, настроенных в <i>Центре Мониторинга</i>, чтобы ограничить количество сообщений, передаваемых из <i>Удаленной системы</i> в <i>Центр Мониторинга</i>. Внимание! Если такой фильтр не настроен, из <i>Удаленной системы</i> будут передаваться все события, что может привести к перегрузке канала связи и неустойчивой работе <i>Центра Мониторинга</i>.

15.1.2.3.2 Закладка Шлюз и прокси

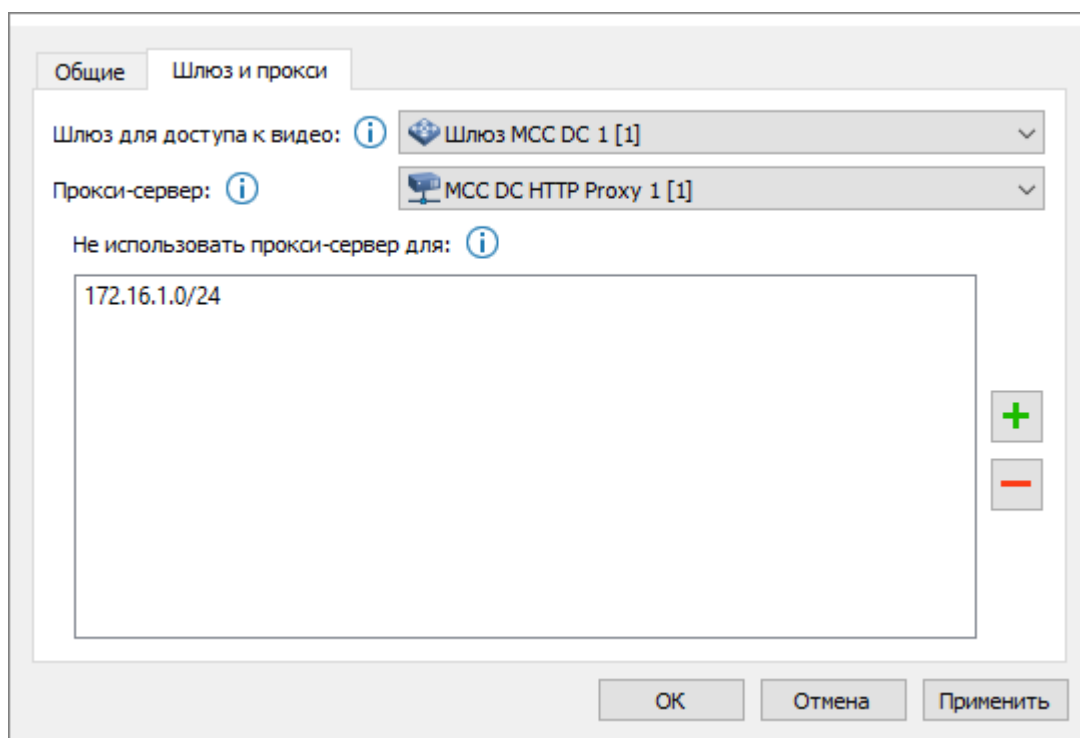


Рис. 278. Окно настройки параметров объекта Удаленная система. Закладка Шлюз и прокси

Таблица 110. Параметры объекта Удаленная система. Зкладка Шлюз и прокси

Параметр	Описание
Шлюз для доступа к видео	Выберите из списка один из Шлюзов MCC DC, настроенных в <i>Центре Мониторинга</i>, если необходимо снизить загрузку канала связи между <i>Удаленной системой</i> и <i>Центром Мониторинга</i>. Снижение нагрузки обеспечивается за счет шлюзования живого видео. Внимание! При шлюзовании видео работа с динамиком <i>Камеры</i> в <i>Центре Мониторинга</i> не поддерживается.
Прокси-сервер	Выберите из списка MCC DC HTTP Proxy для передачи данных между <i>Удаленной системой</i> и <i>Рабочими местами операторов Центра Мониторинга</i> через прокси-сервер, если прямое соединение между ними невозможно или является нестабильным. Примечание. Для передачи данных Модуля SecurOS FaceX через прокси-сервер необходимо выбрать объект MCC DC HTTP Proxy в настройках объекта Система.
Не использовать прокси-сервер для	Укажите список подсетей, для которых не требуется использовать прокси-сервер. <i>Компьютеры</i> из перечисленных подсетей будут подключаться к <i>Удаленной системе</i> напрямую. Формат ввода: [адрес_подсети_(IPv4)] / [длина_префикса_в_битах]. Например: 172.16.1.0/24.

15.1.3 Настройка для работы с SecurOS Auto

При работе с SecurOS Auto оператор *Центра Мониторинга* может получить доступ к результатам распознавания номеров, которое выполняется в *Удаленной системе*. Для этого настройте *Центр Мониторинга* следующим образом (см. рис. 279):

Примечание. На рисунке в *Дереве объектов SecurOS MCC* некоторые *Группы объектов* удалены.

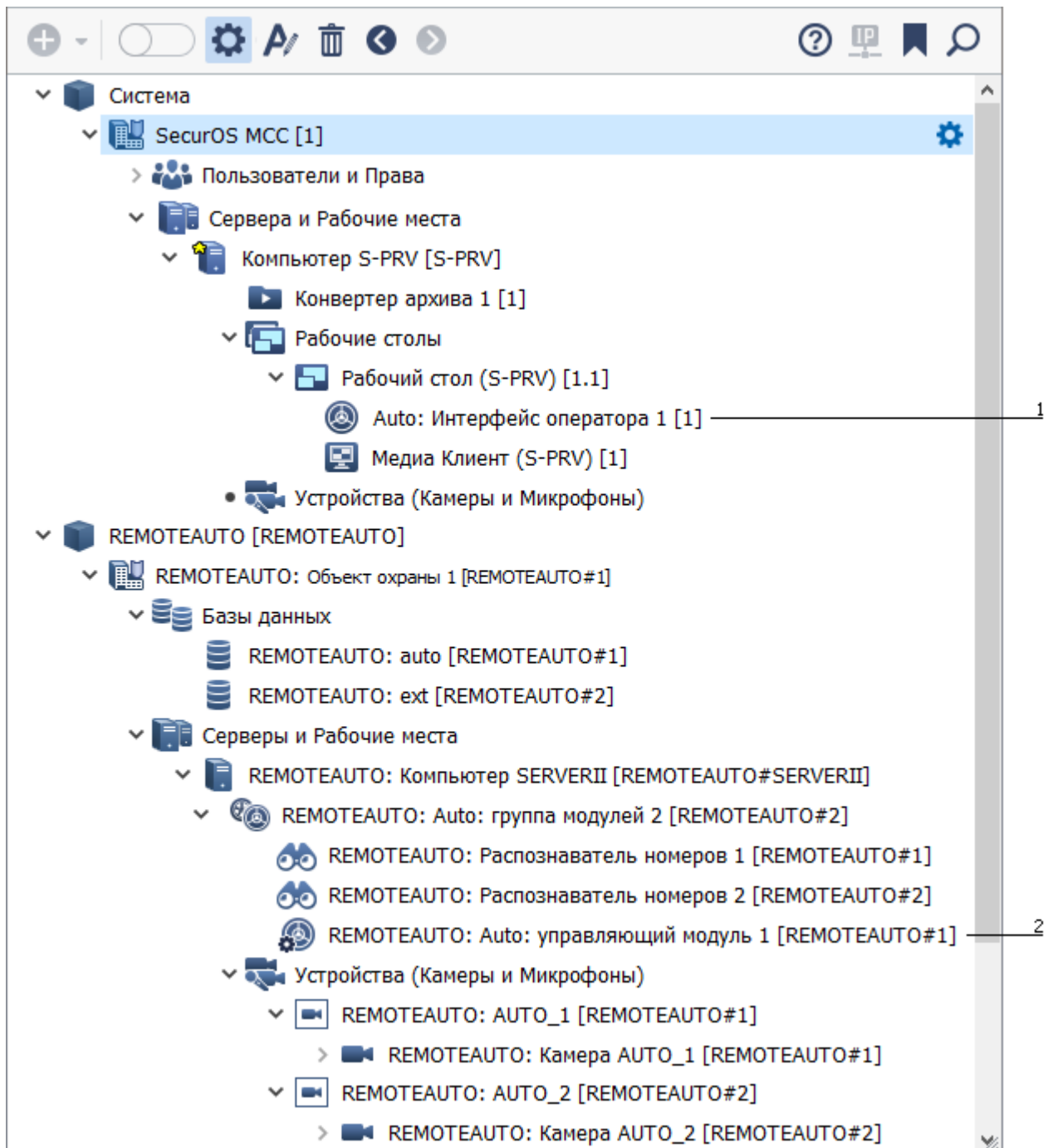


Рис. 279. Дерево объектов Центра Мониторинга для работы с удаленным SecurOS Auto

1. Создайте объект *Auto: интерфейс оператора*.
2. В настройках *Auto: интерфейс оператора* выберите объект *Auto: управляющий модуль 1 Удаленной системы* (см. рис. 280).

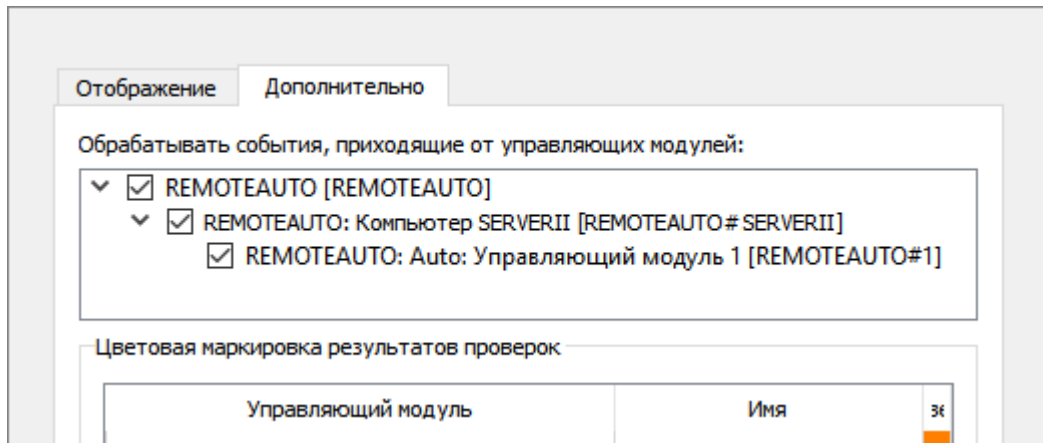


Рис. 280. Настройки объекта Auto: интерфейс оператора в SecurOS MCC

3. Проверьте возможность подключения к БД SecurOS Auto *Удаленной системы*: правила маршрутизации в сети и конфигурационные файлы СУБД PostgreSQL `postgresql.conf` и `pg_hba.conf` (см. [Руководство пользователя SecurOS Auto](#)).
4. В случае, если локальный и публичный IP-адреса удаленного сервера БД SecurOS Auto отличаются, в настройках объекта *Удаленная система* задайте публичный IP-адрес сервера (см. рис. 281). В приведенном примере это базы данных REMOTEAUTO: `auto` и REMOTEAUTO: `ext`.

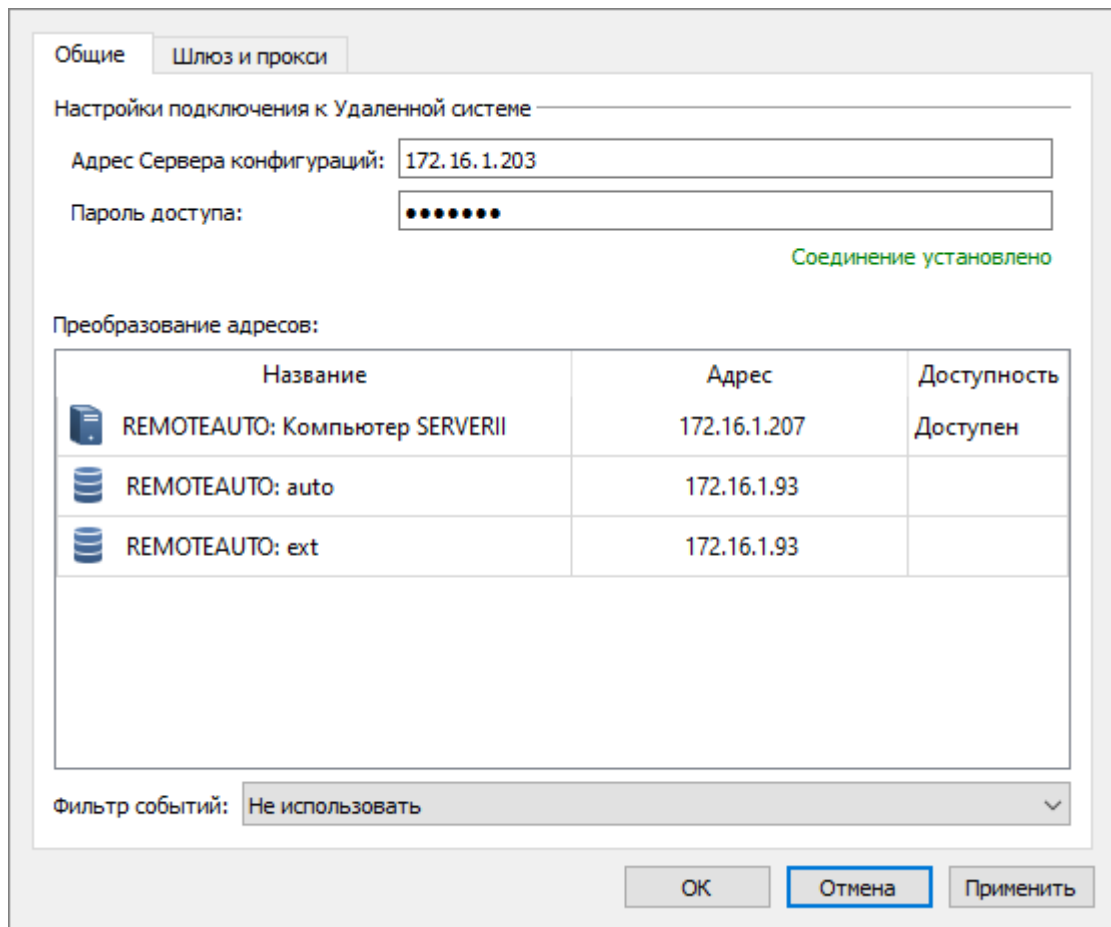


Рис. 281. Настройки объекта Удаленная система в SecurOS MCC

15.2 Привилегированный доступ

Использование типа *SecurOS MCC PA* позволяет оператору *Центра Мониторинга* проводить как обычный мониторинг *Удаленной системы*, так и специальные операции в этой *Удаленной системе*.

Специальные операции в *Удаленной системе* проводятся компетентными органами:

- Государственными силовыми структурами и ведомствами при контроле любых объектов АПК "Безопасный город".
- Частными службами внутренней безопасности предприятия или организации при контроле объектов критической инфраструктуры, не являющихся частью АПК "Безопасный город" (например, банки, предприятия розничной торговли и т.д.).

При проведении специальной операции оператору *Центра Мониторинга* предоставляется привилегированный доступ к интересующим его *Камерам Удаленной системы*. Для получения привилегированного доступа оператор *Центра Мониторинга* должен захватить управление *Камерами Удаленной системы* (см. [Функционирование](#)). После захвата *Камер* доступ к захваченным камерам (управление и просмотр живого видео) предоставляется только операторам *Центра Мониторинга SecurOS MCC PA*. Доступ операторов всех прочих *Центров Мониторинга SecurOS MCC* и операторов *Удаленной системы* к захваченным *Камерам* прекращается. После завершения специальной операции оператор *Центра Мониторинга SecurOS MCC PA* освобождает ранее захваченные *Камеры*. Сразу после освобождения *Камер* доступ операторов прочих *Центров Мониторинга* и операторов *Удаленной системы* к этим *Камерам* восстанавливается.

Вследствие лицензионных и функциональных ограничений, тип *SecurOS MCC PA* является дополнением к типу *SecurOS MCC DC* и устанавливается лишь в той сети, в которой предполагается проведение специальных операций.

Для предоставления привилегированного доступа к *Удаленной системе* *Центр Мониторинга* с типом *SecurOS MCC PA* использует единственный шлюз. Этот шлюз используется как для просмотра видео с *Камер Удаленной системы*, так и для записи "секретного" архива. Использование только одного шлюза позволяет полностью отделить контролируруемую *Удаленную систему* от остальной сети безопасности в случае проведения специальных операций. Функционирование системы более подробно описано в разделе [Функционирование](#).

Функциональные ограничения типа *SecurOS MCC PA* приводятся в разделе [Ограничения](#).

Настройки объектов системы, необходимые для проведения специальных операций, описаны в разделе [Настройка системы](#).

15.2.1 Функционирование

Если возможность *Привилегированного доступа* не включена (см. [Настройка системы](#)), *Центр Мониторинга SecurOS MCC PA* работает аналогично *Центру Мониторинга SecurOS MCC DC*. При этом оператор *Центра Мониторинга SecurOS MCC PA* может просматривать живое или архивное видео с выбранных камер *Удаленной системы* и управлять камерой в обычном режиме совместного управления.

После включения возможности *Привилегированного доступа* оператору *SecurOS MCC PA* становятся доступны специальные операции захвата/освобождения камер *Удаленной системы*. Для выполнения этих операций оператору *SecurOS MCC PA* становятся доступны скрытые элементы управления ячейками камер на *Медиа Клиенте*.

При захвате камеры оператором SecurOS MCC PA:

- Оператор *Удаленной системы* теряет управление данной камерой и возможность просмотра живого видео с данной камеры.
- Автоматически снимается блокировка управления PTZ с *Камер Удаленной системы* независимо от того, в каком режиме осуществлялось управление PTZ и какой оператор управлял камерой до захвата.
- Если камера находилась в режиме записи оперативного архива, то после захвата запись архива в *Удаленной системе* автоматически прекращается.
- Начинается автоматическая запись "секретного" оперативного архива данной камеры на тот *Видеосервер Центра Мониторинга SecurOS MCC PA*, который выбран в настройках шлюза (см. **Настройка системы**). Это архив доступен для просмотра только оператору *Центра Мониторинга SecurOS MCC PA*.
- Детекторы, используемые *Камерами Удаленной системы* (например, Детектор движения) приостанавливают свою работу.

Примечание. После захвата *Камер Удаленной системы* любые действия оператора SecurOS MCC PA скрываются от операторов штатного Центра мониторинга SecurOS MCC DC и операторов *Удаленной системы*. Аудит таких действий не проводится.

При освобождении камеры оператором SecurOS MCC PA:

- Управление *Камерой* и возможность просмотра живого видео возвращаются оператору *Удаленной системы*.
- Запись "секретного" оперативного архива в *Центре Мониторинга SecurOS MCC PA* автоматически прекращается. Этот архив остается недоступным оператору *Удаленной системы*.
- Режим управления PTZ не изменяется (продолжает соответствовать состоянию, активному на момент освобождения *Камеры*).
- Состояние *Камеры* соответствует тому, которое было у *Камеры* на момент освобождения (если это не противоречит ее настройкам). Возврата к состоянию, которое было у *Камеры* до захвата, не происходит.
- Детекторы, используемые *Камерами Удаленной системы*, возобновляют работу.

15.2.2 Ограничения

В отличие от SecurOS MCC DC, при включенном флажке **Привилегированный доступ к Удаленным системам** SecurOS MCC PA работает с *Удаленными системами* со следующими ограничениями:

- В сети наблюдения за *Удаленными системами* может существовать только один *Центр Мониторинга SecurOS MCC PA*, предоставляющий привилегированный доступ к *Удаленной системе*;
- "Секретный" оперативный архив захваченной камеры *Удаленной системы* записывается только на тот *Видеосервер Центра Мониторинга SecurOS MCC PA*, который выбран в качестве шлюза (см. **Настройка системы**);
- "Секретный" оперативный архив захваченной камеры *Удаленной системы*, записанный в *Центре Мониторинга SecurOS MCC PA*, не может быть конвертирован в долговременный;

- Для корректного экспорта архива, хранящегося в *Удаленной системе*, параметр **Приоритет архивов Конвертера архива** Центра Мониторинга SecurOS MCC PA должен принимать значение **Экспортировать из оперативного, дополнять из Долговременного**. В противном случае экспорт завершится с ошибкой;
- При просмотре оперативного архива камеры *Удаленной системы* поиск **Закладок** и **Тревог**, а также установка **Закладок** в этом архиве невозможны;
- При просмотре "секретного" оперативного архива, записанного в *Центре Мониторинга SecurOS MCC PA*, установка **Закладок** в таком архиве невозможна;
- Просмотр *Долговременного архива* камер *Удаленной системы*, который хранится в *Удаленной системе*, невозможен;
- При просмотре живого видео с захваченных камер *Удаленной системы* в *Центре Мониторинга SecurOS MCC PA* прослушивание сопровождающего звука невозможно;
- При записи оперативного архива захваченной камеры *Удаленной системы* в *Центре Мониторинга SecurOS MCC PA* сопровождающий звук не записывается;
- Аудит действий оператора *Центра Мониторинга SecurOS MCC PA* не проводится.

Примечания:

1. При работе с камерами Модуля SecurOS Auto *Удаленной системы* аудит действий оператора SecurOS MCC PA проводится в обычном режиме;
 2. При работе с камерами *Удаленной системы* с помощью SecurOS ActiveMedia Kit аудит действий пользователя проводится в обычном режиме.
-

15.2.3 Настройка системы

Для возможности проведения спецопераций необходимо:

- **Настроить объекты Центра Мониторинга SecurOS MCC PA.**
- **Настроить объекты Удаленной системы.**

Внимание! Возможность проведения спецопераций из *Центра Мониторинга* может быть заблокирована на стороне *Удаленной системы*. (см. [ниже](#)).

Настройка Центра Мониторинга SecurOS MCC PA

Для настройки *Центра Мониторинга* выполните следующие действия в конфигурации SecurOS MCC PA:

1. В настройках объекта **Система**, дополнительно к прочим настройкам объекта, в блоке **Центр Мониторинга и Контроля** отметьте флажок **Привилегированный доступ к Удаленным системам**.

Внимание! Для проведения обычного мониторинга *Удаленной системы* (без возможности проведения специальных операций) флаг отмечать не требуется.

2. В *Дереве объектов* выберите *Видеосервер*, для которого создайте и настройте дочерний объект **Шлюз MCC DC**.

Внимание! Для подключения каждой *Удаленной системы* в конфигурации SecurOS MCC PA используется собственный отдельный объект **Шлюз MCC DC**. В настройках этого шлюза должен быть выбран только один *Видеосервер*.

3. В настройках выбранного *Видеосервера*, на котором создан объект *Шлюз MCC DC*, выберите диски для записи архива (см. [Архив](#)). Выбранные диски будут использоваться для записи "секретного" оперативного архива *Удаленной системы* в *Центре Мониторинга*, поэтому они должны обладать достаточной емкостью.
4. В *Дереве объектов* создайте и настройте объект **Удаленная система**, включая пароль для подключения к *Удаленной системе*. В параметре **Шлюз для доступа к видео** выберите шлюз, созданный на предыдущем этапе.

Если привилегированный доступ из *Центра Мониторинга* запрещен в настройках *Удаленной системы* (см. [Настройка Удаленной системы](#)), то по отношению к этой *Удаленной системе* *Центр Мониторинга SecurOS MCC PA* будет функционировать как обычный *Центр Мониторинга SecurOS MCC DC*.

При запрете доступа в настройках *Удаленной системы*:

- соединение с *Удаленной системой* будет установлено;
- в окне настроек объекта *Удаленная система* в *Центре Мониторинга* будет выведено соответствующее предупреждение (см. рис. [282](#)):

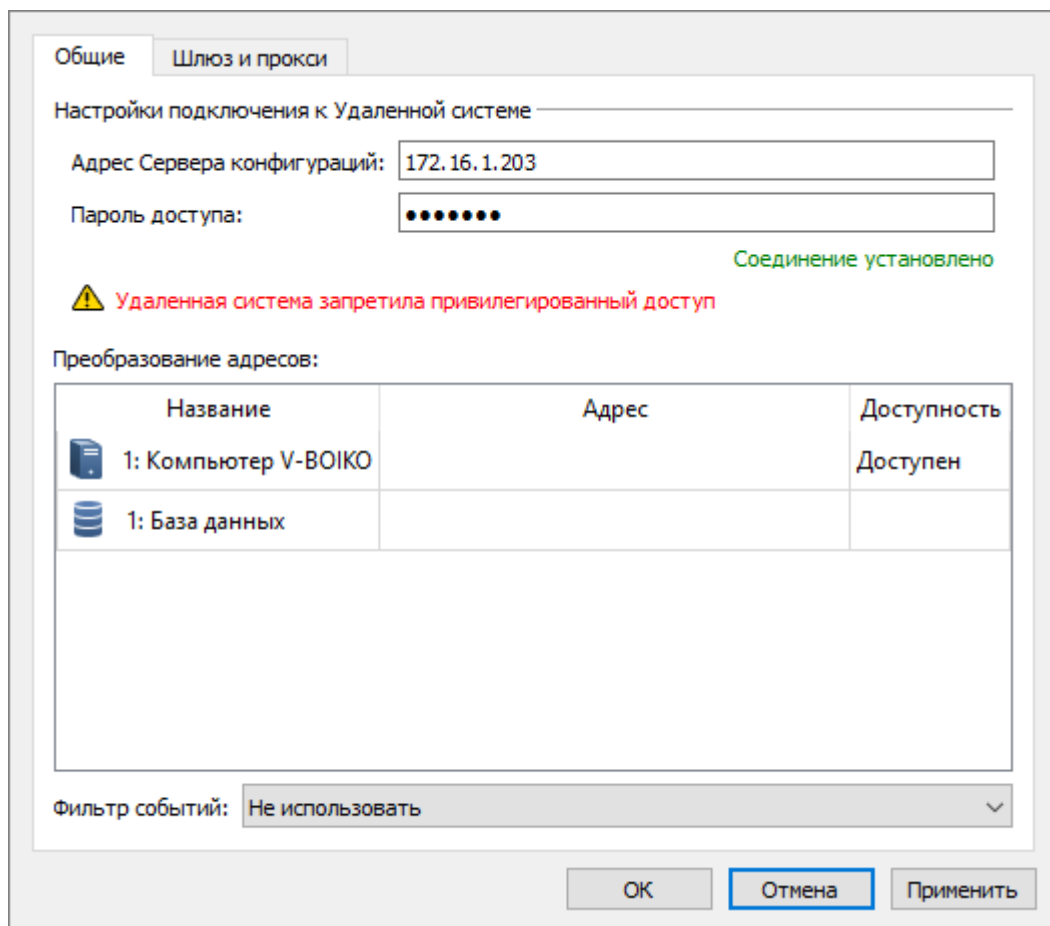


Рис. 282. Привилегированный доступ к *Удаленной системе* запрещен

Настройка Удаленной системы

При настройках *Удаленной системы* по умолчанию *Центр Мониторинга* всегда имеет привилегированный доступ к этой *Удаленной системе*.

Если необходимо запретить привилегированный доступ к данной Удаленной системе из Центра мониторинга, отметьте флажок **Запретить привилегированный доступ** в настройках объекта Система в конфигурации Удаленной системы.

15.2.4 Перенос архива между Удаленной системой и Центром Мониторинга

Оператор Центра Мониторинга может переносить Оперативный архив из Удаленной системы в Центр Мониторинга и в обратном направлении.

Под переносом архива в Центр Мониторинга понимается полное удаление Оперативного архива с Видеосервера Удаленной системы и сохранение его на Видеосервере Центра Мониторинга. Операцию переноса архива можно рассматривать как отложенную запись "секретного" архива в Центре мониторинга при захвате Камеры (см. **Привилегированный доступ**). При этом архив, записанный в Удаленной системе без захвата Камеры, остается доступным для просмотра операторами Удаленной системы до начала операции переноса. По мере выполнения задачи перенесенные фрагменты архива становятся недоступными для операторов Удаленной системы. Такие фрагменты полностью удаляются с временной шкалы архива в Удаленной системе, а в Центре Мониторинга помечаются как "секретный" архив. Для переноса может быть выбран любой интервал архива, созданного любыми Камерами Удаленной системы, которые могут быть захвачены (т. е. в ячейках Камер присутствует кнопка захвата/освобождения управления камерой).

Также возможна обратная операция — полное удаление Оперативного архива с Видеосервера Центра Мониторинга и сохранение его на Видеосервере Удаленной системы. Архив переносится в Удаленную систему вне зависимости от того, как он попал в Центр Мониторинга (был изначально записан как "секретный" или перенесен из Удаленной системы). По мере выполнения задачи, перенесенные фрагменты архива становятся доступны для операторов и появляются на временной шкале архива в Удаленной системе. Если архив во время пребывания на Видеосервере Центра Мониторинга был скопирован в Долговременный архив, то эта копия останется в Долговременном архиве и после переноса Оперативного архива на Видеосервер Удаленной системы.

Функциональность, процедура переноса архива, ее особенности и ограничения, а также настройка системы описаны в следующих подразделах:

- **Функционирование системы при переносе архива.**
- **Ограничения при переносе архива.**
- **Настройка возможности переноса архива.**

Функционирование системы при переносе архива

Перенос архива осуществляется оператором с помощью Медиа Клиента, настроенного в Центре мониторинга (см. **Настройка возможности переноса архива**).

Операции, выполняемые оператором Центра Мониторинга с помощью Медиа Клиента, и подробности переноса архива описаны в **Кратком руководстве пользователя SecurOS**.

Примечание. Перенос архива также возможен с помощью скриптов. Описание команд переноса приведено в **Руководстве программиста SecurOS**.

Ограничения при переносе архива

При переносе архива действуют следующие ограничения:

- Перенос архива возможен только для тех *Камер*, которые можно захватить (т. е. в ячейках *Камер* присутствует кнопка захвата/освобождения управления).
- В *Центр Мониторинга* можно перенести архив, записанный в *Удаленной системе* с установленной системой SecurOS версии 11.4 или выше. Для переноса архива из *Центра Мониторинга* в *Удаленную систему* необходимо, чтобы система SecurOS была обновлена до версии 11.9 или выше.
- Если *Удаленная система* организована как кластер серверов, перенос архива в *Центр Мониторинга* с локальных дисков резервных *Хостов* невозможен. Перенести можно только тот архив, который сохранен на *Нодах* кластера. При переносе архива в *Удаленную систему* он будет сохранен на том *Хосте*, на котором выполняется *Нода*.
- Звук, сопровождающий видеоархив, *Тревоги*, *Закладки* и метаданные ретроспективного поиска не переносятся.
- *Долговременный архив* не переносится.
- После переноса архива из *Центра Мониторинга* в *Удаленную систему*, для копирования записей в *Долговременный архив* потребуется ручной запуск процедуры архивации для требуемого временного интервала.
- Дополнение перенесенного архива новыми фрагментами невозможно (например, при формировании архива, собранного с помощью технологии EdgeStorage Sync). Если архив был перенесен в *Центр мониторинга*, то освободившееся место в *Удаленной системе* может быть перезаписано средствами EdgeStorage Sync. В этом случае перенос архива обратно в *Удаленную систему* приведет к ошибкам наложения фрагментов архива друг на друга и перенести архив будет невозможно.

Настройка возможности переноса архива

Настройка системы для переноса архива выполняется только на стороне *Центра Мониторинга*, настроенного для работы в режиме *Привилегированного доступа* (см. **Настройка системы**). Для возможности переноса архива дополнительно выполните следующие действия:

1. В *Дереве объектов Центра Мониторинга* выберите *Медиа Клиент*, который будет использоваться для переноса архива из *Удаленной системы*. В настройках выбранного *Медиа Клиента* на закладке **Экспорт и архив** отметьте флажок **Возможность переноса архива из Удаленной системы**.
2. После применения новой настройки в окне выбранного *Медиа Клиента* будет отображена дополнительная панель **Перенос архива**.

16 Резервирование

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

Раздел описывает способы резервирования серверов SecurOS. Существует два способа организовать резервирование:

- **Отказоустойчивый кластер.**
- **Кластер резервных серверов.**

16.1 Отказоустойчивый кластер

Для обеспечения дополнительной надежности сети безопасности SecurOS и упрощения процесса обновления аппаратного обеспечения, *Видеосерверы* могут быть объединены в отказоустойчивый кластер. Отказоустойчивый кластер представляет собой группу компьютеров, способную за счет резервных серверов самостоятельно поддерживать работу сети безопасности в случае выхода из строя некоторых из них.

16.1.1 Структура кластера

Кластер представляет собой логическую структуру, состоящую из следующих элементов:

- **Хост** — произвольный физический компьютер, на котором установлено ПО *Видеосервера* SecurOS. Такой компьютер учитывается только в конфигурации кластера, независимой от конфигурации SecurOS, и не отображается в *Дереве объектов* SecurOS;
- **Нода** — абстрактная сущность, представленная в *Дереве объектов* SecurOS объектом *Компьютер* с ролью *Видеосервер*. При этом, в отличие от независимых *Видеосерверов*, *Нода* не привязана к конкретному физическому компьютеру и может выполняться на любом *Хосте* кластера. Для создания *Ноды* в настройках объекта *Компьютер* необходимо активировать опцию **Резервировать Видеосервер и добавить его в кластер**, а также указать свободный виртуальный IP-адрес в поле **IP-адрес сервера**. Этот IP-адрес остается неизменным вне зависимости от того, на каком *Хосте* выполняется *Нода*.

Примечание. Независимый *Видеосервер* представляет собой физический компьютер с фиксированным IP-адресом и установленным ПО SecurOS, который не является членом кластера и отображается в *Дереве объектов*. В конфигурации SecurOS могут одновременно присутствовать как независимые *Видеосерверы*, так и *Ноды*.

Внимание! При резервировании роль *Сервера конфигураций* SecurOS всегда выполняет один из *Хостов* кластера.

Схематичное изображение структуры кластера представлено на рис. 283.

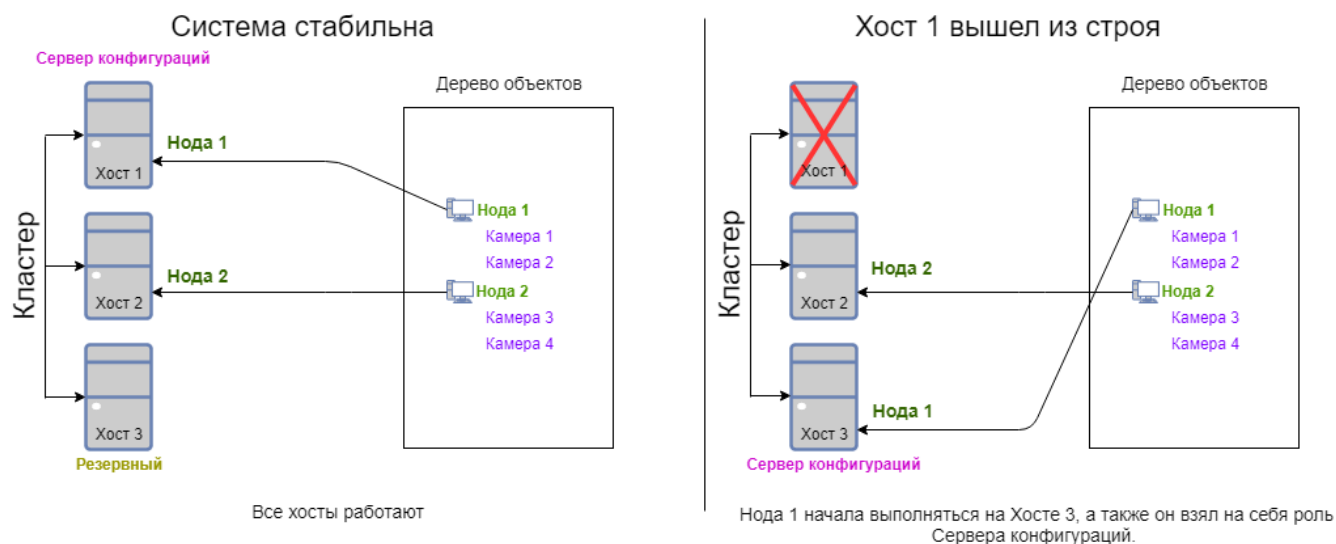


Рис. 283. Структура кластера

16.1.1.1 Конфигурация кластера

Информация о *Хостах* и *Нодах* (их имена, параметры и состояние) представляет собой конфигурацию кластера. Она существует независимо от конфигурации SecurOS и управляется с помощью отдельной утилиты (см. [Конфигурирование кластера](#)).

16.1.1.2 Функционирование кластера. Кворум

Для того, чтобы кластер мог выполнять функцию резервирования, количество *Хостов* должно превышать количество *Нод*. *Хосты* кластера могут находиться в двух состояниях:

- **Действующий хост** — на действующих *Хостах* выполняются *Ноды*. Под выполнением *Ноды* понимается запуск и выполнение всех процессов, которые обеспечивают функционирование SecurOS. На одном *Хосте* может выполняться только одна *Нода*.
- **Резервный хост** — резервные *Хосты* находятся в режиме ожидания. При выходе действующего *Хоста* из строя, выполнявшаяся на нем *Нода* начнет выполняться на резервном *Хосте*. Выбор резервного *Хоста* осуществляется системой автоматически.

Если вышедший из строя *Хост* восстановился после распределения всех *Нод*, он переходит в состояние резервного. Роль *Сервера конфигураций* также автоматически назначается другому *Хосту* в случае необходимости. Это поведение может быть изменено с помощью сервисного режима (см. [Сервисный режим](#)).

Роль *Сервера конфигураций* может быть назначена как действующему, так и резервному хосту.

Работа кластера возможна до тех пор, пока все его *Хосты* (действующие и резервные) поддерживают кворум. Кворум существует, пока более половины *Хостов* находятся в рабочем состоянии.

Потеря кворума

Потеря кворума в кластере имеет следующие последствия:

- Все *Хосты*, включая те, которые сохранили свою работоспособность, не смогут функционировать. В этом случае весь кластер прекратит работу и будет ожидать восстановления кворума (см. [Решение типовых проблем](#)). Это не коснется тех *Видеосерверов* в конфигурации SecurOS, которые не являются членами кластера.

Примечание. Подобное поведение является типичным для всех кластерных структур и не является особенностью реализации SecurOS.

- Большинство команд конфигурирования кластера не сможет быть выполнено.

Пример

Потеря кворума в следующих конфигурациях будет происходить таким образом:

- Кластер из 2 *Хостов*. Кворум будет потерян, если 1 *Хост* выйдет из строя (см. раздел **Кластер резервных серверов** для создания эффективного кластера из двух *Хостов*).
- Кластер из 3 *Хостов*. Кворум будет потерян, если 2 *Хоста* выйдут из строя.
- Кластер из 4 *Хостов*. Кворум будет потерян, если 2 *Хоста* выйдут из строя.
- Кластер из 5 *Хостов*. Кворум будет потерян, если 3 *Хоста* выйдут из строя, и так далее.

Поведение системы при потере и восстановлении кворума изображены на рис. 284.

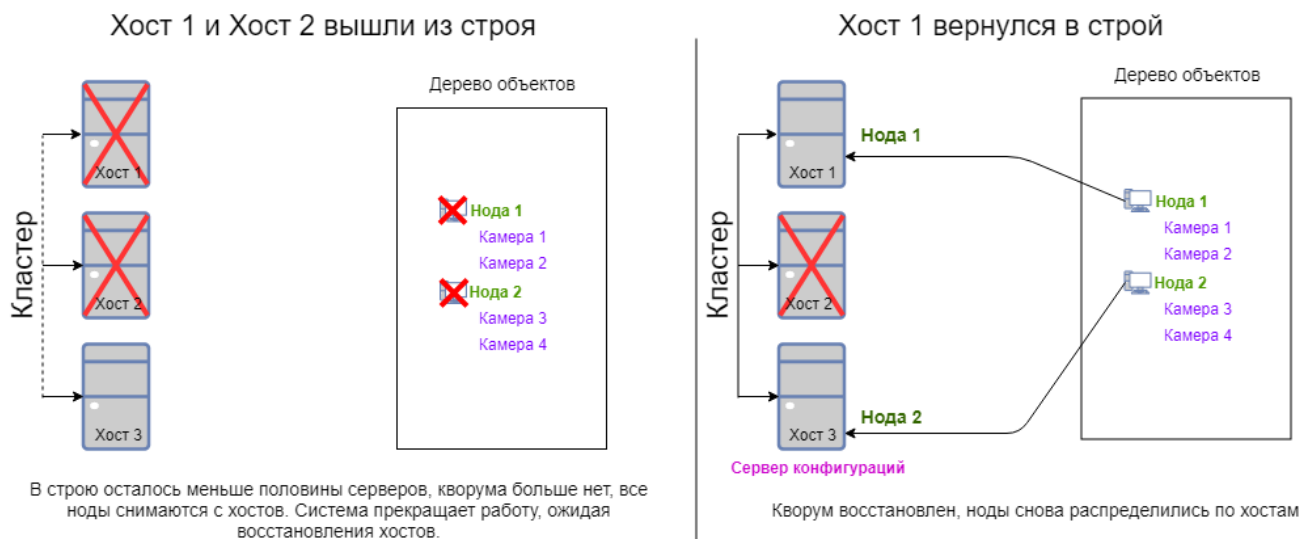


Рис. 284. Потеря и восстановление кворума в конфигурации из трех Хостов

16.1.1.3 Рекомендации

Для связи между серверами кластера рекомендуется использовать отдельный сетевой интерфейс (см. **Изменение сетевого интерфейса для виртуальных адресов**).

Для хранения данных рекомендуется использовать централизованное хранилище. Для хранения видеоданных можно использовать сетевые папки (доступ по протоколам CIFS (SMB)) или iSCSI-диск. Для остальных данных используйте хранилища iSCSI (см. **iSCSI-диск**).

Внимание! Для взаимодействия *Хостов* в кластере необходимо обеспечить доступность сетевых портов (см. **Приложение 5. Используемые в SecurOS сетевые порты**).

16.1.2 Конфигурирование кластера

Для работы с кластером рекомендуется использовать утилиту **Server Manager**. Она имеет удобный графический интерфейс, позволяющий выполнить все необходимые операции с кластером и контролировать его работу в реальном времени.

Альтернативным способом конфигурирования и управления кластером является консольная утилита `clustercli.exe`, которая находится в корневой папке SecurOS.

Внимание! Для выполнения команд с помощью утилиты в ОС Windows требуются права администратора.

Операции создания и настройки кластера с помощью командной строки описываются в следующих разделах:

- **Создание кластера;**
 - **Перенастройка конфигурации SecurOS на работу с кластером;**
 - **Создание конфигурации SecurOS с кластером;**
- **Получение текущей конфигурации кластера;**
- **Создание Объекта охраны;**
- **Добавление Хоста;**
- **Подключение компьютера к кластеру резервных серверов;**
- **Удаление Хоста;**
- **Перевод в режим Видеосервера;**
- **Добавление Ноды;**
- **Удаление Ноды;**
- **Получение списка Нод;**
- **Выбор приоритетного Хоста для Ноды;**
- **Ручной перенос Ноды на Хост;**
- **Пересоздание кластера;**
- **Восстановление конфигурации SecurOS из файла;**
- **Выбор Сервера конфигураций;**
- **Преобразование независимого Видеосервера в Ноду кластера;**
- **Сервисный режим;**
- **Изменение сетевого интерфейса для виртуальных адресов;**
- **Настройка временных интервалов.**

16.1.2.1 Создание кластера

Внимание! Перед созданием кластера рекомендуется сохранить текущую конфигурацию SecurOS (см. Система).

Чтобы создать кластер, выполните на одном из его будущих *Хостов* следующую команду:

```
Clustercli.exe create <heartbeat_nic> <virtual_ip_nic> <config_server_virt_ip>
```

Где:

- `heartbeat_nic` – IP-адрес данного компьютера, по которому он будет доступен для обмена данными с другими *Хостами*;
- `virtual_ip_nic` – IP-адрес сетевого интерфейса на этом компьютере, которому будут назначаться виртуальные IP-адреса;

Примечание. Для компьютера с одним сетевым адаптером необходимо продублировать значение параметра `heartbeat_nic`. Этот адрес в дальнейшем может быть изменен с помощью отдельной команды (см. [Изменение сетевого интерфейса для виртуальных адресов](#)).

- `config_server_virt_ip` – виртуальный IP-адрес, по которому будет доступен *Сервер конфигураций*. Этот адрес должен быть уникальным в локальной сети и будет назначаться сетевому интерфейсу на том *Хосте*, который должен выполнять роль *Сервера конфигураций*. В случае выхода такого *Хоста* из строя этот IP-адрес может мигрировать на другие *Хосты*.

После успешного выполнения команды кластер будет готов к работе. Он будет состоять из одного *Хоста*, который является *Сервером конфигураций*.

Внимание! Если команда выполнялась не на текущем *Сервере конфигураций* SecurOS, то на данном этапе в системе будут существовать две конкурирующие конфигурации. Устранение этой проблемы рассмотрено в разделе [Перенастройка конфигурации SecurOS на работу с кластером. Пример](#).

В зависимости от того, существует ли добавляемых в кластер компьютерах конфигурация SecurOS или нет, дальнейшие действия различаются. Подробности см. в следующих разделах:

- [Перенастройка конфигурации SecurOS на работу с кластером](#);
- [Создание конфигурации SecurOS с кластером](#).

16.1.2.1.1 Перенастройка конфигурации SecurOS на работу с кластером

Выполните команду `create` на компьютере, который уже является частью сети безопасности SecurOS с некоторой конфигурацией. Далее, чтобы начать конфигурирование системы, выполните следующие шаги:

1. Если некоторые *Видеосерверы*, в том числе старый *Сервер конфигураций*, должны остаться независимыми (т.е. их не следует добавлять в кластер), настройте их на работу с новым *Сервером конфигураций*. Для этого на каждом из них с помощью утилиты *Server Role Manager* (см. [Утилита Server Role Manager](#)) укажите IP-адрес нового *Сервера конфигураций* – параметр `config_server_virt_ip`, использованный при выполнении команды создания кластера.
2. Создайте хотя бы одну *Ноду*, к которой сможет подключиться *Рабочее место оператора* (см. [Добавление Ноды](#)). При необходимости можно преобразовать в *Ноду* один из *Видеосерверов* текущей конфигурации (см. [Преобразование независимого Видеосервера в Ноду кластера](#)).

16.1.2.1.2 Создание конфигурации SecurOS с кластером

Если необходимо создать кластер и, одновременно, сеть SecurOS с новой конфигурацией, выполните команду `create` на произвольном компьютере, на котором установлено ПО SecurOS. Далее, чтобы начать конфигурирование системы, выполните следующие шаги:

1. Создайте *Объект охраны* (см. [Создание Объекта охраны](#)).
2. Создайте хотя бы одну *Ноду*, к которой сможет подключиться *Рабочее место оператора* (см. [Добавление Ноды](#)).

Более детально процесс создания кластера при отсутствующей конфигурации рассмотрен в разделе [Примеры создания и настройки кластера](#).

16.1.2.2 Получение текущей конфигурации кластера

Чтобы узнать текущую конфигурацию кластера, на любом из *Хостов* выполните следующую команду:

```
Clustercli.exe state
```

На консоль будет выведена следующая информация:

1. Виртуальный IP-адрес *Сервера конфигураций*.
2. Список *Нод*, с указанием для каждой из них следующих параметров:
 - Ревизия конфигурации SecurOS на момент создания *Ноды*.

Примечание. Ревизия конфигурации представляет собой число, соответствующее количеству изменений, выполненных в этой конфигурации.

- Виртуальный IP-адрес *Ноды*.
 - Приоритетный *Хост* для этой *Ноды* (если задан).
3. Имя *Хоста*, который выполняет роль *Сервера конфигураций*.
 4. Список пар из *Нод* и *Хостов*, на которых эти *Ноды* выполняются.
 5. Список *Хостов* с указанием их IP-адресов и текущей ревизии конфигурации.
 6. Список подключенных к кластеру серверов (см. [Кластер резервных серверов](#)) с указанием текущей ревизии конфигурации.
 7. Список добавленных на этом *Хосте* локальных дисков (см. [Хранение видеоархива на локальных дисках Хостов](#)).
 8. Текущие значения параметров тонкой настройки кластера (см. [Настройка временных интервалов](#)).

Внимание! При отсутствии кворума (см. [Функционирование кластера. Кворум](#)) узнать состояния кластера невозможно.

Внешний вид результата работы команды в командной строке представлен на рис. [285](#):

```
C:\Program Files (x86)\ISS\SecurOS>clustercli.exe state
Created: 2020-10-14T16:01:56
Settings: {
  "csIp": "172.16.11.70",
  "nodes": {
    "NODE": {
      "crRev": "17",
      "ip": "172.16.11.71",
      "prefHost": ""
    }
  }
}
CS host: VQA-45
State: {
  "nodes": {
    "NODE": "VQA-40"
  }
}
Hosts:
  VQA-40(https://172.16.11.160:2381) csRevision=86
  VQA-45(https://172.16.11.145:2381) csRevision=86
Supplementary hosts online:
This host (VQA-40):
  Local drives:
    No local drives configured
Quorum timeout: 5 s., heartbeat interval: 100 ms., election timeout: 1000 ms.
C:\Program Files (x86)\ISS\SecurOS>
```

Рис. 285. Состояние кластера

16.1.2.3 Создание Объекта охраны

Если кластер настраивается в системе, где еще нет конфигурации SecurOS, необходимо сначала создать первый *Объект охраны*. Для этого на любом из хостов выполните команду:

```
Clustercli.exe node createzone <zone_id>
```

Где:

- `zone_id` – идентификатор *Объекта охраны*.

При выполнении команды при необходимости будет автоматически создан корневой объект *Система*.

16.1.2.4 Добавление Хоста

Чтобы сделать компьютер *Хостом* кластера, выполните на этом компьютере следующую команду:

```
Clustercli.exe join <heartbeat_nic> <virtual_ip_nic> <other_host_ip>
```

Где:

- `heartbeat_nic` – IP-адрес данного компьютера, по которому он будет доступен для обмена данными с другими *Хостами*;

- `virtual_ip_nic` – IP-адрес сетевого интерфейса на этом компьютере, которому будут назначаться виртуальные IP-адреса;

Примечание. Для компьютера с одним сетевым адаптером необходимо продублировать значение параметра `heartbeat_nic`. Этот адрес в дальнейшем может быть изменен с помощью отдельной команды (см. [Изменение сетевого интерфейса для виртуальных адресов](#)).

- `other_host_ip` – IP-адрес одного из *Хостов* кластера.

Внимание! Указание неверного или недоступного IP-адреса в качестве значения параметра `this_real_ip` может привести к потере кворума (см. [Решение типовых проблем](#)).

После выполнения команды служба SecurOS перезапустится и начнет работу в режиме *Хоста* кластера.

Внимание! Если на компьютере, добавляемом в кластер, хранится предыдущая конфигурация SecurOS, то она будет перезаписана.

16.1.2.5 Подключение компьютера к кластеру резервных серверов

Для подключения компьютера к кластеру резервных серверов выполните на нем следующую команду:

```
Clustercli.exe attach <virtual_ip_nic> <hosts_list>
```

Где:

- `virtual_ip_nic` – IP-адрес сетевого интерфейса на этом компьютере, которому будут назначаться виртуальные IP-адреса;
- `hosts_list` – список IP-адресов *Хостов* кластера резервных серверов, указанных через пробел. Рекомендуется указать адреса всех *Хостов*.

После выполнения команды служба SecurOS перезапустится.

Внимание! Если на компьютере, добавляемом в кластер, хранится предыдущая конфигурация SecurOS, то она будет перезаписана.

После подключения компьютера к кластеру необходимо сразу сделать его приоритетным для одной из *Нод* (см. [Выбор приоритетного Хоста для Ноды](#)).

Такой сервер не может быть отключен от кластера с помощью команды `remove`. Выполните команду `leave` (см. [Перевод в режим Видеосервера](#)) на этом компьютере, чтобы кластер перестал учитывать его при распределении *Нод*.

16.1.2.6 Удаление Хоста

Чтобы удалить *Хост* из конфигурации кластера, выполните на любом из *Хостов* следующую команду:

```
Clustercli.exe remove <host_to_remove_ip> <other_host_ip>
```

Где:

- `host_to_remove_ip` – IP-адрес *Хоста*, который необходимо удалить из кластера;
- `other_host_ip` – IP-адрес одного из *Хостов* кластера.

Примечание. Чтобы вернуть компьютер в обычный режим работы, недостаточно удалить его из кластера. Необходимо также перевести его в режим *Видеосервера* (см. [Перевод в режим Видеосервера](#)).

16.1.2.7 Перевод в режим Видеосервера

Чтобы окончательно перевести компьютер в режим работы независимого *Видеосервера*, на этом компьютере необходимо выполнить следующую команду:

```
Clustercli.exe leave [-f]
```

Где:

- `[-f]` – необязательный ключ для принудительного выполнения команды.

Команда работает в два шага:

1. Отправляет команду на удаление *Хоста* из кластера (см. [Удаление Хоста](#)).
2. Переводит компьютер в режим независимого *Видеосервера*.

В случае, если первый шаг не может быть завершен, например, в связи с отсутствием кворума (см. [Функционирование кластера. Кворум](#)), второй шаг выполняться не будет. Если же необходимо всё равно выполнить переход в режим *Видеосервера*, пропустите первый шаг. Для этого используйте ключ `-f`, позволяющий осуществить принудительное выполнение команды.

16.1.2.8 Добавление Ноды

Чтобы добавить *Ноду* в конфигурацию кластера, выполните на любом из *Хостов* следующую команду:

```
Clustercli.exe node create <node_name> <node_virt_ip> <zone_id>
```

Где:

- `node_name` – имя и одновременно идентификатор создаваемой *Ноды*;
- `node_virt_ip` – виртуальный IP-адрес, по которому будет доступна *Нода*. Этот адрес должен быть свободным в локальной сети и быть уникальным;
- `zone_id` – идентификатор *Объекта охраны*, который будет родительским для *Ноды*.

Примечание. В отличие от независимых *Видеосерверов*, идентификатор *Ноды* не обязан совпадать с сетевым именем компьютера, на котором она будет выполняться.

Новые *Ноды* можно добавлять и через *Дерево объектов SecurOS*. Для этого выполните следующие шаги:

1. Подключитесь к работающей *Ноды* с помощью клиентского приложения (см. [Подключение Рабочих мест оператора к серверам кластера](#)).
2. Создайте в конфигурации объект *Компьютер* с ролью *Видеосервер*.

3. В настройках этого *Компьютера* отметьте флажок **Резервировать Видеосервер и добавить его в кластер**.

4. Укажите в поле **IP-адрес сервера** виртуальный IP-адрес *Ноды*.

Виртуальный адрес будет закреплен за *Нодой*, которая будет доступна по этому адресу вне зависимости от того, на каком *Хосте* она сейчас выполняется.

16.1.2.9 Удаление Ноды

Чтобы удалить *Ноду* из конфигурации, выполните на любом из *Хостов* следующую команду:

```
Clustercli.exe node remove <node_name>
```

Где:

- `node_name` – идентификатор *Ноды*, которую необходимо удалить.

Внимание! Удаление *Ноды* приведет к удалению всех *Камер* и других дочерних объектов.

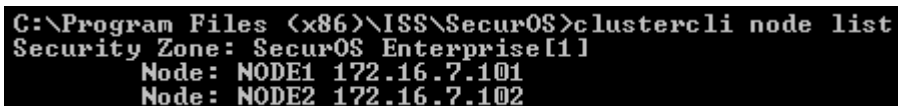
16.1.2.10 Получение списка Нод

Чтобы получить список всех *Нод* конфигурации, выполните следующую команду:

```
Clustercli.exe node list
```

Будет выведен список *Нод* с указанием идентификатора и виртуального IP-адреса для каждой.

Внешний вид результата работы команды в командной строке представлен на рисунке 286:



```
C:\Program Files (x86)\ISS\SecurOS>clustercli node list
Security Zone: SecurOS Enterprise[1]
Node: NODE1 172.16.7.101
Node: NODE2 172.16.7.102
```

Рис. 286. Список Нод

16.1.2.11 Выбор приоритетного Хоста для Ноды

Если необходимо, чтобы определенная *Нода* всегда стремилась выполняться на конкретном *Хосте* (например, в связи с его более высокой производительностью), выполните следующую команду:

```
Clustercli.exe node set <node_name> pref_host=<host_name>
```

Где:

- `node_name` – имя *Ноды*, для которой задается приоритетный *Хост*;
- `host_name` – имя *Хоста*, который будет приоритетным для указанной *Ноды*.

Примечание. Чтобы отменить приоритет *Хоста* для *Ноды*, выполните команду с пустым значением параметра `pref_host`. Например, `Clustercli.exe node set Node_1 pref_host=`.

Ноды с выбранными приоритетными *Хостами* подчиняются следующим правилам:

1. *Нода* будет пытаться занять свой приоритетный *Хост* при первой возможности.

2. Если один *Хост* является приоритетным сразу для нескольких *Нод*, выбор той, которая его займет, происходит случайным образом. При этом она не сможет быть вытеснена с этого *Хоста* автоматически.
3. В момент присваивания *Ноды* приоритетного *Хоста*, она вытеснит ту *Ноду*, которая выполняется на этом *Хосте* в данный момент (при условии, что для текущей *Ноды* выбранный *Хост* не является приоритетным). Вытесненная *Нода* займет другой свободный *Хост*, если такие имеются.

16.1.2.12 Ручной перенос Ноды на Хост

Если необходимо вручную перенести *Ноду* на желаемый *Хост*, выполните следующую команду:

```
Clustercli.exe node move <node_name> <host_name>
```

Где:

- node_name – имя *Ноды*, которую необходимо перенести;
- host_name – имя *Хоста*, на котором будет выполняться указанная *Нода*.

Процесс ручного переноса *Ноды* на *Хост* подчиняется следующим правилам:

1. Если на указанном *Хосте* уже выполняется другая *Нода*, она будет вытеснена.
2. Если при переносе была вытеснена *Нода*, для которой этот *Хост* является приоритетным, дальнейшее поведение будет определено правилами для *Нод* с приоритетом.

Примечание. Не рекомендуется использовать ручной перенос *Нод* в качестве средства для конфигурирования кластера. Грамотная настройка приоритетов для *Нод* позволит достичь лучших результатов (см. [Выбор приоритетного Хоста для Ноды](#)).

16.1.2.13 Пересоздание кластера

При необходимости заново собрать кластер, сохранив его конфигурацию (см. [Конфигурация кластера](#)) за исключением списка *Хостов*, выполните на любом из *Хостов* следующую команду:

```
Clustercli.exe recreate <heartbeat_nic> <virtual_ip_nic>  
<config_server_virt_ip>
```

Где:

- heartbeat_nic – IP-адрес данного компьютера, по которому он будет доступен для обмена данными с другими *Хостами*;
- virtual_ip_nic – IP-адрес сетевого интерфейса на этом компьютере, которому будут назначаться виртуальные IP-адреса;

Примечание. Для компьютера с одним сетевым адаптером необходимо продублировать значение параметра heartbeat_nic. Этот адрес в дальнейшем может быть изменен с помощью отдельной команды (см. [Изменение сетевого интерфейса для виртуальных адресов](#)).

- config_server_virt_ip – виртуальный IP-адрес, по которому будет доступен *Сервер конфигураций*. Этот адрес должен быть уникальным в локальной сети и будет назначаться

сетевому интерфейсу на том *Хосте*, который должен выполнять роль *Сервера конфигураций*. В случае выхода такого *Хоста* из строя этот IP-адрес может мигрировать на другие *Хосты*.

После выполнения команды кластер будет состоять из одного *Хоста*. Остальные хосты должны быть присоединены к кластеру заново (см. [Добавление Хоста](#)).

Примечание. Пересоздание кластера является одним из способов решения проблемы потери кворума (см. [Решение типовых проблем](#)).

16.1.2.14 Восстановление конфигурации SecurOS из файла

Если конфигурация SecurOS была предварительно сохранена в файл, его можно использовать для восстановления конфигурации. Для этого на любом *Хосте* выполните следующую команду:

```
Clustercli.exe config-restore <path_to_file>
```

Где:

- `path_to_file` – полный или относительный путь к файлу с сохраненной конфигурацией.

Примечание. При выполнении команды список *Хостов* кластера не восстанавливается. В случае необходимости их нужно добавить в кластер вручную (см. [Добавление хоста](#)).

Перед тем, как команда будет выполнена, текущая конфигурация SecurOS сохранится в файл `ISS\Sys_config\cluster_backup.json`, путь к которому задается в значении переменной среды `%ProgramData%`.

Внимание!

1. Для восстановления рекомендуется использовать ту копию файла конфигурации, которая соответствует текущей установленной версии SecurOS. При восстановлении конфигурации из файлов других версий корректная работа SecurOS не гарантируется.
2. Файл конфигурации хранится на том *Хосте*, который выполнял роль *Сервера конфигураций* на момент выполнения команды.
3. Текущий пароль суперпользователя (см. [Пользователи в SecurOS](#)) не изменится после восстановления конфигурации.

16.1.2.15 Выбор Сервера конфигураций

Если необходимо, чтобы роль *Сервера конфигураций* выполнял конкретный *Хост* в кластере, выполните на любом из *Хостов* следующую команду:

```
Clustercli.exe set cs=<new_cs_host>
```

Где:

- `new_cs_host` – имя *Хоста*, который должен выполнять роль *Сервера конфигураций*.

Примечания:

1. В случае если *Хост*, выбранный на роль *Сервера конфигураций*, выйдет из строя, новый *Сервер конфигураций* будет назначен автоматически. Это поведение можно изменить с помощью сервисного режима (см. [Сервисный режим](#)).
 2. На роль *Сервера конфигураций* может быть назначен только член кластера.
-

16.1.2.16 Преобразование независимого Видеосервера в Ноду кластера

Если кластер создается на основе существующей конфигурации SecurOS, то после его создания необходимо преобразовать независимые *Видеосерверы* в *Ноды*. Для этого на любом из *Хостов* выполните команду:

```
Clustercli.exe node update <videoserver_id> <node_virt_ip>
```

Где:

- *videoserver_id* – идентификатор *Видеосервера* в *Дереве объектов SecurOS*, который необходимо преобразовать в *Ноду*;
- *node_virt_ip* – виртуальный IP-адрес, который будет присвоен *Ноду*.

Примечание. Эту же команду можно использовать для изменения виртуального IP-адреса существующей *Ноды*.

16.1.2.17 Сервисный режим

Сервисный режим позволяет выполнить замену оборудования или обновление программного обеспечения, не нарушая конфигурацию кластера (см. [Конфигурация кластера](#)). Существует два варианта сервисного режима:

- *Фиксированный Сервер конфигураций* – в этом варианте роль *Сервера конфигураций* не будет назначена другому *Хосту* автоматически.
- *Полная фиксация* – в этом варианте не только *Сервер конфигураций*, но и *Ноды* не будут автоматически менять *Хосты*.

Для входа в сервисный режим на любом из *Хостов* выполните следующую команду:

```
Clustercli.exe set service_mode=<service_mode_name>
```

Где:

- *service_mode_name* – вариант сервисного режима:
 - *fixed_cs* – фиксированный *Сервер конфигураций*;
 - *fixed_all* – полная фиксация.

Для выхода из сервисного режима выполните на любом из *Хостов* следующую команду:

```
Clustercli.exe set service_mode=
```

Эта команда обнулит текущее значение сервисного режима, и перенос *Нод* и роли *Сервера конфигураций* вновь будет выполняться автоматически.

16.1.2.18 Изменение сетевого интерфейса для виртуальных адресов

Рабочие места оператора подключаются к сети безопасности через виртуальные IP-адреса *Нод*. От того, какому сетевому интерфейсу *Хоста* назначены эти виртуальные адреса, зависит распределение нагрузки на сеть. Рекомендуется, чтобы виртуальные адреса были назначены сетевому интерфейсу, отличному от того, который используют *Хосты* кластера для связи друг с другом.

Чтобы изменить сетевой интерфейс, которому следует назначать виртуальные IP-адреса, выполните следующую команду:

```
Clustercli.exe set virtual_ip_nic=<ip_address>
```

Где:

- *ip_address* – IP-адрес сетевого интерфейса на этом компьютере, которому будут назначаться виртуальные IP-адреса.

16.1.2.19 Настройка временных интервалов

Внимание!

1. Перечисленные ниже команды тонкой настройки допускается выполнять только после согласования со Службой технической поддержки Intelligent Security Systems. В противном случае Intelligent Security Systems не несет ответственности за корректное функционирование кластера.
2. При нормальном функционировании кластера применять указанные команды крайне не рекомендуется.

В разделе описаны следующие команды тонкой настройки кластера:

- **set heartbeat_interval election_timeout** — настройка интервала проверки доступности *Хостов* кластера и время, необходимое для признания *Хоста* недоступным;
- **set quorum_timeout** — время, по истечении которого после признания *Хоста* недоступным задействуются механизмы резервирования кластера.

Примечание. Текущие значения всех перечисленных ниже настраиваемых параметров можно узнать с помощью команды **state**.

set heartbeat_interval election_timeout

Доступность *Хостов* кластера определяется периодически, с помощью отправки им широковещательных сообщений (хартбитов). Если *Хост* не отправил членам кластера сообщение о доступности в течение заданного таймаута, то он считается недоступным.

Чтобы изменить указанные интервалы, выполните следующую команду:

```
Clustercli.exe set heartbeat_interval=<time1> election_timeout=<time2>
```

Где:

- *<time1>* – требуемый период отправки сообщений (в миллисекундах). Диапазон возможных значений: [10; 100]. По умолчанию равен 50 мс;

- `<time2>` – таймаут сообщения о доступности (в миллисекундах). Диапазон возможных значений: [100; 1000]. По умолчанию равен 500 мс. Значение `<time2>` должно быть как минимум в 5 раз больше значения `<time1>`.

Внимание! Выполнение этой команды приведет к перезапуску SecurOS на всех *Хостах* кластера! Выполнять эту команду следует только тогда, когда все *Хосты* кластера находятся онлайн. В противном случае могут возникнуть проблемы функционирования кластера.

set quorum_timeout

После признания *Хоста* недоступным спустя заданный таймаут задействуются механизмы резервирования. По умолчанию равен 5 секундам.

Чтобы изменить таймаут, выполните следующую команду:

```
Clustercli.exe set quorum_timeout=<time>
```

Где:

- `<time>` – таймаут до включения механизмов резервирования (в секундах). Диапазон возможных значений: [5; 300].

16.1.3 Подключение Рабочих мест оператора к серверам кластера

Рабочие места оператора могут подключаться к серверам SecurOS, работающим в кластере. Для этого в окне авторизации необходимо указать **виртуальный IP-адрес** одной из *Нод*. В случае, если *Хост* выйдет из строя, клиентское приложение автоматически переподключится к этой же *Нод*е после того, как она запустится на новом *Хосте*.

Примечание. Если в кластере пока нет ни одной *Ноды*, используйте IP-адрес одного из *Хостов*, чтобы сконфигурировать SecurOS.

Ограничение подключения клиентских приложений, запущенных на Хостах кластера

Настройки объекта *Объект охраны* позволяют ограничить подключение клиентских приложений к серверам SecurOS (см. **Закладка Ограничение подключений**). В случае, если *Хост* кластера одновременно используется как *Рабочее место оператора*, в белый список IP-адресов необходимо добавить не только IP-адрес самого компьютера, но и виртуальные IP-адреса всех *Нод* кластера и виртуальный IP-адрес *Сервера конфигураций*.

16.1.4 Организация хранилища в кластере

При работе в кластере особое внимание следует уделить организации хранилища для видеоархива и баз данных.

Для записи видеоархива можно использовать следующие виды хранилищ:

- **Сетевая папка (CIFS)** — наиболее **безопасный** вариант централизованного хранилища.
- **iSCSI-диск** — наиболее **быстрый** вариант централизованного хранилища (подробнее см. **iSCSI-диск**).

Внимание! В ОС Linux возможность использования iSCSI-дисков не поддерживается.

Помимо видеоархива iSCSI-диски могут быть использованы для хранения баз данных. Например, базы данных *Протокола событий*, модулей распознавания и так далее (см. [Перемещаемый PostgreSQL](#)).

- **Локальные диски** позволяют хранить видеоархив непосредственно на *Хостах* кластера. Записи со всех *Хостов* доступны оператору для просмотра в виде объединенного архива. В случае выхода *Хоста* из строя, соответствующая часть архива будет временно недоступна.

Примечание. На *Хосте*, где работает *Нода*, могут быть заданы локальные диски для записи архива. В этом случае приоритет записи архива определяется настройками (см. [Расширенные настройки кластера](#)).

Этот вид хранилища рекомендуется использовать в **Кластере резервных серверов** в связи с его ограничениями. Подробности настройки см. в разделе **Хранение видеоархива на локальных дисках Хостов**.

16.1.4.1 iSCSI-диск

Внимание!

1. В ОС Linux возможность использования iSCSI-дисков не поддерживается.
2. Версии Windows на всех *Хостах*, использующих iSCSI-диски, должны совпадать.
3. Для корректного подключения iSCSI-диска на Windows 10 требуется обновить операционную систему до сборки 1709 или старше.
4. На iSCSI-дисках должен быть создан один раздел, отформатированный в NTFS.
5. Перед началом использования iSCSI-диска в ОС Windows убедитесь, что на всех *Хостах* кластера запущена **Служба инициатора Майкрософт iSCSI** и для нее выбран тип запуска Автоматически.
6. Одновременная запись на iSCSI-диск с нескольких источников может привести к повреждению данных. Для обеспечения дополнительной сохранности данных рекомендуется использовать хранилища с поддержкой контроля эксклюзивности подключения к iSCSI target.

Объект выполняет роль посредника между SecurOS и iSCSI-инициатором Windows, передавая ему все необходимые для подключения данные. Чтобы добавить iSCSI-диск в конфигурацию SecurOS, создайте объект *iSCSI-диск*, дочерний к объекту *Компьютер (Ноде)*.

Примечание. Для записи видеоархива *Ноды* можно использовать только те *iSCSI-диски*, которые являются дочерними для этой *Ноды*.

Родительский объект — **Компьютер**.

Порталы:

IP-адрес	Порт
172.16.11.115	3260
+	
-	

Получить список IQN

IQN:

☒ Использовать аутентификацию

Пользователь:

Пароль:

Получить список LUN Соединение установлено

LUN:

Получить список разделов Соединение установлено

Раздел:

Проверка подключения

OK Отмена Применить

Рис. 287. Окно настройки параметров объекта iSCSI-диск

Таблица 111. Параметры объекта iSCSI-диск

Параметр	Описание
Таблица порталов	Содержит таблицу IP-адресов и портов. Чтобы добавить/удалить портал, нажмите на кнопку добавить/удалить. В столбце IP-адрес укажите IP-адрес сервера, на котором находится диск. В столбце Порт укажите сетевой порт, по которому выполняется подключение. Значение по умолчанию: 3260.
Получить список IQN (кнопка)	Нажмите кнопку, чтобы получить список IQN, доступных на указанных порталах.
IQN	Список IQN, к которым может быть выполнено подключение. Выберите в нем нужное значение.
Использовать аутентификацию	Отметьте этот флаг, если на указанных порталах требуется аутентификация.
Пользователь и Пароль	Укажите данные для аутентификации на порталах.

Параметр	Описание
Получить список LUN (кнопка)	Нажмите, чтобы получить список LUN, доступных на указанном IQN.
LUN	Список LUN для выбранного IQN.
Получить список разделов (кнопка)	Нажмите, чтобы получить список разделов, доступных на указанном LUN.
Раздел	Список разделов для выбранного LUN.
Проверка подключения (кнопка)	Нажмите, чтобы убедиться, что соединение выполняется корректно.

16.1.4.2 Использование iSCSI-диска для хранения видеоархива

Внимание! Использование режима **Экономия места** для записи архива может негативно сказаться на сохранности данных на iSCSI-хранилище. Рекомендуется использовать режим **Оптимальная производительность** (см. [Выбор режима записи архива](#)).

Чтобы записывать видеоархив на *iSCSI-диск*, сначала выполните его настройку (см. [iSCSI-диск](#)). После этого диск можно будет выбрать в настройках объекта *Компьютер*. Для этого выполните следующие действия:

1. Откройте настройки объекта *Компьютер*.
2. Нажмите кнопку **Добавить директорию** в блоке **Архив**.
3. Выберите опцию **iSCSI-диск** и в выпадающем списке найдите нужный *iSCSI-диск*.
4. Нажмите кнопку **Добавить**.

Примечание. Аналогичным образом выполняется настройка объекта *Архиватор* для хранения долговременного архива на *iSCSI-диске* (см. [Архиватор](#)).

16.1.4.3 Перемещаемый PostgreSQL

С целью повышения отказоустойчивости баз данных, они могут быть размещены на *iSCSI-дисках*. Это позволит базам данных оставаться доступными по фиксированному IP-адресу в случае выхода *Хостов* из строя.

Родительский объект — [iSCSI-диск](#).

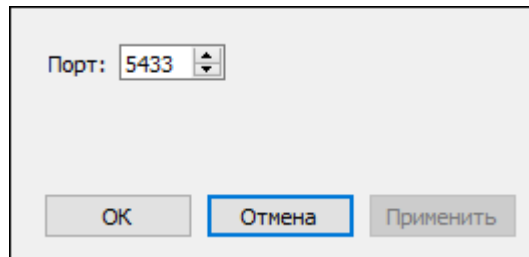


Рис. 288. Окно настройки параметров объекта Перемещаемый PostgreSQL

Таблица 112. Параметры объекта Перемещаемый PostgreSQL

Параметр	Описание
Порт	Укажите сетевой порт, по которому будет доступна переносимая СУБД. Значение по умолчанию: 5433.

Чтобы создать такую отказоустойчивую базу, выполните следующие действия:

1. Создайте объект *Перемещаемый PostgreSQL*, дочерний для объекта *iSCSI-диск*.
2. В настройках созданного объекта укажите порт, по которому должна быть доступна база данных.

На выбранном сервере СУБД PostgreSQL необходимо настроить прием соединений с внешних IP-адресов.

Чтобы настроить прием соединений, отредактируйте конфигурационные файлы `postgresql.conf` и `pg_hba.conf`. В `postgresql.conf` должна присутствовать настройка `listen_addresses = '*'`, а в `pg_hba.conf` добавлены разрешения для *Рабочих мест операторов* или *Видеосерверов*.

Например, в общем случае строка должна выглядеть так:

```
host all all 0.0.0.0/0 md5
```

Примечания:

1. Файлы `postgresql.conf` и `pg_hba.conf` располагаются в папке `%ProgramData %/ISS/iscsi_drives/[iscsi_drive_id]/pg_data`.
 2. Для проверки возможности подключения к удаленной БД, на *Рабочем месте оператора* можно воспользоваться кнопкой **Проверка подключения** в настройках объекта *База данных* или программой `pgAdmin`.
-

3. Выполните подключение к перемещаемой СУБД с помощью программы `PGAdmin`, указав для подключения виртуальный IP-адрес *Ноды*, которая является родительской для объекта *Перемещаемый PostgreSQL*.
4. Средствами `PGAdmin` создайте новую базу данных.
5. С помощью **Утилиты обновления БД** выполните разметку созданной базы данных.
6. Создайте объект *База данных*, дочерний для объекта *Объект охраны* (см. **База данных**).
7. Выполните настройку объекта *База данных*, указав в качестве IP-адреса виртуальный IP-адрес *Ноды*, которая является родительской для *iSCSI-диска*, а в качестве порта — значение, указанное в настройках объекта *Перемещаемый PostgreSQL*.

Теперь созданную *Базу данных* можно выбрать в настройках того объекта, для которого она предназначалась.

16.1.4.4 Хранение видеоархива на локальных дисках Хостов

Локальные жесткие диски *Хостов* кластера могут быть использованы для хранения видеоархива. Каждый *Хост* настраивается отдельно.

Внимание! Настоятельно рекомендуется настроить кластер таким образом, чтобы для каждой *Ноды* был задан приоритетный *Хост* (см. [Выбор приоритетного Хоста для Ноды](#)).

Чтобы настроить локальные диски *Хоста* в качестве хранилища видеоархива, используйте утилиту `clustercli.exe` (см. [Конфигурирование кластера](#)). В ней предусмотрены следующие команды для работы с дисками:

- [Добавление диска](#).
- [Удаление диска](#).
- [Получение списка дисков](#).

Добавление диска

Чтобы добавить диск *Хоста* в качестве хранилища видеоархива, выполните на соответствующем *Хосте* следующую команду:

```
Clustercli.exe drive add <drive_letter> <min_free_space> <read_write> [priority]
```

Где:

- `drive_letter` — буква диска. Допустимы следующие форматы: `C:`, `D:\`, `E:/`.
- `min_free_space` — минимально допустимый объем свободного места на диске в процентах. Когда объем свободного места сократится до указанного значения, начнется запись "по колыцу". Возможные значения: [1; 20].
- `read_write` — уровень доступа к диску. Возможные значения:
 - `rw` — чтение и запись;
 - `r` — только чтение. В этом случае существующий архив на этом диске доступен для просмотра, но новые файлы записываться не будут.
- `priority` — приоритет записи архива на локальный диск *Хоста* относительно настроек *Ноды*. Опциональный параметр. Возможные значения:
 - `high` — высокий приоритет. Архив будет записываться на локальный диск, а при исчерпании свободного пространства — на диски из настроек *Ноды*. Используется по умолчанию.
 - `low` — низкий приоритет. Архив будет записываться на диски из настроек *Ноды*, а при исчерпании свободного пространства — на локальный диск.

Примечание. Если диск с указанной буквой уже был добавлен ранее, его настройки будут перезаписаны.

Результатом выполнения команды будет сообщение об успешном или неуспешно добавлении диска.

Удаление диска

Чтобы удалить ранее добавленный диск *Хоста*, выполните на соответствующем *Хосте* следующую команду:

```
Clustercli.exe drive remove <drive_letter>
```

Где:

- `drive_letter` — буква диска. Допустимы следующие форматы: C:, D:\, E:/.

Результатом выполнения команды будет сообщение об успешном или неуспешном удалении диска.

Получение списка дисков

Чтобы получить список всех дисков, добавленных на этом *Хосте*, выполните на нем следующую команду:

```
Clustercli.exe drive list
```

Результатом выполнения команды будет список дисков с указанием их настроек.

16.1.5 Примеры создания и настройки кластера

В разделе приведены основные сценарии создания и настройки кластера:

- [Создание конфигурации SecurOS с кластером. Пример.](#)
- [Перенастройка конфигурации SecurOS на работу с кластером. Пример.](#)

16.1.5.1 Создание конфигурации SecurOS с кластером. Пример

В данном разделе подробно описаны шаги, необходимые для создания новой конфигурации SecurOS на основе кластера.

16.1.5.1.1 Задача

Создать новую конфигурацию SecurOS и кластер, состоящий из трех *Хостов* и одного *Рабочего места оператора* для выполнения наблюдения (см. [Структура кластера](#)). На двух *Хостах* будут выполняться *Ноды*, один *Хост* будет резервным.

16.1.5.1.2 Требования

Для создания такого кластера потребуется 3 компьютера, на которых установлен SecurOS с ролью *Видеосервер*, и 1 компьютер с ролью *Рабочее место оператора*.

Согласно рекомендациям (см. [Рекомендации](#)), компьютеры, которые будут выполнять роль *Хостов*, должны иметь два разных сетевых интерфейса для взаимодействия между *Хостами* (имя подключения, например, `NIC_CLUSTER`) и для подключения *Рабочих мест оператора* (имя подключения, например, `NIC_VIDEO`). Имена сетевых подключений могут отличаться от указанных.

Компьютеру, выполняющему роль *Рабочего места оператора*, достаточно одного сетевого интерфейса.

Примечание. Все описанные ниже команды выполняются в командной строке от имени администратора Windows.

16.1.5.1.3 Параметры компьютеров

В этом примере компьютеры имеют следующие параметры:

- **Компьютер 1**
 - Доменное имя: Host1.
 - Сетевой интерфейс NIC_CLUSTER: 192.168.0.101.
 - Сетевой интерфейс NIC_VIDEO: 172.16.1.101.
- **Компьютер 2**
 - Доменное имя: Host2.
 - Сетевой интерфейс NIC_CLUSTER: 192.168.0.102.
 - Сетевой интерфейс NIC_VIDEO: 172.16.1.102.
- **Компьютер 3**
 - Доменное имя: Host3.
 - Сетевой интерфейс NIC_CLUSTER: 192.168.0.103.
 - Сетевой интерфейс NIC_VIDEO: 172.16.1.103.
- **Компьютер 4**
 - Доменное имя: Operator.
 - Сетевой интерфейс NIC_VIDEO: 172.16.1.104.

16.1.5.1.4 Шаги

Создание кластера разделено на следующие этапы:

1. Создание кластера, *Объекта охраны* и *Нод*.
2. Добавление второго *Хоста*.
3. Добавление третьего *Хоста*.
4. Подключение *Рабочего места оператора* и дальнейшее конфигурирование SecurOS.

Для этого выполните следующие действия с помощью утилиты `clustercli.exe` (см. **Конфигурирование кластера**):

1. Перейдите к **Компьютеру 1** (первый *Хост*).

1.1. **Создайте Кластер**, выполнив команду

```
clustercli.exe create 192.168.0.101 172.16.1.101 172.16.20.1
```

После этого будет создан кластер. В его конфигурации будет присутствовать один *Хост*, который также станет *Сервером конфигураций* с виртуальным IP-адресом 172.16.20.1.

Виртуальные IP-адреса этого *Хоста* будут назначены сетевому интерфейсу NIC_VIDEO (172.16.1.101). *Рабочие места оператора* будут получать видео именно через него.

1.2. **Создайте Объект охраны**, выполнив команду

```
clustercli.exe node createzone 1
```

Созданный *Объект охраны* будет иметь идентификатор **1**.

1.3. Создайте Ноду, выполнив команду

```
clustercli.exe node create node1 172.16.20.101 1
```

Она начнет выполняться на уже созданном *Хосте*. *Нода* будет представлять собой объект *Компьютер* с ролью *Видеосервер* и идентификатором **node1**, дочерний *Объекту охраны* с идентификатором **1**. Теперь **Компьютер 1** является *Сервером конфигураций* с виртуальным IP-адресом 172.16.20.1, и на нём выполняется *Нода* с виртуальным IP-адресом 172.16.20.101.

1.4. Создайте вторую Ноду, выполнив команду

```
clustercli.exe node create node2 172.16.20.102 1
```

Вторая *Нода* пока не выполняется и ждет добавления новых *Хостов*.

2. Перейдите к **Компьютеру 2** (второй *Хост*).

2.1. Добавьте Компьютер 2 в кластер, выполнив команду

```
clustercli.exe join 192.168.0.102 172.16.1.102 192.168.0.101
```

Теперь связь между *Хостами* установлена и осуществляется по сетевому интерфейсу NIC_CLUSTER. Сразу после добавления этого *Хоста* в кластер, на нем начнет выполняться *Нода* с идентификатором **node2**.

Виртуальные IP-адреса этого *Хоста* будут назначены сетевому интерфейсу NIC_VIDEO (172.16.1.102).

3. Перейдите к **Компьютеру 3** (третий, резервный *Хост*).

3.1. Добавьте Компьютер 3 в кластер, выполнив команду

```
clustercli.exe join 192.168.0.103 172.16.1.103 192.168.0.101
```

Последний *Хост* присоединился к кластеру. Он будет выполнять роль резервного *Хоста*.

Виртуальные IP-адреса этого *Хоста* будут назначены сетевому интерфейсу NIC_VIDEO (172.16.1.103).

3.2. Проверьте состояние кластера, выполнив на любом из компьютеров в кластере команду

```
clustercli.exe state
```

Информация о состоянии кластера должна показать, что в нем находится три *Хоста* и выполняются две *Ноды*.

4. Перейдите к **Компьютеру 4** (*Рабочее место оператора*).

4.1. Запустите интерфейс оператора и в качестве IP-адреса для подключения укажите 172.16.20.101 — виртуальный IP-адрес одной из *Нод*.

4.2. Авторизуйтесь как суперпользователь (см. [Пользователи в SecurOS](#)).

16.1.5.2 Перенастройка конфигурации SecurOS на работу с кластером. Пример

В данном разделе подробно описаны шаги, необходимые для перевода независимых серверов SecurOS на работу в кластере.

16.1.5.2.1 Задача

Перевести существующую конфигурацию SecurOS на работу в кластере. Текущая конфигурация состоит из двух *Видеосерверов* и одного *Рабочего места оператора* для выполнения наблюдения. Планируется задействовать дополнительный компьютер, который будет выполнять роль резервного сервера.

16.1.5.2.2 Требования

Согласно рекомендациям (см. [Рекомендации](#)), *Видеосерверы* и будущий резервный сервер следует обеспечить двумя сетевыми интерфейсами. Один для взаимодействия между *Хостами* кластера (имя подключения, например, NIC_CLUSTER), другой для подключения *Рабочих мест оператора* (имя подключения, например, NIC_VIDEO). Имена сетевых подключений могут отличаться от указанных.

Компьютеру, выполняющему роль *Рабочего места оператора*, достаточно одного сетевого интерфейса.

Примечание. Все описанные ниже команды выполняются в командной строке от имени администратора Windows.

16.1.5.2.3 Параметры компьютеров

В конфигурации SecurOS уже существует *Объект охраны* с идентификатором 1.

Компьютеры из существующей конфигурации в примере имеют следующие параметры:

- **Видеосервер 1**

- Доменное имя: Server1.
- Роль: сервер конфигураций.
- Сетевой интерфейс NIC_CLUSTER: 192.168.0.101.
- Сетевой интерфейс NIC_VIDEO: 172.16.1.101.

- **Видеосервер 2**

- Доменное имя: Server2.
- Роль: периферийный сервер.
- Сетевой интерфейс NIC_CLUSTER: 192.168.0.102.
- Сетевой интерфейс NIC_VIDEO: 172.16.1.102.

- **Рабочее место оператора**

- Доменное имя: Operator.
- Сетевой интерфейс NIC_VIDEO: 172.16.1.104.

Компьютер, который будет выполнять роль **резервного сервера**:

- Доменное имя: Backup.
- Сетевой интерфейс NIC_CLUSTER: 192.168.0.103.
- Сетевой интерфейс NIC_VIDEO: 172.16.1.103.

16.1.5.2.4 Шаги

Переход на работу SecurOS в кластере разделен на следующие этапы:

1. Создание кластера на *Сервере конфигураций*.
2. Добавление второго *Видеосервера* в кластер.
3. Перевод старой конфигурации на работу с кластером.
4. Добавление резервного сервера в кластер.
5. Подключение *Рабочего места оператора* и подтверждение работоспособности.
6. Переход на использование централизованного хранилища.

Выполните следующие действия с помощью утилиты `clustercli.exe` (см. [Конфигурирование кластера](#)):

1. Перейдите к **Видеосерверу 1** (Сервер конфигураций).

1.1. Создайте Кластер, выполнив команду

```
clustercli.exe create 192.168.0.101 172.16.1.101 172.16.20.1
```

После этого будет создан кластер. В его конфигурации будет присутствовать один *Хост*, который продолжит быть *Сервером конфигураций*. В качестве IP-адреса *Сервера конфигураций* теперь будет использоваться виртуальный IP-адрес 172.16.20.1. Конфигурация SecurOS при этом сохраняется.

Периферийный сервер на этом этапе продолжит работу, потеряв связь со своим старым *Сервером конфигураций*. Фактически, он будет существовать со своей собственной конфигурацией SecurOS до момента, пока не будет добавлен в кластер.

Виртуальные IP-адреса этого *Хоста* будут назначены сетевому интерфейсу `NIC_VIDEO` (172.16.1.101). *Рабочие места оператора* будут получать видео именно через него.

2. Перейдите к **Видеосерверу 2** (бывший периферийный сервер).

2.1. Добавьте Видеосервер 2 в кластер, выполнив команду

```
clustercli.exe join 192.168.0.102 172.16.1.102 192.168.0.101
```

Теперь этот *Видеосервер* тоже стал *Хостом* кластера. Связь между *Хостами* установлена и осуществляется по сетевому интерфейсу `NIC_CLUSTER`. Конфигурация SecurOS синхронизировалась.

Виртуальные IP-адреса этого *Хоста* будут назначены сетевому интерфейсу `NIC_VIDEO` (172.16.1.102).

3. Преобразуйте объекты **Компьютер** в **Ноды кластера**, выполнив команды:

```
clustercli.exe node update Server1 172.16.20.101
```

```
clustercli.exe node update Server2 172.16.20.102
```

Если команды выполнены без ошибок, то теперь объекты *Компьютер* представляют собой *Ноды* кластера. Каждая из них может выполняться на любом из двух *Хостов*. *Ноды* будут иметь виртуальные IP-адреса 172.16.20.101 и 172.16.20.102 соответственно.

4. Перейдите к **Компьютеру 3** (резервный сервер).

4.1. Добавьте Компьютер 3 в кластер, выполнив команду

```
clustercli.exe join 192.168.0.103 172.16.1.103 192.168.0.101
```

Последний *Хост* присоединился к кластеру. Он будет выполнять роль резервного *Хоста*.

Виртуальные IP-адреса этого *Хоста* будут назначены сетевому интерфейсу `NIC_VIDEO` (172.16.1.103).

4.2. Проверьте состояние кластера, выполнив на любом из компьютеров в кластере команду

```
clustercli.exe state
```

Информация о состоянии кластера должна показать, что в нем находится три *Хоста* и выполняются две *Ноды*.

5. Перейдите к **Рабочему месту оператора**.

5.1 Запустите интерфейс оператора и в качестве IP-адреса для подключения укажите 172.16.20.101 — виртуальный IP-адрес одной из *Нод*.

5.2 Авторизуйтесь.

6. Настройте объекты *Компьютер*, соответствующие *Нодам* кластера, таким образом, чтобы запись архива велась на централизованное хранилище (см. **Организация хранилища в кластере**).

16.1.6 Решение типовых проблем

В разделе рассмотрены следующие проблемы:

- **Потеря кворума.**
- **Восстановление операционных систем Хостов из резервной копии.**
- **Отсутствие возможности подключиться с Рабочего места оператора.**

16.1.6.1 Потеря кворума

Потеря кворума (см. **Функционирование кластера. Кворум**) может произойти по следующим причинам:

- Половина или более *Хостов* в кластере вышли из строя;
- Допущена ошибка при добавлении *Хоста* в кластер.

Поскольку при отсутствии кворума конфигурация кластера не может быть изменена, добавление новых *Хостов* не является решением проблемы. Существует два способа восстановить кворум:

1. Восстановить работу вышедших из строя *Хостов*.
2. Пересобрать кластер, заново добавив в него только работоспособные *Хосты* (см. **Пересоздание кластера**).

Второй способ позволяет частично восстановить работоспособность системы, а также открывает возможность для добавления новых *Хостов*.

16.1.6.2 Восстановление операционных систем Хостов из резервной копии

Восстановление операционной системы *Хоста* из резервной копии может иметь негативные последствия для состояния кластера. В связи с этим, в зависимости от текущего состояния кластера, процедура может выполняться по-разному:

- **При наличии кворума** — в этом случае работа кластера нарушена не будет. Можно выполнять восстановление без опасений.
- **При отсутствии кворума** — в этом случае после появления кворума *Хосты*, которые были восстановлены из резервных копий, могут повредить конфигурацию кластера. Перед восстановлением рекомендуется выполнить процедуру пересоздания кластера (см. **Пересоздание кластера**). Порядок действий:

1. Выполнить команду для пересоздания кластера на одном из работоспособных *Хостов*.

2. Восстановить состояние операционных систем проблемных *Хостов*.
3. Добавить все *Хосты* в кластер.

16.1.6.3 Отсутствие возможности подключиться с Рабочего места оператора

Существует следующие ситуации, при которых *Рабочие места оператора* могут потерять возможность подключаться к *Видеосерверам*:

- **Ситуация 1:** Настройки системы безопасности не позволяют работающим серверам принять подключение от *Рабочих мест оператора*.

В этом случае решением проблемы будет выполнение подключения от имени суперпользователя (см. [Пользователи в SecurOS](#)) и последующее изменение настроек.

- **Ситуация 2:** В конфигурации нет работоспособных *Нод* или *Видеосерверов*, к которым может подключиться *Рабочее место оператора*.

Если лицензионный ключ позволяет, можно создать еще одну *Ноду* (см. [Добавление Ноды](#)) и выполнить подключение к ней. Если такой возможности нет, можно превратить неработоспособный *Видеосервер* в *Ноду* (см. [Преобразование обычного Видеосервера в Ноду кластера](#)). Если преобразование в *Ноду* не является подходящим вариантом, можно удалить этот *Видеосервер* и создать *Ноду* вместо него.

16.1.6.4 Обновление программного и аппаратного обеспечения в системе с кластером

Чтобы обновить программное/аппаратное обеспечение в конфигурации с кластером выполните следующие действия:

1. Начинать обновление следует с компьютеров, являющихся членами кластера. Переведите кластер в сервисный режим, вариант `fixed_cs` (см. [Сервисный режим](#)). Этот режим не позволит другому *Хосту* получить роль *Сервера конфигураций* в процессе обновления системы. В противном случае возможно повреждение конфигурации.
2. Выясните, какой из *Хостов* кластера является *Сервером конфигураций* (см. [Получение текущей конфигурации кластера](#)). При необходимости, перенесите роль *Сервера конфигураций* на более удобный для обновления *Хост* (см. [Выбор Сервера конфигураций](#)).
3. Выполните все необходимые процедуры обновления программного/аппаратного обеспечения на *Сервере конфигураций*.
4. Обновите резервные *Хосты*, на которых в данный момент отсутствуют *Ноды*.
5. Последовательно обновите *Хосты* с *Нодами*. Для обновления программного обеспечения *Хостов* выполните следующие шаги:
 - На обновляемом *Хосте* остановите службу Video Management System Server и отключите ее автозапуск.
 - Убедитесь, что *Нода* начала выполняться на резервном *Хосте*.
 - Обновите программное обеспечение.
 - Запустите службу Video Management System Server и включите ее автозапуск.
6. Отключите сервисный режим в кластере.
7. Обновите компьютеры, не входящие в кластер.

16.1.7 Ограничения

Использование кластера в конфигурации SecurOS накладывает следующие ограничения:

- Работа кластера возможна только на 64-битных версиях ОС.
- В конфигурации может существовать только один кластер.
- По умолчанию работа кластера возможна только если все IP-адреса, используемые кластером, находятся в одной подсети. Для работы внутри разных подсетей необходимо обеспечить доступность IP-адресов кластера из других подсетей, что может потребовать дополнительной настройки сетевого оборудования.
- Роль *Сервера конфигураций* может выполнять только член кластера.
- На одном *Хосте* может выполняться только одна *Нода*.
- Время на всех *Хостах* должно быть синхронизировано.
- Следующие модули SecurOS не будут работать на *Хостах* кластера:
 - GIS.
 - POS.
 - SNMP.
 - UTSS.
 - UVSS.
 - WebView.
- Использование модуля *Архиватор* на *Хостах* кластера в режимах **Постоянный** и **По расписанию** (см. раздел **Архиватор**) не поддерживается. Для постоянного доступа к создаваемому *Долговременному архиву* рекомендуется использовать *Сетевые папки* или *iSCSI-диск*.
- Особенности настройки *Сервера мобильного приложения* описаны в **Кратком руководстве SecurOS Mobile**.
- Особенности настройки для работы с *ActiveMedia Kit* описаны в **Руководстве SecurOS ActiveMedia Kit**.
- Объекты SecurOS, связанные с настройками компьютера или файлами, размещенными на нем, требуют дублирования этих настроек и файлов на всех *Хостах* кластера.
- По умолчанию некоторые данные (в частности, закладки и тревоги, данные **ретроспективного поиска** и служебные данные **EdgeStorage Sync**) хранятся в базе данных каждого *Хоста* и не перемещаются вместе с *Нодой*. Чтобы обеспечить доступность этих данных в кластере, используйте внешнюю базу данных (см. **Компьютер**, параметр **База данных для записи**).

16.2 Кластер резервных серверов

В некоторых случаях аппаратные требования к конфигурации не позволяют использовать классический кластер для осуществления резервирования. В этом случае может быть создан **Кластер резервных серверов**.

Этот подход строится на возможности кластера выступить в качестве резервной группы для серверов, не входящих в кластер. Число таких серверов может значительно превышать количество членов кластера. Таким образом, большую часть времени *Ноды* работают за пределами кластера. Наиболее частые сценарии использования кластера резервных серверов:

1. Распределенная конфигурация, в которой SecurOS работает на компьютерах, не имеющих стабильной связи с кластером (см. пример в разделе [Создание конфигурации на основе кластера резервных серверов](#)).
2. Конфигурация из двух компьютеров (1+1), в которой один из компьютеров выполняет роль резервного (см. пример в разделе [Перенастройка конфигурации SecurOS на работу с кластером «1+1». Пример](#)).

Внимание! Кластер резервных серверов не рассчитан на работу с централизованным хранилищем данных. Используйте локальные диски компьютеров для сохранения архива и баз данных.

16.2.1 Создание конфигурации на основе кластера резервных серверов

В данном разделе подробно описаны шаги, необходимые для создания конфигурации SecurOS на основе кластера резервных серверов.

16.2.1.1 Задача

Создать новую конфигурацию SecurOS на основе **Кластера резервных серверов**. В такой конфигурации небольшая группа серверов, объединенных в кластер, будет обеспечивать резервирование серверов, подключенных к кластеру в качестве вспомогательных.

16.2.1.2 Шаги

Для того чтобы организовать резервирование на основе кластера резервных серверов, выполните следующие действия:

1. Установите SecurOS на все компьютеры.
2. Запустите на любом сервере утилиту **Server Manager**.
3. Добавьте в список *Хостов* все серверы (см. [Работа со списком хостов](#)).
4. Определите, какие серверы будут резервными.
5. Создайте кластер на основе одного из резервных серверов (см. [Управление кластером, Создание кластера](#)).
6. Добавьте в созданный кластер остальные резервные серверы (см. [Управление кластером, Добавление хоста в кластер](#)).
7. Подключитесь к любому *Хосту* с помощью утилиты **Server Manager** (см. [Подключение к хосту для конфигурирования](#)).
8. С помощью интерфейса оператора создайте требуемое количество *Нод*. Для этого перейдите в настройки каждого созданного объекта *Компьютер* и активируйте опцию **Резервировать Видеосервер и добавить его в кластер**, а также задайте виртуальные IP-адреса *Нод* в поле **IP-**

адрес сервера. Количество *Нод* должно совпадать с количеством компьютеров, которые планируется подключить к кластеру резервных серверов в качестве вспомогательных *Хостов*.

9. Подключите к кластеру компьютеры, на которых большую часть времени будет работать SecurOS (см. [Управление кластером, Добавление хоста в кластер](#)). При добавлении этих *Хостов* в кластер выберите тип Вспомогательный хост.
10. Для каждой *Ноды* определите приоритетный *Хост* из списка вспомогательных *Хостов* (см. [Управление нодами, Установка / просмотр приоритетного хоста](#)).

После выполнения этих шагов система находится в рабочем состоянии, и кластер выполняет функцию резервирования.

16.2.2 Перенастройка конфигурации SecurOS на работу с кластером «1+1».

Пример

В данном разделе подробно описаны шаги, необходимые для организации резервирования с помощью одного резервного сервера.

16.2.2.1 Задача

Перевести существующую конфигурацию SecurOS на работу в кластере по схеме «1+1». Текущая конфигурация состоит из одного *Видеосервера*. Планируется задействовать дополнительный компьютер для обеспечения резервирования.

16.2.2.2 Параметры компьютеров

Кластер будет создаваться на основе следующего оборудования:

- *Server1* — компьютер, на котором изначально работает SecurOS.
- *Server2* — компьютер, который планируется добавить в кластер в качестве резервного *Хоста*.

16.2.2.3 Шаги

Для перенастройки конфигурации SecurOS на работу с кластером «1+1» выполните следующие действия:

1. Сохраните конфигурацию SecurOS компьютера *Server1* (см. [Система](#), блок **Сохранение и восстановление конфигурации**).
2. Установите SecurOS на компьютере *Server2*.
3. Запустите на компьютере *Server2* утилиту **Server Manager**.
4. Добавьте в список *Хостов* компьютеры *Server1* и *Server2* (см. [Работа со списком хостов](#)).
5. Создайте новый кластер на основе компьютера *Server2* (см. [Управление кластером, Создание кластера](#)).
6. Используя утилиту **Server Manager**, выполните на компьютере *Server2* восстановление конфигурации с помощью json-файла, полученного на первом шаге (см. [Восстановление конфигурации SecurOS](#)).
7. Подключите к кластеру компьютер *Server1* в качестве Вспомогательного хоста (см. [Управление кластером, Добавление хоста в кластер](#)).

8. Подключитесь к компьютеру Server2 (см. [Подключение к хосту для конфигурирования](#)).
9. В *Дереве объектов* SecurOS откройте настроечное окно компьютера Server1 (см. [Компьютер](#)). Активируйте опцию **Резервировать Видеосервер и добавить его в кластер**, а также задайте виртуальный IP-адрес *Ноды* в поле **IP-адрес сервера**. После сохранения настроек в списке утилиты **Server Manager** появится *Нода* с именем Server1 (помимо одноименного *Хоста*).
10. Выберите *Хост* Server1 в качестве приоритетного для *Ноды* Server1 (см. [Управление нодами, Установка / просмотр приоритетного хоста](#)).

17 Взаимодействие с внешней Службой реагирования

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

В ОС **Linux** функциональность не поддерживается.

С помощью системы безопасности SecurOS можно сообщить во внешнюю Службу реагирования о происшествии или чрезвычайной ситуации. Сообщение передается в виде *Карточки происшествия*, которая содержит детальную информацию о событии. Дальнейшая обработка предоставленной информации осуществляется оператором Службы реагирования.

Карточка происшествия может быть сформирована с помощью **Протокола событий** или **Медиа Клиента**.

Для формирования *Карточки происшествия* и отправки ее в Службу реагирования в SecurOS необходимо настроить следующие объекты:

- **Служба реагирования** — подготавливаются данные, которые могут быть использованы в *Карточке происшествия*:
 - http-адрес Службы реагирования.
 - список камер, для которых возможно формирование *Карточки происшествия*, и адреса их установки.
 - параметры для формирования ссылок на видео, соответствующее происшествию. Ссылка используется для получения видео Службой реагирования. По ссылкам может быть получено как живое видео, так и видео архив. Для передачи видео используется либо **RTSP-сервер**, либо Модуль WebView.
 - список типов происшествий. Создайте и загрузите в SecurOS список типов происшествий, необходимый для отправки *Карточки происшествия* (см. **Список типов происшествий. Формат файла**).

Примечание. *Карточка происшествия* может быть отправлена как из локальной системы, так и из Центра мониторинга (см. **Центр Мониторинга и Контроля**) при обработке событий *Удаленной системы*. В последнем случае в карточке передается физический адрес установки *Камеры*, заданный в настройках объекта *Служба реагирования Удаленной системы*. Все прочие параметры происшествия и ссылки для доступа к видео происшествия задаются в настройках объекта *Служба реагирования Центра Мониторинга*.

- **Протокол событий** — настраивается возможность формирования и отправки *Карточки происшествия* (параметр **Отправить Карточку в Службу реагирования**). Используя соответствующие записи протокола для объекта *Камера*, оператор может просмотреть живое или архивное видео события в *Медиа Клиенте* и/или создать и отправить *Карточку происшествия*.
- **Медиа Клиент** — настраивается возможность формирования и отправки *Карточки происшествия* (параметр **Отправить Карточку в Службу реагирования**).

После настройки системы взаимодействие с внешней Службой реагирования осуществляется следующим образом:

1. Работая с **Протоколом событий** или **Медиа Клиентом**, оператор контролирует возникновение происшествий или чрезвычайных ситуаций.
2. При появлении в *Протоколе событий* соответствующей записи, оператор просматривает видео и принимает решение о необходимости информирования внешней Службы реагирования. При работе с видео с помощью *Медиа Клиента* оператор контролирует ситуацию визуально.
3. Если решение принято, оператор формирует и отправляет *Карточку происшествия*. Карточку происшествия можно сформировать и отправить как из **Протокола событий**, так и из **Медиа Клиента** (см. **Краткое руководство пользователя SecurOS**).

Отправляемая *Карточка происшествия* содержит данные, одна часть которых отображается в интерфейсе карточки и видна оператору (см. Таблицу 113), а вторая нет (см. Таблицу 114). Данные в Службу реагирования передаются в формате JSON.

Таблица 113. Параметры отправляемого сообщения, отображаемые в Карточке происшествия

Параметр	Описание
Время происшествия	Время происшествия. При отправке <i>Карточки</i> из <i>Протокола событий</i> заполняется временем события. При отправке <i>Карточки</i> из <i>Медиа Клиента</i> заполняется временем кадра.
Место происшествия	Адрес места происшествия. В <i>Карточке происшествия</i> отображается в виде идентификатора и названия <i>Камеры</i> . При этом в сообщении содержится физический адрес камеры, заданный в настройках Службы реагирования .
Координаты происшествия	Координаты камеры, зафиксировавшей происшествие (см. Закладка Общие).
Тип происшествия	Выберите тип происшествия из предустановленного списка типов.
Угроза людям	Отметьте флажок, если происшествие несет потенциальную угрозу людям.
Дополнительная информация	Текстовый комментарий к происшествию. Заполняется системой автоматически (если поле Комментарий объекта <i>Протокол событий</i> содержит запись) или может быть задан вручную.

Таблица 114. Параметры отправляемого сообщения, не отображаемые в Карточке происшествия

Параметр	Описание
Сведения об источнике информации	Данные оператора (ФИО и телефон), создавшего и отправившего <i>Карточку происшествия</i>, где: • ФИО — Название объекта Пользователь из <i>Дерева объектов</i>. Примечание. Данные отправляются в виде структуры <Фамилия><Имя><Отчество>, которая формируется из строки Название следующим образом: в поле <Фамилия> подставляется первая часть Названия объекта. В поле <Имя> подставляется вторая часть строки Название, отделенная от первой пробелом. В поле <Отчество> подставляется третья часть Названия объекта, также отделенная от второй пробелом. Если Название объекта не содержит частей, разделенных пробелом, вся строка подставляется только в поле <Фамилия>. Остальные поля остаются пустыми. Например, Название объекта задано строкой вида Иванов Иван. В этом случае в поле <Фамилия> будет подставлено значение Иванов, в поле <Имя> — значение Иван. Поле <Отчество> при этом останется пустым. • Телефон — значение параметра Телефон из настроек объекта Пользователь.
Ссылки для просмотра видео	Ссылки для обращения к RTSP- или WebView-серверам для просмотра видео. Примечание. Для формирования ссылок используются параметры, заданные в настройках объекта Служба реагирования.

18 Модули специального назначения

В данном разделе описываются модули, измеряющие какие-либо собственные характеристики объекта, который отслеживается в кадре. Такие модули, как правило, работают в комплексе с интеллектуальными модулями SecurOS. В разделе представлено описание следующих модулей специального назначения:

- **Термометр.**

18.1 Термометр

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

В ОС **Linux** функциональность не поддерживается.

Внимание! Для работы модуля требуется специальное оборудование. Для получения списка совместимого оборудования обратитесь в Службу технической поддержки Intelligent Security Systems.

Объект предназначен для измерения температуры тела человека в кадре. Обнаружение и распознавание лиц в кадре выполняется с помощью интеллектуального модуля SecurOS FaceX (см. [Руководство пользователя SecurOS FaceX](#)). При превышении максимально допустимой температуры тела персоны в системе генерируется тревожное событие.

Родительский объект — **Компьютер**.

Внимание! На каждом *Видеосервере* можно создать только один объект *Термометр*.

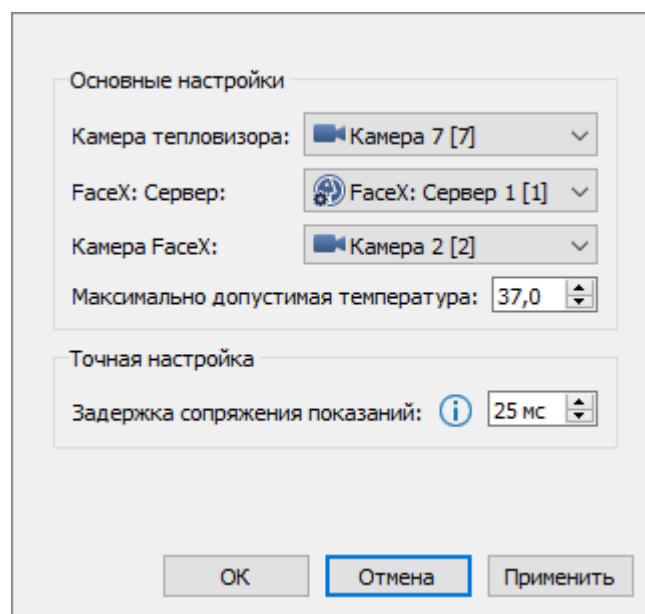


Рис. 289. Окно настройки параметров объекта Термометр

Таблица 115. Параметры объекта Термометр

Параметр	Описание
Основные настройки	
Камера тепловизора	Выберите камеру тепловизора. В списке отображаются только те <i>Камеры</i> , которые относятся к тому же Объекту охраны , что и настраиваемый объект <i>Термометр</i> .
FaceX: Сервер	Выберите <i>FaceX: Сервер</i>, с помощью которого будет осуществляться идентификация персоны. В списке отображаются только те объекты, которые относятся к тому же Объекту охраны, что и настраиваемый объект <i>Термометр</i>. Примечание. В настройках объекта <i>FaceX: Сервер</i> необходимо включить опцию Событие о положении лица на каждом кадре на вкладке Общие настройки.
Камера FaceX	Выберите <i>Камеру</i>, настроенную в модуле <i>FaceX</i> для обнаружения и идентификации лиц в кадре. Внимание! Для обеспечения согласованной работы комплекса выбранная Камера FaceX должна быть настроена на ту же сцену, что и Камера тепловизора. При сопоставлении лица, обнаруженного в кадре, со значением измеренной температуры данной персоны, генерируется событие MEASURE_RESULT (подробнее см. Руководство программиста SecurOS).
Максимально допустимая температура	Задайте максимально допустимую температуру тела персоны, при превышении которой будет генерироваться тревожное событие. В случае, если температура, переданная в событии MEASURE_RESULT, превышает заданное значение, генерируется событие TEMP_EXCEEDED (подробнее см. Руководство программиста SecurOS). Диапазон возможных значений: [0.0 – 200.0]. По умолчанию принимает значение 37.0.
Точная настройка	
Задержка сопряжения показаний	Задайте максимальное расхождение (в миллисекундах) между кадром, по которому была определена температура тела, и кадром, на котором лицо было идентифицировано с максимальной достоверностью. Чем меньше заданное значение, тем более точными будут результаты измерения. При низких значениях может значительно увеличиться время, в течение которого человек должен оставаться в поле зрения камеры. Диапазон возможных значений: [10 – 100]. По умолчанию принимает значение 25.

19 Легкая интеграция

В данном разделе приводится описание легких интеграций SecurOS с внешними системами ОПС-СКУД и системами мониторинга.

19.1 Общее описание

В SecurOS реализована возможность интеграции с внешними системами ОПС-СКУД и радиационного контроля. Модель взаимодействия предполагает, что внешний модуль передает в SecurOS некоторые события, которые могут быть обработаны.

Примечание. Список поддерживаемых SecurOS событий внешней системы определяется во внутреннем модуле интеграции внешней системы.

Результатом обработки внешнего события может быть изменение состояния объекта внешней системы на *Карте*, вывод формы SecurOS, требующей реакции оператора (например, вывод окна отправки SMS-сообщения для вызова тревожной группы) или отправка на внешнюю систему управляющих воздействий (только тем модулям, для которых такая возможность определена во внешней системе).

Интерфейс взаимодействия с внешней системой обеспечивает внутренний исполнитель SecurOS, соответствующий интеграции внешней системы.

Для описания и управления внешней системой в SecurOS используется корневой объект *Интеграция* <имя_интеграции>. Дерево объектов интеграции (дерево модулей внешней системы) строится автоматически на основе файла описания конфигурации внешней системы (см. раздел **Точка интеграции**).

После построения дерева внешней системы любой из его объектов может быть помещен на *Карту*. Дальнейшая работа с помещенным на *Карту* объектом внешней системы ничем не отличается от работы с помещенными на *Карту* типовыми объектами SecurOS.

Управляющие воздействия могут передаваться на внешний модуль одним из следующих способов:

- с помощью *Макрокоманды* (см. **Макрокоманда**);
- при выполнении *Скрипта Node.js* (см. **Скрипт Node.js**);
- в виде результата операции, выполненной с объектом, размещенным на *Карте* (см. **Карта**).

Протоколирование взаимодействия SecurOS с внешней системой и работа с деревом объектов интеграции осуществляется отдельно — события внешней системы заносятся в протокол SecurOS, операции работы с деревом объектов внешней системы сохраняются в независимом log-файле.

19.2 Точка интеграции

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

В ОС **Linux** функциональность не поддерживается.

Объект предназначен для интеграции внешних пользовательских приложений в SecurOS. Представляет собой API, реализующий описание внешней системы в SecurOS и взаимодействие с ней с помощью сообщений, использующих *События* и *Команды* SecurOS.

С помощью интерфейса можно:

1. Устанавливать соединение между внешней системой и SecurOS и контролировать его состояние;
2. Представлять конфигурацию внешней системы в *Дереве объектов* SecurOS в виде иерархической структуры;
3. Представлять и управлять объектами внешней системы с помощью пользовательских интерфейсов SecurOS (**Карты: Интерфейс оператора, Макрокоманд**);
4. Отображать события внешней системы в **Протоколе событий** и статусы ее объектов на **Карте**.

Родительский объект — *Компьютер\группа Интеграция и Автоматизация*.

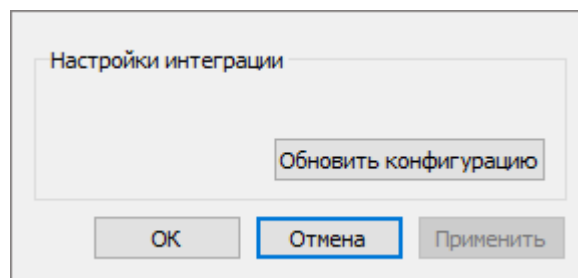


Рис. 290. Окно объекта Точка интеграции

Таблица 116. Параметры объекта Точка интеграции

Параметр	Описание
Обновить конфигурацию (кнопка)	Нажмите кнопку, чтобы построить в <i>Дереве объектов</i> SecurOS конфигурацию внешней системы в виде иерархической структуры объектов.

Детальная информация о порядке настройки системы и использовании *Точки интеграции* приведена в документе **Руководство пользователя UinP**.

Примечание. **Руководство пользователя UinP** не входит в общий комплект документации и предоставляется по запросу.

20 Горячие клавиши

В данном разделе описаны комбинации клавиш, используемые для выполнения действий с различными объектами SecurOS.

20.1 Панель инструментов администратора

Таблица 117. Комбинации клавиш для работы с объектами SecurOS

Клавиши	Описание
Esc	Заккрытие окна настройки параметров объекта или окна <i>Дерева объектов</i> SecurOS
F1	В режиме администрирования: • окно настройки параметров объекта открыто — вызов статьи, посвященной данному объекту; • окно настройки параметров объекта закрыто — вызов статьи, посвященной <i>Центру администрирования</i>.
F2	Переименование выбранного объекта
*	Раскрытие всех дочерних веток дерева к выбранному объекту (плюс дополнительный уровень при каждом нажатии на клавишу)
- (цифровой блок)	Заккрытие дочерней ветки дерева к выбранному объекту
+ (цифровой блок)	Раскрытие дочерней ветки дерева к выбранному объекту (один уровень)
Enter	Открытие окна настройки параметров выбранного объекта
Delete	Удаление выбранного объекта
Пробел	Отключение/включение выбранного объекта или всех дочерних объектов <i>Группы</i>
Ctrl+B	Добавление объекта в <i>Избранное</i> . Удаление объекта из <i>Избранного</i>
Ctrl+F	Открытие/заккрытие <i>Панели поиска объектов</i>
Ctrl+N	Отображение меню создания объектов или всех дочерних объектов <i>Группы</i>

21 Приложения

Раздел содержит описание системных утилит и другую информацию, необходимую для настройки и эксплуатации системы.

21.1 Приложение 1. Обновление/удаление программного обеспечения

В данном разделе приводится описание особенностей обновления/удаления программного обеспечения SecurOS.

21.1.1 Обновление программного обеспечения

Для обновления программного обеспечения выполните следующие действия:

1. Для начала процедуры обновления запустите установочный файл продукта.
2. Дальнейшие шаги процедуры аналогичны шагам первоначальной установки (см. раздел [Установка и обновление SecurOS на Windows](#)).

21.1.2 Удаление программного обеспечения

- [Удаление SecurOS в ОС Windows](#).
- [Удаление SecurOS в ОС Linux](#).

Удаление SecurOS в ОС Windows

Удаление SecurOS выполняется в два этапа:

- удаление программного обеспечения;
- удаление видео-, аудиоархивов и базы данных конфигурации.

Чтобы удалить программное обеспечение SecurOS выполните одно из следующих действий:

- Запустите Мастер установки той версии продукта, которую необходимо удалить. Система выведет окно **Обслуживание программ** (см. рис. [291](#)).

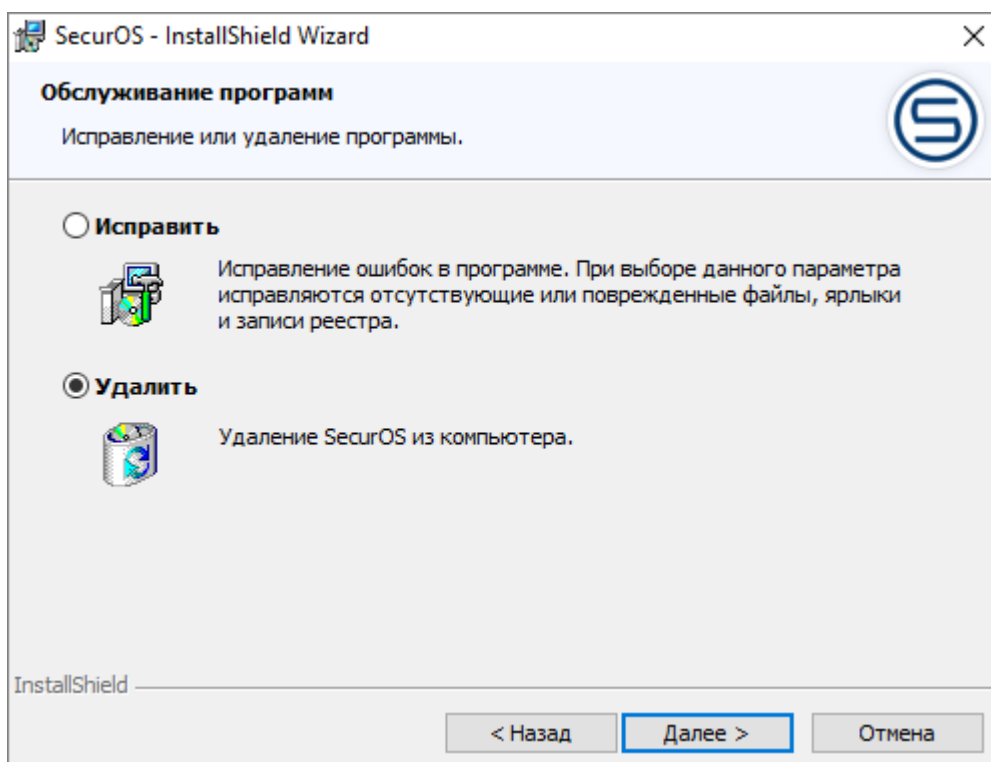


Рис. 291. Окно Обслуживание программ

Для запуска процедуры удаления выберите опцию **Удалить**, нажмите кнопку **Далее**.

- В меню **Пуск** Windows последовательно выберите пункты меню **Все программы** → **SecurOS** → **Uninstall SecurOS**.

Программное обеспечение SecurOS будет удалено в автоматическом режиме.

После удаления программного обеспечения, возможно, понадобится удалить все видео- и аудиоархивы, а также базу данных конфигурации (InstallShield Wizard эти файлы не удаляет).

Таким образом, необходимо это сделать вручную: для удаления оперативного и долговременного архивов удалите каталоги `\ISS_MEDIA` и `\ARCHIVE\ISS_MEDIA` (обычно находятся на одном или нескольких жестких дисках в корневом каталоге, например `C:\ISS_MEDIA`, `D:\ARCHIVE\ISS_MEDIA`).

Для удаления базы данных конфигурации (PostgreSQL) запустите файл `uninstall-postgresql.exe` из каталога `C:\Program Files\PostgreSQL\X.Y`, или используйте оснастку **Установка и удаление программ**.

Удаление SecurOS в ОС Linux

Для удаления SecurOS в ОС Linux выполните одну из двух команд:

- `sudo apt-get remove securos` — стандартное удаление;
- `sudo dpkg -P securos` — полное удаление (с очисткой БД).

После удаления программного обеспечения, при необходимости, удалите архивы и/или базу данных вручную.

21.1.3 Особенности обновления версий SecurOS

В разделе описаны особенности обновления SecurOS с более ранних версий.

21.1.3.1 Обновление версии 9.3 и более ранних

В SecurOS 9.4 внесены некоторые изменения, на которые стоит обратить внимание при обновлении:

- **Запуск серверной части SecurOS как службы ОС.**
- **Администрирование SecurOS с Рабочего места оператора.**
- **Запись архива.**

Запуск серверной части SecurOS как службы ОС

Начиная с релиза 9.4 *Серверная часть* запускается только как служба ОС. *Клиентская часть* реализует интерфейс оператора и запускается как отдельное приложение.

Если ранее вы запускали *Серверную часть* как приложение, обратите особое внимание на следующие моменты:

1. По умолчанию *Серверная часть* запускается от имени системного пользователя Local System. Это может привести к тому, что сетевые папки, смонтированные как сетевые диски и выбранные ранее для записи архива в настройках объекта **Компьютер**, станут недоступны. Для записи архива на сетевой ресурс, в настройках объекта **Компьютер** используйте сетевые пути вместо смонтированных дисков.
2. Информирование об аварийном завершении работы *Серверной части* с помощью окон ОС прекращено. Информацию о таких ошибках ищите в лог-файле журнала ОС (**Просмотр событий** → **Журналы приложений и Служб** → **SecurOS**). Информация о проблемах запуска *Серверной части* выводится в файл `securos_svc.log`, расположенный в папке `%ProgramData%\ISS\logs`.

Администрирование SecurOS с Рабочего места оператора

Прекращена поддержка *Компьютеров* с ролью *Рабочее место администратора*, функции администрирования SecurOS перенесены на *Рабочее место оператора*.

При обновлении обратите особое внимание на следующие моменты:

1. Все *Рабочие места администратора* преобразуются в *Рабочие места оператора*.

Примечание. Список **Сервера для подключения** каждого преобразованного *Рабочего места оператора* будет пуст. Это означает, что *Рабочее место оператора* может подключиться к любому *Видеосерверу* сети. Подробнее о подключении см. раздел **Закладка Серверы для подключения**.

2. На всех *Видеосерверах* и *Рабочих местах операторов* необходимо установить компоненты всех интеллектуальных Модулей SecurOS, которые используются в системе (подробнее см. *Руководство пользователя* соответствующего Модуля).
3. Версии SecurOS и интеллектуальных Модулей SecurOS должны совпадать на всех *Компьютерах* сети (см. **Порядок обновления SecurOS**).

Запись архива

Реализована запись архива в файлы фиксированного размера, что позволяет снизить их фрагментирование и, как следствие, повысить скорость записи на диск. Эффективность механизма зависит от объема свободного места на диске.

Примечание. Intelligent Security Systems рекомендует значение 10%. Это же значение рекомендует Microsoft Corporation для разделов NTFS. Изменить объем свободного места можно в настройках объекта **Компьютер**.

При работе с SecurOS 9.4 обратите особое внимание на следующие моменты:

1. При обновлении до версии 9.4 объем свободного места будет автоматически пересчитан для каждого диска. Данное значение будет предложено по умолчанию. Изменить это значение можно с помощью параметра **Запись архива** (см. раздел **Архив**).
2. При обновлении автоматически выставляется режим **Экономия места** (см. **Архив**).

21.1.3.2 Обновление версии 9.6 и более ранних

В SecurOS 10.0 внесены некоторые изменения, на которые стоит обратить внимание при обновлении:

- **Подключение Рабочих мест оператора к Видеосерверам без дополнительных настроек. Ограничение доступа.**
- **Профили Рабочих мест оператора.**
- **Задействование дополнительных сетевых портов.**

Подключение Рабочих мест оператора к Видеосерверам без дополнительных настроек. Ограничение доступа

Начиная с релиза 10.0 *Клиентская часть* может быть запущена на любом компьютере, даже если он не добавлен в *Дерево объектов SecurOS*.

Настройки ограничения доступа *Рабочих мест оператора* к *Видеосерверам* теперь выполняются в *Объекте охраны*. Закладка **Серверы для подключений** позволяет ограничить подключения к конкретным серверам (см. **Закладка Серверы для подключений**), чтобы обеспечить автобалансировку нагрузки и автоматическое переподключение. Закладка **Ограничение подключений** позволяет создать белый список компьютеров, которым разрешено подключение к *Видеосерверам* системы (см. **Закладка Ограничение подключений**).

Профили Рабочих мест оператора

Появилась возможность создавать унифицированные интерфейсы оператора – *Профили Рабочих мест оператора*, которые могут быть использованы сразу на большом количестве компьютеров. Подробности и ограничения работы с профилями описаны в разделе **Профили Рабочих мест оператора**.

Задействование дополнительных сетевых портов

Для работы SecurOS необходимо открыть сетевой порт 21112, через который происходит взаимодействие *Клиентской* и *Серверной* частей.

21.1.3.3 Обновление версии 10.0 и более ранних

Начиная с релиза 10.0, конфигурация SecurOS может включать кластер (см. [Отказоустойчивый кластер](#)). Последовательность шагов для обновления системы с такой конфигурацией описана в разделе [Обновление программного и аппаратного обеспечения в системе с кластером](#).

21.1.3.4 Обновление версии 10.1 и более ранних

В релизе 10.2 кластер получил расширенные возможности хранения видеоархива на локальных дисках *Хостов*. При этом изменилась процедура настройки дисков. Если Вы использовали локальные диски для хранения видеоархива в кластере, их необходимо перенастроить (см. [Хранение видеоархива на локальных дисках Хостов](#)).

21.1.3.5 Обновление версии 10.2 и более ранних

В релизе 10.3 возможность управления дворником и освещением камеры теперь контролируется *Правами пользователя*. Оператору требуется уровень доступа **Управление** или выше к объекту *Камера*, у которой есть опция управления дворником или освещением.

Переработана функциональность управления обменом событиями. При обновлении SecurOS до версии 10.3 правила обмена событиями между компьютерами системы, настроенные для версии 10.2 или более ранней, необходимо определить заново (см. [Закладка Серверы для подключения](#)).

21.1.3.6 Обновление версии 10.3 и более ранних

В релизе 10.4 появились некоторые отличия в работе объектов *Основной*, *Аудио* - и *Видеоподсистемы*, описанные в следующих подразделах:

- [Особенности работы Основной подсистемы](#).
- [Особенности работы Видеоподсистемы](#).
- [Особенности работы Аудиоподсистемы](#).

Особенности работы Основной подсистемы

При эксплуатации SecurOS некоторые служебные файлы на *Периферийных серверах* и *Рабочих местах оператора* могут быть отредактированы локально и отличаться от таких же файлов на *Сервере конфигураций*. После обновления версии программного обеспечения на версию 10.4 все такие файлы на всех *Периферийных серверах* и *Рабочих местах операторов* в сети SecurOS будут автоматически заменены файлами с *Сервера конфигураций*. Список файлов, которые будут обновлены, приведен в разделе [Синхронизация файлов SecurOS](#).

Особенности работы Видеоподсистемы

Прекращена поддержка автоматической перестановки даты и времени начала и конца фрагмента при проигрывании архива в обратном направлении. В версии 10.4 выбор порядка установки дат при обратном воспроизведении вынесен в настройки системы (подробнее см. раздел [RTSP-сервер](#)).

Особенности работы Аудиоподсистемы

В версии 10.4 поддержан новый формат файлов звукового сопровождения видеоархива. В связи с этим после обновления на версию 10.4 необходимо учесть следующие особенности работы SecurOS:

- Видеоархив, записанный со звуковым сопровождением в SecurOS версии 10.3 и ниже, в версии 10.4 по умолчанию будет проигрываться без звукового сопровождения. Для восстановления возможности проигрывания видеоархива совместно с записанным звуковым сопровождением, необходимо сконвертировать сопровождающий аудиофайл в новый формат (см. раздел [Утилита обновления аудиофайлов устаревшего формата](#)).

Примечание. Для проигрывания в SecurOS MCC архива со звуковым сопровождением, записанного в *Удаленных системах*, конвертация такого архива в *Удаленных системах* не требуется.

- При проигрывании фрагмента видеоархива, записанного со звуковым сопровождением, возможна ситуация, в которой кадры проигрываются без него. При удалении файлов "по кольцу" в случае истечения срока их хранения, нижняя временная граница самых ранних из оставшихся файлов может отличаться. Указанная особенность характерна только для первого часа всего временного периода архива.
- Новый формат аудиофайла не поддерживается утилитой [Media Export Utility](#).
- Устройство аудиозахвата с типом **SoundMixer** удалено. При обновлении на версию 10.4 поле **Тип** в настройках всех существующих устройств такого типа будет обнулено.

21.1.3.7 Обновление версии 10.6 и более ранних

Начиная с релиза 10.7 в SecurOS MCC Direct Connect реализовано ограничение доступа к *Удаленной системе*. Доступ предоставляется только в том случае, если пароль, который передается Центром Мониторинга при подключении к *Удаленной системе*, соответствует ее настройкам.

По этой причине сразу после обновления программного обеспечения SecurOS в *Удаленной системе* на версию 10.7 доступ к ней из SecurOS MCC будет временно невозможен. Для восстановления доступа после обновления выполните следующие действия:

1. В конфигурации *Удаленной системы* в настройках объекта [Система](#) отметьте флажок **Разрешить доступ** и задайте пароль доступа.
2. В конфигурации SecurOS MCC в настройках объектов [Удаленная система](#) задайте соответствующие пароли доступа к *Удаленным системам*.

21.1.3.8 Обновление версии 10.7 и более ранних

Начиная с релиза 10.8, в SecurOS реализован новый, более надежный стандарт авторизации пользователей для работы с модулями SecurOS. В связи с этим, после обновления на версию 10.8, необходимо обновить настройки некоторых модулей (в частности, пароли всех пользователей SecurOS, которые были созданы в ранних версиях). Это обеспечит надежную работу пользователей со всеми имеющимися в конфигурации модулями SecurOS. При обновлении паролей можно использовать старые (текущие) значения, однако их необходимо просто ввести и сохранить заново.

Примечание. Пароли пользователей можно не обновлять, но в этом случае работа с некоторыми модулями (например, *RTSP-сервер*) не гарантируется.

Объекты, настройки которых требуют обновления, называются "проблемными". Для индикации и поиска таких объектов доработан модуль *Health Monitor* (см. раздел [Система](#)) и *Центр администрирования SecurOS* (см. раздел [Объекты, требующие настройки](#)).

Непосредственное описание проблемы настроек объекта и рекомендации администратору приводятся в окне настройки параметров проблемного объекта (см. раздел **Объекты, требующие настройки**).

21.1.3.9 Обновление версии 10.9 и более ранних

В релизе 10.10 в SecurOS имя службы запуска *Серверной части* изменено на Video Management System Server, имя исполняемого файла изменено с `securos_svc.exe` на `vms_server.exe`. По умолчанию запуск службы осуществляется от имени системного пользователя Local System. Если для службы ранней версии SecurOS был указан другой пользователь, в свойствах службы необходимо обновить данные для входа в систему (учетная запись, пароль).

21.1.3.10 Обновление версии 10.10 и более ранних

В релизе SecurOS 11.0 удалены следующие объекты:

- HTML-форма.
- HTML-диалог.

В редакциях SecurOS Xpress (упразднена) и SecurOS Lite релиза 11.0 объекты *База данных* и *HTML5 FrontEnd* более не поддерживаются. Перед обновлением указанных редакции на версию 11.0 данные объекты необходимо удалить из *Дерева объектов* SecurOS.

21.1.3.11 Обновление версии 11.2 и более ранних

Начиная с релиза 11.3 для работы некоторых компонентов SecurOS используется универсальный сетевой порт 21111 (см. **Приложение 5. Используемые в SecurOS сетевые порты**). Использование универсального порта позволяет упростить настройку брандмауэра.

Внимание! Для корректной работы необходимо, чтобы версия SecurOS Видеосервера была не ниже, чем у подключенных к нему Рабочих мест оператора.

21.1.3.12 Обновление версии 11.3 и более ранних

Начиная с релиза 11.4 инсталлятор SecurOS на ОС Windows стал единым для всех редакций. Теперь редакция определяется на основе **лицензионного ключа SecurOS**.

21.1.3.13 Обновление версии 11.4 и более ранних

Начиная с релиза 11.5 в ОС Linux демон `securosd` ядра SecurOS переименован в `vms_server`.

Начиная с версии 11.5 скрипты *Node.js* размещены в папке <корневой каталог SecurOS>\bin64\node.js\node_modules.

21.1.3.14 Обновление версии 11.5 и более ранних

Начиная с релиза 11.6 для работы с *Камерами*, поддерживающими технологию **Edge Storage**, создавать объекты *EdgeStorage Gate* и *EdgeStorage Sync* не требуется. Для использования **Edge Storage** достаточно в настройках объекта *Камера* отметить флажок **Просмотр архива, хранящегося на удаленном устройстве (EdgeStorage Gate)** или **Восстанавливать архив из локального хранилища Камеры (EdgeStorage Sync)** (см. [Закладка Запись](#)).

21.1.3.15 Обновление версии 11.6 и более ранних

Начиная с релиза 11.7 пакет *Integrated Devices Pack* и все необходимые файлы интеграторов, содержащиеся в нем, входят в состав SecurOS.

В релизе 11.7 появилась возможность выбрать кодек для передачи видео клиенту с *RTSP-сервера* в параметрах объекта. Значение по умолчанию — H.264. При необходимости вы можете изменить значение на другое (см. [RTSP-сервер](#)).

21.1.3.16 Обновление версии 11.7 и более ранних

Начиная с релиза 11.8 изменились требования к настройке перспективы для встроенных детекторов плагина *Tracking Kit III*. При обновлении на релиз 11.8 может потребоваться корректировка настроек перспективы для ряда детекторов (см. [Закладка Сцена](#)).

21.1.3.17 Обновление версии 11.8 и более ранних

Начиная с релиза 11.8 для горячей замены диска, используемого для хранения архива, необходимо выполнить определенную последовательность действий (подробнее см. [Горячая замена диска](#)).

21.2 Приложение 2. Обновление версии PostgreSQL

Начиная с релиза 10.7 SecurOS поддерживает работу с версиями PostgreSQL 12.0, 12.1 и 12.3 (далее PostgreSQL 12).

Возможны следующие варианты установки PostgreSQL инсталлятором:

- При первоначальной установке SecurOS — устанавливается PostgreSQL 12.3. В этом случае SecurOS полностью готов к работе сразу после установки. Никаких дополнительных действий предпринимать не следует.
- При обновлении SecurOS — PostgreSQL не устанавливается, SecurOS продолжает работу с текущей версией PostgreSQL. Для обновления скачайте одну из поддерживаемых версий PostgreSQL, далее мигрируйте данные из старой базы в новую одним из указанных ниже способов.
- Если на сервере установлен PostgreSQL 9.X или PostgreSQL 12, но SecurOS устанавливается впервые — PostgreSQL не устанавливается. Для работы с PostgreSQL 12 убедитесь, что установленная версия PostgreSQL 12 поддерживает работу с SecurOS. В противном случае скачайте и установите одну из поддерживаемых версий. Далее мигрируйте данные из старой базы PostgreSQL 9.X в новую одним из указанных ниже способов, или перенастройте SecurOS на работу с уже установленной поддерживаемой версией PostgreSQL 12.

Если при переходе на новую версию необходимо сохранить данные текущей используемой версии PostgreSQL (например, 9.1), их необходимо мигрировать. Миграция может быть выполнена одним из двух методов:

- **С помощью физического копирования данных** — данный метод не представляется сложным в реализации, но требует значительного времени для физического копирования базы данных и остановки серверов SecurOS на все время копирования. На все время копирования данных сервер SecurOS будет неработоспособен.
- **С помощью логической репликации данных** — данный метод является предпочтительным за счет кратковременной (несколько минут) последовательной остановки серверов SecurOS на время выполнения некоторых непродолжительных операций. По сравнению с первым методом требует более тщательной настройки.

Внимание!

1. Сохраните текущую конфигурацию SecurOS (см. **Система**) на случай непредвиденных ошибок во время процедуры миграции данных.
2. Перед использованием любого метода убедитесь, что пользователь, выполняющий миграцию данных, имеет права чтения/записи на директории, где установлены все версии PostgreSQL, вовлеченные в процедуру миграции.
3. Конфигурационные файлы PostgreSQL предыдущей версии при миграции не копируются.

С помощью физического копирования данных

При использовании данного метода миграция осуществляется с помощью скрипта `pgupgrade.bat`, который является оболочкой для штатных инструментов миграции PostgreSQL.

Примечание.	По	умолчанию	скрипт	копируется	в	папку
	<директория_установки_SecurOS\pgupgrade> при установке SecurOS.					

Чтобы мигрировать данные с помощью штатных средств PostgreSQL 12.X:

1. Скачайте и установите последнюю стабильную версию PostgreSQL 12.X, если это необходимо.
2. Убедитесь, что у пользователя есть права чтения/записи на папку <директория_установки_SecurOS\pgupgrade>, где расположен файл `pgupgrade.bat` и куда будут сохраняться лог-файлы процедуры миграции. При необходимости создайте отдельную папку в файловой системе сервера, на котором предполагается миграция. При создании папки наделите пользователя правами чтения/записи. Скопируйте файл `pgupgrade.bat` в созданную папку. Лог-файлы процедуры миграции будут сохраняться в эту же папку.
3. Откройте `pgupgrade.bat` для редактирования.

Внимание! Если пути к папкам со старой и новой версиями PostgreSQL не отличаются от значений по умолчанию (C:\Program Files (x86)\PostgreSQL\9.1 и C:\Program Files\PostgreSQL\12), редактировать файл `pgupgrade.bat` не надо.

4. Замените следующие строки, указав в них пути к папкам старой и новой версий PostgreSQL:

```
@rem set "PGOLD_BIN=c:\Program Files (x86)\PostgreSQL\9.1\bin"
@rem set "PGOLD_DATA=c:\Program Files (x86)\PostgreSQL\9.1\data"
@rem set "PGNEW_BIN=c:\Program Files\PostgreSQL\12\bin"
@rem set "PGNEW_DATA=c:\Program Files\PostgreSQL\12\data", где:
```

- **PG_OLD** — переменные с путями к соответствующим папкам **старой** версии PostgreSQL;
- **PG_NEW** — переменные с путями к соответствующим папкам **новой** версии PostgreSQL.

Внимание! В процессе обновления все данные из директории, указанной в переменной PGNEW_DATA будут удалены. Права пользователя PostgreSQL будут перенесены из директории PGOLD_DATA на директорию PGNEW_DATA.

5. Остановите сервер SecurOS.
6. Остановите все работающие Службы PostgreSQL.
7. Запустите консоль cmd с правами администратора.
8. В командной строке запустите файл pgupgrade.bat с одним из параметров:
 - copy — миграция старой БД копированием (медленная). Возможна миграция на другой диск. В случае ошибок, старая БД остается работоспособной;
 - link — миграция старой БД жесткими ссылками (быстрая). Миграция возможна только на этот же логический диск. В случае ошибки обе БД, старая и новая, будут неработоспособны.

Внимание! Перед запуском pgupgrade.bat с этим параметром рекомендуется создать точку восстановления Windows.

Например:

```
> cd c:\upgrade  
> pgupgrade.bat link
```

9. При отсутствии сообщений об ошибках в консоли cmd миграция считается успешно завершенной.
10. Запустите сервер SecurOS и Службу PostgreSQL 12.3.

Миграция с помощью логической репликации

При использовании данного метода осуществляется репликация БД без остановки сервера SecurOS. Репликация осуществляется с помощью утилиты pgtool.exe, которая является оболочкой для штатных инструментов миграции PostgreSQL.

Примечание. По умолчанию утилита копируется в папку <директория_установки_SecurOS> при установке SecurOS.

Чтобы мигрировать данные с помощью логической репликации:

1. Скачайте и установите последнюю стабильную версию PostgreSQL 12.X, если она не была установлена.

Внимание! Для корректной репликации данных на обновляемом сервере должен быть установлен пакет Microsoft Visual Studio C++ 2010 Redistributable.

2. Создайте системную переменную окружения SLONY_SHARE_DIR. В качестве значения укажите путь к папке share в папке PostgreSQL 12 (например, D:\PostgreSQL12\share).
3. Для корректного запуска и работы утилиты миграции pgtool.exe у пользователя должны быть права чтения/записи на папку установки утилиты (<директория_установки_SecurOS>).
4. Запустите консоль cmd с правами администратора. Для корректного запуска и работы утилиты pgtool.exe в консоли cmd укажите полный путь к папке установки утилиты.
5. Создайте набор скриптов для подготовки новой базы данных версии 12.X. В параметрах скриптов необходимо указать:

- полные пути к папкам со старой и новой версиями PostgreSQL (по умолчанию C:\Program Files (x86)\PostgreSQL\9.1 и C:\Program Files\PostgreSQL\12). Для указанных папок также необходимо задать полные права на чтение/запись.
- хосты и номера портов для подключения (по умолчанию 5432).
- имя и пароль пользователя (по умолчанию postgres/postgres).

Примечание. Если текущие значения всех указанных выше параметров не отличаются от значений по умолчанию, используемых SecurOS, их задавать необязательно.

Например:

```
> set "pgold=c:\Program Files (x86)\PostgreSQL\9.1"
> set "pgnew=c:\Program Files\PostgreSQL\12"
> pgtool --port 5432 --path "%pgold%" --slony clean -o replica_clean.sql
> pgtool --user replica
> pgtool -k create --port 5432 -o pks_create.sql
> pgtool -k drop --port 5432 -o pks_drop.sql
```

Примечание. Если база данных реплицируется впервые, команду `> pgtool --port 5432 --path "%pgold%" --slony clean -o replica_clean.sql` выполнять необязательно.

При этом:

- Номер порта может быть указан в формате `--port <value>` или `-p <value>`.
 - Пароль пользователя может быть указан в формате `--user <value>` или `-U <value>`.
6. Убедитесь, что во всех таблицах реплицируемой базы данных содержится первичный ключ. Далее скопируйте схему базы данных. Для данных операций используются штатные утилиты PostgreSQL `psql` и `pg_dump_all`.

```
> "%pgold%\bin\psql" -p 5432 -U postgres -f pks_create.sql > pks_create.log
2>&1
> "%pgold%\bin\pg_dumpall.exe" -U postgres -p 5432 -sc > cluster_schema.sql
> "%pgnew%\bin\psql" -p 5433 -U postgres -f cluster_schema.sql
```

7. После выполнения указанных операций старая база данных будет подготовлена к репликации данных. Запустите процедуру репликации:

```
> pgtool --path "%pgold%" --slony install
> pgtool --path "%pgnew%" --slony install
> pgtool --path "%pgold%" --port 5432 --port 5433 --slony master
> pgtool --path "%pgnew%" --port 5432 --port 5433 --slony slave
> pgtool --path "%pgold%" --slony start
> pgtool --path "%pgnew%" --slony start
> pgtool --path "%pgold%" --port 5432 --port 5433 --slony subscribe
```

8. В системных службах будут запущены сервисы `slony-VVV_XXX`, где VVV — версия PostgreSQL для старой и новой базы данных, а XXX — тип сборки PostgreSQL (x64 или x86). Сервисы записывают лог-файлы процедуры репликации в папку C:\ProgramData\ISS\logs. Сигналом о том, что обе базы данных обладают одинаковым набором данных, станет наличие записей с префиксом SYNC во всех логах репликации. Для новой базы данных нужно

изменить номер порта, который будет использоваться для подключения. Для этого выполните одно из следующих действий:

- вручную отредактируйте файл `%pgnew%\data\postgresql.conf`.
- выполните команду

```
> pgtool --path "%pgnew%\data\postgresql.conf" --set port=5432.
```

9. Остановите сервер SecurOS.

10. Очистите временную копию базы данных, которая использовалась при репликации:

```
> pgtool --port 5432 --path "%pgnew%" --slony clean -o replica_clean.sql  
> pgtool --user replica
```

11. Остановите системную службу `postgresql-9.1` (если обновление ведется именно с этой версии) и запретите автоматический запуск этой службы.

12. Перезапустите системную службу `postgresql-x64-12`.

13. Запустите сервер SecurOS.

Для некоторых из описанных выше команд требуется подключение к двум базам данных одновременно (например, для репликации данных). Для того, чтобы переопределить параметр подключения ко второй базе данных, необходимо указать оба параметра (даже если для первой базы данных он совпадает со значением по-умолчанию):

```
> pgtool --port 5432 --port 50001 --host localhost --host 192.168.235.209 ...
```

Чтобы дополнительно убедиться в том, что репликация данных прошла успешно, выполните сравнение схем баз данных (требуется подключение к обеим базам). Например:

```
> pgtool --port 50001 --port 50002 -c
```

При выполнении данной команды производится сравнение двух баз данных, начиная с наименований баз данных, схем, таблиц, имен столбцов, заканчивая проверкой первичных ключей и ограничений таблиц. Если различий не выявлено, ответа на команду не предусмотрено.

21.3 Приложение 3. Быстрая настройка видеоподсистемы

По умолчанию, после установки и запуска SecurOS с пустой ("чистой") базой данных, дерево системы состоит из следующих объектов: *Система, SecurOS, Компьютер, Рабочий стол, Медиа Клиент*.

Чтобы создать и настроить основные объекты видеоподсистемы:

1. Настройте параметры объекта *Компьютер*:

- **IP адрес** — нажмите кнопку [**<**] справа от поля (при отсутствии подключения к сети, устанавливается значение адреса 127.0.0.1).
- **Диск** — выберите в таблице (на закладке **Архив**) в столбцах **Видео** и **Аудио** из списка пункт **Чтение/Запись**. Тогда на выбранные диски будет вестись запись видео и аудио архива.

Примечание. Для чтения/записи не рекомендуется выбирать диск с операционной системой.

2. Создайте объект *Устройство видеозахвата*. Данный объект представляет физическое устройство, являющееся источником видеосигнала (IP-камера, IP-энкодер и т.д.). Задайте значения следующих параметров *Устройства видеозахвата*:
 - **Тип** — выберите тип устройства, которое является источником видеосигнала:
 - Если источником сигнала является IP-камера/энкодер, выберите устройство соответствующего производителя.
 - При настройке подключенных IP-устройств, использующих стандартные протоколы, выберите значение ONVIF или Generic RTSP. Убедитесь, что подключенные устройства поддерживают данные протоколы.
 - Для воспроизведения эталонных видеозаписей во время тестирования системы или при проведении презентаций могут быть использованы значения Virtual или Player AVI.
 - **IP-адрес, Пользователь, Пароль** — задайте значения параметров при использовании IP-устройств.
3. Создайте объект *Камера*, дочерний созданному *Устройству видеозахвата*. Объект представляет отдельный видеопоток. В поле **Номер** введите значение идентификатора камеры (начните с 1 и нумеруйте по возрастанию), затем задайте **Название** (например, Офис, Улица, Дом и т.д.). Также можно использовать значения по умолчанию.

Примечания:

1. При использовании IP-камер с одним объективом создается одно *Устройство видеозахвата* с одной дочерней *Камерой*.
 2. Для камер с большим количеством объективов для каждого объектива создается отдельная *Камера*. Все такие *Камеры* являются дочерними для одного и того же *Устройства видеозахвата*.
 3. При использовании камер, подключенных к видеоэнкодеру, для одного *Устройства видеозахвата* может быть создано столько дочерних *Камер*, сколько физических устройств подключено к энкодеру.
-

Задайте значения следующих параметров объекта *Камера*:

- **Номер канала** — выберите номер канала:
 - Для камеры с одним объективом будет использовано значение по умолчанию, равное 1.
 - При использовании камеры с большим количеством объективов объект *Камера* создается для каждого объектива. Такие *Камеры* будут иметь различные номера каналов, нумерация которых последовательно увеличивается, начиная с 1.
 - Если камера подключена к энкодеру, номер канала должен соответствовать номеру порта подключения.
 - **Поворотное устройство** — выберите *Использовать* для IP-камер со встроенным поворотным устройством.
 - **Настройки изображения** — задайте значения параметров на закладке *Дополнительные*.
4. Выберите режим работы *Медиа Клиент* с *Камерами*:
 - **Работать со всеми камерами** — режим по умолчанию. На *Медиа Клиенте* будет выводиться изображение со всех *Камер* системы (флажок **Работать только с указанными Камерами** не отмечен).
 - **Работать только с указанными Камерами** — настраиваемый режим. На *Медиа Клиенте* будет выводиться изображение только от выбранных *Камер*. Для активации режима отметьте флажок **Работать только с указанными Камерами**, в *Дереве объектов* отметьте флажки слева от тех *Камер*, с которыми предполагается работать.

21.4 Приложение 4. Системные утилиты

В комплект поставки SecurOS входит ряд дополнительных программ. Они находятся в корневом каталоге SecurOS или в подкаталоге \Tools папки SecurOS:

- утилита **Server Manager** позволяет вести мониторинг состояния *Серверов конфигурации*, создавать кластер и управлять им (см. раздел [Утилита Server Manager](#)).
- утилита **Hardware Report Utility** составляет отчет обо всех установленных на данный компьютер ключах Guardant (см. раздел [Утилита Hardware Report Utility](#)).
- утилита **SystemInfo** предназначена для сбора системной и сетевой информации, необходимой для Службы технической поддержки Intelligent Security Systems (см. раздел [Утилита SystemInfo](#)).
- утилита экспорта медиа данных **Media Export Utility** воспроизводит архивное видео/аудио, экспортирует выделенную часть архива в файлы формата AVI, ASF и BMP (см. раздел [Утилита Media Export Utility](#)).
- утилита **DSAdmin** предназначена для задания и хранения параметров подключения к используемым базам данных (см. раздел [Утилита настройки подключений к БД \(DSAdmin\)](#)).
- утилита **Database Update Utility** предназначена для доступа к базе данных (см. раздел [Утилита обновления БД \(Database Update Utility\)](#)).
- утилита **Редактор регистрационных файлов** редактирует базу данных типов объектов SecurOS (это не действующая база данных) (см. раздел [Утилита Редактор регистрационных файлов \(DDI\)](#)).
- Утилита **Server Role Manager** используется для назначения роли *Сервер конфигураций* одному из *Периферийных серверов* SecurOS в случае невозможности дальнейшего использования текущего *Сервера конфигураций* (см. раздел [Утилита Server Role Manager](#)).
- Утилита **Server Control Agent** предназначена для работы с *Серверной* и *Клиентской* частями SecurOS, системной службой SecurOS VMSS (Video Management System Server), а также для получения общей информации о текущем состоянии программной и аппаратной частей SecurOS (см. раздел [Утилита Server Control Agent](#)).
- утилита восстановления индексов медиаархива используется для работы с индексными файлами видео- и/или аудиоархива SecurOS (см. раздел [Утилита восстановления индексов медиаархива](#)).
- утилита обновления аудиофайлов устаревшего формата используется для конвертации аудиоархива SecurOS из старого формата в новый (см. раздел [Утилита обновления аудиофайлов устаревшего формата](#)).
- утилита **Certificate Generator** предназначена для создания пробных SSL-сертификатов (см. раздел [Утилита Certificate Generator](#)).
- утилита **AuditClient** предназначена для получения данных аудита SecurOS (см. раздел [Утилита AuditClient](#)).

21.4.1 Утилита Server Manager

Утилита предназначена для централизованного мониторинга и управления состоянием серверов SecurOS (хостов). С ее помощью можно выполнять все операции по созданию и конфигурированию кластера (см. [Резервирование](#)). Возможно управление сразу несколькими конфигурациями.

Внимание!

1. Утилита взаимодействует со службой Video Management System Server на удаленных хостах. Если служба на хосте выключена, он будет недоступен для управления.
2. Для работы утилиты необходимо открыть TCP-порты в настройках брандмауэра (см. [Приложение 5. Используемые в SecurOS сетевые порты](#)).

Основные задачи утилиты:

- Мониторинг состояния хостов;
- Создание отказоустойчивого кластера;
- Наглядное визуальное представление состояния кластера;
- Конфигурирование кластера.

Внимание! Для создания нод кластера и изменения их параметров следует использовать *Дерево объектов SecurOS* (см. [Добавление Ноды](#)).

Нахождение на диске:

- <корневой каталог SecurOS>\ServerManager.exe — для ОС семейства Windows;
- opt/iss/securos/ServerManager — для ОС семейства Linux.

Запуск через главное меню для ОС семейства Windows:

Пуск → Программы → SecurOS → Server Manager

Запуск утилиты в операционных системах семейства Linux производится из корневого каталога SecurOS.

Внешний вид окна утилиты представлен на рис. [292](#).

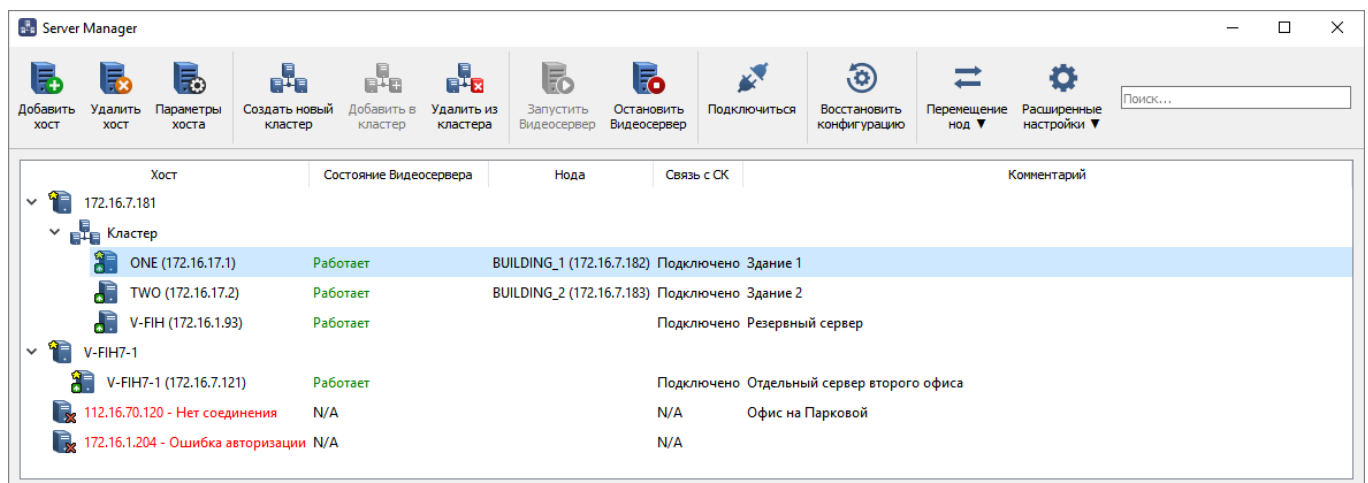


Рис. 292. Окно утилиты Server Manager

В верхней части окна утилиты находится панель управления, состоящая из кнопок и поисковой строки (см. [Панель управления](#)).

Под панелью управления расположена таблица хостов. В ней отображается состояние всех добавленных в утилиту хостов, сгруппированных по *Серверу конфигураций* (см. [Таблица хостов](#)).

21.4.1.1 Панель управления

Внешний вид панели управления *Server Manager* представлен на рис. 293.

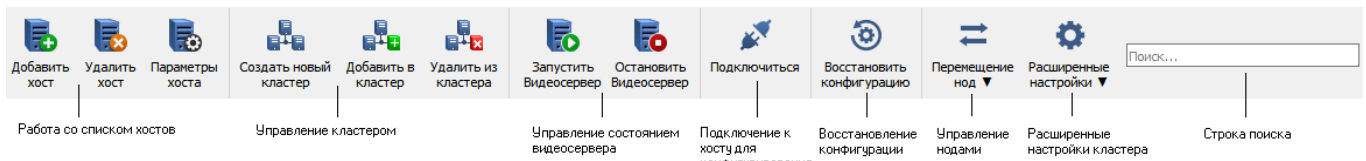


Рис. 293. Панель управления

Панель управления предоставляет следующие возможности:

- Работа со списком хостов.
- Управление кластером.
- Управление состоянием Видеосервера.
- Подключение к хосту для конфигурирования.
- Восстановление конфигурации SecurOS.
- Управление нодами.
- Расширенные настройки кластера.
- Строка поиска.

21.4.1.1.1 Работа со списком хостов

Работа со списком хостов включает следующие операции:

- Добавление хоста в список;
- Удаление хоста из списка;
- Изменение параметров хоста.

Добавление хоста в список

Нажмите кнопку **Добавить хост** или клавишу **Insert** и заполните поля в появившемся окне.

Рис. 294. Окно добавления хоста в список

В качестве **Администратора** необходимо указать пользователя операционной системы, обладающего правами администратора на добавляемом компьютере.

Внимание! При добавлении в список хоста с ОС семейства Linux необходимо указывать пользователя, который принадлежит к группе `sudo` или `astra-admin` (только для Astra Linux) на добавляемом хосте.

Удаление хоста из списка

Выберите хост в списке и нажмите кнопку **Удалить хост** или клавишу **Delete**.

Изменение параметров хоста

Выберите хост в списке и нажмите кнопку **Параметры хоста** или клавишу **Enter**. Для изменения доступны параметры авторизации и комментариев.

21.4.1.1.2 Управление кластером

Управление кластером включает следующие операции:

- **Создание кластера;**
- **Добавление хоста в кластер;**
- **Удаление хоста из кластера.**

Создание кластера

Выберите в списке хост, на основе которого необходимо создать кластер, и нажмите кнопку **Создать новый кластер**. Заполните поля в появившемся окне.

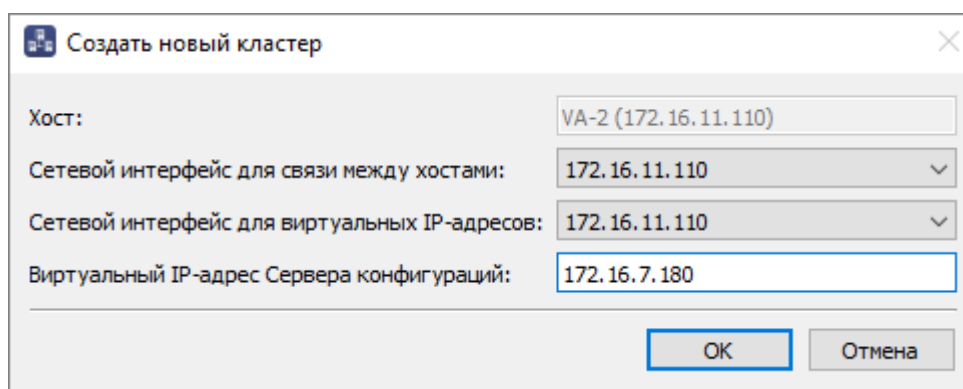


Рис. 295. Окно создания кластера

В качестве **Виртуального IP-адреса Сервера конфигураций** необходимо указать доступный и не занятый IP-адрес.

Примечание. Если был выбран хост, уже состоящий в кластере, существующий кластер будет пересоздан.

Добавление хоста в кластер

Выберите в списке работающий хост, не состоящий в кластере, и нажмите кнопку **Добавить в кластер**. Заполните поля в появившемся окне.

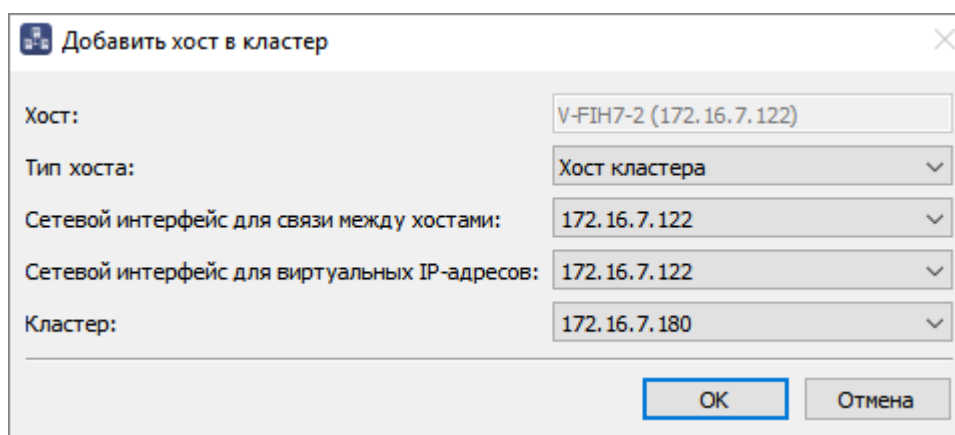


Рис. 296. Окно добавления хоста в кластер

Чтобы подключить выбранный хост к кластеру резервных серверов (см. **Кластер резервных серверов**) выберите вариант **Вспомогательный хост** для параметра **Тип хоста**.

Удаление хоста из кластера

Выберите в списке хост, состоящий в кластере, и нажмите кнопку **Удалить из кластера**.

Процедура удаления хоста из кластера выполняется в два этапа:

1. Удаление хоста из списка членов кластера.
2. Перевод хоста в режим работы *Видеосервера*.

В связи с этим при удалении хоста из кластера возможны три сценария:

1. Удаляемый хост доступен и в кластере есть кворум. В этом случае оба этапа будут выполнены успешно и произойдет полное удаление хоста из кластера.
2. Удаляемый хост доступен, но в кластере нет кворума. В этом случае кластер не сможет удалить хост из списка своих членов. Сам же хост при этом перейдет в режим работы *Видеосервера*. Необходимо повторно выполнить процедуру удаления хоста из кластера после восстановления кворума.
3. Удаляемый хост недоступен, но в кластере есть кворум. В этом случае кластер удалит хост из списка своих членов. Сам же хост не сможет перейти в режим работы *Видеосервера*. Необходимо повторно выполнить процедуру удаления хоста из кластера после восстановления связи с хостом.

21.4.1.1.3 Управление состоянием Видеосервера

Используйте кнопки **Запустить Видеосервер** и **Остановить Видеосервер**, чтобы управлять состоянием Видеосервера SecurOS на выбранном хосте.

21.4.1.1.4 Подключение к хосту для конфигурирования

Выберите хост и нажмите кнопку **Подключиться** или дважды кликните по нему левой кнопкой мыши, чтобы запустить клиентскую часть SecurOS.

21.4.1.1.5 Восстановление конфигурации SecurOS

Выберите хост и нажмите кнопку **Восстановить конфигурацию**, чтобы открыть окно выбора файла конфигурации. Следуйте инструкциям в окне, чтобы восстановить конфигурацию.

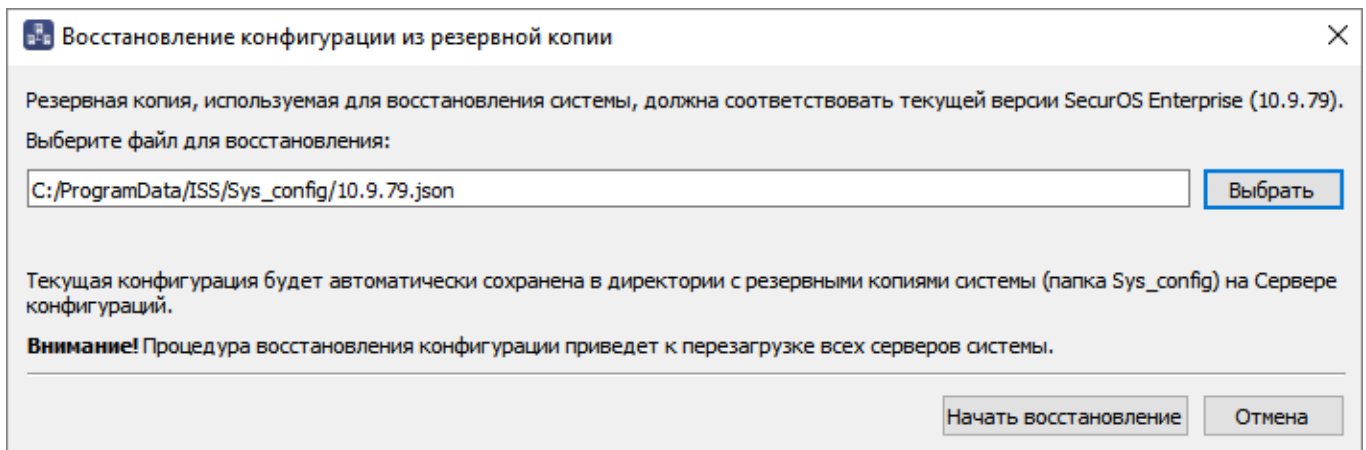


Рис. 297. Окно восстановления конфигурации

Примечание. Текущий пароль суперпользователя (см. [Пользователи в SecurOS](#)) не изменится после восстановления конфигурации.

21.4.1.1.6 Управление нодами

Управление нодами включает следующие операции:

- **Перемещение ноды;**
- **Установка / просмотр приоритетного хоста.**

Перемещение ноды

Выберите в списке хост, где работает нода, которую требуется переместить. Нажмите кнопку **Перемещение нод** и выберите пункт меню **Переместить ноду**. В появившемся окне выберите хост кластера, на который требуется переместить ноду.

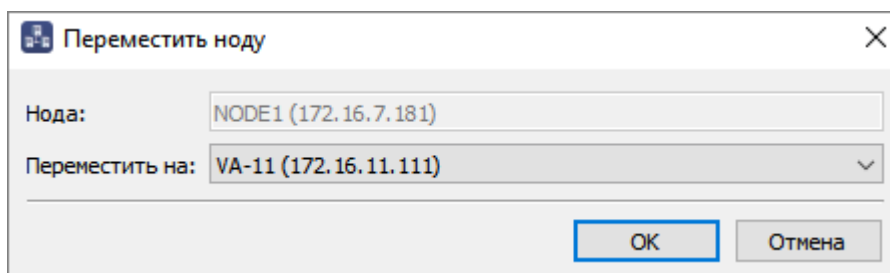


Рис. 298. Окно перемещения ноды

Установка / просмотр приоритетного хоста

Выберите в списке хост, где работает нода, которой необходимо установить приоритетный хост. Нажмите кнопку **Перемещение нод** и выберите пункт меню **Установить приоритетный хост**. В появившемся окне выберите хост кластера, который должен стать приоритетным для ноды. Если параметр **Приоритетный хост** задан, значит выбранный хост уже является приоритетным для этой ноды.

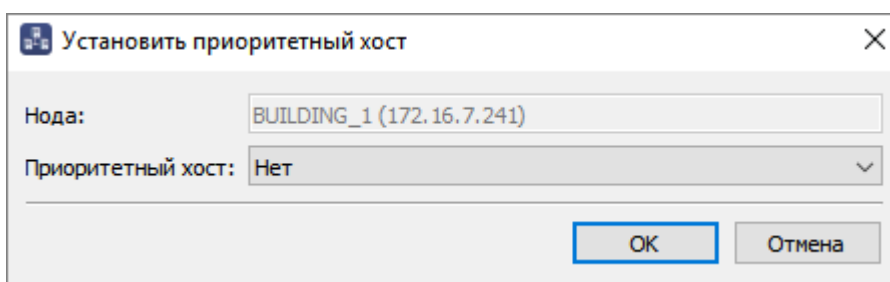


Рис. 299. Окно установки приоритетного хоста

Подробнее о приоритетных хостах см. [Выбор приоритетного Хоста для Ноды](#).

21.4.1.1.7 Расширенные настройки кластера

Расширенные настройки кластера включают следующие операции:

- [Изменение / просмотр сетевого интерфейса для виртуальных IP-адресов](#).
- [Включение / выключение сервисного режима](#).
- [Перенос роли Сервера конфигураций](#).
- [Настройка / просмотр локальных дисков для хранения архива](#).
- [Настройки кворума](#).

Изменение / просмотр сетевого интерфейса для виртуальных IP-адресов

Выберите *Хост* кластера в списке, нажмите кнопку **Расширенные настройки** и выберите пункт **Настройки IP**. В поле **Сетевой интерфейс для виртуальных IP-адресов** будет указан IP-адрес, соответствующий сетевому адаптеру, который используется для поднятия виртуальных IP-адресов. Измените его, если необходимо.

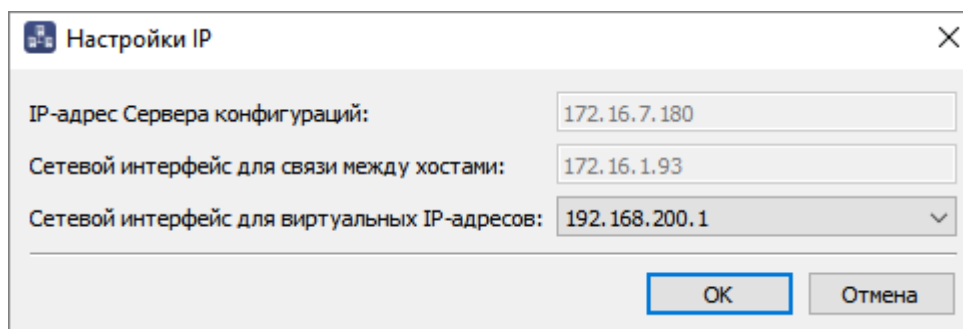


Рис. 300. Окно настроек сетевых интерфейсов

Включение / выключение сервисного режима

Выберите любой *Хост* кластера в списке, нажмите кнопку **Расширенные настройки** и выберите пункт **Сервисный режим**. Текущее значение параметра **Сервисный режим** соответствует типу текущего сервисного режима кластера.

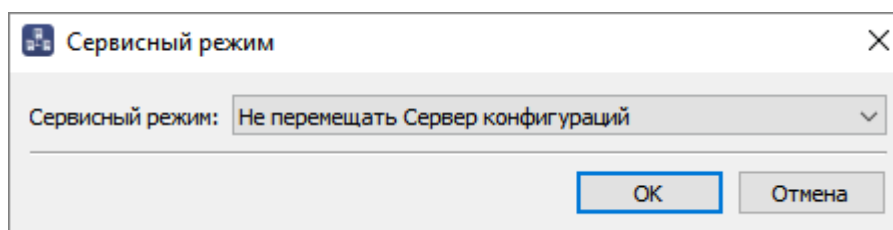


Рис. 301. Окно управления сервисным режимом

Подробнее о сервисном режиме см. [Сервисный режим](#).

Перенос роли Сервера конфигураций

Выберите *Хост* кластера в списке, нажмите кнопку **Расширенные настройки** и выберите пункт **Сделать Сервером конфигураций**.

Настройка / просмотр локальных дисков для хранения архива

Выберите *Хост* кластера в списке, нажмите кнопку **Расширенные настройки** и выберите пункт **Настройки локальных дисков**. Отмеченные в данный момент диски используются для хранения архива на выбранном *Хосте*.

При необходимости измените настройки:

- **Режим** — уровень доступа к диску. Возможные значения:
 - Чтение/Запись — диск доступен для чтения и записи. Значение по умолчанию.
 - Чтение — при выборе значения существующий архив на этом диске останется доступным для просмотра, но новые файлы записываться не будут.
- **Приоритет** — приоритет записи архива на локальный диск *Хоста* относительно настроек *Ноды*.
 - Высокий — высокий приоритет. Архив будет записываться на локальный диск, а при исчерпании свободного пространства — на диски из настроек *Ноды*. Используется по умолчанию.
 - Низкий — низкий приоритет. Архив будет записываться на диски из настроек *Ноды*, а при исчерпании свободного пространства — на локальный диск.
- **Минимальное свободное место** — минимально допустимый объем свободного места на диске в процентах. Когда объем свободного места сократится до указанного значения, начнется запись "по кольцу".

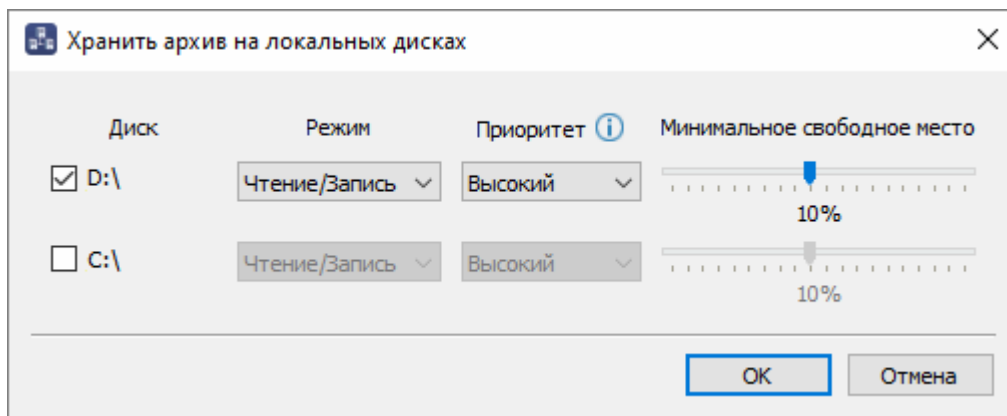


Рис. 302. Окно настройки локальных дисков

Настройки кворума

Внимание!

1. Перечисленные ниже параметры допускается изменять только после согласования со Службой технической поддержки Intelligent Security Systems. В противном случае Intelligent Security Systems не несет ответственности за корректное функционирование кластера.
2. При нормальном функционировании кластера изменять указанные параметры крайне не рекомендуется.

Укажите следующие параметры кворума:

- **Интервал опроса хостов** — интервал проверки доступности *Хостов* кластера. Доступность *Хостов* определяется периодически, с помощью отправки им широковещательных сообщений (хартбитов). Измеряется в миллисекундах. По умолчанию равен 50. Диапазон возможных значений: [10; 100].
- **Таймаут ответа от хоста** — время, необходимое для признания *Хоста* недоступным. Если *Хост* не отправил членам кластера сообщение о доступности в течение заданного таймаута, то он считается недоступным. Измеряется в миллисекундах. По умолчанию равен 500. Диапазон возможных значений: [100; 1000]. Значение данного параметра должно быть как минимум в 5 раз больше значения параметра **Интервал опроса хостов**.
- **Таймаут поддержания кворума** — время, по истечении которого после признания *Хоста* недоступным задействуются механизмы резервирования кластера. Измеряется в секундах. По умолчанию равен 5. Диапазон возможных значений: [5; 300].

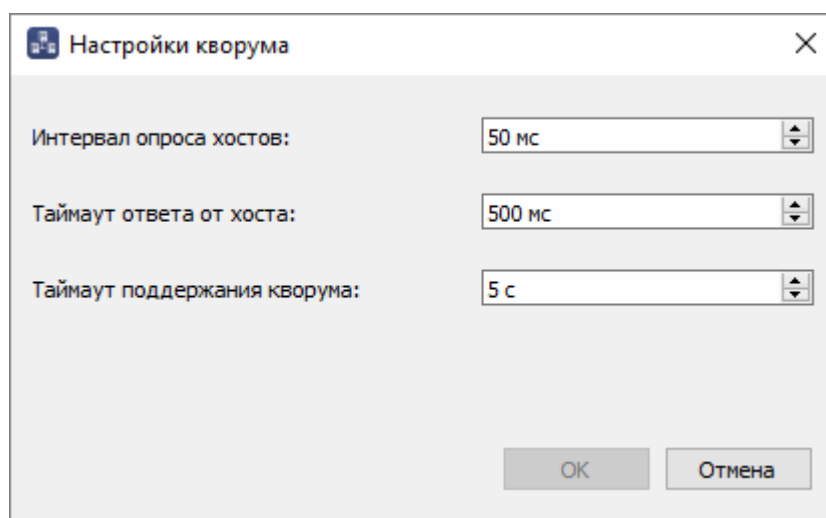


Рис. 303. Окно настроек кворума

21.4.1.1.8 Строка поиска

Введите в поисковую строку часть имени хоста, названия ноды или текста комментария, чтобы найти нужный хост в таблице.

Внимание! Не оставляйте строку поиска заполненной на долгое время, чтобы не пропустить сбои в работе других хостов.

21.4.1.2 Таблица хостов

Таблица хостов содержит все добавленные в утилиту хосты и отображает их в виде дерева. Она включает следующие столбцы:

- **Хост.** Содержит имя хоста, его IP-адрес, а также структуру конфигурации.
- **Состояние Видеосервера.** Если связь с сервером установлена, состоянием *Видеосервера* можно управлять с помощью кнопок **Запустить Видеосервер/Остановить Видеосервер** (см. [Управление состоянием Видеосервера](#)).
- **Нода.** Содержит имя ноды и ее виртуальный IP-адрес, когда хост является членом кластера.
- **Связь с СК.** Содержит статус соединения хоста с его *Сервером конфигураций*.
- **Комментарий.** Содержит дополнительную информацию о хосте, указанную администратором.

Структура дерева хостов представлена на рис. 304.

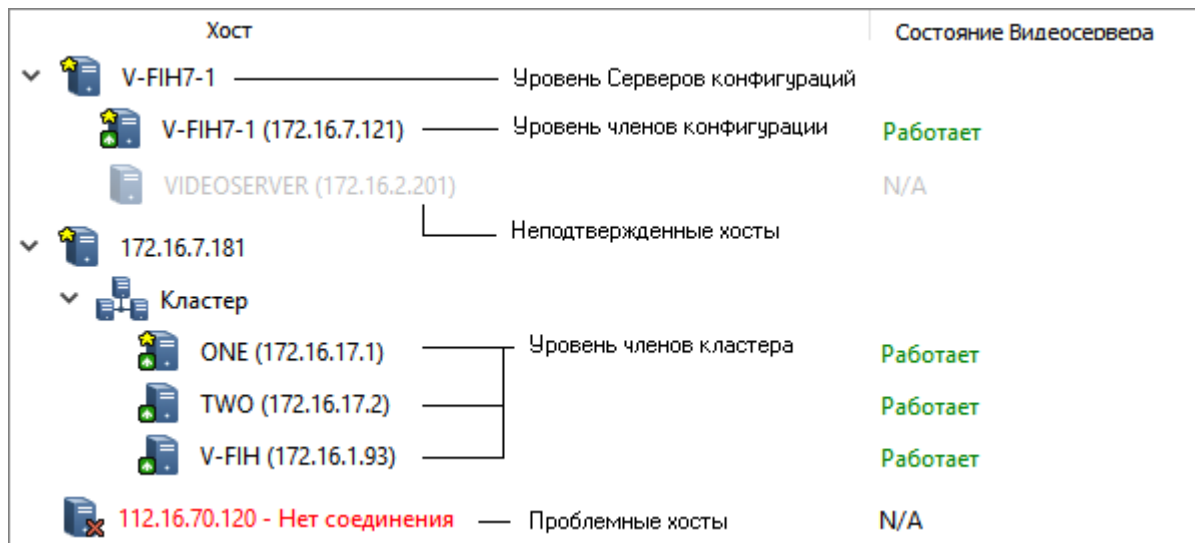


Рис. 304. Структура дерева хостов

Дерево в столбце **Хост** имеет следующую структуру:

1. **Уровень Серверов конфигураций.** На нем расположены *Серверы конфигураций* (имена или IP-адреса).

Примечание. Строка является группирующей. Для выполнения операций над *Сервером конфигураций* добавьте его в утилиту и выберите соответствующую ему строку в таблице на втором уровне.

2. **Уровень членов конфигурации.** На нем расположены хосты, входящие в конфигурацию. В том числе *Сервер конфигураций*.
3. **Уровень членов кластера.** На нем расположены члены кластера, созданного в данной конфигурации. Для хостов кластера в таблице отображаются соответствующие им в данный момент ноды.
4. **Проблемные хосты.** Хосты, с которыми не удалось установить связь. Они перечислены в конце списка с указанием проблемы.
5. **Неподтвержденные хосты** (полупрозрачные элементы в таблице хостов). Не добавленные в утилиту хосты кластера и *Видеосерверы*, о которых она получила информацию от *Сервера конфигураций* или от кластера. Неподтвержденными также становятся компьютеры, состояние или роль которых не удастся определить по каким-либо причинам.

Источники и причины появления неподтвержденных хостов:

- **Кластер**

- Нет связи с добавленным в утилиту хостом кластера.
- Хост есть в списке членов кластера, но не добавлен в утилиту.

- **Сервер конфигураций**

- *Видеосервер* из *Дерева объектов* не добавлен в утилиту.
- *Компьютер* добавлен в утилиту и является хостом кластера, но при этом в *Дереве объектов* есть *Компьютер* с таким же именем и без выбранного параметра **Резервировать Видеосервер** и добавить его в кластер (см. раздел **Компьютер**).

Для неподтвержденных хостов доступны только следующие действия:

- Удаление хоста из кластера (см. раздел [Управление кластером](#)).
- Перемещение ноды и установка приоритетного хоста (см. раздел [Управление нодами](#)).
- Добавление в список компьютеров утилиты (см. раздел [Работа со списком хостов](#)).

Для обозначения ролей и состояний в таблице используются следующие значки:

-  — корневой элемент конфигурации.
-  — корневой элемент кластера внутри конфигурации.
-  — *Сервер конфигураций* в данной конфигурации.
-  — хост данной конфигурации в рабочем состоянии.
-  — вспомогательный хост кластера в рабочем состоянии.
-  — хост доступен, но на нем остановлена *Серверная часть* SecurOS.
-  — состояние хоста неизвестно. Например, *Серверная часть* SecurOS запускается или останавливается.
-  — хост, связь с которым отсутствует. В этом случае к имени хоста добавляется причина отсутствия связи.
-  — хост, аварийно завершивший работу. Наведите курсор на фразу **Аварийное завершение**, чтобы увидеть причину.

21.4.2 Утилита Hardware Report Utility

Утилита определяет все установленные на данный компьютер ключи Guardant, а также уникальный код оборудования. Составляемый с помощью утилиты отчет необходим для генерации файла лицензионного ключа (key.iss) Службой технической поддержки компании Intelligent Security Systems. Утилита также может быть использована для диагностики дополнительного аппаратного обеспечения и сопутствующих драйверов: если идентификатор устройства отсутствует, то это означает некорректность установки драйверов.

- [Работа с утилитой в ОС Windows.](#)
- [Работа с утилитой в ОС Linux.](#)

Работа с утилитой в ОС Windows

Нахождение на диске:

<корневой каталог SecurOS>\Tools\HardwareReportUtility.exe

Запуск через главное меню:

Пуск → Программы → SecurOS → Hardware Report Utility

Внешний вид окна представлен на рис. [305](#).

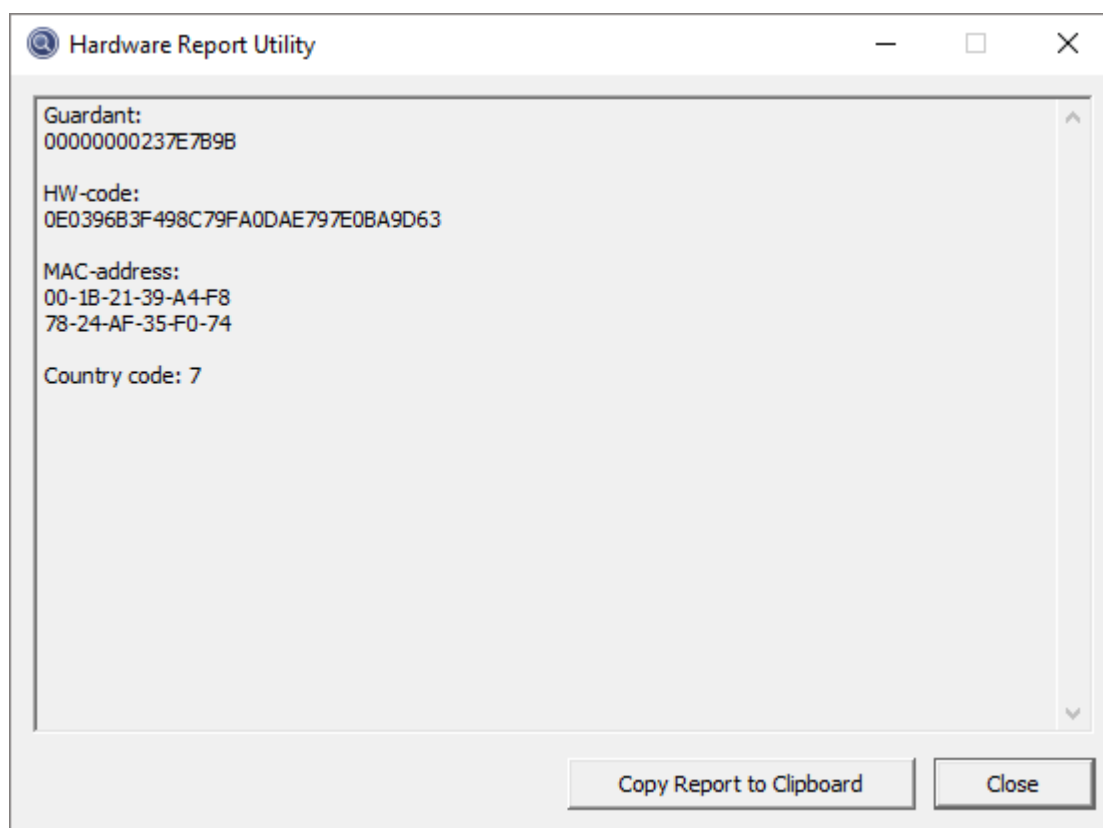


Рис. 305. Результат запроса утилиты Hardware Report Utility

Чтобы записать отчет утилиты в файл:

1. Щелкните кнопку **Copy Report to Clipboard** в окне утилиты.
2. Создайте пустой текстовый файл в любой программе редактирования текстовых файлов (Блокнот, Microsoft Word и т. д.).
3. Вставьте содержимое буфера обмена и сохраните файл отчета.

Работа с утилитой в ОС Linux

Нахождение на диске:

<корневой каталог SecurOS>/hru

Чтобы получить предоставляемые утилитой данные, выполните следующие действия:

1. Запустите консольное приложение *Терминал*.
2. Перейдите в директорию установки SecurOS (по умолчанию `opt/iss/securos`). Для этого выполните следующую команду:

```
cd <директория_установки_SecurOS>
```

3. Запустите исполняемый файл утилиты. Для этого выполните следующую команду:

```
./hru
```

Результат выполнения команды представлен на рис. 306.

```
user@computer:~$ cd /opt/iss/securos
user@computer:/opt/iss/securos$ ./hru
Guardant:
000000003EAB5D26

Hardware:
2AEE1A4F0C32B70F6ABEC98FEDC72E59

user@computer:/opt/iss/securos$ █
```

Рис. 306. Результат выполнения команды `/hru` в консоли

Чтобы сохранить отчет, скопируйте данные и вставьте содержимое буфера обмена в текстовый файл любого формата.

21.4.3 Утилита SystemInfo

Данная утилита предназначена для сбора информации о системе SecurOS, компьютере и сети (см. рис. 307). Такая информация может понадобиться, например, специалистам технической поддержки при устранении неполадок в системе. Собранная информация будет сохранена в отчете SystemInfo.

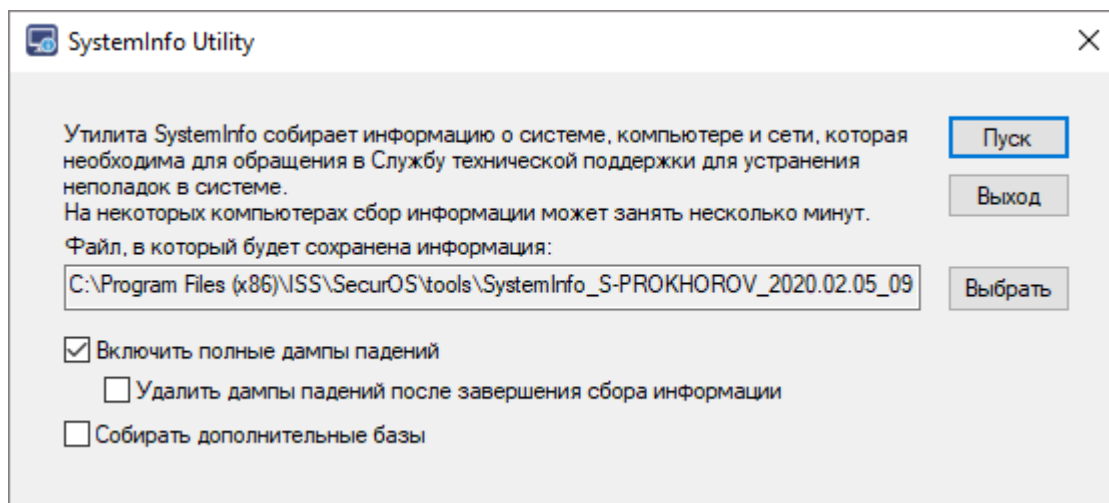


Рис. 307. Окно утилиты SystemInfo в ОС Windows

- Работа с утилитой в ОС Windows.
- Работа с утилитой в ОС Linux.
- Состав отчета.

Работа с утилитой в ОС Windows

Нахождение на диске:

<корневой каталог SecurOS>\Tools\SystemInfo.exe

Чтобы создать отчет

1. Выберите имя файла.
2. Задайте параметры сбора информации (см. **Параметры утилиты** ниже).
3. Нажмите кнопку **Пуск**.

Отчет SystemInfo (см. **Состав отчета**) будет сохранен в файле формата 7z.

Параметры утилиты

- **Включить полные дампы падений** — отметьте флажок, если необходимо включить в отчет информацию об аварийном завершении работы *Сервера* или *Клиента* SecurOS, включая дочерние процессы. Чтобы освободить место на жестком диске компьютера после завершения работы утилиты отметьте флажок **Удалять дампы падений по завершению сбора информации**.

Примечание. При аварийном завершении работы *Клиентского приложения* SecurOS или его дочернего процесса выводится соответствующее информационное сообщение ОС (например, см. рис. 308). При аварийном завершении работы *Серверной части* SecurOS или ее дочернего процесса выводится сообщение модуля самодиагностики **Health Monitor**. Для анализа любых прочих проблем полные дампы падений не требуются.

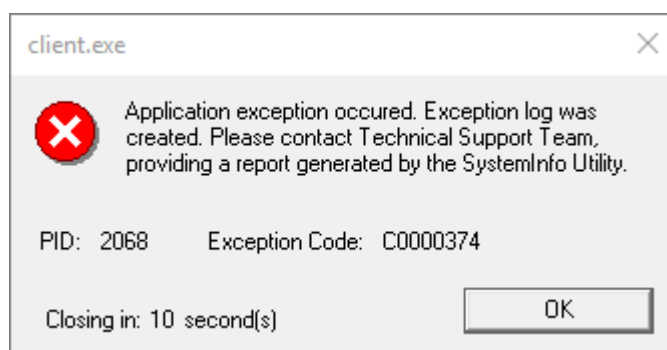


Рис. 308. Сообщение об аварийном завершении работы приложения

- **Собирать дополнительные базы** — отметьте флажок для сбора дополнительной информации о SecurOS и установленных интеллектуальных Модулях. Будут собраны все дополнительные базы данных, которые используются на данном компьютере (см. раздел **Утилита настройки подключений к БД (DSAdmin)**).

Примечание. Дополнительная информация собирается только по запросу сотрудников Службы технической поддержки Intelligent Security Systems. Во всех прочих случаях дополнительная информация не требуется.

Работа с утилитой в ОС Linux

Нахождение на диске:

<корневой каталог SecurOS>/systeminfo

Чтобы получить предоставляемые утилитой данные, выполните следующие действия:

1. Запустите консольное приложение *Терминал*.
2. Перейдите в директорию установки SecurOS (по умолчанию `opt/iss/securos`). Для этого выполните следующую команду:

```
cd <директория_установки_SecurOS>
```

3. Запустите исполняемый файл утилиты от имени суперпользователя. Для этого выполните следующую команду:

```
sudo ./systeminfo
```

Результат выполнения команды `sudo ./systeminfo` представлен на рис. 309.

```
s-p@debian-sp:/opt/iss/securos$ sudo ./systeminfo
[ ok ] Created temp directory
[ ok ] Started collect netstat in background
[ ok ] Started collect databases in background
[ ok ] Collected system info
[ ok ] Collected installed files info
[ ok ] Collected additional files
[ ok ] Collected settings
[ ok ] Collected dallas codes
[ ok ] Collected crash dumps
[ ok ] Collected syslogs
[ ok ] Collected netstat
[ ok ] Collected databases
[ ok ] Compressed collected data to /root/systeminfo_debian-sp_2023.10.09_10.53.21.7z
```

Рис. 309. Результат выполнения команды `sudo ./systeminfo` в консоли

По умолчанию созданный отчет в формате архива сохраняется в директории `/root/`. Указать свою директорию для сохранения отчета можно в конце команды на запуск утилиты:

```
./systeminfo <путь до директории для отчета>
```

Если требуется удалить дампы, то следует добавить к основной команде атрибут `-d`:

```
./systeminfo -d
```

Для сбора дополнительных баз данных добавьте атрибут `-a`:

```
./systeminfo -a
```

Использование в команде атрибута `-v` позволяет определить версию утилиты `SystemInfo`:

```
./systeminfo -v
```

Для получения полной справки по утилите используйте атрибут `-h`:

```
./systeminfo -h
```

Внимание! Версия утилиты `SystemInfo` в ОС Linux не собирает логи PostgreSQL.

Состав отчета

В отчет входят следующие папки и файлы:

- папка `crashlogs` — содержит лог-файлы падений SecurOS и/или ее компонентов;
- папка `cur` — содержит файлы с настройками протоколирования работы модулей, файлы программ и скриптов, xml-файлы библиотек интегрированных камер и видеосерверов и т.д. Файлы размещены во вложенных папках, соответствующих типу файла.

Дополнительно в папке `cur` содержатся следующие файлы:

- `key.iss` — текущий ключевой файл SecurOS;
- `licenced_objects.txt` — информация о количестве имеющихся в системе лицензируемых объектов ((разрешенное) : текущее);
- `securos.sqlite` — содержит копию конфигурации SecurOS, используемую клиентским модулем.
- папка `devices` — содержит бинарный лог-файл проблем взаимодействия с камерами;
- папка `dumps` — содержит полные и/или сокращенные дампы аварийного завершения работы SecurOS и/или ее компонентов;
- папка `installer` — содержит лог-файлы инсталлятора SecurOS;
- папка `logs` — содержит лог-файлы SecurOS;

Примечание. Лог файлы модулей SecurOS записываются в папку `%ProgramData%\ISS\Logs` (в ОС Windows) или `/var/opt/securos/logs` (в ОС Linux).

- папка `logs\tomcat` — содержит лог-файлы сервера Apache TomCat (WebConnect);
- папка `logs\nginx` — содержит лог-файлы сервера nginx (WebConnect);
- папка `syslogs` — содержит системные лог-файлы (только в ОС Linux);
- папка `PostgresLogs` — содержит лог-файлы PostgreSQL;
- папка `TomCat` — содержит лог-файлы сервера Apache TomCat (WebView);
- папка `WindowsEventLogs` — содержит файлы журналов Windows Приложение и Система (файлы `Application.evtx` и `System.evtx`, соответственно);
- файл `DallasCodes.txt` — содержит информацию о кодах установленных устройств (Guardant);
- файлы `data.sql`, `videoi.sql` и `protocol.sql` — содержат информацию из БД `securos`, `fsindex` и `protocol`, соответственно. Если собираются дополнительные базы (см. [Утилита настройки подключений к БД \(DSAdmin\)](#)), то в состав отчета включаются прочие sql-файлы с соответствующими именами;
- файл `DxDiagInfo.txt` — содержит информацию о системных устройствах компьютера, на котором установлен SecurOS и на котором была запущена утилита;
- файл `cluster.json` — содержит информацию о конфигурации кластера, к которому принадлежит данный компьютер;
- файл `ISS_Config.reg` — содержит информацию о разделе реестра `HKLM\SOFTWARE\ISS` (только в ОС Windows);
- файл `securos.conf` — содержит информацию о настройках SecurOS (только в ОС Linux);
- файл `modules.txt` — содержит перечень dll- и exe-файлов с указанием их версии из папки SecurOS;

- файл `system32.txt` — содержит перечень `dll`- и `exe`-файлов с указанием их версии из папки `C:\Windows\System32`;
- файл `netstat.txt` — содержит данные об активных подключениях данного компьютера на момент запуска утилиты;
- файл `SystemInfo.nfo` — содержит основную системную информацию о компьютере, на котором установлен SecurOS и на котором данная утилита была запущена;
- файл `core_rt.conf` — содержит параметры состояния сервера SecurOS на момент последнего выключения (только в ОС Linux);
- файл `journalctl.txt` — содержит выходные данные утилиты `journalctl` (только в ОС Debian).

21.4.4 Утилита Media Export Utility

В ОС **Linux** функциональность не поддерживается.

Нахождение на диске:

<корневой каталог SecurOS>\Backup.exe

Запуск через главное меню:

Пуск → Программы → SecurOS → Media Export Utility

Утилита (см. рис. 310) используется для экспорта видеоархивов и видеоархивов со звуком в файлы формата AVI и ASF, для экспорта видеокадра в формат BMP, а также экспорта звукового файла, записанного с помощью свободного микрофона.

Внимание! Утилита может использоваться для экспорта видеоархивов только на видеосерверах.

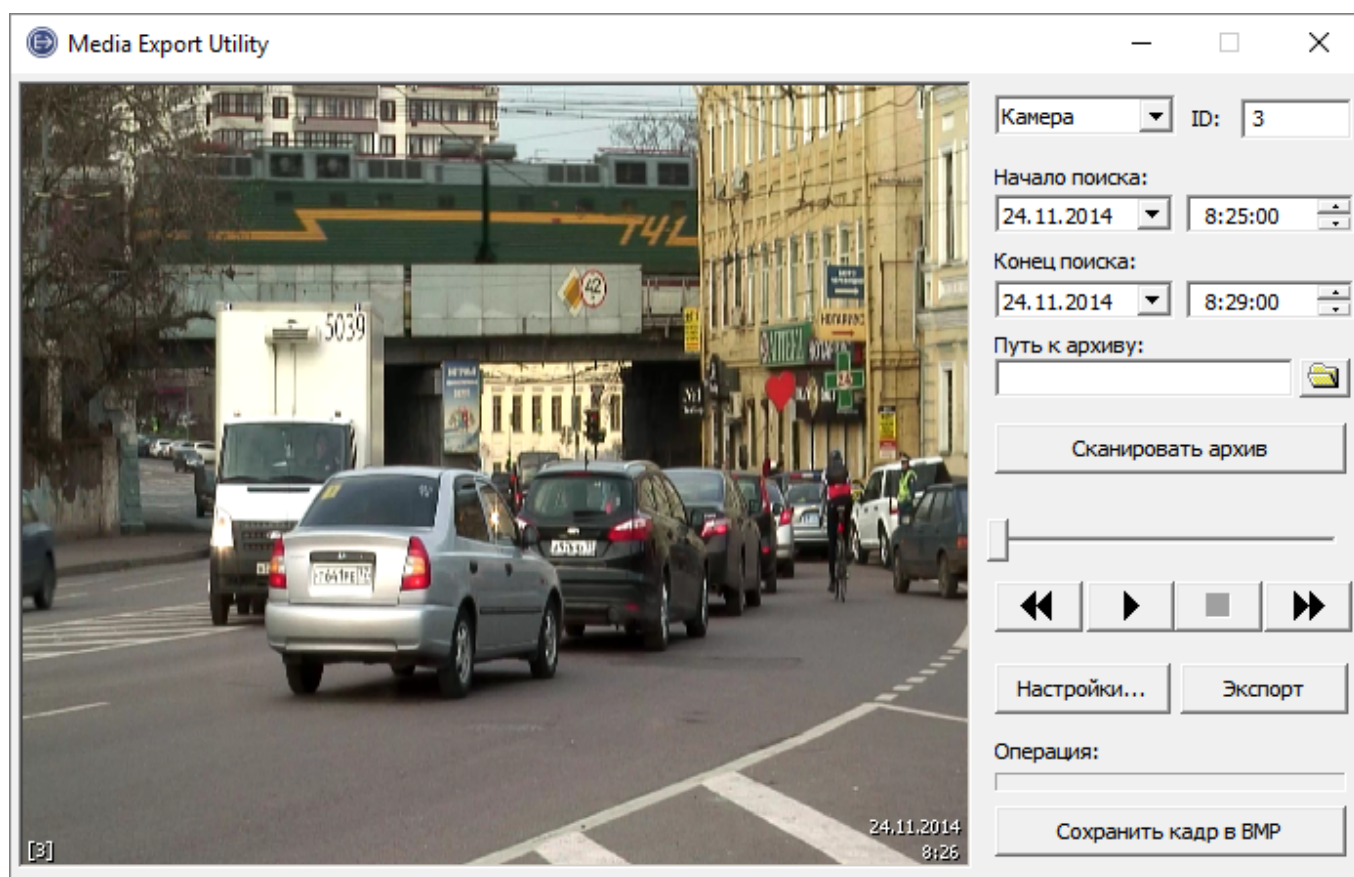


Рис. 310. Окно утилиты Media Export Utility

Чтобы экспортировать видео:

1. В списке источников архива выберите тип **Камера** и укажите идентификатор объекта *Камера*.
2. Определите параметры **Начало поиска** и **Конец поиска** для поиска в архиве.
3. Щелкните кнопку **Путь к архиву** и выберите путь к архиву, который необходимо экспортировать. Оставьте поле пустым для поиска архива по всем логическим дискам компьютера.
4. Щелкните кнопку **Сканировать архив** для указанной *Камеры* и определенного временного интервала.
5. При необходимости просмотреть найденный архив используйте кнопки **Воспроизведение/Стоп** для запуска и остановки воспроизведения. Используйте ползунок или кнопки **Назад/Вперед** для перемещения по найденным записям архива.
6. При необходимости переопределите параметры поиска в архиве, повторно выполнив пп. **1—5**.
7. Определите параметры экспорта (кодеки видео/аудио, папку для сохранения экспортированного файла и т. д.) в диалоговом окне **Настройки экспорта**.
8. Щелкните кнопку **Экспорт** для запуска процедуры экспорта. Данная процедура может занять продолжительное время в зависимости от размера архива и настроек экспорта.
9. Щелкните кнопку **Стоп** во время экспорта, если необходимо прервать процесс. Экспортированная часть архива сохранится в файле формата AVI или ASF.

Примечание. Во время воспроизведения архива или при перемещении по нему можно нажать кнопку **Сохранить кадр в BMP** для сохранения текущего видеокadra в файл формата BMP. Файлы будут сохраняться в папку, указанную в диалоговом окне **Настройки экспорта**.

Внимание! Для просмотра видео, полученного в результате быстрой конвертации, рекомендуется использовать медиа-проигрыватель VLC.

Чтобы экспортировать аудио, записанное с помощью свободного микрофона:

1. В списке источников архива выберите тип **Микрофон** и укажите идентификатор объекта *Микрофон*.
2. Определите параметры **Начало поиска** и **Конец поиска** для поиска в архиве.
3. Щелкните кнопку **Путь к архиву** и выберите путь к архиву, который необходимо экспортировать. Оставьте поле пустым для поиска архива по всем логическим дискам компьютера.
4. Щелкните кнопку **Сканировать архив** для указанного *Микрофона* и определенного временного интервала.
5. Определите параметры экспорта (кодек аудио, папку для сохранения экспортированного файла и т. д.) в диалоговом окне **Настройки экспорта**.
6. Щелкните кнопку **Экспорт** для запуска процедуры экспорта. Данная процедура может занять продолжительное время в зависимости от размера архива и настроек экспорта.
7. Щелкните кнопку **Стоп** во время экспорта, если необходимо прервать процесс. Экспортированная часть архива сохранится в файле формата AVI или ASF.

Примечание. Прослушивание архивной аудио записи с помощью утилиты невозможно.

21.4.4.1 Диалоговое окно настройки экспорта

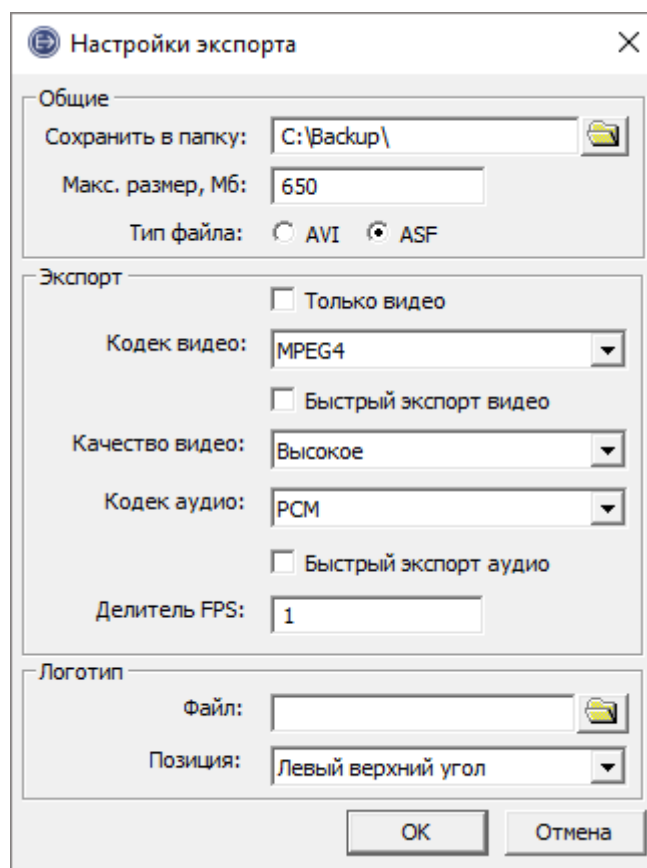


Рис. 311. Диалоговое окно настройки параметров экспорта

Таблица 118. Параметры экспорта

Параметр	Описание
Общие	
Сохранить в папку	Укажите папку для хранения выходных файлов. Введите вручную или используйте кнопку справа для открытия диалогового окна Выбор каталога .
Макс. размер, Мб	Заполните это поле для разбиения большого файла на меньшие размером, определенного в этом поле (в МБ). Значение по умолчанию — 650 МБ. Внимание! Некоторые медиа-проигрыватели не поддерживают AVI-файлы размером более 2 ГБ.
Тип файла	Выберите поле, соответствующее типу выходного файла (AVI или ASF).
Экспорт	
Только видео	Активируйте это поле, чтобы экспортировать архив без звука.
Кодек видео	Выберите кодек видео.
Быстрый экспорт видео	Активируйте это поле для быстрого экспорта видео архива. Быстрый экспорт видео возможен только для архивов, созданных с использованием кодеков H.263, H.264, MPEG-4 и MJPEG. Примечания: 1. При быстром экспорте видео параметры Кодек видео , Качество видео , Делитель FPS , Файл и Позиция будут проигнорированы. 2. Если конвертация в заданном режиме невозможна, будут использованы указанные выше параметры.
Качество видео	Выберите требуемое качество.
Кодек аудио	Выберите кодек аудио.
Быстрый экспорт аудио	Активируйте это поле для быстрого экспорта аудио архива. Быстрый экспорт аудио возможен только для архивов, созданных с использованием кодеков GSM, PCM, ADPCM. Примечания: 1. При быстром экспорте аудио параметр Кодек аудио будет проигнорирован. 2. Если конвертация в заданном режиме невозможна, будет использован указанный выше параметр.

Параметр	Описание
Делитель FPS	Укажите параметр прореживания FPS. Внимание! Опция работает корректно только если изначально при сжатии видео использовался алгоритм без дельта-кадров. Например, MJPEG для IP-камер. В остальных случаях при прореживании могут возникнуть рывки и пропуски кадров на результирующем видео.
Логотип	
Файл	Укажите имя файла логотипа (формата .PNG), накладываемого на область видео.
Позиция	Укажите позицию расположения логотипа на области видео.

21.4.4.2 Параметры командной строки

Можно воспользоваться утилитой экспорта медиа данных (см. [Утилита Media Export Utility](#)), вызвав ее из командной строки или командного файла, для автоматизации процедуры экспорта. При вызове из командной строки будут применяться текущие настройки экспорта. Для изменения текущих настроек запустите утилиту экспорта медиа данных в нормальном (оконном) режиме и задайте новые параметры экспорта, затем закройте утилиту. Требуемые параметры также могут быть указаны при запуске утилиты из командной строки.

Синтаксис командной строки утилиты экспорта медиа данных (в примере указаны наиболее часто используемые параметры):

```
backup.exe --out <out_file> --cam <camera_number> --from "<start_date_time>"
--to "<end_date_time>" --span <span_size> --silent
```

Таблица 119. Параметры командной строки

Параметр	Тип	Описание
Параметры поиска		
--cam	<число>	Номер камеры, видеоархив которой будет экспортироваться.
--from	<дата>	Начальная точка (дата, время) архива для экспорта. Например: 19-02-05 00:00:00.
--to	<дата>	Конечная точка (дата, время) архива для экспорта. Например: 20-02-05 23:59:59.
--frame		Используется для экспорта кадра, заданного параметрами --cam и --from в изображение .BMP.
Директория поиска		
Внимание! При запуске утилиты без параметров --archive-folder или --archive-path поиск будет осуществляться только по оперативному архиву.		
--archive-folder		Поиск по долговременному архиву.

Параметр	Тип	Описание
--archive-path	<абсолютный путь>	Поиск архива только в указанной директории.
Параметры экспорта		
--out	<полное имя файла>	Имя выходного файла с абсолютным путем. Например, C:\export\out.avi.
--video-only		Экспорт видеоархива без звука.
--container	<тип файла>	Тип файла. Возможные значения: AVI или ASF.
--span	<число>/<строка>	Размер результирующих файлов. Укажите либо число (значение в МБ), либо зарезервированные переменные: dvd (4.7 ГБ для записи на DVD-диски), либо cd (650 МБ для записи на CD-диски).
--video-codec	<строка>	Кодек, используемый при экспорте видео. Возможные значения: MJPEG, MPEG4.
--audio-codec	<строка>	Кодек, используемый при экспорте аудио. Возможные значения: PCM, WMA, MP3.
--video-quality	<число>	Качество видео. Укажите число в диапазоне [0; 100].
--raw-video		Быстрый экспорт видео.
--raw-audio		Быстрый экспорт аудио.
--fps-divider	<число>	Делитель FPS. Укажите число в диапазоне [1; 100].

Параметр --silent позволяет запустить утилиту в режиме автоконвертирования по указанным параметрам без появления главного окна приложения.

Параметр --help вызывает подсказку со списком всех параметров утилиты экспорта медиа данных.

Пример 1:

```
backup --cam 1 --from "27-12-06 18:36:42" --to "28-12-06 22:43:12" --span 2
```

Описание: экспорт видеоархива по камере 1 за указанный период, сохраняя в файлы по 2 МБ.

Пример 2:

```
backup --out "C:\custom path\pwnage.avi"
--from "27-12-06 18:36:42" --to "28-12-06 22:43:12" --span cd
```

Описание: экспорт видеоархива за указанный период времени, сохраняя в указанный файл по размеру стандартного CD-диска (650 МБ).

Примечание. Номер камеры и другие неуказанные параметры берутся из настроек утилиты.

21.4.5 Утилита настройки подключений к БД (DSAdmin)

Утилита предназначена для хранения/изменения строки подключения к следующим базам данных:

- **БД настроек.** Хранит настройки объектов системы. Имя базы задается при установке продукта. По умолчанию используется имя `securos`.
- **БД событий.** Хранит информацию о событиях, произошедших в системе. Создается автоматически при установке системы с именем `protocol`.
- **БД аудита.** Хранит данные аудита действий пользователя SecurOS. По умолчанию используется БД `protocol`.
- **БД видеоархива.** Хранит информацию о зарегистрированных тревогах и установленных в видеоархиве закладках. Создается автоматически при установке системы с именем `fsindex`.
- Любой другой базе данных, устанавливаемой дополнительно.

Нахождение на диске:

- <корневой каталог SecurOS>\dsadmin.exe — для ОС семейства Windows.
- `opt/iss/securos/dsadmin` — для ОС семейства Linux.

Внешний вид главного окна утилиты представлен на рис. 312.

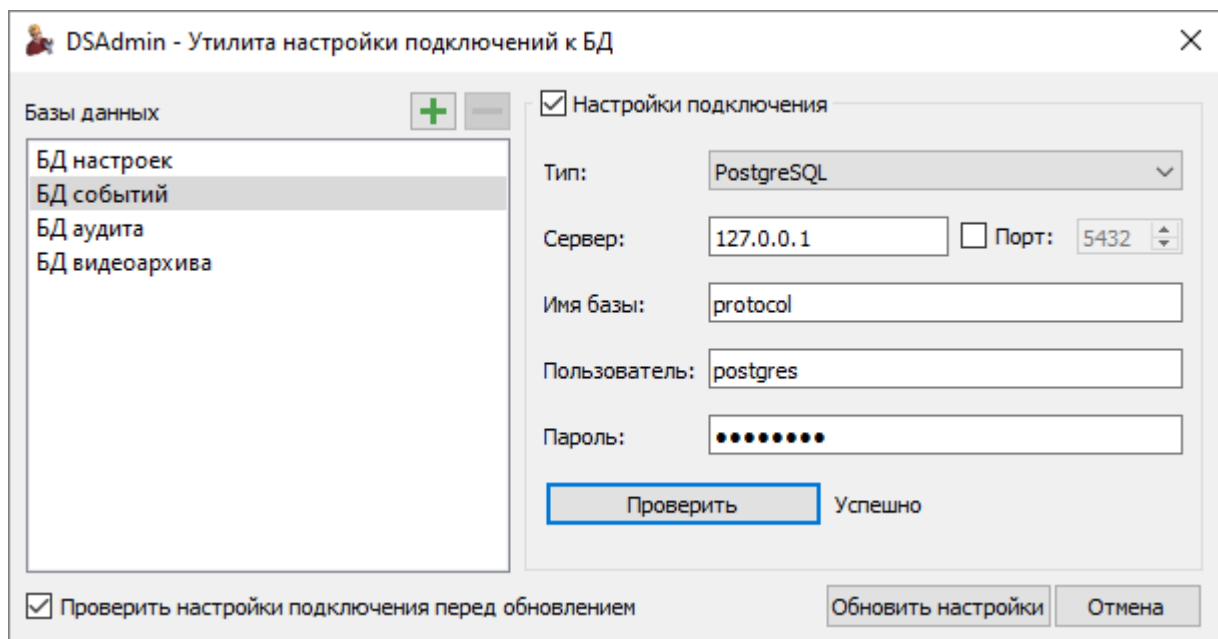


Рис. 312. Главное окно утилиты DSAdmin

Таблица 120. Назначение полей утилиты DSAdmin

Параметр	Описание
Блок Базы данных	

Параметр	Описание
Список баз данных	Всегда содержит следующие базы данных: • БД настроек — обязательная база, активна всегда. • БД событий — обязательная база, но в зависимости от настроек утилиты может не использоваться. По умолчанию активна. • БД аудита — необязательная база. По умолчанию активна. • БД видеоархива — обязательная база, но в зависимости от настроек утилиты может быть неактивна. По умолчанию активна. Помимо указанных выше, список может содержать любое количество баз данных, устанавливаемых дополнительно.
Блок Настройки подключения	
Настройки подключения	Флаг активности базы данных. Отображается только для некоторых основных баз. В остальных случаях флаг отсутствует. Если не отмечен, параметры соединения блокируются, соединение SecurOS с базой данных разрывается. После сохранения таких настроек все параметры соединения с базой обнуляются. Примечания: 1. Флаг учитывается при работе утилиты SystemInfo. При установленном флаге Собирать дополнительные базы будут собираться данные только для тех баз, которые используются. 2. Если в системе установлены дополнительные базы, то сбор аналогичных данных утилитой SystemInfo будет выполняться только для тех из них, которые включены в Список баз данных (см. выше).
Тип	Тип базы данных. Обязательный параметр. Возможные значения: • PostgreSQL (значение по умолчанию). • SQL Server.
Сервер	Имя или IP-адрес сервера, на котором установлена БД. Обязательный параметр.
Порт	Номер порта для подключения. Необязательный параметр. Если флажок отмечен, соединение устанавливается по заданному порту. Если флажок не отмечен, соединение устанавливается по порту 5432 (значение по умолчанию).
Имя базы	Имя базы данных, заданное при ее установке. Обязательный параметр.

Параметр	Описание
Пользователь	Имя учетной записи администратора БД, заданное при ее установке. Обязательный параметр.
Пароль	Пароль учетной записи администратора БД, заданный при ее установке. Обязательный параметр.
Проверить (кнопка)	Нажмите кнопку, чтобы проверить соединение с БД по заданным параметрам. Если соединение устанавливается, справа от кнопки выводится результат Успешно. В противном случае выводится результат Ошибка. Проверьте заданные параметры и повторите тест соединения.
Общие параметры	
Проверить настройки подключения перед обновлением	Снимите флажок, если проверка соединения со всеми указанными базами данных перед обновлением не требуется.
Обновить настройки (кнопка)	Нажмите на кнопку, чтобы применить все изменения и завершить работу с утилитой.
Отмена (кнопка)	Нажмите на кнопку, чтобы отменить все изменения и завершить работу с утилитой.

Для добавления подключения к дополнительной базе данных выполните следующие действия:

1. Нажмите кнопку  над блоком **Базы данных**.
2. В списке **Базы данных** добавится новая строка (см. рис. 313).

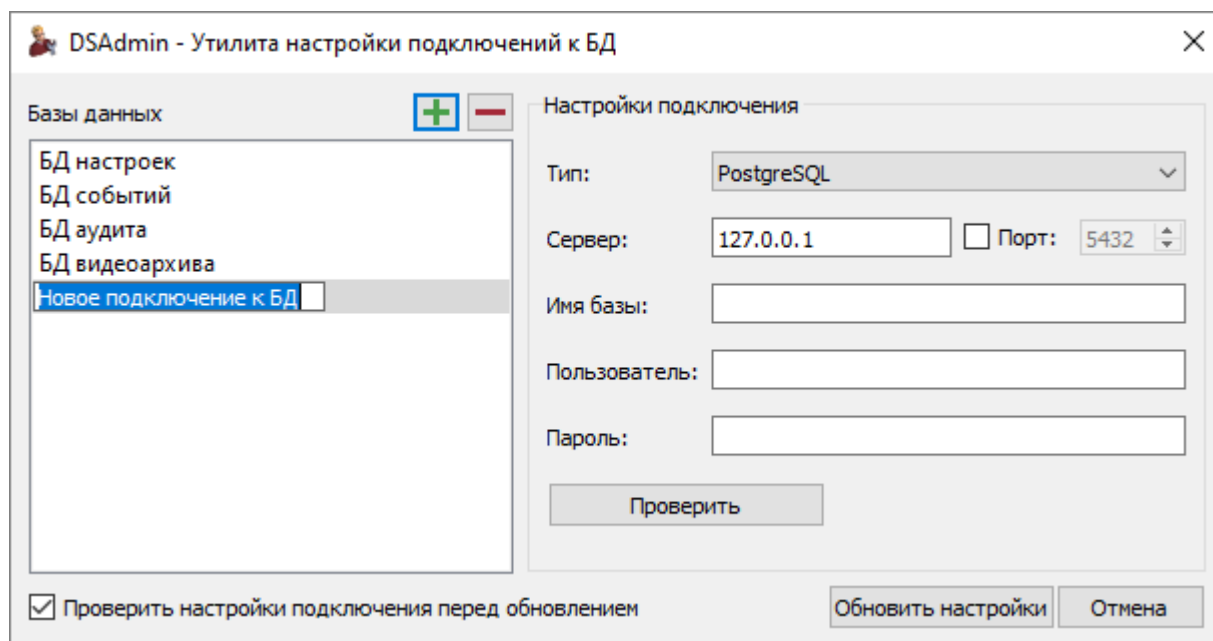


Рис. 313. Добавление новой базы данных

3. В новой строке задайте имя добавляемой базы данных. Нажмите клавишу **Enter**.

4. В блоке **Настройки подключения** задайте необходимые параметры, нажмите кнопку **Проверить** для проверки соединения.
5. При успешном результате проверки нажмите кнопку **Обновить настройки** для сохранения изменений и завершения работы с утилитой.

Для удаления подключения к дополнительной базе данных выполните следующие действия:

1. В блоке **Базы данных** выделите мышью дополнительную базу данных, подключение к которой необходимо удалить из списка.
2. Нажмите кнопку  над блоком **Базы данных**. Подключение к выбранной базе данных будет удалено из списка, при этом:
 - физическая база данных не удаляется;
 - работоспособность продукта, использующего удаленную базу данных, не нарушается.

Примечание. Удалить можно только подключение к дополнительной базе данных, созданное пользователем.

21.4.6 Утилита обновления БД (Database Update Utility)

Утилита предназначена для настройки и обновления базы данных SecurOS, в которой хранятся настройки объектов SecurOS (база данных `securos`). Модификация выполняется с помощью файла `securos.dbi`, в котором хранится описание актуальной структуры БД.

Нахождение на диске:

- <корневой каталог SecurOS>\idb.exe — для ОС семейства Windows.
- `opt/iss/securos/idb` — для ОС семейства Linux.

Внешний вид главного окна представлен на рис. 314.

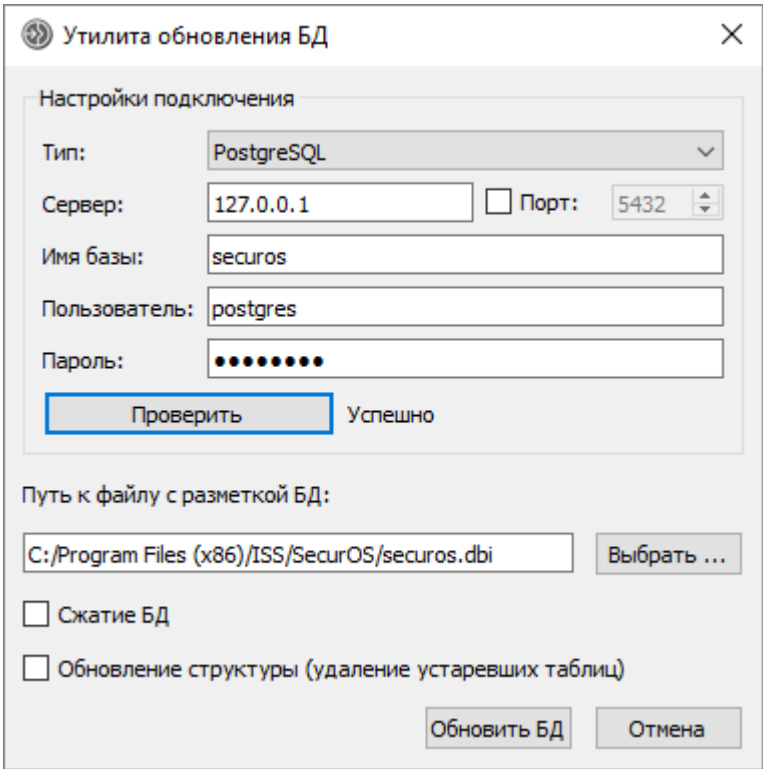


Рис. 314. Окно утилиты ISS Database Update

Таблица 121. Назначение полей утилиты Database Update Utility

Параметр	Описание
Блок Настройки подключения	
Тип	Тип базы данных. Обязательный параметр. Возможные значения: • PostgreSQL (значение по умолчанию). • SQL Server. • SQLite. Примечание. Значение SQLite используется при запуске Клиентского приложения SecurOS на отдельном Компьютере для автоматического создания и обновления локальной БД SecurOS, реализованной на этом Компьютере в виде файла .sqlite.
Сервер	Имя или IP-адрес сервера, на котором установлена БД. Обязательный параметр.
Порт	Номер порта для подключения. Необязательный параметр. Если флажок отмечен, соединение устанавливается по заданному порту. Если флажок не отмечен, соединение устанавливается по порту 5432 (значение по умолчанию).
Имя базы	Имя базы данных, заданное при ее установке. Обязательный параметр.
Пользователь	Имя учетной записи администратора БД, заданное при ее установке. Обязательный параметр.

Параметр	Описание
Пароль	Пароль учетной записи администратора БД, заданный при ее установке. Обязательный параметр.
Проверить (кнопка)	Нажмите кнопку, чтобы проверить соединение с БД по заданным параметрам. Если соединение устанавливается, справа от кнопки выводится результат <i>Успешно</i> . В противном случае выводится результат <i>Ошибка</i> . Проверьте заданные параметры и повторите тест соединения.
Путь к файлу с разметкой БД	Путь к файлу <code>securos.dbi</code>. По умолчанию принимает значения: • <корневой каталог SecurOS>\securos.dbi — для ОС семейства Windows. • <code>opt/iss/securos/securos.dbi</code> — для ОС семейства Linux. Допускается задавать путь вручную или с помощью кнопки Выбрать (см. ниже).
Выбрать (кнопка)	Нажмите кнопку для выбора папки, в которой располагается пользовательский файл <code>.dbi</code> . В стандартном окне файлового менеджера укажите путь к файлу.
Сжатие БД	Отметьте флажок для выполнения стандартной операции <code>VACUUM PostgreSQL</code> .
Обновление структуры БД (удаление устаревших таблиц)	Отметьте флажок для выполнения операции полного удаления устаревших таблиц БД.
Обновить БД (кнопка)	Нажмите кнопку для выполнения операции обновления БД в соответствии с заданными параметрами и завершения работы с утилитой.
Отмена	Нажмите кнопку для отказа от изменений и завершения работы с утилитой.

21.4.7 Утилита Редактор регистрационных файлов (DDI)

Утилита предназначена для описания типов объектов SecurOS — их свойств, характеристик и поведения в системе.

Дополнительная информация

Под типом объекта в SecurOS понимают уникальный символьный идентификатор класса объектов, используемый в программном коде продукта. Тип объекта SecurOS изменить нельзя.

Каждое свойство, характеристика или правило поведения типа объекта в SecurOS задается с помощью соответствующего компонента описания. Компоненты описания типа используются для представления объекта в соответствующих интерфейсах, например, в интерфейсе оператора на *Медиа Клиенте*, в *log-файле Протокола событий*, на *Карте* и т. д.

По умолчанию, описания существующих в SecurOS типов объектов создаются по правилам, определенным разработчиком системы. При добавлении новых типов, например, при интеграции SecurOS с системами или оборудованием сторонних производителей, с помощью утилиты можно создать собственное описание типа добавленного объекта.

Нахождение на диске:

- <корневой каталог SecurOS>\ddi.exe — для ОС семейства Windows.
- opt/iss/securos/ddi — для ОС семейства Linux.

Для начала работы с описанием типов необходимо загрузить соответствующий файл securos_XX.ddi, расположенный в корневом каталоге SecurOS, где XX — идентификатор языка описания, например, fr (французский).

Внешний вид главного окна утилиты после загрузки описания представлен на рис. 315.

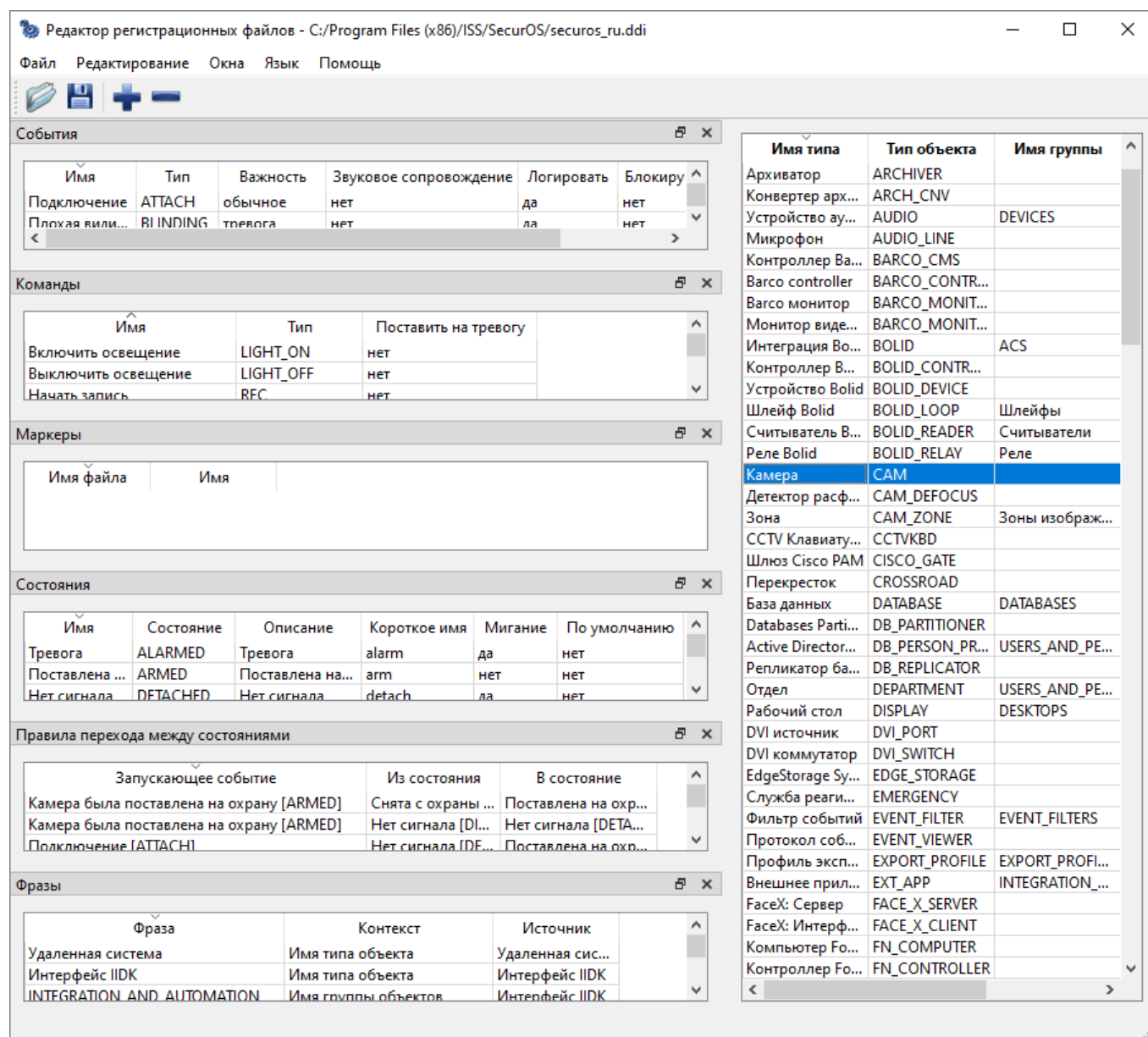


Рис. 315. Главное окно утилиты Редактор регистрационных файлов

В правой части окна выводится список зарегистрированных типов объектов, представленный в виде таблицы:

- **Имя типа** — символьное имя типа. Используется для представления объекта в *Дереве объектов*, на *Карте*, в *Медиа Клиенте*, в *Протоколе событий* и др. Изменяемый параметр.
- **Тип объекта** — уникальный тип объекта. Используется для представления экземпляра класса объектов. Изменяемый параметр.

Примечание. Тип объекта необходимо изменять только в случае его изменения в исходном коде продукта. В противном случае изменения не будут применены в системе, хотя и будут сохранены в файле описания.

- **Имя группы** — имя группирующего объекта в *Дереве объектов* SecurOS. Изменяемый параметр.

Для просмотра описания типа щелкните требуемый объект в списке.

В левой части окна в соответствующих окнах будет выведена следующая информация о типе объекта (по умолчанию выводится вся доступная информация):

- окно **События** — содержит таблицу системных событий, которые может генерировать выделенный тип объекта.
- окно **Команды** — содержит таблицу команд управления для выделенного типа объекта.
- окно **Маркеры** — содержит таблицу, используемую для определения имен файлов с пиктограммами объектов. Пиктограммы объектов, отображаемые в окне *Карта: Интерфейс оператора*, предопределяются в коде объекта. Соответствующие графические файлы формата .png расположены в папке skins_common корневого каталога SecurOS.
- окно **Состояния** — содержит таблицу всех возможных состояний для выделенного типа объекта.
- окно **Правила перехода между состояниями** — содержит таблицу правил перехода из одного состояния объекта в другое. Под правилами перехода подразумевается то, в какое и из какого состояния перейдет выбранный объект при возникновении того или иного события. В таблицу заносятся инициализирующее переход событие, исходное состояние и конечное состояние.
- окно **Фразы** — содержит имена для подписей к объектам, отображаемые во всех элементах интерфейса (в *Дереве объектов*, в окне *Карта: Интерфейс оператора*, в *Медиа Клиенте*, в *Протоколе событий* и др. Также содержит фразы сообщений, выводимых в собственных окнах объектов (например, в окне *Архиватора*).

Управление отображением перечисленных выше окон выполняется с помощью меню **Окна** в главном окне утилиты.

Для изменения значения поля окна дважды щелкните его мышью, далее выберите требуемый вариант из списка либо задайте новое значение вручную.

Остальные элементы **Строки меню** и **Панели инструментов** главного окна понятны интуитивно и в данном документе не рассматриваются.

Окно События

События					
Имя	Тип	Важность	Звуковое сопровождение	Логировать	Блокирующее
Подключение	ATTACH	обычное	нет	да	нет
Плохая видимость	BLINDING	тревога	нет	да	нет
Обрыв	DETACH	тревога	да	да	нет
Потеря фокусировки	DEFOCUSED	тревога	нет	да	нет

Рис. 316. Окно События

В окне задаются следующие параметры *Событий* для типа объекта:

- **Имя** — имя события в том виде, в котором оно будет отображаться в *Протоколе событий*.
- **Тип** — уникальный идентификатор события.

Примечание. Тип события необходимо изменять только в случае его изменения в исходном коде продукта. В противном случае изменения не будут применены в системе, хотя и будут сохранены в файле описания.

- **Важность** — значимость события. Определяет влияние события на систему и необходимость вмешательства оператора. Возможные значения:
 - **обычное** — событие, не требующее привлечения внимания оператора. В *Протоколе событий* выделяется синим цветом.
 - **информационное** — событие, требующее дополнительного внимания оператора. В *Протоколе событий* выделяется белым цветом.
 - **тревога** — событие, требующее вмешательства оператора или технического специалиста. В *Протоколе событий* выделяется красным цветом.
- **Звуковое сопровождение** — атрибут, указывающий на необходимость звукового сопровождения события. Имеет значение только в случае, если звуковое сопровождение определено в исходном коде объекта.
- **Логировать** — признак сохранения записи о событии в базе данных protocol (протокол системы). Возможные значения:
 - **да** — сообщение о локальном событии будет сохранено в БД.
 - **нет** — сообщение о локальном событии не будет сохранено в БД.
- **Блокирующее** — признак рассылки сообщения о локальном событии на все компьютеры сети. Возможные значения:
 - **да** — сообщение о локальном событии не будет передаваться в сеть.
 - **нет** — сообщение о локальном событии будет передаваться в сеть.

Окно Команды

Команды		
Имя	Тип	Поставить на тревогу
Снять с охраны	DISARM	да
Поставить на охрану	ARM	да
Остановка записи	REC_STOP	нет
Начать запись с откатом	REC_ROLLBACK	нет

Рис. 317. Окно Команды

В окне задаются следующие параметры *Команд* типа объекта:

- **Имя** — имя команды.
- **Тип** — уникальный идентификатор команды, предопределенный в коде объекта.
- **Поставить на тревогу** — в текущей версии утилиты не используется.

Окно Маркеры

Маркеры	
Имя файла	Имя
zone_window	Окно
zone_smoke	Дымовой
zone_smk	Геркон
zone_pir	Потолочный

Рис. 318. Окно Маркеры

В окне задаются следующие параметры *Пиктограмм* объектов, выводимых в окне *Карта: Интерфейс оператора*:

Внимание! Параметры пиктограмм имеют смысл только для объектов *Луч* и *Реле*.

- **Имя файла** — значение, используемое в скрипте для определения конечного имени файла графического изображения.
- **Имя** — возможное значение из списка значений соответствующего параметра объекта *Луч* или *Реле*.

Окно Состояния

Состояния					
Имя	Состояние	Описание	Короткое имя	Мигание	По умолчанию
Тревога	ALARMED	Тревога	alarm	да	нет
Поставлена на охрану	ARMED	Поставлена на охрану	arm	нет	нет
Нет сигнала	DETACHED	Нет сигнала	detach	да	нет
Снята с охраны	DISARMED	Снята с охраны	disarm	нет	нет

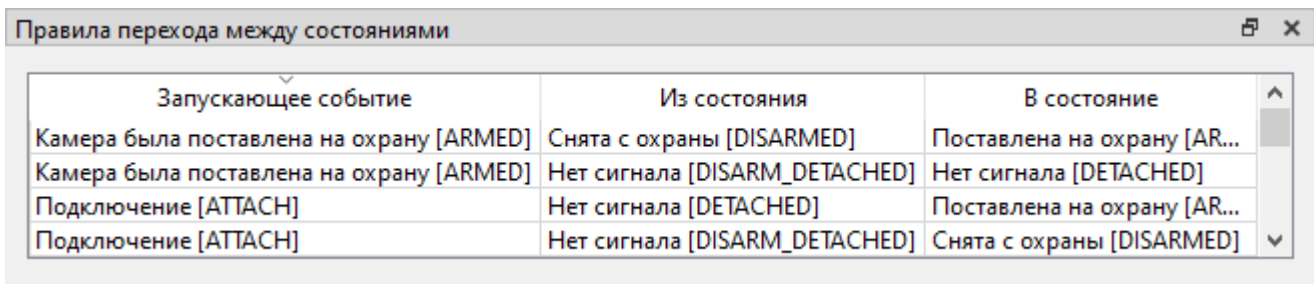
Рис. 319. Окно Состояния

В окне задаются следующие параметры *Состояний* типа объекта:

- **Имя** — строковое имя состояния. Выводится, например, в окне *Карта: Интерфейс оператора*.
- **Состояние** — уникальный идентификатор состояния.

- **Описание** — текстовое описание состояния.
- **Короткое имя** — значение, используемое в скрипте для формирования имени файла графического изображения, используемого для отображения в окне *Карта: Интерфейс оператора* для указанного состояния объекта.
- **Мигание** — дополнительная отметка состояния. Управляет миганием пиктограммы объекта в окне *Карта: Интерфейс оператора* при наступлении данного состояния. Возможные значения:
 - да — пиктограмма мигает.
 - нет — пиктограмма не мигает.

Окно Правила перехода между состояниями



Запускающее событие	Из состояния	В состояние
Камера была поставлена на охрану [ARMED]	Снята с охраны [DISARMED]	Поставлена на охрану [AR...
Камера была поставлена на охрану [ARMED]	Нет сигнала [DISARM_DETACHED]	Нет сигнала [DETACHED]
Подключение [ATTACH]	Нет сигнала [DETACHED]	Поставлена на охрану [AR...
Подключение [ATTACH]	Нет сигнала [DISARM_DETACHED]	Снята с охраны [DISARMED]

Рис. 320. Окно Правила перехода между состояниями

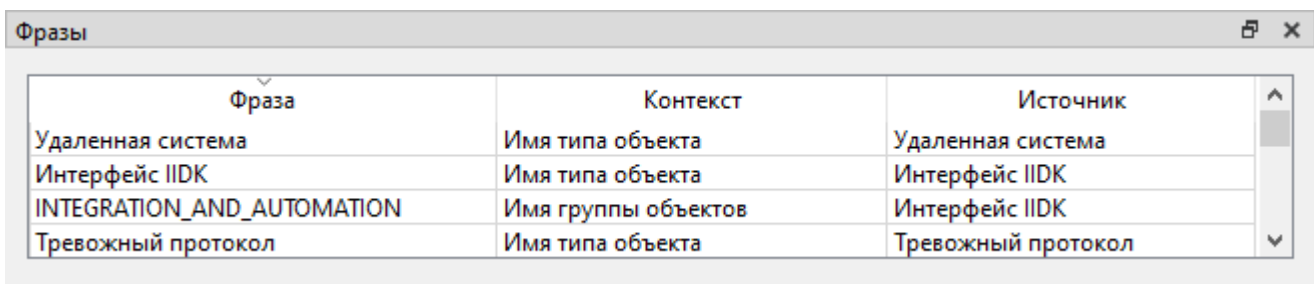
В окне задаются следующие параметры правил:

- **Запускающие событие** — идентификатор события, которое инициализирует переход.
- **Из состояния** — идентификатор состояния, из которого будет произведен переход при наступлении **Запускающего события**.

Внимание! Если поле оставить пустым, то переход будет осуществляться из любого состояния.

- **В состояние** — идентификатор конечного состояния объекта.

Окно Фразы



Фраза	Контекст	Источник
Удаленная система	Имя типа объекта	Удаленная система
Интерфейс IIDK	Имя типа объекта	Интерфейс IIDK
INTEGRATION_AND_AUTOMATION	Имя группы объектов	Интерфейс IIDK
Тревожный протокол	Имя типа объекта	Тревожный протокол

Рис. 321. Окно Фразы

В окне задаются *Фразы*, используемые для подписей к объектам и вывода сообщений в собственных окнах объектов. Содержит следующие поля:

- **Фраза** — фраза, используемая для описания объекта в основных интерфейсных элементах SecurOS (*Дерево объектов*, *Карта: Интерфейс оператора*, *Протокол событий* и пр.) или фраза сообщения в собственном окне объекта.
- **Контекст** — контекст использования фразы.
- **Источник** — источник фразы (т. е. **Тип объекта**).

Примечание. Изменение **Фразы** приводит к автоматическому изменению поля **Источник** и поля **Имя типа** в правом окне.

Внимание! После внесения изменений сохраните файл и перезапустите SecurOS, в противном случае изменения применены не будут.

21.4.8 Утилита Server Role Manager

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*.

Утилита предназначена для назначения роли *Сервер конфигураций* одному из *Периферийных серверов SecurOS* в случае невозможности дальнейшего использования текущего *Сервера конфигураций*.

- **Работа с утилитой в ОС Windows.**
- **Работа с утилитой в ОС Linux.**

Работа с утилитой в ОС Windows

Нахождение на диске:

<корневой каталог SecurOS>\ServerRoleManager.exe

Для смены текущего *Сервера конфигураций* выполните следующие действия:

Внимание! Перед выполнением операции переустановите ключ Guardant с текущего *Сервера конфигураций* на тот *Периферийный сервер*, который будет выполнять роль нового *Сервера конфигураций* (см. **Установка ключа Guardant**). В противном случае запуск системы на новом *Сервере конфигураций* будет невозможен.

1. Запустите утилиту на том из *Периферийных серверов* системы, который будет выполнять роль *Сервера конфигураций*.
2. В окне утилиты выберите опцию **Использовать данный Компьютер как Сервер конфигураций** (см. рис. 322).

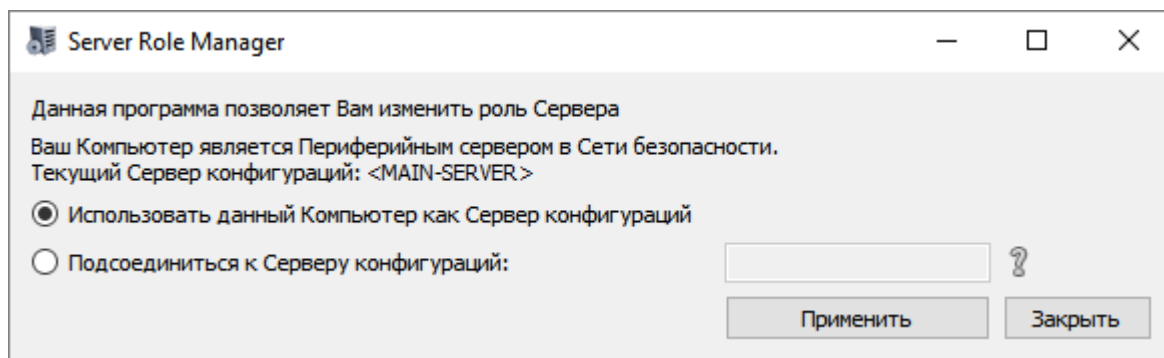


Рис. 322. Определение нового Сервера конфигураций

Примечание. В строке **Текущий Сервер конфигураций** выводится имя заменяемого компьютера.

3. Нажмите кнопку **Применить**.
4. Перезагрузите SecurOS.
5. Последовательно запустите утилиту на каждом из оставшихся *Периферийных серверов* системы и выполните следующие действия:
 - В окне утилиты выберите опцию **Подсоединиться к Серверу конфигураций** (см. рис. 323).

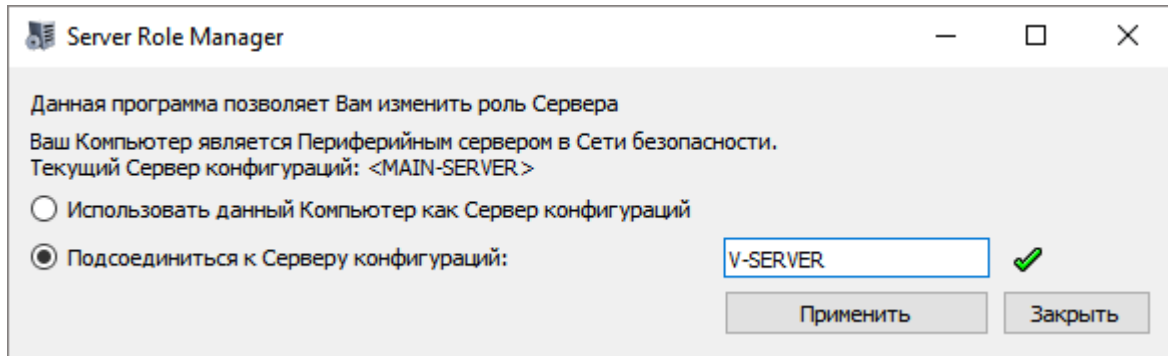


Рис. 323. Переподключение к новому Серверу конфигураций

Примечание. В строке **Текущий сервер конфигураций** выводится имя заменяемого компьютера.

- В текстовом поле задайте имя компьютера, которому была назначена роль *Сервер конфигураций*.

Примечание. Если имя нового *Сервера конфигураций* задано корректно и компьютер доступен в сети SecurOS, справа от поля ввода будет выведен символ . В противном случае — символ .

- Нажмите кнопку **Применить**.
- Перезагрузите SecurOS.

Работа с утилитой в ОС Linux

Нахождение на диске:

opt/iss/securos/ServerRoleManager

Внимание! Перед выполнением операции переустановите ключ Guardant с текущего *Сервера конфигураций* на тот *Периферийный сервер*, который будет выполнять роль нового *Сервера конфигураций* (см. [Установка ключа Guardant](#)). В противном случае запуск системы на новом *Сервере конфигураций* будет невозможен.

Для смены текущего *Сервера конфигураций* выполните следующие действия:

1. Запустите консольное приложение *Терминал*.
2. Перейдите в директорию установки SecurOS (по умолчанию opt/iss/securos) с помощью команды:

```
cd <директория_установки_SecurOS>
```

3. Включите использование компьютера как *Сервера конфигураций* с помощью команды:

```
./ServerRoleManager -r cs
```

4. Перезагрузите SecurOS на *Сервере конфигураций* с помощью команды:

```
sudo service vms_server restart
```

5. Последовательно запустите утилиту на каждом из оставшихся *Периферийных серверов* системы и выполните следующую команду:

```
./ServerRoleManager -r ps -h <адрес_сервера_конфигураций>
```

Чтобы утилита не проверяла адрес *Сервера конфигураций* добавьте в команду следующий параметр:

```
--disable-check-address
```

6. Перезагрузите SecurOS на каждом *Периферийном сервере* с помощью команды:

```
sudo service vms_server restart
```

Чтобы посмотреть текущий статус сервера используйте параметр `-p` или `--print`.

Чтобы посмотреть версию утилиты используйте параметр `-v` или `--version`.

Чтобы посмотреть справку используйте параметр `--help`.

21.4.9 Утилита Server Control Agent

С помощью утилиты можно выполнять следующие операции:

- Запускать/останавливать *Серверную часть* SecurOS;
- Получать дополнительную информацию при ошибках запуска *Серверной части* SecurOS;
- Запускать *Клиентскую часть* SecurOS;
- Управлять службой Video Management System Server;
- Запускать утилиту **SystemInfo**.

Нахождение на диске:

<корневой каталог SecurOS>\ServerControlAgent.exe

Утилита автоматически запускается при запуске ОС. После запуска значок утилиты отображается в системном трее (см. рис. 324).

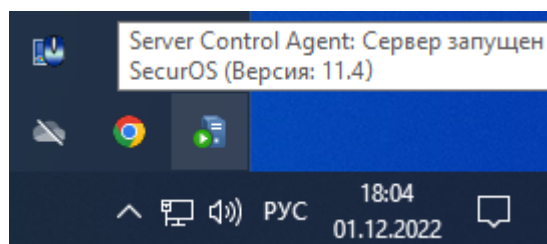


Рис. 324. Значок утилиты Server Control Agent в системном трее

Примечание. Если утилита была выгружена, запустить ее можно из меню **Пуск (Программы → SecurOS → Server Control Agent)**.

Текущее состояние сервера отображается на значке приложения:



— сервер запущен;



— сервер остановлен;



— сервер аварийно остановлен.

При наведении указателя мыши на значок выводится подсказка, в которой также отображается текущее состояние сервера, редакция и версия SecurOS.

Управление осуществляется с помощью контекстного меню утилиты (см. рис. 325), которое содержит следующие команды:

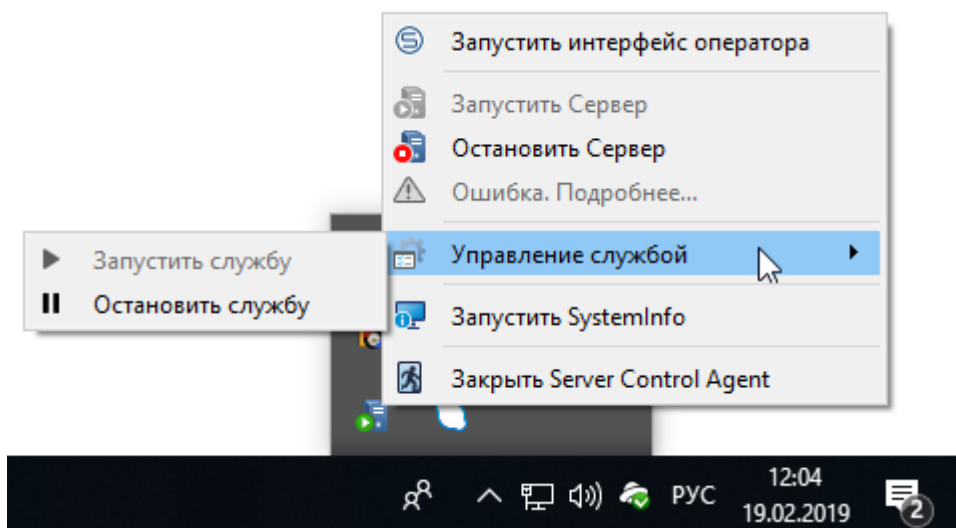


Рис. 325. Контекстное меню утилиты

- **Запустить интерфейс оператора** — запустить *Клиентскую часть* SecurOS на данном компьютере;
- **Запустить Сервер** — запустить *Серверную часть* SecurOS;
- **Остановить Сервер** — остановить *Серверную часть* SecurOS;
- **Ошибка. Подробнее...** — вывести подробную информацию об ошибке запуска *Серверной части*;
- **Управление службой** — изменить состояние службы ОС Video Management System Server:
 - Запустить службу;
 - Остановить службу.
- **Запустить SystemInfo** — запустить утилиту **SystemInfo**;
- **Закрыть Server Control Agent** — завершить работу утилиты.

21.4.10 Утилита восстановления индексов медиаархива

Утилита предназначена для восстановления поврежденных или создания отсутствующих файлов индексов видео- и/или аудиоархива SecurOS, в том числе архива с камер со связанным микрофоном.

Нахождение на диске:

- в ОС Windows — <корневой каталог SecurOS>\MediaIndexRepairer.exe;
- в ОС Linux — <корневой каталог SecurOS>/mediaindex_repairer (см. [Работа с утилитой в ОС Linux](#)).

Утилита реализована в виде консольного приложения, для вызова которого используется следующий синтаксис командной строки (ниже приведен пример для ОС Windows):

```
MediaIndexRepairer.exe [--path <arg>] [--camId <arg>] [--type <arg>]  
[--user <arg>] [--pass <arg>] или
```

MediaIndexRepairer.exe [--help], где:

- --path <arg> — пересоздание индексных файлов, содержащихся в указанной папке. Обязательный параметр. Возможные аргументы:
 - <Полный_путь_к_корневой_папке_архива> — пересоздание индексных файлов всего архива, или
 - <"Полный_путь_к_папке_архива_за_час"> — пересоздание индексного файла для архива, записанного за один час;

Внимание!

1. Имя папки в строке вызова является чувствительным к регистру.
2. При указании пути к папке, содержащей архив за час, использование экранирующих символов "\"" обязательно, т.к. в имени такой папки содержится пробел (см. пример ниже).
3. Допускается указание сетевой папки. При этом необходимо указать пользователя и пароль для доступа (см. ниже).

- --camID <arg> — пересоздание всех индексных файлов для архива, созданного камерой с указанным идентификатором. Необязательный параметр. Если не указан, будут пересозданы индексные файлы архивов, созданных всеми камерами.

Без параметра --path <arg> не используется;

- --type <arg> — тип файлов для восстановления индексов. Может принимать следующие значения:
 - all — перестроение индексов для видео- и аудиоархива, используется по умолчанию;
 - video — перестроение индексов только для видеоархива;
 - audio — перестроение индексов только для аудиоархива;
- --user <arg> — имя пользователя с указанием домена (если есть) для доступа к сетевой папке. Необязательный параметр;
- --pass <arg> — пароль пользователя для доступа к сетевой папке. Необязательный параметр;
- --help — вывод на консоль справочной информации.

Работа с утилитой в ОС Linux

При работе с утилитой в ОС Linux:

- запуск утилиты следует осуществлять от имени пользователя `securos`. Например, так:

```
cd /opt/iss/securos  
sudo -u securos ./mediaindex_repairer --path /mnt/disk1/ISS_MEDIA
```

- при указании путей к папкам должны использоваться только прямые слэши `"/`;
- сетевые папки не могут быть использованы. Т.е. использование параметров `--user <arg>` и `--pass <arg>` не имеет смысла.

Примеры использования:

- `MediaIndexRepairer.exe --path D:\ISS_MEDIA` — пересоздание всех индексных файлов видео и аудиоархива, созданных всеми камерами и сохраненных в папке `D:\ISS_MEDIA`;
- `MediaIndexRepairer.exe --path "D:\ISS_MEDIA\CAM_15\2022-07-01T20+0300" --camId 15 --type video` — пересоздание индексного файла только видеоархива, созданного 1 июля 2022 года в интервале от 20:00 до 21:00 часов камерой с идентификатором 15 и сохраненного в папке `D:\ISS_MEDIA\CAM_15\2022-07-01T20+0300`;
- `MediaIndexRepairer.exe --path \\server\ISS_MEDIA --type audio --user OFFICE\admin --pass password` — пересоздание всех индексных файлов только аудиоархива, созданного всеми камерами и сохраненного в сетевой папке `\\server\ISS_MEDIA`.

Для одновременной обработки архива с различными параметрами используйте несколько экземпляров приложения. При этом архивы, заданные в параметрах каждого экземпляра приложения, не должны пересекаться по дате/времени и/или идентификатору камеры.

Внимание!

1. Переиндексация архивов больших объемов может занимать значительное время (часы).
2. После пересоздания индексных файлов для работы с соответствующими архивами необходимо перезапустить SecurOS.

21.4.11 Утилита обновления аудиофайлов устаревшего формата

В ОС Linux функциональность не поддерживается.

Утилита предназначена для:

- конвертации аудиоархива SecurOS старого формата в новый для связанных с камерами микрофонов;
- автоматического удаления старого аудиоархива SecurOS и создания файла индексов после конвертации.

Внимание!

1. Конвертация аудиоархивов больших объемов может занимать значительное время (часы).
2. Для работы с новым аудиоархивом необходимо перезапустить SecurOS.

Нахождение на диске:

<корневой каталог SecurOS>\AudioArchiveConverter.exe

Утилита реализована в виде консольного приложения, для вызова которого используется следующий синтаксис командной строки:

AudioArchiveConverter.exe [--path <arg>] [--user <arg>] [--pass <arg>] или
AudioArchiveConverter.exe [--help], где:

- --path <arg> — конвертация аудиоархива, содержащегося по указанному пути. Обязательный параметр. Возможные аргументы:
 - <Полный_путь_к_корневой_папке_архива> — конвертация всех старых аудиофайлов архива или
 - <Полный_путь_к_папке_архива_за_час> — конвертация старых аудиофайлов, записанных за один час, или
 - <Полный_путь_к_аудиофайлу> — конвертация только указанного аудиофайла.

Внимание!

1. Имя папки в строке вызова является чувствительным к регистру.
2. При указании пути к папке, содержащей архив за час, использование экранирующих символов "\"" обязательно, т.к. в имени такой папки содержится пробел (см. пример ниже).
3. Допускается указание сетевой папки. При этом необходимо указать пользователя и пароль для доступа (см. ниже).

- --user <arg> — имя пользователя с указанием домена (если есть) для доступа к сетевой папке. Необязательный параметр;
- --pass <arg> — пароль пользователя для доступа к сетевой папке. Необязательный параметр;
- --help — вывод на консоль справочной информации.

Примеры использования:

- AudioArchiveConverter.exe --path D:\VIDEO — конвертация всех аудиофайлов архива, созданного всеми камерами и сохраненного в папке D:\VIDEO;
- AudioArchiveConverter.exe --path \\server\VIDEO --user OFFICE\admin --pass password — конвертация всех аудиофайлов архива, созданного всеми камерами и сохраненного в сетевой папке \\server\VIDEO;
- AudioArchiveConverter.exe --path "D:\VIDEO\12-03-19 12" — конвертация всех аудиофайлов архива, созданного 12 марта 2019 года в интервале от 12:00 до 13:00 часов всеми камерами, сохраненного в папке D:\VIDEO\12-03-19 12;
- AudioArchiveConverter.exe --path "D:\VIDEO\12-03-19 12\4009641.w05" — конвертация аудиоархива, созданного 12 марта 2019 года в 12:40:09.641 камерой с идентификатором 5, сохраненного в папке D:\VIDEO\12-03-19 12;

Для одновременной обработки аудиоархива с различными параметрами используйте несколько экземпляров приложения. При этом аудиофайлы, заданные в параметрах каждого экземпляра приложения, не должны пересекаться по дате и времени.

Результаты конвертации:

- При конвертации папки все старые аудиофайлы будут удалены. Вместо них будут созданы аудиофайлы нового формата, а так же сгенерируется файл индексов.

- При конвертации отдельного файла, будет сгенерирован аудиофайл нового формата. Исходный старый аудиофайл не будет удален. Файл индекса для нового аудиоархива строиться не будет.

21.4.12 Утилита Certificate Generator

В ОС **Linux** функциональность не поддерживается.

Утилита предназначена для создания пробных самоподписанных SSL-сертификатов. Такие сертификаты могут быть использованы для проверки и демонстрации возможностей цифровой подписи (см. [Цифровая подпись](#)) и работы по защищенному протоколу HTTPS таких модулей как *Сервер мобильного приложения* (см. [Краткое руководство SecurOS Mobile](#)), *Сервер AutoMobile* (см. [Руководство пользователя SecurOS AutoMobile](#)), *Rest API* и т.п.

Внимание! Сертификаты, созданные с помощью утилиты, предназначены исключительно для демонстрационных и пусконаладочных целей.

Нахождение на диске:

<корневой каталог SecurOS>\CertificateGenerator.exe

Внешний вид окна утилиты представлен на рис. [326](#).

Внимание! Сертификат, созданный с помощью Certificate Generator, является самоподписанным и предназначен для демонстрационных и пусконаладочных целей.

Выдан: DEMO

Организация: DEMO

Название сертификата: Demo Certificate

Дополнительное имя субъекта: localhost
127.0.0.1

Добавить Удалить

Срок действия: 15.09.2021 13:29:38 - 15.09.2026 13:29:38

Назначение сертификата

☒ Цифровая подпись
☐ HTTPS

☒ Установить в хранилище локального компьютера
☒ Экспортируемый приватный ключ
☒ Сохранить в директорию

C:\ProgramData\ISS\CertificateGenerator\ ...

Сохранить в формате: PFX

☐ Показать лог

Создать сертификат

Рис. 326. Окно утилиты Certificate Generator

Для создания сертификата выполните следующие действия:

1. Заполните поля:

- **Выдан:** значение будет отображаться в свойствах сертификата **Кем выдан** и **Кому выдан**;
- **Организация:** значение будет отображаться в свойстве сертификата **Организация**;
- **Название сертификата:** значение будет отображаться в качестве названия сертификата;
- **Дополнительное имя субъекта:** введите IP-адреса или DNS-имена субъектов, на которые также будет распространяться действие данного сертификата. Субъекты могут быть добавлены или удалены с помощью кнопок **Добавить/Удалить**.

Примечание. Дополнительные имена субъектов следует добавлять только в том случае, если компьютер, на котором сохраняется сертификат, имеет несколько сетевых интерфейсов.

- **Срок действия:** срок действия сертификата.
2. Выберите назначение сертификата:
- **Цифровая подпись:** сертификат будет использован для цифровой подписи.

- **HTTPS:** сертификат будет использован для обеспечения безопасного соединения. Опция доступна только при запуске утилиты с правами администратора.
3. Выберите место установки или сохранения сертификата и его формат:
- Чтобы сделать сертификат доверенным на данном компьютере, отметьте флажок **Установить в хранилище локального компьютера** (значение по умолчанию).
 - Для корректной работы с websocket в ОС Windows отметьте флажок **Экспортируемый приватный ключ**.

Примечания:

1. Флажок доступен только при запуске утилиты с правами администратора.
 2. При установке флажка автоматически устанавливается флажок **Установить в хранилище локального компьютера**.
-

Внимание! При работе с ГИС-картами по протоколу HTTPS флажок должен быть установлен.

- Для сохранения сертификата в заданную директорию отметьте флажок **Сохранить в директорию**. Чтобы задать путь введите значение вручную или используйте файловый менеджер. При этом созданный сертификат также будет установлен и в хранилище локального компьютера. Сохранение сертификата в отдельную папку позволяет в дальнейшем установить и использовать данный сертификат на различных компьютерах сети SecurOS. Например, для обеспечения работы указанных выше модулей в случае использования SecurOS в конфигурации с кластером такой сертификат необходимо установить на каждом компьютере, входящем в кластер.

Примечание. При установке флажка **Сохранить в директорию** автоматически устанавливаются флажки **Установить в хранилище локального компьютера** и **Экспортируемый приватный ключ**.

- В поле **Сохранить в формате** выберите из списка формат сохраняемого сертификата. Возможные значения:
 - PFX — сертификат будет сохранен в файле формата PFX с расширением .pfx. Является значением по умолчанию.
 - PEM — сертификат будет сохранен в файле формата PEM с расширением .pem.

Внимание! Опции выбора места установки или сохранения сертификата доступны только при запуске утилиты с правами администратора.

4. Отметьте флажок **Показать лог**, чтобы увидеть детальную информацию о процессе создания сертификата.
5. Нажмите кнопку **Создать сертификат**, что создать сертификат с заданными параметрами.

21.4.13 Утилита AuditClient

Функциональность доступна в редакциях *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

Утилита предназначена для получения данных аудита действий пользователя SecurOS. Такие данные хранятся в специальных базах данных аудита, которые располагаются на каждом *Видеосервере* SecurOS и дополняют друг друга. При выполнении запроса происходит обращение к базе данных только того *Видеосервера*, с которым в данный момент установлено соединение. Получить данные аудита с нескольких *Видеосерверов* можно при последовательном подключении к каждому из них. Если настроить запись данных аудита в единую для всех *Видеосерверов* сети базу данных с помощью утилиты dsAdmin (см. [Утилита настройки подключений к БД \(DSAdmin\)](#)), агрегированные данные аудита можно получить в рамках одной сессии утилиты.

Внимание! При настройках по умолчанию данные аудита в базу данных не записываются. Для записи данных аудита в базу отметьте флажок **Записывать данные аудита системы** в настройках объекта **Система**.

Данные аудита собираются в соответствии с параметрами запроса, которые задаются пользователем в настройках утилиты. Возможно выполнение запросов как со стандартными, так и с пользовательскими параметрами. В последнем случае запрос может быть сохранен как шаблон для дальнейшего использования.

Нахождение на диске:

- <корневой каталог SecurOS>\audit_client.exe — для ОС семейства Windows.
- opt/iss/securos/audit_client — для ОС семейства Linux.

Для подключения к серверу аудита при запуске утилиты необходимо авторизоваться в SecurOS (см. рис. 327).

Внимание! Авторизоваться и подключиться к серверу аудита может только тот *Пользователь* SecurOS, для которого в *Правах пользователя* отмечен флаг **Разрешить выполнять аудит системы** (см. [Права пользователя](#)). В противном случае подключение к серверу аудита невозможно.

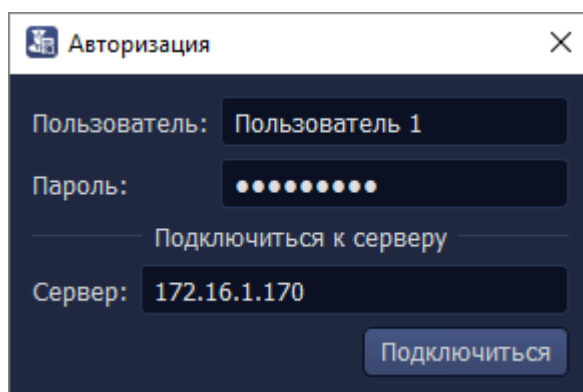


Рис. 327. Утилита AuditClient. Окно Авторизация

Окно содержит следующие поля:

- **Пользователь/Пароль** — имя и пароль *Пользователя* SecurOS или пользователя ОС (см. [Active Directory / LDAP](#)), которому разрешено проведение аудита.

- **Сервер** — IP-адрес или DNS-имя *Видеосервера* SecurOS на котором расположена база данных аудита. При локальном подключении допускается использовать значение 127.0.0.1 или localhost.

В случае успешной авторизации и подключения к серверу аудита станет доступным главное окно утилиты (см. рис. 328).

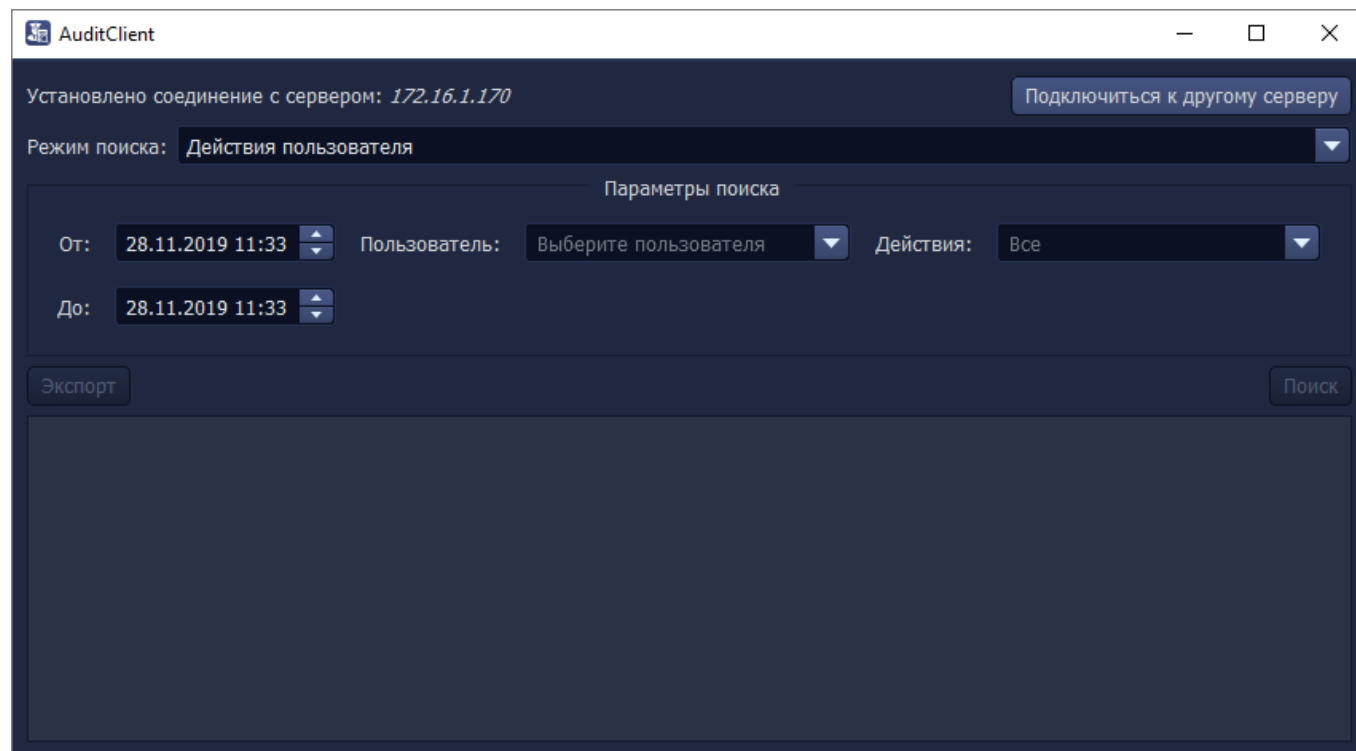


Рис. 328. Главное окно утилиты AuditClient

В верхней части окна находится **Форма задания параметров поиска**, содержащая следующие элементы:

- **Установлено соединение с сервером** — информационное поле, в котором отображается IP-адрес или DNS-имя сервера аудита, с которым установлено соединение.
- **Подключиться к другому серверу** (кнопка) — нажмите кнопку для подключения к другому серверу аудита.
- **Режим поиска** — выберите режим поиска:
 - **Действия пользователя** — используется для запроса всех действий пользователя при работе с системой, для которых предусмотрено проведение аудита.
 - **Изменения в конфигурации и режимах работы объекта** — используется для запроса действий пользователя, связанных с изменением настроек объекта, изменением режима работы объекта и режима записи архива.
 - **Доступ к видео** — используется для запроса действий пользователя, связанных с просмотром живого или архивного видео.
 - **Управление PTZ** — используется для запроса действий пользователя, связанных с управлением PTZ.
 - **Экспорт видео** — используется для запроса действий пользователя, связанных с экспортом видео.
 - **Работа с Модулем Auto** — используется для запроса действий пользователя, выполненных при работе с модулем SecurOS Auto.

- **Расширенный поиск** — используется для формирования сложных запросов, если ни один из описанных выше режимов запроса не подходит для получения требуемых данных.
- **Поиск по шаблону** — режим доступен в случае, если в системе сохранен хотя бы один шаблон поиска. При этом в списке режимов выводится имя сохраненного шаблона. Подробнее см. [Работа с шаблонами поиска](#).
- **Параметры поиска** (блок параметров, зависящих от выбранного режима поиска):
 - **От** — дата и время начала периода поиска, в формате даты и времени ОС.
 - **До** — дата и время окончания периода поиска, в формате даты и времени ОС.
 - **Пользователь** — выберите *Пользователя* SecurOS, действия которого в системе необходимо проанализировать. Список содержит только тех пользователей, действия которых зарегистрированы в базе данных аудита на момент подключения к серверу аудита.
 - **Действия** — выберите действия пользователя, которые необходимо проанализировать.
 - **Тип объекта** — выберите тип объекта, над которым были совершены действия.
 - **ID** — идентификатор объекта выбранного типа.
 - **ID камеры** — идентификатор *Камеры*.
 - **Гос. номер** — госномер автомобиля, с которым совершались какие-либо операции при работе с модулем SecurOS Auto.
 - **Пользователи** — выберите пользователей, действия которых необходимо проанализировать.
 - **Типы объектов** — выберите типы объектов, над которыми были совершены действия.
 - **Продвинутый** — отметьте флажок для задания параметров поиска вручную. Подробнее про создание пользовательских запросов см. подраздел [Продвинутый поиск](#).
- **Экспорт** (кнопка) — нажмите кнопку для экспорта результатов поиска. Подробнее см. ниже подраздел [Экспорт результатов](#).
- **Поиск** (кнопка) — нажмите кнопку, чтобы выполнить поиск с заданными параметрами.
- **Кнопки** (доступны только в режиме поиска *Расширенный* или при работе с ранее созданными шаблонами поиска, подробнее см. подраздел [Работа с шаблонами поиска](#)):
 - **Удалить шаблон** — удалить текущий шаблон из списка режимов поиска.
 - **Сохранить как шаблон** — сохранить текущие параметры поиска как шаблон для дальнейшего использования.

В нижней части окна находится таблица результатов поиска (см. рис. 329). Структура таблицы результатов также зависит от выбранного режима поиска.

Внимание! Данные таблицы результатов динамически не обновляются. Т.е. выводятся только те данные аудита, которые соответствуют заданному временному интервалу запроса, даже если в системе регистрируются новые. Для обновления данных необходимо выполнить запрос с учетом изменившегося временного интервала.

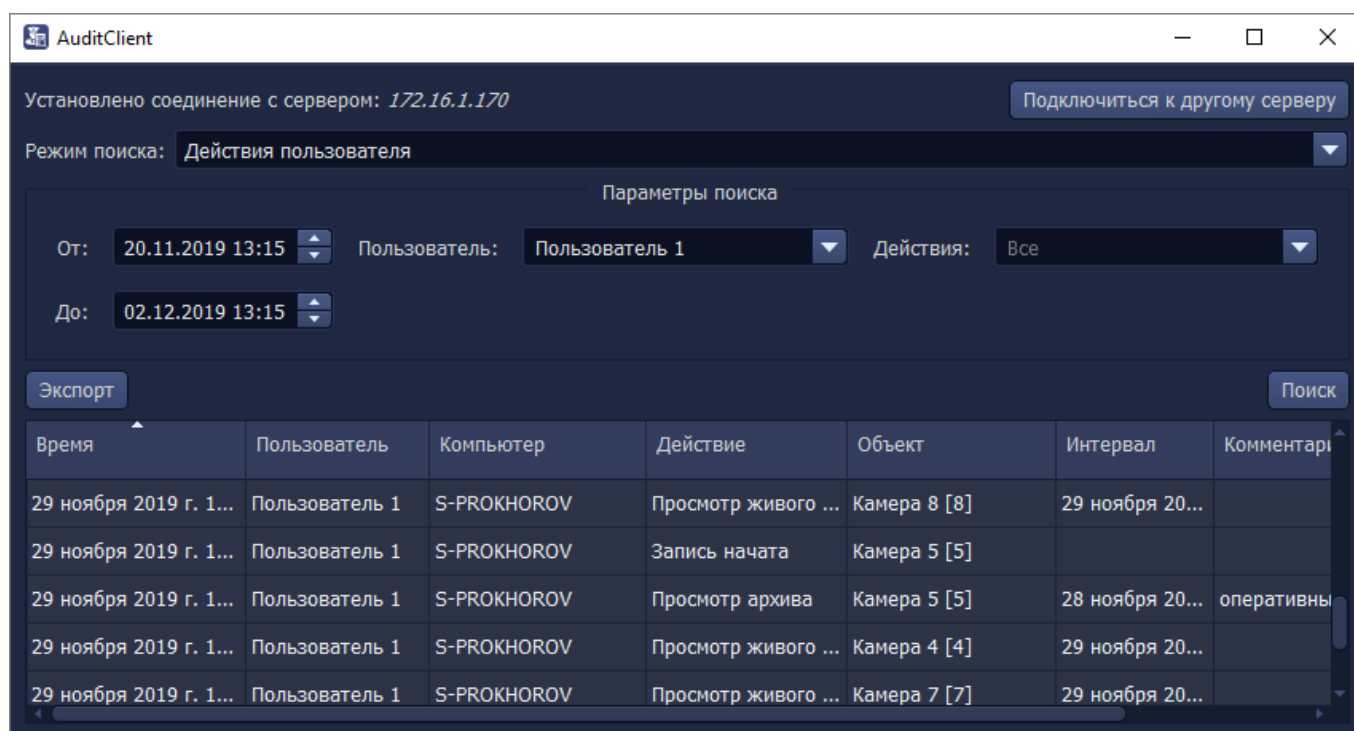


Рис. 329. Таблица результатов поиска

В зависимости от выбранного **Режима поиска** таблица результатов может содержать следующие столбцы:

- **Время** — время совершения действия, в формате даты и времени ОС, включая миллисекунды.
- **Пользователь** — имя пользователя SecurOS, который совершил действие.
- **Компьютер** — название *Компьютера* в сети SecurOS, на котором совершено действие.
- **Действие** — совершенное действие.
- **Объект** — объект, с которым совершалось действие, в формате <Название_объекта> <ID_объекта>.
- **Интервал** — интервал, соответствующий заданному **Периоду аудита** (см. **Система**), в формате даты и времени ОС, включая миллисекунды. Используется при фиксации длительных событий (просмотр живого/архивного видео, управление PTZ). Подробнее про интервал см. раздел **Примеры анализа действий пользователя**.
- **Название** — название и идентификатор *Тура*, *Препоозиции* или название *Контрольного списка*, которые были изменены пользователем.
- **Гос. номер** — текущее значение госномера автомобиля, с которым совершались какие-либо действия при работе с модулем SecurOS Auto или значение поисковой строки.
- **Устаревшее значение номера** — прежнее значение госномера автомобиля, с которым совершались какие-либо действия при работе с модулем SecurOS Auto.
- **Комментарий** — комментарий, создаваемый автоматически системой для некоторых событий.

Продвинутый поиск

Если отмечен флажок **Продвинутый**, пользователь может создать свой собственный шаблон поиска (фильтр) любого уровня сложности, не предусмотренный ни одним из заданных стандартных режимов поиска. Этот запрос также можно сохранить для дальнейшего использования (см. ниже). В качестве параметров запроса можно использовать следующие сущности:

1. `events.id` — идентификатор события в базе данных аудита.
2. `events.server_host` — имя *Компьютера*, на котором работает сервер аудита.
3. `events.server_node` — имя *Ноды*, на которой работает сервер аудита (при работе в кластере). При работе вне кластера совпадает со значением `events.server_host`.
4. `events.event_time` — время события, в формате ГГГГ-ММ-ДД ЧЧ:ММ:СС.XXX.
5. `events.event_action` — идентификатор выполненного действия.
6. `events.user_domain` — домен, в котором зарегистрирован *Пользователь*, чьи действия необходимо проанализировать.
7. `events.user_host` — имя *Компьютера*, на котором пользователем были выполнены действия.
8. `events.user_name` — имя *Пользователя*, чьи действия необходимо проанализировать.
9. `events.comment` — комментарий системы к событию.
10. `intervals.event_id` — идентификатор события.
11. `intervals.time_from` — начало интервала (для длительных событий), в формате ГГГГ-ММ-ДД ЧЧ:ММ:СС.XXX.
12. `intervals.time_to` — конец интервала (для длительных событий), в формате ГГГГ-ММ-ДД ЧЧ:ММ:СС.XXX.
13. `objects.event_id` — идентификатор события.
14. `objects.obj_type` — тип объекта, над которым были выполнены действия.
15. `objects.obj_id` — идентификатор объекта, над которым были выполнены действия.
16. `objects.obj_name` — название объекта, над которым были выполнены действия.
17. `params.param_type` — тип параметра, над которым были выполнены действия (при настройке PTZ или работе с SecurOS Auto).
18. `params.param_value` — значение параметра (при настройке PTZ или при работе с SecurOS Auto).

При создании запроса допускается использовать регулярные выражения и следующие ключевые слова и операторы:

Таблица 122. Ключевые слова и Операторы

Ключевое слово/Оператор	Описание
(,)	Скобки. Максимальная вложенность — 10.
" "	Кавычки. Строки и регулярные выражения должны быть в кавычках.
and, &	Логическое И.
or,	Логическое ИЛИ.
match	Проверка совпадения с заданным регулярным выражением.
nomatch	Проверка отсутствия совпадения с заданным регулярным выражением.
==	Проверка на равенство.

!=	Проверка на неравенство.
>, <, >=, <=	Операторы сравнения.

Ниже приведены примеры пользовательских запросов.

- `events.comment != NULL and objects.obj_type MATCH "CAM"` — запрос всех операций со всеми объектами *Камера* с непустым столбцом **Комментарий**.
- `events.comment MATCH "операт." AND objects.obj_type MATCH "CAM" AND objects.obj_id MATCH "^(8)$"` — запрос всех операций доступа к *Оперативному архиву Камеры 8*.
- `events.user_name MATCH "^(Пользователь 2)$" AND objects.obj_type MATCH "CAM" AND objects.obj_id MATCH "^(1|4|7|.7)$"` — запрос операций пользователя с именем *Пользователь 2* с объектами *Камера*, идентификаторы которых равны 1, 4 и 7 или заканчивается на 7.
- `events.comment MATCH "операт." AND intervals.time_from >= "2019-12-03 09:00" AND intervals.time_to < "2019-12-03 09:30" AND events.event_time > "2019-12-07 14:00" AND events.event_time <= "2019-12-07 14:45"` — запрос действий с фрагментом архива в интервале 2019-12-03 09:00 - 2019-12-03 09:30, которые были выполнены пользователем за период с 2019-12-07 14:00 по 2019-12-07 14:45.

Работа с шаблонами поиска

В режиме **Расширенный поиск** любой заданный в полях формы набор параметров может быть сохранен как шаблон для дальнейшего использования. Запрос, заданный в поле **Продвинутый**, также может быть сохранен как шаблон.

Для сохранения заполните требуемые поля формы, нажмите кнопку **Сохранить шаблон**. В окне **Создание шаблона** (см. рис. 330) задайте имя шаблона и нажмите кнопку **ОК**.

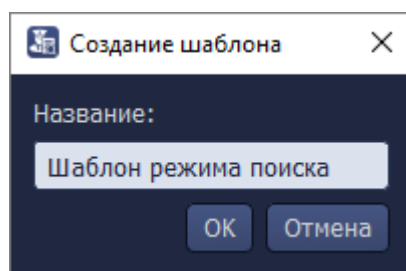


Рис. 330. Окно Создание шаблона

Шаблон поиска будет сохранен в списке **Режим поиска**. Чтобы использовать сохраненный шаблон выберите его в списке и нажмите кнопку **Поиск**.

Экспорт результатов

Экспорт данных аудита осуществляется в файл формата .CSV в директорию, указанную пользователем. Для экспорта данных нажмите кнопку **Экспорт**, в окне **Создать отчет** (см. рис. 331) задайте директорию для сохранения файла и имя файла, нажмите кнопку **Создать отчет**.

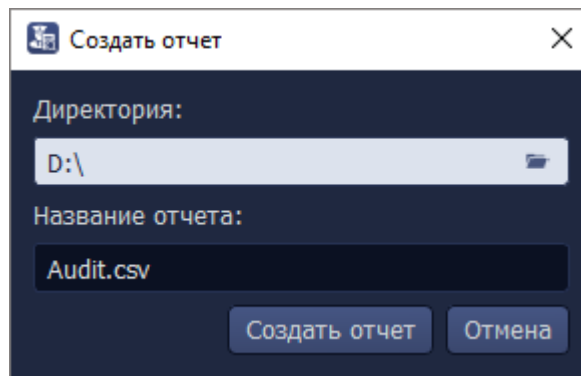


Рис. 331. Окно Создать отчет

Внимание! В качестве разделителя полей данных в созданном .csv-файле используется символ ";" (точка с запятой).

21.4.13.1 Настройка таблицы результатов

Вид *Таблицы результатов* может быть настроен в соответствии с предпочтениями каждого оператора. В окне можно настроить следующие элементы:

- Количество отображаемых столбцов таблицы;
- Порядок столбцов таблицы;
- Ширина столбцов таблицы.

Для **изменения количества отображаемых столбцов** щелкните заголовок таблицы правой кнопкой, в списке столбцов снимите флажки щелчком мыши с тех столбцов, которые не следует отображать в таблице (см. рис. 332). Для отображения скрытых столбцов щелкните мышью столбцы со снятыми флажками.

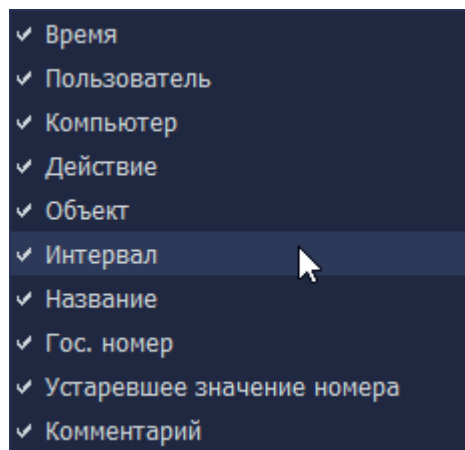
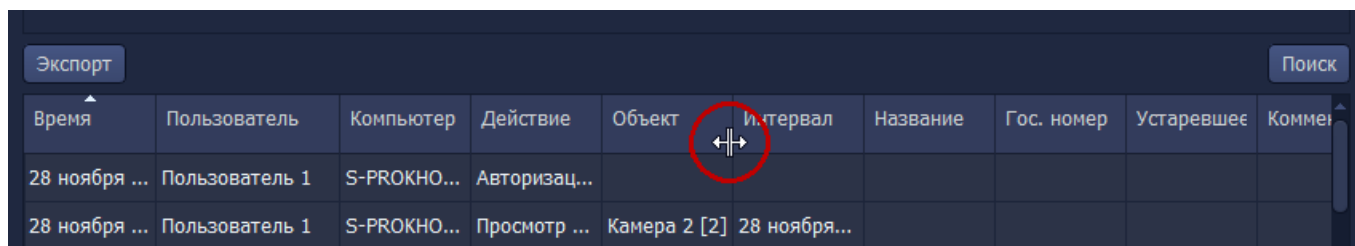


Рис. 332. Отображение/скрытие столбцов таблицы

Для **изменения порядка расположения столбцов таблицы** щелкните требуемый столбец мышью, и, удерживая кнопку мыши нажатой, перетащите столбец в требуемое положение.

Для **изменения ширины столбцов таблицы** наведите указатель мыши на разделитель столбцов. Указатель примет форму, указанную на рис. 333.



Время	Пользователь	Компьютер	Действие	Объект	Интервал	Название	Гос. номер	Устаревшее	Коммент
28 ноября ...	Пользователь 1	S-PROKHO...	Авторизац...						
28 ноября ...	Пользователь 1	S-PROKHO...	Просмотр ...	Камера 2 [2]	28 ноября...				

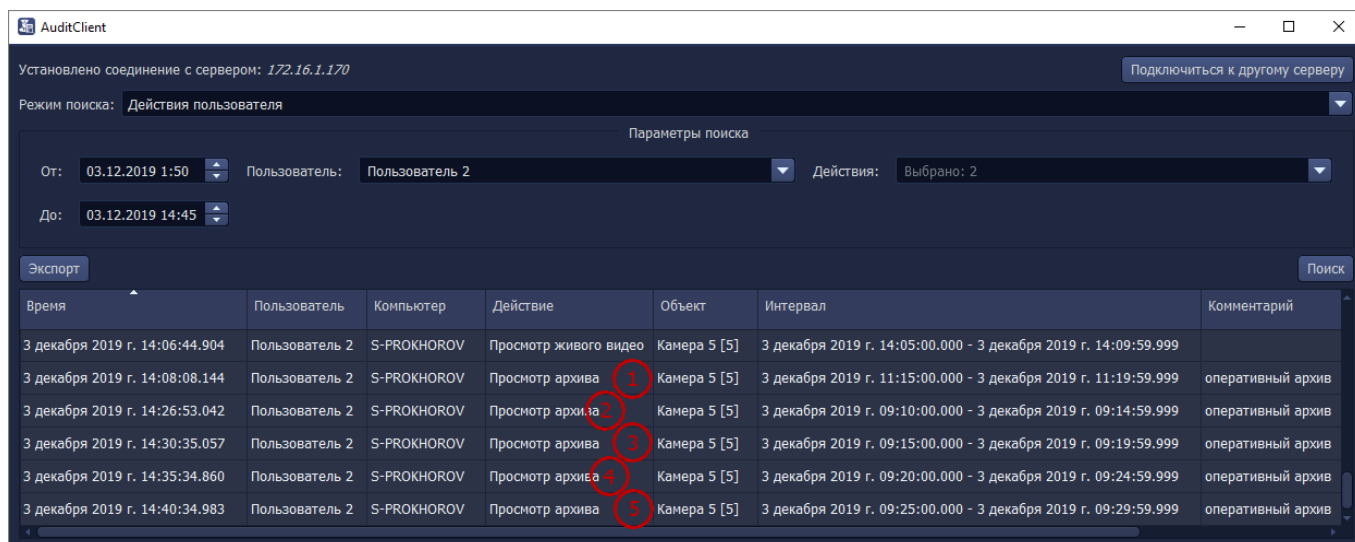
Рис. 333. Изменение ширины колонки таблицы

Нажмите кнопку мыши, и, удерживая кнопку нажатой, переметите указатель мыши в требуемом направлении.

21.4.13.2 Пример анализа действий пользователя

Пример анализа действий пользователя приведен на основе данных о просмотре архива. Анализ операций при просмотре живого видео и управлении PTZ проводится аналогично.

Данные запроса действий пользователя при работе с архивным видео приведены на рис. 334. Установленное значение **Периода аудита** (см. Система) равно 5 минут.



Время	Пользователь	Компьютер	Действие	Объект	Интервал	Комментарий
3 декабря 2019 г. 14:06:44.904	Пользователь 2	S-PROKHOROV	Просмотр живого видео	Камера 5 [5]	3 декабря 2019 г. 14:05:00.000 - 3 декабря 2019 г. 14:09:59.999	
3 декабря 2019 г. 14:08:08.144	Пользователь 2	S-PROKHOROV	Просмотр архива	Камера 5 [5]	3 декабря 2019 г. 11:15:00.000 - 3 декабря 2019 г. 11:19:59.999	оперативный архив
3 декабря 2019 г. 14:26:53.042	Пользователь 2	S-PROKHOROV	Просмотр архива	Камера 5 [5]	3 декабря 2019 г. 09:10:00.000 - 3 декабря 2019 г. 09:14:59.999	оперативный архив
3 декабря 2019 г. 14:30:35.057	Пользователь 2	S-PROKHOROV	Просмотр архива	Камера 5 [5]	3 декабря 2019 г. 09:15:00.000 - 3 декабря 2019 г. 09:19:59.999	оперативный архив
3 декабря 2019 г. 14:35:34.860	Пользователь 2	S-PROKHOROV	Просмотр архива	Камера 5 [5]	3 декабря 2019 г. 09:20:00.000 - 3 декабря 2019 г. 09:24:59.999	оперативный архив
3 декабря 2019 г. 14:40:34.983	Пользователь 2	S-PROKHOROV	Просмотр архива	Камера 5 [5]	3 декабря 2019 г. 09:25:00.000 - 3 декабря 2019 г. 09:29:59.999	оперативный архив

Рис. 334. Аудит действий пользователя при просмотре архивного видео

В рассматриваемом примере *Пользователь 2* выполнил в SecurOS следующие действия:

- В 14:08:08 переключил *Камеру 5* в режим просмотра архива.
- С 14:08:08 до 14:41:12 выполнял некоторые операции с архивом.
- В 14:41:12 переключился в режим просмотра живого видео.

В *Таблице результатов* аудита этим действиям соответствуют следующие записи (в порядке перечисления):

1. В 14:08:08.144 переключил камеру в режим просмотра *Оперативного архива* (тип просматриваемого архива указывается в столбце **Комментарий**). При переключении в режим архива указатель архива был установлен на последний кадр архива. В используемом для примера архиве последний кадр архива соответствует временной отметке 11:18:32. При заданном **Периоде аудита** (5 минут) это положение указателя соответствует **Интервалу** 11:15:00.000 - 11:19:59.999, что и отражено в таблице. После этого, в течение 18 минут, с 14:08:08.144 до 14:26:53.042, пользователь не получал доступа к другому фрагменту архива. Более детально действия пользователя не анализируются (например, он мог

просматривать фрагменты непрерывно или покадрово в пределах текущего **Интервала**, соответствующего **Периоду аудита**).

2. В 14:26:53.042 пользователь установил указатель архива на отметку 09:11:17, которая находится вне предыдущего **Периода аудита** и соответствует **Интервалу** 09:10:00.000 – 09:14:59.999 (по времени архива), и начал просмотр архива.
3. В 14:30:35 пользователь получил доступ к фрагменту архива в **Интервале** 09:15:00.000 – 09:19:59.999 (по времени архива).
4. В 14:35:34 пользователь получил доступ к фрагменту архива в **Интервале** 09:20:00.000 – 09:24:59.999 (по времени архива).
5. В 14:40:34 пользователь получил доступ к фрагменту архива в **Интервале** 09:25:00.000 – 09:29:59.999 (по времени архива). По условию примера пользователь закончил просмотр архива в 14:41:12 и переключился в режим просмотра живого видео. Указатель архива при этом был остановлен на отметке 09:25:34, что не выходит за границы текущего **Интервала** 09:25:00.000 – 09:29:59.999.

21.5 Приложение 5. Используемые в SecurOS сетевые порты

SecurOS и подключаемые модули для взаимодействия используют ряд TCP и UDP портов.

Внимание! Сторонние приложения не должны использовать порты, используемые в ПО SecurOS.

Проверьте настройки брандмауэра и откройте для исполняемых файлов SecurOS (*.exe), расположенных в корневом каталоге SecurOS, следующие порты в оба направления:

- **TCP-порты.**
- **UDP-порты.**

Таблица 123. Порты TCP

Модуль	Номер порта
Основная подсистема	
Базовые компоненты SecurOS	20950, 21111
Базы данных	5432
Health Monitor	23322
Шлюз MCC DC	20904
Кластер	2379, 2380, 2381
Server Manager	20941
Audit API	40943
Видео- и аудиоподсистема	
Видеопоток	20900
Архиватор	20901
EdgeStorage Gate	20903

Модуль	Номер порта
ONVIF Tool	20905
	Примечание. ONVIF Tool используется для получения дополнительной информации об ONVIF-устройствах.
Аудиопоток	20910
Работа по протоколу ONVIF	50000
Подсистема базового интерфейса	
Интерфейс оператора (все элементы)	38880
Протокол событий	20944
Вспомогательные компоненты	
3D карта	26889
Интеграции	
IIDK	21030
	Примечание. Открытие этого порта требуется не для всех интеграций. За дополнительной информацией обращайтесь в Службу технической поддержки компании Intelligent Security Systems (см. раздел Обращение за технической поддержкой).
ActiveMedia Kit	23100
Точка интеграции	23000
SIP	20913
СКУД/ОПС (любая интеграция)	20911
Интеллектуальные модули	
SecurOS Mobile	7779
SecurOS System Dashboard	20945

Таблица 124. Порты UDP

Модуль	Номер порта
Основная подсистема	
Базовые компоненты SecurOS	20950

21.6 Приложение 6. Дополнительные настройки Windows

Дополнительные настройки Windows обеспечивают корректность функционирования SecurOS, необходимы для использования ряда ее функциональных возможностей, позволяют оптимизировать работу с системой.

21.6.1 Установка Media Foundation в среде MS Windows Server 2012 R2

Операционная система Windows Server 2012 является полностью серверной ОС. Это означает, что при инсталляции ОС никакие мультимедийные компоненты и службы не устанавливаются. В то же время для корректной работы SecurOS, в частности *Устройства видеозахвата* с типом **Player AVI**, необходимо наличие установленных в системе фильтров и кодеков. Для установки компонента **Media Foundation** выполните следующие действия:

1. Откройте консоль **Диспетчера сервера**.
2. В меню **Управление** выберите команду **Добавить роли и компоненты**.
3. На странице **Выбор типа установки** выберите опцию **Установка ролей или компонентов**.
4. Чтобы выбрать компоненты нажмите кнопку **Далее**. Выберите компонент **Media Foundation**.
5. На странице **Подтверждение выбранных элементов для установки** проверьте выбранные роли, компоненты и серверы. Если все готово к установке, нажмите кнопку **Установить**.
6. При необходимости перезагрузите сервер.

21.6.2 Установка и настройка почтового SMTP-сервера

Примечание. Все действия необходимо выполнять с правами локального или доменного администратора.

На компьютере с установленной службой *Сервис почтовых сообщений* откройте **Панель управления** и выберите **Установка и удаление программ**, затем **Установка компонентов Windows**.

Выберите в списке поле **Internet Information Services (IIS)** и нажмите кнопку **Состав** (см. рис. 335).

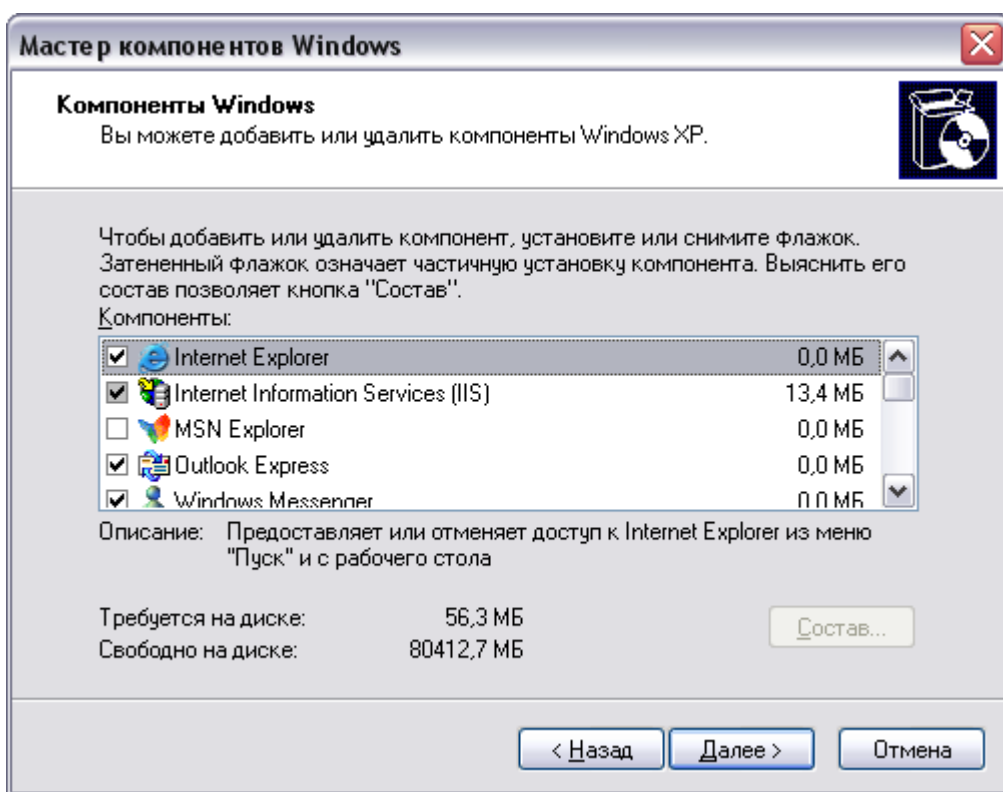


Рис. 335. Мастер компонентов Windows

Активируйте в списке поле **Служба SMTP** (см. рис. 336). Нажмите **ОК** и **Далее** для завершения установки.

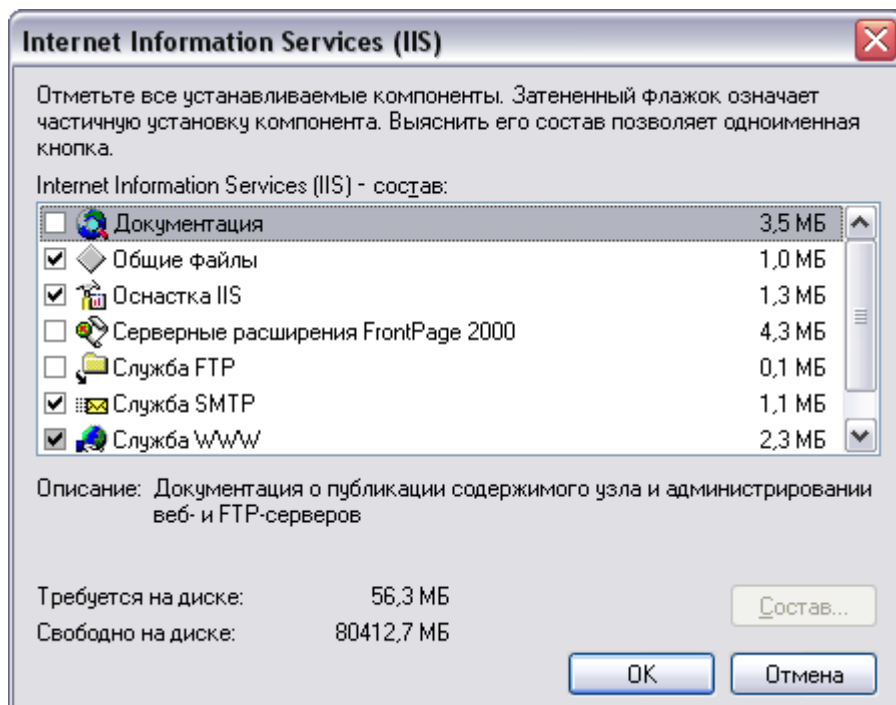


Рис. 336. Компоненты Internet Information Services

Чтобы настроить SMTP-сервер для пересылки сообщений, после установки службы SMTP:

1. Откройте **Панель управления** → **Администрирование** → **Internet Information Services**.
2. В левой части появившегося окна (см. рис. 337) нажмите правой кнопкой **Виртуальный SMTP-сервер** (или другое имя, установленное по умолчанию) и выберите **Свойства**.

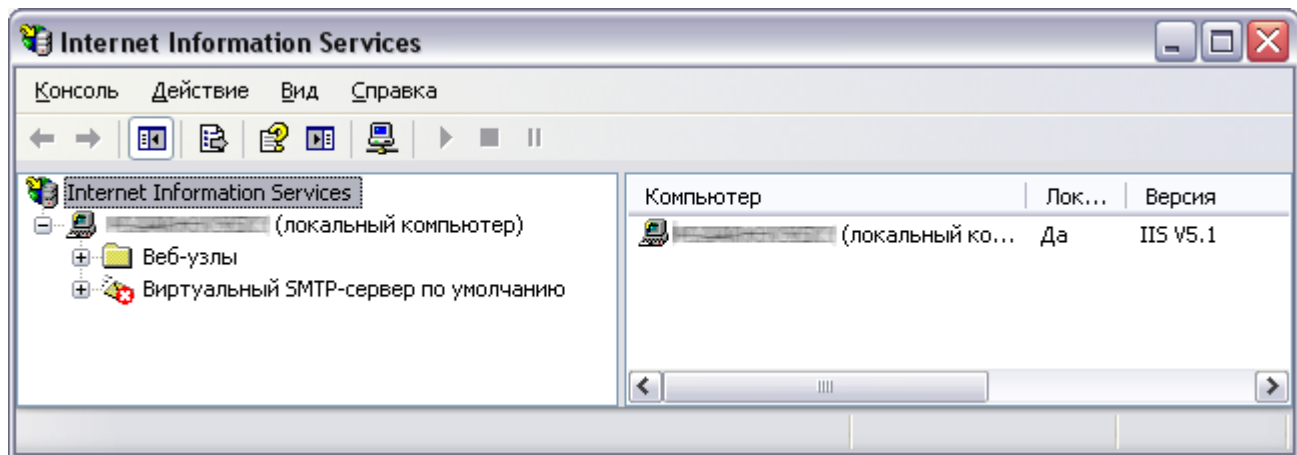


Рис. 337. Дерево служб IIS

3. Выберите закладку **Доступ** и нажмите кнопку **Ретрансляция**.
4. В окне **Ограничения ретрансляции** выберите **Все** для разрешения пересылки всем компьютерам, отправляющим почту через данный сервер, и нажмите **ОК** (см. рис. 338).

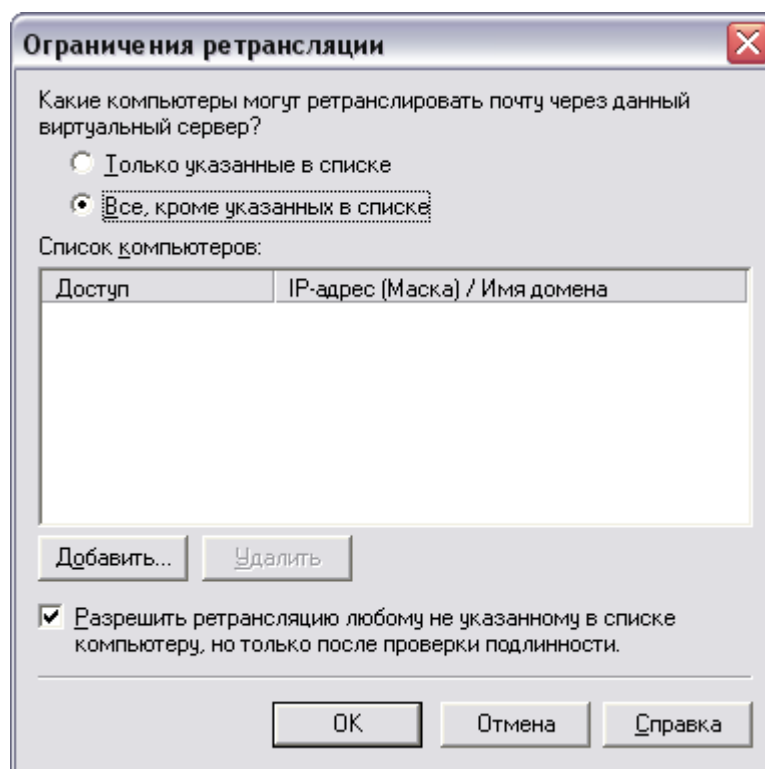


Рис. 338. Настройка ограничений пересылки SMTP-сервера

5. Выберите закладку **Доставка** и нажмите кнопку **Дополнительно**.
6. В окне **Дополнительная настройка доставки** (см. рис. 339) укажите в поле **Направляющий узел** удаленный сервер для маршрутизации всей отправляемой почты, и нажмите **ОК**.

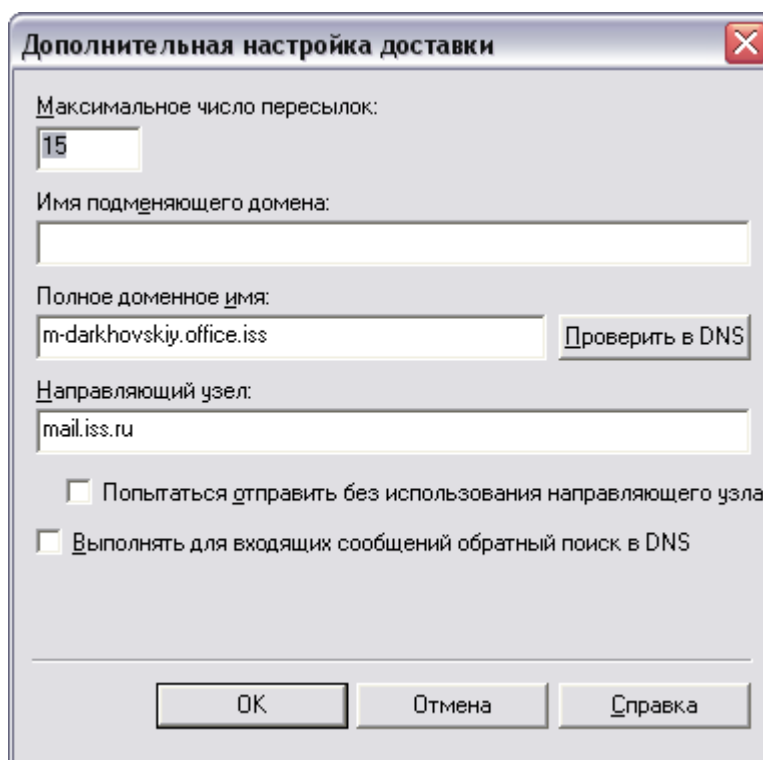


Рис. 339. Настройка удаленного сервера маршрутизации почты

7. Нажмите **ОК** для закрытия окна свойств SMTP-сервера и сохранения всех сделанных изменений.
8. Выберите **Действие** → **Запуск** для запуска службы SMTP-сервера.

21.6.3 Отключение мастера очистки дисков

Для рабочих мест оператора рекомендуется отключить системные предупреждения о переполнении диска.

Чтобы отключить вызов мастера очистки дисков:

1. Откройте редактор реестра (**Пуск** → **Выполнить** → **regedit**).
2. Выберите раздел
`\HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer` и создайте параметр `DWORD` с именем `NoLowDiskSpaceChecks`.
3. Присвойте созданному параметру значение `0`, чтобы отключить проверку переполнения дисков (`1` — чтобы включить).
4. Закройте редактор реестра и перезагрузите компьютер.

21.7 Приложение 7. Дополнительные настройки SecurOS

Дополнительные настройки SecurOS обеспечивают корректность функционирования системы при заданных настройках Windows.

21.7.1 Масштабирование SecurOS при масштабировании Windows

Если SecurOS запускается на мониторах с большой диагональю и высоким текущим разрешением, то при масштабировании Windows (**Пуск → Настройка → Параметры → Система → Дисплей → Масштаб и разметка**) возможны искажения элементов графического интерфейса пользователя SecurOS.

Для автоматической корректировки элементов интерфейса SecurOS при изменении масштаба/разрешения Windows выполните следующие действия:

1. В <корневой_директории_установки_SecurOS> и во вложенной папке `./bin64` найдите файл `qt.conf_` и переименуйте его в `qt.conf`.
2. Перезапустите службу Video Management System Server (см. [Утилита Server Control Agent](#)).

21.8 Приложение 8. Диагностика и решение технических проблем

В разделе приводится описание диагностирования возможных технических проблем и способы их решения.

21.8.1 Создание дампов процессов

Для диагностики возможных проблем, связанных с производительностью или совместимостью продукта, сотрудник Службы технической поддержки может попросить вас снять дамп одного или нескольких процессов в системе.

В разделах ниже приводится описание процесса сбора дампов процессов для операционных систем семейства Linux и Windows:

- [Создание дампа процесса в ОС Windows.](#)
- [Создание дампа процесса в ОС Linux.](#)

21.8.1.1 Создание дампа процесса в ОС Windows

Для создания дампа процесса в ОС Windows выполните следующие действия:

1. Откройте **Диспетчер задач**.
2. Нажмите **Подробнее**. Окно диспетчера задач откроется в расширенном виде.
3. На вкладке **Процессы** нажмите правой кнопкой мыши на необходимый процесс.
4. В открывшемся контекстном меню выберите **Создать файл дампа (Создать файл дампа памяти для Windows 11)**. Начнется процесс создания дампа.
5. В открывшемся окне **Дамп процесса** нажмите кнопку **Открыть расположение файла** для перехода в папку с созданным дампом или **ОК** для закрытия окна.

По умолчанию дамп процесса сохраняется по следующему пути:

```
C:\Users\<имя_пользователя>\AppData\Local\Temp\<имя_процесса>.DMP
```

21.8.1.2 Создание дампа процесса в ОС Linux

Для создания дампа процесса в ОС Linux выполните следующие действия:

1. Установите пакет gdb.

Внимание! Рекомендуется использовать gdb версии 9.0 или выше.

2. Определите идентификатор необходимого процесса, выполнив команду:

```
pidof <имя_процесса>
```

Примечание. Для просмотра списка всех процессов используйте команду `ps -e`.

3. Последовательно выполните команды:

```
sudo gdb --pid <идентификатор_процесса>  
  
generate-core-file  
  
detach  
  
quit
```

Внимание! В ОС Astra Linux при возникновении ошибки `ptrace: Операция не позволена` необходимо выполнить команду `sudo astra-pttrace-lock disable` и перезагрузить компьютер.

По умолчанию дампы процесса сохраняются по следующему пути:

```
/home/<имя_пользователя>/core.<идентификатор_процесса>
```

Для сохранения дампа в определенный каталог, укажите его при выполнении команды `generate-core-file`. Например:

```
generate-core-file /var/dumps/<имя_дампа>
```

Для просмотра списка созданных дампов в текущем каталоге выполните следующую команду:

```
ls -al core.*
```

21.9 Приложение 9. Возможные сообщения об ошибке при запуске системы

При запуске SecurOS может сообщать о проблемах. Список проблем и пояснений к ним представлен в таблице [125](#).

Таблица 125. Возможные сообщения об ошибке при запуске системы

Сообщение	Рекомендации
"Ключ не найден"	Убедитесь, что файл <code>key.iss</code> находится в каталоге, куда было установлено программное обеспечение SecurOS. Если файл отсутствует, то необходимо вручную скопировать его в каталог SecurOS на Сервере конфигураций (файл находится на установочном диске, также его можно получить по электронной почте).
"Ошибка запуска"	Неизвестная ошибка во время запуска системы. Создайте отчет о состоянии системы с помощью утилиты SystemInfo (см. Утилита SystemInfo) и обратитесь в Службу технической поддержки для анализа отчета и поиска возможной ошибки (см. раздел Обращение за технической поддержкой).
"Истек срок действия ключа"	Истек срок действия файла <code>key.iss</code> . Обратитесь в Службу технической поддержки для получения нового ключа (см. раздел Обращение за технической поддержкой).
"Ошибка подключения к БД"	Последовательно проведите следующие действия: • Проверьте корректность параметров подключения к БД при помощи утилиты DSAdmin Utility. • Проверьте возможность подключения к БД при помощи утилиты pgAdmin III из комплекта PostgreSQL. • Убедитесь, что служба Windows PostgreSQL Database Server 9.x существует и запущена. • Убедитесь, что пользователь, под которым запущено ПО, имеет права на чтение ключа <code>HKLM/Software/WOW6432Node/ISS/SecurOS/NISS400/DB</code> в реестре. • Переустановите SecurOS. Обратите особое внимание на разделы установки БД PostgreSQL. • Если перечисленные рекомендации не помогли, обратитесь в Службу технической поддержки. Обязательно приложите к письму информацию о системе, полученную с помощью утилиты SystemInfo.
"Ключ не поддерживает язык"	При установке SecurOS был выбран язык интерфейса, не соответствующий прописанному в вашем лицензионном ключе. Заново переустановите программное обеспечение SecurOS на этом компьютере и выберите другой язык интерфейса либо приобретите новый файл <code>key.iss</code> , который поддерживает этот язык.
"Ключ не поддерживает страну"	Настройки в главном меню (Пуск → Панель управления → Язык и региональные настройки) отличаются от тех, что прописаны в вашем лицензионном ключе. Проверьте эти настройки, либо приобретите новый файл <code>key.iss</code> , который поддерживает текущие настройки.

Сообщение	Рекомендации
"Не удалось загрузить одну из интеграционных библиотек"	Создайте отчет о состоянии системы с помощью утилиты SystemInfo (см. Утилита SystemInfo) и обратитесь в Службу технической поддержки для анализа отчета и поиска возможной ошибки (см. раздел Обращение за технической поддержкой).

21.10 Приложение 10. Информация для Службы технической поддержки

Данный раздел описывает требования к служебной информации, необходимой при обращении в Службу технической поддержки компании Intelligent Security Systems.

Примечание. Собранные сведения необходимо направлять в Службу технической поддержки (см. раздел [Обращение за технической поддержкой](#)).

Для более скорого разрешения проблем подготовьте следующую техническую информацию:

Внимание! Сведения в пунктах, отмеченных знаком "*", являются обязательными для предоставления.

1. (*) Ф. И. О.
2. (*) Название организации.
3. (*) Контактная информация: телефон, e-mail.
4. Если Вы являетесь партнером Intelligent Security Systems, то укажите, с каким менеджером компании Intelligent Security Systems Вы работаете; в ином случае, укажите следующие сведения:
 - Компания, в которой приобретался комплект программного и аппаратного обеспечения.
 - Действия для устранения проблемы, предложенные при обращении к партнеру, у которого приобретался комплект.
5. (*) Описание проблемы (неполадки).
6. (*) Описание действий, которые приводят к возникновению проблемы.
7. Описание изменений в настройках/конфигурации системы, которые привели к возникновению проблемы.
8. Системная и диагностическая информация о компьютере и конфигурации системы SecurOS, полученная с помощью утилиты **SystemInfo** (см. раздел [Утилита SystemInfo](#) для подробной информации об использовании утилиты).

Если невозможно запустить данную утилиту, предоставьте следующую информацию:

- (*) идентификаторы и даллас-коды используемых ключей Guardant;

Примечание. Даллас-коды оборудования можно просмотреть с помощью утилиты **Hardware Report Utility** (см. раздел [Утилита Hardware Report Utility](#) для подробной информации об использовании утилиты).

- (*) наименование и версия установленного ПО производства компании Intelligent Security

Systems;

- общее количество видеосерверов и удаленных рабочих мест оператора в системе;
 - операционная система (наименование платформы, версия сервисного пакета).
9. По возможности предоставьте любую другую полезную информацию, например:
- конфигурация компьютерного оборудования;
 - загрузка центральных процессоров;
 - объемы используемой оперативной и виртуальной памяти;
 - загрузка сети;
 - конфигурация сети и сетевого окружения.

Предметный указатель

A

Active Directory / LDAP, объект, описание, 161
AuditClient, утилита, 583

B

Bgain, параметр,
Интегратор ONVIF, 267

C

CCTV Клавиатура или джойстик, объект, описание, 363

D

Database Partitioner, объект, описание, 192

E

Edge Storage,
 синхронизация времени, 228
 требования к локальному хранилищу камеры, 228
 требования к оборудованию, 227
E-mail, параметр,
 Пользователь, 161

F

FaceX: Сервер, параметр,
 Термометр, 523

H

H264/H265: Использовать маркеры RTP, параметр,
 Интегратор ONVIF, 268
 Устройство видеозахвата Generic RTSP, 272
H265: Игнорировать бит конца FU в заголовке, параметр,
 Интегратор ONVIF, 268
 Устройство видеозахвата Generic RTSP, 272
H265: Игнорировать бит начала FU в заголовке, параметр,
 Интегратор ONVIF, 268
 Устройство видеозахвата Generic RTSP, 272
H265: Игнорировать тип FU в заголовке, параметр,
 Интегратор ONVIF, 268

Устройство видеозахвата Generic RTSP, 273
H265: Игнорировать тип полезной нагрузки в заголовке FU, параметр,
 Интегратор ONVIF, 268
Устройство видеозахвата Generic RTSP, 273
Hardware Report Utility, утилита, 550
HDR преобразование, параметр,
 Камера, 276
Health Monitor, объект, описание, 121
HTML5 FrontEnd, объект, описание, 213
HTTP Event Gate, объект, описание, 400
HTTP адрес Службы реагирования, параметр, 380

I

Image Processor, объект, описание, 305
IP-адрес сервера, параметр,
 Компьютер, 173
IP-адрес управляющего устройства, параметр,
 Камера, 269
IP-адрес, параметр, 244
 Подсистема SIP, 385
 Устройство аудиозахвата, 356
IQN, параметр,
 iSCSI-диск, 504

M

Media Export Utility, утилита, 556

N

Node.js Script, объект, описание, 396

O

ONVIF-сервер, объект, описание, 309

P

PCI канал, параметр, 243
PCI-канал, параметр,
 Устройство аудиозахвата, 357

R

REST API, объект, описание, 401
Rgain, параметр,
 Интегратор ONVIF, 266
RTP поверх RTSP (TCP), параметр,
 Камера, 255
RTSP спецификация, параметр,
 RTSP-сервер, 308
RTSP-сервер, объект, описание, 306
RTSP-сервер, параметр,
 ONVIF-сервер, 310

RTSP-сервер, параметр,
Служба реагирования, 381

S

Server Manager, утилита, 540
SMTP сервер, параметр, 374
SNMP агент, объект, описание, 187
SystemInfo, утилита, 552

U

URL, параметр,
HTML5 FrontEnd, 214
Всплывающее окно HTML5, 373

W

W, H, параметры,
Медиа Клиент, 318
WebView Монитор, параметр,
Служба реагирования, 381
WebView, параметр,
Служба реагирования, 381

X

X, Y, W, H, параметр,
HTML5 FrontEnd, 214
SIP: Интерфейс оператора, 388
Внешнее окно, 213
Всплывающее окно HTML5, 373
Карта: Интерфейс оператора, 209
Протокол событий, 211
X, Y, параметры,
Медиа Клиент, 318

A

Автоматическая авторизация разрешена для
Пользователя, параметр,
Компьютер, 174
Автоматический баланс белого, параметр,
Камера, 274
Автоматическое завершение сеанса пользователя
при блокировке экрана, параметр,
Компьютер, 174
Автоматическое создание резервных копий,
параметр,
Система, 148
Автоматическое усиление, параметр, 275
Автоматическое центрирование по вертикали,
параметр, 276
Автоматическое центрирование по горизонтали,
параметр, 275
Адрес (IPv4) для Мультикастной группы, параметр,

Камера, 255
Адрес группы, параметр,
ONVIF-сервер, 314
Адрес Сервера конфигураций, параметр,
Удаленная система, 477
Активировать рабочий стол, параметр, 173
Алгоритм шифрования, параметр, 295
Алгоритм, параметр,
Детектор движения в запрещенном
направлении, 431
Анализировать прореженный поток, параметр, 287
Аппаратное ускорение, параметр,
Медиа Клиент, 336
Архив, закладка,
Компьютер, 173
Архиватор, объект, описание, 299
Архивировать сопровождающее аудио, параметр,
Архиватор, 302
Архивировать, параметр,
Почтовое сообщение, 377

Б

База данных для записи, параметр,
Компьютер, 175
База данных СКУД/ОПС, параметр,
Компьютер, 176
База данных, объект, описание, 157
Базовый, параметр,
Камера, 252
Медиа Клиент, 323
базу данных, кнопка,
Репликатор баз данных, 193
Базы данных, параметр,
Репликатор баз данных, 193
Баланс белого, параметр,
Интегратор ONVIF, 266
Блок информации о настраиваемом окне,
Рабочий стол, 197
Быстрый экспорт (видео), параметр, 296

В

Вид, объект,
Переименование, 341
Редактирование, 340
Создание, 340
Удаление, 341
Вид, объект, описание, 284
Видео, параметр,
Архиватор, 300
Зона, 287
Визуализировать события Компьютерного Зрения,
параметр,

Визуализировать события Компьютерного Зрения, параметр,
 Медиа Клиент, 328
Включить буферизацию, параметр,
 Медиа Клиент, 327
Включить мультикаст, параметр,
 Камера, 255
Включить передачу необработанных событий, параметр,
 Интегратор ONVIF, 266
Включить синхронизацию потоков, параметр,
 Устройство видеозахвата Virtual, 271
Вложения, параметр,
 Почтовое сообщение, 377
Внешнее окно, объект, описание, 212
Внешняя зона (дополнительная), параметр, 289
Внешняя зона, параметр, 289
Внутренняя зона, параметр, 289
Водяной знак, объект, описание, 181
Возможное отклонение от направления, параметр,
 Детектор движения в запрещенном направлении, 431
Возможность переноса архива из Удаленной системы, параметр,
 Медиа Клиент, 331
Восстанавливать архив из локального хранилища Камеры (Edge Storage), параметр,
 Камера, 259
Восстановить, кнопка,
 Система, 147
Время на подтверждение тревожного события оператором, параметр, 212
Время отображения страницы при автолистании, параметр,
 Медиа Клиент, 320
Время экспозиции, мкс, параметр,
 Камера, 275
Время экспозиции, параметр,
 Интегратор ONVIF, 266
Всегда на охране, параметр, 286
Всплывающее окно HTML5, объект, описание, 372
Выбрать зону, параметр,
 Детектор движения в запрещенном направлении, 432
Выбрать ключ, кнопка,
 ONVIF-сервер, 312
Выбрать сертификат, кнопка,
 ONVIF-сервер, 311
Выбрать, кнопка,
 Внешнее окно, 213
 Конвертер архива, 297
Выполнять локально, параметр, 394
Высокое разрешение, параметр,

 Камера, 252
 Медиа Клиент, 323
Высота кадра, пк, параметр,
 Камера, 275
Высота подвеса Камеры, параметр,
 Счетчик объектов, 449

Г

Громкость, параметр,
 Сервис звукового оповещения, 379
Группировать Камеры и Микрофоны по имени, параметр,
 Медиа Клиент, 319

Д

Дата, с повторением, параметр,
 Расписание, 393
Дворник, параметр,
 Камера, 249
Действие, параметр, 395
Делитель частоты кадров, параметр, 296
Дерево Микрофонов, параметр,
 Медиа Клиент, 334
Дерево объектов, 83
 Дочерний объект, 83
 Рабочий стол, 196
 Родительский объект, 83
Дерево объектов, параметр,
 Луч, 362
 Медиа Клиент, 328
 Шлюз MCC DC, 475
Дерево устройств,
 Карта, 203
Детектор бега, объект, описание, 427
Детектор движения в запрещенном направлении, объект, описание, 430
Детектор дыма, объект, описание, 451
Детектор людей без касок, объект, описание, 452
Детектор оставленных и унесенных предметов, объект, описание, 433
Детектор оставленных предметов, параметр,
 Детектор оставленных и унесенных предметов, 435
Детектор пересечения линии, объект, описание, 436
Детектор подсчета объектов, объект, описание, 447
Детектор праздношатания, объект, описание, 438
Детектор пребывания в зоне, объект, описание, 441
Детектор проникновения в запрещенную зону, объект, описание, 442
Детектор расфокусировки, 281
Детектор скопления людей, объект, описание, 445
Детектор унесенных предметов, параметр,

Детектор унесенных предметов, параметр,
Детектор оставленных и унесенных предметов, 435

Детекция засвечивания, параметр,
Камера, 262

джойстик,
настройка, 353

Динамик, параметр,
Камера, 261

Директория, параметр,
Архиватор, 300

Дисплей, параметр,
HTML5 FrontEnd, 214
SIP: Интерфейс оператора, 388
Внешнее окно, 213
Всплывающее окно HTML5, 373
Карта: Интерфейс оператора, 209
Медиа Клиент, 319
Протокол событий, 211

Дифрагма, параметр,
Интегратор ONVIF, 266

Длительность постзаписи, параметр,
Камера, 257

Длительность пребывания в зоне, параметр,
Нейросетевой детектор праздношатания, 461

Длительность предзаписи, параметр,
Камера, 257

Длительность, параметр,
Детектор праздношатания, 440
Детектор скопления людей, 446

Для детектора движения, параметр,
Камера, 252

Для записи видео, параметр,
Камера, 252

Дни недели, параметр,
Расписание, 392

Добавить данные авторизации в URL, параметр,
Устройство видеозахвата Generic RTSP, 272

Добавить директорию, кнопка,
Архиватор, 301

Добавить колонтитул, параметр,
Медиа Клиент, 320

Дополнительная информация, параметр,
Пользователь, 161

Дополнительно, параметр,
HTML5 FrontEnd, 215
Всплывающее окно HTML5, 373

Дополнительный нейросетевой фильтр автомобилей, параметр,
Детектор движения в запрещенном направлении, 432
Детектор пересечения линии, 437
Детектор праздношатания, 440

Детектор проникновения в запрещенную зону, 444

Дополнительный нейросетевой фильтр людей, параметр,
Детектор бега, 429
Детектор движения в запрещенном направлении, 431
Детектор пересечения линии, 437
Детектор праздношатания, 440
Детектор проникновения в запрещенную зону, 444

Доступ к Долговременному архиву, параметр,
Медиа Клиент, 331

Е

Емкость, параметр,
Архиватор, 300

З

Загрузить из файла, кнопка,
Служба реагирования, 382

Задать размеры человека, параметр,
Нейросетевой детектор праздношатания, 461

Задать характерные размеры объекта, кнопка,
Счетчик объектов, 449

Задержка обнаружения, параметр,
Нейросетевой детектор упавших людей, 466

Задержка сопряжения показаний, параметр,
Термометр, 523

Закладка Классификация,
Плагин Tracking Kit III, 417

Закладка Ретроспективный поиск,
Плагин Tracking Kit III, 419

Закладка Сцена,
Плагин Tracking Kit III, 412

Закладка Трекер,
Плагин Tracking Kit III, 416

Записывать данные аудита системы, параметр,
Система, 148

Записывать дополнительные параметры событий в протокол, параметр, 175

запись архива, 232
запись в файлы фиксированного размера, 177
предел, 233
размер архива, 233

Заполнить все, параметр, 287

Запрашивать аутентификацию, параметр,
ONVIF-сервер, 311
RTSP-сервер, 308

Запретить привилегированный доступ, параметр,
Система, 147

Запретить скрытие интерфейсов системы, параметр, 164
 Запретить совместное управление, параметр,
 Камера, 263
 Звуковая плата, параметр,
 Сервис звукового оповещения, 379
 Зона,
 принципы работы, 225
 Зона, объект, описание, 284

И

Игнорировать RTP SSRC, параметр,
 Устройство видеозахвата Generic RTSP, 272
 Игнорировать номер последовательности в заголовке RTP (только для RTP/TCP), параметр,
 Устройство видеозахвата Generic RTSP, 272
 Игнорировать параметр qop (Quality of protection) со значением auth при дайджест-аутентификации, параметр,
 Камера, 273
 Игнорировать тип полезной нагрузки RTP, параметр,
 Устройство видеозахвата Generic RTSP, 272
 Идентификатор Камеры во внешнем устройстве, параметр,
 Камера, 254
 идентификатор объекта, 85
 Идентификатор, параметр,
 Макрокоманда (Действия), 395
 Макрокоманда (События), 395
 Изменить, кнопка,
 Архиватор, 301
 Иконка, параметр,
 Макрокоманда, 396
 Иконки, параметр,
 Карта, 203
 Имя базы/Пользователь/Пароль, параметры,
 База данных, 158
 Имя пользователя, Пароль, параметр, 163, 374
 Имя файла и кнопка Обзор, параметр,
 SIP: Интерфейс оператора, 389
 интеграция с внешними системами, 399
 Интерфейс IIDK, объект, описание, 399
 Использовать GPU, параметр,
 Детектор людей без касок, 453
 Использовать HTTPS, параметр,
 REST API, 402
 Использовать альтернативный способ синхронизации звука для встроенного микрофона, параметр,
 Камера, 273
 Использовать аутентификацию, параметр,
 iSCSI-диск, 504
 Использовать безопасное соединение (HTTPS), параметр,
 Устройство аудиозахвата, 356
 Устройство видеозахвата, 245
 Использовать встроенный контроллер SecurOS Motus, параметр,
 Камера, 269
 Использовать двухфакторную аутентификацию по e-mail, параметр, 165
 Использовать для двухфакторной аутентификации и сброса пароля, параметр,
 Сервис почтовых сообщений, 375
 Использовать защищенные соединения, параметр,
 Система, 149
 Использовать как Профиль Рабочего места оператора, параметр,
 Компьютер, 173
 Использовать контроллер домена, параметр, 162
 Использовать межкадровые задержки из файла, параметр,
 Устройство видеозахвата Virtual, 271
 Использовать механизм сброса фона, параметр,
 Детектор оставленных и унесенных предметов, 435
 Использовать настройки камеры, параметр,
 Камера, 253
 Использовать поток по запросу, параметр,
 Камера, 255
 Использовать Профили экспорта архива, параметр,
 Медиа Клиент, 331
 Использовать совместимое форматирование URL в методе SETUP, параметр,
 Устройство видеозахвата Generic RTSP, 272
 Использовать только дайджест-аутентификацию, параметр,
 Камера, 250
 Использовать устройство, параметр,
 Нейросетевой детектор дыма и огня, 458
 Нейросетевой детектор праздного шатания, 461
 Нейросетевой детектор уклонения от оплаты, 463
 Нейросетевой детектор упавших людей, 465
 Использовать устройство. параметр,
 Нейросетевой счетчик людей, 467
 Использовать учетную запись операционной системы, параметр, 163
 Использовать Фильтр событий, параметр, 175, 211
 REST API, 402
 Использовать шифрование, параметр, 162
 Используется пономорфный объектив, параметр,
 Камера, 273

К

- Кадров в памяти, параметр, 287
- Камер тепловизора, параметр,
 - Термометр, 523
- камера,
 - настройка изображения, 232
- Камера FaceX, параметр,
 - Термометр, 523
- Камера расфокусирована, когда резкость снизилась на, параметр,
 - Детектор расфокусировки, 280
- Камера сфокусирована, кнопка,
 - Детектор расфокусировки, 280
- Камера, настройка, 344
- Камера, объект, описание, 247
- Камеры, параметр,
 - ONVIF-сервер, 314
 - RTSP-сервер, 308
- Канал PTZ, параметр,
 - Камера, 263
- Канал, параметр,
 - Луч, 361
 - Микрофон, 357
 - Реле, 362
- Карта,
 - Вращение объекта, 207
 - Добавление уровня, 204
 - Дочерний уровень, создать, 206
 - Объекты, позиционирование, 207
 - Отобразить сокращенное имя объекта, 208
 - Перемещение имени объекта, 208
 - Перемещение объекта, 207
 - Поиск объекта по имени, 207
 - Принципы работы, 203
 - Ссылка на уровень, 206
 - Удаление объекта, 209
 - Уровень, редактировать, 206
 - Уровень, удалить, 206
 - Уровни, изображение, 204
- Карта, объект, описание, 201
- Карта, параметр,
 - Карта: Интерфейс оператора, 209
- Карта: Интерфейс оператора, объект, описание, 209
- Карта: Интерфейс оператора, параметр,
 - SIP: Интерфейс оператора, 389
- Качество, параметр,
 - Конвертер архива (Видео), 296
- Класс объекта, параметр,
 - Детектор движения в запрещенном направлении, 431
 - Детектор пересечения линии, 437
 - Детектор праздношатания, 440
 - Детектор проникновения в запрещенную зону, 444
 - Счетчик объектов, 449
- кластер баз данных, кнопка,
 - Репликатор баз данных, 194
- ключ Guardant, 550
 - установка, 25
- Кнопка Воспроизвести, параметр,
 - SIP: Интерфейс оператора, 389
- Кодек для видеопотока с камеры, параметр,
 - Камера, 276
- Кодек для записи видеоархива, параметр,
 - Камера, 276
- Кодек, параметр,
 - ONVIF-сервер, 314
 - RTSP-сервер, 308
 - Конвертер архива (Аудио), 296
 - Конвертер архива (Видео), 296
- Количество записей в секции, параметр,
 - Database Partitioner, 192
- Количество ячеек, параметр,
 - Раскладка, 283
- Команда "Воспроизвести последние N сек / мин записи", параметр,
 - Медиа Клиент, 332
- комбинации клавиш, 526
- Компенсация засветки, параметр,
 - Интегратор ONVIF, 267
- Компьютер, объект, описание, 171
- Компьютеры, с которых разрешено подключение к сети, параметр,
 - Интерфейс IIDK, 400
- Кому, параметр, 376
- Конвертер архива, объект, описание, 289
- Контакт, параметр,
 - SIP-устройство, 387
 - Подсистема SIP, 385
- Контраст, параметр,
 - Зона, Детектор движения, 287
 - Интегратор ONVIF, 266
 - Камера, 262
- конфигурация,
 - быстрая настройка, 538
- Координаты, параметр,
 - Камера, 248
- Копия, параметр, 376
- Короткое сообщение, объект, описание, 378

Л

- Латентность сети, мс, параметр,
 - Камера, 255

Лицензионный ключ, 25, 60
настройка оповещения о сроке действия, 120
обновление, 119
оповещение о сроке действия, 119
Лицензионный ключ для ОС Linux,
заказ, 60
Лицензионный ключ для ОС Windows,
заказ, 26
Луч, объект, описание, 360
Любое количество Камер, без переключения потоков, параметр,
Медиа Клиент, 320

М

Макрокоманда, объект, описание, 393
Макс. FPS, параметр,
Архиватор, 301
Максимально допустимая температура, параметр,
Термометр, 523
Максимальное количество копий, параметр,
Система, 148
Максимальное усиление, параметр, 275
Максимальный размер БД, параметр, 175
Максимальный срок действия пароля (дней),
параметр,
Объект охраны, 155
Масштаб, параметр,
Карта, 203
Масштабирование выделенной области кадра,
параметр,
Интегратор ONVIF, 268
Медиа Клиент, параметр,
SIP: Интерфейс оператора, 388
Менеджер IP-устройств, объект, описание, 96
Микрофон, объект, описание, 357
Микрофон, параметр,
Камера, 261
Минимальное время детекции объекта, параметр,
Детектор оставленных и унесенных предметов,
435
Минимальное количество символов пароля,
параметр,
Объект охраны, 155
Минимальное пересечение объекта и зоны,
параметр,
Детектор праздногошата, 440
Детектор пребывания в зоне, 442
Детектор проникновения в запрещенную зону,
444
Нейросетевой детектор праздногошата, 461
Минимальное усиление, параметр, 275
Минимальное число людей, параметр,
Детектор скопления людей, 446
Минимум/Максимум, параметры,
Медиа Клиент, 322
Модель, параметр,
Устройство аудиозахвата, 356
Устройство видеозахвата, 242
Мультикаст, параметр,
ONVIF-сервер, 314

Н

Название камеры, параметр,
SIP-устройство, 387
название объекта, 85
Название события, параметр,
Детектор бега, 428
Детектор движения в запрещенном направлении, 431
Детектор дыма, 451
Детектор людей без касок, 453
Детектор оставленных и унесенных предметов (Детектор оставленных предметов), 435
Детектор оставленных и унесенных предметов (Детектор унесенных предметов), 435
Детектор пересечения линии, 436
Детектор праздногошата, 439
Детектор пребывания в зоне, 442
Детектор проникновения в запрещенную зону, 443
Детектор скопления людей, 446
Нейросетевой детектор драк, 456
Нейросетевой детектор дыма и огня, 458
Нейросетевой детектор праздногошата, 461
Нейросетевой детектор уклонения от оплаты, 463
Нейросетевой детектор упавших людей, 465
Счетчик объектов, 448
Название события. параметр,
Нейросетевой счетчик людей, 467
Название, параметр,
Архиватор, 301
Карта, 202
Макрокоманда (Действия), 395
Макрокоманда (События), 395
Наложение логотипа, блок параметров,
Конвертер архива, 296
Насыщенность, параметр,
Интегратор ONVIF, 266
Не восстанавливать последние, мин, параметр,
Камера, 259
Не использовать прокси-сервер для, параметр,
Удаленная система, 479
Не корректировать время кадров при ускоренном воспроизведении, параметр,
Камера, 259

Не показывать окно уведомлений при появлении новых проблем, параметр,

Health Monitor, 122

Нейросетевой детектор драк, объект, описание, 455

Нейросетевой детектор дыма и огня, объект, описание, 457

Нейросетевой детектор праздногошатапия, объект, описание, 460

Нейросетевой детектор уклонения от оплаты, объект, описание, 462

Нейросетевой детектор упавших людей, объект, описание, 464

Нейросетевой счетчик людей, объект, описание, 466

Немедленно перезапускать поток при разрыве, параметр,

Интегратор ONVIF, 266

Устройство видеозахвата Generic RTSP, 272

Нестандартные команды управления дворником, параметр,

Интегратор ONVIF, 267

Нестандартные команды управления омывающим устройством, параметр,

Интегратор ONVIF, 268

Низкое разрешение, параметр,

Камера, 252

Медиа Клиент, 323

Новый пароль, параметр,

Система, 146

Номер профиля потока, параметр,

Камера, 260

Номер реле, параметр, 362

Номер, параметр,

Камера, 248

O

Область визуальной настройки,

Рабочий стол, 196

Область детектирования, параметр,

Детектор расфокусировки, 280

Область отображения,

Карта, 203

Обновить конфигурацию, кнопка,

Точка интеграции, 525

Объект охраны, объект, описание, 149

Обязательное соответствие пароля требованиям к сложности, параметр,

Объект охраны, 156

Ограничить FPS живого видео, параметр,

Медиа Клиент, 327

Одна Камера с переключением потоков, параметр,

Медиа Клиент, 320

ОК (Отмена), параметр, 288

Окно приложения (необязательно), параметр,

Внешнее окно, 213

Окно результата отладки сценария (Консоль), параметр,

Скрипт Node.js, 398

Окно сценария, параметр,

Скрипт Node.js, 398

Омывающее устройство, параметр,

Камера, 250

Описание, параметр,

SIP-устройство, 387

Оповещать об окончании срока действия пароля за (дней), параметр,

Объект охраны, 156

Освещение, параметр,

Камера, 251

Основная камера, параметр,

SIP-устройство, 387

От кого, параметр, 376

От, До, параметры,

Расписание, 392

Отдел, объект, описание, 159

Отключить NAT hole punching, параметр,

Устройство видеозахвата Generic RTSP, 272

Отключить локальный протокол, параметр, 174

Отключить при наличии Протокола событий, параметр, 379

Отключить скрипт (режим редактирования), параметр,

Скрипт Node.js, 398

Отображать идентификатор Камеры, параметр,

Медиа Клиент, 320

Отображать идентификатор Медиа Клиента, параметр,

Медиа Клиент, 320

Отображать Камеры в Медиа Клиенте и фильтровать объекты СКУД/ОПС при активации Уровня, параметр,

Карта: Интерфейс оператора, 210

Отображать Макрокоманду в контекстном меню выбранных Камер, параметр,

Макрокоманда, 395

Отображать только выбранные препозиции, параметр,

Камера, 264

Отображение, параметр,

Камера, 249

Отправитель, параметр,

Сервис почтовых сообщений, 375

Отправить Карточку в Службу реагирования, параметр,

Медиа Клиент, 336

Протокол событий, 212

Очистить, параметр, 287

П

- Панель инструментов администратора, 82
- Панель ракладок, параметр,
 - Медиа Клиент, 325
- Панель управления поворотным устройством, параметр,
 - Медиа Клиент, 319
- Параметры, параметр, 395
 - Внешнее приложение, 191
- Пароль доступа, параметр,
 - Удаленная система, 477
- Пароль сертификата, параметр,
 - ONVIF-сервер, 312
- Пароль, параметр,
 - Подсистема SIP, 385
 - Пользователь, 160
 - Устройство аудиозахвата, 356
 - Устройство видеозахвата, 245
- Период аудита, параметр,
 - Система, 149
- Период бездействия до окончания драки, параметр,
 - Нейросетевой детектор драк, 457
- Период детекции, параметр,
 - Детектор людей без касок, 454
- Период проверки, параметр,
 - Детектор расфокусировки, 281
- Периодичность уведомления о количестве людей, параметр,
 - Нейросетевой счетчик людей, 468
- Печать кадров, параметр,
 - Медиа Клиент, 320
- Плагин Tracking Kit III, объект, описание, 410
- Поворотное устройство, параметр,
 - Камера, 249
- Подключение сторонним отладчиком, параметр,
 - Скрипт Node.js, 398
- Подключение через IP-адрес, параметр,
 - Скрипт Node.js, 398
- Подключиться, кнопка,
 - База данных, 157
- Подсветка ближней/средней/дальней зоны, параметр,
 - Камера, 269
- Подтвердите новый пароль, параметр,
 - Система, 146
- Поиск, поле,
 - Карта, 203
- Показывать все зоны, параметр, 287
- Показывать список уровней, параметр,
 - Карта: Интерфейс оператора, 210
- Показывать тревожные уровни, параметр,
 - Карта: Интерфейс оператора, 210
- Полный FPS во время тревоги, параметр,
 - Камера, 258
- Получить препозиции, кнопка,
 - Камера, 264
- Получить список IQN, кнопка,
 - iSCSI-диск, 504
- Пользователи и группы, обладающие этими правами, параметр, 166
- Пользователь и пароль, параметр,
 - iSCSI-диск, 504
- Пользователь, объект, описание, 160
- Пользователь, параметр,
 - Подсистема SIP, 385
 - Устройство аудиозахвата, 356
 - Устройство видеозахвата, 245
- Пользователь/Пароль, параметры,
 - Служба реагирования, 381
- Пользовательские Раскладки, параметр,
 - Медиа Клиент, 322
- Порог детекции касок, параметр,
 - Детектор людей без касок, 454
- Порог детекции людей, параметр,
 - Детектор людей без касок, 454
- Порог длительного пребывания в зоне, параметр,
 - Детектор пребывания в зоне, 442
- Порог кратковременного пребывания в зоне, параметр,
 - Детектор пребывания в зоне, 442
- Порог тревоги, параметр,
 - Детектор людей без касок, 454
- Порог уверенности (дым), параметр,
 - Нейросетевой детектор дыма и огня, 459
- Порог уверенности (огонь), параметр,
 - Нейросетевой детектор дыма и огня, 459
- Порог уверенности, параметр,
 - Нейросетевой детектор драк, 457
 - Нейросетевой детектор уклонения от оплаты, 464
 - Нейросетевой детектор упавших людей, 466
 - Нейросетевой счетчик людей, 468
- Порог, параметр, 358
- Порт HTTP, параметр,
 - RTSP-сервер, 307
- Порт RTSP, параметр,
 - ONVIF-сервер, 313
 - RTSP-сервер, 307
- Порт TCP, параметр,
 - Подсистема SIP, 385
- Порт UDP, параметр,
 - Подсистема SIP, 386
- Порт для Мультикастной группы, параметр,
 - Камера, 255

- Порт, параметр,
 - Active Directory / LDAP, 163
 - MCC DC HTTP Proxy, 475
 - ONVIF-сервер, 311
 - REST API, 402
 - База данных, 158
 - Компьютерное зрение, 406
 - Перемещаемый PostgreSQL, 506
 - Подсистема SIP, 385
 - Сервис почтовых сообщений, 374
- Порт для WebSocket, параметр,
 - REST API, 402
- После завершения тревоги не скрывать Камеру, параметр,
 - Медиа Клиент, 318
- Постзапись, параметр,
 - Микрофон, 358
- Поток 1, параметр,
 - Камера, 252
- Поток 2, параметр,
 - Камера, 252
- Поток 3, параметр,
 - Камера, 252
- Почтовое сообщение, объект, описание, 375
- права на запись архива,
 - выдача права пользователю, 233
- Права пользователей, объект,
 - Настройки для провайдера LDAP, 118
 - Настройки для провайдера Windows NT, 117
- Права пользователя, объект, описание, 163
- Права, параметр, 164
- Праздничные дни, параметр,
 - Объект охраны, 151
 - Расписание, 392
- Преобразование адресов, параметр,
 - Удаленная система, 478
- Препозиция камеры, параметр,
 - SIP-устройство, 387
- При старте запускать Макрокоманду, параметр, 151
- Привилегированный доступ к Удаленным системам, параметр,
 - Система, 147
- Приложение, параметр,
 - Внешнее окно, 213
 - Внешнее приложение, 191
- Приложить SecurOS Evidence Manager, параметр,
 - Конвертер архива, 292
- Примеры настройки, 342
 - Видеосервер и Рабочее место оператора, 343
 - домен для провайдера LDAP, 118
 - домен для провайдера Windows NT, 117
 - одиночная конфигурация, 342
- Принимать только TLS-подключения, параметр,
 - Система, 149
- Принудительное переключение камеры в ночной режим, параметр,
 - Камера, 270
- Приоритет архивов, параметр, 295
- Приоритет события, параметр,
 - Детектор бега, 428
 - Детектор движения в запрещенном направлении, 431
 - Детектор дыма, 451
 - Детектор людей без касок, 454
 - Детектор оставленных и унесенных предметов (Детектор оставленных предметов), 435
 - Детектор оставленных и унесенных предметов (Детектор унесенных предметов), 435
 - Детектор пересечения линии, 437
 - Детектор праздного шатания, 439
 - Детектор пребывания в зоне, 442
 - Детектор проникновения в запрещенную зону, 443
 - Детектор скопления людей, 446
 - Нейросетевой детектор драк, 456
 - Нейросетевой детектор дыма и огня, 458
 - Нейросетевой детектор праздного шатания, 461
 - Нейросетевой детектор уклонения от оплаты, 463
 - Нейросетевой детектор упавших людей, 465
 - Счетчик объектов, 448
- Приоритет события. параметр,
 - Нейросетевой счетчик людей, 467
- Приоритет управления телеметрией, параметр, 166
- Провайдер, параметр, 162
- Провайдеры, параметр, 166
- Проверка подключения, кнопка,
 - iSCSI-диск, 505
 - База данных, 158
- Прокси-сервер для FaceX, параметр,
 - Система, 147
- Прокси-сервер, параметр,
 - Удаленная система, 479
- Прореживание видео, параметр, 296
- Прореживание, макс. FPS, параметр,
 - Камера, 258
- Прореживать на сервере, параметр, 296
- Просмотр архива, хранящегося на удаленном устройстве, параметр,
 - Камера, 259
- Просмотр, параметр,
 - Устройство видеозахвата, 245
- Протокол PTZ, параметр,
 - Камера, 263

Протокол оmyивающего устройства / дворника,
параметр,
 Камера, 273
Протокол событий, объект, описание, 211
Протокол, параметр,
 ONVIF-сервер, 311
 Камера, 254
 Реле, 362
 Устройство аудиозахвата, 356
 Устройство видеозахвата, 242
Протоколирование работы SecurOS, 118
Профиль экспорта архива, объект, описание, 298
Профиль, параметр,
 Камера, 253
Прошивка, параметр,
 Устройство видеозахвата, 246
Путь, параметр,
 Камера, 254

Р

Работа с событиями из разных часовых поясов,
параметр,
 Протокол событий, 212
Работать с АТС, параметр,
 Подсистема SIP, 385
Работать с Видами, параметр,
 Медиа Клиент, 325
Работать с Картой: Интерфейс оператора, параметр,
 HTML5 FrontEnd, 214
Работать с Медиа Клиентом, параметр,
 HTML5 FrontEnd, 214
 Карта: Интерфейс оператора, 210
 Протокол событий, 212
Работать со звуком, параметр,
 Медиа Клиент, 334
Работать согласно выбранному Расписанию,
параметр, 281
 Камера, 262
Работать только с указанными глобальными Видами,
параметр,
 Медиа Клиент, 325
Работать только с указанными Камерами, параметр,
 Медиа Клиент, 327
Работать только с указанными Микрофонами,
параметр,
 Медиа Клиент, 334
Рабочая директория, параметр,
 Внешнее приложение, 191
Рабочий стол, объект, описание, 195
Разделять на файлы размером, параметр, 292
Размер базы протокола (дней), параметр, 151
Размер буфера, параметр,
 Камера, 250
Размер, параметр,
 Зона, 287
 Камера, 262
Размещать Камеру на текущей раскладке/виде
одинарным щелчком мыши, параметр,
 Медиа Клиент, 336
Разрешить воспроизведение кадров BinaryPack,
параметр,
 Устройство видеозахвата Virtual, 271
Разрешить выполнять аудит системы, параметр, 165
Разрешить доступ, параметр,
 Система, 146
Разрешить запрашивать доступ к PTZ, параметр,
165
Разрешить конфигурирование системы, параметр,
165
Разрешить незащищенные соединения, параметр,
 Система, 149
Разрешить редактирование глобальных Видов,
параметр,
 Медиа Клиент, 325
Разрешить редактирование контрольных списков
FaceX, параметр, 165
Разрешить сброс пароля через e-mail при
авторизации, параметр,
 Объект охраны, 156
Разрешить смену пароля через Панель управления,
параметр,
 Объект охраны, 156
Разрешить удерживать управление телеметрией,
параметр, 165
Раскладка, объект, описание, 282
Раскрывать имя пользователя при удержании
управления PTZ, параметр, 165
Расписание, объект, описание, 390
Расписание, параметр,
 Архиватор, 300
Расположение камеры, параметр,
 Камера, 273
Расположение, параметр,
 Конвертер архива, 297
Реакция оператора на тревожное событие, параметр,
212
Редактор регистрационных файлов (ddi.exe),
утилита, 568
Режим WDR, параметр,
 Интегратор ONVIF, 267
Режим администрирования, 76
Режим архивирования, параметр,
 Архиватор, 300
Режим записи, параметр,
 Камера, 257
Режим ожидания, параметр,
 Камера, 276

Режим работы ИК-фильтра, параметр,
Интегратор ONVIF, 267
Режим работы подсветки, параметр,
Камера, 269
Режим работы, параметр,
Медиа Клиент, 316
Режим совместимости диапазонов, параметр,
Камера, 254
Режим, параметр,
Детектор людей без касок, 453
Детектор оставленных и унесенных предметов,
434
Детектор проникновения в запрещенную зону,
445
Резервировать Видеосервер и добавить его в кластер,
параметр,
Компьютер, 173
Резкость, параметр,
Интегратор ONVIF, 266
Реле, объект, описание, 362
Роль Компьютера, параметр, 173
Ручная настройка экспозиции, параметр,
Интегратор ONVIF, 266

С

Световой детектор, объект, описание, 288
Связан с Камерой, параметр,
Микрофон, 358
Сдвиг по вертикали, пк, параметр,
Камера, 276
Сдвиг по горизонтали, пк, параметр,
Камера, 275
Секционировать таблицы базы данных, параметр,
Database Partitioner, 192
Сервер, параметр,
Active Directory / LDAP, 163
База данных, 158
Сервер/Порт, параметры,
Служба реагирования (RTSP-сервер), 381
Служба реагирования (WebView), 381
Сервис для отправки кодов сброса пароля, параметр,
Объект охраны, 156
Сервис для отправки одноразовых кодов доступа,
параметр, 165
Сервис звукового оповещения, объект, описание,
378
Сервис коротких сообщений, объект, описание, 377
Сервис почтовых сообщений, объект, описание, 373
Серийный номер камеры, параметр,
Камера, 274
Сертификат и ключ, параметр,
ONVIF-сервер, 311
Сетевой интерфейс, параметр,
ONVIF-сервер, 311
Сетка, параметр,
Раскладка, 283
Сигнал вызова, параметр,
SIP: Интерфейс оператора, 389
Сигнал, параметр,
Камера, 261
Микрофон, 357
Система, объект, описание, 145
Скорость (ширина человека в секунду), параметр,
Детектор бега, 429
Скорость загрузки относительно FPS, параметр,
Камера, 260
Скрыть кнопку запуска Макрокоманды на Панели
управления, параметр,
Макрокоманда, 395
Скрыть Макрокоманды в меню Камер, параметр,
Медиа Клиент, 337
Служба реагирования, объект, описание, 379
Собственный сигнал вызова, параметр,
SIP: Интерфейс оператора, 389
Событие, параметр,
Макрокоманда, 395
Создать БД и Пользователя, кнопка,
База данных, 159
Создать новую, кнопка,
База данных, 157
Создать новый уровень, кнопка,
Карта, 203
Сообщение, параметр,
Короткое сообщение, 378
Почтовое сообщение, 376
Сохранение кадров, параметр,
Медиа Клиент, 320
Сохранить в файл, кнопка,
Служба реагирования, 382
Сохранить, кнопка,
Система, 147
Сохранять координаты движения (для Умного
поиска), параметр, 286
Сохранять порядок Камер после перезапуска,
параметр,
Медиа Клиент, 337
Список препозиций, параметр,
Камера, 264
Список IP-адресов, параметр,
Интерфейс IIDK, 400
Список Видов, параметр,
Медиа Клиент, 325
Список типов происшествий, параметр,
Служба реагирования, 381
Список Устройств, параметр,
Медиа Клиент, 319

Стандартные раскладки, параметр,
 Медиа Клиент, 322
суперпользователь, 107
Сценарий поведения, объект, описание, 187
Считать большой объект группой объектов,
 параметр,
 Счетчик объектов, 449

Т

Телефон, параметр,
 Короткое сообщение, 378
 Пользователь, 160
Тема, параметр, 376
Термометр, объект, описание, 522
техническая поддержка,
 обращение, 13
 подготовка служебной информации, 600
 утилита сбора системной информации, 540
Тип тура, параметр,
 Камера, 264
Тип устройства, параметр, 362
Тип файла, параметр, 292
Тип, параметр,
 База данных, 158
 Луч, 361
 Макрокоманда (Действия), 395
 Макрокоманда (События), 395
 Устройство аудиозахвата, 356
 Устройство видеозахвата, 242
Типы зон, параметр, 286
Точка интеграции, объект, описание, 525
Точка останова на первой инструкции, параметр,
 Скрипт Node.js, 398
Требовать смену пароля при следующем входе в
 систему, параметр,
 Пользователь, 161
Требуется аутентификация, параметр, 374
Тревога при обнаружении, параметр,
 Нейросетевой детектор дыма и огня, 459
Тревога, если количество людей более, параметр,
 Нейросетевой счетчик людей, 468
Тревожная, параметр, 286
Турникет частично скрыт от камеры, параметр,
 Нейросетевой детектор уклонения от оплаты,
 464

У

Удаленная система, объект, описание, 476
Удалить, кнопка,
 Архиватор, 301
Удалять вместе с оперативным архивом, параметр,
175

Удалять записи старше, параметр,
 База данных, 158
Удалять изображения автомобилей старше,
 параметр,
 Database Partitioner, 192
Удалять результаты распознавания старше,
 параметр,
 Database Partitioner, 192
Удалять спустя, параметр,
 Архиватор, 302
 Камера, 258
Управление записью, параметр,
 Медиа Клиент, 319
Управление поворотным устройством с помощью
 мышы, параметр,
 Медиа Клиент, 320
Управление тревожным режимом Камеры,
 параметр,
 Медиа Клиент, 319
Уровень WDR, параметр,
 Интегратор ONVIF, 267
уровень доступа,
 доступ запрещен, 167
 конфигурирование, 167
 наследуемые права, 168
 полный доступ, 167
 просмотр, 167
 управление, 167
Уровень компенсации засветки, параметр,
 Интегратор ONVIF, 267
Уровень переключения режима день/ночь,
 параметр,
 Камера, 269
Усиление, параметр, 275, 357
 Интегратор ONVIF, 266
 Камера, 261
Условие срабатывания, параметр,
 Луч, 361
Устройство аудиозахвата, объект, описание, 355
Устройство видеозахвата, объект, описание, 241
Устройство, параметр, 377
Утилита AuditClient,
 Интерфейс оператора, настройка, 589
Утилита настройки подключений к БД
 (dsadmin.exe), 562
Утилита обновления БД (idb.exe), 565
учетная запись,
 postgres, 73

Ф

Файл прошивки, параметр,
 Устройство видеозахвата, 246
Фильтр по положению тела, параметр,

Фильтр по положению тела, параметр,
 Нейросетевой детектор праздношатания, 461
Фильтр событий, параметр,
 Удаленная система, 478
Фильтр, параметр,
 SIP-устройство, 387
Фильтрация ложных срабатываний, кнопка,
 Детектор людей без касок, 455
Фильтрация ложных срабатываний, параметр,
 Нейросетевой детектор праздношатания, 461
Фильтрация объектов в СКУД/ОПС: Интерфейсе
оператора, параметр,
 Карта: Интерфейс оператора, 210
Формат пиксельных данных, параметр,
 Камера, 273
Формат, параметр,
 Устройство видеозахвата, 243

Х

Хранить не менее, параметр,
 Камера, 258
Хранить, параметр, 175

Ц

Цвет текста, параметр,
 Карта, 202
Центрирование кадра по выбранной точке,
параметр,
 Интегратор ONVIF, 268
Цифровой зум, параметр,
 Медиа Клиент, 319

Ч

Частота, параметр,
 Камера, 261
 Устройство аудиозахвата, 356
Чувствительность, параметр,
 Детектор движения в запрещенном
 направлении, 432
 Детектор дыма, 452
 Световой детектор, 289

Ш

Шаблон имени, параметр, 293
Ширина кадра, пк, параметр,
 Камера, 275
Широкоформатные раскладки, параметр,
 Медиа Клиент, 322
Шифрование, параметр,
 Сервис почтовых сообщений, 375
Шлюз MCC DC, объект, описание, 474

Шлюз для доступа к видео, параметр,
 Удаленная система, 479

Э

экспорт,
 аудио, 558
экспорт,
 видео, 557
Экспортировать в, параметр, 292
Экспортировать видео со звуком, параметр, 296

Я

Яркость, параметр,
 Интегратор ONVIF, 266