



Industrial Security Incident Manager версия 6.1

Руководство администратора

© Positive Technologies, 2026.

Настоящий документ является собственностью Positive Technologies и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения Positive Technologies.

Документ может быть изменен без предварительного уведомления.

Товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям.

Дата редакции документа: 14.09.2026

Содержание

1.	Об этом документе.....	9
1.1.	Условные обозначения.....	9
1.2.	Другие источники информации о PT ISIM.....	10
2.	О PT ISIM.....	11
2.1.	Архитектура PT ISIM.....	12
2.2.	Редакции PT ISIM View Sensor.....	13
2.3.	Принцип работы PT ISIM.....	15
2.3.1.	Алгоритм обработки трафика.....	15
2.3.2.	Безопасность хранения и передачи данных.....	16
3.	Аппаратные и программные требования.....	17
3.1.	Аппаратные требования.....	17
3.2.	Программные требования.....	24
3.3.	Требования для импорта ISO-образа.....	27
3.4.	Требования к сети.....	28
3.5.	Требования к программному и аппаратному обеспечению конечного устройства.....	33
3.6.	Расчет потребления ресурсов агентом на конечном устройстве.....	35
4.	Лицензирование.....	41
4.1.	Жизненный цикл лицензии.....	41
4.2.	Расширение лицензии.....	42
5.	Развертывание PT ISIM.....	44
5.1.	Установка и обновление ОС.....	44
5.1.1.	Установка Debian 10.....	44
5.1.2.	Установка Debian 12.....	58
5.1.3.	Обновление Debian.....	72
5.1.4.	Установка Astra Linux.....	75
5.1.5.	Обновление Astra Linux.....	90
5.2.	Установочный комплект.....	92
5.3.	Установка PT ISIM View Sensor.....	92
5.3.1.	Подготовка к установке PT ISIM View Sensor.....	92
5.3.2.	Установка PT ISIM View Sensor на физическом сервере.....	93
5.3.3.	Установка PT ISIM View Sensor на удаленном сервере.....	94
5.3.4.	Установка PT ISIM View Sensor в виртуальной среде.....	95
5.3.4.1.	Установка PT ISIM View Sensor на Oracle VM VirtualBox.....	96
5.3.4.2.	Установка PT ISIM View Sensor на VMware vSphere.....	97
5.3.4.3.	Установка PT ISIM View Sensor на VMware Workstation.....	98
5.3.5.	Первоначальная настройка PT ISIM View Sensor.....	99
5.3.5.1.	Настройка сетевых интерфейсов PT ISIM View Sensor.....	100
5.3.5.2.	Активация лицензии PT ISIM View Sensor.....	101
5.3.5.3.	Проверка работоспособности продукта.....	102
5.4.	Установка PT ISIM Endpoint.....	103
5.4.1.	Подготовка к установке PT ISIM Endpoint.....	103
5.4.2.	Процедура установки PT ISIM Endpoint.....	104
5.4.3.	Первоначальная настройка PT ISIM Endpoint.....	107

5.4.4.	Активация лицензии PT ISIM Endpoint	108
5.5.	Установка PT ISIM Collector	110
5.5.1.	Процедура установки PT ISIM Collector	110
5.5.2.	Первоначальная настройка PT ISIM Collector	111
5.5.3.	Активация лицензии коллектора	111
5.6.	Установка PT ISIM Overview Center	111
5.6.1.	Подготовка к установке PT ISIM Overview Center	112
5.6.2.	Установка PT ISIM Overview Center на физическом сервере	112
5.6.3.	Установка PT ISIM Overview Center на удаленном сервере	113
5.6.4.	Установка PT ISIM Overview Center в виртуальной среде	114
5.6.4.1.	Установка PT ISIM Overview Center на Oracle VM VirtualBox	115
5.6.4.2.	Установка PT ISIM Overview Center на VMware vSphere	116
5.6.4.3.	Установка PT ISIM Overview Center на VMware Workstation	117
5.6.5.	Первоначальная настройка PT ISIM Overview Center	118
5.6.5.1.	Первоначальная настройка PT ISIM Overview Center в веб-интерфейсе	118
5.6.5.2.	Подключение PT ISIM Overview Center к серверу обновлений	119
5.7.	Установка PT ISIM Industrial Tablet на виртуальную машину или промышленный планшет	120
5.8.	Порядок установки PT ISIM View Sensor, PT ISIM Endpoint и PT MC на один сервер	122
5.9.	Изменение IP-адреса сервера PT ISIM в параметрах компонентов для конфигурации all-in-one	124
6.	Обновление PT ISIM	125
6.1.	Обновление PT ISIM View Sensor	125
6.2.	Централизованное обновление узлов View Sensor с помощью Overview Center	126
6.2.1.	Настройка автоматического обновления узлов View Sensor с помощью Overview Center	127
6.2.2.	Обновление узлов View Sensor с помощью Overview Center в офлайн-режиме	128
6.3.	Обновление PT ISIM Endpoint	129
6.4.	Обновление PT ISIM Collector	131
6.5.	Обновление PT ISIM Overview Center	131
6.6.	Обновление PT ISIM Industrial Tablet	132
6.7.	Обновление экспертной базы PT ISTI	133
6.7.1.	Обновление PT ISTI в веб-интерфейсе PT ISIM View Sensor	134
6.7.2.	Обновление PT ISTI на узле PT ISIM View Sensor из консоли	135
6.7.3.	Централизованное обновление базы PT ISTI с помощью Overview Center	136
6.7.3.1.	Загрузка PT ISTI с помощью внешнего носителя	137
6.7.3.2.	Ручной запуск обновления PT ISTI на узлах View Sensor	137
6.7.3.3.	Настройка автоматического обновления PT ISTI на узлах View Sensor	138
6.8.	Обновление антивирусных баз и пакета экспертизы в PT ISIM Endpoint	138
6.9.	Изменение адреса сервера обновлений	139
7.	Администрирование PT ISIM	141
7.1.	Администрирование PT ISIM View Sensor	141
7.1.1.	Управление учетными записями пользователей в PT ISIM View Sensor	142
7.1.1.1.	О ролях пользователей	143
7.1.1.2.	Создание учетной записи пользователя	147
7.1.1.3.	Изменение учетной записи пользователя	149
7.1.1.4.	Распечатка данных учетной записи	149
7.1.1.5.	Просмотр и выгрузка журнала действий пользователей	149

7.1.1.6.	Блокировка учетной записи пользователя	150
7.1.1.7.	Настройка временной блокировки пользователя при авторизации	150
7.1.2.	Подключение к PT MC	151
7.1.2.1.	Установка доверенного SSL-сертификата	152
7.1.2.2.	Настройка подключения PT ISIM View Sensor к PT MC	152
7.1.3.	Настройка ротации данных	153
7.1.4.	Настройка параметров хранения PCAP	154
7.1.5.	Настройка интеграции с MaxPatrol VM	155
7.1.6.	Настройка работы с syslog-сервером	156
7.1.6.1.	Настройка отправки сообщений об инцидентах в syslog	157
7.1.6.2.	Настройка приемки сообщений об инцидентах на удаленном syslog-сервере	158
7.1.6.3.	Настройка отправки сообщений о событиях на локальный syslog-сервер ..	159
7.1.6.4.	Настройка отправки сообщений о событиях на удаленный syslog-сервер ..	161
7.1.7.	Настройка почтовых уведомлений об инцидентах	164
7.1.8.	Изменение информации о системе и контактном лице	165
7.1.9.	Включение и отключение оценки уязвимостей	165
7.1.10.	Создание пакета регистрации PT ISIM View Sensor для подключения к PT ISIM Overview Center	166
7.1.11.	Отключение извлечения файлов из трафика	167
7.1.12.	Настройка интеграции с PT Sandbox для проверки файлов	168
7.1.13.	Настройка приема данных от PT ISIM Endpoint	169
7.1.14.	Диагностика состояния PT ISIM View Sensor	170
7.1.14.1.	Просмотр состояния сетевых интерфейсов	170
7.1.14.2.	Просмотр состояния служб и основных параметров системы	171
7.1.14.3.	Просмотр журналов служб	174
7.1.14.4.	Скачивание пакета диагностической информации	174
7.1.15.	Мониторинг использования ресурсов	174
7.1.16.	Контроль целостности файлов	175
7.1.16.1.	Генерация эталонных хеш-сумм	175
7.1.16.2.	Проверка целостности файлов	176
7.1.16.3.	Просмотр и изменение списка проверяемых файлов	176
7.1.17.	Замена SSL-сертификата	177
7.1.18.	Настройка ERSPAN-приемника	178
7.1.19.	Миграция данных модели сети в ручном режиме	179
7.1.20.	Удаление неиспользуемых файлов модели сети	180
7.1.21.	Проверка целостности цифровой подстанции по стандарту МЭК-61850	180
7.1.21.1.	Загрузка файла с эталонными данными для проверки целостности	181
7.1.21.2.	Выявляемые события и регистрируемые инциденты	181
7.1.22.	Экспорт и импорт конфигурации PT ISIM	182
7.1.22.1.	Экспорт конфигурации	183
7.1.22.2.	Импорт конфигурации	184
7.1.23.	Импорт внешнего проекта	185
7.1.23.1.	Особенности импорта проекта СУИК	186
7.1.23.2.	Особенности импорта проекта SCD	186
7.1.24.	Работа с пользовательскими правилами межсетевого экрана	189

7.1.25.	Утилита iptablesctl	189
7.1.26.	Утилита ISIMCTL	191
7.1.26.1.	Системные проверки	191
7.1.26.2.	Работа с инцидентами	192
7.1.26.3.	Работа с хранилищем событий ClickHouse	192
7.1.26.4.	Работа с моделью сети	193
7.1.26.5.	Работа с PCAP-файлами	193
7.1.26.6.	Работа с сетевыми параметрами	193
7.1.26.7.	Работа с PostgreSQL	194
7.1.26.8.	Работа с сенсором	194
7.1.26.9.	Работа с Updater	194
7.2.	Администрирование PT ISIM Endpoint	194
7.2.1.	Работа с агентами	195
7.2.1.1.	Об агентах	195
7.2.1.2.	Установка агента	196
7.2.1.3.	Авторизация агента	198
7.2.1.4.	Обновление агента	200
7.2.1.5.	Блокировка агента	200
7.2.1.6.	Удаление агента	200
7.2.2.	Работа с политиками	201
7.2.3.	Настройка промышленной экспертизы	203
7.2.3.1.	Пакет экспертизы для ПО «Атомик Софт»	204
7.2.3.2.	Пакет экспертизы для ПО «МПС Софт»	206
7.2.3.3.	Пакет экспертизы для ПО AdAstra	208
7.2.3.4.	Пакет экспертизы для ПО AVEVA	209
7.2.3.5.	Пакет экспертизы для ПО Honeywell	210
7.2.3.6.	Пакет экспертизы для ПО Siemens	211
7.2.3.7.	Пакет экспертизы для ПО Yokogawa	212
7.2.3.8.	Настройка аудита файловой системы для папки Windows	213
7.2.4.	Настройка сканирования в режиме аудита	215
7.2.5.	Настройка антивирусной защиты узлов	216
7.2.6.	Изоляция подозрительных файлов	218
7.3.	Администрирование PT ISIM Collector	219
7.3.1.	Включение приема данных от коллекторов	220
7.3.2.	Добавление коллектора в PT ISIM View Sensor	221
7.3.3.	Обновление секретных ключей	222
7.3.4.	Скачивание конфигурации коллектора в PT ISIM View Sensor	222
7.3.5.	Загрузка конфигурации на коллектор	222
7.3.6.	Настройка коллектора для работы с PT ISIM Endpoint	223
7.3.7.	Настройка параметров хранения копии трафика на коллекторе	223
7.3.8.	Удаление коллектора из PT ISIM View Sensor	224
7.4.	Администрирование PT ISIM Overview Center	224
7.4.1.	Управление учетными записями пользователей в PT ISIM Overview Center	225
7.4.1.1.	О ролях пользователей	226
7.4.1.2.	Создание роли	228

7.4.1.3.	Изменение роли.....	228
7.4.1.4.	Настройка доступа к узлам ISIM.....	228
7.4.1.5.	Удаление роли.....	229
7.4.1.6.	Создание учетной записи пользователя.....	229
7.4.1.7.	Изменение учетной записи пользователя.....	230
7.4.1.8.	Скачивание журнала действий пользователей.....	230
7.4.1.9.	Блокировка учетной записи пользователя.....	231
7.4.1.10.	Настройка временной блокировки пользователя при авторизации.....	231
7.4.2.	Подключение к PT MC.....	231
7.4.2.1.	Настройка подключения PT ISIM Overview Center к PT MC.....	232
7.4.2.2.	Установка доверенного SSL-сертификата.....	233
7.4.3.	Настройка провайдера карт в Overview Center.....	233
7.4.3.1.	Настройка онлайн-провайдера карт.....	234
7.4.3.2.	Настройка офлайн-провайдера карт.....	235
7.4.4.	Настройка отправки сообщений об инцидентах в syslog.....	235
7.4.5.	Настройка приемки сообщений об инцидентах на удаленном syslog-сервере.....	237
7.4.6.	Изменение информации о системе и контактном лице.....	238
7.4.7.	Подключение узлов ISIM к PT ISIM Overview Center.....	238
7.4.7.1.	Загрузка пакета регистрации.....	239
7.4.7.2.	Активация пакета регистрации.....	240
7.4.7.3.	Удаление подключенных узлов.....	240
7.4.7.4.	Создание пакета регистрации Overview Center.....	241
7.4.8.	Утилита резервного копирования.....	243
7.4.8.1.	Выбор таблиц с инцидентами для резервного копирования.....	243
7.4.8.2.	Подключение к СУБД PostgreSQL.....	244
7.4.8.3.	Подключение к удаленному узлу по SSH.....	245
7.4.8.4.	Снятие резервной копии данных с локального узла Overview Center.....	246
7.4.8.5.	Снятие резервной копии данных с удаленного узла Overview Center.....	249
7.4.8.6.	Восстановление данных локального узла Overview Center из резервной копии.....	251
7.4.8.7.	Восстановление данных удаленного узла Overview Center из резервной копии.....	251
7.5.	Администрирование PT ISIM Industrial Tablet.....	252
7.5.1.	Настройка интерфейса PT ISIM Industrial Tablet.....	252
7.5.2.	Смена пароля для доступа в PT ISIM Industrial Tablet.....	253
7.5.3.	Изменение IP-адреса сервера для подключения PT ISIM Industrial Tablet к сенсору.....	255
8.	Удаление PT ISIM.....	256
8.1.	Удаление PT ISIM View Sensor.....	256
8.2.	Удаление PT ISIM Endpoint.....	256
8.3.	Удаление PT ISIM Collector.....	257
9.	Решение проблем.....	258
9.1.	Ошибка при обновлении из-за неразрешенных зависимостей.....	258
9.2.	Проблема с выявлением узлов сети.....	259
9.3.	Отсутствие событий в веб-интерфейсе.....	260
9.4.	Отсутствие данных в разделе Диагностика.....	262
9.5.	Ошибки при настройке сетевых интерфейсов.....	263

9.6.	Настройка ограничений GOOSE-событий.....	264
9.7.	Инцидент «Очистка очереди RabbitMQ»	265
9.8.	Чрезмерная загрузка диска запросами на запись статистики.....	266
9.9.	Большое потребление ресурсов сервера антивирусом	267
9.10.	Ошибка unable to resolve host.....	268
9.11.	Ошибка при установке Debian.....	269
9.12.	Установка PT ISIM прерывается на шаге Processing step rules.....	270
10.	О технической поддержке	271
Приложение А. Типы узлов		275
Приложение Б. Формат syslog-сообщений об инцидентах.....		277
Глоссарий.....		279

1. Об этом документе

Руководство администратора содержит справочную информацию и инструкции по развертыванию, настройке и администрированию Positive Technologies Industrial Security Incident Manager (далее также — PT ISIM). Руководство не содержит инструкций по использованию основных функций продукта.

Руководство адресовано специалистам, выполняющим установку, первоначальную настройку и администрирование PT ISIM.

В этом разделе

[Условные обозначения \(см. раздел 1.1\)](#)

[Другие источники информации о PT ISIM \(см. раздел 1.2\)](#)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите OK	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду <i>Stop-Service</i>	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о PT ISIM

Вы можете найти дополнительную информацию о PT ISIM на справочном портале help.ptsecurity.com и на [Позитивном портале](#). Через Позитивный портал вы также можете обратиться [в техническую поддержку](#) (см. раздел 10).

2. О PT ISIM

Positive Technologies Industrial Security Incident Manager (далее также — PT ISIM) — система обеспечения киберустойчивости промышленных инфраструктур.

PT ISIM состоит из нескольких программных компонентов (см. раздел 2.1) и позволяет:

- обнаруживать действия злоумышленников;
- отслеживать действия пользователей АСУ ТП;
- контролировать сетевое окружение за счет идентификации сетевых устройств и обнаружения подключения новых устройств;
- анализировать события технологической сети — осуществляет контроль сетевого взаимодействия, использования вредоносного ПО, уязвимых сетевых компонентов и протоколов;
- отслеживать нелегитимное изменение конфигураций — изменения файлов конфигураций SCADA-систем и контроллеров, попытки изменения системных параметров и нелегитимного использования веб-интерфейсов устройств;
- осуществлять контроль конечных узлов — выполнять сбор данных из системных журналов аудита и журналов ПО, отслеживать изменения в файловой системе или конфигурации узла и реагировать на обнаруженные угрозы ИБ;
- автоматически информировать сотрудников предприятия об обнаруженных инцидентах безопасности;
- определять источники и причины возникновения инцидентов, их возможные последствия и меры по устранению;
- выполнять требования регулирующих организаций и другие требования по обеспечению безопасности АСУ ТП и промышленных объектов критической информационной инфраструктуры.

Выполнение перечисленных функций достигается за счет анализа копии сетевого трафика и сбора и анализа данных с конечных устройств, а также активного опроса конечных устройств сети предприятия.

PT ISIM также может поставляться в составе программно-аппаратных комплексов (ПАК PT ISIM) моделей NS-1050 и NS-2010. Руководства по эксплуатации ПАК PT ISIM доступны для скачивания на сайте storage.ptsecurity.com.

В этом разделе

[Архитектура PT ISIM \(см. раздел 2.1\)](#)

[Редакции PT ISIM View Sensor \(см. раздел 2.2\)](#)

[Принцип работы PT ISIM \(см. раздел 2.3\)](#)

2.1. Архитектура PT ISIM

Система PT ISIM состоит из программных компонентов, которые вы можете размещать как на одном, так и на нескольких серверах (см. типовые схемы развертывания).

Компонент PT ISIM View Sensor

Основной компонент системы. Выполняет сбор и анализ копии сетевого трафика, обработку, хранение и визуализацию событий безопасности, выявленных в трафике и на конечных узлах. Может использоваться как самостоятельное решение без применения других компонентов.

PT ISIM View Sensor — обобщенное название трех редакций (см. раздел 2.2) сенсора:

- PT ISIM microView Sensor;
- PT ISIM netView Sensor;
- PT ISIM proView Sensor.

Компонент PT ISIM Endpoint

Набор приложений для сбора и передачи в PT ISIM View Sensor (напрямую или через PT ISIM Collector) данных о конечных устройствах. PT ISIM Endpoint включает:

- PT ISIM Endpoint Agent (далее также — агент). Позволяет обнаруживать события безопасности на конечных узлах технологической сети и собирать данные об их конфигурации.
- PT ISIM Endpoint Server. Приложение для сбора данных PT ISIM Endpoint Agent и передачи их в PT ISIM View Sensor.
- PT ISIM Endpoint Management. Предоставляет интерфейс для управления распределенными агентами PT ISIM Endpoint, назначения им политик безопасности, настройки расписания работы сервисов и выполнения иных административных задач.

Компонент PT ISIM Collector

PT ISIM Collector (далее также — коллектор) предназначен для сбора и анализа трафика в отдельном сегменте сети АСУ ТП и передачи полученных данных в PT ISIM. PT ISIM Collector имеет встроенный сетевой сканер, позволяющий собирать данные с конечных узлов и передавать их в PT ISIM View Sensor. PT ISIM Collector также может получать данные от PT ISIM Endpoint для их дальнейшей передачи в PT ISIM View Sensor.

Компонент позволяет снизить нагрузку на PT ISIM View Sensor и подходит для установки в удаленных сегментах сети. Не имеет веб-интерфейса.

Компонент PT ISIM Overview Center

Компонент для централизованного мониторинга инцидентов и нарушений на подключенных к нему узлах View Sensor.

Узлы View Sensor могут быть подключены к Overview Center напрямую или через другие узлы Overview Center. Вы можете выстраивать иерархию узлов и назначать права доступа к ним с учетом привилегий пользователей.

PT ISIM Overview Center также позволяет централизованно обновлять узлы View Sensor и экспертную базу PT ISTI.

Компонент PT ISIM Industrial Tablet

Версия PT ISIM View Sensor с упрощенным интерфейсом для работы в режиме информационного киоска с возможностью установки на виртуальную машину или промышленный планшет.

Компонент Positive Technologies Management and Configuration

Positive Technologies Management and Configuration (далее также — PT MC) обеспечивает сервис единого входа в веб-интерфейсы перечисленных компонентов и других продуктов Positive Technologies.

Подробная информация о PT MC представлена [в справке к продукту](#). Поддерживаемые версии PT MC указаны [в программных требованиях](#) (см. раздел 3.2).

2.2. Редакции PT ISIM View Sensor

Таблица 2. Функциональные возможности редакций PT ISIM View Sensor

Функция	microView Sensor	netView Sensor	proView Sensor
Автоматическое построение карты узлов и их сетевого взаимодействия, контроль подключений к сети в реальном времени	+	+	+
Авторизация узлов, изменение их параметров, объединение узлов и распределение в группы и контейнеры	+	+	+
Возможность автоматической авторизации всех новых узлов и разрешения всех новых соединений (режим обучения)	+	+	+
Поддержка промышленных протоколов	+	+	+
Статистика узлов, соединений, инцидентов	+	+	+
Визуализация, корреляция и анализ цепочек событий безопасности, обнаруженных в сетевом трафике, на конечных узлах и технологических сигналах	+	+	+

Функция	microView Sensor	netView Sensor	proView Sensor
Инструменты поиска и фильтрации узлов, соединений и инцидентов	+	+	+
Регистрация, хранение, поиск, группировка, фильтрация событий, а также выгрузка списка событий в виде CSV-файла	–	+	+
Отслеживание нарушений	+	+	+
Визуализация инцидентов и нарушений на схеме сети	+	+	+
Просмотр схемы сети, параметров узлов и соединений за выбранный период	+	+	+
Управление списком разрешенных соединений	+	+	+
Включение и отключение правил обнаружения атак	+	+	+
Создание пользовательских правил обнаружения атак	+	+	+
Выгрузка списка инцидентов и узлов в виде CSV-файла	+	+	+
Хранение и выгрузка копии трафика, относящегося к периоду, соединению или инциденту	+	+	+
Ролевая модель (см. раздел 7.1.1.1) пользователей, история действий (см. раздел 7.1.1.5)	+	+	+
Отправка (см. раздел 7.1.5) результатов сканирования в MaxPatrol VM	–	–	+
Передача (см. раздел 7.1.6.1) сообщений об инцидентах на syslog-сервер	+	+	+
Отправка (см. раздел 7.1.7) почтовых уведомлений об инцидентах	+	+	+
Контроль параметров технологических процессов (технологических сигналов)	+	+	+
Проверка (см. раздел 7.1.21) целостности цифровой подстанции по стандарту МЭК-61850	–	–	+
Использование коллекторов в сегментах АСУ ТП для сбора и анализа трафика и передачи событий в PT ISIM View Sensor	–	+	+
Интеграция с PT ISIM Overview Center	+	+	+

Функция	microView Sensor	netView Sensor	proView Sensor
Интеграция с PT ISIM Endpoint	+	+	+
Сбор данных сетевым сканером с конечных узлов	–	–	+
Обнаружение и оценка уязвимостей на узлах	–	–	+
Поддержка программно-аппаратного комплекса PT ISIM	NS-1050	NS-2010	

2.3. Принцип работы PT ISIM

Ниже приводится основная информация о принципе работы PT ISIM.

В этом разделе

[Алгоритм обработки трафика \(см. раздел 2.3.1\)](#)

[Безопасность хранения и передачи данных \(см. раздел 2.3.2\)](#)

2.3.1. Алгоритм обработки трафика

PT ISIM анализирует сетевой трафик и выявляет в нем инциденты информационной безопасности. Обработка трафика в PT ISIM происходит в несколько этапов:

1. Сбор — захват трафика со SPAN-порта коммутатора и анализ сообщений общесетевых и промышленных протоколов. Исходная копия трафика сохраняется на жестком диске сервера в формате PCAP.
2. Разбор — извлечение информации из сетевых пакетов и создание JSON-документов, пригодных для нормализации. Трафик независимо друг от друга разбирают следующие компоненты, каждый из которых отвечает за свой набор протоколов: служба ptdpi — за протоколы стека TCP/IP, служба ptisim-peony — за фреймовые Ethernet-протоколы.
3. Нормализация — извлечение данных из атрибутов JSON-документов, которые могут иметь разный формат, и приведение их к единому формату нормализованных сообщений. Формат нормализованного сообщения позволяет однозначно определить основные параметры события, отнести его к определенному узлу и устройству, а также провести дальнейший анализ события на основе значений отдельных полей.
4. Фильтрация — удаление сообщений, не представляющих интереса с точки зрения информационной безопасности.
5. Корреляция — проверка потока событий на соответствие определенному правилу. Когда правило срабатывает, регистрируется корреляционное событие.

6. Моделирование анализируемой системы — составление актуальной карты вычислительной сети, отражающей ее реальный состав и взаимодействие между узлами.
7. Заведение записей об инцидентах и нарушениях. PT ISIM проверяет, подходит ли корреляционное событие или событие службы моделирования под правило заведения инцидентов или нарушений. Если подходит — заводит соответствующие записи об инцидентах или нарушениях.

2.3.2. Безопасность хранения и передачи данных

Безопасность хранения и передачи данных при работе с PT ISIM имеет два аспекта:

- Исключается любое воздействие PT ISIM на технологические процессы предприятия, поскольку для сбора трафика PT ISIM подключается к SPAN-портам коммутаторов через диод данных. Подобное решение делает невозможной передачу данных от PT ISIM в сеть АСУ ТП как при нормальной работе продукта, так и в случае непредвиденного изменения параметров коммутатора или PT ISIM.
- Используются следующие инструменты обеспечения собственной безопасности PT ISIM:
 - Компонент ptisim-secure, который настраивает межсетевой экран таким образом, что запрещаются любые входящие соединения из внешней сети, кроме TCP-соединений на порты 22, 80, 443 и ICMP-соединений (эхо-запросов).
 - Служба watchdog, которая перезапускает остановленные службы продукта, а также очищает дисковое пространство, удаляя устаревшие PCAP-файлы и журналы.
 - Защищенное соединение с веб-интерфейсом пользователя по HTTPS, а также перенаправление запросов, адресованных порту 80 (HTTP), на порт 443 (HTTPS).
 - Мониторинг состояния PT ISIM. Потенциально опасные действия в отношении самого продукта (подбор пароля по SSH, HTTP) и важные изменения состояния (перезагрузка сервера, отключение от сети) фиксируются в виде инцидентов.

3. Аппаратные и программные требования

PT ISIM может быть установлен как на физическом сервере, так и в виртуальной среде.

В этом разделе приводятся требования для обоих вариантов установки: для физического сервера, на который планируется устанавливать продукт, а также для хостового сервера, на который планируется импортировать ISO-образ продукта.

В этом разделе

[Аппаратные требования \(см. раздел 3.1\)](#)

[Программные требования \(см. раздел 3.2\)](#)

[Требования для импорта ISO-образа \(см. раздел 3.3\)](#)

[Требования к сети \(см. раздел 3.4\)](#)

[Требования к программному и аппаратному обеспечению конечного устройства \(см. раздел 3.5\)](#)

[Расчет потребления ресурсов агентом на конечном устройстве \(см. раздел 3.6\)](#)

3.1. Аппаратные требования

В таблицах ниже приведены требования к аппаратному обеспечению, необходимому для установки и работы PT ISIM.

При работе с таблицами этого раздела следует учитывать следующее:

- Если процессор использует технологию Hyper-Threading, количество его логических ядер вдвое больше числа физических. Без этой технологии логических ядер столько же, сколько физических.
- Процессор должен поддерживать расширение Advanced Vector Extensions (AVX).

PT ISIM microView Sensor

Таблица 3. Сервер PT ISIM microView Sensor

	Слабонагруженная инсталляция
Компоненты PT ISIM	
Обязательные компоненты	PT ISIM microView Sensor
Опциональные компоненты	PT ISIM Endpoint; PT MC
Обработка трафика	
Скорость обработки трафика	До 10 Мбит/с

Слабонагруженная инсталляция

PT ISIM Endpoint	
Количество агентов PT ISIM Endpoint, подключенных в режиме «Антивирус»	До 100
Количество агентов PT ISIM Endpoint, подключенных с функциональностью сбора данных на конечных узлах (событий из журналов и данных о конфигурации узлов)	До 10
Средний поток событий в секунду от одного агента PT ISIM Endpoint	3
Частота аудита на агенте PT ISIM Endpoint	Один раз в сутки

Минимальные аппаратные требования

Центральный процессор	Логические ядра: 16. Частота: 2,1 ГГц или выше. Семейство: Intel Atom	Логические ядра: 8. Частота: 2,1 ГГц или выше. Семейство: Intel Core i5
Память (ОЗУ)	32 ГБ DDR4	
Дисковое пространство	480 ГБ SSD	
Сетевой адаптер	Порты для захвата трафика: 1 (или более) × 1 Гбит/с. Порты для внутреннего взаимодействия: 1 × 1 Гбит/с	
Исполнение в виде ПАК	NS-1050	—

PT ISIM netView Sensor

Таблица 4. Сервер PT ISIM netView Sensor

	Средненагруженная инсталляция	Высоконагруженная инсталляция
Компоненты PT ISIM		
Обязательные компоненты	PT ISIM netView Sensor	
Опциональные компоненты	PT ISIM Endpoint;	

	Средненагруженная инсталляция	Высоконагруженная инсталляция
	PT MC	
Обработка трафика		
Скорость обработки трафика	До 100 Мбит/с	До 500 Мбит/с
PT ISIM Endpoint		
Количество агентов PT ISIM Endpoint, подключенных в режиме «Антивирус»	До 500	
Количество агентов PT ISIM Endpoint, подключенных с функциональностью сбора данных на конечных узлах (событий из журналов и данных о конфигурации узлов)	До 100	
Средний поток событий в секунду от одного агента PT ISIM Endpoint	3	
Частота аудита на агенте PT ISIM Endpoint	Один раз в сутки	Один раз в час
Подключение PT ISIM Collector		
Число подключенных коллекторов	До 100	
Скорость обработки трафика, количество агентов PT ISIM Endpoint и сканируемых узлов	Соответствуют общим ограничениям инсталляции PT ISIM netView Sensor	
Минимальные аппаратные требования		
Центральный процессор	Логические ядра: 8. Частота: 2,1 ГГц или выше. Семейство: Intel Xeon или Core i7	Логические ядра: 32. Частота: 2,1 ГГц или выше. Семейство: Intel Xeon или Core i7
Память (ОЗУ)	32 ГБ DDR4	64 ГБ DDR4
Дисковое пространство	Варианты конфигурации: — 1 ТБ SSD;	

	Средненагруженная инсталляция	Высоконагруженная инсталляция
	– 1 ТБ SSD и 4 ТБ HDD. Дополнительный HDD используется для хранения PCAP-файлов. Это позволяет увеличить общее время хранения событий, статистики и PCAP-файлов, а также повысить стабильность работы ОС	
Сетевой адаптер	Порты для захвата трафика: 1 (или более) × 1 Гбит/с. Порты для внутреннего взаимодействия: 1 × 1 Гбит/с	
Исполнение в виде ПАК	—	NS-2010

PT ISIM proView Sensor

Таблица 5. Сервер PT ISIM proView Sensor

	Средненагруженная инсталляция	Высоконагруженная инсталляция
Компоненты PT ISIM		
Обязательные компоненты	PT ISIM proView Sensor	
Опциональные компоненты	PT ISIM Endpoint; PT MC	
Обработка трафика		
Скорость обработки трафика	До 100 Мбит/с	До 500 Мбит/с
PT ISIM Endpoint		
Количество агентов PT ISIM Endpoint, подклю- ченных в режиме «Антиви- рус»	До 500	
Количество агентов PT ISIM Endpoint, подклю- ченных с функционально- стью сбора данных на конеч- ных узлах (событий из жур- налов и данных о configura- ции узлов)	До 100	
Средний поток событий в се- кунду от одного агента PT ISIM Endpoint	3	

	Средненагруженная инсталляция	Высоконагруженная инсталляция
Частота аудита на агенте PT ISIM Endpoint	Один раз в сутки	Один раз в час
Анализ уязвимостей		
Возможность анализа уязви- мостей на просканирован- ных узлах	—	Есть. Необходимые условия: — 10 ГБ свободной оперативной памяти для работы службы оценки уязвимостей; — 10 ГБ свободного места на SSD для распаковки базы уязвимостей
Сканирование методом активного опроса с помощью встроенного сетевого сканера		
Количество одновременно сканируемых узлов	5	10
Общее число сканируемых узлов	До 100	
Частота сканирования	Один раз в сутки	Один раз в час
Подключение PT ISIM Collector		
Число подключенных кол- лекторов	До 100	
Скорость обработки трафи- ка, количество агентов PT ISIM Endpoint и сканируе- мых узлов	Соответствуют общим ограничениям инсталляции PT ISIM proView Sensor	
Минимальные аппаратные требования		
Центральный процессор	Логические ядра: 8. Частота: 2,1 ГГц или выше. Семейство: Intel Xeon или Core i7	Логические ядра: 32. Частота: 2,1 ГГц или выше. Семейство: Intel Xeon или Core i7
Память (ОЗУ)	32 ГБ DDR4	64 ГБ DDR4
Дисковое пространство	Варианты конфигурации: — 1 ТБ SSD; — 1 ТБ SSD и 4 ТБ HDD.	

	Средненагруженная инсталляция	Высоконагруженная инсталляция
	Дополнительный HDD используется для хранения PCAP-файлов. Это позволяет увеличить общее время хранения событий, статистики и PCAP-файлов, а также повысить стабильность работы ОС	
Сетевой адаптер	Порты для захвата трафика: 1 (или более) × 1 Гбит/с. Порты для внутреннего взаимодействия: 1 × 1 Гбит/с	
Исполнение в виде ПАК	—	NS-2010

PT ISIM Collector

Таблица 6. Сервер PT ISIM Collector

	Слабонагруженная инсталляция	Средненагруженная инсталляция	
Компоненты PT ISIM			
Обязательные компоненты	PT ISIM Collector		
Опциональные компоненты	PT ISIM Endpoint; PT MC		
Обработка трафика			
Скорость обработки трафика	До 50 Мбит/с		До 100 Мбит/с
PT ISIM Endpoint			
Количество агентов PT ISIM Endpoint, подключенных в режиме «Антивирус»	—	До 100	До 500
Количество агентов PT ISIM Endpoint, подключенных с функциональностью сбора данных на конечных узлах (событий из журналов и данных о конфигурации узлов)		До 10	До 100
Средний поток событий в секунду от одного агента PT ISIM Endpoint		3	
Частота аудита на агенте PT ISIM Endpoint		Один раз в сутки	Один раз в час

	Слабонагруженная инсталляция	Средненагруженная инсталляция	
Сканирование методом активного опроса с помощью встроенного сетевого сканера			
Количество одновременно сканируемых узлов	—	2	5
Общее число сканируемых узлов	—	Соответствуют ограничениям инсталляции proView Sensor или netView Sensor, куда коллектор передает данные	
Частота сканирования			
Минимальные аппаратные требования			
Центральный процессор	Rockchip RK3588 (ARM архитектура)	Логические ядра: 16. Частота: 2,1 ГГц или выше. Семейство: Intel Atom	Логические ядра: 8. Частота: 2,1 ГГц или выше. Семейство: Intel Xeon или Core i7
		Логические ядра: 8. Частота: 2,1 ГГц или выше. Семейство: Intel Core i5	
Память (ОЗУ)	32 ГБ DDR4	32 ГБ DDR4	64 ГБ DDR4
Дисковое пространство	— 480 ГБ SSD для ОС и PT ISIM Collector; — 1—4 ТБ HDD для хранения PCAP-файлов		
Сетевой адаптер	Порты для захвата трафика: 1 (или более) × 1 Гбит/с. Порты для внутреннего взаимодействия: 1 × 1 Гбит/с		
Исполнение в виде ПАК	—	NS-1050	—

PT ISIM Overview Center

Таблица 7. Сервер Overview Center

Компоненты PT ISIM	
Обязательные компоненты	PT ISIM Overview Center
Опциональные компоненты	PT MC

Требования к инфраструктуре

Количество подключенных узлов microView Sensor, netView Sensor, proView Sensor	До 100
Количество подключенных узлов Overview Center	До 10

Минимальные аппаратные требования

Центральный процессор	Логические ядра: 32. Частота: 2,1 ГГц или выше. Семейство: Intel Xeon или Core i7
Память (ОЗУ)	64 ГБ DDR4
Дисковое пространство	1 ТБ SSD
Сетевая карта	Порты для внутреннего взаимодействия: 1 × 1 Гбит/с
Исполнение в виде ПАК	NS-2010

3.2. Программные требования

Общие программные требования:

- В параметрах даты и времени операционной системы указан часовой пояс по шкале UTC.
- Установлено актуальное время.

Для удаленного подключения к серверу продукта рекомендуется использовать SSH-клиент: OpenSSH или PuTTY.

Требования к операционной системе

PT ISIM совместим с 64-разрядными серверными версиями следующих операционных систем:

- Debian 10.12.0 Buster.
- Debian 12.8.0 Bookworm.
- Astra Linux Special Edition 1.7.6 UU2 в режиме защищенности «Воронеж» или «Смоленск».

Рекомендуется устанавливать PT ISIM на чистую операционную систему.

Операционная система должна содержать раздел и файл подкачки, равный 32 ГБ.

Вы можете скачать образы для установки Debian по ссылкам в таблице ниже или на сайте [deb.debian.org](https://deb.debian.org/debian), дистрибутив операционной системы Astra Linux приобретается отдельно.

Перед установкой операционной системы рекомендуется сверить контрольную сумму образа дистрибутива с указанной в таблице, чтобы убедиться, что скачана верная версия.

Таблица 8. Контрольные суммы образов дистрибутивов

Операционная система	Образ дистрибутива	Контрольная сумма образа (MD5)
Debian 10.12.0 Buster	debian-10.12.0-amd64-DVD-1.iso	45929e2426cf7fece1fb73d563e75026
Debian 11.11.0	debian-11.11.0-amd64-DVD-1.iso Версия не поддерживается PT ISIM и используется только при обновлении Debian (см. раздел 5.1.3)	3caf8ce03d39f8363357beae179a27ae
Debian 12.8.0 Bookworm	debian-12.8.0-amd64-DVD-1.iso	109c1125c7e022f218c97582ac7f054b
Astra Linux Special Edition 1.7.6 UU2	installation-1.7.6.15-1 5.11.24_17.20.iso	d0193cd8b1995be0d732918bbe0d4bf0

В таблице ниже содержатся сведения о поддерживаемых ОС в зависимости от установленных на одном сервере компонентов PT ISIM.

Таблица 9. Совместимость версий ОС и установленных компонентов

Компоненты	Debian 10.12.0 Buster	Debian 12.8.0 Bookworm	Astra Linux SE 1.7.6 UU2 («Воронеж», «Смоленск»)
PT ISIM View Sensor	+	+	+
PT ISIM Overview Center	+	+	+
PT ISIM Industrial Tablet	+	+	+
PT MC	–	+	+
PT ISIM Endpoint	+	+	+
PT ISIM Endpoint + PT ISIM View Sensor + PT MC	–	+	+
PT ISIM Endpoint + PT ISIM View Sensor	+	+	+
PT ISIM Endpoint + PT MC	–	+	+
PT ISIM View Sensor + PT MC	–	+	+
PT ISIM Overview Center + PT MC	–	+	+

Совместимость с предыдущими версиями и другими продуктами

Далее приведены данные о совместимости PT ISIM версии 6.1 с предыдущими версиями PT ISIM и другими продуктами.

Таблица 10. Таблица совместимости версии 6.1 с предыдущими

Компонент	Версии	Поддерживаемые функции
PT ISIM View Sensor	5.1–6.0 (только на узлах с Debian 10, Debian 12 и Astra Linux 1.7.6)	Обновление (см. раздел 6.1) до версии 6.1 инсталлятором
	5.9 ¹ , 5.10–6.0 (только на узлах с Debian 10, Debian 12 и Astra Linux 1.7.6)	Обновление (см. раздел 6.2.1) до версии 6.1 с помощью PT ISIM Overview Center (все узлы PT ISIM Overview Center в иерархии должны быть обновлены до версии 5.1 или выше)
	5.1–6.1	Подключение (см. раздел 7.4.7) к PT ISIM Overview Center версии 6.1
	5.1–6.1	Обновление базы PT ISTI (см. раздел 6.7.3) с помощью PT ISIM Overview Center версии 6.1
	6.1	Импорт (см. раздел 7.1.22) конфигурации PT ISIM следующих версий: — 5.4–6.1 (импорт узлов, групп, контейнеров и разрешений соединений); — 5.11–6.1 (импорт представлений и исключений из правил обнаружения атак); — 5.12–6.1 (импорт инцидентов и связанных с ними событий)
PT ISIM Overview Center	5.1–6.0 (только на узлах с Debian 10, Debian 12 и Astra Linux 1.7.6)	Обновление (см. раздел 6.5) до версии 6.1 инсталлятором

¹ На узлы PT ISIM View Sensor версии 5.9 требуется вручную установить deb-пакет, который вы можете получить в службе технической поддержки Positive Technologies.

[Централизованное обновление \(см. раздел 6.2\)](#) PT ISIM View Sensor версий ниже 5.9 до версии 6.1 возможно только после их промежуточного обновления до версии 5.9 (вручную или с помощью PT ISIM Overview Center) и установки deb-пакета на узлы PT ISIM View Sensor версии 5.9 вручную.

Компонент	Версии	Поддерживаемые функции
PT ISIM Industrial Tablet	5.1—6.0 (только на узлах с Debian 10, Debian 12 и Astra Linux 1.7.6)	Обновление (см. раздел 6.6) до версии 6.1 инсталлятором

Обновление компонентов версии 4.5 до версии 6.1 возможно только с обязательным промежуточным обновлением до одной из версий 5.1—5.11. При обновлении PT ISIM View Sensor 4.5 до версии 5.8, 5.9, 5.10 или 5.11 требуется выполнить миграцию данных модели сети [вручную \(см. раздел 7.1.19\)](#).

При обновлении PT ISIM View Sensor версий ниже 6.0 до версии 6.0 или выше ранее сохраненные PCAP-файлы будут удалены. Это связано с изменением механизмов сохранения копии трафика в версии 6.0. Если требуется сохранить такие PCAP-файлы, перенесите их до начала обновления в другой каталог. После обновления PT ISIM View Sensor рекомендуется [настроить хранение PCAP-файлов \(см. раздел 7.1.4\)](#).

Таблица 11. Таблица совместимости PT ISIM версии 6.1 с другими продуктами

Продукт	Версии	Поддерживаемые функции
MaxPatrol VM	27.6.39922	Отправка результатов сканирования (см. раздел 7.1.5) в MaxPatrol VM
MaxPatrol SIEM	27.6.39922	Отправка инцидентов (см. раздел 7.1.6.1) информационной безопасности из PT ISIM View Sensor
PT MC	101.20.19012	Управление учетными записями пользователей и применение технологии единого входа в PT ISIM View Sensor, PT ISIM Overview Center
PT Sandbox	5.35.1.152178	Проверка файлов (см. раздел 7.1.12) , извлеченных PT ISIM View Sensor из трафика, на угрозы информационной безопасности

Требования к браузеру

Для работы в интерфейсе PT ISIM рекомендуется использовать один из следующих браузеров:

- Google Chrome версии 98 или выше;
- Mozilla Firefox версии 94 или выше.

3.3. Требования для импорта ISO-образа

В этом разделе описаны поддерживаемые гипервизоры и приведены требования к хостовому серверу для импорта ISO-образа.

Поддерживаемые гипервизоры

Вы можете импортировать ISO-образ с помощью следующих гипервизоров:

- VMware Workstation версий 14.1.5, 15.0.0, 15.0.2, 15.5.1, 17.0;
- VMware vSphere версии 7.0.3.01900;
- Oracle VM VirtualBox версий 5.1.38, 5.2.26, 6.0.4, 6.0.14, 7.0.4.

Требования к хостовому серверу

Сервер, на котором планируется развертывать ISO-образ, должен иметь возможность выделить виртуальной машине не меньше ресурсов, чем указано в приемлемой конфигурации. Объем дискового пространства, занимаемый виртуальной машиной, ограничен [аппаратными требованиями \(см. раздел 3.1\)](#).

Требования к сетевым интерфейсам для компонентов PT ISIM приведены в разделе [о требованиях к сети \(см. раздел 3.4\)](#).

3.4. Требования к сети

Для корректной работы компонентов PT ISIM требуются сетевые интерфейсы:

- Сервисный интерфейс (или интерфейс управления) — для предоставления пользователям доступа к веб-интерфейсу продукта (по HTTPS) и к его серверу (по SSH), а также для сбора данных с конечных узлов и для связи с агентами PT ISIM Endpoint. Требуется для всех компонентов PT ISIM.
- Технологический интерфейс — для получения копии трафика, зеркалируемого из анализируемой технологической сети. Технологический интерфейс должен входить в виртуальный интерфейс bond и, если для получения копии трафика используется сетевой мост, работать в неразборчивом режиме (promiscuous mode). Требуется [настроить \(см. раздел 5.3.5.1\)](#) только для PT ISIM View Sensor и PT ISIM Collector.

Требования к сети для PT ISIM View Sensor

Между сервером продукта и браузером, используемым для работы в веб-интерфейсе, должен быть разрешен обмен данными по WebSocket.

По умолчанию служба ptisim-firewall настраивает межсетевой экран сервера, на котором установлен продукт, таким образом, что разрешаются только ICMP-соединения и соединения с минимальным набором портов, необходимых PT ISIM: ICMP type 8 (IP) для отправки ICMP-сообщений типа «эхо-запрос» с целью проверки связи с другими узлами и порты, перечисленные в таблице ниже. Соединения по портам 25, 587 (TCP) разрешаются автоматически при настройке почтовых уведомлений об инцидентах, по порту 514 (TCP) — при настройке отправки [сообщений в syslog \(см. раздел 7.1.6.1\)](#).

Для портов, указанных в интерфейсе продукта при настройке соединения со службами syslog, SMTP, PT MC, разрешения в цепочках INPUT и OUTPUT правил фильтрации будут добавлены автоматически. Если изменить порты в параметрах настройки взаимодействия с указанными службами, будут созданы разрешения для новых портов взамен предыдущих. Если требуется, вы также можете [добавлять собственные правила ptisim-firewall \(см. раздел 7.1.24\)](#). На уровне вашего сетевого оборудования указанные порты должны быть также разрешены.

Внимание! Не рекомендуется вносить изменения в правила, поставляемые вместе с PT ISIM. При обновлении продукта эти правила будут также обновлены, а внесенные изменения утрачены. Пользовательские правила и правила, автоматически созданные при настройке взаимодействия с сервисами, при обновлении продукта не меняются и остаются включенными.

Таблица 12. Используемые порты и типы взаимодействия для PT ISIM View Sensor

Порт (транспортный протокол)	Узел, с которым осуществляется взаимодействие	Описание взаимодействия	Характеристика взаимодействия
22 (TCP)	PT ISIM	Подключение к серверу по SSH-протоколу	Двустороннее (с участием пользователя)
25, 587 (TCP)	SMTP-сервер	Отправка данных об инцидентах с помощью почтовых сообщений, отправляемых на SMTP-сервер. Соединение разрешается автоматически при настройке взаимодействия	Одностороннее (без участия пользователя)
53 (UDP)	DNS-сервер	Преобразования доменных имен в IP-адреса	Одностороннее (без участия пользователя)
80, 443 (TCP)	PT ISIM	Доступ к веб-интерфейсу PT ISIM и синхронизация данных с PT ISIM Overview Center	Двустороннее (с участием пользователя)
443 (TCP)	Сервер обновлений	Доступ к серверу обновлений для загрузки обновлений	Двустороннее (с участием пользователя)

Порт (транспортный протокол)	Узел, с которым осуществляется взаимодействие	Описание взаимодействия	Характеристика взаимодействия
123 (UDP)	NTP-сервер	Синхронизация времени на узле сенсора через удаленный NTP-сервер	Одностороннее (без участия пользователя)
514 (TCP, UDP)	Другие серверы (например, MaxPatrol SIEM)	Передача данных об инцидентах с помощью syslog-протокола. Соединение разрешается автоматически при настройке взаимодействия	Одностороннее (без участия пользователя)
2222 (TCP)	PT ISIM Overview Center	Синхронизация пакетов обновлений сенсора с PT ISIM Overview Center	Одностороннее (без участия пользователя)
3334 (TCP)	PT MC	Соединение сенсора с PT MC. Соединение разрешается автоматически при успешном подключении	Одностороннее (без участия пользователя)
Порт, указанный при настройке интеграции (см. раздел 7.1.5) с MaxPatrol VM (TCP)	MaxPatrol VM	Соединение сенсора с MaxPatrol VM. Соединение разрешается автоматически при настройке взаимодействия	Одностороннее (без участия пользователя)
Порт, указанный при настройке интеграции (см. раздел 7.1.12) с PT Sandbox (TCP)	PT Sandbox	Соединение сенсора с PT Sandbox. Соединение разрешается автоматически при настройке взаимодействия	Двустороннее (без участия пользователя)
Порт, указанный при включении приема данных от коллекторов (см. раздел 7.3.1) (TCP, UDP)	PT ISIM Collector	Соединение коллектора с сенсором. Соединение разрешается автоматически при настройке взаимодействия	Одностороннее (без участия пользователя)

Порт (транспортный протокол)	Узел, с которым осуществляется взаимодействие	Описание взаимодействия	Характеристика взаимодействия
Порт, указанный в задаче типа Syslog на сбор данных (TCP, UDP)	Источник данных	Передача данных с помощью syslog-протокола. Соединение разрешается автоматически при настройке взаимодействия	Одностороннее (без участия пользователя)

Требования к сети для PT ISIM Endpoint

Для работы PT ISIM Endpoint и агентов требуется открыть порты, указанные в таблицах, для входящих и исходящих соединений.

Таблица 13. Используемые порты и типы взаимодействия для PT ISIM Endpoint

Порт (транспортный протокол)	Узел, с которым осуществляется взаимодействие	Описание взаимодействия	Характеристика взаимодействия
3334 (TCP)	PT MC	Соединение PT ISIM Endpoint с PT MC	Одностороннее (без участия пользователя)
4443 (TCP)	PT ISIM Endpoint	Доступ к веб-интерфейсу PT ISIM Endpoint	Двустороннее (с участием пользователя)
6192 (TCP, UDP)	PT ISIM View Sensor	Передача событий и данных сканирования в режиме аудита конечных узлов от PT ISIM Endpoint на сенсор или коллектор	Одностороннее (без участия пользователя)
	PT ISIM Collector		
8443 (TCP)	Агент PT ISIM Endpoint	Передача данных о событиях и данных сканирования в режиме аудита от конечного узла в PT ISIM Endpoint. Передача данных для работы агента (например, модулей политик) от PT ISIM Endpoint на конечный узел.	Двустороннее (без участия пользователя)

Порт (транспортный протокол)	Узел, с которым осуществляется взаимодействие	Описание взаимодействия	Характеристика взаимодействия
		Соединение разрешается автоматически при установке PT ISIM Endpoint на одном сервере с PT ISIM View Sensor	

Таблица 14. Используемые порты и типы взаимодействия для агента PT ISIM Endpoint

Порт (транспортный протокол)	Узел, с которым осуществляется взаимодействие	Описание взаимодействия	Характеристика взаимодействия
8443 (TCP)	PT ISIM Endpoint	Передача данных о событиях и данных сканирования в режиме аудита от конечного узла в PT ISIM Endpoint	Двустороннее (без участия пользователя)
		Передача данных для работы агента (например, модулей политик) от PT ISIM Endpoint на конечный узел	

Требования к сети для PT ISIM Overview Center

Для работы в PT ISIM Overview Center требуется открыть порты, указанные в таблице, для входящих и исходящих соединений.

Таблица 15. Используемые порты и типы взаимодействия для Overview Center

Порт (транспортный протокол)	Узел, с которым осуществляется взаимодействие	Описание взаимодействия	Характеристика взаимодействия
22 (TCP)	PT ISIM Overview Center	Подключение к серверу по SSH-протоколу	Двустороннее (с участием пользователя)
80, 443 (TCP)	PT ISIM Overview Center	Доступ к веб-интерфейсу PT ISIM Overview Center	Двустороннее (с участием пользователя)

Порт (транспортный протокол)	Узел, с которым осуществляется взаимодействие	Описание взаимодействия	Характеристика взаимодействия
443 (TCP)	Сервер обновлений (см. раздел 5.6.5.2)	Доступ к серверу обновлений для загрузки обновлений	Двустороннее (с участием пользователя)
443 (TCP)	PT ISIM View Sensor	Синхронизация данных с подключенными узлами View Sensor	Двустороннее (без участия пользователя)
514 (TCP, UDP)	Другие серверы (например, MaxPatrol SIEM)	Передача данных об инцидентах с помощью syslog-протокола	Одностороннее (без участия пользователя)
2222 (TCP)	PT ISIM Overview Center из иерархии (нижестоящий) или View Sensor	Синхронизация пакетов обновлений узлов View Sensor	Одностороннее (без участия пользователя)
3334 (TCP)	PT MC	Соединение PT ISIM Overview Center с PT MC	Одностороннее (без участия пользователя)

3.5. Требования к программному и аппаратному обеспечению конечного устройства

В этом разделе приведены требования к программному и аппаратному обеспечению конечных устройств для корректной работы PT ISIM Endpoint.

Программные требования

Агент поддерживает установку на конечные устройства под управлением следующих операционных систем:

- Windows 7, 8.1, 10, 11 (только редакции Pro);
- Windows Server 2016, 2019, 2022, 2025;
- Debian 10, 11, 12, 13;
- Astra Linux Special Edition 1.7 («Орел», «Воронеж»), 1.8 («Орел», «Воронеж»);
- Astra Linux Common Edition 2.12 («Орел»);
- AlterOS Desktop 7.5;
- CentOS Stream 9, Stream 10;
- Oracle Linux 9;

- Red Hat Enterprise Linux 9, 10;
- Ubuntu 20.04 LTS, 22.04 LTS, 24.04 LTS, 25.04 LTS;
- «Альт Сервер» 9, 10.2, 10.4;
- «Альт Рабочая станция» 10.2, 10.4;
- «ОСнова» 2.0 «Оникс»;
- «РЕД ОС Рабочая станция» 7.3, 8.0.

Внимание! В текущей версии PT ISIM Endpoint невозможно сканирование в режиме аудита на узлах под управлением следующих ОС: Windows 11, Astra Linux Common Edition 2.12 («Орел»), «РЕД ОС Рабочая станция» 7.3, AlterOS Desktop 7.5, «ОСнова» 2.0 «Оникс», «Альт Сервер» 9, 10.2, 10.4 и «Альт Рабочая станция» 10.2, 10.4.

Внимание! В текущей версии PT ISIM Endpoint невозможна установка модуля антивирусной защиты на узлах под управлением следующих ОС: Windows 7 (редакция Pro), CentOS Stream 9 и Stream 10, «Альт Сервер» 10.2 и 10.4, «Альт Рабочая станция» 10.4.

Примечание. Если на конечном устройстве под управлением Linux нет доступа к пакетным менеджерам, то для корректной установки и работы агента в ОС должны быть установлены пакеты `libpthread`, `libnsl` и `libcrypto`.

На момент установки [модуля антивирусной защиты \(см. раздел 7.2.5\)](#) на конечном устройстве под управлением Linux необходимо наличие перечисленных ниже пакетов. Если на конечном устройстве есть доступ к интернету, эти пакеты будут установлены автоматически. Список пакетов:

- для модуля антивирусной защиты на узлах под управлением Debian-подобных ОС:
 - `gcc-multilib`;
 - `libayatana-appindicator3-1`;
 - `libnotify4`;
- модуля антивирусной защиты на узлах под управлением «РЕД ОС»:
 - `glibc-devel.i686`;
 - `gtk3`;
 - `libatomic.i686`;
 - `libayatana-appindicator-gtk3` (не требуется для «РЕД ОС» 7);
 - `libnotify`.

Аппаратные требования

Агенты необходимо устанавливать на конечные устройства, удовлетворяющие приведенным ниже аппаратным требованиям.

Таблица 16. Аппаратные требования к конечному устройству

Компонент	Минимальные требования	Рекомендуемые требования
Центральный процессор	Тактовая частота 2,2 ГГц, суммарно 2 логических ядра. Поддержка инструкций SSE4.2 и AES-NI (например, процессоры Intel Westmere или новее)	Тактовая частота 2,2 ГГц, суммарно 4 логических ядра. Поддержка инструкций SSE4.2 и AES-NI
Память (ОЗУ)	Зависит от установленных модулей, количества обрабатываемых событий и ряда других факторов (см. раздел 3.6)	
Сетевой адаптер	От 200 Кбит/с	От 5 Мбит/с
Жесткий диск (HDD) или твердотельный накопитель (SSD)	От 500 МБ	От 1000 МБ

3.6. Расчет потребления ресурсов агентом на конечном устройстве

Потребление агентом ресурсов на конечном устройстве зависит от установленных модулей, количества обрабатываемых событий и ряда других факторов. В целях оптимизации потребления ресурсов нужно при настройке политик придерживаться следующих рекомендаций:

- В модулях сбора необходимо использовать фильтры и исключать события, не представляющие интереса с точки зрения информационной безопасности.
- Для каждой группы конечных устройств, на которых установлено нестандартное ПО, необходимо использовать отдельные политики, в которых учтены особенности такого ПО.
- Модуль «YARA-сканер» при сканировании резервирует память, соизмеримую с размером проверяемого файла или процесса. При настройке автоматического реагирования нужно учитывать, что проверка больших файлов или процессов может вызвать резкий рост потребления ресурсов.
- Не рекомендуется использовать модуль «Проверка файлов по хеш-сумме» на большом потоке уникальных файлов. Чем больше размер файла или их количество, тем больше ресурсов будет тратиться на их проверку.

Ниже приведены расчеты потребления ресурсов агентом. Тестирование выполнялось в двух режимах. В первом режиме использовались реальные потоки событий с узлов, работающих без высокой нагрузки и с низкой вредоносной активностью. Во втором режиме использовались синтетические потоки событий, в которых большинство цепочек событий приводили к сработке модуля «Коррелятор». Такой тест имитирует работу узла, на котором

происходит постоянная подозрительная или вредоносная активность. Расчеты производились на виртуальной машине на компьютере с процессором семейства Intel Xeon Ice Lake (частота 2,89 ГГц). Исследование проводилось на следующих наборах модулей:

— В Windows:

- Сбор данных — «WinEventLog: сбор данных из журнала событий Windows», «Установщик Sysmon», «Нормализатор».
- Сбор данных и обнаружение — «WinEventLog: сбор данных из журнала событий Windows», «Установщик Sysmon», «Нормализатор», «Коррелятор (Windows)».
- Сбор данных, расширенное обнаружение и реагирование — «WinEventLog: сбор данных из журнала событий Windows», «Установщик Sysmon», «Нормализатор», «YARA-сканер», «Коррелятор (Windows)» и модули реагирования.
- Сбор данных и интеграция с PT Sandbox — «WinEventLog: сбор данных из журнала событий Windows», «Установщик Sysmon», «Нормализатор», «Проверка файлов в PT Sandbox», «Сканирование в режиме аудита (ISIM VM)».

— В Linux:

- Сбор данных — «Установщик auditd», «Сбор данных из файлов журналов», «Нормализатор».
- Сбор данных и обнаружение — «Установщик auditd», «Сбор данных из файлов журналов», «Нормализатор», «Коррелятор (Linux)».
- Сбор данных, расширенное обнаружение и реагирование — «Установщик auditd», «Сбор данных из файлов журналов», «Нормализатор», «YARA-сканер», «Коррелятор (Linux)» и модули реагирования.
- Сбор данных, обнаружение и интеграция с PT Sandbox — «Установщик auditd», «Сбор данных из файлов журналов», «Нормализатор», «Коррелятор (Linux)», «Проверка файлов в PT Sandbox», «Сканирование в режиме аудита (ISIM VM)».

Внимание! Расчет является ориентировочным, в других условиях потребление ресурсов может отличаться. На загрузку центрального процессора может влиять множество факторов.

Примечание. При использовании антивируса дополнительно нужно учитывать потребление ресурсов этим модулем.

Расчет для обычного режима работы конечного устройства

Таблица 17. Потребление ресурсов агентом (от 2 до 10 событий в секунду)

ОС	Набор модулей	Память (ОЗУ)	Центральный процессор ²
Windows	Сбор данных	До 150 МБ	1 ядро, до 5%
	Сбор данных и обнаружение	До 700 МБ	1 ядро, до 10%
	Сбор данных, расширенное обнаружение и реагирование	До 900 МБ	1 ядро, до 10%
	Сбор данных и интеграция с PT Sandbox	До 170 МБ	1 ядро, до 5%
Linux	Сбор данных	До 200 МБ	1 ядро, до 5%
	Сбор данных и обнаружение	До 540 МБ	1 ядро, до 10%
	Сбор данных, расширенное обнаружение и реагирование	До 700 МБ	1 ядро, до 10%
	Сбор данных, обнаружение и интеграция с PT Sandbox	До 560 МБ	1 ядро, до 10%

Таблица 18. Потребление ресурсов агентом (до 20 событий в секунду)

ОС	Набор модулей	Память (ОЗУ)	Центральный процессор ²
Windows	Сбор данных	До 150 МБ	1 ядро, до 5%
	Сбор данных и обнаружение	До 720 МБ	1 ядро, до 10%
	Сбор данных, расширенное обнаружение и реагирование	До 920 МБ	1 ядро, до 10%
	Сбор данных и интеграция с PT Sandbox	До 170 МБ	1 ядро, до 5%
Linux	Сбор данных	До 200 МБ	1 ядро, до 10%
	Сбор данных и обнаружение	До 540 МБ	1 ядро, до 10%
	Сбор данных, расширенное обнаружение и реагирование	До 700 МБ	1 ядро, до 15%
	Сбор данных, обнаружение и интеграция с PT Sandbox	До 560 МБ	1 ядро, до 10%

² 100% соответствует полной загрузке одного логического ядра ЦП. Показатель «3 ядра, до 220%» означает, что агент использует три логических ядра: два из них загружены полностью, а третье — на 20%.

Таблица 19. Потребление ресурсов агентом (до 50 событий в секунду)

ОС	Набор модулей	Память (ОЗУ)	Центральный процессор ²
Windows	Сбор данных	До 160 МБ	1 ядро, до 10%
	Сбор данных и обнаружение	До 800 МБ	1 ядро, до 30%
	Сбор данных, расширенное обнаружение и реагирование	До 980 МБ	1 ядро, до 30%
	Сбор данных и интеграция с PT Sandbox	До 170 МБ	1 ядро, до 10%
Linux	Сбор данных	До 200 МБ	1 ядро, до 15%
	Сбор данных и обнаружение	До 540 МБ	1 ядро, до 20%
	Сбор данных, расширенное обнаружение и реагирование	До 700 МБ	1 ядро, до 20%
	Сбор данных, обнаружение и интеграция с PT Sandbox	До 560 МБ	1 ядро, до 15%

Таблица 20. Потребление ресурсов агентом (до 100 событий в секунду)

ОС	Набор модулей	Память (ОЗУ)	Центральный процессор ²
Windows	Сбор данных	До 160 МБ	1 ядро, до 15%
	Сбор данных и обнаружение	До 850 МБ	1 ядро, до 60%
	Сбор данных, расширенное обнаружение и реагирование	До 1,05 ГБ	1 ядро, до 60%
	Сбор данных и интеграция с PT Sandbox	До 170 МБ	1 ядро, до 10%
Linux	Сбор данных	До 200 МБ	1 ядро, до 20%
	Сбор данных и обнаружение	До 540 МБ	1 ядро, до 30%
	Сбор данных, расширенное обнаружение и реагирование	До 700 МБ	1 ядро, до 30%
	Сбор данных, обнаружение и интеграция с PT Sandbox	До 560 МБ	1 ядро, до 30%

Расчет для работы конечного устройства в режиме активных угроз

Таблица 21. Потребление ресурсов агентом (от 2 до 10 событий в секунду)

ОС	Набор модулей	Память (ОЗУ)	Центральный процессор ²
Windows	Сбор данных	До 150 МБ	1 ядро, до 5%
	Сбор данных и обнаружение	До 800 МБ	1 ядро, до 50%
	Сбор данных, расширенное обнаружение и реагирование	До 1,6 ГБ	3 ядра, до 210%
	Сбор данных и интеграция с PT Sandbox	До 170 МБ	1 ядро, до 5%
Linux	Сбор данных	До 200 МБ	1 ядро, до 5%
	Сбор данных и обнаружение	До 560 МБ	1 ядро, до 20%
	Сбор данных, расширенное обнаружение и реагирование	До 780 МБ	2 ядра, до 150%
	Сбор данных, обнаружение и интеграция с PT Sandbox	До 580 МБ	1 ядро, до 40%

Таблица 22. Потребление ресурсов агентом (до 20 событий в секунду)

ОС	Набор модулей	Память (ОЗУ)	Центральный процессор ²
Windows	Сбор данных	До 150 МБ	1 ядро, до 10%
	Сбор данных и обнаружение	До 850 МБ	1 ядро, до 50%
	Сбор данных, расширенное обнаружение и реагирование	До 1,6 ГБ	3 ядра, до 210%
	Сбор данных и интеграция с PT Sandbox	До 170 МБ	1 ядро, до 10%
Linux	Сбор данных	До 200 МБ	1 ядро, до 10%
	Сбор данных и обнаружение	До 580 МБ	1 ядро, до 20%
	Сбор данных, расширенное обнаружение и реагирование	До 800 МБ	2 ядра, до 150%
	Сбор данных, обнаружение и интеграция с PT Sandbox	До 600 МБ	1 ядро, до 40%

Таблица 23. Потребление ресурсов агентом (до 50 событий в секунду)

ОС	Набор модулей	Память (ОЗУ)	Центральный процессор ²
Windows	Сбор данных	До 160 МБ	1 ядро, до 10%
	Сбор данных и обнаружение	До 960 МБ	1 ядро, до 50%
	Сбор данных, расширенное обнаружение и реагирование	До 1,6 ГБ	3 ядра, до 230%
	Сбор данных и интеграция с PT Sandbox	До 180 МБ	1 ядро, до 10%
Linux	Сбор данных	До 200 МБ	1 ядро, до 15%
	Сбор данных и обнаружение	До 650 МБ	1 ядро, до 25%
	Сбор данных, расширенное обнаружение и реагирование	До 900 МБ	2 ядра, до 150%
	Сбор данных, обнаружение и интеграция с PT Sandbox	До 660 МБ	1 ядро, до 40%

Таблица 24. Потребление ресурсов агентом (до 100 событий в секунду)

ОС	Набор модулей	Память (ОЗУ)	Центральный процессор ²
Windows	Сбор данных	До 160 МБ	1 ядро, до 15%
	Сбор данных и обнаружение	До 1,3 ГБ	1 ядро, до 90%
	Сбор данных, расширенное обнаружение и реагирование	До 2 ГБ	3 ядра, до 230%
	Сбор данных и интеграция с PT Sandbox	До 180 МБ	1 ядро, до 15%
Linux	Сбор данных	До 200 МБ	1 ядро, до 20%
	Сбор данных и обнаружение	До 700 МБ	1 ядро, до 40%
	Сбор данных, расширенное обнаружение и реагирование	До 1 ГБ	2 ядра, до 180%
	Сбор данных, обнаружение и интеграция с PT Sandbox	До 720 МБ	1 ядро, до 50%

4. Лицензирование

Для работы PT ISIM View Sensor, PT ISIM Endpoint, PT ISIM Collector и PT ISIM Overview Center, защиты этих компонентов от нелегального использования и получения обновлений нужна лицензия.

Предусмотрены два типа лицензий:

- Платная лицензия для полноценного использования продукта. Срок действия платной лицензии устанавливается поставщиком продукта в зависимости от условий поставки.
- Пробная лицензия, предназначенная для демонстрационных целей и действующая 90 дней.

В этом разделе

[Жизненный цикл лицензии \(см. раздел 4.1\)](#)

[Расширение лицензии \(см. раздел 4.2\)](#)

См. также

[Активация лицензии PT ISIM View Sensor \(см. раздел 5.3.5.2\)](#)

[Активация лицензии PT ISIM Endpoint \(см. раздел 5.4.4\)](#)

4.1. Жизненный цикл лицензии

Первоначальное приобретение лицензии

Приобретение любого компонента PT ISIM (PT ISIM View Sensor, PT ISIM Collector, PT ISIM Overview Center или PT ISIM Endpoint) предполагает необходимость приобретения базовой лицензии на этот компонент в зависимости от требуемой функциональности, суммарной скорости передачи данных обрабатываемого трафика и условий применения компонента.

Продление срока действия срочной лицензии

Продлевать приобретенные срочные лицензии необходимо заранее, до истечения срока их действия.

Продление срока разрешенного использования лицензии производится путем приобретения соответствующей лицензии на продление. По умолчанию срок действия лицензии на продление составляет один год, но может быть иным.

Окончание срока действия лицензии (периода предоставления обновлений)

По окончании указанного в бланке лицензии срока действия срочная лицензия становится недействительной, прекращаются предоставление обновлений программного обеспечения PT ISIM и оказание услуг технической поддержки. Если срок действия срочной лицензии не продлевается, по истечении срока разрешенного использования программное обеспечение PT ISIM необходимо удалить (деинсталлировать).

Лицензии, выданные на весь срок действия исключительных прав, в том числе лицензии в составе ПАК PT ISIM, не требуют продления срока разрешенного использования, однако с даты окончания периода предоставления обновлений, указанной в бланке лицензии, доступ к технической поддержке, к обновлениям программного обеспечения, баз экспертных правил PT ISTI и антивирусной базы PT ISIM Endpoint прекращается до момента приобретения конечным пользователем соответствующей лицензии на обновления.

4.2. Расширение лицензии

Увеличение состава приобретенных лицензий или расширение лицензий может потребоваться в случаях, указанных в таблице ниже.

Таблица 25. Ситуации, требующие расширения лицензии

Ситуация	Решение
Увеличилось количество территориально распределенных точек съема трафика или существенно возросла скорость сетевого трафика	Может потребоваться приобретение: — дополнительных базовых лицензий и установка дополнительных PT ISIM View Sensor или PT ISIM Collector в зависимости от изменений архитектуры сети; — дополнительных лицензий для серверов управления PT ISIM Overview Center, если они необходимы для управления распределенной системой сенсоров
Изменилась инфраструктура	
Возникла потребность мониторинга событий информационной безопасности на рабочих станциях и серверах АСУ ТП	Может потребоваться приобретение базовых лицензий на PT ISIM Endpoint в количестве, соответствующем количеству серверов и АРМ, на которые необходима установка агентов. Резервные или непродуктивные АРМ также считаются
Изменились требования к PT ISIM	Пересмотр спецификации с участием специалистов Positive Technologies

Ситуация	Решение
Возникла потребность увеличения лицензированной пропускной способности сенсора и (или) его функциональных возможностей (например, переход от netView Sensor на proView Sensor или с 500 Мбит/с на 1 Гбит/с)	Может потребоваться расширение функциональных возможностей ранее приобретенного ПО при помощи покупки лицензии на пакет расширений

5. Развертывание PT ISIM

В этом разделе приведены инструкции по установке компонентов PT ISIM.

В этом разделе

[Установка и обновление ОС \(см. раздел 5.1\)](#)

[Установочный комплект \(см. раздел 5.2\)](#)

[Установка PT ISIM View Sensor \(см. раздел 5.3\)](#)

[Установка PT ISIM Endpoint \(см. раздел 5.4\)](#)

[Установка PT ISIM Collector \(см. раздел 5.5\)](#)

[Установка PT ISIM Overview Center \(см. раздел 5.6\)](#)

[Установка PT ISIM Industrial Tablet на виртуальную машину или промышленный планшет \(см. раздел 5.7\)](#)

[Порядок установки PT ISIM View Sensor, PT ISIM Endpoint и PT MC на один сервер \(см. раздел 5.8\)](#)

[Изменение IP-адреса сервера PT ISIM в параметрах компонентов для конфигурации all-in-one \(см. раздел 5.9\)](#)

5.1. Установка и обновление ОС

В этом разделе приведены инструкции по установке и обновлению ОС.

В этом разделе

[Установка Debian 10 \(см. раздел 5.1.1\)](#)

[Установка Debian 12 \(см. раздел 5.1.2\)](#)

[Обновление Debian \(см. раздел 5.1.3\)](#)

[Установка Astra Linux \(см. раздел 5.1.4\)](#)

[Обновление Astra Linux \(см. раздел 5.1.5\)](#)

5.1.1. Установка Debian 10

Перед началом установки Debian в меню настройки BIOS требуется указать загрузочное устройство (например, USB-накопитель) с необходимым образом операционной системы.

► Чтобы установить Debian:

1. Подключите к компьютеру внешний носитель с загрузочным образом Debian.
2. Дождавшись загрузки первичного окна выбора вариантов установки, выберите **Install** или **Graphical Install** (на рисунках ниже представлены снимки экрана для выбранного варианта **Graphical Install**).
3. На этапе выбора языка (**Select a language**) выберите **Русский** и нажмите **Continue**.

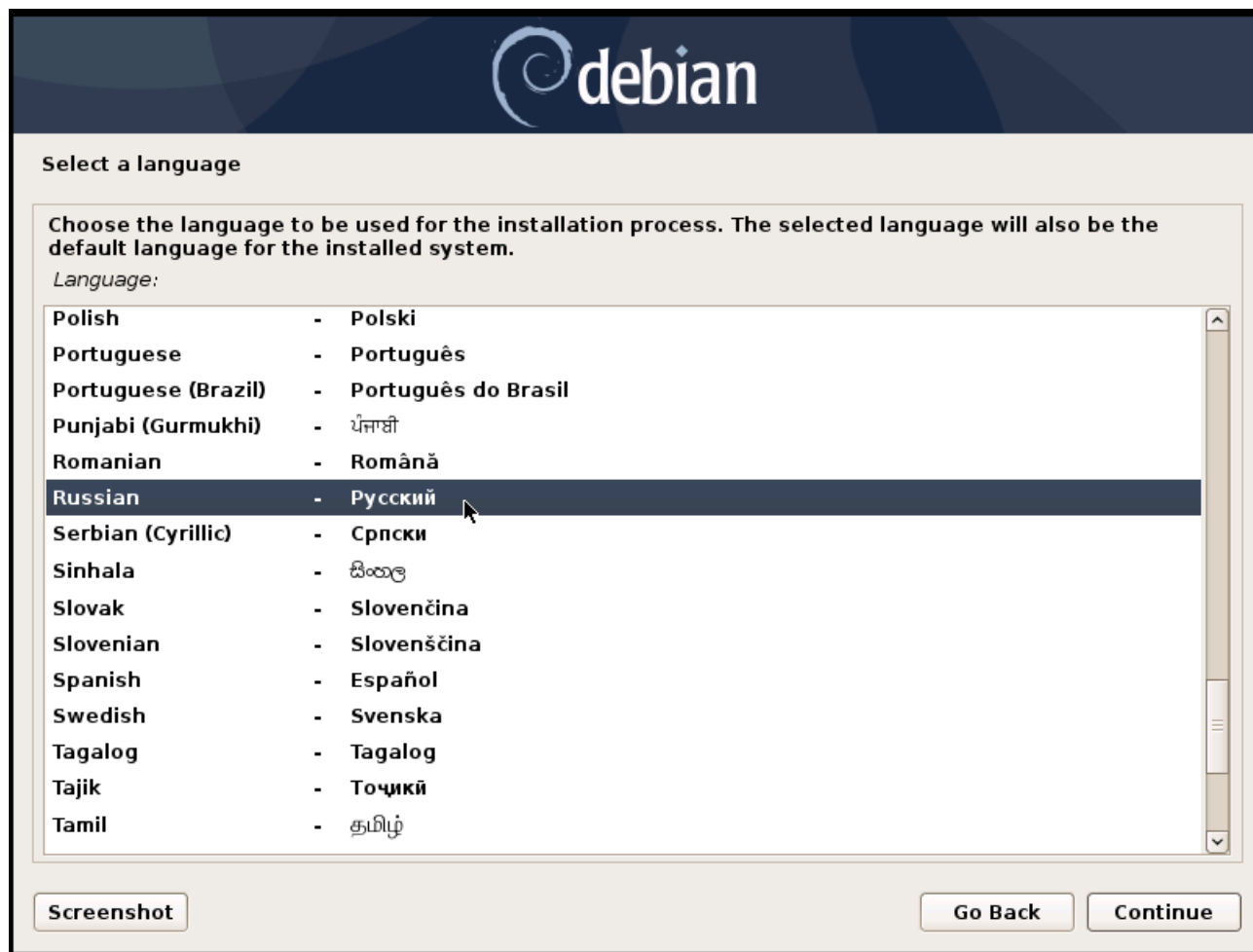


Рисунок 1. Выбор языка ОС

4. На этапе выбора местонахождения выберите страну, в которой располагается сервер, и нажмите **Продолжить**.



The image shows a window from the Debian installer. At the top is the Debian logo. The title bar reads "Выберите местонахождение" (Select location). The main text explains that the selected location will be used for time zone and locale settings, and that the list is based on the chosen language. It asks the user to select "другая" (other) if their location is not in the list. Below this, a list box titled "Страна, область или регион:" (Country, region or province:) contains three items: "Российская Федерация" (Russian Federation), "Украина" (Ukraine), and "другая" (other). The "Российская Федерация" item is highlighted with a mouse cursor. At the bottom, there are three buttons: "Снимок экрана" (Screenshot), "Вернуться" (Back), and "Продолжить" (Continue).

Выберите местонахождение

Выбранное местоположение будет учтено при настройке часового пояса и создании списка при выборе системной локали. Обычно, здесь указывается страна, в которой вы живёте.

Данный сокращённый список основан на выбранном вами языке. Выберите "другая", если вашего местоположения нет в списке.

Страна, область или регион:

- Российская Федерация
- Украина
- другая

Снимок экрана Вернуться Продолжить

Рисунок 2. Выбор местонахождения

5. На этапе выбора клавиатурной раскладки выберите **Русская** и нажмите **Продолжить**.

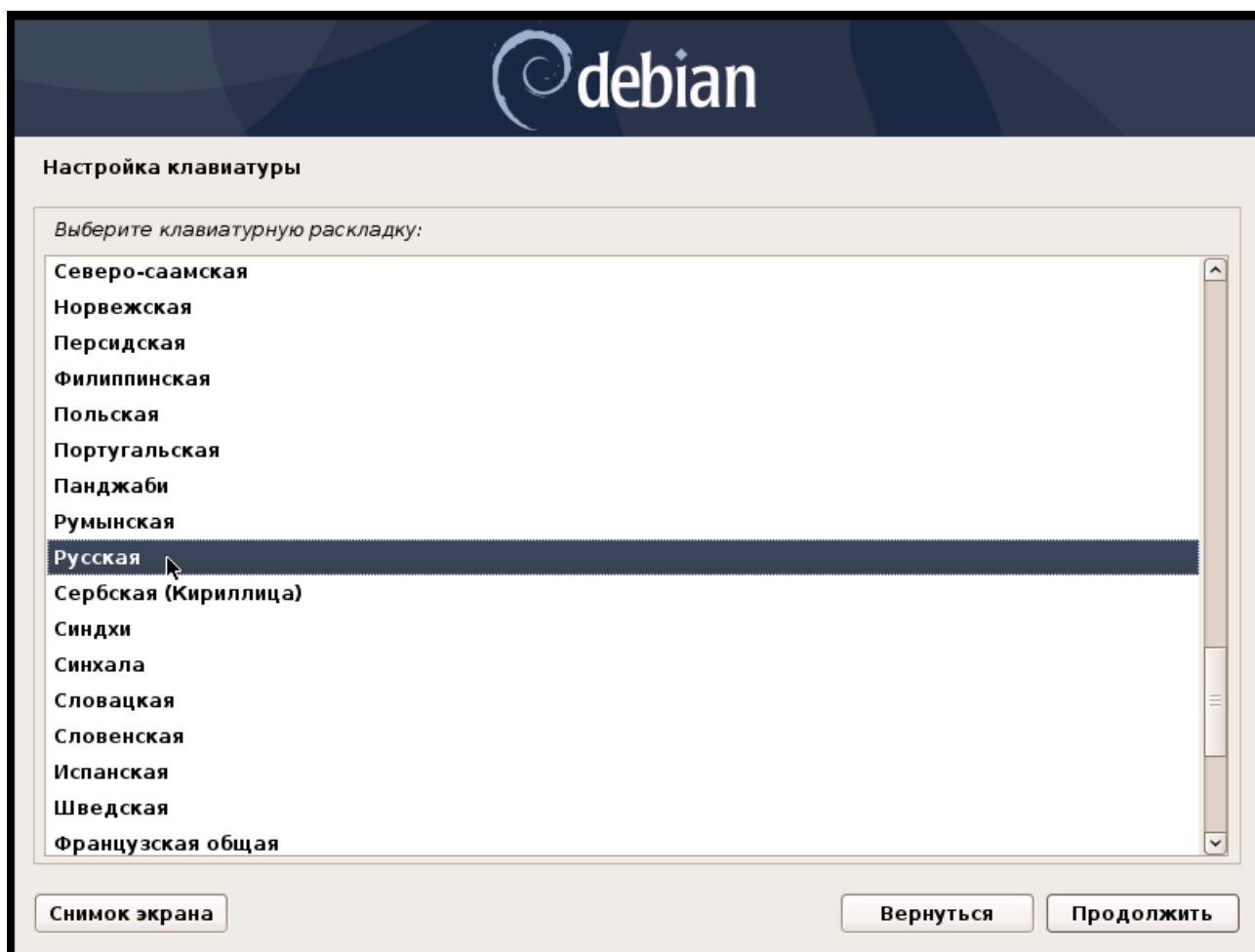
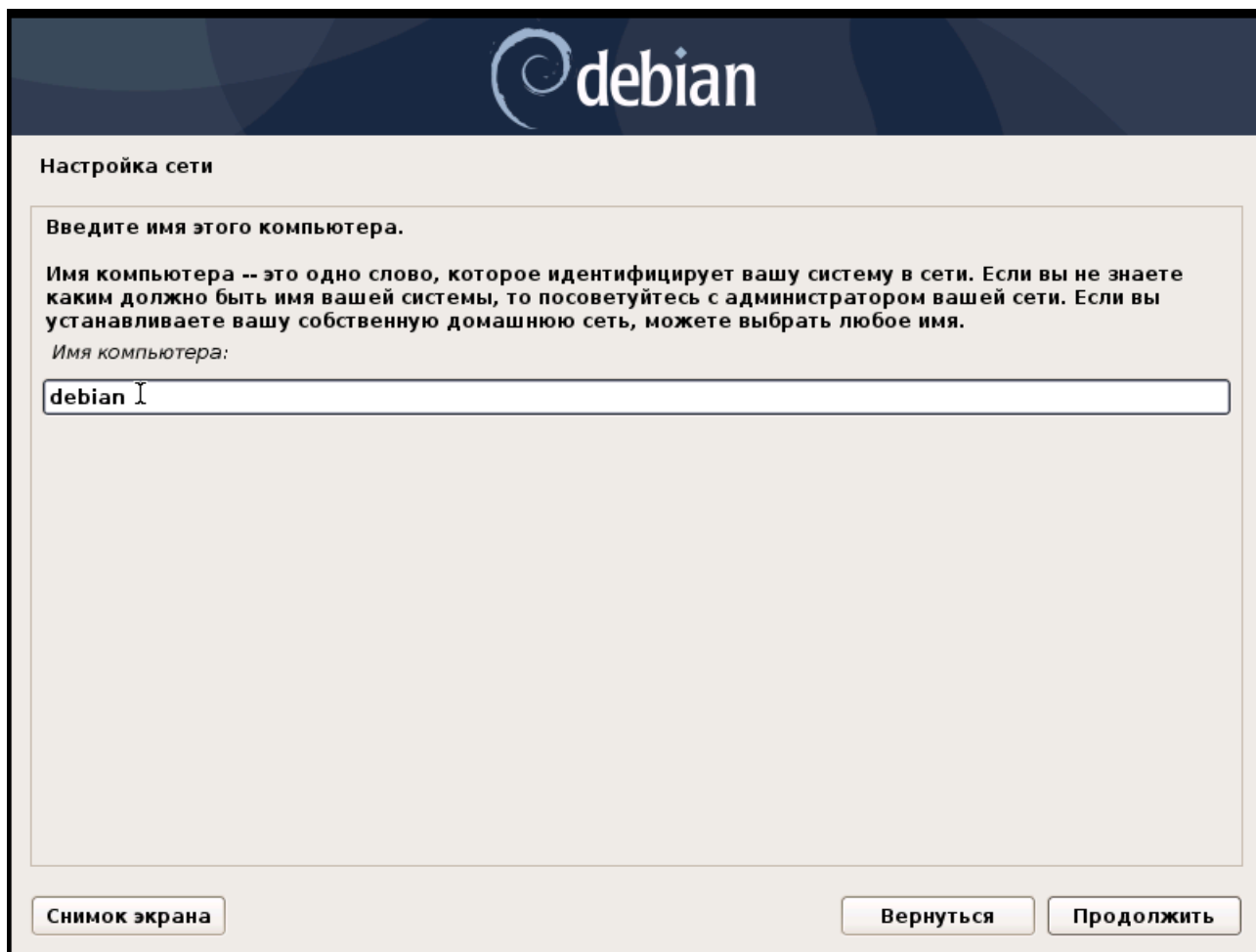


Рисунок 3. Выбор клавиатурной раскладки

6. На этапе выбора способа переключения между национальной и латинской раскладкой выберите сочетание клавиш и нажмите **Продолжить**.
7. Если требуется, на этапе настройки сети выберите основной сетевой интерфейс и нажмите **Продолжить**.
8. На этапе настройки сети задайте имя компьютера и нажмите **Продолжить**.



Настройка сети

Введите имя этого компьютера.

Имя компьютера -- это одно слово, которое идентифицирует вашу систему в сети. Если вы не знаете каким должно быть имя вашей системы, то посоветуйтесь с администратором вашей сети. Если вы устанавливаете вашу собственную домашнюю сеть, можете выбрать любое имя.

Имя компьютера:

debian

Снимок экрана Вернуться Продолжить

Рисунок 4. Настройка имени компьютера

9. Если требуется, задайте доменное имя и нажмите **Продолжить**.



Настройка сети

Имя домена -- это часть вашего Интернет-адреса, справа от имени компьютера. Зачастую она заканчивается на .com, .net, .edu или .org. Если вы настраиваете сеть дома, то можете указать что-нибудь своё, но убедитесь, что используете одинаковое имя домена на всех ваших машинах.

Имя домена:

Снимок экрана Вернуться Продолжить

Рисунок 5. Настройка имени домена

10. На этапе настройки учетных записей пользователей и паролей задайте пароль суперпользователя (root), введите его повторно и нажмите **Продолжить**.



debian

Настройка учётных записей пользователей и паролей

Необходимо ввести пароль учётной записи суперпользователя (root), используемой для администрирования системы. Доступ к компьютеру с использованием этой учётной записи злонамеренных или низкоквалифицированных пользователей может привести к катастрофическим последствиям. Поэтому пароль суперпользователя не должен легко угадываться, подбираться по словарю, и он не должен быть связан с вашей личностью.

Хороший пароль представляет из себя смесь букв, цифр и знаков препинания, и должен периодически меняться.

Пароль учётной записи суперпользователя не должен быть пустым, иначе она будет заблокирована, а настроенной в программе установки пользовательской учётной записи будет разрешено работать с правами суперпользователя через команду "sudo".

Во время ввода пароля вводимые символы не будут отображаться на экране.

Пароль суперпользователя:

●●●●●●●●

☐ Показывать вводимый пароль

Введите тот же самый пароль ещё раз, чтобы убедиться в правильности ввода.

Введите пароль ещё раз:

●●●●●●●● I

☐ Показывать вводимый пароль

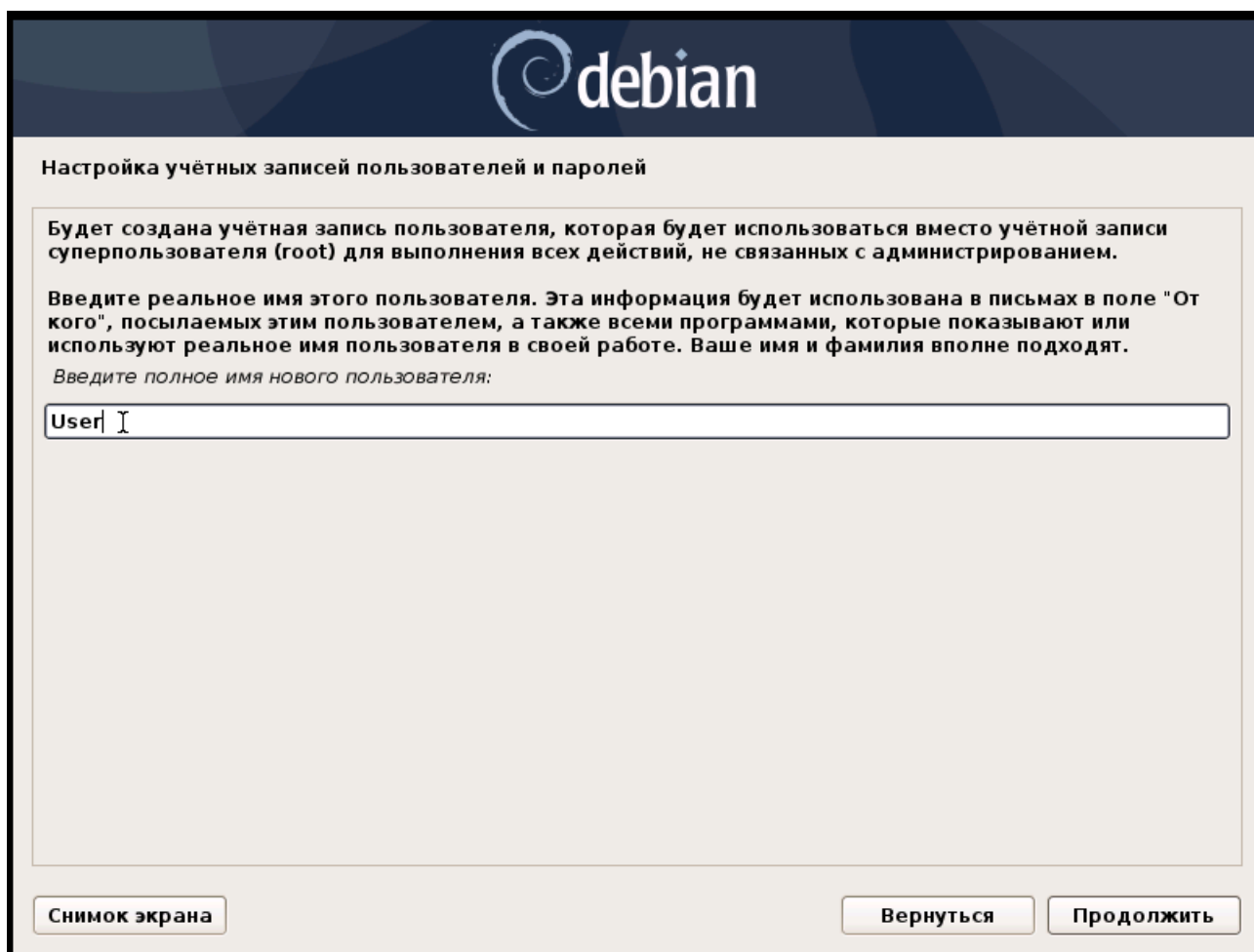
Снимок экрана

Вернуться

Продолжить

Рисунок 6. Настройка учетной записи root

11. Создайте учетную запись обычного пользователя, указав полное имя нового пользователя, имя учетной записи и дважды указав пароль.



The image shows a window from the Debian installer. At the top is the Debian logo. The title bar reads "Настройка учётных записей пользователей и паролей". The main text explains that a regular user account will be created instead of root. It asks for a real name, which will be used in emails and by programs. A text input field contains "User". At the bottom are three buttons: "Снимок экрана", "Вернуться", and "Продолжить".

debian

Настройка учётных записей пользователей и паролей

Будет создана учётная запись пользователя, которая будет использоваться вместо учётной записи суперпользователя (root) для выполнения всех действий, не связанных с администрированием.

Введите реальное имя этого пользователя. Эта информация будет использована в письмах в поле "От кого", посылаемых этим пользователем, а также всеми программами, которые показывают или используют реальное имя пользователя в своей работе. Ваше имя и фамилия вполне подходят.

Введите полное имя нового пользователя:

User |

Снимок экрана Вернуться Продолжить

Рисунок 7. Настройка учетной записи обычного пользователя

12. На этапе настройки времени выберите часовой пояс и нажмите **Продолжить**.

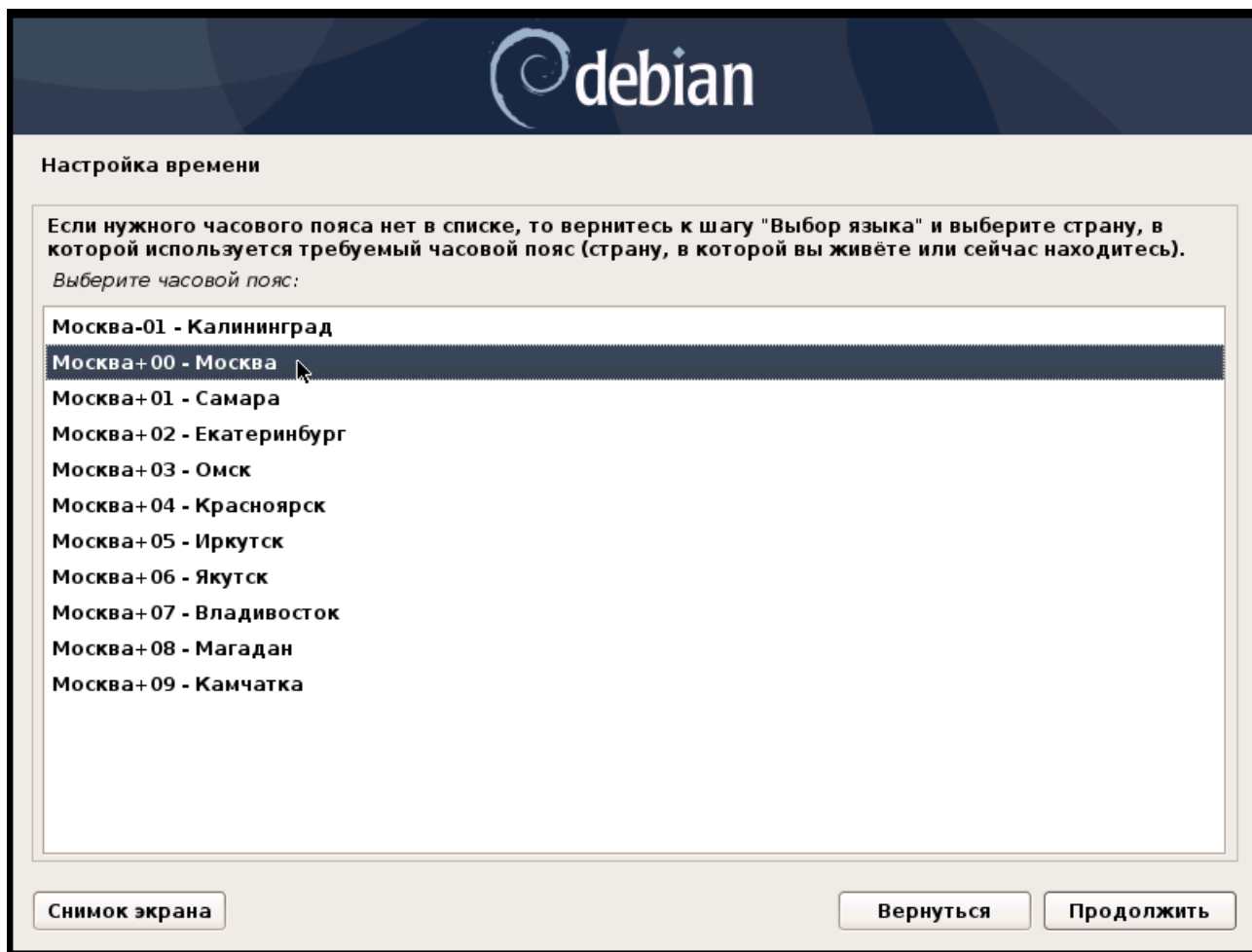


Рисунок 8. Выбор часового пояса

13. На этапе разметки дисков выберите вариант **Вручную** и нажмите **Продолжить**.

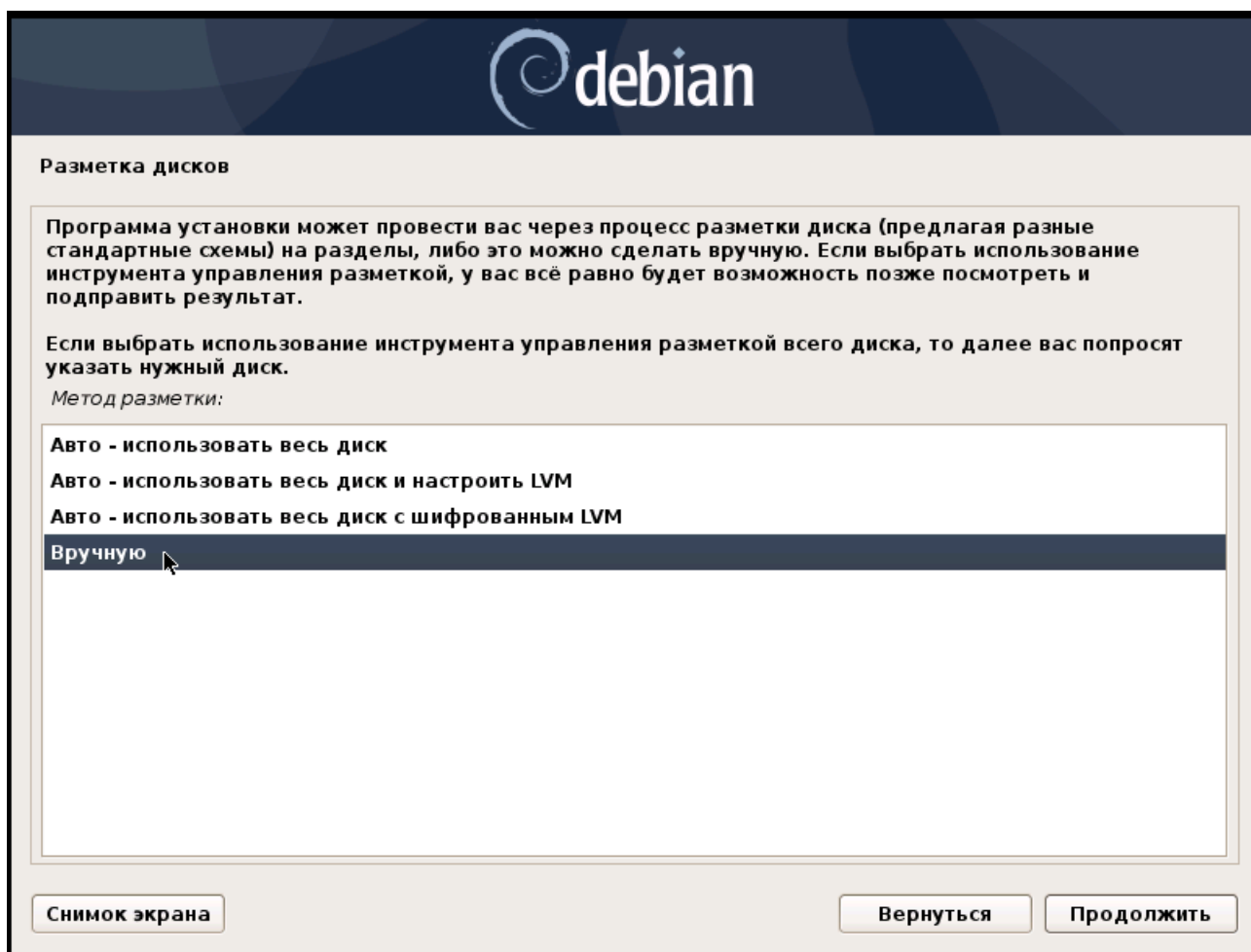


Рисунок 9. Выбор способа разметки диска

14. Выберите жесткий диск.
15. Подтвердите создание новой таблицы разделов, выбрав **Да** и нажав **Продолжить**.
16. Создайте основной корневой раздел системы:
 - Выберите в таблице разделов область с пометкой **Свободное место**.
 - На этапе выбора действий со свободным пространством выберите вариант **Создать новый раздел**.
 - В поле **Новый размер раздела** введите объем основного раздела (доступное дисковое пространство минус объем раздела подкачки в соответствии с [программными требованиями \(см. раздел 3.2\)](#)).
 - На этапе выбора типа нового раздела выберите вариант **Первичный**.
 - На этапе выбора местоположения нового раздела выберите вариант **Начало**.
 - В таблице **Настройки раздела** выберите параметры, как показано на рисунке ниже, и после этого выберите вариант **Настройка раздела закончена**.

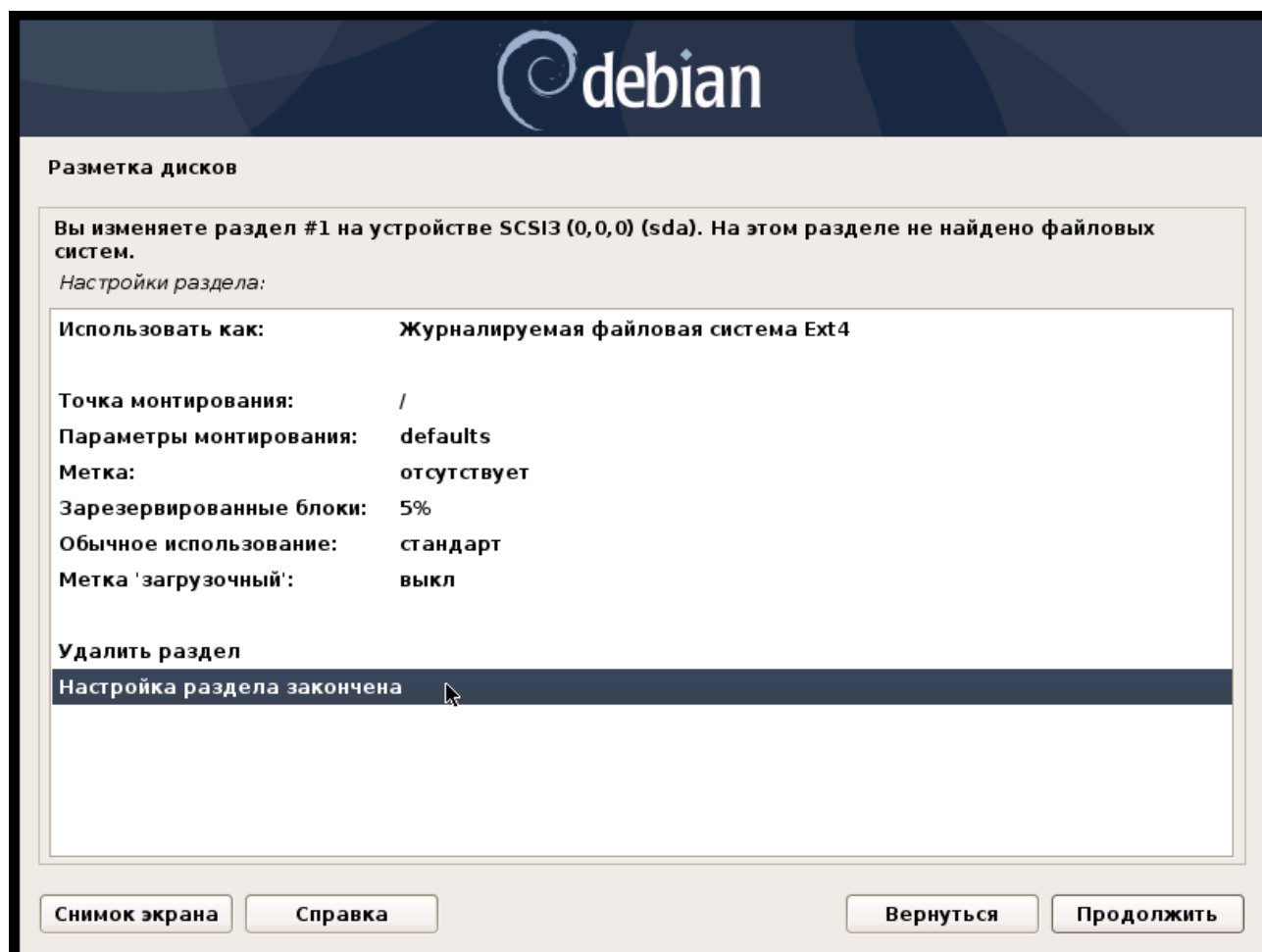


Рисунок 10. Параметры корневого раздела системы

В таблице разделов появится вторая область с пометкой **Свободное место**.

17. Создайте раздел подкачки:

- Выберите в таблице разделов вторую область с пометкой **Свободное место**.
- На этапе выбора действий со свободным пространством выберите вариант **Создать новый раздел**.
- В поле **Новый размер раздела** введите объем раздела подкачки в соответствии с [программными требованиями \(см. раздел 3.2\)](#).
- На этапе выбора типа нового раздела выберите вариант **Логический**.
- В таблице **Настройки раздела** выберите параметр **Использовать как** и выберите для него значение **Раздел подкачки**.
- По окончании настройки выберите вариант **Настройка раздела закончена**.

18. На этапе разметки дисков выберите вариант **Закончить разметку и записать изменения на диск** и нажмите **Продолжить**.

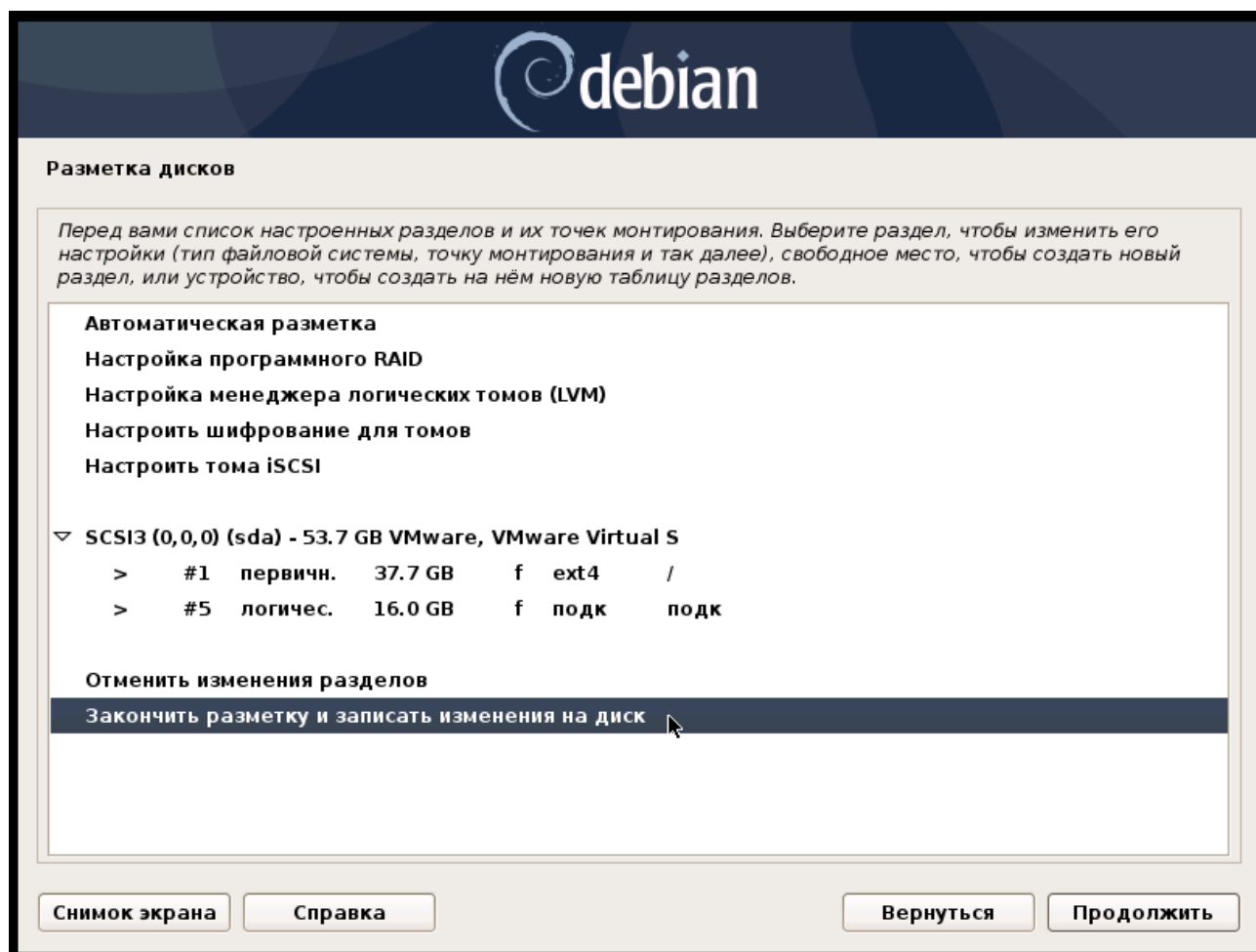


Рисунок 11. Разметка дисков

19. Подтвердите запись изменений на диск, выбрав **Да** и нажав **Продолжить**.

Запустится процесс установки базовых компонентов системы.

20. На этапе настройки менеджера пакетов выберите вариант **Нет** при ответе на вопрос о сканировании другого диска и нажмите **Продолжить**.

21. Выберите вариант **Нет** при ответе на вопрос об использовании зеркала архива и нажмите **Продолжить**.

Запустится процесс автоматического выбора и установки базовых компонентов системы.

22. На этапе настройки пакета popularity-contest выберите вариант **Нет** при ответе на вопрос об участии в опросе и нажмите **Продолжить**.

23. На этапе выбора программного обеспечения выберите **SSH-сервер** и **Стандартные системные утилиты**.

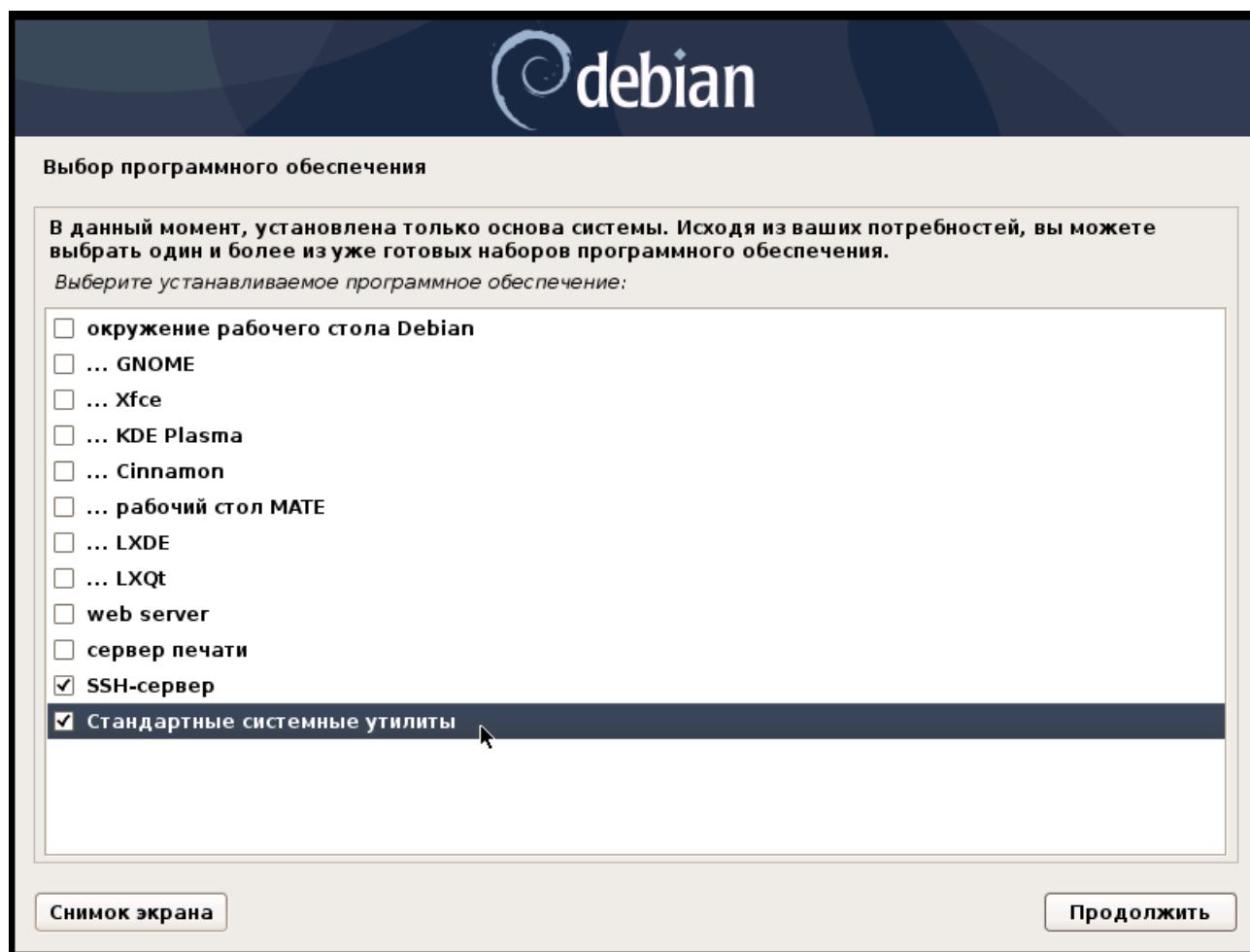


Рисунок 12. Выбор программного обеспечения

24. Снова запустится процесс автоматического выбора и установки базовых компонентов системы.

25. Подтвердите установку системного загрузчика GRUB на жесткий диск, выбрав **Да** и нажав **Продолжить**.



Рисунок 13. Установка системного загрузчика GRUB

26. Укажите раздел для загрузки ОС и нажмите **Продолжить**.



Рисунок 14. Выбор раздела загрузки ОС

27. На этапе завершения установки отключите внешний носитель от компьютера и после этого нажмите **Продолжить**.

Система перезапустится.

Внимание! На этом этапе не отключайте питание и принудительно не перезагружайте компьютер, поскольку это приведет к неработоспособности системы.

Установка Debian завершена.

5.1.2. Установка Debian 12

Перед началом установки Debian в меню настройки BIOS требуется указать загрузочное устройство (например, USB-накопитель) с необходимым образом операционной системы.

► Чтобы установить Debian:

1. Подключите к компьютеру внешний носитель с загрузочным образом Debian.
2. Дождавшись загрузки первичного окна выбора вариантов установки, выберите **Install** или **Graphical Install** (на рисунках ниже представлены снимки экрана для выбранного варианта **Graphical Install**).
3. На этапе выбора языка (**Select a language**) выберите **Русский** и нажмите **Continue**.



Рисунок 15. Выбор языка ОС

4. На этапе выбора местонахождения выберите страну, в которой располагается сервер, и нажмите **Продолжить**.

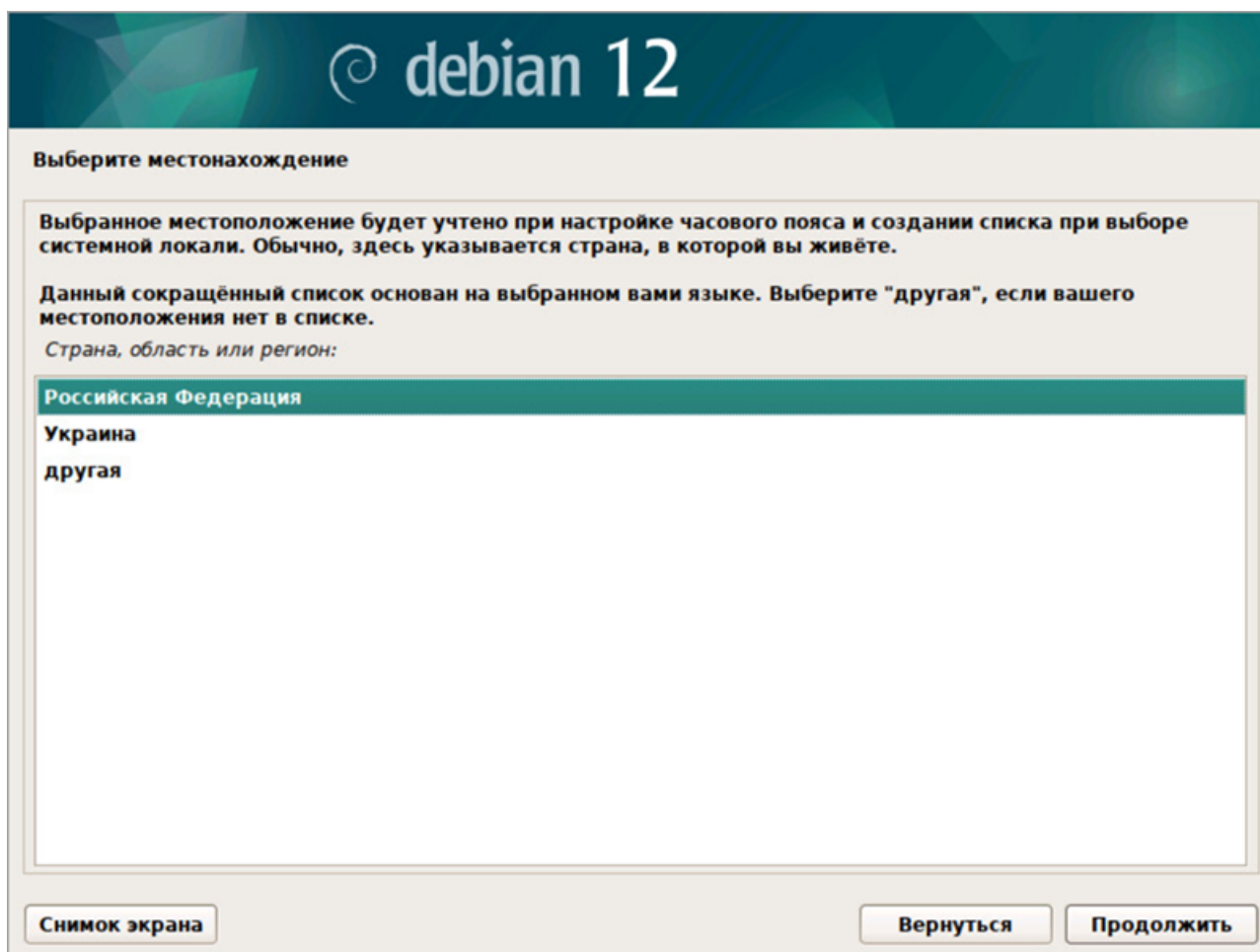


Рисунок 16. Выбор местонахождения

5. На этапе выбора клавиатурной раскладки выберите **Русская** и нажмите **Продолжить**.

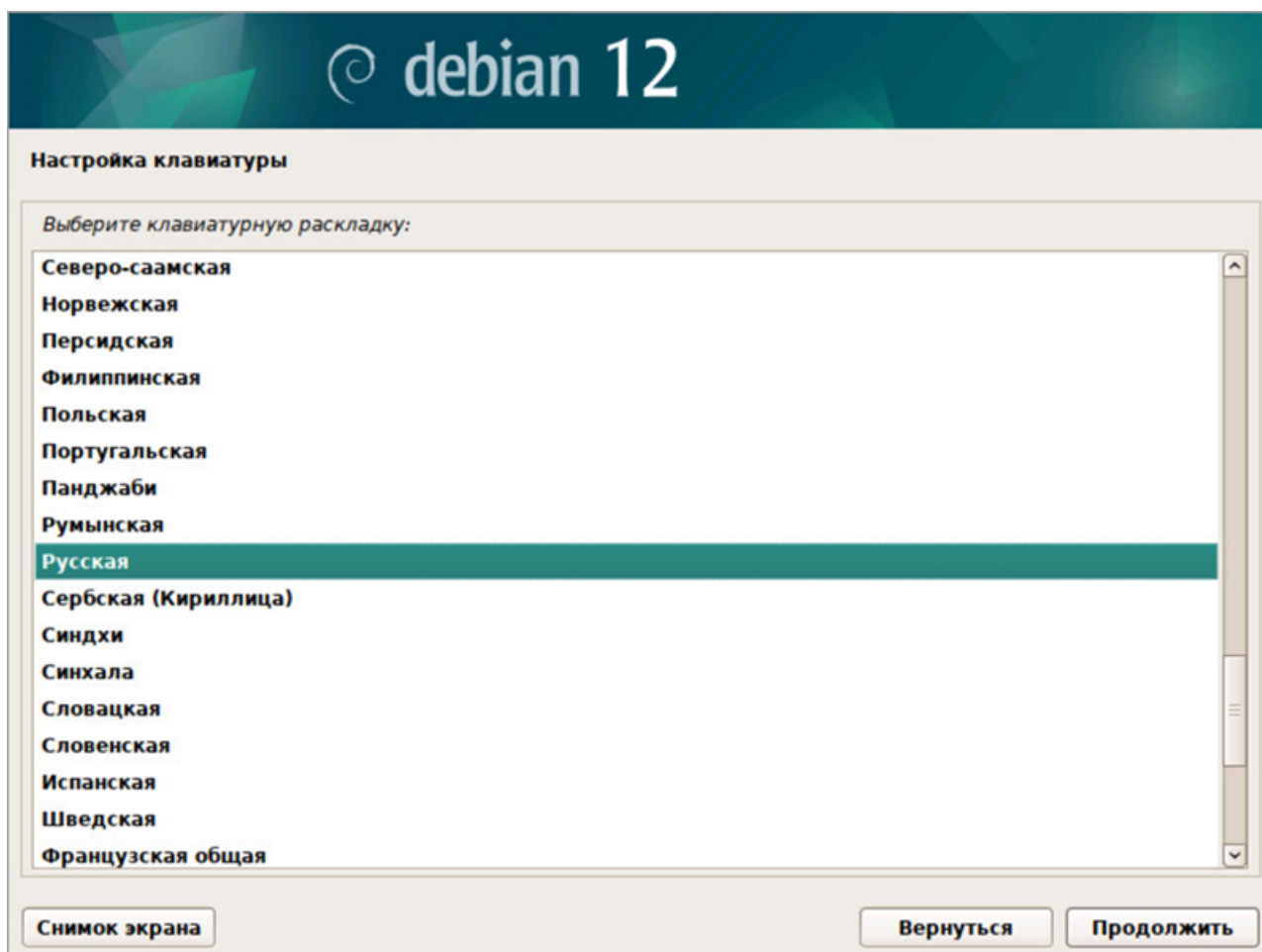
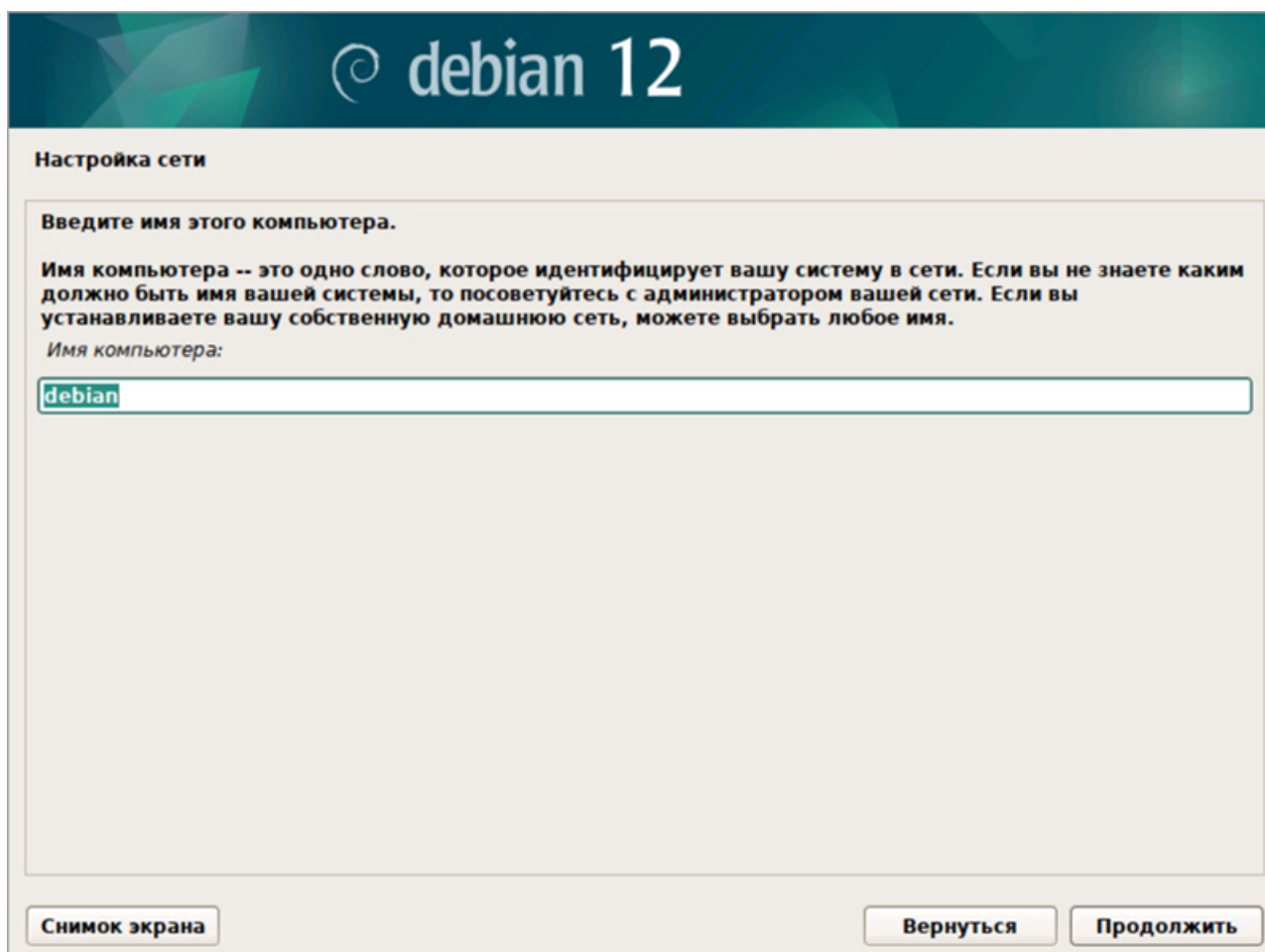


Рисунок 17. Выбор клавиатурной раскладки

6. На этапе выбора способа переключения между национальной и латинской раскладкой выберите сочетание клавиш и нажмите **Продолжить**.
7. Если требуется, на этапе настройки сети выберите основной сетевой интерфейс и нажмите **Продолжить**.
8. На этапе настройки сети задайте имя компьютера и нажмите **Продолжить**.



The screenshot shows the 'debian 12' logo at the top. Below it, the window title is 'Настройка сети' (Network Configuration). The main content area has the heading 'Введите имя этого компьютера.' (Enter the name of this computer.) followed by a paragraph explaining that the computer name is a single word used for network identification and that users can choose any name for a home network. Below the text is a label 'Имя компьютера:' (Computer name:) and a text input field containing the word 'debian'. At the bottom of the window, there are three buttons: 'Снимок экрана' (Screenshot), 'Вернуться' (Back), and 'Продолжить' (Continue).

Рисунок 18. Настройка имени компьютера

9. Если требуется, задайте доменное имя и нажмите **Продолжить**.



The screenshot shows the 'debian 12' logo at the top. Below it, the window title is 'Настройка сети' (Network Configuration). The main text explains that the domain name is the part of the Internet address after the computer name, typically ending in .com, .net, .edu, or .org. It advises that if setting up a home network, one can choose anything, but it must be the same on all machines. Below this text is a label 'Имя домена:' followed by a large empty text input field. At the bottom, there are three buttons: 'Снимок экрана' (Screenshot), 'Вернуться' (Back), and 'Продолжить' (Continue).

debian 12

Настройка сети

Имя домена -- это часть вашего Интернет-адреса, справа от имени компьютера. Зачастую она заканчивается на .com, .net, .edu или .org. Если вы настраиваете сеть дома, то можете указать что-нибудь своё, но убедитесь, что используете одинаковое имя домена на всех ваших машинах.

Имя домена:

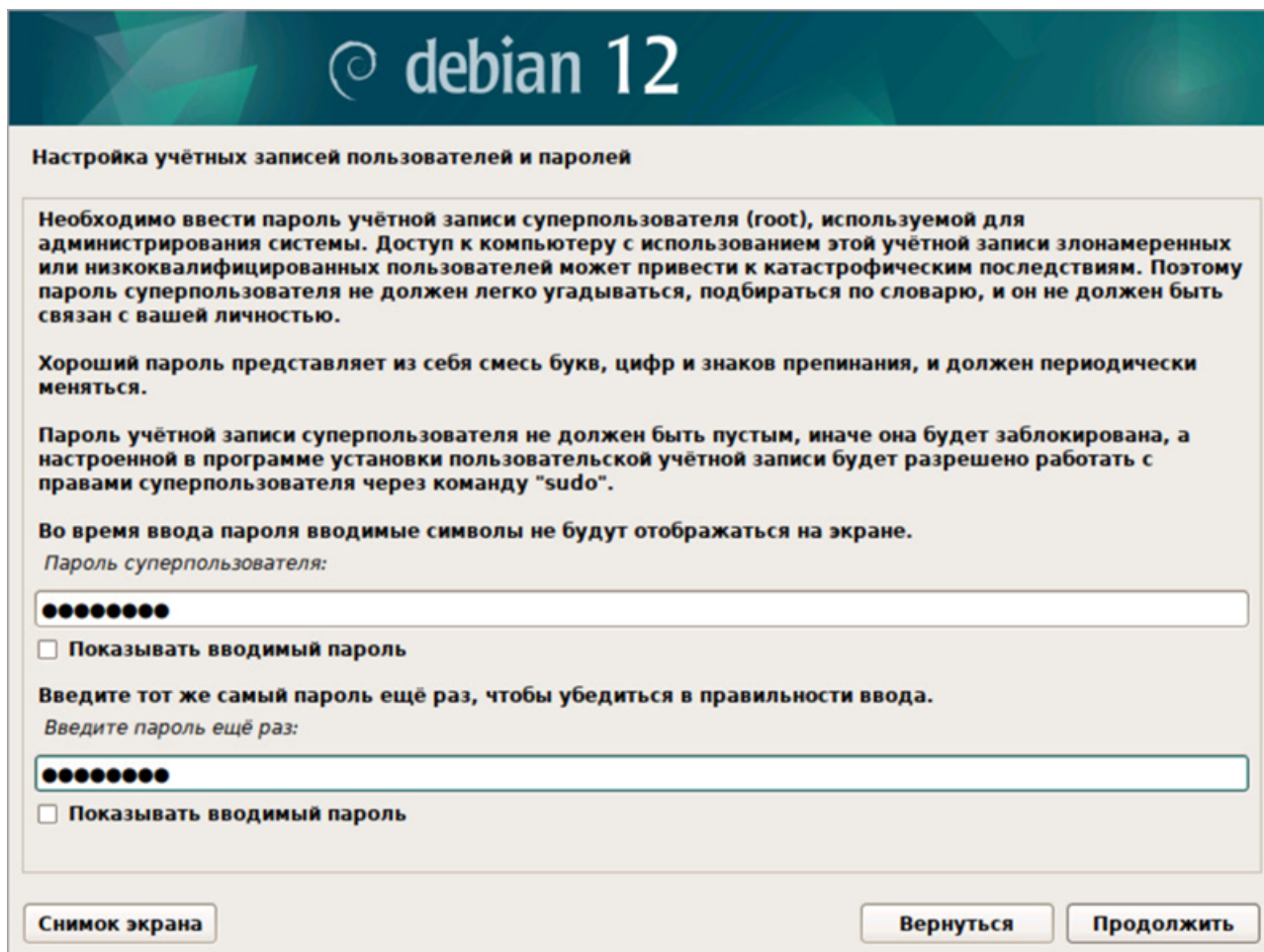
Снимок экрана

Вернуться

Продолжить

Рисунок 19. Настройка имени домена

10. На этапе настройки учетных записей пользователей и паролей задайте пароль суперпользователя (root), введите его повторно и нажмите **Продолжить**.



The screenshot shows the 'debian 12' installer window with the title 'Настройка учётных записей пользователей и паролей'. It contains several paragraphs of text explaining the importance of a strong root password and instructions on how to enter it. There are two password input fields, each with a 'Показывать вводимый пароль' checkbox. At the bottom, there are three buttons: 'Снимок экрана', 'Вернуться', and 'Продолжить'.

debian 12

Настройка учётных записей пользователей и паролей

Необходимо ввести пароль учётной записи суперпользователя (root), используемой для администрирования системы. Доступ к компьютеру с использованием этой учётной записи злонамеренных или низкоквалифицированных пользователей может привести к катастрофическим последствиям. Поэтому пароль суперпользователя не должен легко угадываться, подбираться по словарю, и он не должен быть связан с вашей личностью.

Хороший пароль представляет из себя смесь букв, цифр и знаков препинания, и должен периодически меняться.

Пароль учётной записи суперпользователя не должен быть пустым, иначе она будет заблокирована, а настроенной в программе установки пользовательской учётной записи будет разрешено работать с правами суперпользователя через команду "sudo".

Во время ввода пароля вводимые символы не будут отображаться на экране.

Пароль суперпользователя:

••••••••

☐ Показывать вводимый пароль

Введите тот же самый пароль ещё раз, чтобы убедиться в правильности ввода.

Введите пароль ещё раз:

••••••••

☐ Показывать вводимый пароль

Снимок экрана Вернуться Продолжить

Рисунок 20. Настройка учетной записи root

11. Создайте учетную запись обычного пользователя, указав полное имя нового пользователя, имя учетной записи и дважды указав пароль.



debian 12

Настройка учётных записей пользователей и паролей

Будет создана учётная запись пользователя, которая будет использоваться вместо учётной записи суперпользователя (root) для выполнения всех действий, не связанных с администрированием.

Введите реальное имя этого пользователя. Эта информация будет использована в письмах в поле "От кого", посылаемых этим пользователем, а также всеми программами, которые показывают или используют реальное имя пользователя в своей работе. Ваше имя и фамилия вполне подходят.

Введите полное имя нового пользователя:

User

Снимок экрана Вернуться Продолжить

Рисунок 21. Настройка учетной записи обычного пользователя

12. На этапе настройки времени выберите часовой пояс и нажмите **Продолжить**.

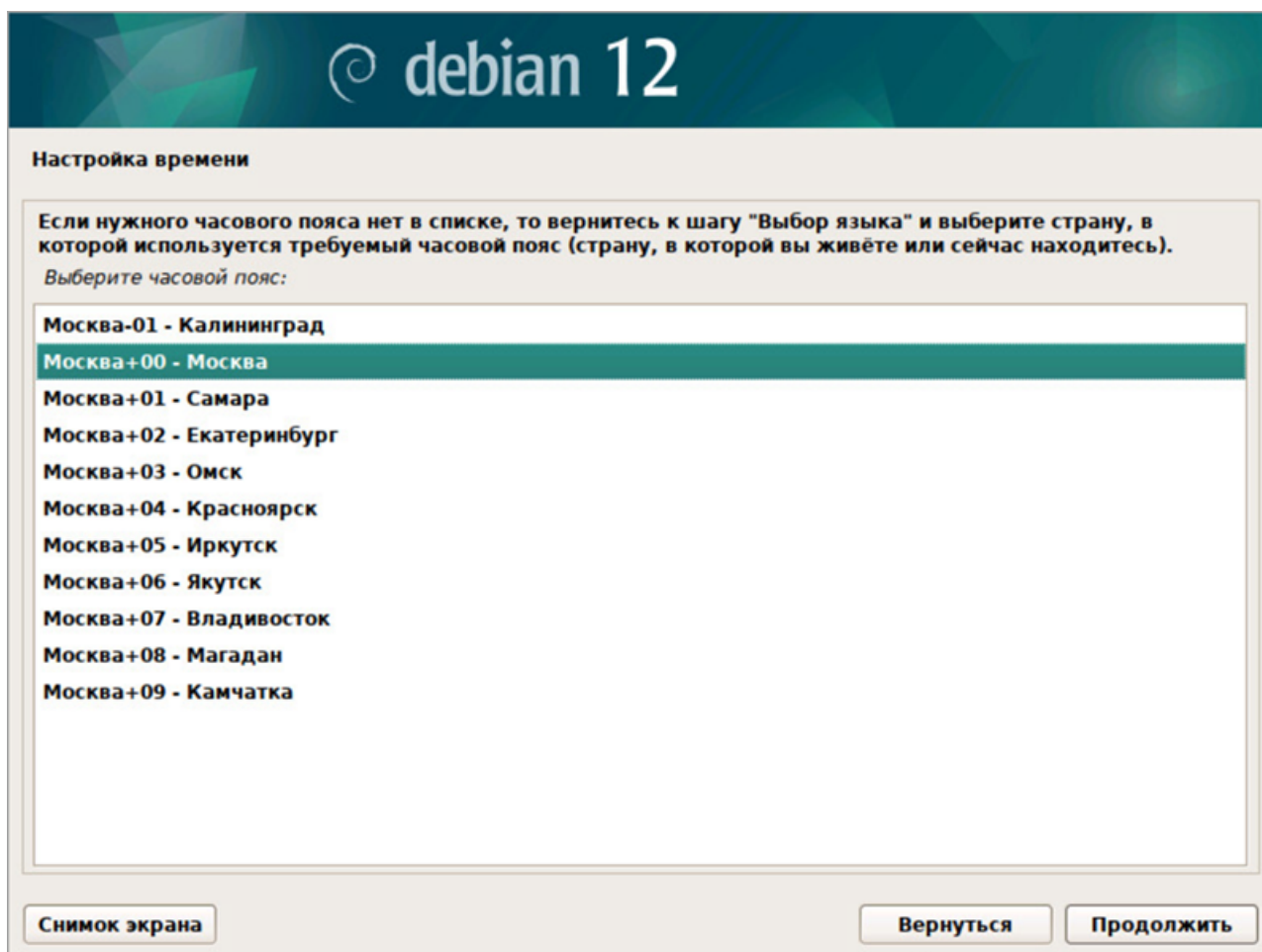


Рисунок 22. Выбор часового пояса

13. На этапе разметки дисков выберите вариант **Вручную** и нажмите **Продолжить**.

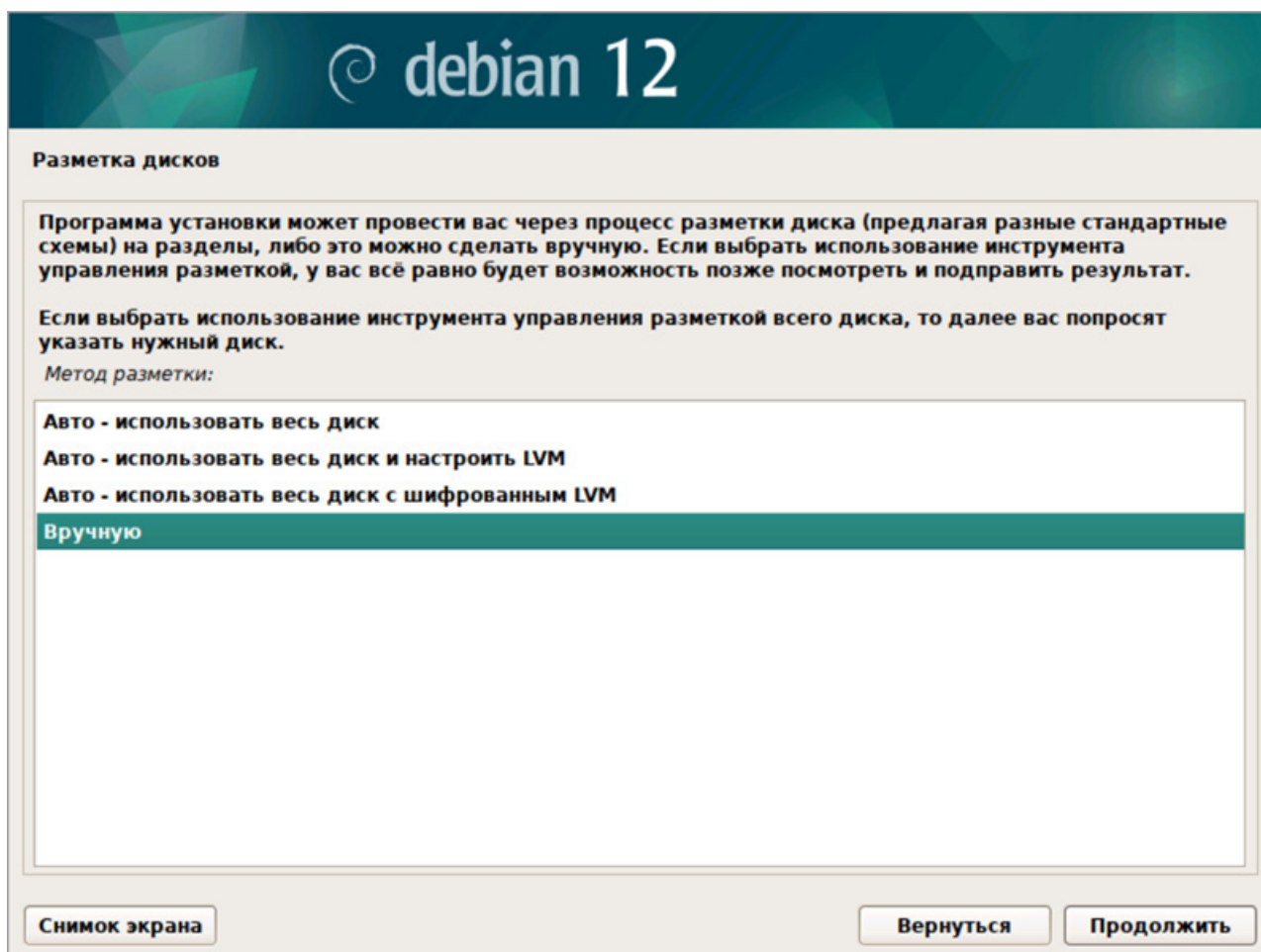


Рисунок 23. Выбор способа разметки диска

14. Выберите жесткий диск.
15. Подтвердите создание новой таблицы разделов, выбрав **Да** и нажав **Продолжить**.
16. Создайте основной корневой раздел системы:
 - Выберите в таблице разделов область с пометкой **Свободное место**.
 - На этапе выбора действий со свободным пространством выберите вариант **Создать новый раздел**.
 - В поле **Новый размер раздела** введите объем основного раздела (доступное дисковое пространство минус объем раздела подкачки в соответствии с [программными требованиями](#) (см. раздел 3.2)).
 - На этапе выбора типа нового раздела выберите вариант **Первичный**.
 - На этапе выбора местоположения нового раздела выберите вариант **Начало**.
 - В таблице **Настройки раздела** выберите параметры, как показано на рисунке ниже, и после этого выберите вариант **Настройка раздела закончена**.



Рисунок 24. Параметры корневого раздела системы

В таблице разделов появится вторая область с пометкой **Свободное место**.

17. Создайте раздел подкачки:

- Выберите в таблице разделов вторую область с пометкой **Свободное место**.
- На этапе выбора действий со свободным пространством выберите вариант **Создать новый раздел**.
- В поле **Новый размер раздела** введите объем раздела подкачки в соответствии с [программными требованиями \(см. раздел 3.2\)](#).
- На этапе выбора типа нового раздела выберите вариант **Логический**.
- В таблице **Настройки раздела** выберите параметр **Использовать как** и выберите для него значение **Раздел подкачки**.
- По окончании настройки выберите вариант **Настройка раздела закончена**.

18. На этапе разметки дисков выберите вариант **Закончить разметку и записать изменения на диск** и нажмите **Продолжить**.

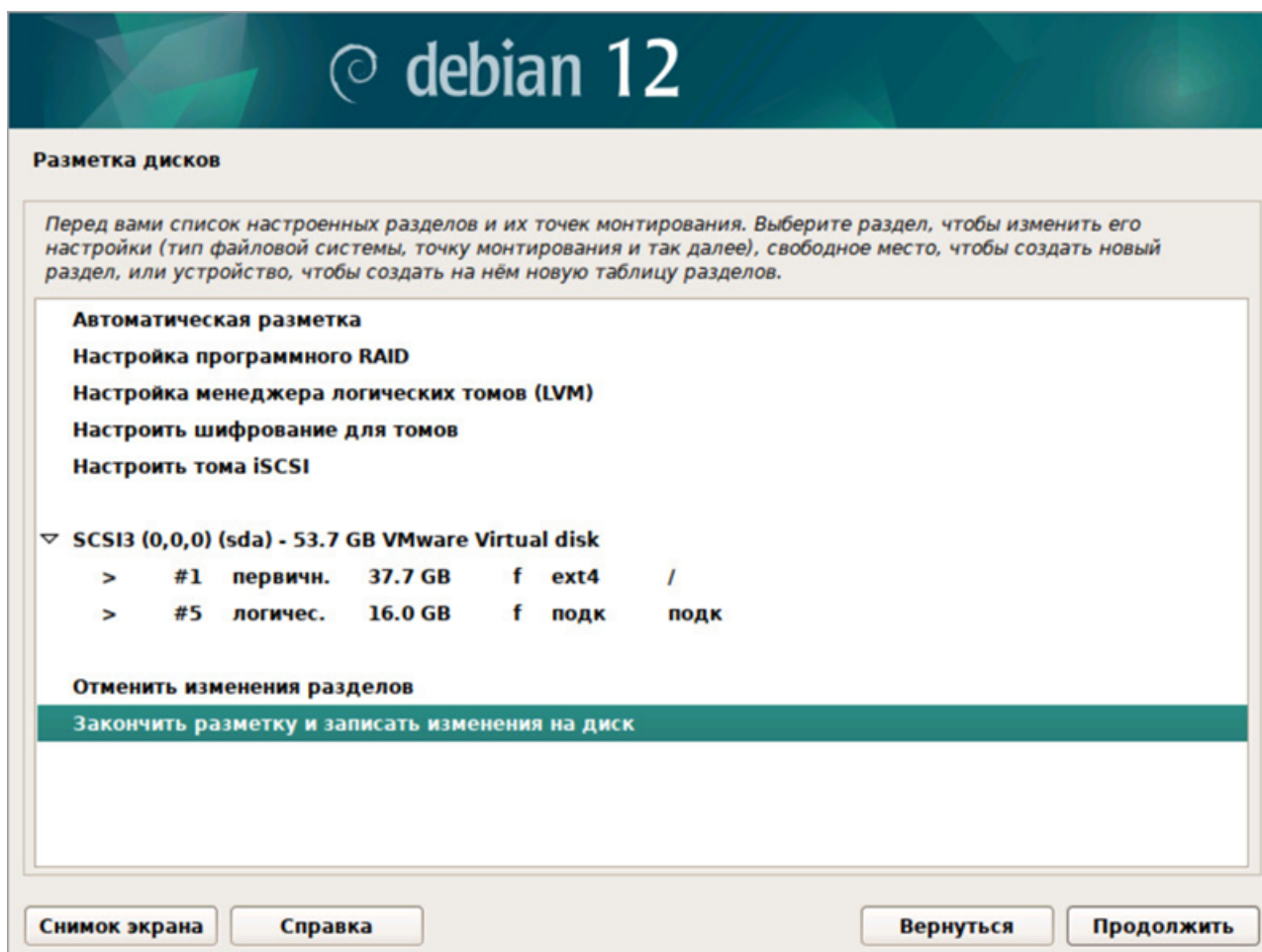


Рисунок 25. Разметка дисков

19. Подтвердите запись изменений на диск, выбрав **Да** и нажав **Продолжить**.

Запустится процесс установки базовых компонентов системы.

20. На этапе настройки менеджера пакетов выберите вариант **Нет** при ответе на вопрос о сканировании другого диска и нажмите **Продолжить**.

21. Выберите вариант **Нет** при ответе на вопрос об использовании зеркала архива и нажмите **Продолжить**.

Запустится процесс автоматического выбора и установки базовых компонентов системы.

22. На этапе настройки пакета popularity-contest выберите вариант **Нет** при ответе на вопрос об участии в опросе и нажмите **Продолжить**.

23. На этапе выбора программного обеспечения выберите **SSH-сервер** и **Стандартные системные утилиты**.

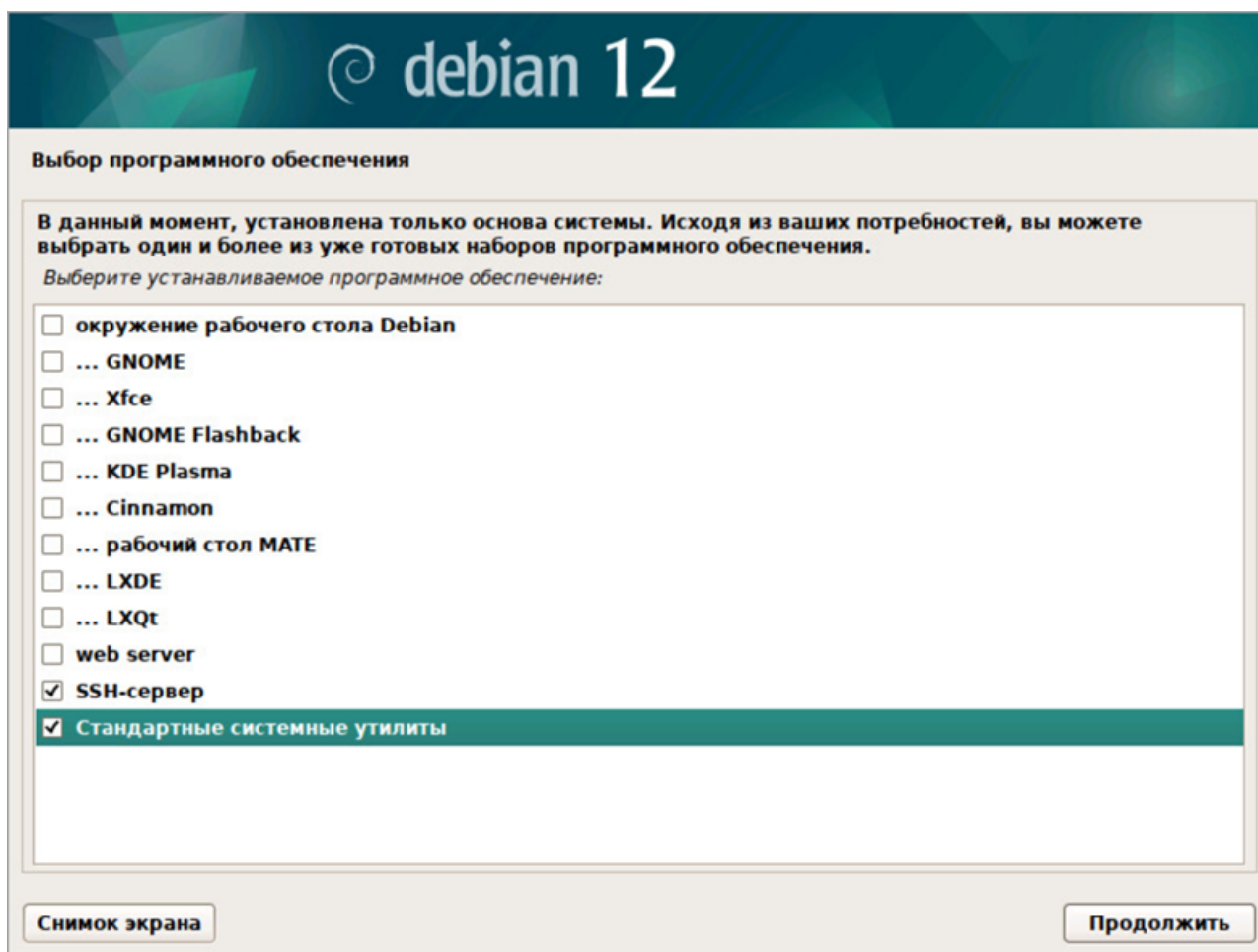


Рисунок 26. Выбор программного обеспечения

Снова запустится процесс автоматического выбора и установки базовых компонентов системы.

24. Подтвердите установку системного загрузчика GRUB на жесткий диск, выбрав **Да** и нажав **Продолжить**.

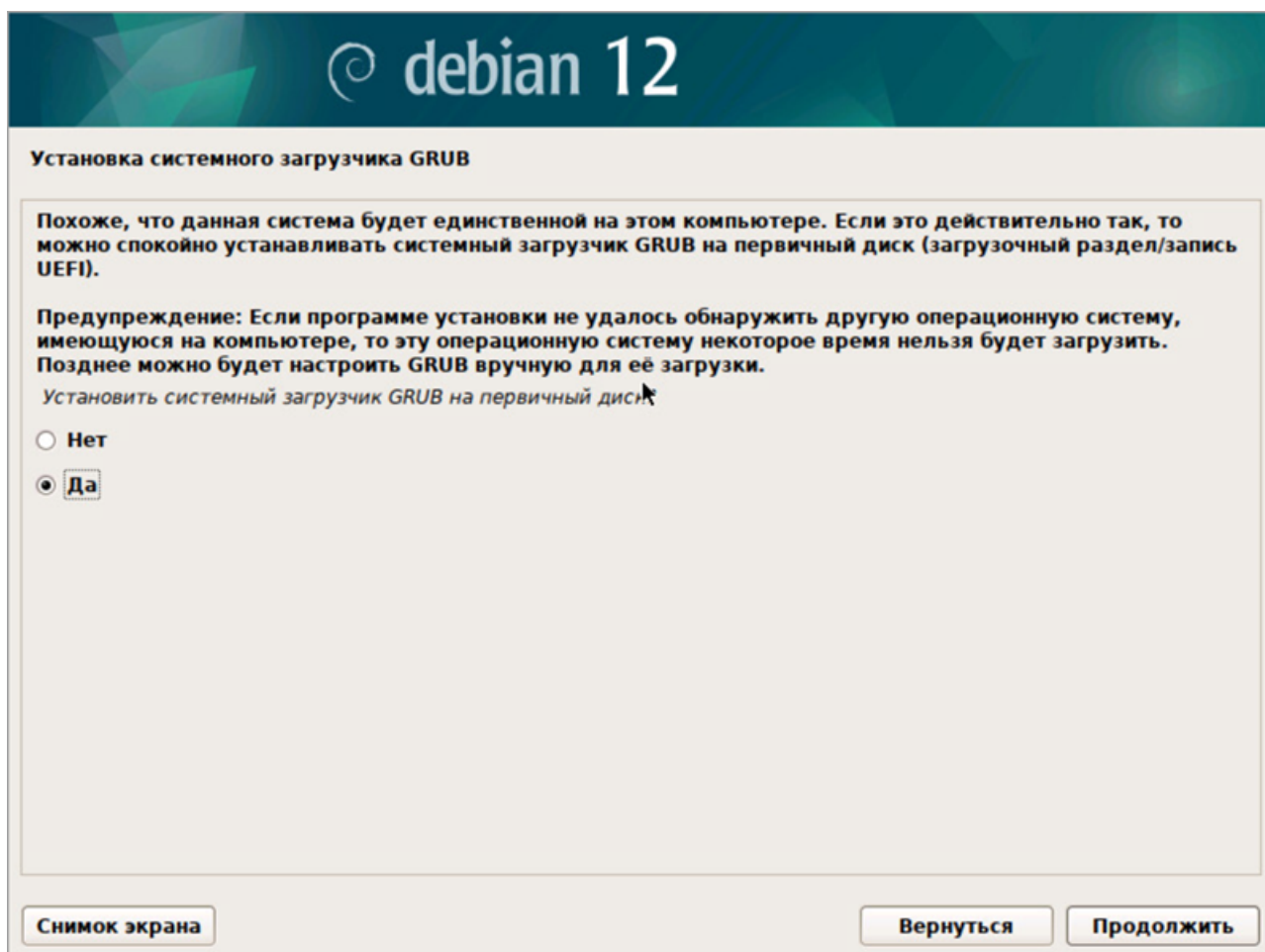


Рисунок 27. Установка системного загрузчика GRUB

25. Укажите раздел для загрузки ОС и нажмите **Продолжить**.



Рисунок 28. Выбор раздела загрузки ОС

26. На этапе завершения установки отключите внешний носитель от компьютера и после этого нажмите **Продолжить**.

Система перезапустится.

Внимание! На этом этапе не отключайте питание и принудительно не перезагружайте компьютер, поскольку это приведет к неработоспособности системы.

Установка Debian завершена.

5.1.3. Обновление Debian

Вы можете обновить операционную систему Debian 10 до Debian 12 без потери накопленных данных PT ISIM. Для обновления требуется, чтобы на сервере были сохранены [установочные образы \(см. раздел 3.2\)](#) Debian 11 и Debian 12, а также установочный комплект PT ISIM версии 5.1 или выше для Debian 12. Перед обновлением операционной системы необходимо обновить PT ISIM до версии 5.1 или выше.

Внимание! Если перед установкой PT ISIM корневой раздел диска был создан с помощью Logical Volume Management, то после обновления PT ISIM и операционной системы может потребоваться активация новой лицензии.

Примечание. Для обновления операционной системы Debian 9 до Debian 12 необходимо сначала выполнить обновление до Debian 10 по инструкции, приведенной в Руководстве администратора PT ISIM версии 4.5, а затем обновить Debian до версии 12 по инструкции ниже.

► Чтобы обновить Debian:

1. Создайте скрипт обновления:

```
touch upgrade_deb10_to_deb11.sh
```

2. Откройте созданный файл для редактирования:

```
nano upgrade_deb10_to_deb11.sh
```

3. Добавьте в файл следующее содержание:

```
#!/bin/bash \
set -ex \
ISO_NAME=${1:-/root/debian-11.11.0-amd64-DVD-1.iso} \
MOUNT_POINT=${2:-/media/iso/} \
mkdir -p "$MOUNT_POINT" \
umount "$MOUNT_POINT" || true \
mount -o loop "$ISO_NAME" "$MOUNT_POINT" \
find /etc/apt/sources.list.d \
-name *.list \
-type f \
-exec bash -c 'mv $0 ${0}.$(date -I).save' {} \; \
cat >/etc/apt/sources.list <<EOL \
deb [trusted=yes arch=amd64] file:///"$MOUNT_POINT" bullseye main contrib \
EOL \
export DEBIAN_FRONTEND=noninteractive \
apt-get update \
apt --yes remove pt-g++-11 chromium || true \
apt --yes --quiet \
-o Dpkg::Options::="--force-confdef" \
-o Dpkg::Options::="--force-confold" \
upgrade --allow-unauthenticated --no-install-recommends --no-install-suggests \
dpkg -l | grep nginx-light && apt-mark hold nginx-light libnginx-mod-http-lua || true \
systemctl stop ptisim-watchdog.timer || true \
for i in `systemctl | awk '{print $1}' | grep ptisim-`; \
do \
    systemctl stop $i && echo "$i stopped" || echo "$i skipped!"; \
done \
systemctl stop rabbitmq-server.service || true \
apt-get --yes --quiet --force-yes \
-o Dpkg::Options::="--force-confdef" \
-o Dpkg::Options::="--force-confold" \
dist-upgrade --allow-unauthenticated \
```

```
dpkg -l | grep nginx-light && apt-mark unhold nginx-light libnginx-mod-http-lua || true \
apt --yes autoremove || true \
```

4. Сохраните изменения с помощью комбинации клавиш Ctrl+O и закройте файл.
5. Предоставьте созданному скрипту права на исполнение:

```
chmod +x upgrade_deb10_to_deb11.sh
```
6. Запустите скрипт обновления:

```
./upgrade_deb10_to_deb11.sh
```
7. Если требуется, на этапе подтверждения обновления выберите вариант **Yes** при ответе на вопрос **Do you want to upgrade glibc now?**
8. Если требуется, на этапе настройки автоматического перезапуска сервисов выберите вариант **Yes** при ответе на вопрос **Restart services during package upgrades without asking?**
9. Если требуется, на этапе настройки обновления конфигурационного файла `sshd_config` выберите вариант **install the package maintainer's version** и нажмите кнопку **OK**.
10. Перезагрузите систему:

```
sudo reboot
```
11. Создайте скрипт обновления:

```
touch upgrade_deb11_to_deb12.sh
```
12. Откройте созданный файл для редактирования:

```
nano upgrade_deb11_to_deb12.sh
```
13. Добавьте в файл следующее содержание:

```
#!/bin/bash \
set -ex \
ISO_NAME=${1:-/root/debian-12.8.0-amd64-DVD-1.iso} \
MOUNT_POINT=${2:-/media/iso/} \
mkdir -p "$MOUNT_POINT" \
umount "$MOUNT_POINT" || true \
mount -o loop "$ISO_NAME" "$MOUNT_POINT" \
find /etc/apt/sources.list.d \
-name *.list \
-type f \
-exec bash -c 'mv $0 ${0}.$(date -I).save' {} \; \
cat >/etc/apt/sources.list <<EOL \
deb [trusted=yes arch=amd64] file:///"$MOUNT_POINT" bookworm main contrib \
EOL \
export DEBIAN_FRONTEND=noninteractive \
apt-get update \
apt --yes --quiet \
-o Dpkg::Options::="--force-confdef" \
-o Dpkg::Options::="--force-confold" \
upgrade --allow-unauthenticated --no-install-recommends --no-install-suggests \
dpkg -l | grep nginx-light && apt-mark hold nginx-light libnginx-mod-http-lua || true \
```

```
apt-get --yes --quiet --force-yes \
-o Dpkg::Options::="--force-confdef" \
-o Dpkg::Options::="--force-confold" \
dist-upgrade --allow-unauthenticated \
dpkg -l | grep nginx-light && apt-mark unhold nginx-light libnginx-mod-http-lua || true \
apt --yes autoremove || true \
```

14. Сохраните изменения с помощью комбинации клавиш Ctrl+O и закройте файл.
15. Предоставьте созданному скрипту права на исполнение:

```
chmod +x upgrade_deb11_to_deb12.sh
```
16. Запустите скрипт обновления:

```
./upgrade_deb11_to_deb12.sh
```
17. Если требуется, на этапе подтверждения обновления выберите вариант **Yes** при ответе на вопрос **Do you want to upgrade glibc now?**.
18. Если требуется, на этапе настройки автоматического перезапуска сервисов выберите вариант **Yes** при ответе на вопрос **Restart services during package upgrades without asking?**.
19. Если требуется, на этапе настройки обновления конфигурационного файла `sshd_config` выберите вариант **install the package maintainer's version** и нажмите кнопку **OK**.
20. Перезагрузите систему:

```
sudo reboot
```

5.1.4. Установка Astra Linux

В этом разделе приведена инструкция по установке Astra Linux Special Edition 1.7.6 UU2 в режиме защищенности «Воронеж» или «Смоленск».

Перед началом установки Astra Linux в меню настройки BIOS требуется указать загрузочное устройство (например, USB-накопитель) с необходимым образом операционной системы.

► Чтобы установить Astra Linux:

1. Подключите к компьютеру внешний носитель с загрузочным образом Astra Linux.
2. Дождавшись загрузки первичного окна выбора вариантов установки, выберите **Графическая установка** или **Установка** (на рисунках ниже представлены снимки экрана для выбранного варианта **Графическая установка**).
3. В левом нижнем углу экрана в меню выбора языка выберите **Русский**.

Примечание. Через пять секунд после загрузки первичного окна установки операционной системы будет автоматически выбран вариант **Графическая установка** и язык **Русский**. Если вы хотите изменить язык, вам нужно нажать кнопку **Вернуться**. Если вы хотите изменить вариант установки, вам нужно отменить установку или перезагрузить компьютер и начать установку заново.

Отобразится лицензионное соглашение.

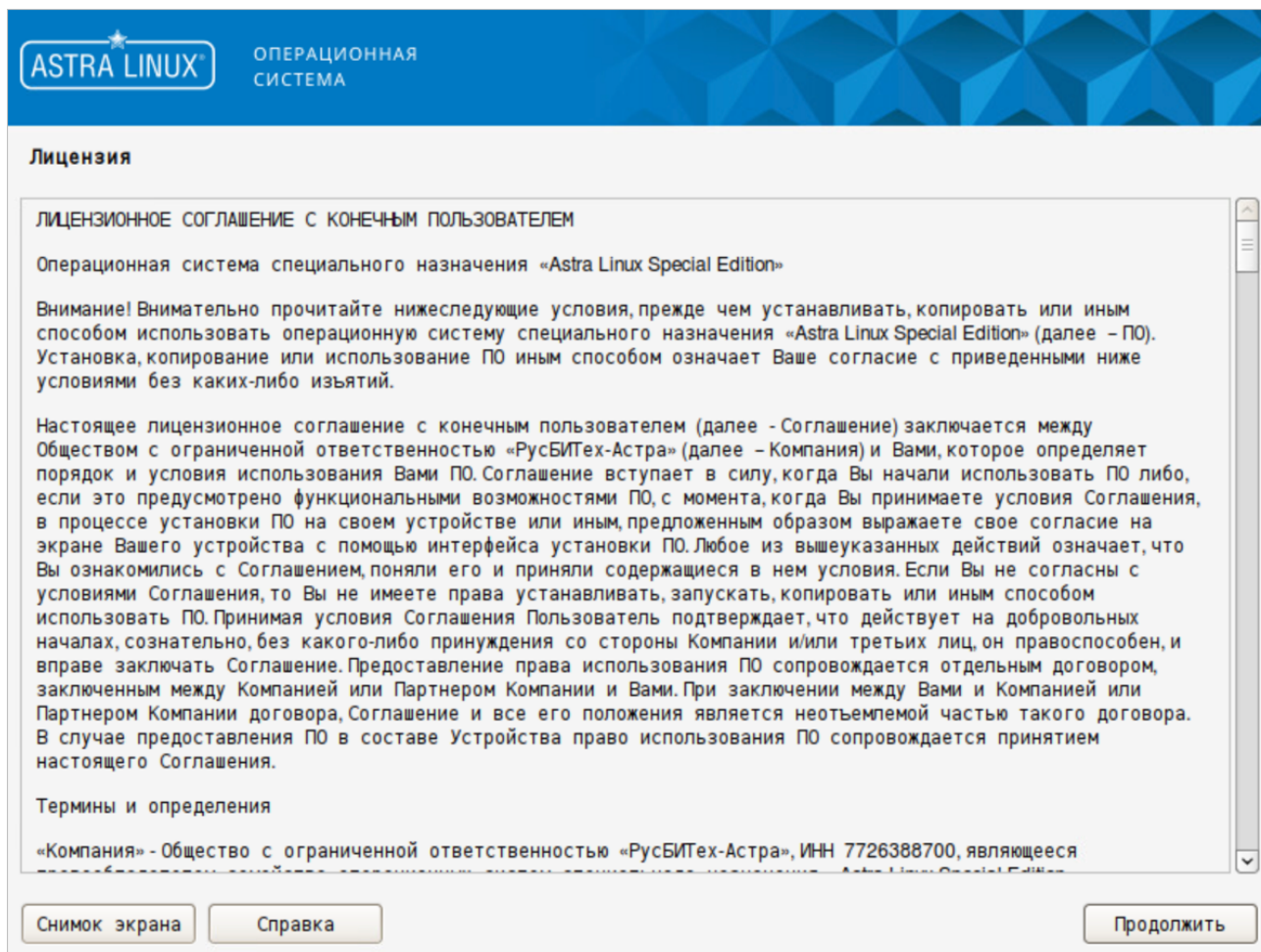


Рисунок 29. Лицензионное соглашение Astra Linux

4. Примите условия лицензионного соглашения, выбрав **Да** и нажав **Продолжить**.
5. На этапе выбора способа переключения между национальной и латинской раскладкой выберите сочетание клавиш и нажмите **Продолжить**.
6. Если требуется, выберите основной сетевой интерфейс.
7. На этапе настройки сети задайте имя компьютера и нажмите **Продолжить**.

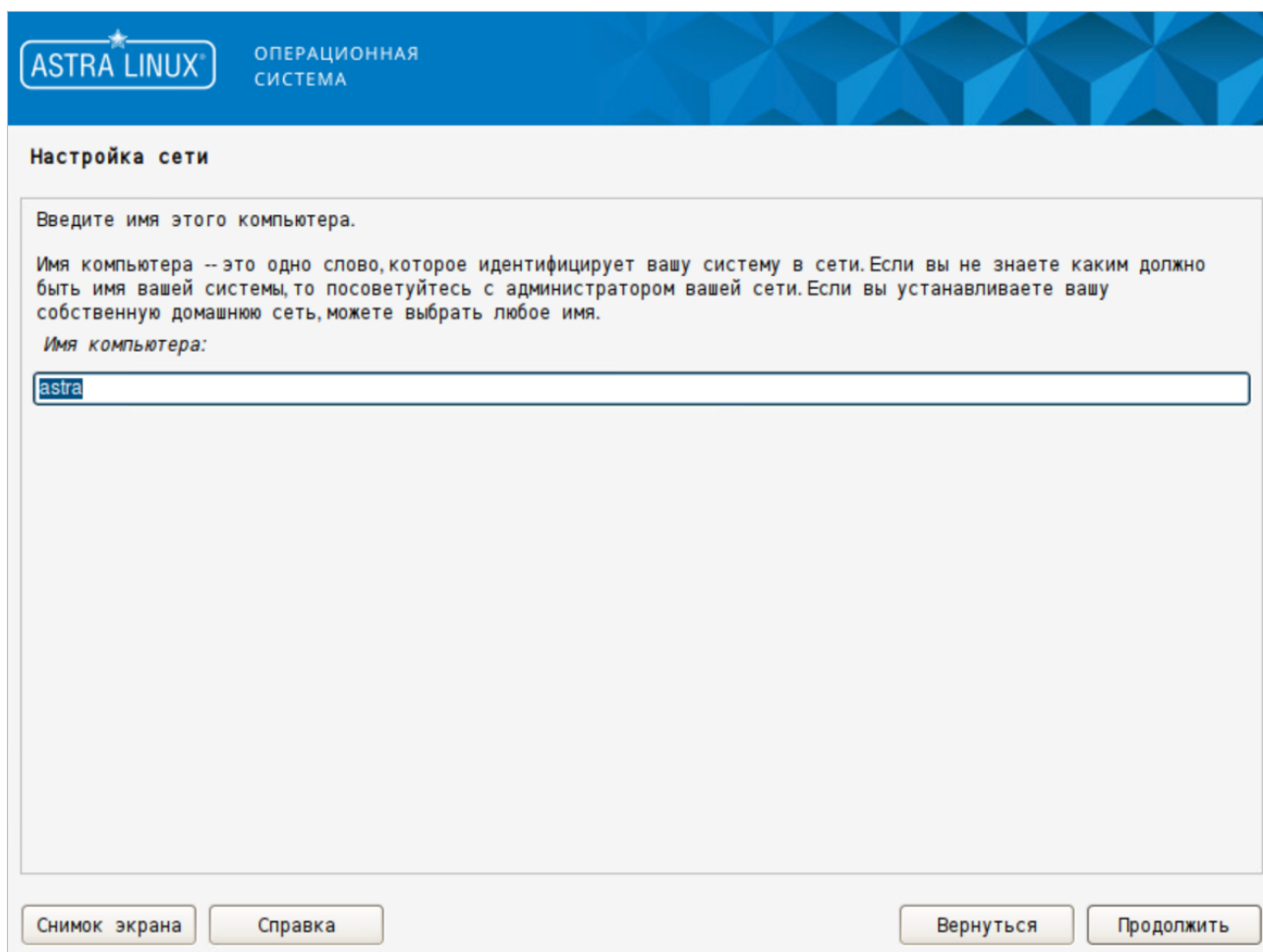


Рисунок 30. Настройка сети

8. Задайте имя домена и нажмите **Продолжить**.

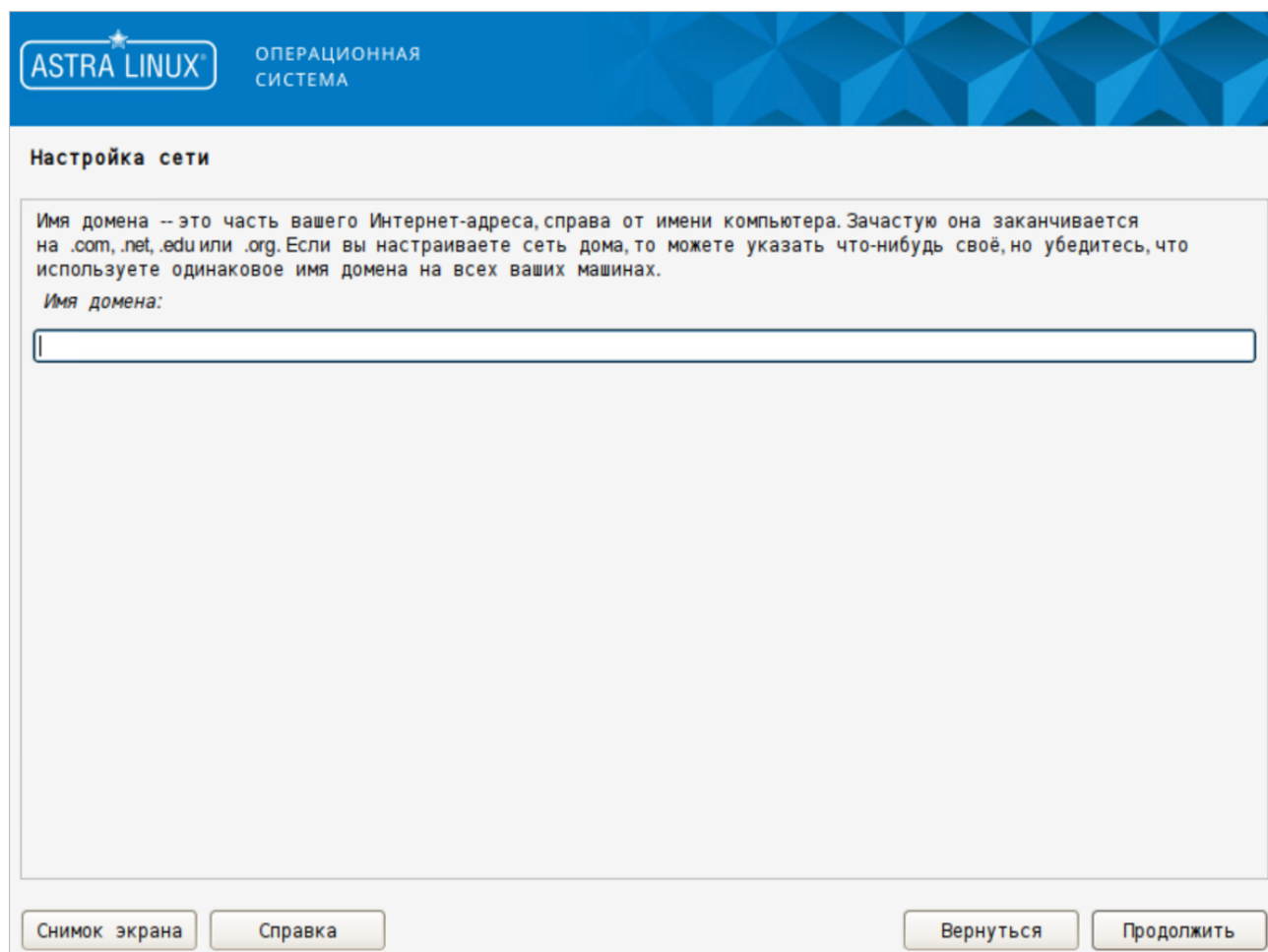
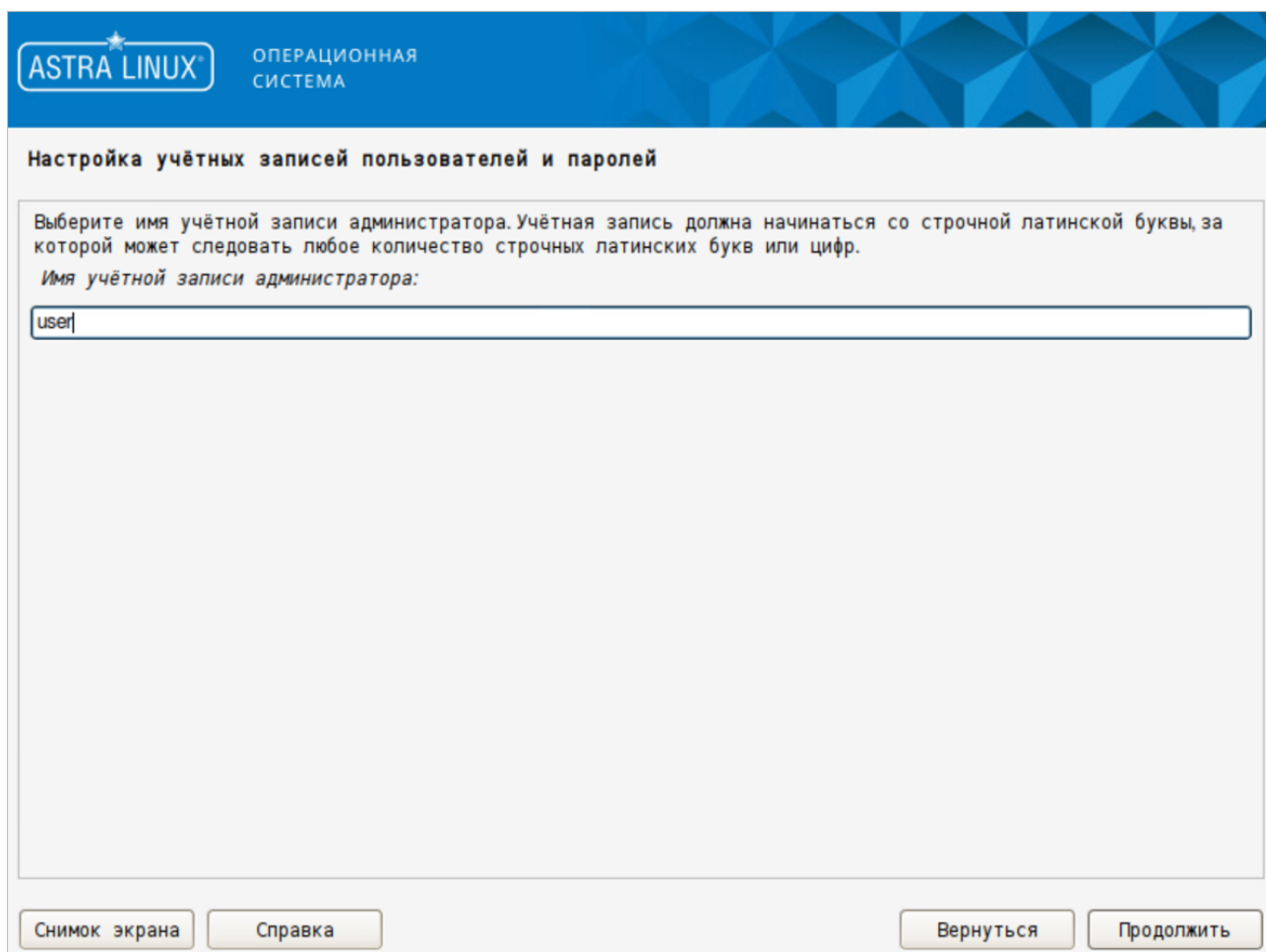


Рисунок 31. Настройка сети

9. На этапе настройки учетных записей пользователей и паролей создайте новую учетную запись администратора, указав ее имя и нажав **Продолжить**.



The screenshot shows the 'ASTRA LINUX' logo and 'ОПЕРАЦИОННАЯ СИСТЕМА' (Operating System) in the top header. The main title is 'Настройка учётных записей пользователей и паролей' (User account and password configuration). The instructions state: 'Выберите имя учётной записи администратора. Учётная запись должна начинаться со строчной латинской буквы, за которой может следовать любое количество строчных латинских букв или цифр.' (Choose the administrator account name. The account name must start with a lowercase Latin letter, followed by any number of lowercase Latin letters or digits). Below this, it says 'Имя учётной записи администратора:' (Administrator account name:). A text input field contains the text 'user'. At the bottom, there are four buttons: 'Снимок экрана' (Screenshot), 'Справка' (Help), 'Вернуться' (Back), and 'Продолжить' (Continue).

ASTRA LINUX[®] ОПЕРАЦИОННАЯ СИСТЕМА

Настройка учётных записей пользователей и паролей

Выберите имя учётной записи администратора. Учётная запись должна начинаться со строчной латинской буквы, за которой может следовать любое количество строчных латинских букв или цифр.

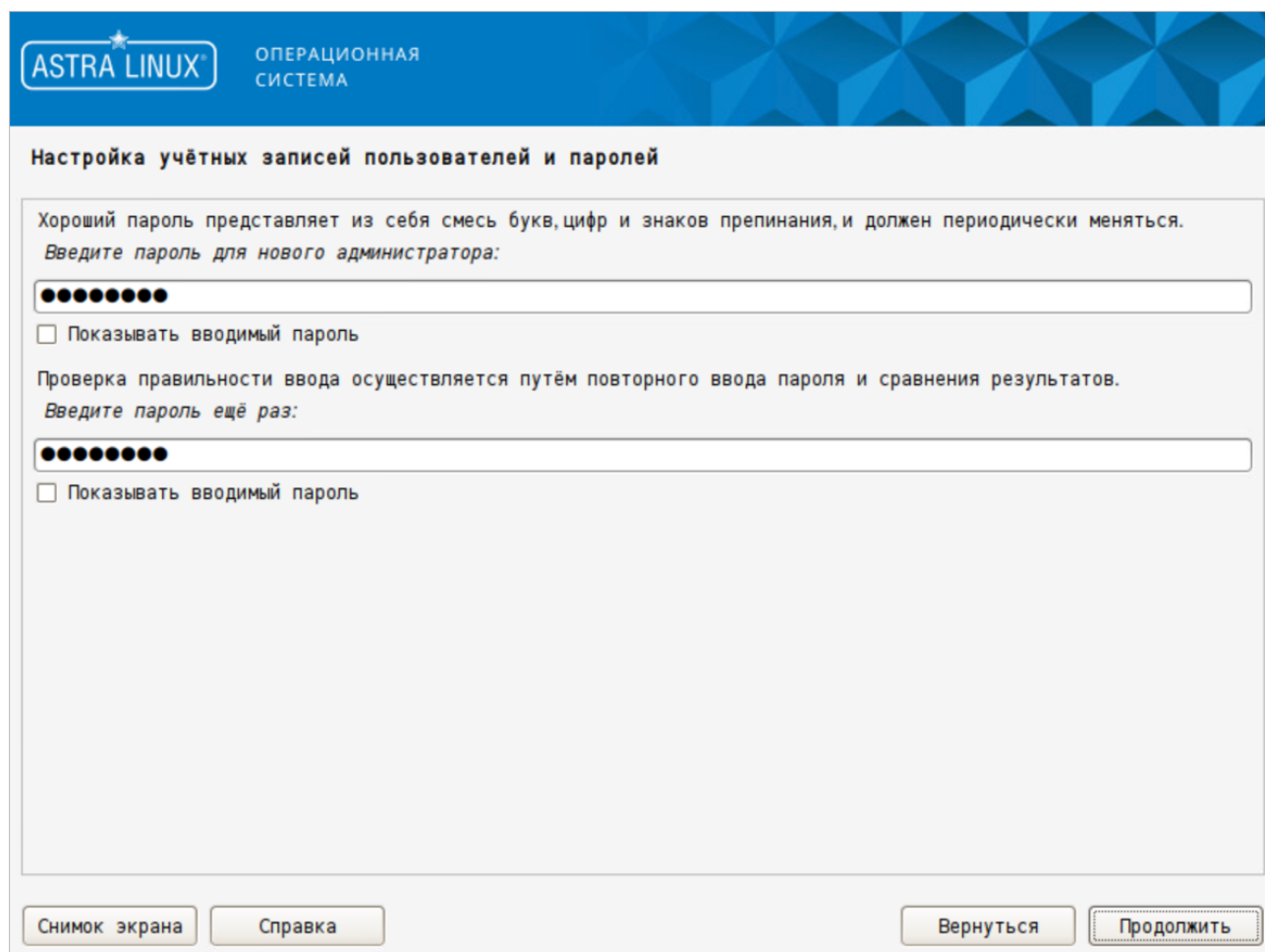
Имя учётной записи администратора:

user

Снимок экрана Справка Вернуться Продолжить

Рисунок 32. Настройка учетных записей пользователей и паролей

10. Укажите пароль для новой учетной записи администратора, введите его повторно и нажмите **Продолжить**.



The screenshot shows the 'ASTRA LINUX' logo and 'ОПЕРАЦИОННАЯ СИСТЕМА' (Operating System) in the top left. The main title is 'Настройка учётных записей пользователей и паролей' (User account configuration). The text explains that a good password is a mix of letters, numbers, and punctuation, and should change periodically. It prompts the user to 'Введите пароль для нового администратора:' (Enter password for the new administrator:). Below this is a password input field with 10 dots. A checkbox 'Показывать вводимый пароль' (Show entered password) is present. The next instruction is 'Проверка правильности ввода осуществляется путём повторного ввода пароля и сравнения результатов.' (Verification of correct input is performed by re-entering the password and comparing the results). It then prompts 'Введите пароль ещё раз:' (Enter password again:). This is followed by another password input field with 10 dots and the same 'Показывать вводимый пароль' checkbox. At the bottom, there are four buttons: 'Снимок экрана' (Screenshot), 'Справка' (Help), 'Вернуться' (Back), and 'Продолжить' (Continue).

ASTRA LINUX[®] ОПЕРАЦИОННАЯ СИСТЕМА

Настройка учётных записей пользователей и паролей

Хороший пароль представляет из себя смесь букв, цифр и знаков препинания, и должен периодически меняться.
Введите пароль для нового администратора:

●●●●●●●●

☐ Показывать вводимый пароль

Проверка правильности ввода осуществляется путём повторного ввода пароля и сравнения результатов.
Введите пароль ещё раз:

●●●●●●●●

☐ Показывать вводимый пароль

Снимок экрана Справка Вернуться Продолжить

Рисунок 33. Настройка учетной записи администратора

11. На этапе настройки времени выберите часовой пояс и нажмите **Продолжить**.

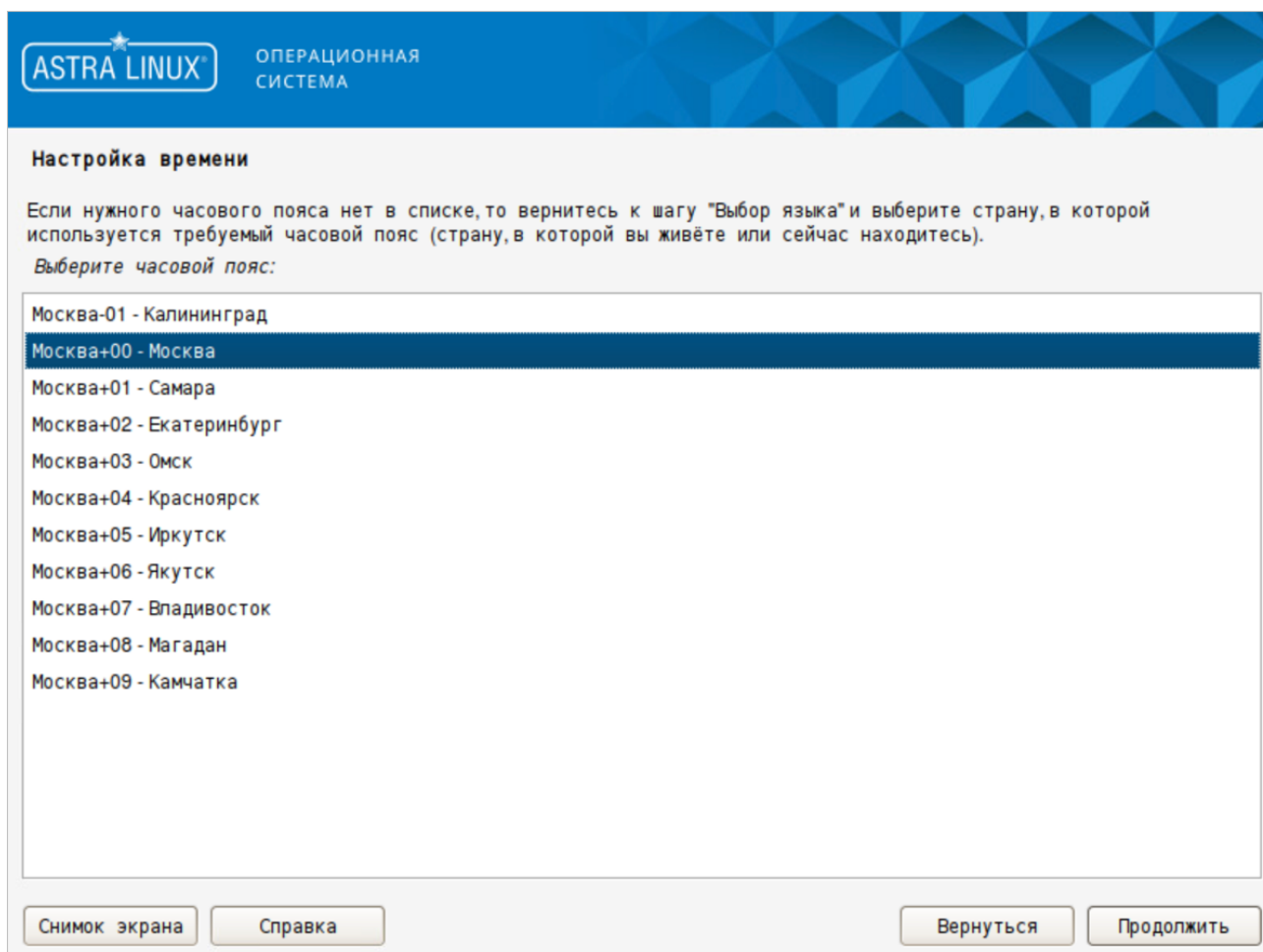


Рисунок 34. Выбор часового пояса

12. На этапе разметки дисков выберите вариант **Вручную** и нажмите **Продолжить**.

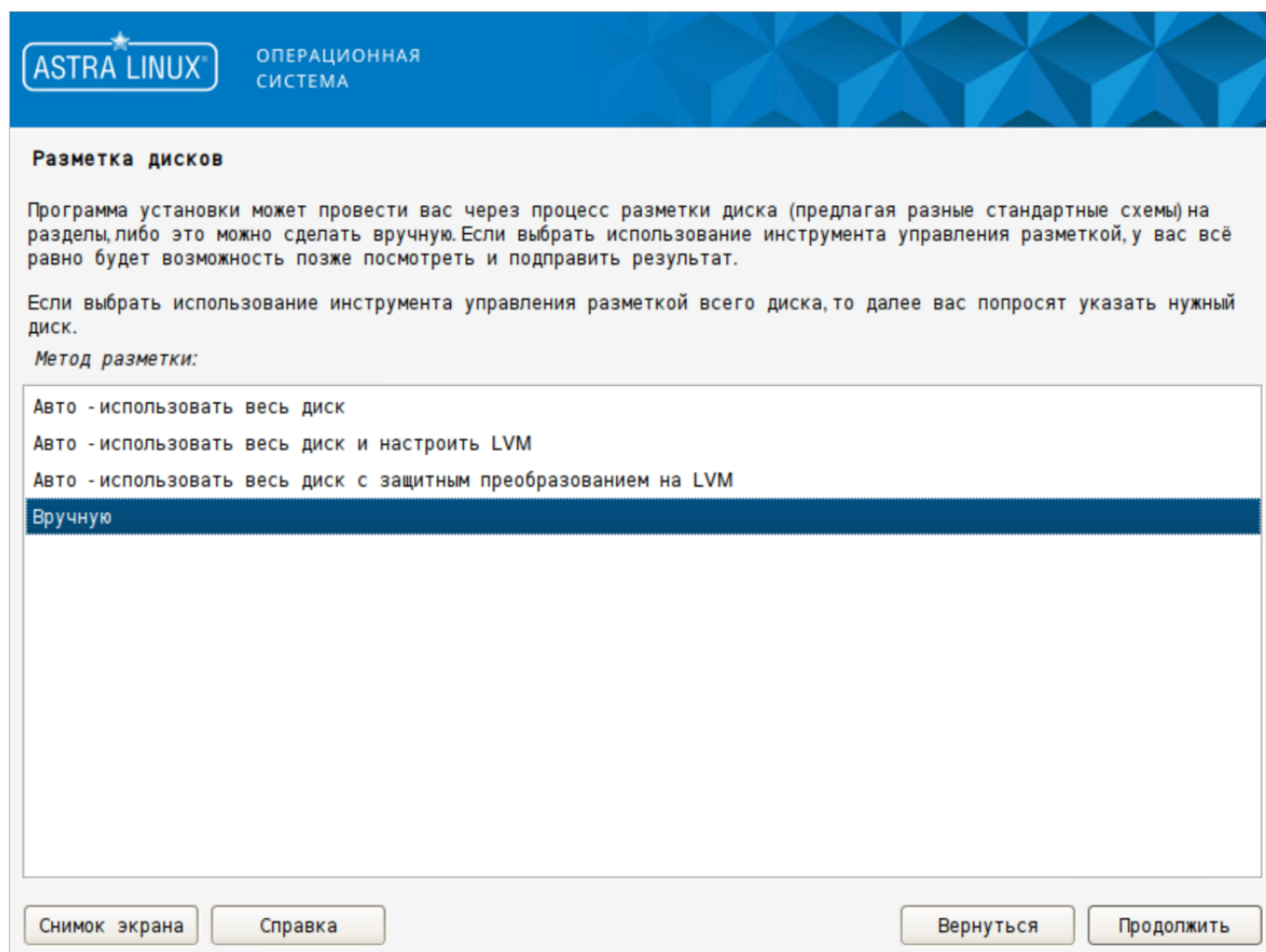


Рисунок 35. Выбор способа разметки диска

13. Выберите жесткий диск.
14. Подтвердите создание новой таблицы разделов, выбрав **Да** и нажав **Продолжить**.
15. Создайте основной корневой раздел системы:
 - Выберите в таблице разделов область с пометкой **Свободное место**.
 - На этапе выбора действий со свободным пространством выберите вариант **Создать новый раздел**.
 - В поле **Новый размер раздела** введите объем основного раздела (доступное дисковое пространство минус объем раздела подкачки в соответствии с [программными требованиями](#) (см. раздел 3.2)).
 - На этапе выбора типа нового раздела выберите вариант **Первичный**.
 - На этапе выбора местоположения нового раздела выберите вариант **Начало**.
 - В таблице **Настройки раздела** выберите параметры, как показано на рисунке ниже, и после этого выберите вариант **Настройка раздела закончена**.

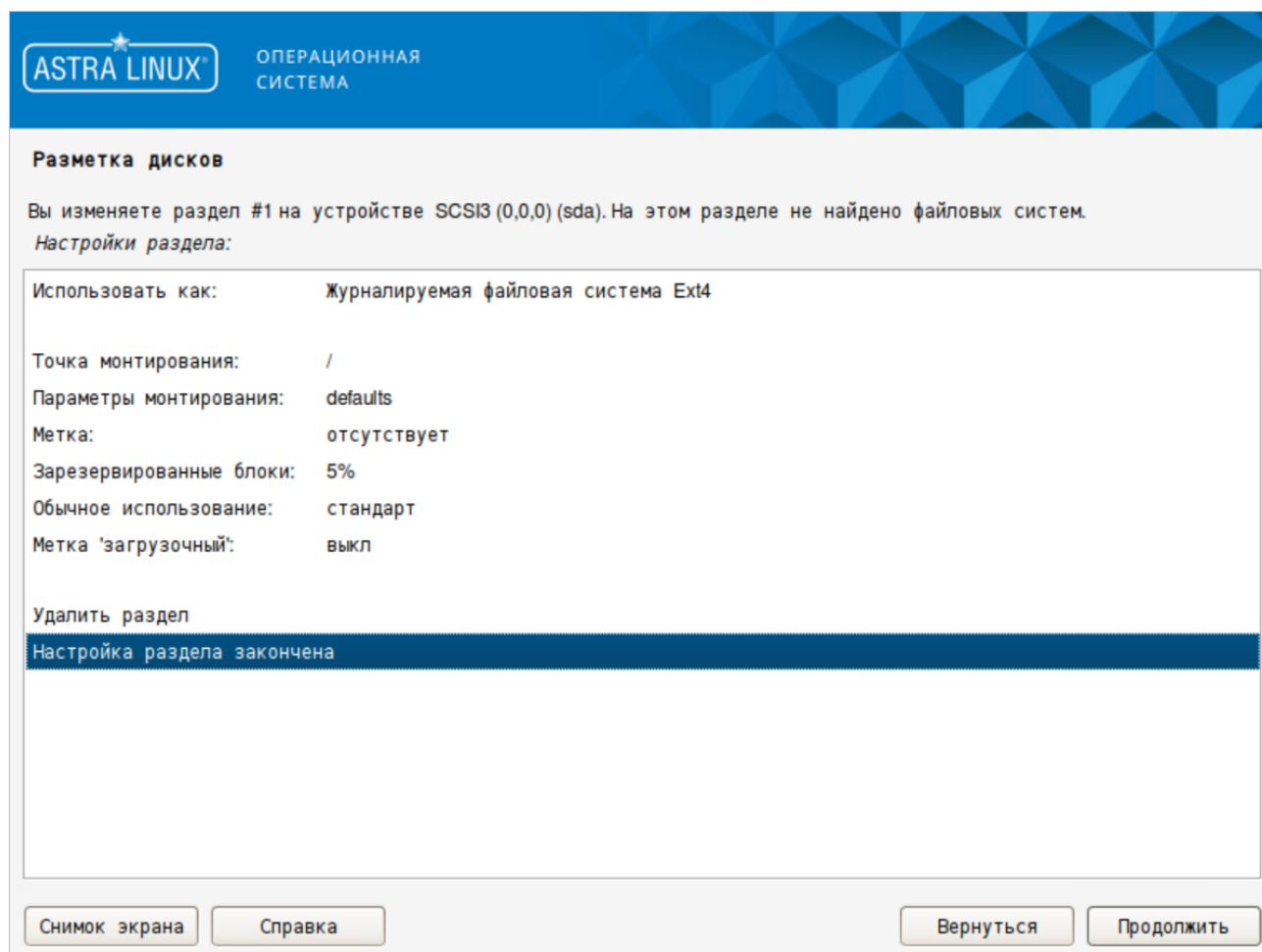


Рисунок 36. Параметры корневого раздела системы

В таблице разделов появится вторая область с пометкой **Свободное место**.

16. Создайте раздел подкачки:

- Выберите в таблице разделов вторую область с пометкой **Свободное место**.
- На этапе выбора действий со свободным пространством выберите вариант **Создать новый раздел**.
- В поле **Новый размер раздела** введите объем раздела подкачки в соответствии с [программными требованиями \(см. раздел 3.2\)](#).
- На этапе выбора типа нового раздела выберите вариант **Логический**.
- В таблице **Настройки раздела** выберите параметр **Использовать как** и выберите для него значение **Раздел подкачки**.
- По окончании настройки выберите вариант **Настройка раздела закончена**.

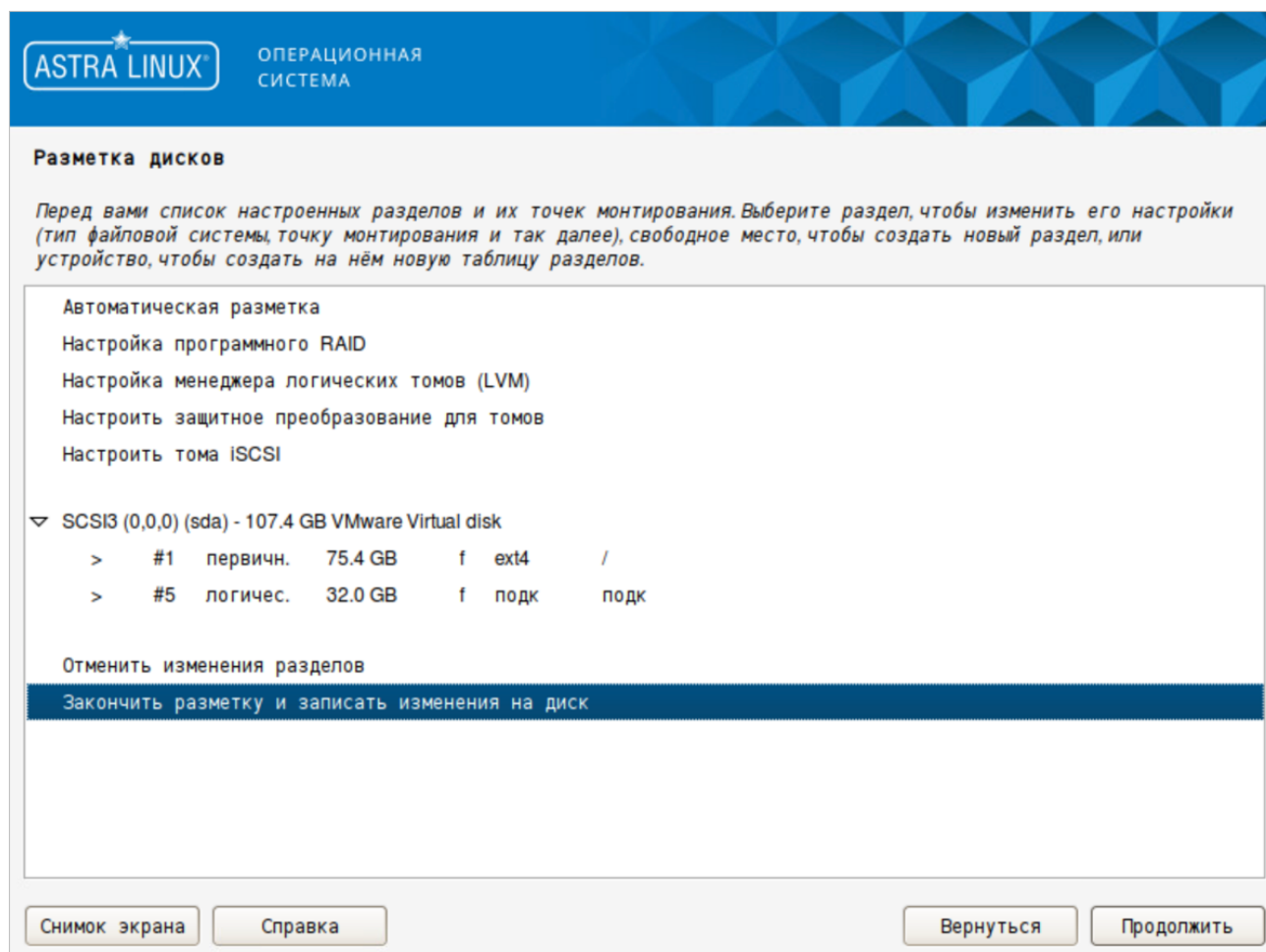


Рисунок 37. Разметка дисков

17. На этапе разметки дисков выберите вариант **Закончить разметку и записать изменения на диск** и нажмите **Продолжить**.
18. Подтвердите запись изменений на диск, выбрав **Да** и нажав **Продолжить**.
19. На этапе установки базовой системы оставьте выбранным ядро для установки по умолчанию (**linux-6.1-generic**) и нажмите **Продолжить**.

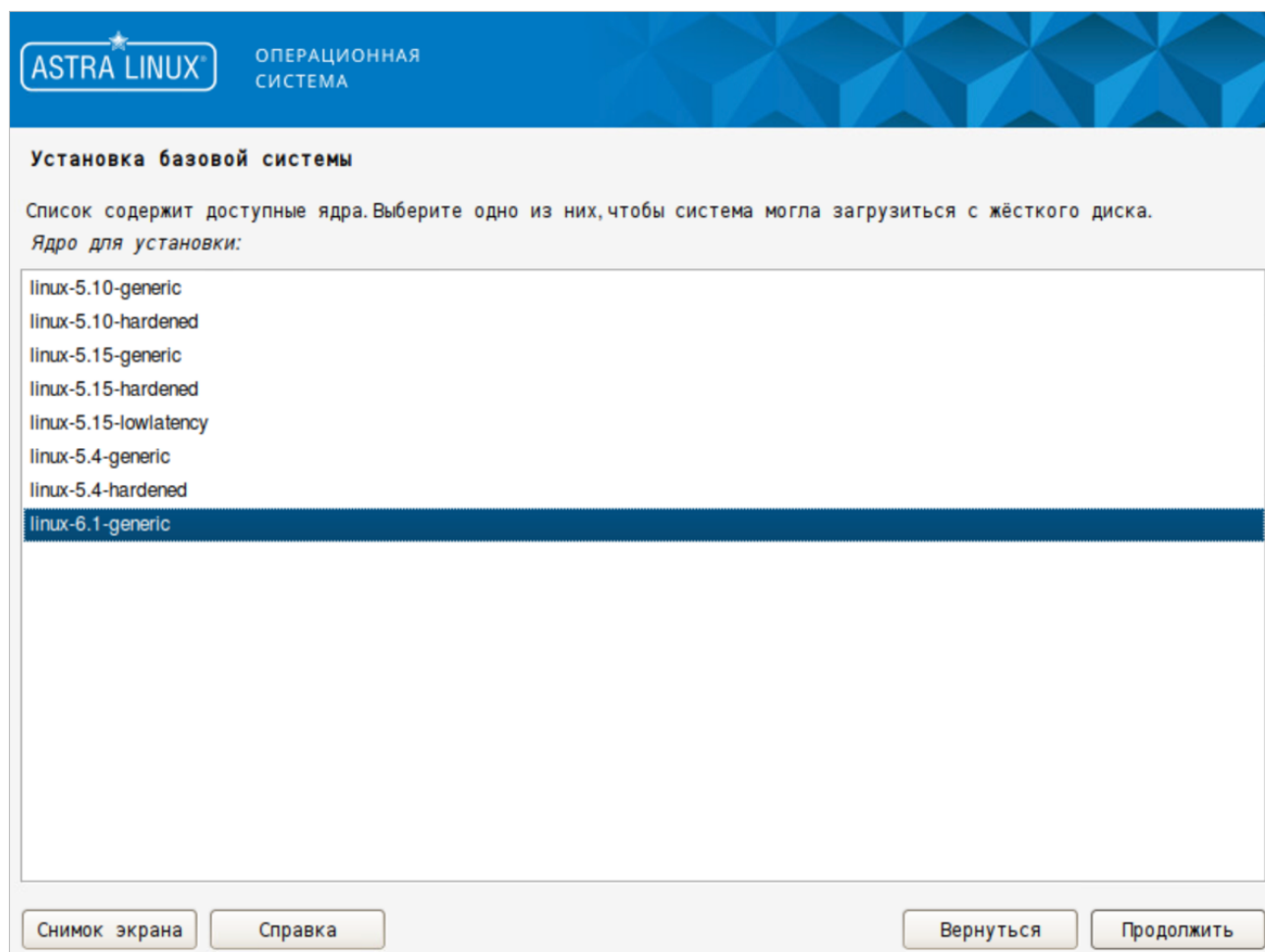


Рисунок 38. Установка базовой системы

20. На этапе выбора программного обеспечения выберите **Консольные утилиты** и **Средства удаленного подключения SSH** и нажмите **Продолжить**.

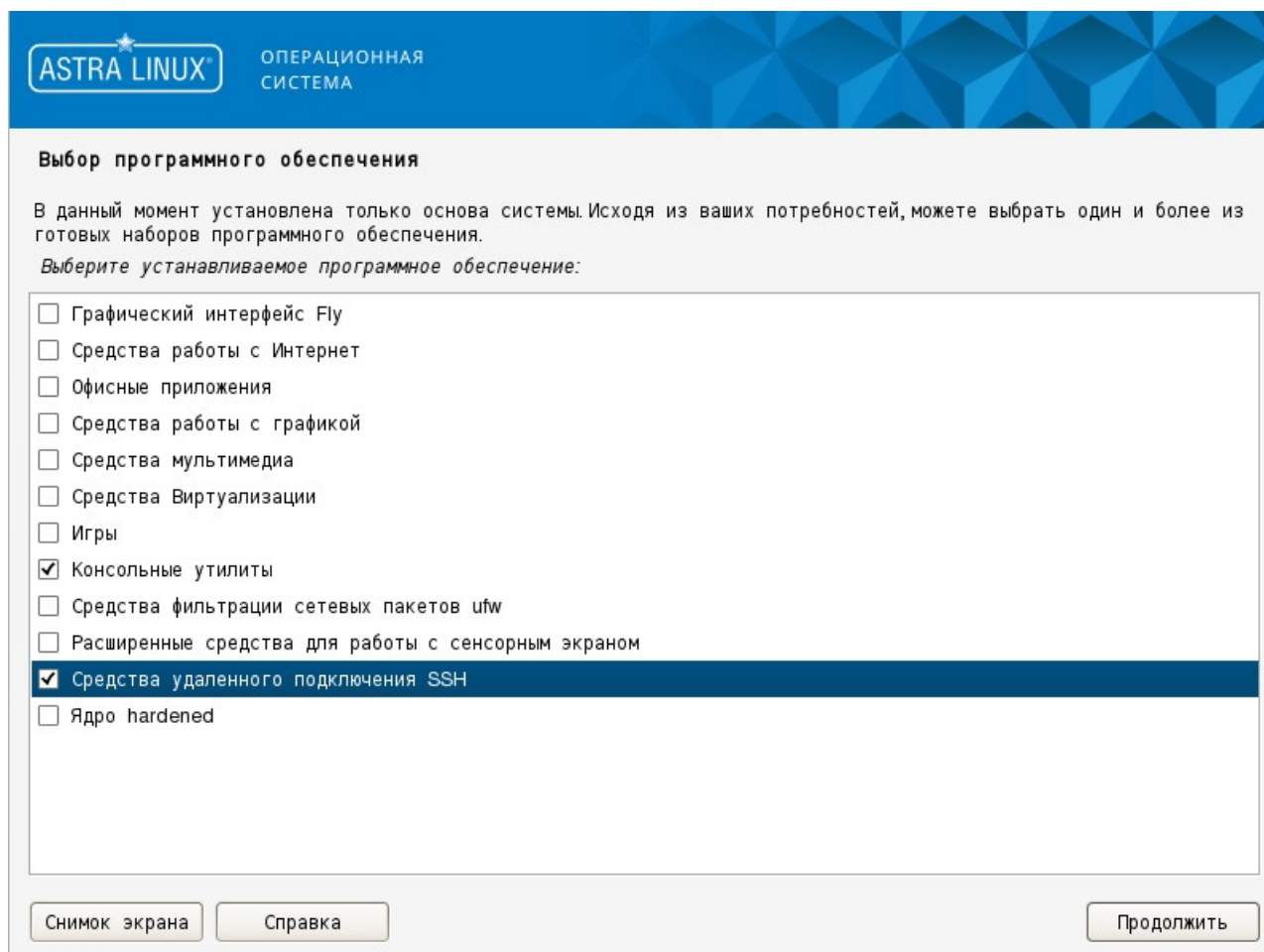


Рисунок 39. Выбор программного обеспечения

21. На этапе дополнительной настройки ОС выберите **Максимальный уровень защищенности «Смоленск»** или **Усиленный уровень защищенности «Воронеж»** и нажмите кнопку **Продолжить**.

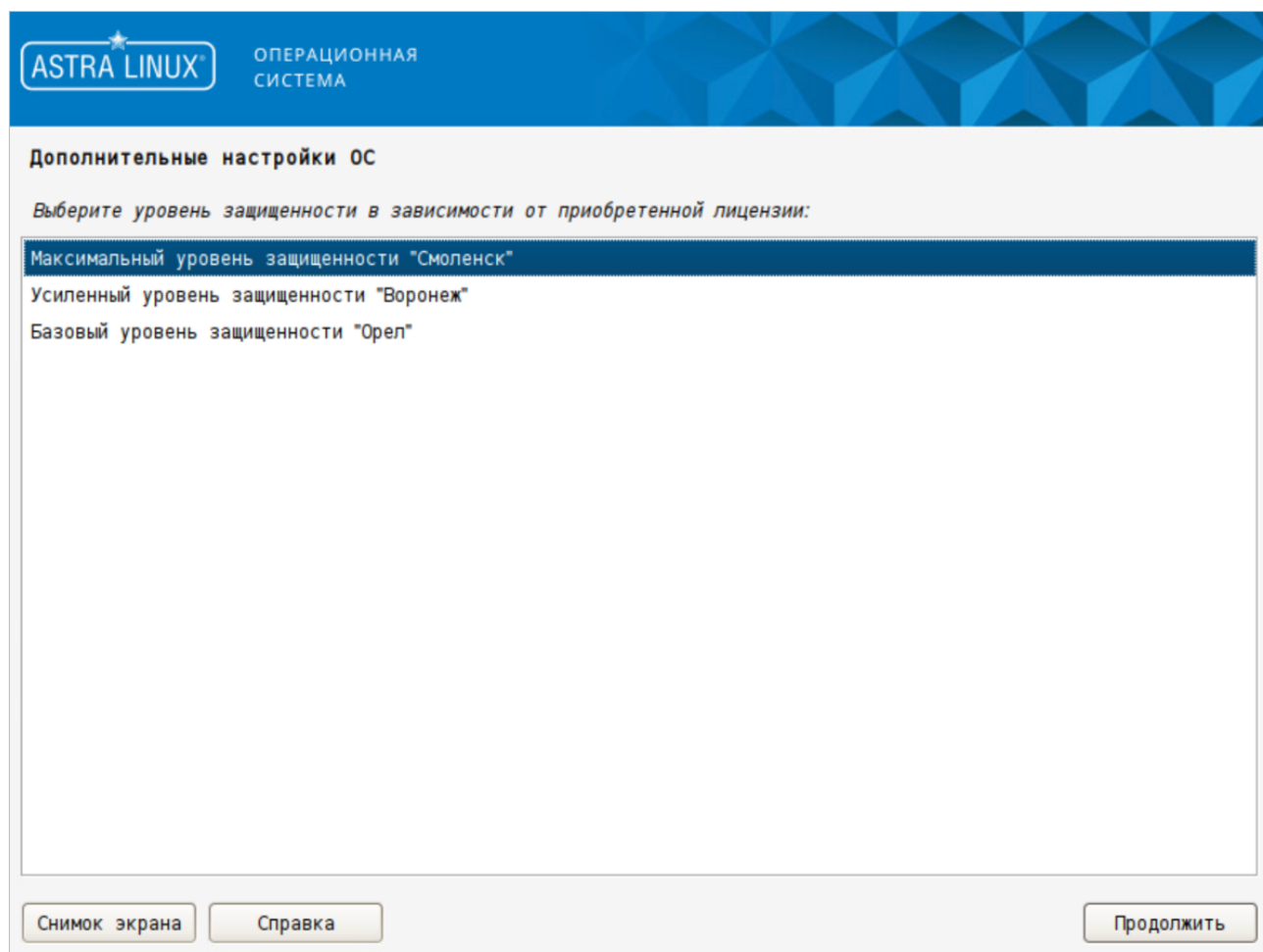


Рисунок 40. Выбор уровня защищенности

22. На этапе настройки параметров безопасности ОС оставьте значения по умолчанию в зависимости от выбранного уровня защищенности, как показано на рисунках ниже, и нажмите кнопку **Продолжить**.

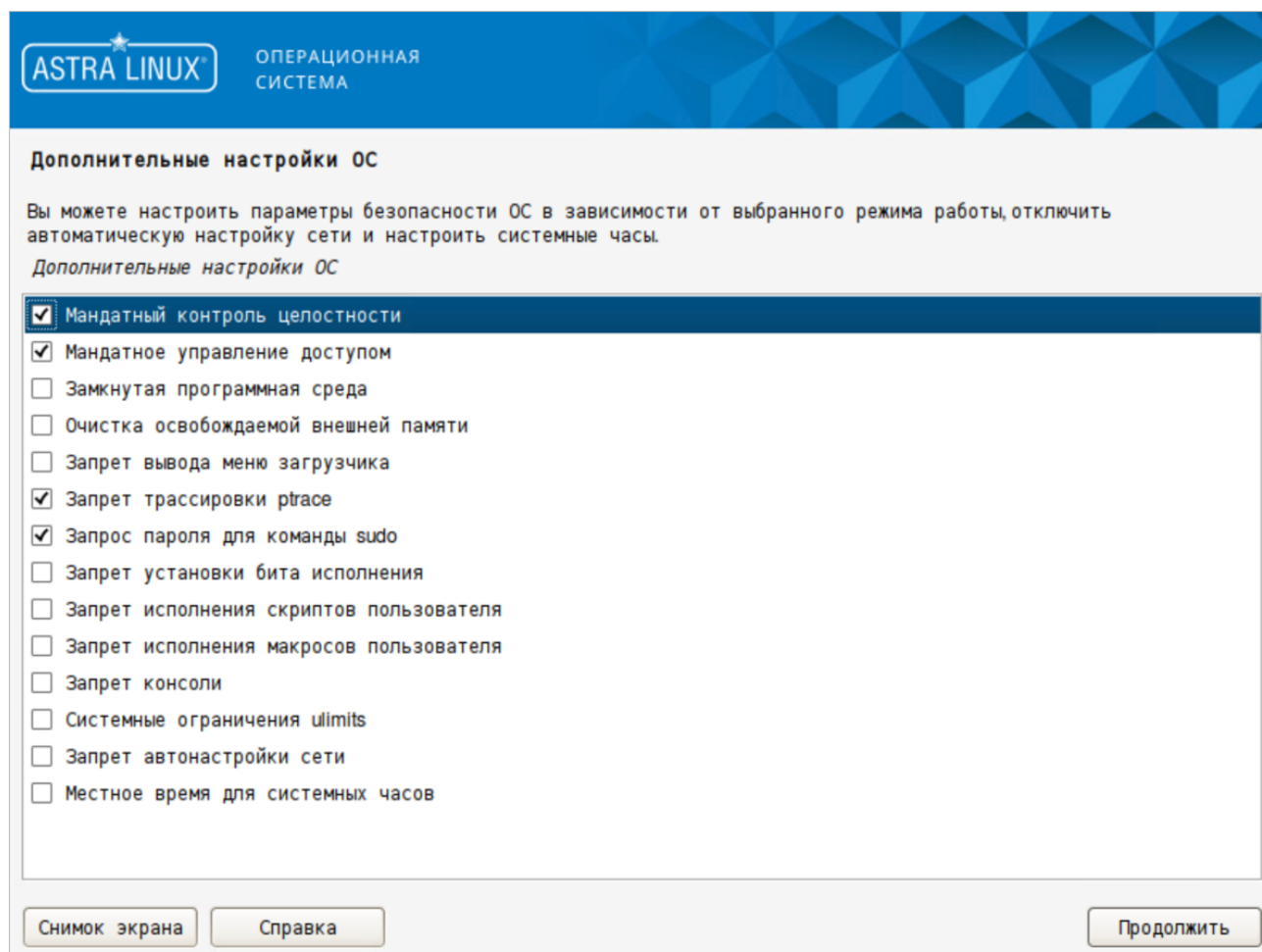


Рисунок 41. Настройка дополнительных параметров ОС при выбранном уровне защищенности «Смоленск»

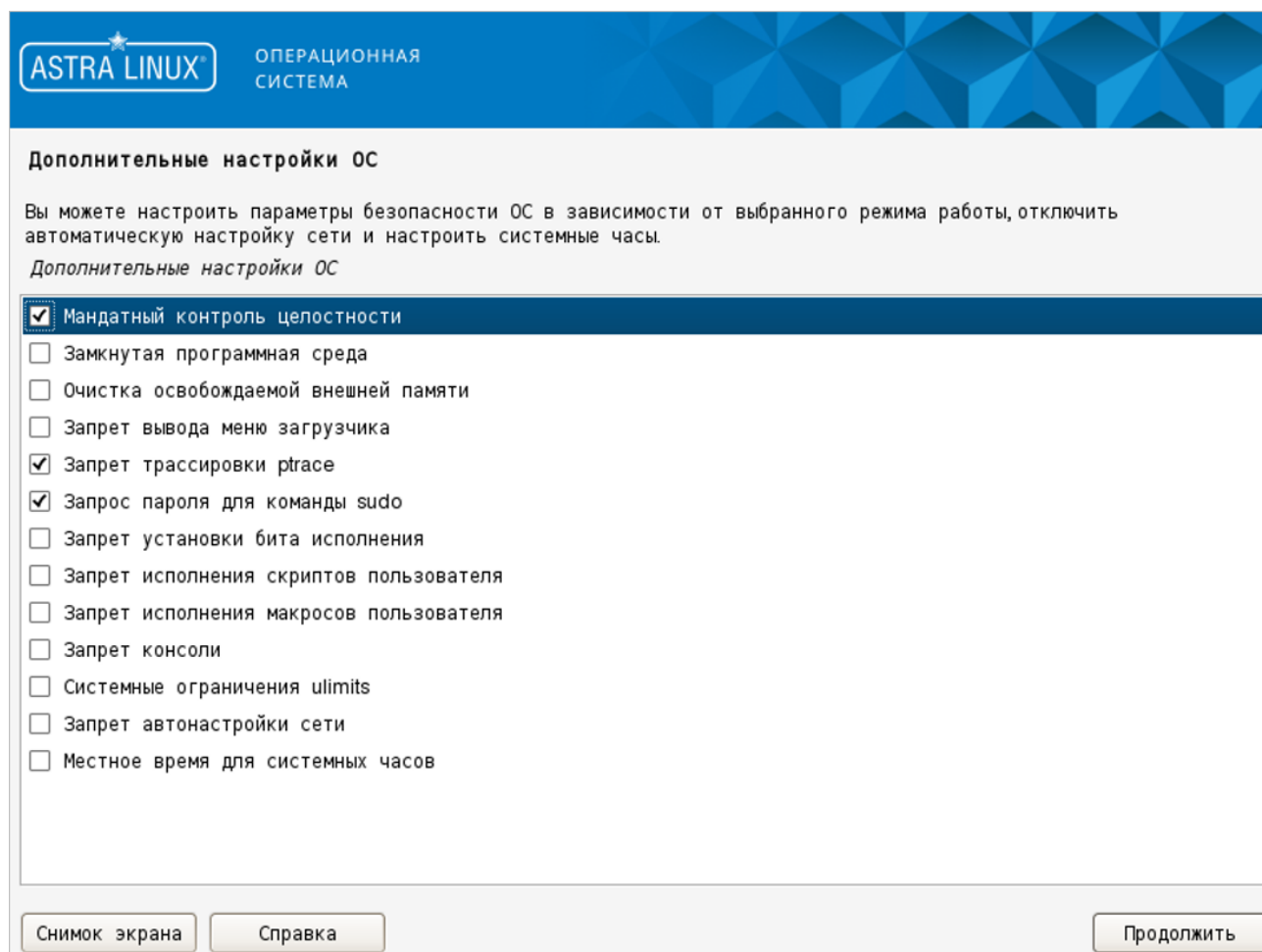


Рисунок 42. Настройка дополнительных параметров ОС при выбранном уровне защищенности «Воронеж»

23. Подтвердите установку системного загрузчика GRUB на жесткий диск, выбрав **Да** и нажав **Продолжить**.

24. Укажите пароль для системного загрузчика GRUB и нажмите **Продолжить**.

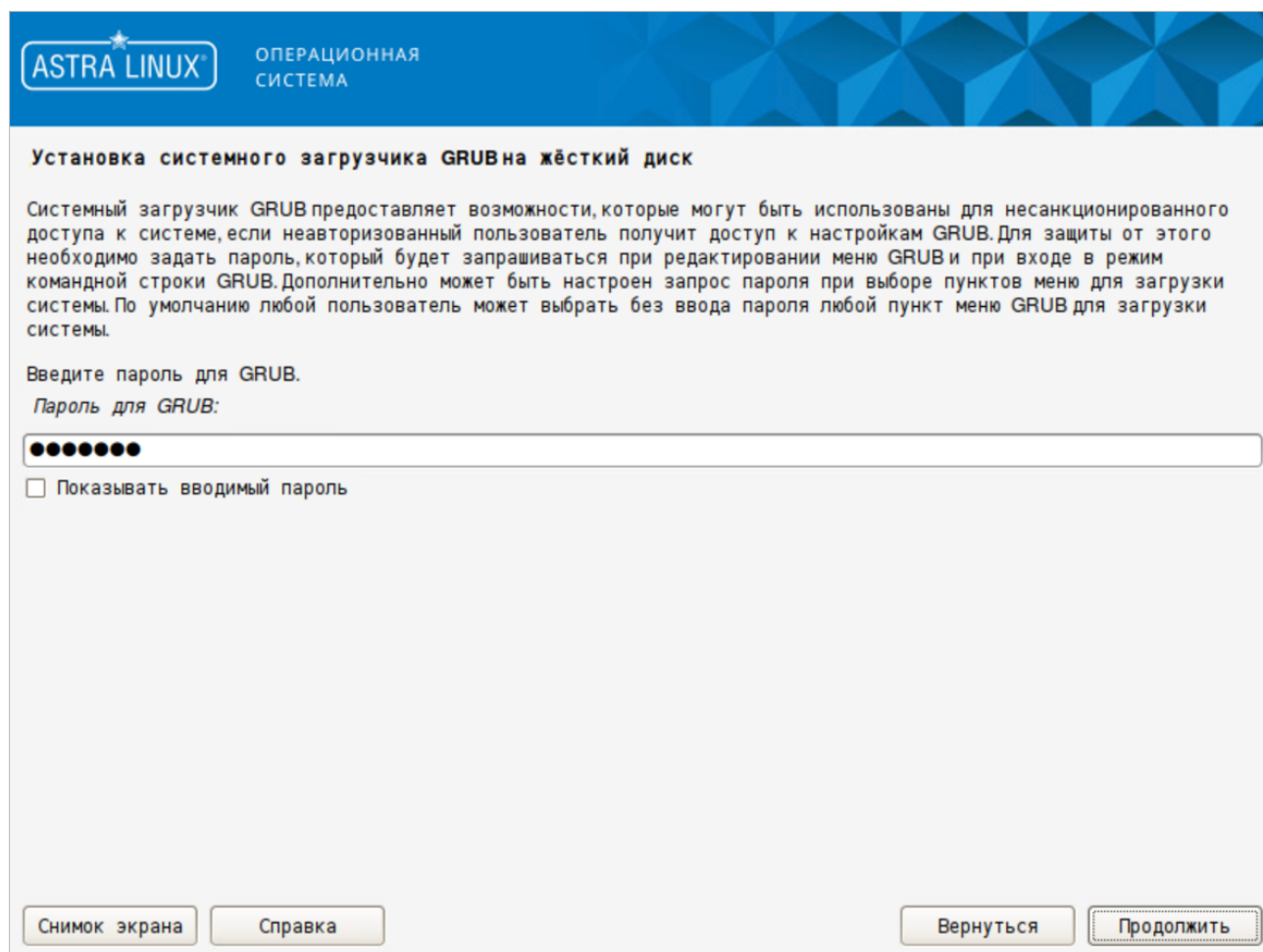


Рисунок 43. Установка системного загрузчика GRUB

25. Повторно введите пароль и нажмите **Продолжить**.

26. На этапе завершения установки отключите внешний носитель от компьютера и после этого нажмите **Продолжить**.

Система перезапустится.

Внимание! На этом этапе не отключайте питание и принудительно не перезагружайте компьютер, поскольку это приведет к неработоспособности системы.

Установка Astra Linux завершена.

5.1.5. Обновление Astra Linux

Вы можете обновить операционную систему Astra Linux SE 1.7.2 до версии 1.7.6 UU2 без потери накопленных данных PT ISIM. Ядро Linux будет обновлено до версии 5.15.0-111.

Для обновления требуется, чтобы на сервере был сохранен образ `repository-update.iso` для обновления Astra Linux до версии 1.7.6. Обновление операционной системы необходимо выполнять до обновления PT ISIM.

Внимание! Если перед установкой PT ISIM корневой раздел диска был создан с помощью Logical Volume Management, то после обновления PT ISIM и операционной системы может потребоваться активация новой лицензии.

► Чтобы обновить Astra Linux:

1. Создайте скрипт обновления:

```
touch upgrade_astra_linux.sh
```

2. Откройте созданный файл для редактирования:

```
nano upgrade_astra_linux.sh
```

3. Добавьте в файл следующее содержимое:

```
#!/bin/bash \
set -ex \
ISO_NAME=${1:-/root/repository-update.iso} \
MOUNT_POINT=${2:-/media/cdrom/} \
mkdir -p "$MOUNT_POINT" \
mount "$ISO_NAME" "$MOUNT_POINT" \
sed -i 's/#$nrconf{restart} = '"'"'i'"'"';/$nrconf{restart} = '"'"'l'"'"';/g' /etc/needrestart/needrestart.conf || true \
apt install $MOUNT_POINT/pool/non-free/a/astra-update/astra-update_*.deb \
umount "$MOUNT_POINT" \
apt-get update \
apt-mark hold libpq-dev || true \
systemctl stop postgresql || true \
systemctl stop postgresql@12-main.service || true \
systemctl stop postgresql || true \
touch /etc/apt/sources.list \
astra-update -A -T $ISO_NAME \
apt-mark unhold libpq-dev || true \
```

4. Сохраните изменения с помощью комбинации клавиш Ctrl+O и закройте файл.

5. Предоставьте созданному скрипту права на исполнение:

```
chmod +x upgrade_astra_linux.sh
```

6. Запустите скрипт обновления:

```
./upgrade_astra_linux.sh
```

7. Перезагрузите систему:

```
sudo reboot
```

5.2. Установочный комплект

Установочные комплекты компонентов PT ISIM могут быть следующих видов:

- Архивный файл с дистрибутивом компонента. Требуется предварительная [установка ОС \(см. раздел 5.1\)](#).
- ISO-образ с дистрибутивом ОС (64-разрядной серверной версии Debian 12) и дистрибутивом компонента. Установка компонента выполняется вместе с установкой ОС.

Установка из ISO-образа предусмотрена только для следующих компонентов:

PT ISIM View Sensor, PT ISIM Collector и PT ISIM Overview Center.

Перечисленные варианты установочных комплектов подходят для установки как на физическом сервере, так и в виртуальной среде.

5.3. Установка PT ISIM View Sensor

PT ISIM View Sensor может быть установлен как на физическом сервере, так и в виртуальной среде. PT ISIM View Sensor также может быть установлен на удаленном сервере путем подключения к нему по SSH.

В этом разделе

[Подготовка к установке PT ISIM View Sensor \(см. раздел 5.3.1\)](#)

[Установка PT ISIM View Sensor на физическом сервере \(см. раздел 5.3.2\)](#)

[Установка PT ISIM View Sensor на удаленном сервере \(см. раздел 5.3.3\)](#)

[Установка PT ISIM View Sensor в виртуальной среде \(см. раздел 5.3.4\)](#)

[Первоначальная настройка PT ISIM View Sensor \(см. раздел 5.3.5\)](#)

См. также

[Порядок установки PT ISIM View Sensor, PT ISIM Endpoint и PT MC на один сервер \(см. раздел 5.8\)](#)

5.3.1. Подготовка к установке PT ISIM View Sensor

Для установки PT ISIM View Sensor (proView Sensor, netView Sensor или microView Sensor) вам потребуется [установочный комплект \(см. раздел 5.2\)](#), аппаратное обеспечение без установленной операционной системы или виртуальная машина и гипервизор.

Перед установкой PT ISIM View Sensor необходимо:

1. При установке на физический сервер проверить, что сервер соответствует [аппаратным требованиям \(см. раздел 3.1\)](#). При установке в виртуальной среде проверить, что соблюдены [требования для импорта ISO-образа \(см. раздел 3.3\)](#).
2. Перенести на сервер с помощью внешнего носителя установочный комплект.
3. Если установочный комплект не содержит образа дистрибутива ОС, перенести на сервер образ дистрибутива ОС и [установить ОС \(см. раздел 5.1\)](#). Контрольная сумма образа дистрибутива ОС должна соответствовать указанной [в программных требованиях \(см. раздел 3.2\)](#).

Примечание. Образ дистрибутива Debian вы можете скачать по ссылкам, указанным [в программных требованиях \(см. раздел 3.2\)](#).

4. Авторизоваться в операционной системе, используя учетную запись, созданную во время установки ОС, и повысить ее привилегии до root с помощью команды `sudo su -`.
5. При установке антивируса Kaspersky Endpoint Security 12 на этот же сервер добавить в антивирус исключение на каталог `/opt/ptisim/lib/rules/`, выполнив команду `kesl-control --set-settings 1 --add-exclusion /opt/ptisim/lib/rules/**/*`, иначе процесс установки может быть [прерван \(см. раздел 9.12\)](#).

5.3.2. Установка PT ISIM View Sensor на физическом сервере

PT ISIM View Sensor может быть установлен в следующих редакциях: PT ISIM proView Sensor, PT ISIM netView Sensor и PT ISIM microView Sensor.

В этом разделе описана установка PT ISIM View Sensor из установочного комплекта, в который входят пакеты и установочный скрипт. Помимо установки компонентов продукта и необходимых зависимостей, скрипт также изменит на сервере локаль `en_US.UTF-8` и настроит использование часового пояса UTC.

Внимание! Крайне не рекомендуется менять часовой пояс после установки, так как это может привести к некорректной работе сенсора.

Внимание! При установке PT MC и PT ISIM View Sensor на одном сервере необходимо соблюсти следующую последовательность действий: установить PT MC, изменив в процессе установки порт PostgreSQL с 5432 на 6432 (или другой свободный порт); установить PT ISIM View Sensor и выполнить команду `/opt/ptisim/bin/local_ptmc_rules.sh 6432`, указав тот же порт PostgreSQL, что был указан на этапе установки PT MC.

Примечание. Для установки PT ISIM View Sensor необходимо повысить привилегии учетной записи до root с помощью команды `sudo su -`.

► Чтобы установить PT ISIM View Sensor:

1. Распакуйте установочный комплект и перейдите в распакованный каталог:

```
tar xzvf ptisim-package-<Версия продукта>.tgz  
cd ptisim-package-<Версия продукта>
```

2. Запустите установочный скрипт:

```
sudo ./ptisim-install
```

Примечание. Перед началом установки скрипт проверит объем свободного дискового пространства на сервере. Если он меньше указанного значения (20% по умолчанию), установка не будет выполнена.

Если в виртуальном интерфейсе bond не настроены сетевые интерфейсы, отобразится сообщение `You have to configure bond interface`, после чего потребуется [настроить сетевые интерфейсы \(см. раздел 5.3.5.1\)](#).

По умолчанию для сохранения исходной копии трафика будет создан каталог. Если требуется, вы можете [изменить этот каталог \(см. раздел 7.1.4\)](#).

PT ISIM View Sensor установлен. Для начала работы в продукте необходимо [активировать лицензию \(см. раздел 5.3.5.2\)](#). После этого вы можете [проверить работоспособность продукта \(см. раздел 5.3.5.3\)](#).

См. также

[Порядок установки PT ISIM View Sensor, PT ISIM Endpoint и PT MC на один сервер \(см. раздел 5.8\)](#)

5.3.3. Установка PT ISIM View Sensor на удаленном сервере

Вы можете установить PT ISIM View Sensor на удаленном сервере, подключившись к нему по SSH. В этом разделе приведена инструкция по установке PT ISIM View Sensor с помощью утилиты `screen`.

Примечание. Вы можете использовать терминальный мультиплексор, чтобы установочный скрипт запускался в своем терминале на удаленном сервере, независимо от SSH-сессии. Иначе, если во время установки SSH-сессия будет прервана, установка может завершиться некорректно.

Примечание. Для установки PT ISIM View Sensor необходимо повысить привилегии учетной записи до `root` с помощью команды `sudo su -`.

► Чтобы установить PT ISIM View Sensor на удаленном сервере:

1. Подключитесь к серверу, на котором планируете установить продукт:
`ssh <Имя пользователя>@<IP-адрес или доменное имя сервера>`
2. Распакуйте установочный комплект и перейдите в распакованный каталог:
`tar xzvf ptisim-package-<Версия продукта>.tgz`
`cd ptisim-package-<Версия продукта>`
3. Установите утилиту screen:
`sudo dpkg -i ptisim/screen*`
4. Настройте использование неинтерактивного способа установки:
`export DEBIAN_FRONTEND=noninteractive`

Примечание. При неинтерактивном способе установки процесс установки не будет ожидать пользовательского ввода. Настройка сетевых интерфейсов будет пропущена, и ее потребуется выполнить отдельно после завершения установки.

5. Запустите установочный скрипт в процессе screen:
`screen -d -m -S ptisim-install ./ptisim-install`

Следить за ходом установки вы можете с помощью файла журнала ptisim-install:
`tail -f /var/log/ptisim-install.log`

После завершения установки потребуется выполнить [настройку сетевых интерфейсов](#) (см. раздел 5.3.5.1).

5.3.4. Установка PT ISIM View Sensor в виртуальной среде

Для установки PT ISIM View Sensor в виртуальной среде потребуется ISO-образ виртуальной машины и [гипервизор для импорта образа](#) (см. раздел 3.3).

После импорта ISO-образа и [настройки сетевых интерфейсов](#) (см. раздел 5.3.5.1) при первом запуске виртуальной машины необходимо выполнить авторизацию на сервере PT ISIM View Sensor с помощью SSH. Для авторизации нужно использовать логин `root` (в Debian) или `administrator` (в Astra Linux) и пароль — `P@ssw0rd`. После авторизации нужно повысить привилегии учетной записи до `root`, выполнив команду `sudo su -`.

Внимание! После первого входа рекомендуется сменить пароль пользователя с помощью команды `passwd`.

Если к `root`-пользователю виртуальной машины необходим удаленный доступ по SSH, откройте на редактирование файл `/etc/ssh/sshd_config`, для параметра **PermitRootLogin** укажите значение `Yes`, сохраните изменения и выполните команду `systemctl restart sshd.service`.

Примечание. Если PT ISIM View Sensor установлен на виртуальной машине под управлением Windows, то дата и время в интерфейсе PT ISIM View Sensor и в операционной системе могут отличаться.

В этом разделе

[Установка PT ISIM View Sensor на Oracle VM VirtualBox \(см. раздел 5.3.4.1\)](#)

[Установка PT ISIM View Sensor на VMware vSphere \(см. раздел 5.3.4.2\)](#)

[Установка PT ISIM View Sensor на VMware Workstation \(см. раздел 5.3.4.3\)](#)

5.3.4.1. Установка PT ISIM View Sensor на Oracle VM VirtualBox

► Чтобы установить PT ISIM View Sensor на Oracle VM VirtualBox:

1. Запустите Oracle VM VirtualBox.
2. В меню **Машина** выберите пункт **Создать**.
Откроется окно создания виртуальной машины.
3. Введите имя виртуальной машины.
4. В поле **Образ ISO** выберите файл с образом ISO.
В поле **Тип** автоматически подставится значение **Linux**, в поле **Версия** — **Debian (64-bit)**. Если этого не произошло, выберите эти значения вручную.
5. Установите флажок **Пропустить автоматическую установку** и нажмите кнопку **Далее**.
6. Укажите необходимый объем памяти и количество задействованных ядер центрального процессора с учетом [аппаратных требований \(см. раздел 3.1\)](#) и нажмите **Далее**.
7. Выберите пункт **Создать новый виртуальный жесткий диск**, укажите размер диска в соответствии с [аппаратными требованиями \(см. раздел 3.1\)](#) и нажмите **Далее**.
Откроется окно с описанием выбранной конфигурации виртуальной машины.
Примечание. Если требуется, вы можете вернуться на предыдущие шаги и внести исправления.
8. Нажмите кнопку **Готово** для создания виртуальной машины.
9. В контекстном меню созданной виртуальной машины выберите пункт **Настроить**.
10. В открывшемся окне в разделе **Сеть** выберите вкладку **Адаптер 1**.
11. Установите флажок **Включить сетевой адаптер**.
12. В раскрывающемся списке **Тип подключения** выберите значение **Сетевой мост**.
Если требуется, вы можете выбрать другой тип подключения для доступа к интерфейсу PT ISIM View Sensor. В этом случае следующие шаги могут отличаться от представленных.
13. В раскрывающемся списке **Имя** выберите название сетевого адаптера, соответствующего сервисному интерфейсу.

14. Выберите вкладку **Адаптер 2**.
15. Установите флажок **Включить сетевой адаптер**.
16. В раскрывающемся списке **Тип подключения** выберите **Сетевой мост**.
17. В раскрывающемся списке **Имя** выберите название сетевого адаптера, который принимает зеркалируемый трафик.
18. В раскрывающемся блоке **Дополнительно** в раскрывающемся списке **Неразборчивый режим** выберите **Разрешить все**.
19. Если вы планируете использовать для зеркалирования технологического трафика дополнительные интерфейсы PT ISIM View Sensor, выполните такую же настройку на вкладках **Адаптер 3** и **Адаптер 4**.
20. Нажмите кнопку **ОК**.

Откроется окно со списком виртуальных машин.

21. Запустите созданную виртуальную машину двойным щелчком мыши.
22. На открывшейся странице выберите пункт **Auto Install ISIM on one disk**.
23. Нажмите клавишу **Enter** или подождите 10 секунд.

Запустится автоматическая установка PT ISIM View Sensor.

При первом запуске виртуальной машины вы можете [настроить сетевые интерфейсы](#) (см. раздел 5.3.5.1).

5.3.4.2. Установка PT ISIM View Sensor на VMware vSphere

► Чтобы установить PT ISIM View Sensor на VMware vSphere:

1. Запустите приложение клиента VMware vSphere.
2. Подключитесь к удаленному серверу VMware vSphere.
3. В приложении VMware vSphere нажмите **Файл** → **Новая виртуальная машина** и выберите ранее подключенный удаленный сервер.
4. В открывшемся окне выберите тип конфигурации **Обычный** и нажмите кнопку **Далее**.
5. Укажите расположение виртуальной машины и нажмите кнопку **Далее**.
6. Выберите хранилище виртуальной машины и нажмите кнопку **Далее**.
7. В блоке параметров **Гостевая операционная система** выберите вариант **Linux**.
8. В раскрывающемся списке **Версия** выберите версию, для которой предназначен ISO-образ, — **Debian GNU/Linux 10 (64-bit)** — и нажмите кнопку **Далее**.
9. В поле **Имя виртуальной машины** введите имя виртуальной машины и нажмите кнопку **Далее**.

10. Укажите размер диска в соответствии с аппаратными требованиями (см. раздел 3.1) и нажмите **Далее**.
11. Нажмите кнопку **Настройка оборудования**.
12. В открывшемся окне **Оборудование** в списке устройств выберите **Память** и **Процессор** и укажите необходимый объем памяти и количество задействованных ядер центрального процессора в соответствии с аппаратными требованиями (см. раздел 3.1).
13. В списке устройств выберите **Новый CD/DVD (IDE)**, в блоке параметров **Подключение** выберите вариант **Файл образа ISO** и с помощью кнопки **Обзор** выберите файл ISO-образа с редакцией PT ISIM View Sensor.
14. В списке устройств выберите **Сетевой адаптер** и в поле **Подключение к сети** выберите сервисный интерфейс для доступа к веб-интерфейсу PT ISIM View Sensor.
15. Нажмите кнопку **Добавить**, в открывшемся окне выберите вариант **Сетевой адаптер** и нажмите кнопку **Финиш**.

В списке устройств появится **Сетевой адаптер 2**.

16. В списке устройств выберите **Сетевой адаптер 2**, в поле **Подключение к сети** укажите интерфейс, который принимает зеркалируемый трафик, и нажмите кнопку **Заккрыть**.
17. В окне **Мастер создания виртуальной машины** нажмите кнопку **Финиш**.
Откроется окно со списком виртуальных машин.
18. В контекстном меню созданной виртуальной машины выберите пункт **Питание** и нажмите кнопку **Включить**.
19. На открывшейся странице выберите пункт **Auto Install ISIM on one disk**.
20. Нажмите клавишу **Enter** или подождите 10 секунд.

Запустится автоматическая установка PT ISIM View Sensor.

При первом запуске виртуальной машины вы можете [настроить сетевые интерфейсы](#) (см. раздел 5.3.5.1).

5.3.4.3. Установка PT ISIM View Sensor на VMware Workstation

► Чтобы установить PT ISIM View Sensor на VMware Workstation:

1. Запустите VMware Workstation.
2. Нажмите **Файл** → **Новая виртуальная машина**.
3. В открывшемся окне выберите тип конфигурации **Обычный** и нажмите кнопку **Далее**.

4. В блоке параметров выберите вариант **Файл образа установки (iso)**, с помощью кнопки **Обзор** выберите файл ISO-образа с PT ISIM View Sensor и нажмите кнопку **Далее**.
5. В блоке параметров **Гостевая операционная система** выберите вариант **Linux**.
6. В раскрывающемся списке **Версия** выберите версию, для которой предназначен ISO-образ, — Debian GNU/Linux 10 (64-bit) — и нажмите кнопку **Далее**.
7. Укажите имя и расположение виртуальной машины и нажмите кнопку **Далее**.
8. Укажите размер диска в соответствии с [аппаратными требованиями](#) (см. раздел 3.1) и нажмите **Далее**.
9. Нажмите кнопку **Настройка оборудования**.
10. В открывшемся окне **Оборудование** в списке устройств выберите **Память** и **Процессор** и укажите необходимый объем памяти и количество задействованных ядер центрального процессора в соответствии с [аппаратными требованиями](#) (см. раздел 3.1).
11. В списке устройств выберите **Сетевой адаптер** и в поле **Подключение к сети** выберите сервисный интерфейс для доступа к веб-интерфейсу PT ISIM View Sensor.
12. Нажмите кнопку **Добавить**, в открывшемся окне выберите вариант **Сетевой адаптер** и нажмите кнопку **Финиш**.

В списке устройств появится **Сетевой адаптер 2**.

13. В списке устройств выберите **Сетевой адаптер 2**, в поле **Подключение к сети** укажите интерфейс, который принимает зеркалируемый трафик, и нажмите кнопку **Заккрыть**.

14. В окне **Мастер создания виртуальной машины** нажмите кнопку **Финиш**.

Откроется окно со списком виртуальных машин.

15. В контекстном меню созданной виртуальной машины выберите пункт **Питание** и нажмите кнопку **Включить**.

16. На открывшейся странице выберите пункт **Auto Install ISIM on one disk**.

17. Нажмите клавишу **Enter** или подождите 10 секунд.

Запустится автоматическая установка PT ISIM View Sensor.

При первом запуске виртуальной машины вы можете [настроить сетевые интерфейсы](#) (см. раздел 5.3.5.1).

5.3.5. Первоначальная настройка PT ISIM View Sensor

После установки PT ISIM View Sensor необходимо выполнить [настройку сетевых интерфейсов](#) (см. раздел 5.3.5.1), [активировать лицензию](#) (см. раздел 5.3.5.2) и [проверить работоспособность](#) (см. раздел 5.3.5.3) продукта.

Кроме того, вы можете просмотреть журнал установочного скрипта и версию установленного продукта.

Просмотр журнала установочного скрипта

- ▶ Чтобы просмотреть журнал установочного скрипта,

выполните команду:

```
less /var/log/ptisim-install.log
```

Просмотр версии установленного продукта

Версия установленного продукта доступна в веб-интерфейсе по нажатию , а также в файле `/opt/ptisim/Manifest.pt` в параметрах `meta` → `release` (номер версии) и `meta` → `build` (номер сборки).

В этом разделе

[Настройка сетевых интерфейсов PT ISIM View Sensor \(см. раздел 5.3.5.1\)](#)

[Активация лицензии PT ISIM View Sensor \(см. раздел 5.3.5.2\)](#)

[Проверка работоспособности продукта \(см. раздел 5.3.5.3\)](#)

5.3.5.1. Настройка сетевых интерфейсов PT ISIM View Sensor

Для корректной работы PT ISIM View Sensor требуется настроить минимум два [сетевых интерфейса \(см. раздел 3.4\)](#): сервисный интерфейс (или интерфейс управления) и технологический интерфейс.

Технологические интерфейсы включаются в виртуальный интерфейс `bond`.

Автоматическая настройка сетевых интерфейсов выполняется в процессе установки продукта, если ни один интерфейс в `bond0` не настроен. Настройка сетевых интерфейсов PT ISIM View Sensor может быть запущена также вручную с помощью команды `/opt/ptisim/bin/configure_interfaces`. Если вы хотите использовать более одного технологического интерфейса, добавьте их на физический сервер или, если используете образ виртуальной машины, с помощью гипервизора, а затем добавьте в `bond` по инструкции ниже.

- ▶ Чтобы настроить сетевые интерфейсы:

1. Выполните команду:

```
/opt/ptisim/bin/configure_interfaces
```

2. Нажмите клавишу 3 (`add to bond`).

3. В открывшемся списке интерфейсов выберите технологический интерфейс, который требуется добавить в bond.

Отобразится стартовое окно настройки интерфейсов.

4. Нажмите клавишу 2 (`configure interface`).
5. В открывшемся списке интерфейсов выберите сервисный интерфейс.
6. Введите статический IP-адрес сервисного интерфейса.
7. По окончании настройки сетевых интерфейсов нажмите клавишу 7 (`exit`).
8. Нажмите клавишу 1 (`save and exit`) для сохранения параметров.

См. также

[Просмотр состояния сетевых интерфейсов \(см. раздел 7.1.14.1\)](#)

[Требования к сети \(см. раздел 3.4\)](#)

[Ошибки при настройке сетевых интерфейсов \(см. раздел 9.5\)](#)

5.3.5.2. Активация лицензии PT ISIM View Sensor

В этом разделе приведены инструкции по активации лицензии PT ISIM View Sensor.

Номер лицензионного ключа и срок действия лицензии вы можете проверить по значку  в веб-интерфейсе PT ISIM View Sensor.

Внимание! Крайне не рекомендуется переводить системное время назад, так как в этом случае механизм лицензирования может заблокировать основные функции продукта.

Активация платной лицензии

Для активации платной лицензии требуется V2C-файл, предоставляемый поставщиком продукта на основе переданного вами C2V-файла. C2V-файл представляет собой отпечаток характеристик сервера, на котором установлен продукт. Вы можете скачать C2V-файл в веб-интерфейсе PT ISIM View Sensor.

► Чтобы скачать C2V-файл:

1. В главном меню выберите  → **Лицензия**.
2. Нажмите **Скачайте отпечаток системы**.

► Чтобы активировать лицензию:

1. В главном меню выберите  → **Лицензия**.
2. Нажмите **Загрузите лицензию** и выберите V2C-файл.

Активация пробной лицензии

Для активации пробной лицензии потребуется V2C-файл, выпускаемый поставщиком PT ISIM View Sensor без привязки к серверу.

Примечание. Пробная лицензия может быть активирована только один раз. По истечении срока ее действия рекомендуется приобрести платную лицензию.

► Чтобы активировать лицензию:

1. В главном меню выберите  → **Лицензия**.
2. Нажмите **Загрузите лицензию** и выберите V2C-файл.

См. также

[Лицензирование \(см. раздел 4\)](#)

5.3.5.3. Проверка работоспособности продукта

После установки и активации лицензии вы можете проверить работоспособность PT ISIM View Sensor, чтобы убедиться, что продукт обнаруживает события, инциденты и сетевые узлы.

Проверка выполняется с помощью отправки ICMP-пакета (эхо-запроса) размером 100 байт на мультикаст-адрес 224.0.0.42 с любого сетевого узла, трафик которого должен перехватываться.

► Чтобы проверить работоспособность PT ISIM View Sensor,

выполните команду:

- Для Windows:

```
ping -l 100 224.0.0.42
```

- Для ОС семейства Unix:

```
ping -c4 -s100 224.0.0.42
```

В результате проверки в веб-интерфейсе PT ISIM View Sensor должны появиться следующие данные:

- на странице **Инциденты** — инциденты «Проверка работоспособности PT ISIM», «Неавторизованный узел»;
- на странице **События** — события по протоколу ICMP «Пакет для проверки работоспособности PT ISIM»;
- на странице **Сеть** → **Узлы** — узел источника запроса с IP-адресом сервера, с которого был выполнен запрос. Так как 224.0.0.42 является мультикаст-адресом, узел-адресат не отобразится.

Дата и время	Протокол	Источник	Цель	Событие
25.04 15:45:13	ICMP	192.0.2.49	224.0.0.42	Пакет для проверки работоспособности PT ISIM ...
25.04 15:45:13	ICMP	192.0.2.49	224.0.0.42	Пакет для проверки работоспособности PT ISIM ...
25.04 15:45:13	ICMP	192.0.2.49	224.0.0.42	Пакет для проверки работоспособности PT ISIM ...
25.04 15:45:13	ICMP	192.0.2.49	224.0.0.42	Пакет для проверки работоспособности PT ISIM ...

Рисунок 44. Тестовые события «Пакет для проверки работоспособности PT ISIM»

5.4. Установка PT ISIM Endpoint

В этом разделе приводятся инструкции по установке PT ISIM Endpoint.

В этом разделе

[Подготовка к установке PT ISIM Endpoint \(см. раздел 5.4.1\)](#)

[Процедура установки PT ISIM Endpoint \(см. раздел 5.4.2\)](#)

[Первоначальная настройка PT ISIM Endpoint \(см. раздел 5.4.3\)](#)

[Активация лицензии PT ISIM Endpoint \(см. раздел 5.4.4\)](#)

См. также

[Настройка приема данных от PT ISIM Endpoint \(см. раздел 7.1.13\)](#)

[Подключение к PT MC \(см. раздел 7.1.2\)](#)

[Порядок установки PT ISIM View Sensor, PT ISIM Endpoint и PT MC на один сервер \(см. раздел 5.8\)](#)

5.4.1. Подготовка к установке PT ISIM Endpoint

Перед установкой PT ISIM Endpoint необходимо:

- Проверить сервер и конечные узлы на соответствие [аппаратным и программным требованиям \(см. раздел 3\)](#).
- Установить PT MC. Инструкция по развертыванию PT MC и добавлению учетных записей пользователей описана [в справке к продукту](#). Поддерживаемые версии PT MC указаны [в программных требованиях \(см. раздел 3.2\)](#).
- Установить PT ISIM View Sensor, [настроить подключение \(см. раздел 7.1.2\)](#) к PT MC и [настроить сервис \(см. раздел 7.1.13\)](#) ptisim-rester для приема данных от PT ISIM Endpoint.

5.4.2. Процедура установки PT ISIM Endpoint

Установка PT ISIM Endpoint возможна в следующих конфигурациях:

1. PT ISIM Endpoint, PT ISIM View Sensor и PT MC установлены на одном сервере.
2. PT ISIM Endpoint и PT ISIM View Sensor установлены на разных серверах. PT MC установлен на одном сервере с PT ISIM Endpoint.

Установка PT ISIM Endpoint на отдельном сервере может применяться в технологических сегментах, в которых требуется физическая изоляция от смежных сетей и передача данных возможна только через однонаправленные диоды данных.

3. PT ISIM Endpoint, PT ISIM View Sensor и PT MC установлены на разных серверах.

Поддерживаемые операционные системы в зависимости от конфигурации приведены [в программных требованиях \(см. раздел 3.2\)](#).

Далее приведена инструкция по установке PT ISIM Endpoint с учетом особенностей каждой конфигурации.

Внимание! При установке PT ISIM Endpoint на одном сервере с PT MC и PT ISIM View Sensor необходимо соблюсти следующую последовательность действий: установить PT MC, изменив в процессе установки порт PostgreSQL с 5432 на 6432 (или другой свободный порт); установить PT ISIM View Sensor и выполнить команду `/opt/ptisim/bin/local_ptmc_rules.sh 6432`, указав тот же порт PostgreSQL, что был указан на этапе установки PT MC; установить PT ISIM Endpoint.

► Чтобы установить PT ISIM Endpoint:

1. Распакуйте установочный комплект в отдельный каталог и перейдите в него:


```
tar xf isim-endpoint.<Версия продукта>.tar.gz
cd isim-endpoint.<Версия продукта>
```
2. Откройте файл `install.cfg`:


```
sudo nano install.cfg
```
3. Задайте в файле параметры установки (см. таблицу 26).

Пример файла `install.cfg` для конфигурации, когда PT ISIM Endpoint, PT ISIM View Sensor и PT MC устанавливаются на разных серверах:

```
pt_mc_address=198.51.100.12
pt_mc_port=3334
isim_address=198.51.100.46
isim_port=6192
isim_transport=tcp
ui_server_host=198.51.100.25
ui_port=4443
db_root_password=PtEdrDBRootPassword
db_global_password=PtEdrDBGlobalPassword
db_instance_password=PtEdrDBInstancePassword
mc_version=101.20.19012
```

Пример файла `install.cfg` для конфигурации, когда PT ISIM Endpoint, PT ISIM View Sensor и PT MC устанавливаются на одном сервере:

```
pt_mc_address=<IP-адрес сервера, на котором выполняется установка>
pt_mc_port=3334
isim_address=127.0.0.1
isim_port=6192
isim_transport=tcp
ui_server_host=<IP-адрес сервера, на котором выполняется установка>
ui_port=4443
db_root_password=PtEdrDBRootPassword
db_global_password=PtEdrDBGlobalPassword
db_instance_password=PtEdrDBInstancePassword
mc_version=<Версия PT MC>
```

4. Сохраните изменения (Ctrl+O) и закройте файл (Ctrl+X).
5. Для работы компонента Observability получите сертификаты и ключ сервиса PT MC collector-agent. Для этого выполните следующие действия:
 - На сервере с установленным PT MC, адрес которого указан в файле `install.cfg` в параметре `pt_mc_address`, создайте каталог:


```
mkdir -p <Путь к каталогу>
```
 - Скопируйте файлы `Portal.key`, `Portal.crt`, `rootCA.crt` в созданный каталог:


```
cp /var/lib/deployed-roles/<Название роли Management and Configuration>/managementandconfiguration/certs/{Portal.key,Portal.crt,rootCA.crt} <Путь к каталогу>
```
 - Если PT MC установлен на отдельном сервере, скопируйте созданный каталог на сервер с установочным комплектом PT ISIM Endpoint.
 - На сервере с установочным комплектом PT ISIM Endpoint в файле манифеста `endpoint_manifest_template.json` в секции `hosts.127.0.0.1` измените путь к каталогу с файлами `Portal.key`, `Portal.crt`, `rootCA.crt` на актуальный:


```
{
  "hosts": {
    "127.0.0.1": {
      "mc_otel_certs": {
        "cert": "<Путь к каталогу>/Portal.crt",
        "key": "<Путь к каталогу>/Portal.key",
        "root_ca": "<Путь к каталогу>/rootCA.crt"
      },

```
6. Запустите установочный скрипт:


```
sudo ./install.sh
```
7. Ознакомьтесь с лицензионным соглашением и примите его условия.

Начнется установка PT ISIM Endpoint.

8. На этапе подтверждения установки компонентов при ответе на вопрос **Are you sure what you want to install ['agent_server', 'dbms', 'observability', 'edr_update', 'api', 'custom_expertise'] on this server? (y/n)?** выберите вариант **y**.
9. При ответе на вопрос **Standalone installation, go to MC and approve registration of EDR. Press Y after approve for installation continue process... (y/n)?** выберите вариант **y**.

После установки PT ISIM Endpoint в PT MC появится соответствующая площадка. Вы можете изменить ее название (подробнее см. [в справке к продукту](#)). Это поможет различать площадки при наличии нескольких PT ISIM Endpoint, подключенных к одному PT MC.

После завершения установки веб-интерфейс PT ISIM Endpoint будет доступен по адресу <https://<IP-адрес PT ISIM Endpoint>:<Порт PT ISIM Endpoint>>. Вход в PT ISIM Endpoint выполняется под учетной записью пользователя PT MC. При первом запуске PT ISIM Endpoint потребуется [активировать лицензию \(см. раздел 5.4.4\)](#).

Таблица 26. Параметры установки PT ISIM Endpoint

Параметр	Описание	Значение по умолчанию
pt_mc_address	IP-адрес узла с установленным PT MC. Значение по умолчанию не используется	127.0.0.1
pt_mc_port	Порт для подключения к PT MC	3334
mc_version	Версия PT MC	Версия установленного PT MC
isim_address	IP-адрес узла, на котором установлен PT ISIM View Sensor. Если PT ISIM Endpoint устанавливается на одном узле с PT ISIM View Sensor, оставьте значение по умолчанию	127.0.0.1
isim_port	Порт для подключения к PT ISIM View Sensor	6192
isim_transport	Протокол передачи данных к PT ISIM View Sensor. При настройке (см. раздел 7.1.13) PT ISIM View Sensor в файле <code>endpoint.conf</code> в параметре, соответствующем этому протоколу, должно быть указано значение <code>true</code>	tcp
ui_server_host	IP-адрес сервера, на который устанавливается PT ISIM Endpoint. Значение по умолчанию не используется	127.0.0.1

Параметр	Описание	Значение по умолчанию
ui_port	Порт для подключения к PT ISIM Endpoint. При установке PT ISIM Endpoint на тот же сервер, что и PT ISIM View Sensor, используйте значение по умолчанию или укажите другой свободный порт	4443
db_root_password	Используется значение по умолчанию	PtEdrDBRootPassword
db_global_password	Используется значение по умолчанию	PtEdrDBGlobalPassword
db_instance_password	Используется значение по умолчанию	PtEdrDBInstancePassword

См. также

[Порядок установки PT ISIM View Sensor, PT ISIM Endpoint и PT MC на один сервер \(см. раздел 5.8\)](#)

5.4.3. Первоначальная настройка PT ISIM Endpoint

После установки PT ISIM Endpoint нужно:

- [активировать лицензию \(см. раздел 5.4.4\)](#) PT ISIM Endpoint;
- [установить агенты \(см. раздел 7.2.1.2\)](#) на конечные устройства и добавить папки с файлами агентов в исключения антивируса;
- настроить PT ISIM Endpoint:
 - [создать политики на основе шаблонов \(см. раздел 7.2.2\)](#) и, если требуется, настроить модули политик;
 - [назначить политики на группы агентов \(см. раздел 7.2.2\)](#);
 - [добавить агенты в группы агентов \(см. раздел 7.2.1.3\)](#).

Сразу после добавления агентов в группы на агентах будут установлены и запущены модули политик.

На узлах Windows и Linux необходимо настроить сбор и обнаружение событий с использованием стандартных политик по инструкциям ниже.

Вы также можете настроить:

- [работу с пакетами промышленной экспертизы \(см. раздел 7.2.3\)](#) для отслеживания событий безопасности, связанных с работой промышленного ПО на конечных узлах;
- [сканирование узлов в режиме аудита \(см. раздел 7.2.4\)](#) для получения данных о конфигурации конечных узлов;
- [антивирусную защиту узлов \(см. раздел 7.2.5\)](#).

Настройка PT ISIM Endpoint для узлов под управлением Linux

► Чтобы настроить PT ISIM Endpoint для сбора событий с узлов под управлением Linux:

1. Создайте две политики на основе шаблонов «Сбор данных с рабочих станций (Linux)» и «Обнаружение угроз (Linux)».

Примечание. Для сбора данных с серверов под управлением Linux вы также можете создать политику на основе шаблона «Сбор данных с серверов (Linux)».

2. Назначьте созданные политики на группу «Рабочие станции Linux».
3. После установки агентов на конечных узлах авторизуйте их в PT ISIM Endpoint, добавив в группу «Рабочие станции Linux».

Настройка PT ISIM Endpoint для узлов под управлением Windows

► Чтобы настроить PT ISIM Endpoint для сбора событий с узлов под управлением Windows:

1. Создайте две политики на основе шаблонов «Сбор данных с рабочих станций (Windows)» и «Обнаружение угроз (Windows)».

Примечание. Для сбора данных с серверов и контроллеров доменов под управлением Windows вы также можете создать политики на основе шаблонов «Сбор данных с серверов (Windows)» и «Сбор данных с контроллеров доменов (Windows)».

2. Назначьте созданные политики на группу «Рабочие станции Windows».
3. После установки агентов на конечных узлах авторизуйте их в PT ISIM Endpoint, добавив в группу «Рабочие станции Windows».

5.4.4. Активация лицензии PT ISIM Endpoint

Для работы PT ISIM Endpoint и его защиты от нелегального использования нужно активировать лицензию.

Управление лицензией осуществляется в PT MC. Для лицензии указываются срок ее действия, максимальное количество авторизованных агентов и возможность разработки модулей. Просмотреть параметры лицензий вы можете на странице **Лицензии**, открывающейся по нажатию  **Система** → **Лицензия**.

После истечения срока действия лицензии будут ограничены обновление системы, авторизация и перемещение агентов между группами, создание и настройка политик, а также обновление модулей на конечных устройствах

Для активации лицензии нужно:

1. Добавить лицензию в РТ МС (если она не была добавлена ранее).

Примечание. Файл с лицензией нужно запросить у вашего менеджера Positive Technologies.

2. В РТ МС привязать добавленную лицензию к приложению.

Примечание. Для управления лицензиями в РТ МС нужны соответствующие привилегии.

Добавление лицензии в РТ МС

- ▶ Чтобы добавить лицензию при наличии доступа к интернету:

1. В главном меню выберите **Лицензии**.
2. Нажмите **Обновить список лицензий**.

Для добавления лицензии вручную вам потребуется ZIP-файл с лицензией из комплекта поставки. Если ваш комплект не содержит ZIP-файла с лицензией, вы можете запросить его в службе технической поддержки.

- ▶ Чтобы добавить лицензию в РТ МС вручную, без доступа к интернету:

1. В главном меню выберите **Лицензии**.
2. Нажмите **Добавить**.
3. Выберите ZIP-файл с лицензией.

Файл может содержать как одну, так и несколько лицензий. В систему будут добавлены все корректные лицензии, которые содержатся в файле.

4. Нажмите **Добавить**.

Привязка лицензии в РТ МС

- ▶ Чтобы привязать лицензию к приложению PT ISIM Endpoint:

1. В главном меню выберите **Лицензии**.
2. Выберите лицензию и нажмите **Привязать**.
3. Выберите установленное приложение PT ISIM Endpoint, к которому нужно привязать лицензию.
4. Нажмите **Привязать**.

5.5. Установка PT ISIM Collector

Далее приведены инструкции по установке и первоначальной настройке коллекторов.

Примечание. Работа с коллекторами доступна в редакциях PT ISIM proView Sensor и PT ISIM netView Sensor.

В этом разделе

[Процедура установки PT ISIM Collector \(см. раздел 5.5.1\)](#)

[Первоначальная настройка PT ISIM Collector \(см. раздел 5.5.2\)](#)

[Активация лицензии коллектора \(см. раздел 5.5.3\)](#)

5.5.1. Процедура установки PT ISIM Collector

В этом разделе приводятся инструкции по установке коллектора на узел. В установочный комплект входят пакеты и установочный скрипт.

Примечание. Для установки коллектора на одном узле с антивирусом Kaspersky Endpoint Security 12 необходимо до начала установки коллектора добавить в антивирус исключение на каталог `/opt/ptisim/lib/rules/`, выполнив команду `kesl-control --set-settings 1 --add-exclusion /opt/ptisim/lib/rules/**/*`, иначе процесс установки может быть прерван (см. раздел 9.12).

► Чтобы установить коллектор:

1. Распакуйте установочный комплект и перейдите в распакованный каталог:

```
tar xzvf ptisim-package-collector-<Версия продукта>.tgz
cd ptisim-package-collector-<Версия продукта>
```

2. Запустите установочный скрипт:

```
sudo ./ptisim-install
```

3. Выберите язык мастера установки.

4. Ознакомьтесь с лицензионным соглашением и примите его условия.

Начнется установка коллектора.

Журнал установочного скрипта вы можете просмотреть в файле `/var/log/ptisim-install.log`.

Если в виртуальном интерфейсе bond не настроены сетевые интерфейсы, отобразится сообщение `You have to configure bond interface`, после чего потребуется настроить сетевые интерфейсы. Настройка выполняется аналогично [настройке сетевых интерфейсов \(см. раздел 5.3.5.1\)](#) сенсора.

После завершения установки коллектора необходимо выполнить [первоначальную настройку \(см. раздел 5.5.2\)](#) его работы.

5.5.2. Первоначальная настройка PT ISIM Collector

После установки коллектора для настройки его работы нужно:

- активировать лицензию (см. раздел 5.5.3) коллектора;
- если в PT ISIM View Sensor отключен прием данных от коллектора, включить его (см. раздел 7.3.1);
- добавить коллектор (см. раздел 7.3.2) в PT ISIM View Sensor;
- в PT ISIM View Sensor скачать конфигурацию (см. раздел 7.3.4) с параметрами передачи данных;
- загрузить (см. раздел 7.3.5) конфигурацию на коллектор;
- если требуется, настроить (см. раздел 7.3.6) прием данных от PT ISIM Endpoint.

5.5.3. Активация лицензии коллектора

Для работы коллектора и его защиты от нелегального использования нужно активировать лицензию.

Для активации лицензии необходимо выполнить следующие шаги:

- сгенерировать отпечаток;
- отправить отпечаток по электронной почте вашему менеджеру Positive Technologies для создания файла лицензии;
- активировать лицензию.

- Чтобы сгенерировать отпечаток,

на узле с коллектором выполните команду:

```
sudo /opt/ptisim/bin/generate-c2v
```

- Чтобы активировать лицензию,

на узле с коллектором выполните команду:

```
sudo /opt/ptisim/bin/upload-v2c <Путь к каталогу с файлом лицензии>
```

Лицензия активирована.

Примечание. Если потребуется повторно активировать лицензию или обновить истекшую, после активации необходимо перезапустить сервис `ptisim-core.service`, выполнив команду `sudo systemctl restart ptisim-core.service`.

5.6. Установка PT ISIM Overview Center

В этом разделе приводятся инструкции по установке PT ISIM Overview Center.

В этом разделе

[Подготовка к установке PT ISIM Overview Center \(см. раздел 5.6.1\)](#)

[Установка PT ISIM Overview Center на физическом сервере \(см. раздел 5.6.2\)](#)

[Установка PT ISIM Overview Center на удаленном сервере \(см. раздел 5.6.3\)](#)

[Установка PT ISIM Overview Center в виртуальной среде \(см. раздел 5.6.4\)](#)

[Первоначальная настройка PT ISIM Overview Center \(см. раздел 5.6.5\)](#)

5.6.1. Подготовка к установке PT ISIM Overview Center

Для установки PT ISIM Overview Center вам потребуется [установочный комплект \(см. раздел 5.2\)](#), аппаратное обеспечение без установленной операционной системы или виртуальная машина и гипервизор.

Перед установкой PT ISIM Overview Center необходимо:

1. При установке на физический сервер проверить, что сервер соответствует [аппаратным требованиям \(см. раздел 3.1\)](#). При установке в виртуальной среде проверить, что соблюдены [требования для импорта ISO-образа \(см. раздел 3.3\)](#).
2. Перенести на сервер с помощью внешнего носителя установочный комплект.
3. Если установочный комплект не содержит образа дистрибутива ОС, перенести на сервер образ дистрибутива ОС и [установить ОС \(см. раздел 5.1\)](#). Контрольная сумма образа дистрибутива ОС должна соответствовать указанной [в программных требованиях \(см. раздел 3.2\)](#).

Примечание. Образ дистрибутива Debian вы можете скачать по ссылкам, указанным [в программных требованиях \(см. раздел 3.2\)](#).

4. Авторизоваться в операционной системе, используя учетную запись, созданную во время установки ОС, и повысить ее привилегии до root с помощью команды `sudo su -`.

5.6.2. Установка PT ISIM Overview Center на физическом сервере

Для установки PT ISIM Overview Center потребуется установочный комплект PT ISIM Overview Center. В комплект входят пакеты и установочный скрипт. Помимо компонентов продукта и необходимых зависимостей, скрипт также изменит на сервере локаль `en_US.UTF-8` и настроит использование часового пояса UTC.

Внимание! Крайне не рекомендуется менять часовой пояс после установки, так как это может привести к некорректной работе PT ISIM Overview Center.

Внимание! При установке PT MC и PT ISIM Overview Center на одном сервере необходимо соблюсти следующую последовательность действий: установить PT MC, изменив в процессе установки порт PostgreSQL с 5432 на 6432 (или другой свободный порт) и установить PT ISIM Overview Center.

Примечание. Для установки PT ISIM Overview Center необходимо повысить привилегии учетной записи до root с помощью команды `sudo su -`.

► Чтобы установить PT ISIM Overview Center:

1. Распакуйте установочный комплект PT ISIM Overview Center и перейдите в распакованный каталог:

```
tar xzvf ptisim-package-overview-server-«Версия продукта».tgz
cd ptisim-package-overview-server-«Версия продукта»
```

2. Запустите установочный скрипт:

```
sudo ./ptisim-install
```

Начнется установка PT ISIM Overview Center.

После установки продукта требуется выполнить его [предварительную настройку](#) (см. раздел 5.6.5.1), а также [подключить узлы ISIM](#) (см. раздел 7.4.7).

5.6.3. Установка PT ISIM Overview Center на удаленном сервере

Вы можете установить PT ISIM Overview Center на удаленном сервере, подключившись к нему по SSH. В этом разделе приводится инструкция по установке PT ISIM Overview Center с помощью утилиты screen.

Примечание. Вы можете использовать терминальный мультиплексор, чтобы установочный скрипт запускался в своем терминале на удаленном сервере, независимо от SSH-сессии. Иначе, если во время установки SSH-сессия будет прервана, установка может завершиться некорректно.

Примечание. Для установки PT ISIM Overview Center необходимо повысить привилегии учетной записи до root с помощью команды `sudo su -`.

► Чтобы установить PT ISIM Overview Center на удаленном сервере:

1. Подключитесь к серверу, на котором планируете установить PT ISIM Overview Center:

```
ssh <Имя пользователя>@<IP-адрес или доменное имя сервера>
```

2. Распакуйте установочный комплект PT ISIM Overview Center и перейдите в распакованный каталог:

```
tar xzvf ptisim-package-overview-server-«Версия продукта».tgz
cd ptisim-package-overview-server-«Версия продукта»
```

3. Установите утилиту screen:

```
sudo dpkg -i ptisim/screen*
```

4. Настройте использование неинтерактивного способа установки:

```
export DEBIAN_FRONTEND=noninteractive
```

Примечание. При неинтерактивном способе установки процесс установки не будет ожидать пользовательского ввода. Настройка сетевых интерфейсов будет пропущена, и ее потребуется выполнить отдельно после завершения установки.

5. Запустите установочный скрипт в процессе screen:

```
screen -d -m -S ptisim-install ./ptisim-install
```

Следить за ходом установки вы можете с помощью файла журнала ptisim-install:

```
tail -f /var/log/ptisim-install.log
```

5.6.4. Установка PT ISIM Overview Center в виртуальной среде

Для установки PT ISIM Overview Center в виртуальной среде потребуется ISO-образ виртуальной машины и [гипервизор для импорта образа \(см. раздел 3.3\)](#).

После импорта ISO-образа и настройки сетевых интерфейсов при первом запуске виртуальной машины необходимо выполнить авторизацию на сервере PT ISIM Overview Center с помощью SSH. Для авторизации нужно использовать логин `root` (в Debian) или `administrator` (в Astra Linux) и пароль — `P@ssw0rd`. После авторизации нужно повысить привилегии учетной записи до `root`, выполнив команду `sudo su -`.

Внимание! После первого входа рекомендуется сменить пароль пользователя с помощью команды `passwd`.

Если к `root`-пользователю виртуальной машины необходим удаленный доступ по SSH, откройте на редактирование файл `/etc/ssh/sshd_config`, для параметра **PermitRootLogin** укажите значение `Yes`, сохраните изменения и выполните команду `systemctl restart sshd.service`.

Примечание. Если PT ISIM Overview Center установлен на виртуальной машине под управлением Windows, то дата и время в интерфейсе PT ISIM Overview Center и в операционной системе будут отличаться.

В этом разделе

[Установка PT ISIM Overview Center на Oracle VM VirtualBox \(см. раздел 5.6.4.1\)](#)

[Установка PT ISIM Overview Center на VMware vSphere \(см. раздел 5.6.4.2\)](#)

[Установка PT ISIM Overview Center на VMware Workstation \(см. раздел 5.6.4.3\)](#)

5.6.4.1. Установка PT ISIM Overview Center на Oracle VM VirtualBox

► Чтобы установить PT ISIM Overview Center на Oracle VM VirtualBox:

1. Запустите Oracle VM VirtualBox.
2. В меню **Машина** выберите пункт **Создать**.
Откроется окно создания виртуальной машины.
3. Введите имя виртуальной машины.
4. В поле **Образ ISO** выберите файл с образом ISO.
В поле **Тип** автоматически подставится значение **Linux**, в поле **Версия** — **Debian (64-bit)**. Если этого не произошло, выберите эти значения вручную.
5. Установите флажок **Пропустить автоматическую установку** и нажмите кнопку **Далее**.
6. Укажите необходимый объем памяти и количество задействованных ядер центрального процессора с учетом [аппаратных требований \(см. раздел 3.1\)](#) и нажмите **Далее**.
7. Выберите пункт **Создать новый виртуальный жесткий диск**, укажите размер диска в соответствии с [аппаратными требованиями \(см. раздел 3.1\)](#) и нажмите **Далее**.
Откроется окно с описанием выбранной конфигурации виртуальной машины.
Примечание. Если требуется, вы можете вернуться на предыдущие шаги и внести исправления.
8. Нажмите кнопку **Готово** для создания виртуальной машины.
9. В контекстном меню созданной виртуальной машины выберите пункт **Настроить**.
10. В открывшемся окне в разделе **Сеть** выберите вкладку **Адаптер 1**.
11. Установите флажок **Включить сетевой адаптер**.
12. В раскрывающемся списке **Тип подключения** выберите значение **Сетевой мост**.
Если требуется, вы можете выбрать другой тип подключения для доступа к интерфейсу PT ISIM Overview Center. В этом случае следующие шаги могут отличаться от представленных.
13. В раскрывающемся списке **Имя** выберите название сетевого адаптера, соответствующего сервисному интерфейсу.
14. Нажмите кнопку **ОК**.
Откроется окно со списком виртуальных машин.
15. Запустите созданную виртуальную машину двойным щелчком мыши.

16. На открывшейся странице выберите пункт **Auto Install ISIM on one disk**.

17. Нажмите клавишу **Enter** или подождите 10 секунд.

Запустится автоматическая установка PT ISIM Overview Center.

5.6.4.2. Установка PT ISIM Overview Center на VMware vSphere

► Чтобы установить PT ISIM Overview Center на VMware vSphere:

1. Запустите приложение клиента VMware vSphere.
2. Подключитесь к удаленному серверу VMware vSphere.
3. В приложении VMware vSphere нажмите **Файл** → **Новая виртуальная машина** и выберите ранее подключенный удаленный сервер.
4. В открывшемся окне выберите тип конфигурации **Обычный** и нажмите кнопку **Далее**.
5. Укажите расположение виртуальной машины и нажмите кнопку **Далее**.
6. Выберите хранилище виртуальной машины и нажмите кнопку **Далее**.
7. В блоке параметров **Гостевая операционная система** выберите вариант **Linux**.
8. В раскрывающемся списке **Версия** выберите версию, для которой предназначен ISO-образ, — **Debian GNU/Linux 10 (64-bit)** — и нажмите кнопку **Далее**.
9. В поле **Имя виртуальной машины** введите имя виртуальной машины и нажмите кнопку **Далее**.
10. Укажите размер диска в соответствии [с аппаратными требованиями \(см. раздел 3.1\)](#) и нажмите **Далее**.
11. Нажмите кнопку **Настройка оборудования**.
12. В открывшемся окне **Оборудование** в списке устройств выберите **Память** и **Процессор** и укажите необходимый объем памяти и количество задействованных ядер центрального процессора в соответствии [с аппаратными требованиями \(см. раздел 3.1\)](#).
13. В списке устройств выберите **Новый CD/DVD (IDE)**, в блоке параметров **Подключение** выберите вариант **Файл образа ISO** и с помощью кнопки **Обзор** выберите файл ISO-образа с PT ISIM.
14. В списке устройств выберите **Сетевой адаптер** и в поле **Подключение к сети** выберите сервисный интерфейс для доступа к веб-интерфейсу PT ISIM Overview Center.
15. Нажмите кнопку **Заккрыть**.
16. В окне **Мастер создания виртуальной машины** нажмите кнопку **Финиш**.

Откроется окно со списком виртуальных машин.

17. В контекстном меню созданной виртуальной машины выберите пункт **Питание** и нажмите кнопку **Включить**.
18. На открывшейся странице выберите пункт **Auto Install ISIM on one disk**.
19. Нажмите клавишу **Enter** или подождите 10 секунд.
Запустится автоматическая установка PT ISIM Overview Center.

5.6.4.3. Установка PT ISIM Overview Center на VMware Workstation

► Чтобы установить PT ISIM Overview Center на VMware Workstation:

1. Запустите VMware Workstation.
2. Нажмите **Файл** → **Новая виртуальная машина**.
3. В открывшемся окне выберите тип конфигурации **Обычный** и нажмите кнопку **Далее**.
4. В блоке параметров выберите вариант **Файл образа установки (iso)**, с помощью кнопки **Обзор** выберите файл ISO-образа с PT ISIM Overview Center и нажмите кнопку **Далее**.
5. В блоке параметров **Гостевая операционная система** выберите вариант **Linux**.
6. В раскрывающемся списке **Версия** выберите версию, для которой предназначен ISO-образ, — Debian GNU/Linux 10 (64-bit) — и нажмите кнопку **Далее**.
7. Укажите имя и расположение виртуальной машины и нажмите кнопку **Далее**.
8. Укажите размер диска в соответствии с [аппаратными требованиями \(см. раздел 3.1\)](#) и нажмите **Далее**.
9. Нажмите кнопку **Настройка оборудования**.
10. В открывшемся окне **Оборудование** в списке устройств выберите **Память** и **Процессор** и укажите необходимый объем памяти и количество задействованных ядер центрального процессора в соответствии с [аппаратными требованиями \(см. раздел 3.1\)](#).
11. В списке устройств выберите **Сетевой адаптер** и в поле **Подключение к сети** выберите сервисный интерфейс для доступа к веб-интерфейсу PT ISIM Overview Center.
12. Нажмите кнопку **Заккрыть**.
13. В окне **Мастер создания виртуальной машины** нажмите кнопку **Финиш**.
Откроется окно со списком виртуальных машин.
14. В контекстном меню созданной виртуальной машины выберите пункт **Питание** и нажмите кнопку **Включить**.
15. На открывшейся странице выберите пункт **Auto Install ISIM on one disk**.
16. Нажмите клавишу **Enter** или подождите 10 секунд.

Запустится автоматическая установка PT ISIM Overview Center.

5.6.5. Первоначальная настройка PT ISIM Overview Center

После установки PT ISIM Overview Center нужно:

- выполнить [первоначальную настройку](#) (см. раздел 5.6.5.1) в веб-интерфейсе PT ISIM Overview Center;
- активировать лицензию;

Примечание. Лицензия PT ISIM Overview Center активируется при его [подключении к серверу обновлений](#) (см. раздел 5.6.5.2).

- [подключить](#) (см. раздел 7.4.7) узлы PT ISIM View Sensor — напрямую или через другие узлы PT ISIM Overview Center.

В этом разделе

[Первоначальная настройка PT ISIM Overview Center в веб-интерфейсе](#) (см. раздел 5.6.5.1)

[Подключение PT ISIM Overview Center к серверу обновлений](#) (см. раздел 5.6.5.2)

5.6.5.1. Первоначальная настройка PT ISIM Overview Center в веб-интерфейсе

Перед началом использования PT ISIM Overview Center необходимо выполнить его предварительную настройку: выбрать язык системы, указать название и геолокацию узла, создать учетную запись пользователя и указать данные контактного лица.

- Чтобы выполнить первоначальную настройку PT ISIM Overview Center в веб-интерфейсе:

1. В адресной строке браузера введите IP-адрес или доменное имя веб-сервера PT ISIM Overview Center.

Откроется окно **Регистрация PT ISIM Overview Center**.

2. В раскрывающемся списке **Язык системы** выберите язык отображения веб-интерфейса.
3. В поле **Название узла ISIM** введите название настраиваемого узла.

Поскольку в системе может быть несколько узлов ISIM, рекомендуется присваивать им уникальные названия, чтобы различать их в списке узлов ISIM.

4. В поле **Геолокация узла ISIM** введите координаты объекта, на котором установлен PT ISIM Overview Center.

Вы также можете выбрать местоположение объекта на географической карте. В этом случае поле **Геолокация узла ISIM** заполнится автоматически.

5. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Далее**.

6. В полях **Логин** и **Пароль** введите учетные данные пользователя PT ISIM Overview Center.

После завершения предварительной настройки будет создана локальная учетная запись пользователя с ролью **Администратор**.

7. В поле **Электронная почта** введите адрес электронной почты и нажмите кнопку **Далее**.
8. В окне **Контактное лицо** введите данные контактного лица: имя, адрес электронной почты и телефон.

Контактное лицо может не быть пользователем PT ISIM. Его контактные данные являются составной частью пакета регистрации и могут понадобиться для получения информации о состоянии объекта и оперативного реагирования на инциденты.

9. Нажмите кнопку **Завершить**.

5.6.5.2. Подключение PT ISIM Overview Center к серверу обновлений

PT ISIM Overview Center позволяет централизованно обновлять все нижестоящие узлы View Sensor (в том числе подключенные не напрямую, а через другие узлы Overview Center). Чтобы пакеты с обновлениями автоматически появлялись на PT ISIM Overview Center, требуется подключить Overview Center к серверу обновлений с помощью специального ключа, который поставляется вместе с продуктом.

Примечание. Адрес сервера обновлений по умолчанию — update.ptsecurity.com. Если требуется, вы можете [изменить его](#) (см. [раздел 6.9](#)).

- Чтобы подключить PT ISIM Overview Center к серверу обновлений:

1. В панели инструментов выберите пункт **Узлы ISIM** → **Подключение к серверу обновлений**.
2. Нажмите **Загрузить ключ** и в открывшемся окне выберите ключ для подключения к серверу обновлений.
В случае успешной загрузки ключа отобразится его идентификатор и срок действия.
3. В раскрывающемся списке **Проверка обновлений** выберите частоту, с которой PT ISIM Overview Center будет проверять наличие обновлений на сервере обновлений и скачивать их по мере доступности.

Вы можете отключить проверку обновлений, если планируете устанавливать обновления вручную.

PT ISIM Overview Center подключен к серверу обновлений.

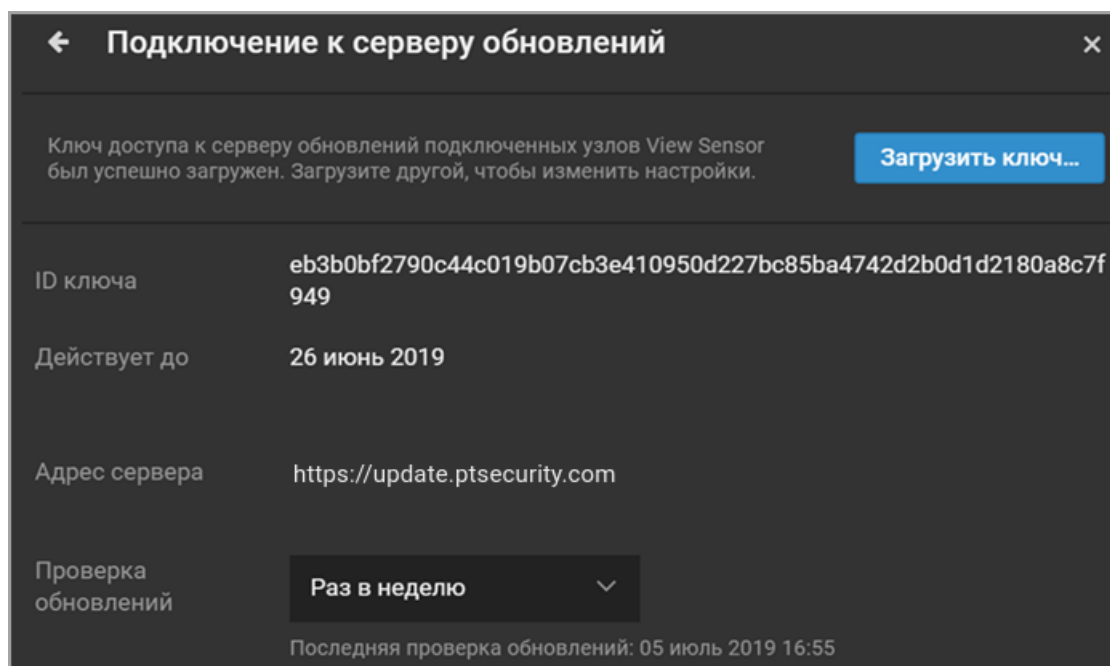


Рисунок 45. Подключение к серверу обновлений

После подключения PT ISIM Overview Center будет периодически проверять наличие обновлений на сервере обновлений, скачивать их по мере доступности и передавать подключенным узлам View Sensor. Когда обновление передано, оно становится доступно в веб-интерфейсе PT ISIM Overview Center для установки на узлы View Sensor.

5.7. Установка PT ISIM Industrial Tablet на виртуальную машину или промышленный планшет

PT ISIM View Sensor может работать в режиме информационного киоска с помощью программного продукта PT ISIM Industrial Tablet, представляющего собой упрощенный интерфейс сенсора.

Вы можете использовать PT ISIM Industrial Tablet через веб-интерфейс без установки дополнительных компонентов. Через браузер вы можете просматривать инциденты и закрывать их, но не можете выгружать данные инцидентов и пакет диагностической информации. Для использования этой функции необходимо установить PT ISIM Industrial Tablet на виртуальную машину или промышленный планшет.

Для установки PT ISIM Industrial Tablet потребуется установочный комплект PT ISIM Industrial Tablet. В него входят пакеты и установочный скрипт.

► Чтобы установить PT ISIM Industrial Tablet:

1. Установите на виртуальной машине или промышленном планшете операционную систему [Astra Linux](#) (см. раздел 5.1.4), [Debian 10](#) (см. раздел 5.1.1) или [Debian 12](#) (см. раздел 5.1.2).
2. Авторизуйтесь в операционной системе, используя учетную запись, созданную во время установки ОС, и повысьте привилегии до root с помощью команды `sudo su -`.
3. Распакуйте установочный комплект PT ISIM Industrial Tablet и перейдите в распакованный каталог:

```
tar -xvf ptisim-package-kiosk-<Версия продукта>.tgz
cd ptisim-package-kiosk-<Версия продукта>
```
4. Запустите установочный скрипт:

```
sudo ./ptisim-install
```
5. Начнется установка PT ISIM Industrial Tablet.
6. В строке **Enter the IP address of the remote machine** введите IP-адрес сервера, на котором установлен PT ISIM View Sensor.

```

user@debian: ~
File Edit View Search Terminal Help
=====
prepare disable_ipv6
Execute systemctl -p
=====
prepare create_user
Execute getent group ptisim
Execute addgroup --system ptisim
Execute getent passwd ptisim
Execute adduser --system --ingroup ptisim --home /opt/ptisim --disabled-login pt
isim
Execute usermod -aG adm ptisim
Execute chown ptisim:ptisim /opt/ptisim
=====
All actions done.
=== :> [1/1] Processing step kiosk
Execute apt-get install -y --allow-downgrades ptisim-web-kiosk-daemon-master=4.2
.184 ptisim-web-kiosk-client-master=0.0.44 beep alsa-utils coreutils dosfstools
python3 systemd libcurl4-openssl-dev python3-pycurl ntfs-3g nginx chromium xinit
xserver-xorg jq
Execute apt-mark auto beep alsa-utils coreutils dosfstools python3 systemd libcu
rl4-openssl-dev python3-pycurl ntfs-3g nginx chromium xinit xserver-xorg jq
Execute chmod +x /opt/ptisim/bin/configure-kiosk-client.sh
=====
Enter the IP address of the remote machine (default is 127.0.0.1): 192.168.31.7

```

Рисунок 46. Настройка подключения к серверу

7. Дождитесь завершения установки.

8. Если у вас установлены операционная система Debian 10 или 12 и антивирус Kaspersky Endpoint Security 12, то отключите модуль проверки зашифрованного трафика антивирусом, выполнив команду `kesl-control -N --set-net-settings EncryptedConnectionsScan=No`.
9. Если у вас установлена операционная система Debian, то перезапустите PT ISIM Industrial Tablet.
10. Если у вас установлена операционная система Astra Linux, то выполните следующие действия:
 - Задайте пароль для учетной записи пользователя с именем **kiosk**, выполнив команду `sudo passwd kiosk`.
 - Задайте уровень целостности для учетной записи пользователя с именем **kiosk**, выполнив команду `sudo pdpl-user -i 63 kiosk`.
 - Перезапустите PT ISIM Industrial Tablet.
 - Авторизуйтесь в PT ISIM Industrial Tablet, используя учетную запись пользователя с именем **kiosk** и заданный вами пароль.

Примечание. Авторизация пользователя с именем **kiosk** должна быть выполнена через локальный терминал виртуальной машины или промышленного планшета, где установлен PT ISIM Industrial Tablet.

- Для параметра **Integrity level** (уровень целостности) введите значение **63**.

Когда связь с сенсором будет установлена, на экране отобразится окно входа в PT ISIM Industrial Tablet.

После установки PT ISIM Industrial Tablet рекомендуется [изменить пароли](#) (см. раздел 7.5.2) для доступа, используемые по умолчанию.

Если впоследствии PT ISIM View Sensor будет переустановлен или IP-адрес текущего сенсора будет изменен, то потребуются [изменить IP-адрес сервера](#) (см. раздел 7.5.3) для подключения PT ISIM Industrial Tablet к сенсору.

5.8. Порядок установки PT ISIM View Sensor, PT ISIM Endpoint и PT MC на один сервер

Внимание! Компоненты устанавливаются в следующей последовательности: PT MC → PT ISIM View Sensor → PT ISIM Endpoint. Изменение последовательности шагов, описанных ниже, может привести к неработоспособности конфигурации.

- ▶ Чтобы установить PT ISIM View Sensor, PT ISIM Endpoint и PT MC на один сервер:
 1. [Установите ОС](#) (см. раздел 5.1).
 2. Повысьте привилегии учетной записи до root с помощью команды `sudo su -`.
 3. Перенесите установочные комплекты компонентов на сервер.

4. Установите PT MC, выполнив установку ролей в следующей последовательности: Deployer → SqlStorage → LogConnector → Observability → Management and Configuration.

Внимание! При установке роли SqlStorage нужно изменить порт PostgreSQL с 5432 на 6432 (или другой свободный порт), указав новый порт в параметре PgPort набора параметров **Basic configuration**.

Примечание. Инструкции по установке ролей приведены [в справке](#) PT MC. Поддерживаемые версии PT MC указаны [в программных требованиях \(см. раздел 3.2\)](#).

5. Войдите в PT MC.

Примечание. Веб-интерфейс PT MC доступен по адресу `https://<IP-адрес PT MC>:3334`. Логин по умолчанию — administrator, пароль — P@ssw0rd.

После успешного входа система попросит сменить пароль пользователя.

6. Смените пароль пользователя.
7. Активируйте лицензию PT MC офлайн (см. раздел «Активация PT MC» [в справке](#) PT MC).
8. [Установите \(см. раздел 5.3.2\)](#) PT ISIM View Sensor.
9. [Активируйте лицензию \(см. раздел 5.3.5.2\)](#) PT ISIM View Sensor.

10. Выполните команду:

```
/opt/ptisim/bin/local_ptmc_rules.sh <Порт PostgreSQL, указанный при установке PT MC. По умолчанию – 6432>
```

11. [Настройте сервис ptisim-rester \(см. раздел 7.1.13\)](#) для получения данных от агентов PT ISIM Endpoint в PT ISIM View Sensor.

12. Войдите в PT ISIM View Sensor.

Примечание. Веб-интерфейс PT ISIM View Sensor доступен по адресу `https://<IP-адрес PT ISIM View Sensor>:443`. Логин по умолчанию — administrator, пароль — P@ssw0rd.

13. [Настройте подключение \(см. раздел 7.1.2\)](#) к PT MC.

Примечание. Установка доверенного SSL-сертификата при установке PT ISIM View Sensor на одном сервере с PT MC не требуется.

После успешного подключения в PT MC отобразится соответствующая площадка.

14. [Установите \(см. раздел 5.4.2\)](#) PT ISIM Endpoint.

15. Войдите в PT ISIM Endpoint.

Примечание. Веб-интерфейс PT ISIM Endpoint доступен по адресу `https://<IP-адрес PT ISIM Endpoint>:4443`. Вход в PT ISIM Endpoint выполняется под учетной записью пользователя PT MC.

16. [Активируйте лицензию \(см. раздел 5.4.4\)](#) PT ISIM Endpoint.

Установка компонентов на один сервер выполнена. Если IP-адрес сервера изменится, например при переносе из одной сети в другую, нужно [изменить IP-адрес в параметрах компонентов \(см. раздел 5.9\)](#).

5.9. Изменение IP-адреса сервера PT ISIM в параметрах компонентов для конфигурации all-in-one

В конфигурации all-in-one на сервере PT ISIM устанавливаются следующие компоненты: PT ISIM View Sensor, PT MC и PT ISIM Endpoint. Если IP-адрес сервера PT ISIM изменился, например при переносе сервера из одной сети в другую, то для корректной работы конфигурации all-in-one нужно изменить IP-адрес сервера в параметрах компонентов на новый.

- ▶ Чтобы изменить IP-адрес сервера PT ISIM в параметрах компонентов для конфигурации all-in-one:

1. Обновите конфигурацию PT MC:

```
/opt/deployer/bin/Restart-Configuration.ps1 '*' -Verbose
```

Примечание. Выполнение команды может занять длительное время.

2. Если на предыдущем шаге появились ошибки, выполните команду:

```
deployer instance reconfigure -type deployer && deployer instance reconfigure --diff
```

Веб-интерфейс PT MC будет доступен по ссылке [https://<Новый IP-адрес сервера PT ISIM>:<Порт для подключения к PT MC \(по умолчанию — 3334\)>](https://<Новый IP-адрес сервера PT ISIM>:<Порт для подключения к PT MC (по умолчанию — 3334)>).

3. Выполните команду:

```
/opt/ptisim/bin/local_ptmc_rules.sh <Номер порта, который был указан при установке PT MC для базы данных PostgreSQL>.
```

Например, `/opt/ptisim/bin/local_ptmc_rules.sh 6432`.

4. Перейдите в каталог с установочным пакетом PT ISIM Endpoint.

5. Откройте файл `install.cfg`.

6. В параметре **pt_mc_address** введите новый IP-адрес сервера.

7. В параметре **ui_server_host** введите новый IP-адрес сервера.

8. Сохраните изменения и закройте файл.

9. Выполните команду:

```
sudo ./install.sh
```

10. Войдите в веб-интерфейс PT ISIM View Sensor под учетной записью с правами администратора и [измените \(см. раздел 7.1.2.2\)](#) параметры подключения к PT MC.

6. Обновление PT ISIM

В этом разделе приводятся инструкции по обновлению компонентов PT ISIM, экспертной базы PT ISTI на узлах PT ISIM View Sensor и антивирусных баз на конечных узлах.

Обновление узлов PT ISIM View Sensor и экспертной базы PT ISTI на них вы можете выполнять централизованно с помощью PT ISIM Overview Center.

В этом разделе

[Обновление PT ISIM View Sensor \(см. раздел 6.1\)](#)

[Централизованное обновление узлов View Sensor с помощью Overview Center \(см. раздел 6.2\)](#)

[Обновление PT ISIM Endpoint \(см. раздел 6.3\)](#)

[Обновление PT ISIM Collector \(см. раздел 6.4\)](#)

[Обновление PT ISIM Overview Center \(см. раздел 6.5\)](#)

[Обновление PT ISIM Industrial Tablet \(см. раздел 6.6\)](#)

[Обновление экспертной базы PT ISTI \(см. раздел 6.7\)](#)

[Обновление антивирусных баз и пакета экспертизы в PT ISIM Endpoint \(см. раздел 6.8\)](#)

[Изменение адреса сервера обновлений \(см. раздел 6.9\)](#)

6.1. Обновление PT ISIM View Sensor

Примечание. Информация о совместимости версий PT ISIM View Sensor указана [в программных требованиях \(см. раздел 3.2\)](#).

Для обновления PT ISIM View Sensor вам потребуется установочный комплект с новой версией продукта, предоставляемый службой технической поддержки Positive Technologies, а также действующая лицензия.

Установка новой версии возможна при выполнении следующих условий:

- Лицензия действительна на момент обновления. Информация о сроке действия лицензии доступна в веб-интерфейсе продукта по нажатию ⓘ. Если срок действия лицензии истек, потребуется загрузить новую лицензию перед обновлением продукта.
- Объем свободного дискового пространства на сервере с PT ISIM View Sensor не ниже [заданного минимального объема \(см. раздел 7.1.3\)](#) (20% по умолчанию).

Кроме того, перед выполнением обновления установочный скрипт проверит статус всех [служб \(см. раздел 7.1.14.2\)](#), необходимых для корректной работы продукта. Если не все службы запущены, отобразится сообщение с вопросом, запускать ли обновление. В этом случае рекомендуется отложить обновление, проверить и при необходимости перезапустить указанные службы.

Примечание. Если вы используете Debian 10, то после обновления PT ISIM вы также можете [обновить операционную систему до Debian 12 \(см. раздел 5.1.3\)](#) без потери данных сенсора.

Примечание. Если вы используете Astra Linux 1.7.2, то до обновления PT ISIM View Sensor нужно [обновить операционную систему до версии 1.7.6 \(см. раздел 5.1.5\)](#). Это можно сделать без потери накопленных данных.

Примечание. Если требуется обновить PT MC, установленный на одном сервере с PT ISIM View Sensor, то нужно сначала обновить PT ISIM View Sensor, а затем PT MC, после чего выполнить команду `/opt/ptisim/bin/local_ptmc_rules.sh <Номер порта>`, который был указан при установке PT MC, по умолчанию 6432.

Процедура обновления идентична для обоих способов установки продукта (на физическом сервере или виртуальной машине): комплект с новой версией продукта устанавливается поверх текущей версии с помощью установочного скрипта `ptisim-install`.

Внимание! Во время обновления не выполняйте жесткую перезагрузку сервера или виртуальной машины, на которой установлен продукт.

► Чтобы обновить PT ISIM View Sensor:

1. Перенесите установочный комплект на сервер или виртуальную машину, на которой планируется обновить продукт.
2. Распакуйте установочный комплект PT ISIM и перейдите в распакованный каталог:

```
tar xzvf ptisim-package-<Версия продукта>.tgz  
cd ptisim-package-<Версия продукта>
```
3. Запустите установочный скрипт:

```
sudo ./ptisim-install
```

Начнется установка новой версии PT ISIM View Sensor.

После успешного обновления PT ISIM View Sensor 5.1–5.7 до версии 5.8 или выше вы можете [удалить неиспользуемые файлы модели сети \(см. раздел 7.1.20\)](#).

Если вы используете PT ISIM Industrial Tablet, узел, на котором он установлен, необходимо перезагрузить после завершения обновления PT ISIM View Sensor.

См. также

[Настройка автоматического обновления узлов View Sensor с помощью Overview Center \(см. раздел 6.2.1\)](#)

6.2. Централизованное обновление узлов View Sensor с помощью Overview Center

Далее приведена основная информация о централизованном обновлении узлов PT ISIM View Sensor, подключенных к PT ISIM Overview Center, а также даны инструкции по выполнению такого обновления в автоматическом и офлайн-режиме.

В этом разделе

Настройка автоматического обновления узлов View Sensor с помощью Overview Center (см. раздел 6.2.1)

Обновление узлов View Sensor с помощью Overview Center в офлайн-режиме (см. раздел 6.2.2)

6.2.1. Настройка автоматического обновления узлов View Sensor с помощью Overview Center

PT ISIM Overview Center позволяет централизованно обновлять узлы View Sensor. Для этого требуется, чтобы все узлы Overview Center в иерархической структуре были [обновлены](#) (см. раздел 6.5) до поддерживаемой [версии](#) (см. раздел 3.2) и чтобы PT ISIM Overview Center был [подключен к серверу обновлений](#) (см. раздел 5.6.5.2).

Примечание. Информация о совместимости версий PT ISIM View Sensor и PT ISIM Overview Center указана [в программных требованиях](#) (см. раздел 3.2).

Когда пакет с обновлением попадает на PT ISIM Overview Center, он автоматически передается на нижестоящие узлы View Sensor. При этом учитываются следующие параметры узла View Sensor:

- Тип узла (proView, netView или microView). На узел передается только обновление того же типа.
- Вариант поставки, который определяет характеристики продукта, такие как набор функций и правил заведения инцидентов и событий, отображение элементов интерфейса. Вариант поставки может быть универсальным (**base**) или специфичным для определенной индустрии или объекта. На узел View Sensor передается обновление, относящееся к тому же варианту поставки, что и сам узел.
- Версия обновления. На узел передается только обновление не ниже установленного.
- Тип и версия операционной системы. На узел передается только обновление, соответствующее используемой операционной системе.

Список всех узлов View Sensor, которые можно обновить, отображается на странице **Обновление View Sensor** с указанием версий, доступных для установки.

► Чтобы настроить автоматическое обновление узлов View Sensor:

1. Проверьте сетевое соединение.

При наличии сетевого соединения с сервером обновлений PT ISIM Overview Center будет периодически проверять наличие обновлений на сервере, скачивать их по мере доступности и передавать подключенным узлам View Sensor, в результате чего они станут доступны в веб-интерфейсе PT ISIM Overview Center для установки на узлы View Sensor согласно следующим шагам инструкции.

2. Если сетевое соединение с сервером обновлений отсутствует, распакуйте пакет с обновлением на сервере с PT ISIM Overview Center [в офлайн-режиме](#) (см. раздел 6.2.2).

Обновления станут доступны в веб-интерфейсе PT ISIM Overview Center для установки на узлы View Sensor согласно следующим шагам инструкции.

3. В веб-интерфейсе PT ISIM Overview Center в панели инструментов выберите пункт **Узлы ISIM → Обновление View Sensor**.

В нижней части окна **Обновление View Sensor** отображается последняя версия обновления, полученная PT ISIM Overview Center.

4. Если необходимо установить версию обновления, отличную от последней, нажмите **К списку версий** и в открывшемся окне выберите версию обновления.
5. Выберите узлы View Sensor, на которые вы хотите установить указанную версию, и нажмите **Установить**.

Примечание. Вы можете фильтровать узлы по типу (microView, netView или proView), по номеру установленной версии и по узлу Overview Center, к которому они подключены.

Запустится процесс обновления.

Проверить успешность установки всех обновлений вы можете с помощью вкладки **Статус обновлений**. Обновление может иметь следующий статус:  — обновление установлено успешно,  — обновление происходит в текущий момент,  — отсутствует информация о статусе обновления (возможно, потеряно соединение с обновляемым узлом),  — произошла ошибка, обновить узел не удалось.

Список обновлений, доступных для отдельного узла View Sensor, отображается по нажатию кнопки **Доступно обновление** в карточке узла. По этой кнопке вы можете обновить каждый узел отдельно, а также просмотреть историю обновления узла через Overview Center.

6.2.2. Обновление узлов View Sensor с помощью Overview Center в офлайн-режиме

Примечание. Информация о совместимости версий PT ISIM View Sensor и PT ISIM Overview Center указана [в программных требованиях \(см. раздел 3.2\)](#).

Если PT ISIM Overview Center не подключен к серверу обновлений (например, отсутствует доступ в интернет или сетевое соединение с этим сервером), вы можете запросить специальный пакет с обновлением и распаковать его на сервере с PT ISIM Overview Center. После распаковки начнется автоматическая передача обновления подключенным узлам View Sensor. Если в вашей структуре узлов ISIM несколько узлов Overview Center, обновление требуется распаковать только на стороне PT ISIM Overview Center, расположенного на самом верхнем уровне: все нижестоящие узлы View Sensor (в том числе подключенные не напрямую, а через другие узлы Overview Center) автоматически получают данный пакет.

► Чтобы распаковать пакет обновления на сервере с PT ISIM Overview Center:

1. Перенесите полученный пакет с обновлением на сервер с PT ISIM Overview Center.
2. Запустите скрипт распаковки:

```
sudo su
/opt/ptisim-overview/bin/register_sensor_package.sh --path <Расположение пакета с
обновлением>
```

Например:

```
/opt/ptisim-overview/bin/register_sensor_package.sh --path /home/isim/overview-repo-isim-
proview-base_stretch.4.4.2716166.tar.gz
```

Передача распакованного пакета обновления подключенным узлам View Sensor может занять некоторое время. Когда пакет обновления передан, он становится доступным в веб-интерфейсе PT ISIM Overview Center [для установки на узлы View Sensor \(см. раздел 6.2.1\)](#).

6.3. Обновление PT ISIM Endpoint

Для обновления PT ISIM Endpoint вам потребуется установочный комплект с новой версией PT ISIM Endpoint, предоставляемый службой технической поддержки Positive Technologies, а также действующая лицензия.

Примечание. Начиная с версии 5.9 управление лицензиями PT ISIM Endpoint осуществляется только в PT MC. Если вы используете устаревший способ лицензирования через PT ISIM Endpoint, потребуется [добавить \(см. раздел 5.4.4\)](#) лицензию в PT MC и после обновления PT ISIM Endpoint привязать ее к приложению PT ISIM Endpoint в PT MC.

► Чтобы обновить PT ISIM Endpoint:

1. Если PT ISIM Endpoint развернут на одном сервере с PT ISIM View Sensor и PT MC, выполните команду:


```
systemctl stop edr.service
```
2. Перенесите установочный комплект с новой версией на сервер с установленным PT ISIM Endpoint.
3. Распакуйте установочный комплект в отдельный каталог и перейдите в него:


```
tar xf isim-endpoint.<Версия продукта>.tar.gz
cd isim-endpoint.<Версия продукта>
```
4. В конфигурационном файле `install.cfg` задайте параметры установки.

Пример файла `install.cfg` для конфигурации, когда PT ISIM View Sensor, PT MC и PT ISIM Endpoint находятся на одном сервере:

```
pt_mc_address=198.51.100.12
pt_mc_port=3334
isim_address=127.0.0.1
isim_port=6192
isim_transport=tcp
ui_server_host=198.51.100.12
```

```
ui_port=4443
db_root_password=PtEdrDBRootPassword
db_global_password=PtEdrDBGlobalPassword
db_instance_password=PtEdrDBInstancePassword
db_expertise_password=PtEdrDBExpertisePassword
mc_version=101.4.9271
```

5. Если обновление выполняется на узле под управлением Astra Linux, добавьте в файл `/etc/parsec/fs-ilev.conf` строки:

```
min /opt/edr
min /opt/edr_data
min /opt/edr_tmp
```

6. Для работы компонента Observability получите сертификаты и ключ сервиса PT MC collector-agent. Для этого выполните следующие действия:

- На сервере с установленным PT MC, адрес которого указан в файле `install.cfg` в параметре `pt_mc_address`, создайте каталог `certs`:

```
mkdir -p certs
```

- Скопируйте файлы `Portal.key`, `Portal.crt`, `rootCA.crt` в каталог `certs`:

```
cp /var/lib/deployed-roles/<Название роли Management and Configuration>/
managementandconfiguration/certs/{Portal.key,Portal.crt,rootCA.crt} <Путь к каталогу>/
certs
```

- Если PT MC установлен на отдельном сервере, скопируйте каталог `certs` на сервер с установочным комплектом PT ISIM Endpoint.
- На сервере с установочным комплектом PT ISIM Endpoint в файле манифеста `endpoint_manifest_template.json` добавьте параметры расположения файлов `Portal.key`, `Portal.crt`, `rootCA.crt` в секцию `hosts.127.0.0.1`:

```
{
  "hosts": {
    "127.0.0.1": {
      "mc_otel_certs": {
        "cert": "<Путь к каталогу>/Portal.crt",
        "key": "<Путь к каталогу>/Portal.key",
        "root_ca": "<Путь к каталогу>/rootCA.crt"
      },
    },
  },
}
```

7. Запустите установочный скрипт:

```
sudo ./install.sh
```

Начнется установка новой версии PT ISIM Endpoint.

8. При ответе на вопрос **Standalone installation, go to MC and approve registration of EDR. Press Y after approve for installation continue process... (y/n)?** выберите вариант **y**.

После завершения установки необходимо [активировать лицензию \(см. раздел 5.4.4\)](#) PT ISIM Endpoint (если требуется), [настроить \(см. раздел 7.1.13\)](#) PT ISIM View Sensor и [обновить агенты \(см. раздел 7.2.1.4\)](#).

6.4. Обновление PT ISIM Collector

Внимание! Версия коллектора должна совпадать с версией PT ISIM View Sensor.

► Чтобы обновить коллектор:

1. Перенесите установочный комплект на сервер или виртуальную машину, на которой планируется обновить продукт.

2. Распакуйте установочный комплект и перейдите в распакованный каталог:

```
tar xzvf ptisim-package-collector-«Версия продукта».tgz  
cd ptisim-package-collector-«Версия продукта»
```

3. Запустите установочный скрипт:

```
sudo ./ptisim-install
```

Начнется установка новой версии коллектора.

После обновления нужно заново [выгрузить \(см. раздел 7.3.4\)](#) конфигурацию из PT ISIM View Sensor и [загрузить \(см. раздел 7.3.5\)](#) ее на коллектор.

6.5. Обновление PT ISIM Overview Center

Внимание! Размер свободного места на диске должен быть больше, чем размер используемой базы PostgreSQL, иначе обновление не будет завершено.

Для обновления PT ISIM Overview Center вам потребуется установочный комплект с новой версией продукта. Процедура обновления идентична для обоих способов установки продукта (на физическом сервере или виртуальной машине): комплект с новой версией продукта устанавливается поверх текущей версии с помощью установочного скрипта `ptisim-install`.

Информация о совместимости версий PT ISIM Overview Center указана [в программных требованиях \(см. раздел 3.2\)](#).

Внимание! Если вы используете иерархическую структуру узлов ISIM, то обновление узлов PT ISIM Overview Center необходимо осуществлять согласно алгоритму, представленному ниже.

Для обновления узлов PT ISIM Overview Center при использовании иерархической структуры узлов ISIM нужно:

1. Отключить все узлы PT ISIM Overview Center [от сервера обновлений \(см. раздел 5.6.5.2\)](#).
2. Обновить согласно инструкции ниже все узлы PT ISIM Overview Center по порядку начиная с узла, являющегося корневым в иерархической структуре ISIM.
3. Подключить корневой узел PT ISIM Overview Center [к серверу обновлений \(см. раздел 5.6.5.2\)](#).

► Чтобы обновить PT ISIM Overview Center:

1. Распакуйте установочный комплект PT ISIM Overview Center и перейдите в распакованный каталог:

```
tar xzvf ptisim-package-overview-server-<Версия продукта>.tgz  
cd ptisim-package-overview-server-<Версия продукта>
```

2. Запустите установочный скрипт:

```
sudo ./ptisim-install
```

Начнется установка новой версии PT ISIM Overview Center.

6.6. Обновление PT ISIM Industrial Tablet

Процедура обновления идентична для обоих способов установки продукта (на виртуальной машине или на промышленном планшете): комплект с новой версией продукта устанавливается поверх текущей версии с помощью установочного скрипта `ptisim-install`.

Информация о совместимости версий PT ISIM Industrial Tablet указана [в программных требованиях \(см. раздел 3.2\)](#).

► Чтобы обновить PT ISIM Industrial Tablet:

1. Перенесите установочный комплект на сервер или виртуальную машину, на которой планируется обновить продукт.
2. Распакуйте установочный комплект PT ISIM Industrial Tablet и перейдите в распакованный каталог:

```
tar -xvf ptisim-package-kiosk-<Версия продукта>.tgz  
cd ptisim-package-kiosk-<Версия продукта>
```

3. Запустите установочный скрипт:

```
sudo ./ptisim-install
```

Начнется установка новой версии PT ISIM Industrial Tablet.

4. В строке **Enter the IP address of the remote machine** введите IP-адрес сервера, на котором установлен PT ISIM View Sensor.

```

user@debian: ~
File Edit View Search Terminal Help
=====
prepare disable_ipv6
Execute sysctl -p
=====
prepare create_user
Execute getent group ptisim
Execute addgroup --system ptisim
Execute getent passwd ptisim
Execute adduser --system --ingroup ptisim --home /opt/ptisim --disabled-login pt
isim
Execute usermod -aG adm ptisim
Execute chown ptisim:ptisim /opt/ptisim
=====
All actions done.
=== :> [1/1] Processing step kiosk
Execute apt-get install -y --allow-downgrades ptisim-web-kiosk-daemon-master=4.2
.184 ptisim-web-kiosk-client-master=0.0.44 beep alsa-utils coreutils dosfstools
python3 systemd libcurl4-openssl-dev python3-pycurl ntfs-3g nginx chromium xinit
xserver-xorg jq
Execute apt-mark auto beep alsa-utils coreutils dosfstools python3 systemd libcu
rl4-openssl-dev python3-pycurl ntfs-3g nginx chromium xinit xserver-xorg jq
Execute chmod +x /opt/ptisim/bin/configure-kiosk-client.sh
=====
Enter the IP address of the remote machine (default is 127.0.0.1): 192.168.31.7

```

Рисунок 47. Настройка подключения к сенсору

5. Дождитесь завершения установки.

PT ISIM Industrial Tablet обновлен.

6.7. Обновление экспертной базы PT ISTI

Для обработки трафика, заведения событий и обнаружения инцидентов PT ISIM View Sensor использует специальную экспертную базу Positive Technologies Industrial Security Threat Indicators (PT ISTI), выпускаемую в виде пакета `ptisim-rules`. Если в PT ISTI произошли изменения (например, добавлены правила разбора нового протокола или выявления новых инцидентов и нарушений, исправлена ошибка в существующих правилах), то вы можете обновить этот пакет отдельно от остального продукта.

Вы можете обновить базу PT ISTI [на одном узле \(см. раздел 6.7.1\)](#) PT ISIM View Sensor или централизованно сразу на нескольких.

Запуск обновления PT ISTI на узле PT ISIM View Sensor возможен [в веб-интерфейсе \(см. раздел 6.7.1\)](#) и [из консоли \(см. раздел 6.7.2\)](#).

[Централизованное обновление \(см. раздел 6.7.3\)](#) выполняется с помощью PT ISIM Overview Center и возможно на всей иерархии сенсоров, подключенных к нему напрямую или через другие узлы Overview Center.

Информация о совместимости версий PT ISIM Overview Center и PT ISIM View Sensor при обновлении базы PT ISTI указана в [программных требованиях \(см. раздел 3.2\)](#). Для установки доступны пакеты, версия которых выше текущей. Каждый пакет обновления базы PT ISTI содержит все предыдущие изменения, поэтому нет необходимости устанавливать обновления последовательно, достаточно установить последнюю версию.

Примечание. Версия базы PT ISTI должна соответствовать версии сенсора. Например, установить обновление экспертной базы PT ISTI версии 5.12 на узел PT ISIM версии 5.1 не получится, необходимо сначала обновить узел PT ISIM до версии 5.12.

Обновление базы PT ISTI возможно как в офлайн-режиме, так и онлайн — через сервер обновлений.

Примечание. Адрес сервера обновлений по умолчанию — update.ptsecurity.com. Если требуется, вы можете [изменить его \(см. раздел 6.9\)](#).

В этом разделе

[Обновление PT ISTI в веб-интерфейсе PT ISIM View Sensor \(см. раздел 6.7.1\)](#)

[Обновление PT ISTI на узле PT ISIM View Sensor из консоли \(см. раздел 6.7.2\)](#)

[Централизованное обновление базы PT ISTI с помощью Overview Center \(см. раздел 6.7.3\)](#)

6.7.1. Обновление PT ISTI в веб-интерфейсе PT ISIM View Sensor

Примечание. Обновление PT ISTI доступно при наличии действующей лицензии.

В PT ISIM View Sensor предусмотрено три режима обновления PT ISTI:

- **Отключено** — проверка и установка обновлений PT ISTI не осуществляются.
- **Сервер** — PT ISIM View Sensor подключается к серверу обновлений, проверяет наличие новых версий и автоматически скачивает их для установки.
- **Внешний диск** — обновления доставляются на внешнем носителе и передаются через USB-порт.

Вы можете просмотреть номера и даты выхода текущей и последней доступной версий PT ISTI в веб-интерфейсе продукта, нажав  → **Обновление экспертной базы PT ISTI**. Если для установки доступна новая версия PT ISTI, в главном меню отобразится значок .

Обновление PT ISTI с помощью сервера обновлений

При данном способе обновления PT ISIM раз в час автоматически проверяет доступность новых версий PT ISTI на сервере обновлений Positive Technologies. Если обнаружена новая версия, она выгружается на сервер PT ISIM и становится доступной для установки. При каждой следующей проверке более новая версия заменяет собой предыдущую, и для установки всегда доступна последняя версия PT ISTI.

► Чтобы обновить PT ISTI с помощью сервера обновлений:

1. В главном меню выберите  → **Обновление экспертной базы PT ISTI**.
2. Выберите вкладку **Сервер**.

Если для установки доступна новая версия PT ISTI, ее номер отобразится в нижней части окна. Вы также можете вручную проверить наличие новых версий на сервере, нажав кнопку **Проверить сейчас**.

3. Нажмите **Установить**.

Начнется установка новой версии PT ISTI.

Обновление PT ISTI с помощью внешнего носителя

Если у вас отсутствует стабильное подключение к серверу обновлений Positive Technologies, вы можете обновить PT ISTI с помощью внешнего носителя с пакетом правил, выданным Positive Technologies.

► Чтобы обновить PT ISTI с помощью внешнего носителя:

1. Вставьте в USB-порт сервера, на котором установлен продукт, внешний носитель с новой версией PT ISTI.
2. В главном меню выберите  → **Обновление экспертной базы PT ISTI**.
3. Выберите вкладку **Внешний диск** и нажмите **Проверить наличие пакета**.

PT ISIM проверит наличие и целостность deb-пакета на внешнем носителе. Если подходящий пакет обнаружен, номер версии PT ISTI отобразится в нижней части окна.

4. Нажмите **Установить**.

Начнется установка новой версии PT ISTI.

6.7.2. Обновление PT ISTI на узле PT ISIM View Sensor из КОНСОЛИ

Для обновления базы PT ISTI на узле PT ISIM View Sensor вы можете использовать файл `ptisti-package-<Версия продукта>.tgz` или `overview-repo-isti-<Версия продукта>.tar.gz`.

► Чтобы запустить обновление PT ISTI на узле PT ISIM View Sensor из консоли:

1. Скопируйте базу PT ISTI на сервер, на котором установлен PT ISIM View Sensor.
2. Распакуйте файл с базой PT ISTI и перейдите в распакованный каталог, выполнив одно из следующих действий:

- Если используете файл `ptisti-package-⟨Версия продукта⟩.tgz`, выполните команды:

```
tar xzvf ptisti-package-⟨Версия продукта⟩.tgz
cd ptisti-package-⟨Версия продукта⟩
```
 - Если используете файл `overview-repo-isti-⟨Версия продукта⟩.tar.gz`, выполните команды:

```
tar xzvf overview-repo-isti-⟨Версия продукта⟩.tar.gz
cd overview-repo-isti-⟨Версия продукта⟩
```
3. Запустите установочный скрипт:
- ```
sudo ./ptisim-install
```
- Начнется обновление базы PT ISTI.

### 6.7.3. Централизованное обновление базы PT ISTI с помощью Overview Center

Централизованное обновление базы PT ISTI на узлах View Sensor возможно после их подключения к PT ISIM Overview Center.

Для обновления базы PT ISTI на нижестоящих узлах View Sensor необходимо:

1. Загрузить обновление базы PT ISTI на сервер Overview Center одним из двух способов:
  - [подключив \(см. раздел 5.6.5.2\)](#) PT ISIM Overview Center к серверу обновлений Positive Technologies;
  - [вручную с помощью внешнего носителя \(см. раздел 6.7.3.1\)](#).

После этого запустится автоматическая выгрузка базы PT ISTI с Overview Center на серверы нижестоящих узлов View Sensor. Обновление передается, если оно относится к тому же варианту поставки, что и сам узел. После успешной выгрузки обновление будет доступно в интерфейсе PT ISIM Overview Center.

2. В PT ISIM Overview Center вручную запустить установку обновления базы PT ISTI на одном или нескольких узлах View Sensor. На узлах, для которых в PT ISIM Overview Center включено автообновление базы PT ISTI, установка будет запущена автоматически.

**Примечание.** Обновление базы PT ISTI не будет запущено для узлов, на которых идет [обновление \(см. раздел 6.2\)](#) самого узла PT ISIM. Необходимо дождаться завершения обновления узла и запустить обновление PT ISTI.

Просмотреть текущую версию и статус обновления базы PT ISTI на узлах PT ISIM в веб-интерфейсе Overview Center можно нажав в панели инструментов кнопку **Узлы ISIM** и выбрав в раскрывшемся меню пункт **Обновление PT ISTI**. История обновлений и описание версий PT ISTI отображается в карточке узла, которая открывается при выборе узла в списке.

Кроме того, информация о версии PT ISIM View Sensor и экспертной базы PT ISTI, а также о наличии обновлений доступна на вкладке **Об узле** при выборе узла в структуре узлов PT ISIM.

## В этом разделе

[Загрузка PT ISTI с помощью внешнего носителя \(см. раздел 6.7.3.1\)](#)

[Ручной запуск обновления PT ISTI на узлах View Sensor \(см. раздел 6.7.3.2\)](#)

[Настройка автоматического обновления PT ISTI на узлах View Sensor \(см. раздел 6.7.3.3\)](#)

### 6.7.3.1. Загрузка PT ISTI с помощью внешнего носителя

Если у вас отсутствует стабильное подключение к серверу обновлений Positive Technologies, вы можете загрузить PT ISTI с пакетом правил, выданным Positive Technologies, на узел Overview Center с помощью внешнего носителя. Вы также можете скопировать базу PT ISTI на Overview Center с помощью консольных утилит, например `wget` или `scp`.

► Чтобы загрузить PT ISTI с помощью внешнего носителя:

1. Вставьте в USB-порт сервера, на котором установлен PT ISIM Overview Center, внешний носитель с новой версией PT ISTI.
2. Скопируйте базу PT ISTI на сервер PT ISIM Overview Center.
3. Зарегистрируйте пакет с помощью команды:

```
/opt/ptisim-overview/bin/register_sensor_package.sh --path <Имя пакета>
```

Например, `/opt/ptisim-overview/bin/register_sensor_package.sh --path overview-repo-isti-proview-base.5.12.22191.2.tar.gz`

Запустится автоматическая выгрузка базы PT ISTI с Overview Center на серверы нижестоящих узлов View Sensor.

### 6.7.3.2. Ручной запуск обновления PT ISTI на узлах View Sensor

► Чтобы запустить обновление PT ISTI на узлах View Sensor вручную:

1. В панели инструментов нажмите кнопку **Узлы ISIM** и в раскрывшемся меню выберите пункт **Обновление PT ISTI**.

Откроется окно со списком доступных узлов. Для каждого узла будет указана версия PT ISTI и статус обновления.

2. Если вы хотите просмотреть список доступных обновлений для узла, ознакомиться с их описанием или историей обновлений, нажмите на строку с узлом.

Откроется карточка узла. Вы можете запустить установку любой из доступных версий базы PT ISTI на узле, нажав кнопку **Установить** в строке с версией.

3. Если требуется обновление до последней доступной версии, в окне **Обновление PT ISTI** выполните одно из следующих действий:

- Для запуска обновления на одном узле нажмите кнопку **Обновить** в строке с этим узлом.
- Для запуска обновления на всех узлах нажмите кнопку **Обновить все**.

### 6.7.3.3. Настройка автоматического обновления PT ISTI на узлах View Sensor

Обновление базы PT ISTI на узлах View Sensor может запускаться автоматически после загрузки базы PT ISTI на Overview Center и успешной его выгрузки с Overview Center на нижестоящие узлы View Sensor.

- Чтобы настроить автоматическое обновление базы PT ISTI на узлах View Sensor:
1. В панели инструментов нажмите **Узлы ISIM** → **Обновление PT ISTI**.  
Откроется окно со списком доступных узлов.
  2. Если требуется включить автообновление на всех узлах, в верхней части окна **Обновление PT ISTI** нажмите **Включить автообновление на всех узлах**.
  3. Если требуется включить автообновление только на нескольких узлах, настройте автообновление с помощью переключателей в строке каждого узла.

## 6.8. Обновление антивирусных баз и пакета экспертизы в PT ISIM Endpoint

Антивирусные базы и пакет экспертизы в PT ISIM Endpoint могут обновляться отдельно от обновления PT ISIM Endpoint.

Обновление пакета экспертизы содержит новые YARA-правила и хеш-суммы подозрительных файлов для модулей «YARA-сканер» и «Проверка файлов по хеш-сумме», использующихся в политиках «Обнаружение угроз» (Windows), «Обнаружение угроз» (Linux).

Передача обновлений антивирусных баз на конечные узлы выполняется с помощью модуля «Доставщик антивирусных баз».

**Примечание.** Обновление доступно при наличии [действующей лицензии](#) (см. раздел 5.4.4).

В PT ISIM Endpoint обновления скачиваются автоматически с сервера обновлений Positive Technologies. Проверка обновлений и их установка выполняются каждый час. Вы также можете запускать проверку и установку обновлений вручную.

### Запуск проверки и установки обновлений вручную

- Чтобы запустить проверку и установку обновлений антивирусных баз и пакета экспертизы вручную,
- на сервере с установленным PT ISIM Endpoint выполните команду `edr-update`.

Если обновление прошло успешно, в журнале контейнера последнее сообщение после обновления будет `done`. Вы можете проверить его с помощью команды `sudo docker logs modules.EDR-Application.EDR`.

## Просмотр версии экспертизы

Версия экспертизы отображается в веб-интерфейсе PT ISIM Endpoint на странице соответствующего модуля в составе политики рядом с версией самого модуля.

► Чтобы просмотреть версию экспертизы для модуля:

1. В главном меню выберите  **Политики**.
2. Выберите политику, в которую входит модуль.
3. На вкладке **Модули** выберите модуль.

Откроется страница модуля в составе политики. В поле **Экспертиза** будет отображен номер версии экспертизы.

Для антивирусных баз версия экспертизы отображается:

- в веб-интерфейсе PT ISIM Endpoint — на странице модуля «Доставщик антивирусных баз» в составе политики в поле **Экспертиза**;
- на конечных узлах Windows — при наведении курсора на значок агента в области уведомлений;
- на узлах Linux — в файле `/opt/vxagent/logs/agent.log`.

## 6.9. Изменение адреса сервера обновлений

Адрес сервера обновлений по умолчанию — [update.ptsecurity.com](https://update.ptsecurity.com). Если требуется, вы можете изменить его.

В этом разделе приведены инструкции для изменения адреса сервера обновлений на узлах PT ISIM View Sensor (для получения обновлений экспертной базы PT ISTI) и на узлах PT ISIM Overview Center (для получения обновлений подключенных PT ISIM View Sensor и экспертной базы PT ISTI на них).

### На узле PT ISIM View Sensor

► Чтобы изменить адрес сервера обновлений на узле PT ISIM View Sensor:

1. Откройте файл `/etc/environment`.
2. В переменной окружения `FLUS_WEB_PROTOCOL` укажите протокол для доступа к серверу обновлений:

`FLUS_WEB_PROTOCOL="http"` или `FLUS_WEB_PROTOCOL="https"`

3. В переменной окружения FLUS\_ADDR укажите новый адрес сервера обновлений. Например:

```
FLUS_ADDR="new-update-server-address.ru"
```

4. Сохраните изменения и закройте файл.

5. Перезапустите службу ptisim-httpapi:

```
systemctl restart ptisim-httpapi.service
```

## На узле PT ISIM Overview Center

- ▶ Чтобы изменить адрес сервера обновлений на узле PT ISIM Overview Center:

1. Откройте файл `/etc/environment`.

2. В переменной окружения FLUS\_URL укажите новый адрес сервера обновлений полностью. Например:

```
FLUS_URL="https://new-update-server-address.ru"
```

3. Сохраните изменения и закройте файл.

4. Перезапустите PT ISIM Overview Center:

```
systemctl restart ptisim-overview-server.service
```

## 7. Администрирование PT ISIM

В этом разделе содержатся инструкции по администрированию компонентов PT ISIM.

### В этом разделе

[Администрирование PT ISIM View Sensor \(см. раздел 7.1\)](#)

[Администрирование PT ISIM Endpoint \(см. раздел 7.2\)](#)

[Администрирование PT ISIM Collector \(см. раздел 7.3\)](#)

[Администрирование PT ISIM Overview Center \(см. раздел 7.4\)](#)

[Администрирование PT ISIM Industrial Tablet \(см. раздел 7.5\)](#)

### 7.1. Администрирование PT ISIM View Sensor

В этом разделе содержатся инструкции по администрированию PT ISIM View Sensor.

#### В этом разделе

[Управление учетными записями пользователей в PT ISIM View Sensor \(см. раздел 7.1.1\)](#)

[Подключение к PT MC \(см. раздел 7.1.2\)](#)

[Настройка ротации данных \(см. раздел 7.1.3\)](#)

[Настройка параметров хранения PCAP \(см. раздел 7.1.4\)](#)

[Настройка интеграции с MaxPatrol VM \(см. раздел 7.1.5\)](#)

[Настройка работы с syslog-сервером \(см. раздел 7.1.6\)](#)

[Настройка почтовых уведомлений об инцидентах \(см. раздел 7.1.7\)](#)

[Изменение информации о системе и контактном лице \(см. раздел 7.1.8\)](#)

[Включение и отключение оценки уязвимостей \(см. раздел 7.1.9\)](#)

[Создание пакета регистрации PT ISIM View Sensor для подключения к PT ISIM Overview Center \(см. раздел 7.1.10\)](#)

[Отключение извлечения файлов из трафика \(см. раздел 7.1.11\)](#)

[Настройка интеграции с PT Sandbox для проверки файлов \(см. раздел 7.1.12\)](#)

[Настройка приема данных от PT ISIM Endpoint \(см. раздел 7.1.13\)](#)

[Диагностика состояния PT ISIM View Sensor \(см. раздел 7.1.14\)](#)

[Мониторинг использования ресурсов \(см. раздел 7.1.15\)](#)

[Контроль целостности файлов \(см. раздел 7.1.16\)](#)

[Замена SSL-сертификата \(см. раздел 7.1.17\)](#)

[Настройка ERSPAN-приемника \(см. раздел 7.1.18\)](#)

[Миграция данных модели сети в ручном режиме \(см. раздел 7.1.19\)](#)

[Удаление неиспользуемых файлов модели сети \(см. раздел 7.1.20\)](#)

[Проверка целостности цифровой подстанции по стандарту МЭК-61850 \(см. раздел 7.1.21\)](#)

[Экспорт и импорт конфигурации PT ISIM \(см. раздел 7.1.22\)](#)

[Импорт внешнего проекта \(см. раздел 7.1.23\)](#)

[Работа с пользовательскими правилами межсетевого экрана \(см. раздел 7.1.24\)](#)

[Утилита iptablesctl \(см. раздел 7.1.25\)](#)

[Утилита ISIMCTL \(см. раздел 7.1.26\)](#)

## 7.1.1. Управление учетными записями пользователей в PT ISIM View Sensor

Максимальная длительность сессии пользователя определяется параметрами конфигурации продукта. По истечении этого периода выполняется принудительная деавторизация пользователя, после которой для входа в продукт необходимо заново ввести учетные данные.

**Примечание.** Если пользователь, который был авторизован через PT MC, выйдет из PT ISIM View Sensor, будет выполнен выход из PT MC, а также всех подключенных к нему продуктов в пределах одного браузера.

Когда администратор меняет права доступа или блокирует пользователя, изменения применяются не сразу, а спустя время, определяемое параметрами конфигурации продукта. Кроме того, изменения применяются при обновлении пользователем страницы в браузере.

Таблица 27. Параметры продолжительности сессии, обновления прав доступа и блокировки пользователя

| Параметр                                                                                                         | Локальный пользо-<br>ватель | Пользователь PT MC |
|------------------------------------------------------------------------------------------------------------------|-----------------------------|--------------------|
|                                                                                                                  | Значение                    |                    |
| Длительность сессии пользователя                                                                                 | 14 дней                     |                    |
| Интервал, в течение которого обновляются права доступа пользователя при внесении в них изменений администратором | 30 минут                    | 30 минут           |
| Интервал, в течение которого пользователь будет заблокирован при его блокировке администратором                  | 30 минут                    | 30 минут           |

Далее приводятся инструкции по управлению локальными учетными записями пользователей. Управление учетными записями пользователей, используемыми при входе в PT ISIM View Sensor через PT MC, осуществляется в PT MC.

## В этом разделе

[О ролях пользователей \(см. раздел 7.1.1.1\)](#)

[Создание учетной записи пользователя \(см. раздел 7.1.1.2\)](#)

[Изменение учетной записи пользователя \(см. раздел 7.1.1.3\)](#)

[Распечатка данных учетной записи \(см. раздел 7.1.1.4\)](#)

[Просмотр и выгрузка журнала действий пользователей \(см. раздел 7.1.1.5\)](#)

[Блокировка учетной записи пользователя \(см. раздел 7.1.1.6\)](#)

[Настройка временной блокировки пользователя при авторизации \(см. раздел 7.1.1.7\)](#)

### 7.1.1.1. О ролях пользователей

В PT ISIM View Sensor используется ролевая модель управления доступом. Пользователь в PT ISIM View Sensor может иметь одну из следующих ролей: оператор, специалист по безопасности, администратор.

Таблица 28. Роли пользователей и доступные функции

| Объект     | Оператор                                           | Специалист по безопасности                                                                                                       | Администратор |
|------------|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|---------------|
|            | Доступные функции                                  |                                                                                                                                  |               |
| Статистика | Просмотр статистики, изменение периода отображения |                                                                                                                                  |               |
| Инциденты  | Просмотр, фильтрация инцидентов                    |                                                                                                                                  |               |
|            | Выгрузка данных инцидента                          |                                                                                                                                  |               |
|            | Просмотр цепочек инцидентов                        |                                                                                                                                  |               |
|            | —                                                  | Изменение параметров инцидента, создание и изменение цепочки инцидентов                                                          |               |
|            | —                                                  | Перенос одной цепочки в другую, перенос инцидентов из одной цепочки в другую, удаление инцидента из цепочки, объединение цепочек |               |
|            | Выгрузка CSV-файла со списком инцидентов           |                                                                                                                                  |               |
| Уязвимости | Просмотр, фильтрация, группировка уязвимостей      |                                                                                                                                  |               |
|            | Выгрузка списка уязвимостей в формате CSV          |                                                                                                                                  |               |

| Объект                           | Оператор                                                                                      | Специалист по безопасности                                                                                                                                               | Администратор |
|----------------------------------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
|                                  | Доступные функции                                                                             |                                                                                                                                                                          |               |
| Сеть                             | Просмотр схемы групп узлов, контейнеров и соединений между ними                               |                                                                                                                                                                          |               |
|                                  | Просмотр групп, соединений, узлов и объектов конфигурации узлов                               |                                                                                                                                                                          |               |
|                                  | Фильтрация соединений, узлов и объектов конфигурации узлов                                    |                                                                                                                                                                          |               |
|                                  | Выгрузка списка узлов и списка объектов конфигурации узлов с данными из таблицы в формате CSV |                                                                                                                                                                          |               |
|                                  | Выгрузка списка соединений в формате CSV                                                      |                                                                                                                                                                          |               |
|                                  | Выгрузка копии трафика по соединению в формате PCAP                                           |                                                                                                                                                                          |               |
|                                  | —                                                                                             | Изменение параметров узлов, авторизация, деавторизация узлов, разрешение соединений, перенос интерфейса в другой узел, удаление интерфейса, объединение и удаление узлов |               |
|                                  | —                                                                                             | Создание узла на основе сетевого интерфейса                                                                                                                              |               |
|                                  | —                                                                                             | Создание и удаление группы, контейнера                                                                                                                                   |               |
|                                  | —                                                                                             | Добавление узла в группу, исключение узла из группы                                                                                                                      |               |
|                                  | —                                                                                             | Изменение параметров групп и контейнеров (в том числе их положения на схеме сети)                                                                                        |               |
|                                  | —                                                                                             | Выгрузка списка узлов для импорта в формате CSV и импорт списка узлов                                                                                                    |               |
| События (кроме microView Sensor) | Просмотр, фильтрация, группировка событий                                                     |                                                                                                                                                                          |               |
|                                  | Выгрузка списка событий в формате CSV                                                         |                                                                                                                                                                          |               |
|                                  | Выгрузка файлов, переданных в рамках событий                                                  |                                                                                                                                                                          |               |
| Технологические сигналы          | Просмотр, фильтрация технологических сигналов                                                 |                                                                                                                                                                          |               |
|                                  | —                                                                                             | Создание, изменение параметров и удаление технологических сигналов                                                                                                       |               |
|                                  | —                                                                                             | Изменение статусов технологических сигналов и операций чтения и записи сигналов                                                                                          |               |
| Разрешения                       | Просмотр списков разрешений                                                                   |                                                                                                                                                                          |               |
|                                  | Создание резервной копии списка                                                               |                                                                                                                                                                          |               |
|                                  | —                                                                                             | Создание, изменение и удаление списков                                                                                                                                   |               |

| Объект                   | Оператор                                          | Специалист по безопасности                                                                       | Администратор |
|--------------------------|---------------------------------------------------|--------------------------------------------------------------------------------------------------|---------------|
|                          | Доступные функции                                 |                                                                                                  |               |
|                          | —                                                 | Создание, изменение и удаление разрешений                                                        |               |
|                          | —                                                 | Перенос разрешений в другой список                                                               |               |
|                          | —                                                 | Восстановление резервной копии списка                                                            |               |
| Правила обнаружения атак | Просмотр, фильтрация правил обнаружения атак      |                                                                                                  |               |
|                          | —                                                 | Создание, изменение, удаление правил обнаружения атак                                            |               |
|                          | —                                                 | Включение и отключение правил обнаружения атак                                                   |               |
|                          | —                                                 | Добавление, изменение и удаление исключений                                                      |               |
| Система                  | Изменение языка веб-интерфейса                    |                                                                                                  |               |
|                          | Выполнение диагностики                            |                                                                                                  |               |
|                          | Просмотр состояния режимов обучения               |                                                                                                  |               |
|                          | —                                                 | Включение, отключение режимов обучения                                                           |               |
|                          | —                                                 | Управление отслеживанием нарушений                                                               |               |
|                          | —                                                 | Создание пакета регистрации                                                                      |               |
|                          | —                                                 | Изменение информации о системе (названия узла View Sensor, геолокации и данных контактного лица) |               |
|                          | —                                                 | Управление учетными записями пользователей                                                       |               |
|                          | —                                                 | Просмотр и выгрузка журнала действий пользователей                                               |               |
|                          | Скачивание копии трафика за период в формате PCAP |                                                                                                  |               |
|                          | —                                                 | Изменение параметров хранения PCAP-файлов                                                        |               |

| Объект | Оператор                                   | Специалист по безопасности | Администратор                                                                               |
|--------|--------------------------------------------|----------------------------|---------------------------------------------------------------------------------------------|
|        | Доступные функции                          |                            |                                                                                             |
|        | —                                          |                            | Настройка подключения к PT MC                                                               |
|        | —                                          |                            | Включение и отключение извлечения файлов из трафика                                         |
|        | —                                          |                            | Настройка дискового пространства для ротации данных                                         |
|        | —                                          |                            | Включение и отключение передачи файлов на проверку в PT Sandbox                             |
|        | —                                          |                            | Настройка отправки результатов сканирования в MaxPatrol VM                                  |
|        | —                                          |                            | Настройка интеграции с syslog-сервером, настройка хранения данных                           |
|        | —                                          |                            | Настройка почтовых уведомлений                                                              |
|        | —                                          |                            | Обновление экспертной базы PT ISTI                                                          |
|        | —                                          |                            | Экспорт и импорт конфигурации PT ISIM                                                       |
|        | —                                          |                            | Импорт внешнего проекта                                                                     |
|        | Просмотр добавленных в PT ISIM коллекторов |                            |                                                                                             |
|        | —                                          |                            | Включение приема данных от коллекторов, добавление, изменение, скачивание конфигурации, об- |

| Объект | Оператор                                                                                                                  | Специалист по безопасности                                                        | Администратор                                    |
|--------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------|
|        | Доступные функции                                                                                                         |                                                                                   |                                                  |
|        |                                                                                                                           |                                                                                   | новление секретных ключей и удаление коллекторов |
|        | —                                                                                                                         |                                                                                   | Мониторинг использования ресурсов                |
|        | —                                                                                                                         |                                                                                   | Включение и отключение оценки уязвимостей        |
|        | Работа с представлениями для фильтрации, сортировки, группировки и отображения данных                                     |                                                                                   |                                                  |
|        | Просмотр задач на сбор данных, в том числе их статусов и результатов запуска; просмотр и скачивание журналов сбора данных |                                                                                   |                                                  |
|        | —                                                                                                                         | Создание, изменение параметров, запуск и остановка, удаление задач на сбор данных |                                                  |
|        | Профиль пользователя                                                                                                      | Смена пароля, адреса электронной почты                                            |                                                  |
|        | Подписка на уведомления об инцидентах                                                                                     |                                                                                   |                                                  |

### 7.1.1.2. Создание учетной записи пользователя

Для предоставления пользователю доступа к веб-интерфейсу PT ISIM View Sensor требуется создать учетную запись пользователя. Впоследствии вы можете [заблокировать](#) (см. раздел 7.1.1.6), но не удалить учетную запись.

► Чтобы создать учетную запись пользователя:

1. В главном меню выберите  → **Управление пользователями**.
2. Нажмите **Добавить пользователя**.

Создать нового пользователя

Логин

operator

Роль

Оператор

Пароль

\*\*\*\*\*

Сгенерировать Копировать в буфер обмена

Имя

Иван Иванов

Почта

user@example.org

Активен ☒

Распечатать Сохранить Отмена

Рисунок 48. Создание учетной записи пользователя

3. Введите логин учетной записи.
4. В раскрывающемся списке **Роль** выберите роль пользователя.
5. Нажмите **Сгенерировать**, чтобы сгенерировать пароль учетной записи.
6. Введите имя пользователя.
7. Введите адрес электронной почты.

8. Активируйте учетную запись с помощью переключателя **Активен**.

9. Нажмите **Сохранить**.

### 7.1.1.3. Изменение учетной записи пользователя

► Чтобы изменить учетную запись пользователя:

1. В главном меню выберите  → **Управление пользователями**.
2. Выберите учетную запись.
3. В открывшейся карточке учетной записи нажмите  **Изменить**.
4. Внесите изменения.
5. Нажмите **Сохранить**.

### 7.1.1.4. Распечатка данных учетной записи

Чтобы предоставить пользователю логин и пароль для доступа к веб-интерфейсу продукта, вы можете распечатать данные учетной записи.

**Внимание!** Распечатка данных учетной записи доступна непосредственно после генерации пароля. Если вы закроете карточку учетной записи, распечатать данные не получится.

► Чтобы распечатать данные учетной записи:

1. В главном меню выберите  → **Управление пользователями**.
2. Выберите учетную запись.
3. В открывшейся карточке учетной записи нажмите  **Изменить**.
4. Нажмите **Сгенерировать** для формирования нового пароля учетной записи.
5. Нажмите **Распечатать**.

### 7.1.1.5. Просмотр и выгрузка журнала действий пользователей

Журнал действий пользователей позволяет отслеживать историю журналируемых действий, совершенных локальными пользователями и пользователями PT MC в веб-интерфейсе PT ISIM View Sensor, в том числе неуспешных операций. Вы можете выгрузить историю действий пользователей в виде CSV-файла. Выгружаемый файл может содержать записи обо всех действиях всех пользователей либо только о действиях, отфильтрованных и отсортированных по выбранным параметрам.

► Чтобы просмотреть журнал действий пользователей:

1. В главном меню выберите  → **Журнал действий пользователей**.  
Откроется история действий всех пользователей PT ISIM View Sensor.
  2. Если требуется, отфильтруйте действия пользователей по одному или нескольким значениям в столбцах таблицы.
  3. Если требуется выгрузить историю действий, нажмите .
- Начнется скачивание CSV-файла.

**Примечание.** Кириллические символы CSV-файла могут некорректно отображаться в Microsoft Excel. В этом случае потребуется переоткрыть файл и указать кодировку UTF-8. Для этого в Microsoft Excel на вкладке **Данные** → **Получить данные** нажмите кнопку **Из текстового/CSV-файла**, выберите CSV-файл и в открывшемся окне в раскрывающемся списке **Источник файла** выберите **UTF-8** и нажмите кнопку **Загрузить**.

### 7.1.1.6. Блокировка учетной записи пользователя

Вы можете заблокировать учетную запись пользователя. Если в момент блокировки пользователь работал в веб-интерфейсе, его сессия в браузере будет завершена.

**Примечание.** Вы не можете заблокировать собственную учетную запись.

► Чтобы заблокировать учетную запись пользователя:

1. В главном меню выберите  → **Управление пользователями**.
  2. Выберите учетную запись.
  3. В открывшейся карточке учетной записи нажмите  **Изменить**.
  4. Заблокируйте учетную запись с помощью переключателя **Активен**.
- Учетная запись заблокирована.

### 7.1.1.7. Настройка временной блокировки пользователя при авторизации

Если превышено допустимое количество попыток авторизации, IP-адрес, с которого выполняется вход в PT ISIM View Sensor, временно блокируется. По умолчанию допустимое количество попыток авторизации — 5, длительность блокировки IP-адреса пользователя — 300 секунд.

► Чтобы настроить параметры временной блокировки при авторизации:

1. Откройте файл `/etc/fail2ban/jail.d/system-failed-http-login.conf`, расположенный на сервере с PT ISIM View Sensor.
2. В секции `system-failed-http-login` в параметре `maxretry` введите допустимое количество попыток авторизации пользователя.
3. В секции `system-failed-http-login` в параметре `bantime` введите длительность блокировки в секундах.
4. Перезапустите сервис:  

```
systemctl restart fail2ban
```

Временная блокировка пользователя при авторизации настроена.

## 7.1.2. Подключение к PT MC

Positive Technologies Management and Configuration (далее также — PT MC) — приложение, которое позволяет использовать технологию единого входа для продуктов Positive Technologies. Учетные записи пользователей и роли, созданные в PT MC, синхронизируются с продуктом при его подключении к PT MC и становятся доступными для входа в продукт через PT MC.

Переключение между веб-интерфейсами подключенных к PT MC приложений доступно по кнопке  в главном меню каждого приложения.

Подробная информация о PT MC представлена [в справке к продукту](#). Поддерживаемые версии PT MC указаны [в программных требованиях \(см. раздел 3.2\)](#).

Для подключения PT ISIM View Sensor к PT MC нужно:

1. [Установить \(см. раздел 7.1.2.1\)](#) на сенсоре SSL-сертификат, предоставляемый PT MC.
2. [Настроить подключение \(см. раздел 7.1.2.2\)](#) к PT MC в веб-интерфейсе PT ISIM View Sensor.

### В этом разделе

[Установка доверенного SSL-сертификата \(см. раздел 7.1.2.1\)](#)

[Настройка подключения PT ISIM View Sensor к PT MC \(см. раздел 7.1.2.2\)](#)

### 7.1.2.1. Установка доверенного SSL-сертификата

► Чтобы установить доверенный SSL-сертификат в PT ISIM View Sensor:

1. Скопируйте файл SSL-сертификата `/usr/local/share/ca-certificates/deployerCA.crt`, расположенный на сервере PT MC, в домашний каталог на сервере PT ISIM View Sensor.
2. Перенесите файл сертификата из домашнего каталога в каталог для хранения сертификатов:  

```
sudo mv deployerCA.crt /usr/local/share/ca-certificates/deployerCA.crt
```
3. Выполните команду:  

```
sudo update-ca-certificates
```

При обновлении PT ISIM View Sensor повторная установка доверенного SSL-сертификата не требуется.

### 7.1.2.2. Настройка подключения PT ISIM View Sensor к PT MC

**Внимание!** На сервере PT ISIM View Sensor должен быть [установлен \(см. раздел 7.1.2.1\)](#) SSL-сертификат, предоставляемый PT MC.

**Внимание!** Если требуется повторно подключить PT ISIM View Sensor к PT MC (после отключения от PT MC или изменения параметров подключения), до выполнения инструкции ниже нужно войти в веб-интерфейс PT MC и удалить приложение, соответствующее подключенному ранее PT ISIM View Sensor.

► Чтобы настроить подключение PT ISIM View Sensor к PT MC:

1. Войдите в веб-интерфейс PT ISIM View Sensor с локальной учетной записью пользователя.
2. В главном меню выберите  → **Подключение к PT MC**.
3. В поле **IP-адрес или URL PT ISIM** введите адрес PT ISIM View Sensor, подключаемого к PT MC.

**Примечание.** Название приложения в PT MC соответствует имени узла PT ISIM View Sensor.

4. В поле **IP-адрес или FQDN PT MC** введите адрес PT MC, к которому необходимо подключиться.
5. В поле **Порт PT MC** введите порт для подключения к PT MC.

По умолчанию для подключения к PT MC используется порт 3334.

**Примечание.** Соединения по указанному порту в цепочках INPUT и OUTPUT будут автоматически разрешены в правилах фильтрации после успешного подключения к PT MC. При отключении от PT MC созданные правила удаляются.

6. Нажмите **Подключиться**.

Подключение может занять некоторое время. В PT MC будет зарегистрировано приложение PT ISIM View Sensor.

Статус подключения к PT MC отображается в окне **Подключение к PT MC**.

Если требуется, вы можете отключить PT ISIM View Sensor от PT MC, нажав **Отключиться**. После отключения пользователи PT MC не смогут работать в PT ISIM View Sensor.

### 7.1.3. Настройка ротации данных

Для обеспечения работоспособности PT ISIM служба watchdog поддерживает на сервере определенный объем свободного дискового пространства, поэтапно удаляя данные. Этапы и критерии удаления данных по умолчанию заданы в конфигурационном файле `/opt/ptisim/etc/watchdog.yaml` в секции `steps`. После каждого этапа удаления служба watchdog проверяет объем свободного дискового пространства и, если он меньше указанного значения (20% по умолчанию), переходит к следующему этапу.

**Примечание.** Интервал проверки дискового пространства по умолчанию равен 10 минутам и настраивается в файле `/usr/lib/systemd/system/ptisim-disk-cleaner.timer`.

**Примечание.** Ротация PCAP-файлов выполняется службой `ptisim-peony` и зависит от параметров хранения PCAP (см. раздел 7.1.4).

В веб-интерфейсе PT ISIM вы можете задать минимальный объем свободного дискового пространства, а также период хранения событий, после которого их можно удалять. Настроенные таким образом критерии будут считаться приоритетными по отношению к этапам, указанным по умолчанию в конфигурационном файле, — с них watchdog будет начинать удаление при нехватке минимального свободного объема. Однако, если удаления данных согласно этим критериям будет недостаточно для поддержания минимального свободного объема, watchdog продолжит удалять данные согласно этапам, указанным в конфигурационном файле, пока объем свободного дискового пространства не достигнет указанного значения.

► Чтобы изменить параметры ротации данных:

1. В главном меню выберите  → **Настройка дискового пространства**.
2. Выберите минимальный объем свободного дискового пространства.
3. Выберите период хранения событий, после истечения которого их можно удалять для поддержания объема свободного дискового пространства.
4. Нажмите **Сохранить**.

## См. также

[Настройка параметров хранения PCAP \(см. раздел 7.1.4\)](#)

## 7.1.4. Настройка параметров хранения PCAP

Вы можете настроить хранение копии трафика:

- изменить каталог для хранения копии трафика (по умолчанию копия трафика в виде PCAP-файлов сохраняется в каталоге `/opt/ptisim/data/peony/pcapdb`);

**Внимание!** Перед изменением каталога необходимо активировать [лицензию](#) (см. раздел 5.3.5.2).

**Внимание!** После изменения каталога ранее сохраненные PCAP-файлы будут недоступны для скачивания в веб-интерфейсе PT ISIM View Sensor.

- задать максимальный объем, который могут занимать PCAP-файлы на диске.

Если требуется изменить каталог для хранения PCAP-файлов, нужно:

1. Создать новый каталог:  
`sudo mkdir -p <Путь к каталогу>`
2. Предоставить права доступа к каталогу пользователю `ptisim`:  
`sudo chown -R ptisim:ptisim <Путь к каталогу>`  
`sudo chmod 2754 <Путь к каталогу>`
3. В веб-интерфейсе PT ISIM View Sensor указать новый каталог в параметрах хранения копии трафика по инструкции ниже.

► Чтобы настроить хранение копии трафика:

1. В главном меню выберите  → **Скачать PCAP**.
2. Нажмите **Изменить параметры хранения**.
3. Если требуется изменить каталог для хранения копии трафика, введите путь к новому каталогу.
4. Если требуется, отключите удаление файлов из прежнего каталога.

**Примечание.** Возможность управлять удалением файлов появляется после ввода пути к каталогу.

5. Введите максимальный объем, который могут занимать PCAP-файлы на диске.

**Примечание.** Рекомендуется выделять не больше 50% объема общего раздела с данными системы или использовать отдельный раздел для хранения PCAP-файлов.

**Примечание.** Если для записи очередного PCAP-файла не хватит места в пределах выделенного максимального объема, будет запущена ротация PCAP-файлов: дисковое пространство для записи новых файлов будет освобождено за счет удаления старых PCAP-файлов. Кроме того, при уменьшении свободного места на диске до 20%

(значение по умолчанию) от общего объема диска за вычетом значения, указанного в поле **Максимальный объем**, будет запущена [ротация других данных \(см. раздел 7.1.3\)](#) и продолжится, пока свободное место не достигнет 40% (значение по умолчанию) от указанного объема.

#### 6. Нажмите **Сохранить**.

После подачи трафика вы можете проверить наличие сохраненных PCAP-файлов в новом каталоге, выбрав в главном меню  → **Скачать PCAP** и просмотрев список доступных PCAP-файлов.

## 7.1.5. Настройка интеграции с MaxPatrol VM

Positive Technologies MaxPatrol VM (MaxPatrol VM) обеспечивает комплексное управление уязвимостями в ИТ-инфраструктуре предприятия и позволяет автоматизировать управление активами, анализ защищенности активов ИБ и приоритизацию и проверку устранения уязвимостей на активах ИБ. Поддерживаемые версии MaxPatrol VM указаны [в программных требованиях \(см. раздел 3.2\)](#).

Уязвимости определяются на основе данных о конфигурации узлов, полученных в результате их сканирования в режиме аудита. Вы можете настроить интеграцию с MaxPatrol VM для отправки в MaxPatrol VM результатов сканирования (сканов) из PT ISIM View Sensor. Для этого нужно:

- в PT MC, связанном с MaxPatrol VM, создать токен доступа;
- в PT ISIM View Sensor настроить отправку результатов сканирования в MaxPatrol VM.

### Создание токена доступа

► Чтобы создать токен доступа:

1. В главном меню MaxPatrol VM перейдите в приложение PT MC.
2. В главном меню PT MC выберите  → **Токены доступа**.
3. Нажмите **Создать**.
4. Введите название токена.
5. Выберите приложение MaxPatrol VM.
6. Нажмите **Создать**.

**Примечание.** Вы можете создать не более 100 токенов. Список всех созданных токенов пользователя доступен на странице **Токены доступа**.

7. Сохраните токен, чтобы он был доступен только вам.

**Внимание!** Скопируйте и сохраните токен сразу: после перехода на другую страницу скопировать созданный токен будет невозможно. Потребуется создавать новый.

Вы также можете изменить токен доступа по кнопке  и удалить токен доступа по кнопке .

**Внимание!** Если в ответ на запрос к API сервис возвращает ошибку 500 (Internal Server Error), необходимо назначить пользователю дополнительную роль приложения PT MC и создать новый токен доступа. Вы можете назначить роль **Пользователь** или создать новую роль с минимальными привилегиями.

## Настройка отправки результатов сканирования в MaxPatrol VM

► Чтобы настроить отправку результатов сканирования в MaxPatrol VM:

1. В главном меню PT ISIM View Sensor выберите  → **Отправка результатов сканирования в MaxPatrol VM**.
2. Включите отправку результатов сканирования в MaxPatrol VM.
3. Введите IP-адрес или FQDN MaxPatrol VM.
4. Введите порт MaxPatrol VM.

**Примечание.** По умолчанию для подключения к MaxPatrol VM используется порт 443.

5. Введите токен доступа, созданный в PT MC.
6. Нажмите **Сохранить**.

PT ISIM View Sensor будет передавать результаты сканирования, полученные после включения отправки, в виде запросов типа PUT к API MaxPatrol VM с данными сырого скана. Если запрос не удалось отправить, попытка отправки запроса повторится через некоторое время (по умолчанию — 5 минут) до достижения максимального количества попыток (по умолчанию — 3).

Вы можете проверить подключение к API MaxPatrol VM по кнопке **Проверить соединение**.

**Примечание.** Результаты сканирования, полученные в PT ISIM View Sensor до настройки интеграции, в MaxPatrol VM не передаются.

Включение и отключение отправки результатов сканирования в MaxPatrol VM, а также изменение параметров подключения фиксируется [в истории действий пользователей \(см. раздел 7.1.1.5\)](#).

### 7.1.6. Настройка работы с syslog-сервером

В этом разделе содержатся инструкции для настройки отправки сообщений о событиях и инцидентах на syslog-сервер, а также об их приемке.

#### В этом разделе

[Настройка отправки сообщений об инцидентах в syslog \(см. раздел 7.1.6.1\)](#)

[Настройка приемки сообщений об инцидентах на удаленном syslog-сервере \(см. раздел 7.1.6.2\)](#)

[Настройка отправки сообщений о событиях на локальный syslog-сервер \(см. раздел 7.1.6.3\)](#)

[Настройка отправки сообщений о событиях на удаленный syslog-сервер \(см. раздел 7.1.6.4\)](#)

## 7.1.6.1. Настройка отправки сообщений об инцидентах в syslog

PT ISIM View Sensor может выступать в качестве источника сообщений о новых инцидентах для syslog-сервера. Для этого вам нужно указать адрес и порт syslog-сервера, на который PT ISIM View Sensor будет отправлять сообщения, и выбрать транспортный протокол для передачи сообщений.

Сообщения об инцидентах содержат уровень опасности инцидента и имеют следующий формат:

```
<Узел — отправитель сообщений> : <Дата инцидента>:[Уровень опасности инцидента]:Created <Идентификатор инцидента> <Название инцидента> incident at step <Текущий этап инцидента> <Ссылка на инцидент в веб-интерфейсе> <Статус инцидента> <Время начала инцидента> <IP-адрес источника инцидента> <MAC-адрес источника инцидента> <IP-адрес цели инцидента> <MAC-адрес цели инцидента> <Группа инцидентов> <Название узла View Sensor> <Время обновления инцидента> <Тип инцидента>
```

Например:

```
10.0.2.8 : 2021-11-24T08:48:11Z:[high]:Created `1171` `WannaCry activity detected` incident at step 1/1 `[https://10.0.2.8/#/incidents?id=1171]` `Open` `2021-11-24T08:48:00Z` `192.168.71.40` `00:0c:29:ed:d2:40` `192.168.71.1` `00:50:56:c0:00:01` `Attack` `ISIM Sensor` `2021-11-24T08:48:03Z` `Snort_WCry_Ransomware_Termination_URL_Call`
```

**Примечание.** Вы можете изменять текст и набор полей в syslog-сообщении с помощью [специальных шаблонов \(см. приложение Б\)](#). Для применения изменений в шаблонах потребуется перезапустить службу ptisim-httpapi командой `systemctl restart ptisim-httpapi`.

Вы можете отправлять сообщения об инцидентах в MaxPatrol SIEM, в этом случае в качестве syslog-сервера может выступать узел MP 10 Collector. Со стороны MaxPatrol SIEM необходимо создать и запустить задачу на сбор событий, подробности описаны в разделе «Системы SIEM. Сбор событий» в Справочнике по настройке источников MaxPatrol SIEM. Поддерживаемые версии продукта указаны в [программных требованиях \(см. раздел 3.2\)](#).

► Чтобы настроить отправку сообщений об инцидентах в syslog:

1. В главном меню выберите  → **Отправка сообщений об инцидентах в syslog**.
2. Включите отправку сообщений.

3. В блоке параметров **Syslog-сервер** введите IP-адрес или доменное имя, укажите порт syslog-сервера, а также выберите транспортный протокол для передачи сообщений (TCP или UDP).

Для проверки корректности указанных параметров вы можете нажать кнопку **Отправить тестовое сообщение**, предварительно сохранив параметры. В результате на указанный сервер будет отправлено тестовое сообщение Настройка пользовательских уведомлений.

**Примечание.** Для порта, указанного в параметрах подключения, будут автоматически созданы разрешения в цепочках INPUT и OUTPUT правил фильтрации. По умолчанию используется порт 514. При отключении отправки сообщений в syslog созданные правила удаляются.

4. Нажмите кнопку **Сохранить**.

Отправка сообщений об инцидентах в syslog настроена.

На стороне syslog-сервера требуется также [настроить приемку сообщений](#) (см. раздел 7.1.6.2) от PT ISIM View Sensor.

## 7.1.6.2. Настройка приемки сообщений об инцидентах на удаленном syslog-сервере

На удаленном syslog-сервере может использоваться служба rsyslog или syslog-ng.

- Чтобы настроить приемку сообщений об инцидентах в службе rsyslog:

1. Откройте файл `/etc/rsyslog.conf`.
2. Если требуется получать сообщения по протоколу UDP, в секции `Modules` раскомментируйте строки:

```
#module(load="imudp")
#input(type="imudp" port="514")
```

3. Если требуется получать сообщения по протоколу TCP, в секции `Modules` раскомментируйте строки:

```
#module(load="imtcp")
#input(type="imtcp" port="514")
```

Указываемый порт (514 по умолчанию) должен совпадать с портом, указанным в параметрах syslog в веб-интерфейсе PT ISIM.

4. Перезапустите службу rsyslog:  
`sudo systemctl restart rsyslog`

► Чтобы настроить приемку сообщений об инцидентах в службе syslog-ng:

1. В каталоге `/etc/syslog-ng/conf.d/` создайте конфигурационный файл `10_events.conf`.
2. Откройте файл `10_events.conf`.
3. Если требуется получать сообщения по протоколу UDP, добавьте в файл следующие строки:

```
source s_net { udp(ip(<IP-адрес syslog-сервера>) port(514)); };
log { source(s_net); destination(d_syslog); };
```

4. Если требуется получать сообщения по протоколу TCP, добавьте в файл следующие строки:

```
source s_net { tcp(ip(<IP-адрес syslog-сервера>) port(514)); };
log { source(s_net); destination(d_syslog); };
```

Указываемый порт (514 по умолчанию) должен совпадать с портом, указанным в параметрах syslog в веб-интерфейсе PT ISIM.

5. Перезапустите службу syslog-ng:

```
sudo systemctl restart syslog-ng
```

### 7.1.6.3. Настройка отправки сообщений о событиях на локальный syslog-сервер

Вы можете настроить отправку сообщений о новых событиях на локальный syslog-сервер.

**Внимание!** После обновления PT ISIM необходимо заново настроить отправку сообщений о событиях на syslog-сервер.

Сообщения о событиях имеют следующий формат:

```
<Время сообщения> <Имя узла> ISIM: @cee {"msg":{<Все атрибуты события>}, <Атрибуты, заданные пользователем>}
```

Атрибуты событий передаются в syslog-сообщении после маркера @cee. Атрибуты могут быть переданы в виде нормализованного события (то есть списка всех атрибутов в формате JSON или в формате gzip, закодированного в Base64) или списка отдельных атрибутов (вы можете указать атрибуты события и задать им собственные названия для syslog, например отображать в syslog поле `Network.Ipv4.TCPv4.dst_port` в виде поля `dst.port`).

Для отправки сообщений о событиях в syslog требуется включить эту функцию в конфигурационном файле PT ISIM и выбрать вид, в котором будут отображаться атрибуты события (или настроить использование и того и другого вида).

► Чтобы настроить отправку сообщений о событиях на локальный syslog-сервер:

1. Создайте файл в формате TXT для сопоставления атрибутов события и полей syslog-сообщения со следующим форматом:

```
<Поле в syslog> = [<Атрибут события>]
```

Вы можете указать несколько атрибутов событий для одного поля syslog. В этом случае в syslog будет направлено значение первого обнаруженного атрибута.

Например:

```
time = [time]
src.ip = [Network.IPv4.src_addr]
dst.ip = [Network.IPv4.dst_addr]
src.port = [Network.IPv4.TCPv4.src_port, Network.IPv4.UDPv4.src_port,
Network.IPv4.ICMPv4.src_port]
dst.port = [Network.IPv4.TCPv4.dst_port, Network.IPv4.UDPv4.dst_port,
Network.IPv4.ICMPv4.dst_port]
class = [class]
protocol = [Protocol.protocol, Protocol.Flow.app_proto]
```

2. В каталоге `/opt/ptisim/etc/core.d/` создайте конфигурационный файл с разрешением `.conf`.

**Примечание.** Системный пользователь `ptisim` из группы `ptisim` должен иметь права на чтение файлов, созданных на шагах 1 и 2. Вы можете проверить права пользователя с помощью команды: `ls -l <Путь к файлу>`. Вы можете выдать пользователю права с помощью команды: `chown ptisim:ptisim <Путь к файлу>`.

3. Откройте созданный конфигурационный файл.
4. В секции `siem` в параметре `config` укажите путь текстового файла для сопоставления атрибутов.
5. В секции `siem` в параметре `mode` укажите способ отправки нормализованного события: `json` (JSON), `gzip` (gzip, закодированный в Base64) или `drop` (не отправлять нормализованное событие).

Например:

```
{
 "core": {
 "features": {
 "siem": true
 },
 "siem": {
 "config": "/opt/ptisim/etc/core.d/siem.txt",
 "mode": "json"
 }
 }
}
```

6. В секции `features` для параметра `siem` укажите значение `true`, чтобы включить отправку сообщений о событиях в syslog.
7. Перезапустите службу анализа трафика:
 

```
sudo systemctl restart ptisim-core
```
8. В каталоге `/etc/syslog-ng/conf.d/` создайте конфигурационный файл `10_events.conf`.

9. Откройте файл `10_events.conf`.

10. Добавьте в файл следующие строки:

```
filter f_events { program("ISIM"); };
log { source(s_src); filter(f_events); destination(d_syslog); };
```

11. Перезапустите службу `syslog-ng`:

```
sudo systemctl restart syslog-ng
```

Пример сообщения о событии с отображением только выбранных атрибутов:

```
Aug 29 09:28:43 isimhostname ISIM: @cee:{"time":"2019-08-29T09:28:34.249Z",
"dst.ip":"192.0.2.5", "dst.ip":"192.0.2.6","src.port":35807,"dst.port":53}
```

► Чтобы отключить отправку сообщений о событиях на локальный `syslog`-сервер:

1. Удалите конфигурационный файл `10_events.conf` из каталога `/etc/syslog-ng/conf.d/`.

2. Перезапустите службу `syslog-ng`:

```
sudo systemctl restart syslog-ng
```

## 7.1.6.4. Настройка отправки сообщений о событиях на удаленный `syslog`-сервер

Вы можете настроить отправку сообщений о новых событиях на удаленный `syslog`-сервер.

**Внимание!** После обновления PT ISIM необходимо заново настроить отправку сообщений о событиях на `syslog`-сервер.

Сообщения о событиях имеют следующий формат:

```
<Время сообщения> <Имя узла> ISIM: @cee {"msg":{<Все атрибуты события>}, <Атрибуты,
заданные пользователем>}
```

Атрибуты событий передаются в `syslog`-сообщении после маркера `@cee`. Атрибуты могут быть переданы в виде нормализованного события (то есть списка всех атрибутов в формате JSON или в формате gzip, закодированного в Base64) или списка отдельных атрибутов (вы можете указать атрибуты события и задать им собственные названия для `syslog`, например отображать в `syslog` поле `Network.IPv4.TCPv4.dst_port` в виде поля `dst.port`).

Для отправки сообщений о событиях в `syslog` требуется включить эту функцию в конфигурационном файле PT ISIM и выбрать вид, в котором будут отображаться атрибуты события (или настроить использование и того и другого вида).

**Внимание!** Входящие и исходящие соединения с портом `syslog`-сервера должны быть разрешены в правилах фильтрации. Для настройки правил фильтрации вы можете использовать [утилиту iptablesctl](#) (см. [раздел 7.1.25](#)). Название группы правил должно отличаться от других существующих названий и названия `syslog`, зарезервированного под правила фильтрации для разрешения отправки сообщений об инцидентах. Порт для

отправки сообщений о событиях должен отличаться от порта, зарезервированного для отправки сообщений об инцидентах (см. раздел 3.4). Например, вы можете использовать название группы правил `syslog_events` и порт 515.

Примеры команд для разрешения входящих и исходящих соединений с портом syslog-сервера для отправки сообщений о событиях:

```
iptablesctl add syslog_events "INPUT -p tcp --sport 515 -m state --state ESTABLISHED -j ACCEPT"
iptablesctl add syslog_events "OUTPUT -p tcp --dport 515 -m state --state NEW,ESTABLISHED -j ACCEPT"
```

► Чтобы настроить отправку сообщений о событиях на удаленный syslog-сервер:

1. Создайте файл в формате TXT для сопоставления атрибутов события и полей syslog-сообщения со следующим форматом:

<Поле в syslog> = [<Атрибут события>]

Вы можете указать несколько атрибутов событий для одного поля syslog. В этом случае в syslog будет направлено значение первого обнаруженного атрибута.

Например:

```
time = [time]
src.ip = [Network.IPv4.src_addr]
dst.ip = [Network.IPv4.dst_addr]
src.port = [Network.IPv4.TCPv4.src_port, Network.IPv4.UDPv4.src_port,
Network.IPv4.ICMPv4.src_port]
dst.port = [Network.IPv4.TCPv4.dst_port, Network.IPv4.UDPv4.dst_port,
Network.IPv4.ICMPv4.dst_port]
class = [class]
protocol = [Protocol.protocol, Protocol.Flow.app_proto]
```

2. В каталоге `/opt/ptisim/etc/core.d/` создайте конфигурационный файл с разрешением `.conf`.

**Примечание.** Системный пользователь `ptisim` из группы `ptisim` должен иметь права на чтение файлов, созданных на шагах 1 и 2. Вы можете проверить права пользователя с помощью команды: `ls -l <Путь к файлу>`. Вы можете выдать пользователю права с помощью команды: `chown ptisim:ptisim <Путь к файлу>`.

3. Откройте созданный конфигурационный файл.
4. В секции `siem` в параметре `config` укажите путь текстового файла для сопоставления атрибутов.
5. В секции `siem` в параметре `mode` укажите способ отправки нормализованного события: `json` (JSON), `gzip` (gzip, закодированный в Base64) или `drop` (не отправлять нормализованное событие).

Например:

```
{
 "core": {
 "features": {
```

```

"siem": true
},
"siem": {
"config": "/opt/ptisim/etc/core.d/siem.txt",
"mode": "json"
}
}
}

```

6. В секции `features` для параметра `siem` укажите значение `true`, чтобы включить отправку сообщений о событиях в `syslog`.
7. Перезапустите службу анализа трафика:  

```
sudo systemctl restart ptisim-core
```
8. В каталоге `/etc/syslog-ng/conf.d/` создайте конфигурационный файл `10_events.conf`.
9. Откройте файл `10_events.conf`.
10. Если требуется отправлять сообщения по протоколу TCP, добавьте в файл следующие строки:  

```
destination d_net { tcp("<IP-адрес или доменное имя syslog-сервера>" port(<Порт syslog-сервера>)); };
filter f_events { program("ISIM"); };
log { source(s_src); filter(f_events); destination(d_net); };
```
11. Если требуется отправлять сообщения по протоколу UDP, добавьте в файл следующие строки:  

```
destination d_net { udp("<IP-адрес или доменное имя syslog-сервера>" port(<Порт syslog-сервера>)); };
filter f_events { program("ISIM"); };
log { source(s_src); filter(f_events); destination(d_net); };
```
12. Перезапустите службу `syslog-ng`:  

```
sudo systemctl restart syslog-ng
```

Пример сообщения о событии с отображением только выбранных атрибутов:

```
Aug 29 09:28:43 isimhostname ISIM: @cee:{"time":"2019-08-29T09:28:34.249Z",
"dst.ip":"192.0.2.5", "dst.ip":"192.0.2.6", "src.port":35807, "dst.port":53}
```

- Чтобы отключить отправку сообщений о событиях на удаленный `syslog`-сервер:
  1. Удалите конфигурационный файл `10_events.conf` из каталога `/etc/syslog-ng/conf.d/`.
  2. Перезапустите службу `syslog-ng`:  

```
sudo systemctl restart syslog-ng
```

## 7.1.7. Настройка почтовых уведомлений об инцидентах

Вы можете настроить отправку почтовых уведомлений о новых инцидентах, о смене статуса инцидентов или о наступлении нового этапа у существующих инцидентов. Уведомления приходят на адрес электронной почты пользователя PT ISIM View Sensor, указанный в его профиле, если пользователь включил прием уведомлений.

Включить или отключить прием уведомлений, посмотреть адрес электронной почты для уведомлений и при необходимости сменить его пользователь может, выбрав в главном меню .

**Примечание.** Если учетная запись [заблокирована \(см. раздел 7.1.1.6\)](#), уведомления на связанный с ней адрес электронной почты не отправляются.

► Чтобы настроить почтовые уведомления об инцидентах:

1. В главном меню выберите  → **Настройка почтовых уведомлений**.
2. Включите отправку уведомлений.
3. В поле **SMTP-сервер** введите IP-адрес или доменное имя SMTP-сервера.
4. В поле **Порт** укажите порт, который использует SMTP-сервер.

**Примечание.** Для порта, указанного в параметрах подключения, будут автоматически созданы разрешения в цепочках INPUT и OUTPUT правил фильтрации. По умолчанию используются порты 25 и 587. При отключении почтовых уведомлений созданные правила удаляются.

5. Если требуется аутентификация на SMTP-сервере, в полях **SMTP-логин** и **SMTP-пароль** введите учетные данные для аутентификации.
6. В поле **Адрес отправителя** введите адрес электронной почты, от имени которого будут приходить почтовые уведомления.
7. Нажмите **Сохранить**.

Почтовые уведомления об инцидентах настроены.

Вы можете проверить выполненную настройку, отправив тестовое сообщение на произвольный адрес.

► Чтобы отправить тестовое сообщение:

1. В блоке **Отправка тестового сообщения** введите адрес электронной почты, на который требуется отправить тестовое сообщение.
2. Нажмите **Отправить**.

Если почтовые уведомления настроены правильно, на указанный адрес придет тестовое письмо.

## 7.1.8. Изменение информации о системе и контактном лице

Информация о системе — это название узла View Sensor и его геолокация. Эти параметры используются для идентификации PT ISIM на стороне узла Overview Center: название используется, чтобы отличать ваш PT ISIM в списке других узлов ISIM, а геолокация — чтобы отображать его на географической карте.

Информация о контактном лице (адрес электронной почты и телефон) также отображается на стороне узла Overview Center и может потребоваться для получения информации об объекте, на котором установлен PT ISIM, или оперативного реагирования на инциденты.

Информация о системе и контактном лице является частью [пакета регистрации](#) (см. раздел 7.1.10).

► Чтобы изменить информацию о системе и контактном лице:

1. В главном меню выберите  → **Информация о системе и контакты**.
2. В поле **Название узла View Sensor** введите название, идентифицирующее ваш PT ISIM или объект, на котором он установлен.  
  
Поскольку в системе может быть несколько узлов ISIM, рекомендуется присваивать им уникальные названия, чтобы различать их в списке узлов ISIM.
3. В поле **Геолокация** введите координаты объекта, на котором установлен продукт.
4. В поле **Контактное лицо** введите имя и фамилию контактного лица, имеющего доступ к объекту, на котором установлен PT ISIM.
5. В поле **Почта** введите адрес электронной почты контактного лица.
6. В поле **Телефон** введите номер телефона контактного лица.
7. Нажмите кнопку **Сохранить**.

## 7.1.9. Включение и отключение оценки уязвимостей

Уязвимость — это обнаруженный в ИТ-системе недостаток, используя который злоумышленник может нарушить конфиденциальность, целостность или доступность данных. PT ISIM View Sensor выявляет уязвимости на конечных узлах технологической сети путем сопоставления результатов сканирования узлов с данными публичных баз уязвимостей, если оценка уязвимостей включена.

По умолчанию после установки PT ISIM View Sensor оценка уязвимостей отключена (служба оценки уязвимостей [запущена](#) (см. раздел 7.1.14.2), но не выполняет оценку уязвимостей). Обновление PT ISIM View Sensor не влияет на состояние оценки уязвимостей. Если до начала обновления оценка уязвимостей была включена, после его завершения оценка уязвимостей останется включенной.

Вы можете включать и отключать оценку уязвимостей в веб-интерфейсе PT ISIM View Sensor.

► Чтобы включить оценку уязвимостей:

1. В главном меню выберите  → **Оценка уязвимостей**.
2. Включите оценку уязвимостей.

**Примечание.** Включение оценки уязвимостей выполняется в фоновом режиме и может занимать несколько минут.

► Чтобы отключить оценку уязвимостей:

1. В главном меню выберите  → **Оценка уязвимостей**.

**Внимание!** После отключения оценки перестанут регистрироваться новые уязвимости. При повторном сканировании узлов ранее обнаруженные на них уязвимости будут закрыты.

2. Отключите оценку уязвимостей.

## 7.1.10. Создание пакета регистрации PT ISIM View Sensor для подключения к PT ISIM Overview Center

Пакет регистрации — это набор параметров, необходимых для подключения узла ISIM (View Sensor или Overview Center) к узлу Overview Center.

Перед созданием пакета регистрации необходимо убедиться в соблюдении следующих условий:

- Заполнена [информация о системе и контактном лице](#) (см. раздел 7.1.8).
- В параметрах межсетевого экрана открыт TCP-порт 2222 для получения обновлений от узла Overview Center.

► Чтобы создать пакет регистрации PT ISIM View Sensor:

1. В главном меню выберите  → **Создать пакет регистрации**.

Откроется окно **Пакет регистрации View Sensor**.

2. В поле **Сетевой адрес View Sensor** введите IP-адрес или доменное имя PT ISIM View Sensor.

Данный адрес будет использоваться для подключения к регистрируемому узлу ISIM и перехода в его веб-интерфейс.

3. В поле **Комментарий** опишите процедуру получения пароля к пакету регистрации.
4. Выберите способ отправки пакета:

- Для отправки пакета напрямую по сети в раскрывающемся списке **Способ отправки** выберите **Отправить по сети**, в поле **Сетевой адрес узла регистрации** введите IP-адрес или доменное имя узла Overview Center, на котором требуется зарегистрировать PT ISIM View Sensor, и нажмите кнопку **Отправить по сети**.
- Для отправки пакета иным способом в раскрывающемся списке **Способ отправки** выберите **Сохранить на диск** и нажмите кнопку **Сохранить на диск**.

Откроется окно с паролем созданного пакета регистрации.

5. Скопируйте пароль и передайте его получателю пакета регистрации.

Пакет регистрации PT ISIM View Sensor создан.

## См. также

[Подключение узлов ISIM к PT ISIM Overview Center \(см. раздел 7.4.7\)](#)

## 7.1.11. Отключение извлечения файлов из трафика

При обнаружении событий, связанных с передачей файла по сети (например, «Передача файла по FTP» или «Передача файла по HTTP»), PT ISIM сохраняет переданный файл на сервер в каталог `/opt/ptsecurity/data/files`. Такой файл становится доступным для скачивания в карточке события в веб-интерфейсе PT ISIM. Типы сохраняемых файлов перечислены в файле `/opt/ptsecurity/etc/current/file-store.yaml`. Размер сохраняемых файлов ограничен 101 МБ.

Если сохранение файлов чрезмерно нагружает систему (например, файлы занимают слишком много дискового пространства), вы можете отключить извлечение файлов из трафика. При этом события, связанные с передачей файлов, не будут регистрироваться. Передача файлов на проверку в PT Sandbox будет отключена.

**Примечание.** При изменении этого параметра автоматически перезапускается служба `ptdri`, поэтому на некоторое время будет прерван захват и разбор трафика.

- ▶ Чтобы отключить извлечение файлов из трафика:

1. В главном меню выберите  → **Анализ файлов**.
2. Отключите извлечение файлов из трафика.
3. Нажмите **Сохранить**.

Включение и отключение извлечения файлов из трафика фиксируется [в истории действий пользователей \(см. раздел 7.1.1.5\)](#).

## 7.1.12. Настройка интеграции с PT Sandbox для проверки файлов

Positive Technologies Sandbox (PT Sandbox) — это программный комплекс, предназначенный для проверки файлов и электронных писем на предмет угрозы информационной безопасности. Поддерживаемые версии PT Sandbox указаны в [программных требованиях](#) (см. раздел 3.2).

Вы можете настроить передачу извлеченных из трафика файлов в PT Sandbox для их проверки на наличие угроз информационной безопасности. Для этого необходимо настроить интеграцию в обоих продуктах.

В PT Sandbox необходимо:

- создать токен доступа с разрешенным действием `SCAN_WITH_PREDEFINED_SETTINGS` (проверка с параметрами источника);
- создать внешний источник с типом **API с выбранными параметрами проверки** и использовать проверку с параметрами источника.

Подробнее работа с PT Sandbox описана в документации к продукту: подключение источников — в [Руководстве администратора](#), а работа с токенами доступа — в [Руководстве разработчика](#).

► Чтобы настроить интеграцию с PT Sandbox в PT ISIM View Sensor:

1. В главном меню выберите  → **Анализ файлов**.
2. Если извлечение файлов из трафика отключено, включите его.

При изменении этого параметра автоматически перезапускается служба `ptdpi`, поэтому на некоторое время будет прерван захват и разбор трафика.

**Примечание.** После извлечения из трафика файлы сохраняются на диске. В PT Sandbox будут отправляться копии сохраненных файлов. Если файл большой, для экономии дискового пространства сохраняется только часть файла (первые 101 МБ). Это необходимо учитывать при оценке результатов проверки больших файлов.

3. Включите проверку файлов в PT Sandbox.
4. Введите IP-адрес или FQDN PT Sandbox.
5. Введите порт PT Sandbox.
6. Введите токен доступа, созданный в PT Sandbox.
7. Выберите типы файлов для передачи на проверку в PT Sandbox.
8. Нажмите **Сохранить**.

Вы можете проверить соединение с API PT Sandbox по кнопке **Проверить соединение**.

По результатам проверки файлов в PT Sandbox в PT ISIM View Sensor регистрируется событие. Событие содержит информацию о статусе проверки, вердикте PT Sandbox, ошибках проверки, а также активную ссылку для просмотра информации о проверке в PT Sandbox. При обнаружении угроз в файле PT ISIM View Sensor также регистрирует инцидент.

Включение и отключение передачи файлов на проверку в PT Sandbox, а также изменение параметров подключения фиксируется [в истории действий пользователей \(см. раздел 7.1.1.5\)](#).

## 7.1.13. Настройка приема данных от PT ISIM Endpoint

Для приема данных от агентов PT ISIM Endpoint на сервере, где установлен PT ISIM View Sensor, необходимо настроить сервис ptisim-rester.

► Чтобы настроить в PT ISIM View Sensor прием данных от агентов PT ISIM Endpoint:

1. Создайте конфигурационный файл `/opt/ptisim/etc/rester.d/endpoint.conf`:

```
nano /opt/ptisim/etc/rester.d/endpoint.conf
```

2. Добавьте в файл `endpoint.conf` содержимое вида:

```
{
 "rester": {
 "endpoint": {
 "host": String,
 "port": Integer,
 "udp_enabled": Boolean,
 "tcp_enabled": Boolean
 }
 }
}
```

- Если PT ISIM Endpoint установлен на отдельном сервере, в параметре `host` укажите внешний IP-адрес узла, на котором установлен PT ISIM View Sensor и который будет использовать порт 6192 для приема событий от агентов.
- Если PT ISIM Endpoint установлен на одном сервере с PT ISIM View Sensor, в параметре `host` укажите значение `172.19.0.1`.
- В параметре `port` укажите значение 6192.
- В параметрах `udp_enabled` и `tcp_enabled` установите значения `true` и `false` так, чтобы значение `true` соответствовало протоколу передачи данных к PT ISIM View Sensor, указанному в файле `install.cfg` при установке PT ISIM Endpoint.

Пример файла `endpoint.conf` для конфигурации, когда PT ISIM Endpoint и PT ISIM View Sensor установлены на одном сервере:

```
{
 "rester": {
 "endpoint": {
 "host": "172.19.0.1",
 "port": 6192,
 "udp_enabled": false,
```

```

 "tcp_enabled": true
 }
}
}

```

3. Перезапустите сервис ptisim-rester:

```
systemctl restart ptisim-rester.service
```

4. Включите в политиках iptables порт 6192 для прослушивания сервисом ptisim-rester входящих сообщений, указав транспортный протокол для передачи данных к PT ISIM View Sensor и IP-адрес из параметра host в файле endpoint.conf:

```
/opt/ptisim/bin/rester_port add -p 6192 -t <Протокол> -a <IP-адрес>
```

Например:

```
/opt/ptisim/bin/rester_port add -p 6192 -t tcp -a 172.19.0.1.
```

## См. также

[Установка PT ISIM Endpoint \(см. раздел 5.4\)](#)

[Администрирование PT ISIM Endpoint \(см. раздел 7.2\)](#)

## 7.1.14. Диагностика состояния PT ISIM View Sensor

В веб-интерфейсе PT ISIM View Sensor вы можете проводить диагностику работы продукта и сервера, на котором он установлен. Для диагностики доступны следующие параметры:

- состояние сетевых интерфейсов;
- состояние служб (с возможностью просмотреть журнальные файлы по каждой службе);
- место на жестком диске, объем выделенного ОЗУ, сетевое подключение.

### В этом разделе

[Просмотр состояния сетевых интерфейсов \(см. раздел 7.1.14.1\)](#)

[Просмотр состояния служб и основных параметров системы \(см. раздел 7.1.14.2\)](#)

[Просмотр журналов служб \(см. раздел 7.1.14.3\)](#)

[Скачивание пакета диагностической информации \(см. раздел 7.1.14.4\)](#)

### 7.1.14.1. Просмотр состояния сетевых интерфейсов

- Чтобы просмотреть состояние сетевых интерфейсов,

в главном меню выберите .

Откроется окно, позволяющее просмотреть наличие подключения к сетевым интерфейсам, среднюю скорость передачи пакетов и событий и количество пакетов и событий за последние 15 секунд и 30 минут.

| События                        |        |        |       |
|--------------------------------|--------|--------|-------|
| Приблизительная скорость (e/s) | 15 сек | 30 мин |       |
| 0                              | 0      | 0      |       |
| Пакеты                         |        |        |       |
| Приблизительная скорость (p/s) | 15 сек | 30 мин |       |
| ▼ ■ <b>bond0</b>               | 876    | 103686 |       |
| ■ eth1                         | 29.2   | 438    | 51843 |
| ■ eth2                         | 29.2   | 438    | 51843 |
| ■ eth0                         | 66.7   | 1000   | 88111 |

Рисунок 49. Просмотр состояния сетевых интерфейсов

Сетевые интерфейсы, с которых необходимо перехватывать технологический трафик, должны быть объединены в виртуальный интерфейс bond0.

**Примечание.** Если требуется перенастроить сетевые интерфейсы после установки продукта, вы можете вызвать окно настройки интерфейсов, запустив скрипт `/opt/ptisim/bin/configure_interfaces`.

## 7.1.14.2. Просмотр состояния служб и основных параметров системы

- ▶ Чтобы просмотреть состояние служб и основных параметров системы,

в главном меню выберите  → **Диагностика**.

Откроется окно **Диагностика**.

Окно **Диагностика** позволяет просматривать следующие параметры системы:

- состояние служб (см. таблицу ниже):

- **ОК** — служба запущена;
- **Ошибка** — служба не запущена;

**Примечание.** Перезапустить службу вы можете командой: `systemctl restart <Название службы в командной строке>`.

- **Ошибка запроса** — не удалось [запросить состояние службы \(см. раздел 9.4\)](#).
- наличие подключения на bond0 — параметр, показывающий, что bond-интерфейс настроен и на него приходит трафик;
- однонаправленное подключение к анализируемой сети — параметр, показывающий, что подключение PT ISIM View Sensor к анализируемой сети является односторонним: PT ISIM View Sensor получает от сети копию трафика, но не передает в нее данные.

Проверка подключения выполняется путем отправки запросов вида `ping -c1 -W1 -I<Название интерфейса> <IP-адрес авторизованного узла>` для каждого интерфейса и всех авторизованных узлов сети. Если IP-адрес недоступен, подключение считается однонаправленным. Если IP-адрес доступен, проверка подключения через указанный интерфейс прерывается и подключение через него не считается однонаправленным. Если требуется, вы можете [исключать \(см. раздел 7.1.14.2\)](#) IP-адреса из проверки.

- изолированность сенсора от интернета — параметр, показывающий, что сервер, на котором установлен PT ISIM View Sensor, не имеет доступа в интернет;
- место на жестком диске. Отображается объем доступной и использованной памяти, а также общий объем. Если доступно от 2 до 25 ГБ, отображается предупреждение «Мало места»; если доступно меньше 2 ГБ — «Критический уровень»;
- объем выделенного ОЗУ. Отображается объем доступной и использованной памяти, а также общий объем. Если доступно от 2 до 8 ГБ, отображается предупреждение «Мало памяти»; если доступно меньше 2 ГБ — «Критический уровень».

Подробная информация о каждом из параметров доступна по нажатию .

Таблица 29. Службы PT ISIM View Sensor

| Название службы в веб-интерфейсе                     | Название службы в командной строке |
|------------------------------------------------------|------------------------------------|
| Служба базы событий (отсутствует в microView Sensor) | clickhouse-server.service          |
| Служба PT DPI Broker Server                          | ptdpi-broker-srv.service           |
| Служба PT DPI Broker                                 | ptdpi-broker.service               |
| Служба PT DPI Networking                             | ptdpi-networking.service           |
| Служба PT DPI                                        | ptdpi.service                      |
| Служба учета инцидентов                              | ptisim-alerts.service              |
| Служба PT Artifacts                                  | ptisim-artifacts.service           |
| Служба обработки результатов сканирования            | ptisim-assets.scans                |
| Служба обработки данных                              | ptisim-backend.service             |
| Служба сбора статистики                              | ptisim-bucket.service              |
| Служба цепочек инцидентов                            | ptisim-chains.service              |
| Служба анализа трафика                               | ptisim-core.service                |
| Служба активации пользовательских правил             | ptisim-eva.service                 |
| Служба HTTP API                                      | ptisim-httpapi.service             |
| Служба моделирования                                 | ptisim-model-service-ng.service    |

| Название службы в веб-интерфейсе              | Название службы в командной строке                                           |
|-----------------------------------------------|------------------------------------------------------------------------------|
| Служба мониторинга <sup>3</sup>               | ptisim-grafana.service<br>ptisim-otlp-collector.service<br>ptisim-vm.service |
| Служба PT Peony                               | ptisim-peony.service                                                         |
| Служба приема событий от ISIM Endpoint        | ptisim-rester.service                                                        |
| Служба управления пользовательскими правилами | ptisim-rum.service                                                           |
| Служба сканирования узлов                     | ptisim-scanningworker.service                                                |
| Служба таксономии                             | ptisim-taxonomy.service                                                      |
| Служба технологических сигналов               | ptisim-tech-signal.service                                                   |
| Служба обмена сообщениями <sup>3</sup>        | rabbitmq-server.service                                                      |
| Служба проверки файлов в PT Sandbox           | ptisim-backend.service                                                       |

## Исключение IP-адресов из проверки однонаправленного подключения к анализируемой сети

- Чтобы исключить IP-адреса из проверки однонаправленного подключения к анализируемой сети:
  1. Создайте файл с расширением `.yaml` в каталоге `/opt/ptisim/etc/fullview/httpapi.conf.d/`.
  2. Добавьте в файл следующее содержимое со списком исключаемых IP-адресов для каждого интерфейса:
 

```
httpapi:
 modules:
 diagnostics:
 integrity_exclusions:
 <Название интерфейса>:
 - <IP-адрес или диапазон IP-адресов>
 # Добавьте строки для исключения других IP-адресов
 # Добавьте блоки с IP-адресами для других интерфейсов
```

Например:

```
httpapi:
 modules:
 diagnostics:
 integrity_exclusions:
```

<sup>3</sup> Служба перезапускается автоматически. Перезапустить службу вручную с помощью команды `systemctl restart` не получится.

```
eth0:
- 10.0.0.1
- 172.16.1.0/24
- 192.168.*.*
eth1:
- 10.0.0.0/8
```

### 3. Перезапустите службу HTTP API:

```
systemctl restart ptisim-httpapi.service
```

## 7.1.14.3. Просмотр журналов служб

► Чтобы просмотреть журнал службы:

1. В главном меню выберите  → **Диагностика**.
2. Выберите название службы и в раскрывшемся меню выберите пункт **Показать журнал**.  
Откроется окно с журналом выбранной службы.

Интервал, за который показывается журнал, зависит от параметров ротации журнала.

## 7.1.14.4. Скачивание пакета диагностической информации

► Чтобы скачать пакет диагностической информации:

1. В главном меню выберите  → **Диагностика**.
2. В нижней части окна **Диагностика** нажмите **Скачать пакет диагностической информации**.

Начнется скачивание архива.

**Примечание.** Если веб-интерфейс PT ISIM View Sensor недоступен, вы можете выполнить консольную команду `/opt/ptisim/lib/ptisim-httpapi/tools/log_collector.sh` для скачивания пакета диагностической информации.

## 7.1.15. Мониторинг использования ресурсов

Вы можете отслеживать использование ресурсов сервера с установленным PT ISIM View Sensor с помощью встроенных в продукт инструментов.

► Чтобы отследить использование ресурсов на сервере PT ISIM View Sensor,

в главном меню выберите  → **Мониторинг**.

Откроется страница **Мониторинг**.

Данные на странице представлены в удобном для анализа графическом виде. Доступна информация об использовании ресурсов на сервере отдельными процессами (например, загрузка центрального процессора, памяти и дисков), данные об использовании ресурсов базами данных и другие характеристики. Вы можете выбрать период для отображения и настроить частоту обновления данных.

## 7.1.16. Контроль целостности файлов

Контроль целостности исполняемых и конфигурационных файлов PT ISIM View Sensor выполняется с помощью утилиты `control-sum`, входящей в комплект поставки продукта. Утилита позволяет вычислять и записывать эталонные хеш-суммы файлов продукта, а затем сравнивать их с актуальными, в результате чего могут быть выявлены изменения в файлах продукта. Файлы, сгенерированные утилитой, не подписываются защищенным ключом.

### В этом разделе

[Генерация эталонных хеш-сумм \(см. раздел 7.1.16.1\)](#)

[Проверка целостности файлов \(см. раздел 7.1.16.2\)](#)

[Просмотр и изменение списка проверяемых файлов \(см. раздел 7.1.16.3\)](#)

### 7.1.16.1. Генерация эталонных хеш-сумм

Вы можете сгенерировать хеш-суммы исполняемых и конфигурационных файлов PT ISIM View Sensor, например, сразу после установки или обновления продукта. Полученные значения будут использованы в качестве эталонных при проверке целостности файлов.

► Чтобы сгенерировать эталонные хеш-суммы:

1. Перейдите в каталог с утилитой:  
`cd /opt/ptisim/lib/ptisim-httpapi/tools/`
2. Запустите скрипт генерации эталонных хеш-сумм:  
`control-sum-init.sh`

Откроется список файлов, для которых были сгенерированы хеш-суммы.

В каталоге `/opt/ptisim/var/lib` создан файл `control-sum.json`, в котором записаны эталонные хеш-суммы исполняемых и конфигурационных файлов PT ISIM View Sensor.

## 7.1.16.2. Проверка целостности файлов

► Чтобы проверить целостность файлов PT ISIM View Sensor:

1. Перейдите в каталог с утилитой:  
`cd /opt/ptisim/lib/ptisim-httpapi/tools/`
2. Запустите скрипт проверки хеш-сумм:  
`control-sum.sh`

Появится информация об изменениях в исполняемых и конфигурационных файлах PT ISIM View Sensor в формате:

```
"add": [<Добавленный файл>],
"delete": [<Удаленный файл>],
"modify": [<Измененный файл>],
"skip": [<Пропущенный файл, целостность которого не была проверена>]
```

История проверки целостности файлов сохраняется в файле `/var/log/ptisim/control-sum.log`. В нем указаны полные пути до файлов PT ISIM View Sensor и статус их проверки. Если файл PT ISIM View Sensor не изменился, в истории проверки указывается его контрольная хеш-сумма. Если файл изменился, контрольная сумма не указывается.

Сведения об изменении файлов также фиксируются в файле `/var/log/ptisim/control-sum.change`.

Ошибки проверки сохраняются в файле `/var/log/ptisim/control-sum.error`.

## 7.1.16.3. Просмотр и изменение списка проверяемых файлов

► Чтобы просмотреть или изменить список файлов PT ISIM View Sensor, по которым рассчитываются контрольные суммы:

1. Откройте файл `/opt/ptisim/etc/control-sum.yaml`.

Отобразится список файлов, разделенных на блоки:

"files" — каталоги, в которых находятся проверяемые файлы;

"exclude\_dirs" — каталоги, исключенные из проверки;

"ignore" — расширения файлов, игнорируемых при расчете контрольных хеш-сумм.

2. Если требуется, измените блоки с файлами.

## 7.1.17. Замена SSL-сертификата

SSL-сертификат нужен для того, чтобы пользователи PT ISIM имели доступ к страницам веб-интерфейса продукта через HTTPS-соединение. При установке deb-пакета PT ISIM устанавливается самоподписанный сертификат Positive Technologies. Поэтому при подключении к веб-интерфейсу пользователи по умолчанию получают предупреждение о том, что создаваемое подключение не защищено.

Вы можете заменить сертификат Positive Technologies на собственный доверенный. Он должен отвечать следующим требованиям:

- иметь формат PEM, CER/DER или PFX;
- использовать алгоритм подписи SHA-256;
- использовать алгоритм шифрования ключей RSA;
- иметь длину закрытого ключа не менее 2048 бит;
- включать область применения сертификата Digital Signature или Key Encipherment;
- в расширении Subject Alternative Name (SAN) содержать запись о доменном имени или IP-адресе сервера с установленным веб-интерфейсом продукта.

**Примечание.** Если пользователи будут подключаться к веб-интерфейсу с того же сервера, на котором он установлен, в полях SAN также должны быть прописаны доменное имя localhost и IP-адрес 127.0.0.1.

Перед выполнением инструкции вам нужно загрузить на узел с установленным PT ISIM файл SSL-сертификата открытого ключа и файл закрытого ключа, идущего с ним в паре. Если у вас есть промежуточные сертификаты, которые нужно использовать, они должны быть сохранены в одном файле вместе с сертификатом открытого ключа (записаны после него).

► Чтобы заменить SSL-сертификат:

1. Перейдите в каталог, в котором хранятся файлы вашего сертификата.

Например:

```
cd /home/<Имя пользователя>/cert
```

2. Если ваш сертификат в формате PEM, то переименуйте файлы сертификата:

```
ср <Название файла сертификата открытого ключа> ptisim.crt
ср <Название файла закрытого ключа> ptisim.key
```

3. Если ваш сертификат в формате CER/DER, то сконвертируйте его в формат CRT:

```
openssl x509 -inform DER -in <Название файла сертификата> -out ptisim.crt
```

4. Если ваш сертификат в формате PFX, то экспортируйте сертификат и закрытый ключ из PFX-контейнера:

```
openssl pkcs12 -in <Название файла сертификата> -clcerts -nokeys -out ptisim.crt
openssl pkcs12 -in <Название файла сертификата> -nocerts -out ptisim.key
```

5. Если сертификат имеет закрытый ключ, снимите с него пароль:

```
openssl rsa -in <Название файла сертификата> -out ptisim.key
```

6. Создайте резервную копию сертификата Positive Technologies:  
`tar cvzf <Название архива с создаваемой резервной копией> /etc/ptisim/ptisim*`
7. Удалите старый сертификат и ключ из каталога `/etc/ptisim`:  
`rm /etc/ptisim/*`
8. Скопируйте файлы вашего сертификата и открытый ключ в каталог `/etc/ptisim`:  
`cp /<Каталог с файлами сертификата>/ ptisim.* /etc/ptisim`

**Внимание!** Ваш сертификат и ключ должны называться так же, как старый сертификат и ключ — `ptisim.crt` и `ptisim.key`.

9. Перезагрузите веб-сервер `nginx`:  
`sudo systemctl restart nginx.service`

SSL-сертификат заменен.

Вы можете проверить работоспособность нового сертификата, открыв веб-интерфейс PT ISIM. В адресной строке браузера слева от адреса должен появиться значок .

## 7.1.18. Настройка ERSPAN-приемника

Для захвата копии сетевого трафика с помощью технологии ERSPAN необходимо настроить ERSPAN-интерфейс на узле PT ISIM View Sensor:

- создать ERSPAN-интерфейс для приема копии трафика;
- добавить созданный интерфейс в `bond`.

**Примечание.** Если требуется, вы можете создать несколько ERSPAN-интерфейсов и добавить их в `bond`.

Данная инструкция описывает настройку ERSPAN-интерфейса на узлах со службой `networking`.

- Чтобы настроить ERSPAN-интерфейс на приемнике:

1. Проверьте, что на узле PT ISIM View Sensor запущена служба `networking`:  
`systemctl status networking.service`
2. Откройте на редактирование файл конфигурации сетевых интерфейсов:  
`sudo nano /etc/network/interfaces`
3. Добавьте в файл следующие строки с конфигурацией ERSPAN-интерфейса:

**Внимание!** Важно, чтобы конфигурация ERSPAN-интерфейса располагалась в файле до конфигурации интерфейса `bond0`.

```
auto <Имя интерфейса>
iface <Имя интерфейса> inet manual
 pre-up ip link add dev <Имя интерфейса> type erspan local <IP-адрес ERSPAN-интерфейса
PT ISIM View Sensor> remote <IP-адрес источника> seq key <GRE-ключ> erspan_ver <Версия
ERSPAN> erspan <Идентификатор сессии>
 up ip link set <Имя интерфейса> up
 down ip link del dev <Имя интерфейса>
```

Пример конфигурации для интерфейса erspan1:

```
auto erspan1
iface erspan1 inet manual
 pre-up ip link add dev erspan1 type erspan local 192.168.2.13 remote 192.168.2.12 seq
key 300 erspan_ver 1 erspan 300
 up ip link set erspan1 up
 down ip link del dev erspan1
```

4. Сохраните изменения и закройте файл.
5. Перезапустите службу networking:  
`sudo systemctl restart networking.service`
6. Для проверки настройки ERSPAN-интерфейса выполните команду `ip a`.

В выводе команды должны присутствовать следующие параметры:

- `gre0@NONE` — базовый GRE-интерфейс;
  - `erspan0@NONE` — системный ERSPAN интерфейс;
  - `<Имя интерфейса>@NONE` — созданный вами ERSPAN интерфейс со статусом UP.
7. Добавьте ERSPAN-интерфейс в bond с помощью команды (см. раздел 5.3.5.1) `/opt/ptisim/bin/configure_interfaces`.

## 7.1.19. Миграция данных модели сети в ручном режиме

**Внимание!** Миграцию данных модели сети в ручном режиме нужно выполнять при обновлении PT ISIM View Sensor 4.5 до версий 5.8—5.11. При этом в новую версию переносятся данные об узлах, группах, контейнерах и разрешениях для соединений.

**Примечание.** Для выполнения миграции данных модели сети в ручном режиме потребуется файл `export_config_45.py`, который можно получить в службе технической поддержки.

► Чтобы выполнить миграцию данных модели сети в ручном режиме:

1. Скопируйте файл `export_config_45.py` в каталог `root` на сервере PT ISIM View Sensor 4.5.
2. Выгрузите данные модели сети, выполнив команду:  
`sudo sh -c "cd /root && python3 /root/export_config_45.py"`  
После завершения выгрузки в каталоге `root` появится файл вида `export_configuration_<Дата и время создания архива (UTC)>` с данными модели сети.
3. Сохраните выгруженный файл на машине с доступом к веб-интерфейсу PT ISIM View Sensor для последующего импорта.
4. Обновите (см. раздел 6.1) PT ISIM View Sensor 4.5 до версии 5.8 или выше.
5. Войдите в веб-интерфейс PT ISIM View Sensor под учетной записью с правами администратора.

6. В главном меню выберите  → **Экспорт и импорт конфигурации PT ISIM**.
7. Выберите вкладку **Импорт**.
8. Нажмите **Импортировать**.
9. Выберите файл с данными модели сети, выгруженный на шаге 2, и нажмите **Открыть**.

Начнется импорт модели сети.

В случае успешного завершения импорта появится соответствующее сообщение, при появлении проблем — сообщение об ошибке.

## 7.1.20. Удаление неиспользуемых файлов модели сети

После обновления PT ISIM View Sensor 5.1–5.7 до версии 5.8 или выше на диске остаются файлы модели сети, используемые в предыдущей версии. На диске также могут остаться файлы резервной копии модели сети, автоматически создаваемые в случае появления проблем во время миграции данных. После успешного завершения обновления PT ISIM View Sensor вы можете удалить эти файлы.

**Внимание!** Прежде чем удалять файлы по инструкциям ниже, необходимо убедиться в наличии данных модели сети в новой версии.

- Чтобы удалить неиспользуемые файлы модели сети,

выполните команды:

```
sudo rm -rf /opt/ptisim/data/model-service-ng/storage/snapshots
sudo rm -rf /opt/ptisim/data/model-service-ng/storage/operations
```

- Чтобы удалить файлы резервной копии модели сети,

выполните команды:

```
sudo rm -rf /opt/ptisim/data/model-service-ng/storage/snapshots-*.bak
sudo rm -rf /opt/ptisim/data/model-service-ng/storage/operations-*.bak
```

## 7.1.21. Проверка целостности цифровой подстанции по стандарту МЭК-61850

Контроль целостности цифровой подстанции по стандарту МЭК-61850 выполняется с помощью утилиты integrity-control, входящей в комплект поставки продукта. Утилита позволяет импортировать SCD-файлы (substation configuration description) с эталонным описанием цифровых связей, а затем сравнивать их с реальной сетью на объекте, в результате чего могут быть выявлены неизвестные соединения или теги, а также нарушения целостности связи между узлами цифровой подстанции и нарушения структуры передаваемых данных.

## В этом разделе

[Загрузка файла с эталонными данными для проверки целостности \(см. раздел 7.1.21.1\)](#)

[Выявляемые события и регистрируемые инциденты \(см. раздел 7.1.21.2\)](#)

### 7.1.21.1. Загрузка файла с эталонными данными для проверки целостности

Вы можете загрузить в утилиту SCD-файл, описывающий допустимые связи по протоколам GOOSE и MMS. Содержащиеся в файле названия узлов (терминалы РЗА и серверы SCADA) и список GOOSE- и MMS-тегов и их структур будут использованы в качестве эталонных при проверке целостности.

► Чтобы загрузить файл с эталонными данными:

1. Перейдите в каталог с утилитой:

```
cd /opt/ptisim/bin/61850-integrity-control/
```

2. Запустите утилиту, указав абсолютный или относительный путь к SCD-файлу в качестве аргумента:

```
/opt/ptisim/bin/61850-integrity-control <Путь к файлу>
```

Откроется меню со списком возможных действий.

3. Выберите действие из списка, нажав соответствующую ему клавишу от 1 до 5:

**1. Load the network model and lists of GOOSE and MMS tags from the configuration** (Загрузить модель сети и справочники GOOSE- и MMS-тегов из конфигурации).

**2. Load the lists of GOOSE and MMS tags from the configuration** (Загрузить справочники GOOSE- и MMS-тегов из конфигурации).

**3. Load the list of MMS tags from the configuration** (Загрузить справочник MMS-тегов из конфигурации).

**4. Load the list of GOOSE tags from the configuration** (Загрузить справочник GOOSE-тегов из конфигурации).

**5. Load the network model from the configuration** (Загрузить модель сети из конфигурации).

Файл с эталонными данными загружен.

### 7.1.21.2. Выявляемые события и регистрируемые инциденты

При разборе трафика по протоколам GOOSE и MMS PT ISIM View Sensor выявляет события и на их основе регистрирует инциденты. Инциденты по каждому из событий регистрируются не чаще одного раза в 6 часов.

Зарегистрированные инциденты отображаются в пользовательском интерфейсе PT ISIM View Sensor, и оператор может работать с ними в обычном режиме. При необходимости оператор может добавить исключения в правила обнаружения атак или отключить правила целиком. Информацию о работе с правилами и исключениями можно найти в Руководстве пользователя в разделе «Управление правилами обнаружения атак».

Таблица 30. События и инциденты, регистрируемые утилитой integrity-control

| Событие                               | Инцидент                   | Правило обнаружения атак                                                               |
|---------------------------------------|----------------------------|----------------------------------------------------------------------------------------|
| Correlated_GOOSE_Unregistered_Dataset | GOOSE_Unregistered_Dataset | GOOSE: обнаружен датасет, которого нет в конфигурации                                  |
| Correlated_GOOSE_Dataset_Change       | GOOSE_Dataset_Change       | GOOSE: обнаружено изменение структуры датасета по сравнению с описанной в конфигурации |
| Correlated_GOOSE_Change_MAC           | GOOSE_Change_MAC           | GOOSE: изменение MAC-адреса источника датасета или MAC-адреса рассылки для датасета    |
| Correlated_GOOSE_Forbidden_Dataset    | GOOSE_Forbidden_Dataset    | GOOSE: отсутствует рассылка зарегистрированного датасета                               |

Список инцидентов, регистрируемых при разборе сообщений по протоколу MMS, приведен в Руководстве пользователя в разделе «Источники данных. Поддерживаемые протоколы».

Зарегистрированные инциденты отображаются в пользовательском интерфейсе PT ISIM View Sensor. При необходимости вы можете добавить исключения в правила обнаружения атак или отключить правила целиком. Информация о работе с правилами и исключениями представлена в Руководстве пользователя в разделе «Работа с PT ISIM View Sensor. Управление правилами обнаружения атак».

Перечень инцидентов, регистрируемых при разборе сообщений по протоколу MMS, приведен в разделе «Источники данных».

## 7.1.22. Экспорт и импорт конфигурации PT ISIM

Под конфигурацией PT ISIM понимается набор объектов и их параметров, выгруженный из PT ISIM View Sensor для сохранения и последующего восстановления объектов в этом же или другом PT ISIM View Sensor. Возможность экспорта и импорта конфигурации позволяет сократить ручную работу при восстановлении системы при сбое или при переносе PT ISIM View Sensor с одного узла на другой.

**Примечание.** Информация о совместимости версий PT ISIM View Sensor при импорте конфигурации указана в [программных требованиях \(см. раздел 3.2\)](#).

Вы можете выбрать, какие объекты включать в конфигурацию при экспорте:

- группы и контейнеры;
- узлы;
- исключения из правил обнаружения атак;
- инциденты — вместе с каждым инцидентом выгружаются все связанные события и учетная запись пользователя, изменившего статус инцидента на текущий;
- списки разрешений для соединений — все или некоторые;
- представления — все или только для выбранных страниц (**Задачи на сбор данных, Инциденты, События, Узлы и их конфигурация, Соединения** или **Технологические сигналы**).

Операции импорта и экспорта конфигурации PT ISIM фиксируются [в журнале действий пользователей \(см. раздел 7.1.1.5\)](#).

## В этом разделе

[Экспорт конфигурации \(см. раздел 7.1.22.1\)](#)

[Импорт конфигурации \(см. раздел 7.1.22.2\)](#)

### 7.1.22.1. Экспорт конфигурации

► Чтобы выгрузить конфигурацию PT ISIM:

1. В главном меню выберите  → **Экспорт и импорт конфигурации PT ISIM**.
2. На вкладке **Экспорт** выберите объекты для экспорта.

**Примечание.** Группа «Нераспределенные узлы» не включается в конфигурацию при экспорте групп, так как создается в PT ISIM View Sensor по умолчанию.

**Примечание.** Информация о том, в какие группы входит узел, выгружается только при одновременной выгрузке узлов, групп и контейнеров.

3. Нажмите **Экспортировать**.

Начнется экспорт конфигурации PT ISIM. По завершении экспорта на диск будет выгружен ZIP-архив с названием вида `export_configuration_<Дата и время создания архива (UTC)>.zip`. В зависимости от выбранных объектов для экспорта архив может содержать следующие файлы в формате JSON:

- `metainfo.json` — обязательный файл со служебной информацией;
- `model.json` — данные узлов, групп и контейнеров;
- `alerts.json` — параметры инцидентов, а также связанных с ними событий и учетных записей пользователей, изменивших статус инцидентов на текущий;

- `exceptions.json` — параметры исключений из правил обнаружения атак;
- `whitelist.json` — перечень списков разрешений. Данные каждого списка выгружаются в отдельных файлах в формате CSV с названиями вида <Идентификатор списка разрешений>\_permissions\_<Дата и время создания файла (UTC)>.csv;
- `table_views.json` — перечень представлений, сохраненных в системе, без учета локальных изменений пользователей. Для каждого представления указывается уникальный идентификатор. Данные каждого представления выгружаются в отдельных файлах в формате JSON.

## 7.1.22.2. Импорт конфигурации

Особенности импорта конфигурации PT ISIM зависят от типа загружаемых объектов:

- **Группы и контейнеры.** Существующие группы и контейнеры будут полностью заменены новыми из файла конфигурации. Если группы и контейнеры не были выбраны при экспорте и данные о них отсутствуют в файле конфигурации, существующие группы и контейнеры не будут удалены.
- **Узлы.** Существующие узлы не удаляются. Будут добавлены новые узлы или обновлены существующие при совпадении их идентификатора с указанным в файле конфигурации. Узлы без интерфейсов не импортируются.
- **Инциденты.** Будут добавлены новые инциденты и связанные с ними события, а также учетные записи пользователей, изменивших статус инцидента на текущий, если в системе нет учетных записей с таким же логином. Учетные записи добавляются со статусом пользователя **Заблокирован**.
- **Исключения из правил обнаружения атак.** Будут заменены все существующие исключения для правил, идентификаторы которых совпадают с указанными в файле. Исключения по другим правилам не изменяются.

**Примечание.** Существующий комментарий для исключения останется без изменений, если в файле для исключения с такими же параметрами комментарий не указан.

- **Списки разрешений.** Существующие списки разрешений не удаляются. Будут добавлены новые или обновлены существующие при совпадении названий списков.
- **Представления.** Будут обновлены существующие при совпадении идентификаторов или добавлены новые. Существующие не удаляются.

Импорт узлов и групп выполняется с учетом условий автонаполнения групп. Если параметры нового или существующего узла соответствуют условиям автонаполнения группы, то узел будет добавлен в группу, а если не соответствуют — исключен. Узлы, которые при импорте конфигурации были исключены из всех групп, добавляются в системную группу «Нераспределенные узлы».

**Внимание!** Перед импортом конфигурации рекомендуется экспортировать текущую, чтобы иметь возможность загрузить ее при необходимости.

**Внимание!** Если во время импорта будет обнаружено некорректное содержание файла конфигурации, объекты из этого файла в PT ISIM не загружаются и импорт останавливается.

► Чтобы загрузить конфигурацию PT ISIM:

1. В главном меню выберите  → **Экспорт и импорт конфигурации PT ISIM**.
2. Выберите вкладку **Импорт**.
3. Нажмите **Импортировать**.
4. Выберите ZIP-архив с конфигурацией PT ISIM и нажмите **Открыть**.

Начнется импорт объектов из файлов конфигурации.

В случае успешного завершения импорта появится соответствующее сообщение, при появлении проблем — сообщение об ошибке.

## 7.1.23. Импорт внешнего проекта

Вы можете импортировать в PT ISIM View Sensor проект, выгруженный из внешней системы.

**Примечание.** Прежде чем загружать проект, рекомендуется [экспортировать конфигурацию \(см. раздел 7.1.22.1\)](#) PT ISIM View Sensor, чтобы сохранить существующие узлы, группы и контейнеры.

► Чтобы импортировать внешний проект:

1. В главном меню выберите  → **Импорт внешнего проекта**.
2. Выберите тип проекта.
3. Выберите объекты для импорта.
4. Нажмите **Импортировать**.
5. Выберите ZIP-архив с внешним проектом и нажмите **Открыть**.

Начнется импорт объектов из внешнего проекта.

Рекомендуется не закрывать окно для отслеживания статуса импорта. В случае успешного завершения импорта появится соответствующее сообщение, при появлении проблем — сообщение об ошибке или предупреждение. В случае ошибки импорт будет остановлен, в случае предупреждения продолжится.

### В этом разделе

[Особенности импорта проекта СУИК \(см. раздел 7.1.23.1\)](#)

[Особенности импорта проекта SCD \(см. раздел 7.1.23.2\)](#)

## 7.1.23.1. Особенности импорта проекта СУИК

Проект СУИК содержит данные об объектах микропроцессорной системы централизации (МПЦ), используемой на транспорте. Вы можете выбрать, какие объекты из проекта загружать в PT ISIM View Sensor. Особенности импорта зависят от типа загружаемых объектов:

- **Узлы.** Будут добавлены новые или изменены существующие при совпадении сетевых интерфейсов. Возможно объединение узлов и перенос интерфейсов между узлами, чтобы сетевые интерфейсы каждого соответствовали загружаемым из проекта. Узлы, оставшиеся без интерфейсов после переноса, будут удалены. В импортируемом проекте для каждого узла должен быть указан сетевой интерфейс.
- **Группы и контейнеры.** Существующие группы и контейнеры будут полностью удалены и заменены созданными по умолчанию и новыми из внешнего проекта.

По умолчанию будет создана группа «Нераспределенные узлы», а также контейнер Public network, включающий автонаполняемую группу Internet. В группу Internet будут входить все узлы согласно условиям автонаполнения этой группы, кроме импортируемых. Для этого в условия автонаполнения группы Internet будут автоматически добавлены исключаящие условия по IP-адресам импортируемых узлов. Остальные ранее существующие в системе и не измененные во время импорта узлы будут добавлены в группу «Нераспределенные узлы».

Узлы из проекта, а также существующие узлы, объединенные с ними во время импорта, будут добавлены в новые группы с названиями, соответствующими типам узлов, указанным в проекте, а группы — в новые контейнеры. Если название контейнера в проекте не указано, группы будут добавлены в контейнер с названием «МПЦ».

- **Справочники.** Обязательный объект для импорта. На основе загруженных справочников в PT ISIM View Sensor будут заменены правила нормализации событий, связанных с работой внешней системы.

Обнаруженные в трафике по протоколу COS технологические сигналы будут авторизованными, а операции их чтения и записи разрешенными, если они соответствуют данным загруженного в систему проекта СУИК независимо от того, включен ли режим обучения в PT ISIM View Sensor.

## 7.1.23.2. Особенности импорта проекта SCD

### Объекты для импорта

Проект SCD (Substation Configuration Description) содержит данные об объектах цифровой подстанции и их связях, описанные в соответствии со стандартом МЭК-61850. В текущей версии PT ISIM View Sensor для загрузки из проекта SCD доступны справочники. На основе

загруженных справочников в PT ISIM View Sensor будут заменены правила обогащения событий, связанных с работой внешней системы. Вы можете выбрать протоколы, справочники для которых нужно загружать в систему:

- MMS;
- GOOSE.

## Проверки при импорте

Таблица 31. Проверки при импорте проекта SCD

| Проверка                                                                     | Протокол   |
|------------------------------------------------------------------------------|------------|
| <b>Непрохождение проверки приводит к остановке импорта</b>                   |            |
| Файл с конфигурацией непустой                                                | MMS, GOOSE |
| Расширение файла — .scd                                                      | MMS, GOOSE |
| SCD-файл открывается                                                         | MMS, GOOSE |
| Совместимость версий МЭК-61850 (в файле редакции 1 нет признаков редакции 2) | MMS, GOOSE |
| В файле наборы данных GOOSE расположены в логическом узле LLNO               | GOOSE      |
| Открывающие теги соответствуют закрывающим                                   | MMS, GOOSE |
| <b>Непрохождение проверки не приводит к остановке импорта</b>                |            |
| Длина имени набора данных не больше 32 символов                              | MMS, GOOSE |
| Нет повторяющихся MAC-адресов назначения                                     | GOOSE      |
| Нет повторяющихся имен устройств (IED)                                       | MMS, GOOSE |
| Нет повторяющихся IP-адресов                                                 | MMS, GOOSE |
| Длина идентификатора приложения (appID) от 1 до 64 символов                  | GOOSE      |
| Нет повторяющихся идентификаторов приложений (appID)                         | GOOSE      |
| Длина имени блока управления (GoCB) не больше 28 символов                    | GOOSE      |
| Длина идентификатора GOOSE (goID) не больше 129 символов                     | GOOSE      |
| Длина имени устройства (IED) от 4 до 64 символов                             | MMS, GOOSE |
| В наборе данных не больше 256 элементов FCDA                                 | MMS        |
| Длина имени блока управления отчетами (RCB) не больше 30 символов            | MMS        |

| Проверка                                                                            | Протокол   |
|-------------------------------------------------------------------------------------|------------|
| Длина идентификатора отчета (rptID) не больше 129 символов                          | MMS        |
| Длина идентификатора потока SV не больше 65 символов                                | SV         |
| В атрибутах блока управления SV не больше 16 элементов FCDA                         | SV         |
| В блоке управления SV один набор данных                                             | SV         |
| Нет повторяющихся наборов данных                                                    | MMS, GOOSE |
| Нет повторяющихся элементов FCDA в наборе данных                                    | MMS, GOOSE |
| Нет наборов данных без элементов FCDA                                               | MMS, GOOSE |
| Нет повторяющихся MAC-адресов блока управления (GoCB)                               | GOOSE      |
| Нет пустых или одинаковых имен идентификаторов GOOSE (goID)                         | GOOSE      |
| Число аналоговых сигналов в сообщении не больше 8                                   | GOOSE      |
| Редакции конфигурации GOOSE (confRev) у отправителя и подписчика совпадают          | GOOSE      |
| Число наборов данных GOOSE для устройства IED не больше 4                           | GOOSE      |
| Не больше 20 элементов FCDA в блоке управления (GoCB)                               | GOOSE      |
| Общее число элементов FCDA не больше 80                                             | GOOSE      |
| Корректное значение интервала передачи данных                                       | GOOSE      |
| Нет GOOSE-сообщений без подписчиков                                                 | GOOSE      |
| Идентификатор приложения (applID) в диапазоне от 0000 до 3FFF                       | GOOSE      |
| Нет повторяющихся идентификаторов приложения (applID) в адресе GSE                  | GOOSE      |
| Число логических устройств не больше 4                                              | MMS, GOOSE |
| Атрибуты данных устройства IED содержат не больше 1500 элементов FCDA               | MMS, GOOSE |
| Длина имени логического устройства не больше 64 символов                            | MMS, GOOSE |
| В одном наборе данных не используются элементы ST и MX с разной частотой обновления | MMS        |
| Есть буферизованные отчеты                                                          | MMS        |

| Проверка                                                                            | Протокол   |
|-------------------------------------------------------------------------------------|------------|
| Набор данных содержит атрибуты качества                                             | MMS, GOOSE |
| Корректный порядок размещения атрибутов качества                                    | MMS, GOOSE |
| В блоке управления отчетами (RCB) не больше 10 наборов данных или 80 элементов FCDA | MMS        |
| Нет подписок на несуществующие данные                                               | GOOSE      |
| В наборе данных нет элементов без подписчиков                                       | MMS, GOOSE |
| Идентификатор VLAN в диапазоне от 000 до FFF                                        | GOOSE      |
| Приоритет VLAN в диапазоне от 0 до 7                                                | GOOSE      |

## 7.1.24. Работа с пользовательскими правилами межсетевого экрана

Служба `ptisim-firewall` настраивает межсетевой экран таким образом, что разрешаются только TCP-соединения с портами 2222, 22, 25, 80, 443, 514, 587, 3334, передача UDP-пакетов по портам назначения 123, 514 и 53, а также отправка и прием ICMP-сообщений (echo request, echo reply). Соответствующие правила iptables поставляются вместе с продуктом или создаются автоматически при настройке взаимодействия со службами syslog, SMTP, PT MC в веб-интерфейсе продукта PT ISIM и хранятся в файле `/opt/ptisim/bin/iptables_rules.json`.

Если требуется, вы можете добавить пользовательские правила межсетевого экрана. При этом необходимо убедиться, что соединения с указываемыми портами также разрешены на уровне вашего сетевого оборудования.

Для добавления, удаления, изменения, включения, отключения, восстановления и просмотра пользовательских правил межсетевого экрана используется [утилита iptablesctl](#) (см. раздел 7.1.25).

## 7.1.25. Утилита iptablesctl

Утилита `iptablesctl` отвечает за добавление, редактирование, удаление, отключение, включение, восстановление и просмотр правил фильтрации. Справочная информация о работе с утилитой доступна по команде `iptablesctl --help`.

Команды утилиты `iptablesctl`:

- `iptablesctl default <Имя файла>` — применить правила по умолчанию из файла. Используется, только если файл `/opt/ptisim/bin/iptables_rules.json` был перемещен или удален.

Например, в результате выполнения команды `iptablesctl default /opt/ptisim/etc/default.rules` будет создан файл `iptables_rules.json` со стандартными правилами из файла `default.rules`, поставляемыми с PT ISIM.

- `iptablesctl restore` — восстановить правила фильтрации из файла `/opt/ptisim/bin/iptables_rules.json`. Если в файле были правила для взаимодействия со службами или пользовательские правила, то они также восстановятся.
- `iptablesctl list` — вывести список текущих правил фильтрации с указанием статуса (on или off).
- `iptablesctl clear` — полностью очистить правила фильтрации, установленные для сенсора через утилиту `iptablesctl`.

**Внимание!** В результате выполнения команды очистки с узла сенсора полностью удаляются текущие правила фильтрации, и поэтому SSH-сессия с узлом сенсора будет прервана, так же как и другие возможные соединения. Для восстановления правил фильтрации потребуется выполнить команду `iptablesctl restore`, после чего правила фильтрации восстановятся из файла `/opt/ptisim/bin/iptables_rules.json`.

- `iptablesctl add <Название группы правил> <Правила фильтрации>` — добавить пользовательские правила фильтрации.

Для правил фильтрации нужно использовать уникальные имена групп, отличные от названий групп правил, поставляемых с PT ISIM View Sensor. Тогда при перезагрузке PT ISIM View Sensor добавленные вами правила не будут затерты. Например, вы можете добавлять к общепринятым названиям групп постфикс — `syslog_123`, `syslog_user`. Кроме того, названия новых групп правил не должны повторять уже используемые. Просмотреть список используемых правил вы можете с помощью команды `iptablesctl list`.

При добавлении правил в одну и ту же группу по очереди каждое следующее правило будет затирать предыдущее, поэтому необходимо добавлять сразу все правила, которые требуются для взаимодействия со службой. Пример команды добавления правил для службы telnet: `iptablesctl add telnet "INPUT -p tcp --sport 23 -m state --state ESTABLISHED -j ACCEPT" "OUTPUT -p tcp --dport 23 -m state --state NEW,ESTABLISHED -j ACCEPT"`.

- `iptablesctl del <Название группы правил>` — удалить правила фильтрации из группы. Например, `iptablesctl del telnet`.
- `iptablesctl on <Название группы правил>` — включить группу правил.

Пример команды включения группы правил syslog: `iptablesctl on syslog`.

- `iptablesctl off <Название группы правил>` — выключить группу правил.
- `iptablesctl get <Название группы правил>` — вывести правила группы.

- `iptablesctl policy <Название цепочки правил фильтрации> ACCEPT` — разрешить политику для указанной цепочки правил фильтрации. Пример разрешения цепочки правил `INPUT:iptablesctl policy INPUT ACCEPT`. Просмотреть измененную политику `INPUT ACCEPT` можно выполнив команду `iptables-save -t filter`.
- `iptablesctl policy <Название цепочки правил фильтрации> DROP` — запретить политику для указанной цепочки правил фильтрации.

## 7.1.26. Утилита ISIMCTL

Утилита ISIMCTL призвана облегчить администратору выполнение типовых задач в командной строке при работе с PT ISIM View Sensor. Утилита позволяет взаимодействовать с компонентами PT ISIM View Sensor, базами данных и операционной системой, используя специальный облегченный синтаксис команд ISIMCTL, которые заменяют собой традиционные команды в Debian, запросы ClickHouse (для proView Sensor и netView Sensor), PostgreSQL и другие.

В этом разделе приводится описание основных команд ISIMCTL. Вы можете просмотреть полный список команд, выполнив команду `isimctl` без аргументов.

### В этом разделе

[Системные проверки \(см. раздел 7.1.26.1\)](#)

[Работа с инцидентами \(см. раздел 7.1.26.2\)](#)

[Работа с хранилищем событий ClickHouse \(см. раздел 7.1.26.3\)](#)

[Работа с моделью сети \(см. раздел 7.1.26.4\)](#)

[Работа с PCAP-файлами \(см. раздел 7.1.26.5\)](#)

[Работа с сетевыми параметрами \(см. раздел 7.1.26.6\)](#)

[Работа с PostgreSQL \(см. раздел 7.1.26.7\)](#)

[Работа с сенсором \(см. раздел 7.1.26.8\)](#)

[Работа с Updater \(см. раздел 7.1.26.9\)](#)

### 7.1.26.1. Системные проверки

Проверить статус всех служб:

```
isimctl check services
```

Проверить свободное дисковое пространство:

```
isimctl check disk
```

Проверить, что владельцем каталогов `/opt/ptisim` и `/var/log/ptisim` и файлов в них является пользователь `ptisim`:

```
isimctl check perms
```

Запустить все три вышеперечисленные проверки:

```
isimctl check all
```

## 7.1.26.2. Работа с инцидентами

Показать количество инцидентов, зарегистрированных за все время:

```
isimctl alerts count
```

Показать 50 последних зарегистрированных инцидентов:

```
isimctl charts alerts_by_time
```

Показать количество инцидентов каждого вида, отсортированных по алфавиту:

```
isimctl alerts stats
```

Пример вывода команды:

```
count | type
-----+-----
2 | ARP_Spoofing_Warning
1 | CIP_Malformed_Metasploit_CrashCPU
1 | CIP_Malformed_Metasploit_CrashEther
1 | CIP_Malformed_Metasploit_ResetEther
1 | CIP_Rockwell_PLC_Stop
1 | DNS_Server_Replace
8 | Echo_Request_Unknown_Server
```

## 7.1.26.3. Работа с хранилищем событий ClickHouse

Хранилище событий ClickHouse используется только в PT ISIM proView Sensor и PT ISIM netView Sensor.

Показать все таблицы ClickHouse:

```
isimctl clickhouse tables
```

Показать общее количество событий, зарегистрированных за все время:

```
isimctl events count
```

Показать структуру таблицы events (все параметры событий и их типы данных):

```
isimctl clickhouse events_schema
```

Показать количество событий по каждому протоколу:

```
isimctl events stats
```

Вывести описание таблицы `system.processes`, которая содержит список запросов, выполняющихся в ClickHouse в данный момент:

```
isimctl clickhouse process_list
```

Вывод этой команды может быть пустым, если в данный момент трафик не обрабатывается.

## 7.1.26.4. Работа с моделью сети

Авторизовать узел:

```
isimctl modelservice auth <Идентификатор узла>
```

Показать список всех узлов с их названиями и идентификаторами:

```
isimctl modelservice hosts
```

Далее приведены команды для работы с режимом обучения «Авторизация новых узлов и разрешение соединений».

Включить режим обучения:

```
isimctl modelservice learning_mode on
```

Отключить режим обучения:

```
isimctl modelservice learning_mode off
```

Показать статус режима обучения (true — включен, false — отключен):

```
isimctl modelservice learning_mode show
```

## 7.1.26.5. Работа с PCAP-файлами

Воспроизвести PCAP-файл, направив его на интерфейс bond0:

```
isimctl pcaps run <Имя PCAP-файла>
```

Вы можете нажать клавишу Tab после ввода команды, чтобы просмотреть список всех доступных для запуска PCAP-файлов. Наличие PCAP-файлов проверяется в каталогах /opt, /root и /opt/ptisim/lib/ptisim-isimctl/assets/pcaps.

Постоянно воспроизводить PCAP-файл, пока не будет нажата комбинация клавиш Ctrl+C:

```
isimctl pcaps loop <Имя PCAP-файла>
```

Вывести список PCAP-файлов, созданных службой ptdpi (состав каталога /opt/ptsecurity/data/pcaps):

```
isimctl pcaps list
```

## 7.1.26.6. Работа с сетевыми параметрами

Показать список открытых портов:

```
isimctl os open_ports
```

Разрешить все входящие и исходящие соединения на сервере:

```
isimctl os iptables off
```

Ограничить входящие и исходящие соединения с помощью политик iptables:

```
isimctl os iptables on
```

## 7.1.26.7. Работа с PostgreSQL

Показать все таблицы в базе данных `ptisim` в PostgreSQL:

```
isimctl postgresql ptisim_tables
```

Показать описание столбцов определенной таблицы из базы данных `ptisim` в PostgreSQL:

```
isimctl postgresql ptisim_columns <Название таблицы>
```

Выполнить запрос в базе данных `ptisim` с правами пользователя `ptisim`:

```
isimctl postgresql query <SQL-запрос>
```

Выполнить запрос в базе данных `ptisim` с правами пользователя `postgres`:

```
isimctl postgresql query_pg <SQL-запрос>
```

## 7.1.26.8. Работа с сенсором

Назначить файлам в каталогах `/opt/ptisim` и `/var/log/ptisim` владельца `ptisim` и группу `ptisim`:

```
isimctl sensor fix_perms
```

Установить `en_US.UTF-8` в качестве локализации сервера:

```
isimctl sensor install_locale
```

## 7.1.26.9. Работа с Updater

Компонент Updater служит для взаимодействия PT ISIM View Sensor с PT ISIM Overview Center.

Запустить службу `ptisim-overview-updater`:

```
isimctl updater start
```

Остановить службу `ptisim-overview-updater`:

```
isimctl updater stop
```

## 7.2. Администрирование PT ISIM Endpoint

В этом разделе содержатся инструкции по администрированию и настройке PT ISIM Endpoint.

### В этом разделе

[Работа с агентами \(см. раздел 7.2.1\)](#)

[Работа с политиками \(см. раздел 7.2.2\)](#)

[Настройка промышленной экспертизы \(см. раздел 7.2.3\)](#)

[Настройка сканирования в режиме аудита \(см. раздел 7.2.4\)](#)

[Настройка антивирусной защиты узлов \(см. раздел 7.2.5\)](#)

[Изоляция подозрительных файлов \(см. раздел 7.2.6\)](#)

## 7.2.1. Работа с агентами

Далее приведены инструкции по установке, авторизации, обновлению, блокировке и удалению агентов PT ISIM Endpoint.

### В этом разделе

[Об агентах \(см. раздел 7.2.1.1\)](#)

[Установка агента \(см. раздел 7.2.1.2\)](#)

[Авторизация агента \(см. раздел 7.2.1.3\)](#)

[Обновление агента \(см. раздел 7.2.1.4\)](#)

[Блокировка агента \(см. раздел 7.2.1.5\)](#)

[Удаление агента \(см. раздел 7.2.1.6\)](#)

### 7.2.1.1. Об агентах

Агент PT ISIM Endpoint — это приложение, которое необходимо установить на конечном устройстве для сбора данных, обнаружения угроз и реагирования на них. После установки вам необходимо авторизовать агент и добавить его в группу, на которую назначена хотя бы одна политика.

Агент в PT ISIM Endpoint может иметь один из двух статусов:

- **Подключен.** У агента есть связь с сервером агентов, все функции продукта выполняются штатно.
- **Отключен.** У агента нет связи с сервером агентов, конечное устройство отключено или служба агента остановлена. В частности, возможен такой вариант, при котором устройство включено, служба выполняется (все модули работают локально), но данные на сервер агентов и в сторонние системы не отправляются. Все операции с агентом будут выполнены после восстановления связи. Кроме того, этот статус имеют заблокированные агенты.

Список агентов и информация о них отображаются в веб-интерфейсе PT ISIM Endpoint на странице **Агенты**. Вы можете фильтровать список агентов по времени их последнего нахождения в сети. Фильтр доступен по кнопке  в панели инструментов.

При выборе агента в списке откроется карточка агента. В карточке агента вы можете запускать реагирование, изменять название агента, добавлять агенту метки для быстрого поиска и просматривать информацию об узле, установленные модули, их конфигурацию и зависимости.

**Примечание.** У одного агента не может быть больше 20 меток, на одном сервере агентов — не больше 300 уникальных меток.

## 7.2.1.2. Установка агента

Для установки агента PT ISIM Endpoint необходимо скачать в PT ISIM Endpoint и перенести на конечное устройство дистрибутив агента. После установки агента на конечном устройстве необходимо добавить папку, в которую он был установлен, в исключения антивируса.

При установке агента вы можете добавить для него метки (не более 20) с помощью параметра EDR\_AGENT\_TAGS, например EDR\_AGENT\_TAGS="tag1;tag2". Метки должны быть уникальными и содержать не более 30 символов. Допускаются буквы латинского алфавита, цифры, подчеркивание и дефис. Метки, которые не прошли валидацию, не будут добавлены.

► Чтобы скачать дистрибутив агента:

1. В главном меню PT ISIM Endpoint выберите  **Система** → **Дистрибутивы агентов**.
2. Нажмите кнопку, соответствующую версии ОС и архитектуре, и выберите тип дистрибутива.

Дистрибутив агента сохранен на вашем компьютере. После установки агента необходимо авторизовать его в PT ISIM Endpoint, добавив в группу агентов для назначения политики.

## Установка агента в Linux

В зависимости от используемого дистрибутива Linux вы можете установить агент либо из deb-пакета, либо из RPM-пакета. При установке агента в операционных системах с версией библиотеки glibc ниже 2.28 (AlterOS Desktop 7.5, «Альт Сервер» 9) рекомендуется использовать дистрибутив с именем `linux_<Архитектура>_agent-bundle`, в остальных ОС — стандартный.

**Внимание!** Для установки агента в операционных системах «Альт Сервер» 10.2 и 10.4 необходимо использовать отдельный RPM-пакет (доступен на странице **Дистрибутивы агентов**).

► Чтобы установить агент из deb-пакета:

1. Перейдите в каталог с deb-пакетом:  
`cd <Имя каталога>`
2. Запустите установку агента:  
`sudo VXSERVER_CONNECT=wss://<IP-адрес или полное доменное имя сервера агентов>:<Порт> dpkg -i ./linux_<Архитектура>_agent.deb`

**Примечание.** Порт сервера агентов по умолчанию — 8443.

**Примечание.** При установке агента в виртуальной среде на сервере, на котором уже установлен агент, а также в клонированных виртуальных средах или в системах, развернутых по шаблону, необходимо добавить в команду параметр `AGENT_ID_SALT=<Любое уникальное для конкретного агента значение>`. Этот

параметр задает дополнительный идентификатор для агентов и предотвращает конфликты при совпадении основного идентификатора, который генерируется на основе параметров ОС. При стандартной установке использовать параметр `AGENT_ID_SALT` не нужно. При переустановке агента значение параметра не должно меняться. В значении допускаются буквы латинского алфавита и цифры.

Пример команды установки со всеми параметрами:

```
sudo VXSERVER_CONNECT=wss://10.0.11.21:8443 EDR_AGENT_TAGS="<Список меток>"
AGENT_ID_SALT=<Уникальное значение> dpkg -i ./linux_amd64_agent.deb
```

► Чтобы установить агент из RPM-пакета:

1. Перейдите в каталог с RPM-пакетом:

```
cd <Имя каталога>
```

2. Если установка выполняется на конечном устройстве, с которого недоступны пакетные менеджеры Linux, установите пакеты `libpthread`, `libnsl` и `libcrypto`.
3. Если пакет `initscripts` не установлен, установите его:

```
yum install -y initscripts
```

4. Запустите установку агента:

Если установка выполняется на конечном устройстве, с которого доступны пакетные менеджеры Linux (рекомендуемый вариант):

```
sudo VXSERVER_CONNECT=wss://<IP-адрес или полное доменное имя сервера агентов>:<Порт> yum
--nogpgcheck localinstall ./linux_<Архитектура>_agent.rpm
```

Если установка выполняется на конечном устройстве, с которого недоступны пакетные менеджеры Linux:

```
sudo VXSERVER_CONNECT=wss://<IP-адрес или полное доменное имя сервера агентов>:<Порт> rpm
-i ./linux_<Архитектура>_agent.rpm
```

Если установка выполняется в ОС «Альт Сервер»:

```
sudo VXSERVER_CONNECT=wss://<IP-адрес или полное доменное имя сервера агентов>:<Порт> apt-
get install ./linux_amd64_agent_alt-server_10-2.rpm
```

**Примечание.** Порт сервера агентов по умолчанию — 8443.

**Примечание.** При установке агента в виртуальной среде на сервере, на котором уже установлен агент, а также в клонированных виртуальных средах или в системах, развернутых по шаблону, необходимо добавить в команду параметр `AGENT_ID_SALT=<Любое уникальное для конкретного агента значение>`. Этот параметр задает дополнительный идентификатор для агентов и предотвращает конфликты при совпадении основного идентификатора, который генерируется на основе параметров ОС. При стандартной установке использовать параметр `AGENT_ID_SALT` не нужно. При переустановке агента значение параметра не должно меняться. В значении допускаются буквы латинского алфавита и цифры.

Пример команды установки со всеми параметрами, если пакетные менеджеры Linux доступны:

```
sudo VXSERVER_CONNECT=wss://10.0.11.21:8443 EDR_AGENT_TAGS="<Список меток>"
AGENT_ID_SALT=<Уникальное значение> yum --nogpgcheck localinstall ./
linux_amd64_agent.rpm
```

## Установка агента в Windows

► Чтобы установить MSI-дистрибутив агента в Windows:

1. Откройте интерфейс командной строки Windows от имени администратора.
2. Перейдите в папку с дистрибутивом:

```
cd <Имя папки>
```

3. Запустите установку агента:

```
msiexec /quiet /i windows_<Архитектура>_agent.msi VXSERVER_CONNECT=wss://<IP-адрес или
полное доменное имя сервера агентов>:<Порт>
```

**Примечание.** Порт сервера агентов по умолчанию — 8443.

**Примечание.** При установке агента в виртуальной среде на сервере, на котором уже установлен агент, а также в клонированных виртуальных средах или в системах, развернутых по шаблону, необходимо добавить в команду параметр AGENT\_ID\_SALT=<Любое уникальное для конкретного агента значение>. Этот параметр задает дополнительный идентификатор для агентов и предотвращает конфликты при совпадении основного идентификатора, который генерируется на основе параметров ОС. При стандартной установке использовать параметр AGENT\_ID\_SALT не нужно. При переустановке агента значение параметра не должно меняться. В значении допускаются буквы латинского алфавита и цифры.

### 7.2.1.3. Авторизация агента

Перед авторизацией агента в PT ISIM Endpoint необходимо [установить \(см. раздел 7.2.1.2\)](#) его на конечный узел. После установки агент отображается в PT ISIM Endpoint со статусом **Не авторизован**. Для дальнейшей работы с агентом вам нужно авторизовать его путем добавления в группу.

### Добавление агента в группу

Для авторизации агента его нужно добавить в группу, после чего к нему автоматически будут применены политики, назначенные на группу, и модули политик будут установлены на соответствующий ему узел.

► Чтобы добавить агент в группу:

1. В главном меню выберите  **Агенты**.
2. Выберите фильтр **Неавторизованные**.

3. Выберите один или несколько агентов с помощью флажков.
4. Нажмите **Переместить**.
5. В открывшемся окне выберите группу, в которую будет добавлен агент и политики которой будут применены к агенту.
6. Нажмите **Применить**.

Агент авторизован.

## Исключение агента из группы

Если агент был добавлен в группу по ошибке или необходимо остановить работу модулей на конечном устройстве, вы можете исключить агент из группы. При этом на агенте удаляются все модули.

► Чтобы исключить агент из группы:

1. В главном меню выберите  **Агенты**.
2. Выберите один или несколько агентов с помощью флажков.

**Примечание.** Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.

3. Нажмите **Переместить**.
4. Выберите **Без группы**.
5. Нажмите **Применить**.

## Перемещение агента в другую группу

Если на агенте требуется изменить набор модулей или их конфигурацию, вы можете переместить агент в другую группу. При этом с него удаляются все модули политик, назначенных на исходную группу. Затем на агент будут установлены модули политик, назначенных на группу, в которую его переместили.

► Чтобы переместить агент в другую группу:

1. В главном меню выберите  **Агенты**.
2. Выберите один или несколько агентов с помощью флажков.

**Примечание.** Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.

3. Нажмите **Переместить**.
4. Выберите группу, в которую вы хотите добавить агент, или введите название новой группы.
5. Нажмите **Применить**.

### 7.2.1.4. Обновление агента

Если для агента доступно обновление, то его версия в таблице будет выделена желтым цветом. Вы можете обновлять только авторизованные агенты.

► Чтобы обновить агент:

1. В главном меню выберите  **Агенты**.
2. Выберите агент.

**Примечание.** Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.

3. Нажмите **Обновить агент**.

Запустится обновление агента. После успешного обновления в таблице будет указана его новая версия.

**Примечание.** Если агент отключен, то он будет обновлен после подключения.

### 7.2.1.5. Блокировка агента

Если в систему добавляется неизвестный агент или поведение авторизованного агента стало подозрительным, вы можете заблокировать агент. При блокировке авторизованного агента на нем удаляются все модули. В дальнейшем вы можете авторизовать заблокированные агенты, добавив их в группу.

► Чтобы заблокировать агент:

1. В главном меню выберите  **Агенты**.
2. Нажмите на название агента.

**Примечание.** Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.

3. Нажмите  → **Заблокировать**.

### 7.2.1.6. Удаление агента

В этом разделе приведены инструкции по удалению агента из PT ISIM Endpoint и с конечного устройства.

#### Удаление агента из PT ISIM Endpoint

Вы можете удалить агент из PT ISIM Endpoint, например если он продолжительное время отключен или был добавлен в группу по ошибке. При удалении агента из PT ISIM Endpoint он не удаляется с конечного устройства.

► Чтобы удалить агент из PT ISIM Endpoint:

1. В главном меню выберите  **Агенты**.
2. Выберите агент.

**Примечание.** Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.

3. Нажмите .

**Примечание.** Вы также можете удалить агент, нажав на название агента, а затем нажав  → **Удалить**.

Если после удаления из PT ISIM Endpoint агент начнет присылать данные, то он автоматически будет добавлен обратно со статусом **Не авторизован**. При удалении агента из PT ISIM Endpoint на нем удаляются все модули.

## Удаление агента с конечного устройства

Если на конечном устройстве установлен драйвер самозащиты, то удалить агент невозможно. Перед удалением агента нужно отключить самозащиту.

► Чтобы удалить агент в Windows:

1. Нажмите **Пуск** → **Приложения и возможности**.
2. В списке установленных программ выберите **Positive Technologies ISIM EDR Agent** и нажмите **Удалить**.

Откроется окно мастера удаления агента.

3. Нажмите **Удалить**.

► Чтобы удалить агент в Linux,

выполните одно из следующих действий:

- если агент был установлен из deb-пакета, выполните команду `dpkg --purge vxagent;`
- если агент был установлен из RPM-пакета, выполните команду `rpm -e vxagent;`
- если агент был установлен из RPM-пакета в ОС «Альт Сервер», выполните команду `apt-get remove --purge vxagent.`

## 7.2.2. Работа с политиками

В этом разделе приведены инструкции по работе с политиками.

## Создание политики на основе шаблона

► Чтобы создать политику на основе шаблона:

1. В главном меню выберите  **Политики**.
2. Нажмите **+**.
3. Выберите шаблон.
4. Введите название политики.
5. Если требуется, добавьте метки и описание.
6. Выберите версии модулей для автоматического обновления или отключите его.
7. Нажмите **Сохранить**.

## Назначение политики на группы агентов

► Чтобы назначить политику на группы агентов:

1. В главном меню выберите  **Политики**.
2. Выберите вкладку **Группы**.
3. Выполните одно из следующих действий:
  - Если политика еще не назначена на группы, нажмите **Назначить**.
  - Если политика уже назначена на некоторые группы, нажмите **Назначить на группы**.
4. Выберите одну или несколько групп.
5. Нажмите **Назначить**.

## Назначение политик на группу агентов

► Чтобы назначить политики на группу агентов:

1. В главном меню выберите  **Группы агентов**.
2. Выберите вкладку **Политики**.
3. Выполните одно из следующих действий:
  - Если на группу еще не назначены политики, нажмите **Назначить**.
  - Если на группу назначены некоторые политики, нажмите **+**.
4. Выберите одну или несколько политик.
5. Нажмите **Назначить**.

## 7.2.3. Настройка промышленной экспертизы

PT ISIM позволяет отслеживать события безопасности на конечных узлах с промышленным ПО следующих производителей:

- «Атомик Софт» (Alpha.Platform);
- «МПС Софт» (MasterSCADA);
- «Прософт-Системы» (Astra Regul, Redkit);
- AdAstra (Trace Mode);
- AVEVA (Wonderware) System Platform;
- Honeywell (Experion PKS);
- Siemens (SIMATIC WinCC, SIMATIC PCS 7);
- Yokogawa (CENTUM, ProSafe-RS).

Пакеты промышленной экспертизы представляют собой модули с правилами для выявления событий безопасности на конечных узлах сети с учетом особенностей установленного промышленного ПО.

Модули добавлены в шаблоны политик PT ISIM Endpoint и включаются в политику при ее [создании по шаблону \(см. раздел 7.2.2\)](#). Модули в составе политики автоматически устанавливаются на конечные узлы, входящие в группу агентов, на которую назначена политика.

Для работы пакета промышленной экспертизы необходимо:

- создать политику сбора данных;
- создать политику обнаружения угроз;
- создать политику конфигулятора аудита (только для узлов с Windows);
- [назначить созданные политики на группы агентов \(см. раздел 7.2.2\)](#), которые установлены на конечные узлы с промышленным ПО.

Кроме того, может потребоваться настройка конечных узлов. Например, на конечных узлах под управлением Windows требуется настройка расширенного аудита файловой системы.

Далее приведено описание настройки PT ISIM Endpoint и конечных узлов для работы пакетов промышленной экспертизы.

### В этом разделе

[Пакет экспертизы для ПО «Атомик Софт» \(см. раздел 7.2.3.1\)](#)

[Пакет экспертизы для ПО «МПС Софт» \(см. раздел 7.2.3.2\)](#)

[Пакет экспертизы для ПО AdAstra \(см. раздел 7.2.3.3\)](#)

[Пакет экспертизы для ПО AVEVA \(см. раздел 7.2.3.4\)](#)

[Пакет экспертизы для ПО Honeywell \(см. раздел 7.2.3.5\)](#)

[Пакет экспертизы для ПО Siemens \(см. раздел 7.2.3.6\)](#)

[Пакет экспертизы для ПО Yokogawa \(см. раздел 7.2.3.7\)](#)

[Настройка аудита файловой системы для папки Windows \(см. раздел 7.2.3.8\)](#)

### 7.2.3.1. Пакет экспертизы для ПО «Атомик Софт»

Пакет включает экспертизу для обнаружения событий информационной безопасности на конечных узлах под управлением Windows и Linux для ПО Alpha.Platform в части следующих компонентов:

- Alpha.Alarms;
- Alpha.Historian;
- Alpha.HMI;
- Alpha.Server;
- Alpha.Security;
- Alpha.Trends.

**Примечание.** Описание инцидентов, регистрируемых в PT ISIM View Sensor по результатам работы пакетов промышленной экспертизы, приведено в Руководстве пользователя в разделе «Источники данных» — «Промышленное ПО».

### Создание политики для сбора данных с узлов под управлением Windows

Для сбора данных с узлов под управлением Windows необходимо в PT ISIM Endpoint [создать политику \(см. раздел 7.2.2\)](#) на основе шаблона «Сбор данных с AutomiQ Alpha.Platform (Windows)».

Дополнительная настройка политики не требуется.

### Создание политики для сбора данных с узлов под управлением Linux

Для сбора данных с узлов под управлением Linux необходимо в PT ISIM Endpoint [создать политику \(см. раздел 7.2.2\)](#) на основе шаблона «Сбор данных с AutomiQ Alpha.Platform (Linux)».

Если компонент Alpha.HMI установлен на узле под управлением Linux или если базы данных Alpha.Historian расположены в каталоге, отличном от `/opt/AutomiQ/`, необходимо настроить созданную политику.

► Чтобы настроить политику:

1. В PT ISIM Endpoint на странице  **Политики** выберите созданную политику.
2. На вкладке **Модули** выберите модуль «Установщик auditd».
3. В блоке **Основные параметры** в поле **Правила** внесите изменения:
  - Если компонент Alpha.HMI установлен на узле под управлением Linux, добавьте строку  
`-w <Путь к файлам проекта Alpha.HMI> -p wa -k ptsiem_automiq_alpha_files_modify.`
  - Если базы данных Alpha.Historian расположены в каталоге, отличном от /opt/Automiq/, добавьте строку  
`-w <Путь к базам данных Alpha.Historian> -p wa -k ptsiem_automiq_alpha_files_modify.`
4. Нажмите **Сохранить**.

## Создание политики обнаружения угроз

В PT ISIM Endpoint для обнаружения угроз на конечных узлах под управлением Windows необходимо [создать политику](#) (см. раздел 7.2.2) на основе шаблона «Обнаружение угроз (Windows)», а для обнаружения угроз на конечных узлах под управлением Linux — политику на основе шаблона «Обнаружение угроз (Linux)».

## Создание политики конфигулятора аудита

В PT ISIM Endpoint для конечных узлов под управлением Windows необходимо [создать политику](#) (см. раздел 7.2.2) конфигулятора аудита на основе шаблона «Конфигуратор аудита Windows».

## Настройка конечного узла под управлением Windows

Для контроля файлов ПО необходимо [настроить аудит файловой системы](#) (см. раздел 7.2.3.8) на конечном узле для каждой из следующих папок (указано расположение по умолчанию):

- C:\Program Files\Automiq;
- C:\Program Files (x86)\Automiq;
- C:\ProgramData\AlphaPlatform;
- C:\ProgramData\Automiq Software;
- C:\Users\All Users\AlphaPlatform;
- C:\Users\All Users\Automiq Software;
- C:\Program Files\OpenLDAP;

- для папки с базами данных Alpha.Historian — указаны в файле `Alpha.Historian.Server.xml` (расположен в папке, в которой установлен Alpha.Historian);
- папки с файлами проекта Alpha.HMI.

### 7.2.3.2. Пакет экспертизы для ПО «МПС Софт»

Пакет включает экспертизу для обнаружения событий информационной безопасности на конечных узлах под управлением Windows и Linux для ПО MasterSCADA.

**Примечание.** Описание инцидентов, регистрируемых в PT ISIM View Sensor по результатам работы пакетов промышленной экспертизы, приведено в Руководстве пользователя в разделе «Источники данных» — «Промышленное ПО».

### Создание политики для сбора данных с узлов под управлением Windows

Для сбора данных с узлов под управлением Windows с установленным ПО необходимо в PT ISIM Endpoint [создать политику](#) (см. раздел 7.2.2) на основе шаблона «Сбор данных с MasterSCADA (Windows)».

Дополнительная настройка политики не требуется.

### Создание политики для сбора данных с узлов под управлением Linux

Для сбора данных с узлов под управлением Linux с установленным ПО в PT ISIM Endpoint [создать политику](#) (см. раздел 7.2.2) на основе шаблона «Сбор данных с MasterSCADA (Linux)» и настроить ее.

► Чтобы настроить политику:

1. В PT ISIM Endpoint на странице  **Политики** выберите созданную политику.
2. На вкладке **Модули** выберите модуль «Установщик auditd».
3. В блоке **Основные параметры** в поле **Правила** внесите изменения:
  - Если рабочий каталог среды исполнения MasterSCADA 4D отличается от `/opt/mpmc4`, измените строку `-w /opt/mpmc4 -p wa -k pt_siem_mplc4_modify`, указав нужный путь.
  - Если рабочий каталог клиента визуализации MasterSCADA 4D отличается от `/opt/MasterSCADA4DClient-linux-x64`, измените строку `-w /opt/MasterSCADA4DClient-linux-x64 -p wa -k pt_siem_ms4d_client_modify`, указав нужный путь.
  - Если рабочий каталог монитора MasterSCADA 4D отличается от `/opt/mpmc4_monitor`, измените строку `-w /opt/mpmc4_monitor -p wa -k pt_siem_mplc4_monitor_modify`, указав нужный путь.

- Если каталоги с файлами конфигурации для Multi-Protocol MasterOPC Server отличаются от `/opt/mpsrtfolder/servercfg` и `/opt/mpsrtfolder/serveruacfg`, измените строки `-w /opt/mpsrtfolder/servercfg -p wa -k pt_siem_mps1_modify` и `-w /opt/mpsrtfolder/serveruacfg -p wa -k pt_siem_mps2_modify`, указав нужный путь.
- Если каталоги с файлами конфигурации для Modbus Universal MasterOPC Server отличаются от `/opt/mbsrtfolder/servercfg` и `/opt/mbsrtfolder/serveruacfg`, измените строки `-w /opt/mbsrtfolder/servercfg -p wa -k pt_siem_mbs1_modify` и `-w /opt/mbsrtfolder/serveruacfg -p wa -k pt_siem_mbs2_modify`, указав нужный путь.

4. Нажмите **Сохранить**.

## Создание политики обнаружения угроз

В PT ISIM Endpoint для обнаружения угроз на конечных узлах под управлением Windows необходимо [создать политику](#) (см. раздел 7.2.2) на основе шаблона «Обнаружение угроз (Windows)», а для обнаружения угроз на конечных узлах под управлением Linux — политику на основе шаблона «Обнаружение угроз (Linux)».

## Создание политики конфигулятора аудита

В PT ISIM Endpoint для конечных узлов под управлением Windows необходимо [создать политику](#) (см. раздел 7.2.2) конфигулятора аудита на основе шаблона «Конфигуратор аудита Windows».

## Настройка конечного узла под управлением Windows

Для контроля файлов ПО необходимо на конечном узле [настроить аудит файловой системы](#) (см. раздел 7.2.3.8) для каждой из следующих папок (указано расположение по умолчанию):

- для папки установки программного обеспечения — по умолчанию `C:\Program Files (x86)\MPSSoft` или `C:\Program Files\MPSSoft`;
- папки с файлами проекта MasterSCADA 3 и MasterSCADA 4D;
- папки с конфигурационными файлами MasterOPC Universal Modbus Server и Multi-Protocol MasterOPC Server;
- рабочей папки среды исполнения — по умолчанию `C:\ProgramData\MPSSoft\MasterSCADA4D_RT` или `C:\Users\<user>\AppData\Roaming\MPSSoft\MasterSCADA4D<версия>`.

## Настройка конечного узла под управлением Linux

Дополнительная настройка конечного узла под управлением Linux не требуется.

### 7.2.3.3. Пакет экспертизы для ПО AdAstra

Пакет включает экспертизу для обнаружения событий информационной безопасности на конечных узлах под управлением Windows и Linux для ПО Trace Mode 6.

**Примечание.** Описание инцидентов, регистрируемых в PT ISIM View Sensor по результатам работы пакетов промышленной экспертизы, приведено в Руководстве пользователя в разделе «Источники данных» — «Промышленное ПО».

#### Создание политики для сбора данных с узлов под управлением Windows

Для сбора данных с узлов под управлением Windows необходимо в PT ISIM Endpoint [создать политику](#) (см. раздел 7.2.2) на основе шаблона «Сбор данных с AdAstra Trace Mode 6 (Windows)».

Дополнительная настройка политики не требуется.

#### Создание политики для сбора данных с узлов под управлением Linux

Для сбора данных с узлов под управлением Linux необходимо в PT ISIM Endpoint [создать политику](#) (см. раздел 7.2.2) на основе шаблона «Сбор данных с AdAstra Trace Mode 6 (Linux)» и настроить ее.

► Чтобы настроить политику:

1. В PT ISIM Endpoint на странице  **Политики** выберите созданную политику.
2. На вкладке **Модули** выберите модуль «Установщик auditd».
3. В блоке **Основные параметры** в поле **Правила** добавьте строки:
 

```
-w <Каталог с установленным ПО Trace Mode> -p wa -k pt_siem_tracemode_inst_modify
-w <Каталог с файлами исполняемой среды ПО Trace Mode> -p wa -k
pt_siem_tracemode_pjt_modify
```
4. Нажмите **Сохранить**.

#### Создание политики обнаружения угроз

В PT ISIM Endpoint для обнаружения угроз на конечных узлах под управлением Windows необходимо [создать политику](#) (см. раздел 7.2.2) на основе шаблона «Обнаружение угроз (Windows)», а для обнаружения угроз на конечных узлах под управлением Linux — политику на основе шаблона «Обнаружение угроз (Linux)».

## Создание политики конфигуратора аудита

В PT ISIM Endpoint для конечных узлов под управлением Windows необходимо [создать политику](#) (см. раздел 7.2.2) конфигуратора аудита на основе шаблона «Конфигуратор аудита Windows».

## Настройка конечного узла под управлением Windows

Для контроля файлов ПО необходимо [настроить аудит файловой системы](#) (см. раздел 7.2.3.8) на конечном узле для каждой из следующих папок (указано расположение по умолчанию в зависимости от разрядности ОС):

- для папки установки ПО SCADA Trace Mode:
  - C:\Program Files (x86)\AdAstra Research Group;
  - C:\Program Files\AdAstra Research Group;
- папки с файлами проекта SCADA Trace Mode;
- папки с файлами исполняемой среды SCADA Trace Mode;
- других папок, например с архивными проектами SCADA Trace Mode.

### 7.2.3.4. Пакет экспертизы для ПО AVEVA

Пакет включает экспертизу для обнаружения событий информационной безопасности на конечных узлах под управлением Windows для ПО Wonderware System Platform.

**Примечание.** Описание инцидентов, регистрируемых в PT ISIM View Sensor по результатам работы пакетов промышленной экспертизы, приведено в Руководстве пользователя в разделе «Источники данных» — «Промышленное ПО».

## Создание политики для сбора данных с узлов под управлением Windows

Для сбора данных с узлов под управлением Windows необходимо в PT ISIM Endpoint [создать политику](#) (см. раздел 7.2.2) на основе шаблона «Сбор данных с AVEVA (Wonderware) System Platform».

Дополнительная настройка политики не требуется.

## Создание политики обнаружения угроз

В PT ISIM Endpoint для обнаружения угроз на конечных узлах под управлением Windows необходимо [создать политику](#) (см. раздел 7.2.2) на основе шаблона «Обнаружение угроз (Windows)».

## Создание политики конфигулятора аудита

В PT ISIM Endpoint для конечных узлов под управлением Windows необходимо [создать политику](#) (см. раздел 7.2.2) конфигулятора аудита на основе шаблона «Конфигуратор аудита Windows».

## Настройка конечного узла под управлением Windows

Для контроля файлов ПО необходимо на конечном узле [настроить расширенный аудит файловой системы](#) (см. раздел 7.2.3.8) для следующих папок:

- для папки репозитория проектов — по умолчанию `C:\Program Files (x86)\Archestra\Framework\FileRepository`;
- папки для хранения файлов журналов — по умолчанию `C:\ProgramData\Archestra\LogFiles`.

### 7.2.3.5. Пакет экспертизы для ПО Honeywell

Пакет включает экспертизу для обнаружения событий информационной безопасности на конечных узлах под управлением Windows для ПО Experion PKS (Process Knowledge System) в части следующих компонентов:

- Administer the control strategy database;
- Advanced Parameter Security;
- Configuration Studio;
- Control Builder;
- HMIWeb Display Builder;
- IEC61850 System Configurator;
- System Configuration.

**Примечание.** Описание инцидентов, регистрируемых в PT ISIM View Sensor по результатам работы пакетов промышленной экспертизы, приведено в Руководстве пользователя в разделе «Источники данных» — «Промышленное ПО».

## Создание политики для сбора данных с узлов под управлением Windows

Для сбора данных с узлов с установленным ПО необходимо в PT ISIM Endpoint [создать политику](#) (см. раздел 7.2.2) на основе шаблона «Сбор данных с Honeywell Experion PKS».

Дополнительная настройка политики не требуется.

## Создание политики обнаружения угроз

В PT ISIM Endpoint для обнаружения угроз на конечных узлах под управлением Windows необходимо [создать политику](#) (см. раздел 7.2.2) на основе шаблона «Обнаружение угроз (Windows)».

## Создание политики конфигулятора аудита

В PT ISIM Endpoint для конечных узлов под управлением Windows необходимо [создать политику](#) (см. раздел 7.2.2) конфигулятора аудита на основе шаблона «Конфигуратор аудита Windows».

## Настройка конечного узла под управлением Windows

Для контроля файлов ПО необходимо [настроить аудит файловой системы](#) (см. раздел 7.2.3.8) на конечном узле для следующих папок (указаны пути по умолчанию):

- для папок с файлами конфигурации системы Experion PKS:
  - C:\ProgramData\Honeywell\Experion PKS\Server\data\mapping;
  - C:\ProgramData\Honeywell\Experion PKS\Client\Advanced Parameter Security;
  - C:\ProgramData\Honeywell\Experion PKS\IEC61850\Configuration;
  - C:\Program Files (x86)\Honeywell\Experion PKS\Client\System\R511;
- папки с экранными формами технологического процесса.

### 7.2.3.6. Пакет экспертизы для ПО Siemens

Пакет включает экспертизу для обнаружения событий информационной безопасности на конечных узлах под управлением Windows для ПО Siemens SIMATIC WinCC, SIMATIC PCS 7 и TIA Portal.

**Примечание.** Описание инцидентов, регистрируемых в PT ISIM View Sensor по результатам работы пакетов промышленной экспертизы, приведено в Руководстве пользователя в разделе «Источники данных» — «Промышленное ПО».

## Создание политики для сбора данных с узлов под управлением Windows

Для сбора данных с узлов с установленным ПО Siemens SIMATIC STEP 7 необходимо в PT ISIM Endpoint [создать политику](#) (см. раздел 7.2.2) на основе шаблона «Сбор данных с Siemens SIMATIC STEP 7», для сбора данных с узлов с установленным ПО Siemens SIMATIC WinCC — политику на основе шаблона «Сбор данных с Siemens SIMATIC WinCC», для сбора данных с узлов с установленным ПО Siemens TIA Portal — политику на основе шаблона «Сбор данных с Siemens TIA Portal».

Дополнительная настройка политики не требуется.

## Создание политики обнаружения угроз

В PT ISIM Endpoint для обнаружения угроз на конечных узлах под управлением Windows необходимо [создать политику](#) (см. раздел 7.2.2) на основе шаблона «Обнаружение угроз (Windows)».

## Создание политики конфигулятора аудита

В PT ISIM Endpoint для конечных узлов под управлением Windows необходимо [создать политику](#) (см. раздел 7.2.2) конфигулятора аудита на основе шаблона «Конфигуратор аудита Windows».

## Настройка конечного узла под управлением Windows

Для контроля файлов ПО необходимо [настроить аудит файловой системы](#) (см. раздел 7.2.3.8) на конечном узле для следующих папок:

- C:\Program Files (x86)\Siemens\Step7\S7BIN — для Siemens SIMATIC STEP 7;
- C:\Program Files (x86)\Siemens\WinCC\bin — для Siemens SIMATIC WinCC;
- папок с файлами проектов WinCC, которые необходимо контролировать, — для Siemens SIMATIC WinCC;
- C:\Program Files\Siemens\Automation\Portal V<Номер версии>\Bin — для Siemens TIA Portal.

### 7.2.3.7. Пакет экспертизы для ПО Yokogawa

Пакет включает экспертизу для обнаружения событий информационной безопасности на конечных узлах под управлением Windows для ПО Yokogawa — распределенной системы управления CENTUM VP и системы противоаварийной защиты ProSafe-RS.

**Примечание.** Описание инцидентов, регистрируемых в PT ISIM View Sensor по результатам работы пакетов промышленной экспертизы, приведено в Руководстве пользователя в разделе «Источники данных» — «Промышленное ПО».

## Создание политики для сбора данных с узлов под управлением Windows

Для сбора данных с узлов с установленным ПО необходимо в PT ISIM Endpoint [создать политику](#) (см. раздел 7.2.2) на основе шаблона «Сбор данных с Yokogawa».

Дополнительная настройка политики не требуется.

## Создание политики обнаружения угроз

В PT ISIM Endpoint для обнаружения угроз на конечных узлах под управлением Windows необходимо [создать политику \(см. раздел 7.2.2\)](#) на основе шаблона «Обнаружение угроз (Windows)».

## Создание политики конфигулятора аудита

В PT ISIM Endpoint для конечных узлов под управлением Windows необходимо [создать политику \(см. раздел 7.2.2\)](#) конфигулятора аудита на основе шаблона «Конфигуратор аудита Windows».

## Настройка конечного узла под управлением Windows

Для контроля файлов ПО необходимо [настроить аудит файловой системы \(см. раздел 7.2.3.8\)](#) на конечном узле для следующих папок:

- для папок установки программного обеспечения (указано расположение по умолчанию):
  - C:\CENTUMVP;
  - C:\Program Files (x86)\Yokogawa;
  - C:\Program Files\Yokogawa;
  - C:\ProgramData\Yokogawa;
  - C:\Program Files (x86)\ProSafe-RS;
- папки с файлами проекта ПО;
- других папок, например с архивными проектами ПО.

### 7.2.3.8. Настройка аудита файловой системы для папки Windows

► Чтобы настроить аудит файловой системы для папки:

1. В контекстном меню папки выберите **Свойства**.
2. Выберите вкладку **Безопасность**.
3. Нажмите **Дополнительно**.
4. Выберите вкладку **Аудит**.
5. Нажмите **Добавить**.
6. Нажмите **Выберите субъект**.
7. В поле **Введите имена выбираемых объектов** введите название группы пользователей **Все**.

**Примечание.** Вы можете проверить корректность ввода названия, нажав **Проверить имена**.

8. Нажмите **ОК**.
9. В раскрывающемся списке **Тип** выберите вариант **Успех**.
10. В раскрывающемся списке **Применить к** выберите вариант **Для этой папки, ее подпапок и файлов**.
11. По ссылке **Отображение дополнительных разрешений** откройте список дополнительных разрешений.
12. Нажмите **Очистить все**.
13. Установите флажки **Траверс папок / выполнение файлов**, **Содержание папки / чтение данных**, **Создание файлов / запись данных**, **Создание папок / дозапись данных**, **Удаление подпапок и файлов**, **Удаление**.

Субъект: Все Выберите субъект

Тип: Успех

Применяется к: Для этой папки, ее подпапок и файлов

Дополнительные разрешения:

|                                                                       |                                                                |
|-----------------------------------------------------------------------|----------------------------------------------------------------|
| <input type="checkbox"/> Полный доступ                                | <input type="checkbox"/> Запись атрибутов                      |
| <input checked="" type="checkbox"/> Траверс папок / выполнение файлов | <input type="checkbox"/> Запись дополнительных атрибутов       |
| <input checked="" type="checkbox"/> Содержание папки / чтение данных  | <input checked="" type="checkbox"/> Удаление подпапок и файлов |
| <input type="checkbox"/> Чтение атрибутов                             | <input checked="" type="checkbox"/> Удаление                   |
| <input type="checkbox"/> Чтение дополнительных атрибутов              | <input type="checkbox"/> Чтение разрешений                     |
| <input checked="" type="checkbox"/> Создание файлов / запись данных   | <input type="checkbox"/> Смена разрешений                      |
| <input checked="" type="checkbox"/> Создание папок / дозапись данных  | <input type="checkbox"/> Смена владельца                       |

☐ Применять эти параметры аудита к объектам и контейнерам только внутри этого контейнера

Очистить все

ОК Отмена

Рисунок 50. Настройка расширенного аудита файловой системы для папки в Windows

14. Нажмите **ОК**.
15. В окне **Дополнительные параметры безопасности для <Название файла>** нажмите **ОК**.
16. В окне **Свойства <Название файла>** нажмите **ОК**.

## 7.2.4. Настройка сканирования в режиме аудита

В PT ISIM Endpoint вы можете настроить сканирование в режиме аудита на конечном узле. Модуль сканирования определяет конфигурацию узла (перечень установленного и удаленного программного обеспечения, характеристики аппаратного обеспечения, перечень и параметры учетных записей пользователей и групп, а также других данные о системе, включая перечень политик и служб) и передает данные о конфигурации в PT ISIM View Sensor напрямую или через коллектор.

На конечном узле должен быть [установлен \(см. раздел 7.2.1.2\)](#) агент и [авторизован \(см. раздел 7.2.1.3\)](#) в PT ISIM Endpoint.

**Примечание.** Сканирование для определения конфигурации узла также может быть выполнено безагентным способом с помощью сетевого сканера. Инструкции по работе с ним приведены в Руководстве пользователя PT ISIM в разделе «Работа с задачами на сбор данных».

► Чтобы настроить в PT ISIM Endpoint сканирование в режиме аудита на узле:

1. В главном меню выберите  **Политики**.
2. Нажмите **+**.
3. Введите название политики.
4. Нажмите **Создать**.
5. Выберите вкладку **Модули**.
6. Нажмите **Добавить** и в открывшемся окне выберите модуль «Сканирование в режиме аудита (ISIM VM)».
7. Нажмите **Добавить**.  
Политика с модулем для сканирования в режиме аудита добавлена в PT ISIM Endpoint.
8. В выпадающем списке **Версия MaxPatrol 10** выберите значение **27.6**.
9. В блоке параметров **Частичный сбор данных** очистите поле **Маски модели активов для сбора данных**.
10. Если требуется, в блоке параметров **Расписание** настройте расписание. Вы также можете запускать сканирование вручную.
11. Нажмите **Сохранить**.
12. [Назначьте политику на группы агентов \(см. раздел 7.2.2\)](#), на которых необходимо выполнять сканирование в режиме аудита.

► Чтобы запустить сканирование вручную на одном агенте:

1. В главном меню выберите  **Агенты**.
2. Напротив нужного агента нажмите .
3. Нажмите **Сканировать узел в режиме аудита**.
4. Нажмите **Запустить сканирование**.

Сканирование запущено. Вы можете остановить сканирование по кнопке **Остановить сканирование**.

Скачать журнал работы модуля вы можете по кнопке **Скачать журнал модуля**.

► Чтобы запустить сканирование вручную на всех агентах группы:

1. В главном меню выберите  **Группы агентов**.
2. Нажмите на название группы, на агентах которой вы хотите запустить сканирование.
3. Выберите вкладку **Политики**.
4. Выберите модуль «Сканирование в режиме аудита (ISIM VM)».
5. Нажмите **Операции** и выберите управляющий сервер.
6. Нажмите **Запустить сканирование в группе**.

Сканирование на агенте из группы не будет запущено, если с ним нет связи или на нем уже выполняется сканирование.

## 7.2.5. Настройка антивирусной защиты узлов

Вы можете настроить антивирусную защиту конечного узла в PT ISIM Endpoint, установив на агент модуль «Антивирус». Этот модуль позволяет обнаруживать вирусы и вредоносные программы в операционной системе. Для полноценной работы антивируса на агенте также должен быть установлен модуль «Доставщик антивирусных баз». Антивирусная проверка выполняется автоматически при операциях с файлами на конечном узле, а также может запускаться вручную или автоматически по расписанию.

Модуль устанавливает на конечном устройстве службу и драйвер антивируса, которые работают независимо от соединения с PT ISIM Endpoint. Удалить антивирус на узле можно только из интерфейса PT ISIM Endpoint.

**Внимание!** В текущей версии PT ISIM Endpoint модуль «Антивирус» представлен в предварительной версии и может содержать ошибки. Если антивирус работает нестабильно или некорректно, временно отключите модуль в политике и сообщите об этом в службу технической поддержки Positive Technologies.

Результаты работы антивируса отображаются в PT ISIM View Sensor в виде соответствующих событий и инцидентов. Отслеживаются обнаружение и блокировка вредоносных объектов, попытки отключить антивирус, ошибки проверки объектов и другие события.

## Установка антивируса

На конечном узле должен быть [установлен \(см. раздел 7.2.1.2\)](#) агент и [авторизован \(см. раздел 7.2.1.3\)](#) в PT ISIM Endpoint.

► Чтобы настроить антивирусную защиту на конечном узле:

1. В главном меню выберите  **Политики**.
  2. Нажмите **+**.
  3. Введите название политики.
  4. Нажмите **Создать**.
  5. Выберите вкладку **Модули**.
  6. Нажмите **Добавить**.
  7. Выберите модули «Антивирус», «Доставщик антивирусных баз» и «Доставщик драйвера модулей».
  8. Нажмите **Сохранить**.
  9. Если требуется, в блоке параметров **Проверки по расписанию** настройте расписание. Вы также можете запускать сканирование вручную.
- Примечание.** Вы можете настроить несколько расписаний, например для полной проверки в выходные и быстрой проверки в будние дни.
10. [Назначьте созданную политику на группу агентов \(см. раздел 7.2.2\)](#), на которых необходимо установить антивирусную защиту.

Модуль будет автоматически установлен на всех агентах группы.

## Действия на конечном узле

В PT ISIM Endpoint на странице модуля «Антивирус» на агенте доступны следующие действия:

- Запуск антивирусной проверки на узле с выбором типа проверки. Доступны следующие типы проверки:
  - быстрая (проверка важных системных файлов, выбранных экспертами Positive Technologies);
  - полная (проверка всех файлов и объектов в оперативной памяти на конечном узле);
  - проверка файла;
  - проверка папки;
  - проверка оперативной памяти и автоматически запускаемых файлов.
- Включение и отключение антивируса.

- Включение и отключение самозащиты.
- Удаление и повторная установка антивируса. Вы также можете удалить антивирус, отключив или удалив модуль из политики.
- Чтобы в PT ISIM Endpoint открыть страницу модуля «Антивирус», установленного на агенте:
  1. В главном меню выберите  **Агенты**.
  2. Нажмите .
  3. В панели фильтрации выберите **Модули** → **Антивирус** и нажмите **Применить**.
  4. В столбце **Модули** для выбранного агента нажмите **Антивирус**.

Откроется страница модуля на агенте с операциями, доступными для выполнения.

## 7.2.6. Изоляция подозрительных файлов

Вы можете настроить изоляцию подозрительных файлов на конечных узлах с помощью модуля «Карантин». Модуль изолирует подозрительные файлы в зашифрованном хранилище на время их проверки с помощью модулей «YARA-сканер» или «Проверка файлов в PT Sandbox», входящих в шаблонные политики «Обнаружение угроз (Windows)» и «Обнаружение угроз (Linux)». При этом в карантин помещается не сам файл, а его копия. Из-за этого в целях безопасности исходный файл рекомендуется удалять модулем «Удаление файла».

На конечном узле должен быть [установлен \(см. раздел 7.2.1.2\)](#) агент и [авторизован \(см. раздел 7.2.1.3\)](#) в PT ISIM Endpoint.

- Чтобы настроить изоляцию подозрительных файлов:
  1. В главном меню выберите  **Политики**.
  2. Нажмите .
  3. Введите название политики.
  4. Нажмите **Создать**.
  5. Выберите вкладку **Модули**.
  6. Нажмите **Добавить**.
  7. Выберите модуль «Карантин».
  8. Нажмите **Добавить**.
  9. Настройте параметры модуля.
  10. Нажмите **Сохранить**.
  11. Настройте автоматическое реагирование, назначив действия модуля «Карантин» на события других модулей.

**Примечание.** На страницах политик на вкладке **Модули** в блоке параметров **События** вы можете назначать действия на события модулей вручную или с помощью мастера назначения действий. Например, на странице модуля «Антивирус» на событие «Файл проверен антивирусом. Вердикт: вредоносный» вы можете назначить действие «Поместить копию файла-объекта в карантин» для дальнейшего анализа файла.

12. **Назначьте созданную политику на группы агентов (см. раздел 7.2.2)**, на которых необходимо выполнять изоляцию подозрительных файлов.

Модуль будет автоматически установлен на всех агентах групп.

Таблица 32. Параметры модуля «Карантин»

| Параметр или блок параметров                     | Описание                                                                                                                |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Пароль для архива</b>                         | Пароль, который будет установлен для скачанного из карантина архива с файлами                                           |
| <b>Исключения → Папки и файлы</b>                | Путь до файла или путь до папки, файлы в которой не будут помещаться в карантин                                         |
| <b>Исключения для расширений файлов</b>          | Список расширений файлов, которые не будут помещаться в карантин                                                        |
| <b>Максимальный размер файла в карантине, МБ</b> | Максимальный размер файла, который может быть помещен в карантин (в мегабайтах)                                         |
| <b>Размер хранилища, МБ</b>                      | Размер хранилища файлов в карантине (в мегабайтах). При заполнении хранилища из него будут удаляться самые старые файлы |
| <b>Запасная папка для восстановления</b>         | Папка, в которую будет восстановлен файл, если его невозможно восстановить в изначальную папку                          |

## 7.3. Администрирование PT ISIM Collector

В этом разделе содержатся инструкции по администрированию PT ISIM Collector.

**Внимание!** Компонент (см. раздел 2.1) PT ISIM Collector не имеет собственного веб-интерфейса. Настройка работы коллекторов выполняется в веб-интерфейсе PT ISIM View Sensor.

**Примечание.** Работа с коллекторами доступна в редакциях PT ISIM proView Sensor и PT ISIM netView Sensor.

Просмотр информации о коллекторах в PT ISIM View Sensor описан в разделе «Работа с PT ISIM Collector» Руководства пользователя PT ISIM.

После установки коллектора для настройки его работы нужно:

- [активировать лицензию \(см. раздел 5.5.3\)](#) коллектора;
- если в PT ISIM View Sensor отключен прием данных от коллектора, [включить его \(см. раздел 7.3.1\)](#);
- [добавить коллектор \(см. раздел 7.3.2\)](#) в PT ISIM View Sensor;
- в PT ISIM View Sensor [скачать конфигурацию \(см. раздел 7.3.4\)](#) с параметрами передачи данных;
- [загрузить \(см. раздел 7.3.5\)](#) конфигурацию на коллектор;
- если требуется, [настроить \(см. раздел 7.3.6\)](#) прием данных от PT ISIM Endpoint.

В дальнейшем может потребоваться повторная загрузка конфигурации на коллектор. Например, при изменении параметров коллектора в PT ISIM или при создании, изменении или удалении задачи на сбор данных с конечных устройств с использованием коллектора. В этом случае в PT ISIM View Sensor на странице  → **Коллекторы** для коллектора в поле **Конфигурация на коллекторе** будет отображаться значение **Требуется обновление**.

В журнале действий пользователей (см. раздел 7.1.1.5) PT ISIM View Sensor фиксируются включение, изменение параметров и отключение приема данных от коллекторов, добавление и удаление коллекторов, а также изменение их параметров, включая обновление секретных ключей.

## В этом разделе

[Включение приема данных от коллекторов \(см. раздел 7.3.1\)](#)

[Добавление коллектора в PT ISIM View Sensor \(см. раздел 7.3.2\)](#)

[Обновление секретных ключей \(см. раздел 7.3.3\)](#)

[Скачивание конфигурации коллектора в PT ISIM View Sensor \(см. раздел 7.3.4\)](#)

[Загрузка конфигурации на коллектор \(см. раздел 7.3.5\)](#)

[Настройка коллектора для работы с PT ISIM Endpoint \(см. раздел 7.3.6\)](#)

[Настройка параметров хранения копии трафика на коллекторе \(см. раздел 7.3.7\)](#)

[Удаление коллектора из PT ISIM View Sensor \(см. раздел 7.3.8\)](#)

## 7.3.1. Включение приема данных от коллекторов

► Чтобы включить прием данных от коллекторов:

1. В главном меню выберите  → **Коллекторы**.
2. Нажмите **Настроить прием данных**.
3. В открывшемся окне включите прием данных от коллекторов.

4. В поле **IP-адрес PT ISIM** введите IP-адрес PT ISIM View Sensor, на который коллекторы будут отправлять данные.
5. В поле **Порт PT ISIM** введите порт PT ISIM View Sensor, на который коллекторы будут отправлять данные.

**Примечание.** По умолчанию для подключения к PT ISIM View Sensor используется порт 1888. Вы можете использовать любой порт, не задействованный [в других соединениях \(см. раздел 3.4\)](#). Соединения по указанному порту будут автоматически разрешены с помощью политик iptables.

6. Нажмите **Сохранить**.

Если позже вы отключите прием данных от коллекторов, разрешение соединений по порту, указанному при настройке приема данных, будет автоматически удалено.

Если изменить IP-адрес или порт, на который коллекторы будут передавать данные, после [загрузки конфигурации \(см. раздел 7.3.5\)](#) на коллектор, данные не будут доставляться, пока конфигурация на коллекторе не будет обновлена.

## 7.3.2. Добавление коллектора в PT ISIM View Sensor

**Примечание.** Добавление коллектора доступно, если [включен прием данных от коллектора \(см. раздел 7.3.1\)](#).

► Чтобы добавить коллектор:

1. В главном меню выберите  → **Коллекторы**.
2. Нажмите **Добавить коллектор**.
3. Введите имя коллектора.
4. Выберите канал передачи данных.
5. Введите интервал передачи диагностических данных в секундах.

**Примечание.** Коллектор будет считаться неактивным, если данные от него не были получены в течение трех интервалов подряд.

6. Введите максимальное количество событий в пакете.
7. Введите максимальное время формирования пакета в секундах.
8. Нажмите **Сохранить**.

Коллектор добавлен в PT ISIM View Sensor со статусом **Не активирован**. Для активации коллектора нужно [скачать его конфигурацию \(см. раздел 7.3.4\)](#) и [загрузить \(см. раздел 7.3.5\)](#) на коллектор.

Позже вы можете изменить параметры коллектора в PT ISIM View Sensor. Это потребует повторной [загрузки конфигурации на коллектор \(см. раздел 7.3.5\)](#), если не было изменено только имя коллектора.

### 7.3.3. Обновление секретных ключей

Данные от коллектора к PT ISIM View Sensor передаются в зашифрованном виде. Если требуется остановить прием данных от коллектора, вы можете обновить секретные ключи в PT ISIM View Sensor.

**Внимание!** Для возобновления приема данных после обновления секретных ключей нужно заново [скачать](#) (см. [раздел 7.3.4](#)) конфигурацию и [загрузить](#) (см. [раздел 7.3.5](#)) ее на коллектор.

► Чтобы обновить секретные ключи:

1. В главном меню выберите  → **Коллекторы**.
2. Выберите коллектор.
3. Нажмите  и подтвердите обновление ключей.

### 7.3.4. Скачивание конфигурации коллектора в PT ISIM View Sensor

Конфигурация скачивается в виде ZIP-архива с файлами, которые содержат параметры для настройки передачи данных в PT ISIM View Sensor на коллекторе, а также параметры для сбора данных с конечных устройств при наличии задач на сбор данных с использованием коллектора.

**Примечание.** Скачивание конфигурации доступно, если [включен прием данных от коллектора](#) (см. [раздел 7.3.1](#)).

► Чтобы скачать конфигурацию:

1. В главном меню выберите  → **Коллекторы**.
2. Выберите коллектор.
3. Нажмите **Скачать конфигурацию**.

### 7.3.5. Загрузка конфигурации на коллектор

Активация коллектора выполняется путем загрузки файла конфигурации, предварительно скачанного в PT ISIM View Sensor. При изменении конфигурации коллектора в PT ISIM View Sensor необходимо заново скачать ее и загрузить на коллектор.

**Внимание!** Для загрузки конфигурации на коллектор необходимо повысить привилегии учетной записи до root с помощью команды `sudo su -`.

- Чтобы загрузить конфигурацию на коллектор:

1. Скопируйте файл конфигурации на коллектор.

2. Выполните команду:

```
sudo /opt/ptisim/lib/ptisim-collectorcli/CollectorCli apply-config <Путь к файлу конфигурации>
```

Например, `sudo /opt/ptisim/lib/ptisim-collectorcli/CollectorCli apply-config /root/2_collector_configs_2026-01-20T08_33_14.298Z.zip`.

Начнется загрузка конфигурации. После ее завершения коллектор будет перезагружен.

Коллектор активирован.

## 7.3.6. Настройка коллектора для работы с PT ISIM Endpoint

Коллектор может принимать от PT ISIM Endpoint результаты сканирования конечных узлов и обнаруженные на них события безопасности и передавать их в PT ISIM View Sensor.

**Примечание.** Настройка работы PT ISIM Endpoint для взаимодействия с коллектором аналогична [настройке работы \(см. раздел 5.4.3\)](#) для взаимодействия с PT ISIM View Sensor. [При установке \(см. раздел 5.4.2\)](#) PT ISIM Endpoint в параметрах `isim_address`, `isim_port` и `isim_transport` необходимо указать IP-адрес коллектора и порт и транспортный протокол, используемые при передаче данных коллектору.

- Чтобы настроить коллектор для приема данных от PT ISIM Endpoint,

на узле с PT ISIM Collector в политиках iptables включите порт для прослушивания сервисом `ptisim-rester` входящих сообщений, указав транспортный протокол. Например:

```
/opt/ptisim/bin/rester_port add -p 6192 -t tcp
```

## 7.3.7. Настройка параметров хранения копии трафика на коллекторе

Копия трафика, полученная коллектором, сохраняется на диске в формате PCAP. Вы можете настроить параметры хранения PCAP-файлов — задать расположение PCAP-файлов и максимальный объем, который они могут занимать на диске.

- Чтобы настроить параметры хранения PCAP-файлов,

выполните команду:

```
/opt/ptisim/lib/ptisim-collectorcli/CollectorCli pcaps set-location <Путь к новому каталогу с PCAP-файлами> <Максимальный размер хранилища PCAP в гигабайтах>
```

Вы также можете задать только максимальный размер хранилища PCAP без изменения его расположения.

- ▶ Чтобы задать максимальный объем, который могут занимать PCAP-файлы на диске,

выполните команду:

```
/opt/ptisim/lib/ptisim-collectorcli/CollectorCli pcaps set-limit <Максимальный размер хранилища PCAP в гигабайтах>
```

## 7.3.8. Удаление коллектора из PT ISIM View Sensor

- ▶ Чтобы удалить коллектор из PT ISIM View Sensor:

1. В главном меню выберите  → **Коллекторы**.

2. Выберите коллектор.

Откроется карточка коллектора.

3. Нажмите **Изменить**.

4. Нажмите **Удалить коллектор** и подтвердите удаление.

**Примечание.** Если удаленный коллектор использовался для контроля технологических сигналов, в параметрах сигналов вместо его имени будет использоваться строка вида Коллектор <Идентификатор коллектора>.

## 7.4. Администрирование PT ISIM Overview Center

В этом разделе содержатся инструкции по администрированию PT ISIM Overview Center.

### В этом разделе

[Управление учетными записями пользователей в PT ISIM Overview Center \(см. раздел 7.4.1\)](#)

[Подключение к PT MC \(см. раздел 7.4.2\)](#)

[Настройка провайдера карт в Overview Center \(см. раздел 7.4.3\)](#)

[Настройка отправки сообщений об инцидентах в syslog \(см. раздел 7.4.4\)](#)

[Настройка приемки сообщений об инцидентах на удаленном syslog-сервере \(см. раздел 7.4.5\)](#)

[Изменение информации о системе и контактном лице \(см. раздел 7.4.6\)](#)

[Подключение узлов ISIM к PT ISIM Overview Center \(см. раздел 7.4.7\)](#)

[Утилита резервного копирования \(см. раздел 7.4.8\)](#)

## 7.4.1. Управление учетными записями пользователей в PT ISIM Overview Center

Максимальная длительность сессии пользователя определяется параметрами конфигурации продукта. По истечении этого периода выполняется принудительная деавторизация пользователя, после которой для входа в продукт необходимо заново ввести учетные данные.

**Примечание.** Если пользователь, который был авторизован через PT MC, выйдет из PT ISIM Overview Center, будет выполнен выход из PT MC, а также всех подключенных к нему продуктов в пределах одного браузера.

Когда администратор меняет права доступа пользователя PT MC или блокирует его, изменения применяются не сразу, а спустя время, определяемое параметрами конфигурации PT MC.

Таблица 33. Параметры продолжительности сессии, обновления прав доступа и блокировки пользователя

| Параметр                                                                                                       | Локальный пользователь             | Пользователь PT MC |
|----------------------------------------------------------------------------------------------------------------|------------------------------------|--------------------|
|                                                                                                                | Значение                           |                    |
| Длительность сессии пользователя                                                                               | 14 дней                            |                    |
| Интервал, в течение которого обновятся права доступа пользователя при внесении в них изменений администратором | Сразу после изменения прав доступа | 1 час              |
| Интервал, в течение которого пользователь будет заблокирован при его блокировке администратором                | Сразу после блокировки             | 1 час              |

Далее приводятся инструкции по управлению локальными учетными записями пользователей.

### В этом разделе

[О ролях пользователей \(см. раздел 7.4.1.1\)](#)

[Создание роли \(см. раздел 7.4.1.2\)](#)

[Изменение роли \(см. раздел 7.4.1.3\)](#)

[Настройка доступа к узлам ISIM \(см. раздел 7.4.1.4\)](#)

[Удаление роли \(см. раздел 7.4.1.5\)](#)

[Создание учетной записи пользователя \(см. раздел 7.4.1.6\)](#)

[Изменение учетной записи пользователя \(см. раздел 7.4.1.7\)](#)

[Скачивание журнала действий пользователей \(см. раздел 7.4.1.8\)](#)

[Блокировка учетной записи пользователя \(см. раздел 7.4.1.9\)](#)

[Настройка временной блокировки пользователя при авторизации \(см. раздел 7.4.1.10\)](#)

### 7.4.1.1. О ролях пользователей

В PT ISIM Overview Center используется ролевая модель управления доступом. Роль — это набор привилегий, определяющих права доступа к функциям продукта.

При установке PT ISIM Overview Center по умолчанию создаются роли **Администратор** и **Оператор**, а также учетная запись пользователя с ролью **Администратор** (логин — `administrator`, пароль — `P@ssw0rd`). После первого входа рекомендуется сменить пароль администратора.

Администратор имеет права доступа ко всем функциям продукта. Оператор имеет права только на просмотр данных об узлах и о системе. Вы не можете удалять или изменять эти роли.

Вы можете [создавать собственные роли \(см. раздел 7.4.1.2\)](#), настраивать для них привилегии и назначать роли учетным записям пользователей. Роли действительны только на том Overview Center, на котором они выданы.

**Примечание.** При первом обновлении PT ISIM Overview Center до версии, поддерживающей ролевую модель (4.5 или выше), всем ранее созданным пользователям назначается роль **Администратор**. После обновления рекомендуется [изменить учетные записи пользователей \(см. раздел 7.4.1.7\)](#), назначив роли в соответствии с их полномочиями.

Таблица 34. Ролевая модель доступа пользователей PT ISIM Overview Center

| Привилегия                                         | Описание                                                                                                                                                                                                                                                            | Роль     |               |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------------|
|                                                    |                                                                                                                                                                                                                                                                     | Оператор | Администратор |
| Работа с узлами                                    |                                                                                                                                                                                                                                                                     |          |               |
| Просмотр данных узлов, к которым выдан доступ      | Просмотр данных узлов: общих данных, отображаемых на стартовом экране; инцидентов; нарушений; информации о наличии обновлений для узла.<br><br>В привилегию не входит просмотр истории обновлений узла через Overview Center, а также доступных обновлений для узла | +        | +             |
| Просмотр данных всех узлов                         |                                                                                                                                                                                                                                                                     | +        | +             |
| Регистрация узла и настройка доступа ролей к узлам | Загрузка и удаление пакета регистрации узла; подтверждение регистрации узла; получение уведомления о загрузке нового пакета регистрации узла.                                                                                                                       | —        | +             |

| Привилегия                                | Описание                                                                                                                                                                                                                                                                        | Роль     |               |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------------|
|                                           |                                                                                                                                                                                                                                                                                 | Оператор | Администратор |
|                                           | Привилегия не дает права на просмотр узла после его регистрации                                                                                                                                                                                                                 |          |               |
| Обновление узлов                          | Просмотр доступных обновлений PT ISIM на узлах; обновление и проверка статуса обновления; просмотр истории обновлений, выполненных через Overview Center.<br><br>Просмотр доступных обновлений и их установка возможны только на тех узлах, к которым пользователь имеет доступ | —        | +             |
| <b>Доступ к параметрам системы</b>        |                                                                                                                                                                                                                                                                                 |          |               |
| Просмотр информации о системе             | Просмотр раздела <b>Информация о системе</b> в панели инструментов (версии Overview Center; лицензионного соглашения и документации в формате PDF), а также переход по внешним ссылкам «Справочный центр», «Что нового», «Техническая поддержка» из этого раздела               | +        | +             |
| Настройка параметров системы              | Изменение названия и геолокации узла, данных контактного лица; настройка syslog-сервера; создание пакета регистрации (для регистрации на другом Overview Center); настройка подключения к PT MC и серверу обновлений                                                            | —        | +             |
| <b>Управление пользователями и ролями</b> |                                                                                                                                                                                                                                                                                 |          |               |
| Управление пользователями                 | Просмотр списка пользователей; создание, изменение, блокировка учетной записи пользователя и снятие блокировки; выгрузка журнала действий пользователя Overview Center                                                                                                          | —        | +             |
| Управление ролями                         | Просмотр списка существующих ролей; создание, изменение и удаление роли                                                                                                                                                                                                         | —        | +             |

## 7.4.1.2. Создание роли

► Чтобы создать роль:

1. В панели инструментов нажмите кнопку **Система** и в раскрывшемся меню выберите пункт **Роли**.

Откроется список ролей, созданных в PT ISIM Overview Center.

2. Нажмите кнопку **Добавить роль**.

Откроется карточка новой роли со списком доступных привилегий.

3. В поле **Название роли** введите название.

4. В блоке **Привилегии** установите флажки у привилегий, которые должны быть у создаваемой роли.

5. Нажмите кнопку **Сохранить**.

Роль создана.

## 7.4.1.3. Изменение роли

► Чтобы изменить роль:

1. В панели инструментов нажмите кнопку **Система** и в раскрывшемся меню выберите пункт **Роли**.

Откроется список ролей, созданных в PT ISIM Overview Center.

2. Выберите роль, параметры которой необходимо изменить.

**Примечание.** Изменение параметров ролей **Администратор** и **Оператор** невозможно.

Откроется карточка выбранной роли со списком доступных привилегий.

3. Внесите изменения.

4. Нажмите кнопку **Сохранить**.

Роль изменена.

## 7.4.1.4. Настройка доступа к узлам ISIM

**Примечание.** Доступ к узлам Overview Center не настраивается, они доступны для всех ролей.

Доступ к узлам ISIM настраивается для ролей. Предоставить доступ роли к узлу можно, если у роли есть привилегия **Просмотр данных узлов, к которым выдан доступ**. Роли с привилегией **Просмотр данных всех узлов** имеют доступ ко всем узлам ISIM, настроить доступ вручную для таких ролей невозможно.

Настроить доступ можно как для локальных ролей, так и для созданных в PT MC.

► Чтобы настроить доступ к узлам ISIM:

1. В панели инструментов нажмите кнопку **Система** и в раскрывшемся меню выберите пункт **Доступ к узлам**.
2. Выберите удобный способ группировки: по узлам или по ролям.
3. Выполните одно из следующих действий:
  - Если выбрана группировка по узлам, нажмите значок  в строке с нужным узлом и выберите роли, у которых должен быть доступ к этому узлу.
  - Если выбрана группировка по ролям, нажмите значок  в строке с нужной ролью и выберите узлы, к которым должен быть доступ у этой роли.
4. Нажмите кнопку **Сохранить**.

Доступ к узлам ISIM настроен.

## 7.4.1.5. Удаление роли

► Чтобы удалить роль:

1. В панели инструментов нажмите кнопку **Система** и в раскрывшемся меню выберите пункт **Роли**.

Откроется список ролей, созданных в PT ISIM Overview Center.

2. Выберите роль, которую необходимо удалить.

**Примечание.** Удаление ролей **Администратор** и **Оператор** невозможно.

Откроется карточка выбранной роли со списком доступных привилегий.

3. В правом верхнем углу карточки нажмите кнопку **Удалить**.
4. Подтвердите удаление роли.

Роль удалена.

## 7.4.1.6. Создание учетной записи пользователя

Для предоставления пользователю доступа к веб-интерфейсу PT ISIM Overview Center требуется создать учетную запись пользователя. Впоследствии вы можете заблокировать, но не удалить учетную запись.

► Чтобы создать учетную запись пользователя:

1. В панели инструментов нажмите **Система** → **Пользователи**.

Откроется список пользователей.

2. Нажмите кнопку **Добавить пользователя**.

Откроется карточка нового пользователя.

3. В поле **Логин** введите логин учетной записи.
4. В поле **Пароль** введите пароль учетной записи или нажмите кнопку **Сгенерировать**.
5. В раскрывающемся списке **Роль** выберите роли, которые должны быть назначены пользователю.

Пользователь, которому не назначено ни одной роли, будет иметь доступ только к изменению данных своей учетной записи, а также к выбору языка интерфейса.

6. В поле **Электронная почта** введите адрес электронной почты.
7. В раскрывающемся списке **Статус** выберите значение **Активен**.
8. Нажмите кнопку **Сохранить**.

Учетная запись пользователя создана.

### 7.4.1.7. Изменение учетной записи пользователя

► Чтобы изменить учетную запись пользователя:

1. В панели инструментов нажмите **Система** → **Пользователи**.

Откроется список пользователей.

2. Выберите учетную запись.

Откроется карточка учетной записи.

3. Внесите изменения.
4. Нажмите кнопку **Сохранить**.

Учетная запись пользователя изменена.

### 7.4.1.8. Скачивание журнала действий пользователей

Журнал действий пользователей позволяет отслеживать историю журналируемых действий, совершенных локальными пользователями и пользователями PT MC в интерфейсе PT ISIM Overview Center, в том числе неуспешные операции.

► Чтобы скачать журнал действий пользователей:

1. В панели инструментов нажмите **Система** → **Пользователи**.
2. Нажмите **Скачать журнал действий пользователей**.

### 7.4.1.9. Блокировка учетной записи пользователя

► Чтобы заблокировать учетную запись пользователя:

1. В панели инструментов нажмите **Система** → **Пользователи**.  
Откроется список пользователей.
2. Выберите учетную запись.  
Откроется карточка учетной записи.
3. В раскрывающемся списке **Статус** выберите значение **Заблокирован**.
4. Нажмите кнопку **Сохранить**.

Учетная запись пользователя заблокирована.

### 7.4.1.10. Настройка временной блокировки пользователя при авторизации

Если превышено допустимое количество попыток авторизации, IP-адрес, с которого выполняется вход в PT ISIM Overview Center, временно блокируется. По умолчанию допустимое количество попыток авторизации — 5, длительность блокировки IP-адреса пользователя — 300 секунд.

► Чтобы настроить параметры временной блокировки при авторизации:

1. Откройте файл `/etc/fail2ban/jail.d/system-failed-http-login.conf`, расположенный на сервере с PT ISIM Overview Center.
2. В секции `system-failed-http-login` в параметре `maxretry` введите допустимое количество попыток авторизации пользователя.
3. В секции `system-failed-http-login` в параметре `bantime` введите длительность блокировки в секундах.
4. Перезапустите сервис:

```
systemctl restart fail2ban
```

Временная блокировка пользователя при авторизации настроена.

## 7.4.2. Подключение к PT MC

Positive Technologies Management and Configuration позволяет использовать технологию единого входа для продуктов Positive Technologies. Учетные записи пользователей и роли, созданные в PT MC, синхронизируются с PT ISIM Overview Center при его подключении к PT MC и становятся доступными для входа в PT ISIM Overview Center через PT MC.

Переключение между веб-интерфейсами подключенных к РТ МС приложений доступно по кнопке  в главном меню каждого приложения.

Подробная информация о РТ МС представлена [в справке к продукту](#). Поддерживаемые версии РТ МС указаны [в программных требованиях \(см. раздел 3.2\)](#).

Далее приводятся инструкции по подключению РТ ISIM Overview Center к РТ МС. Если требуется, вы можете также [установить доверенный сертификат \(см. раздел 7.4.2.2\)](#), предоставляемый РТ МС, в РТ ISIM Overview Center.

## В этом разделе

[Настройка подключения РТ ISIM Overview Center к РТ МС \(см. раздел 7.4.2.1\)](#)

[Установка доверенного SSL-сертификата \(см. раздел 7.4.2.2\)](#)

### 7.4.2.1. Настройка подключения РТ ISIM Overview Center к РТ МС

► Чтобы настроить подключение Overview Center к РТ МС:

1. Войдите в РТ ISIM Overview Center с локальной учетной записью пользователя.
2. В панели инструментов нажмите **Система** → **Подключение к РТ МС**.
3. В поле **IP-адрес или URL Overview Center** введите адрес Overview Center, подключаемого к РТ МС.

**Примечание.** Название приложения в РТ МС соответствует имени узла Overview Center.

4. В поле **IP-адрес или FQDN РТ МС** введите адрес РТ МС, к которому необходимо подключиться.
5. В поле **Порт РТ МС** введите порт для подключения к РТ МС.

По умолчанию для подключения к РТ МС используется порт 3334.

6. Нажмите **Подключиться**.

Подключение может занять некоторое время. В РТ МС будет зарегистрировано приложение РТ ISIM Overview Center.

Статус подключения к РТ МС отображается в окне **Подключение к РТ МС**.

Если требуется, вы можете отключиться от РТ МС, нажав **Отключиться**. После отключения пользователи РТ МС не смогут работать в Overview Center.

## 7.4.2.2. Установка доверенного SSL-сертификата

► Чтобы установить доверенный SSL-сертификат в PT ISIM Overview Center:

1. Скопируйте файл SSL-сертификата `/usr/local/share/ca-certificates/deployerCA.crt`, расположенный на сервере PT MC, на сервер PT ISIM Overview Center.
2. В файле `/etc/environment` на сервере PT ISIM Overview Center в переменной окружения `OIDC_VERIFY_SSL` укажите расположение скопированного файла SSL-сертификата `deployerCA.crt` на сервере PT ISIM Overview Center. Например:  
`OIDC_VERIFY_SSL="/ABSOLUTE/PATH/TO/FILE/deployerCA.crt"`
3. Перезапустите PT ISIM Overview Center:  
`systemctl restart ptisim-overview-server.service`

При обновлении PT ISIM Overview Center повторная установка доверенного SSL-сертификата не требуется.

## 7.4.3. Настройка провайдера карт в Overview Center

PT ISIM Overview Center поддерживает три типа карт:

- От онлайн-провайдера — пакет с картой скачивается с внешнего сервера.
- От офлайн-провайдера — пакет с картой хранится на сервере с PT ISIM Overview Center.
- Без провайдера (по умолчанию) — в интерфейсе PT ISIM Overview Center вместо карты отображается серый фон.

Параметры PT ISIM Overview Center, связанные с провайдером карт, хранятся в файлах:

- `/opt/ptisim-overview/etc/map_provider.json`. Файл содержит информацию о выбранном провайдере (раздел `provider_config`) и параметрах карты (раздел `ui_config`). PT ISIM Overview Center обращается к этому файлу при каждом запуске.
- `/etc/nginx/sites-available/ptisim-overview-map.conf`. Файл содержит параметры перенаправления запросов от PT ISIM Overview Center к выбранному провайдеру карты.

Настройка провайдера карт выполняется с помощью утилиты `configure_map`.

► Чтобы получить информацию о текущем провайдере,

выполните команду:

```
/opt/ptisim-overview/bin/configure_map.sh get_provider
```

В консоли отобразится содержимое конфигурационных файлов с информацией о типе провайдера, параметрах карты и настройках проху-запросов через nginx.

- ▶ Чтобы проверить доступность выбранного провайдера и корректность его настройки:

1. Выполните команду:  

```
/opt/ptisim-overview/bin/configure_map.sh test_provider
```
2. Введите тестовое значение уровня масштабирования (**Set zoom level**) и нажмите Enter.
3. Введите тестовую координату по оси X (**Set x**) и нажмите Enter.
4. Введите тестовую координату по оси Y (**Set y**) и нажмите Enter.

Будет выполнен тестовый запрос к nginx на загрузку одного пакета с картой. В консоли отобразится результат проверки.

**Примечание.** Не все онлайн-провайдеры позволяют выполнить данную проверку.

- ▶ Чтобы отключить использование карты любого провайдера:

1. Выполните команду:  

```
/opt/ptisim-overview/bin/configure_map.sh set_provider
```
2. На этапе выбора провайдера (**Select provider type**) введите **no\_provider** и нажмите Enter.

В консоли отобразится подтверждение смены типа провайдера.

## В этом разделе

[Настройка онлайн-провайдера карт \(см. раздел 7.4.3.1\)](#)

[Настройка офлайн-провайдера карт \(см. раздел 7.4.3.2\)](#)

### 7.4.3.1. Настройка онлайн-провайдера карт

При наличии доступа в интернет PT ISIM Overview Center может использовать географическую карту от онлайн-провайдера.

- ▶ Чтобы включить использование карты от онлайн-провайдера:

1. Выполните команду:  

```
/opt/ptisim-overview/bin/configure_map.sh set_provider
```
2. На этапе выбора провайдера (**Select provider type**) введите **online** и нажмите Enter.

**Примечание.** Во всех последующих шагах в квадратных скобках указаны значения по умолчанию для карты от провайдера OpenStreetMap.org. Вы можете нажать Enter для применения каждого из этих значений, и тогда в результате в PT ISIM Overview Center будет использоваться карта от этого провайдера.

3. Введите адрес для загрузки пакета с картой (**Enter URL pattern with \$z, \$x, and \$y placeholders**) и нажмите Enter.

4. Введите минимальное значение уровня масштабирования (**Enter min zoom limit**) и нажмите Enter.
5. Введите максимальное значение уровня масштабирования (**Enter max zoom limit**) и нажмите Enter.
6. Укажите, нужно ли добавлять имя провайдера внизу карты в интерфейсе PT ISIM Overview Center (**Add attributions to the map?**) и нажмите Enter.
7. Введите имя провайдера, которое будет указано внизу карты в виде ссылки (**Enter attribution text in HTML format**) и нажмите Enter.

В консоли отобразится подтверждение смены типа провайдера.

### 7.4.3.2. Настройка офлайн-провайдера карт

Если у PT ISIM Overview Center отсутствует доступ в интернет, вы можете установить географическую карту в виде отдельного пакета.

► Чтобы включить использование карты от офлайн-провайдера:

1. Перенесите пакет с картой на сервер с PT ISIM Overview Center.
2. Выполните команду:  
`/opt/ptisim-overview/bin/configure_map.sh set_provider`
3. На этапе выбора провайдера (**Select provider type**) введите **offline** и нажмите Enter.
4. Укажите путь до локального каталога на сервере с PT ISIM Overview Center, содержащего пакет с картой (**Enter path to tile directory**) и нажмите Enter.

**Примечание.** Внутри каталога должны быть вложенные каталоги для каждого из желаемых уровней масштабирования, содержащие соответствующие пакеты с картой.

В консоли отобразится подтверждение смены типа провайдера.

### 7.4.4. Настройка отправки сообщений об инцидентах в syslog

PT ISIM Overview Center может выступать в качестве источника сообщений о новых инцидентах для syslog-сервера. Для этого вам нужно указать адрес и порт syslog-сервера, на который PT ISIM Overview Center будет отправлять сообщения, и выбрать транспортный протокол для передачи сообщений.

В результате PT ISIM Overview Center будет отправлять в syslog сообщения при каждом обнаружении нового инцидента на подключенных узлах PT ISIM. Сообщения имеют следующий формат:

```
Created incident: id=`<Идентификатор инцидента>` type=`<Тип инцидента>`
progress=`<Текущий этап инцидента>` capacity=`<Общее количество возможных этапов
инцидента>` url=`<Ссылка на инцидент в веб-интерфейсе>` status=`<Статус инцидента>`
```

```
src_ip=`<IP-адрес источника инцидента>` src_mac=`<MAC-адрес источника инцидента>`
dst_ip=`<IP-адрес цели инцидента>` dst_mac=`<MAC-адрес цели инцидента>`
group=`<Группа инцидентов>` start=`<Время начала инцидента>` end=`<Время обновления
инцидента>` incident.severity_level=`<Уровень опасности инцидента>`
incident.name.eng=`<Название инцидента на английском языке>`
incident.name.rus=`<Название инцидента на русском языке>`
```

Например:

```
Created incident: id=`1163` type=`Network_Scan` progress=`1` capacity=`1`
url=`https://10.20.10.100/#/incidents?id=1163` status=`open` src_ip=`10.125.25.100`
src_mac=`2c:56:dc:93:f9:07` dst_ip=`10.60.30.120` dst_mac=`00:1d:a2:af:57:c3`
group=`attack` start=`2022-05-24T07:13:58+00:00` end=`2022-05-24T07:13:58+00:00`
incident.severity_level=`info` incident.name.eng=`Network scan`
incident.name.rus=`Сканирование сети`
```

Вы можете отправлять сообщения об инцидентах в MaxPatrol SIEM, в этом случае в качестве syslog-сервера может выступать узел MP 10 Collector. Со стороны MaxPatrol SIEM необходимо создать и запустить задачу на сбор событий, подробности описаны в разделе «Системы SIEM. Сбор событий» в Справочнике по настройке источников MaxPatrol SIEM. Поддерживаемые версии продукта указаны в [программных требованиях \(см. раздел 3.2\)](#).

► Чтобы настроить отправку сообщений об инцидентах в syslog:

1. В панели инструментов нажмите кнопку **Система** и в раскрывшемся меню выберите пункт **Настройка syslog-сервера**.
2. В поле **Syslog-сервер** введите IP-адрес или доменное имя и порт syslog-сервера.
3. Выберите транспортный протокол для передачи сообщений (TCP или UDP).
4. Нажмите кнопку **Сохранить**.

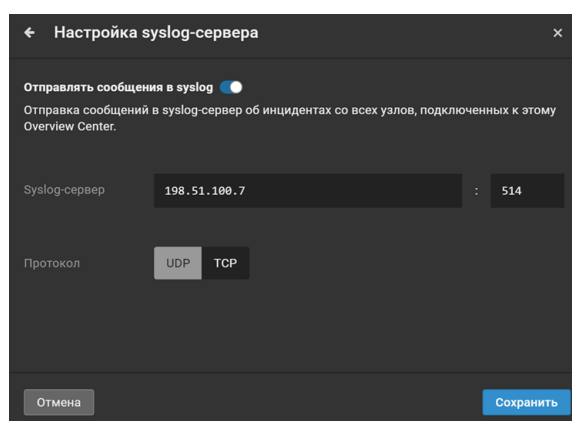


Рисунок 51. Настройка отправки сообщений в syslog

На стороне syslog-сервера требуется также [настроить приемку сообщений \(см. раздел 7.4.5\)](#) от PT ISIM Overview Center.

## 7.4.5. Настройка приемки сообщений об инцидентах на удаленном syslog-сервере

На удаленном syslog-сервере может использоваться служба rsyslog или syslog-ng.

► Чтобы настроить приемку сообщений об инцидентах в службе rsyslog:

1. Откройте файл `/etc/rsyslog.conf`.
2. Если требуется получать сообщения по протоколу UDP, в секции `Modules` раскомментируйте строки:
 

```
#module(load="imudp")
#input(type="imudp" port="514")
```

3. Если требуется получать сообщения по протоколу TCP, в секции `Modules` раскомментируйте строки:
 

```
#module(load="imtcp")
#input(type="imtcp" port="514")
```

Указываемый порт (514 по умолчанию) должен совпадать с портом, указанным в параметрах syslog в веб-интерфейсе PT ISIM Overview Center.

4. Перезапустите службу rsyslog:
 

```
sudo systemctl restart rsyslog
```

Приемка сообщений в службе rsyslog настроена.

► Чтобы настроить приемку сообщений об инцидентах в службе syslog-ng:

1. В каталоге `/etc/syslog-ng/conf.d/` создайте конфигурационный файл `10_events.conf`.
2. Откройте файл `10_events.conf`.
3. Если требуется получать сообщения по протоколу UDP, добавьте в файл следующие строки:
 

```
source s_net { udp(ip(<IP-адрес syslog-сервера>) port(514)); };
log { source(s_net); destination(d_syslog); };
```

4. Если требуется получать сообщения по протоколу TCP, добавьте в файл следующие строки:
 

```
source s_net { tcp(ip(<IP-адрес syslog-сервера>) port(514)); };
log { source(s_net); destination(d_syslog); };
```

Указываемый порт (514 по умолчанию) должен совпадать с портом, указанным в параметрах syslog в веб-интерфейсе PT ISIM Overview Center.

5. Перезапустите службу syslog-ng:
 

```
sudo systemctl restart syslog-ng
```

Приемка сообщений в службе syslog-ng настроена.

## 7.4.6. Изменение информации о системе и контактном лице

Указание информации о системе (названия узла PT ISIM и координат объекта, на котором он установлен) и контактном лице (имени, адреса электронной почты и телефона) является одним из этапов [предварительной настройки продукта](#) (см. раздел 5.6.5.1). Если изменились координаты узла, контактное лицо, его адрес или телефон, вы можете изменить эти данные в веб-интерфейсе PT ISIM Overview Center.

► Чтобы изменить информацию о контактном лице:

1. В панели инструментов нажмите **Система** → **Контактное лицо**.
2. Внесите изменения.
3. Нажмите **Сохранить**.

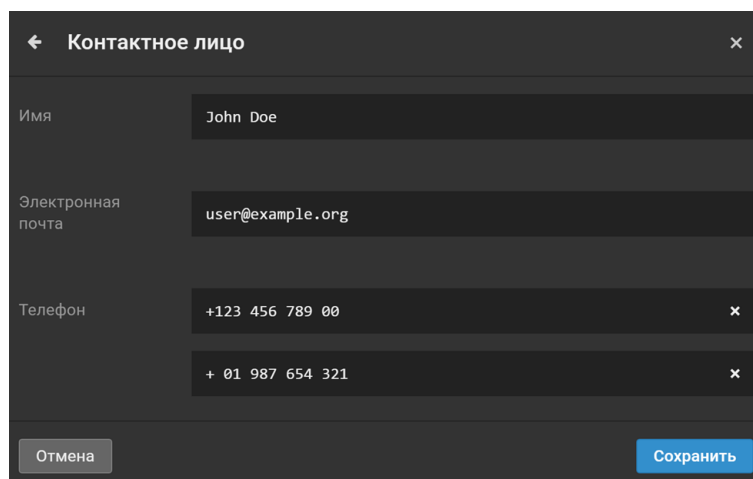


Рисунок 52. Изменение информации о контактном лице

► Чтобы изменить информацию о системе:

1. В панели инструментов нажмите **Система** → **О системе**.
2. Внесите изменения.
3. Нажмите **Сохранить**.

Узел отображается на карте согласно новым координатам, а в структуре узлов ISIM — с новым названием.

## 7.4.7. Подключение узлов ISIM к PT ISIM Overview Center

Чтобы PT ISIM Overview Center мог собирать информацию с узла ISIM, требуется подключить его, активировав пакет регистрации такого узла. Для активации пакета необходимо ввести специальный пароль, заданный на стороне узла ISIM при создании пакета регистрации.

Информация о совместимости версий PT ISIM View Sensor и PT ISIM Overview Center указана [в программных требованиях \(см. раздел 3.2\)](#).

Пакеты регистрации, доступные для активации, отображаются в окне **Подключение узлов ISIM**. Если пакет регистрации был отправлен вам по сети, он автоматически появляется в этом списке. Если пакет регистрации был выгружен в виде JSON-файла, требуется предварительно загрузить его.

Если больше нет необходимости собирать информацию с узла ISIM, вы можете удалить его из PT ISIM Overview Center.

**Примечание.** Чтобы создать многоуровневую иерархию узлов, в PT ISIM Overview Center можно подключать не только узлы ISIM, но и другие узлы Overview Center. Подключение и удаление узлов Overview Center выполняется аналогично подключению узлов ISIM, за исключением настройки доступа. Доступ к узлам ISIM необходимо настроить при подключении, а доступ к узлам Overview Center по умолчанию есть у всех пользовательских ролей и не требует настройки.

## В этом разделе

[Загрузка пакета регистрации \(см. раздел 7.4.7.1\)](#)

[Активация пакета регистрации \(см. раздел 7.4.7.2\)](#)

[Удаление подключенных узлов \(см. раздел 7.4.7.3\)](#)

[Создание пакета регистрации Overview Center \(см. раздел 7.4.7.4\)](#)

### 7.4.7.1. Загрузка пакета регистрации

Если пакет регистрации был передан в виде JSON-файла, требуется загрузить его в PT ISIM Overview Center. Если пакет регистрации был отправлен вам напрямую по сети, загрузка пакета не требуется, вы можете сразу активировать его.

► Чтобы загрузить пакет регистрации:

1. В панели инструментов нажмите кнопку **Узлы ISIM** и в раскрывшемся меню выберите пункт **Подключение узлов ISIM**.
2. Нажмите кнопку **Добавить пакет**.
3. В окне **Загрузка пакета регистрации узла ISIM** нажмите кнопку **Загрузить** и в открывшемся окне выберите пакет регистрации.
4. Нажмите кнопку **Применить**.

Пакет регистрации загружен и отображается в списке на странице **Подключение узлов ISIM**. Теперь вы можете активировать его.

## 7.4.7.2. Активация пакета регистрации

► Чтобы активировать пакет регистрации:

1. В панели инструментов нажмите кнопку **Узлы ISIM** и в раскрывшемся меню выберите пункт **Подключение узлов ISIM**.

Откроется окно со списком доступных для активации пакетов регистрации.

2. Выберите в списке пакет регистрации узла, который вы хотите подключить.
3. В раскрывающемся списке **Роли, имеющие доступ к узлу** выберите роли.
4. В поле **Пароль пакета регистрации** введите пароль, автоматически заданный при создании пакета регистрации.
5. Нажмите кнопку **Подключить узел**.

Подключенные узлы, соединение с которыми устанавливается впервые, в структуре узлов ISIM будут отмечены значком . Общее количество таких узлов отображается в меню **Узлы ISIM**.

PT ISIM Overview Center проверяет сетевую доступность подключенных узлов с помощью периодических запросов к их API. Если узел будет недоступен в течение 10 минут, в структуре узлов ISIM рядом с его именем отобразится значок , а в карточке узла на вкладке **Об узле** — сообщение с указанием времени, когда узел был доступен в последний раз. Количество подключенных узлов, недоступных по сети, отображается в меню **Узлы ISIM**.

**Примечание.** Если вы не хотите активировать пакет регистрации (например, он был отправлен по ошибке или узел ISIM требуется подключить к другому Overview Center), вы можете удалить пакет.

## 7.4.7.3. Удаление подключенных узлов

Интерфейс PT ISIM Overview Center позволяет удалять как подключенные узлы ISIM, так и подключенные узлы Overview Center. Из PT ISIM Overview Center удаляется информация об узле и все его данные, а также дочерние узлы и все их данные (при наличии). При необходимости узлы можно подключить повторно.

**Примечание.** Удаляйте узлы из интерфейса того Overview Center, к которому они подключены напрямую. Иначе при синхронизации удаленные узлы будут добавлены заново.

► Чтобы удалить подключенный узел:

1. В структуре узлов ISIM выберите узел.  
Откроется карточка узла.
2. В правом верхнем углу карточки узла нажмите , в раскрывшемся меню выберите пункт **Удалить узел** или **Удалить узел и его дочерние узлы** и подтвердите удаление.

Удаление займет некоторое время и будет выполняться в фоновом режиме. Изменения в списке узлов отобразятся после обновления страницы.

#### 7.4.7.4. Создание пакета регистрации Overview Center

В анализируемой системе могут использоваться несколько узлов Overview Center, например для разделения доступа к подключенным View Sensor и инцидентам, обнаруженным такими узлами. Если информацию с вашего PT ISIM Overview Center (и подключенных к нему узлов View Sensor View Sensor) требуется передавать на другой Overview Center, вы можете подключить к нему свой PT ISIM Overview Center. Для подключения PT ISIM Overview Center требуется создать его пакет регистрации. Узел, на котором зарегистрирован ваш PT ISIM Overview Center, называется узлом регистрации или вышестоящим узлом.

**Примечание.** Вы можете одновременно зарегистрировать узел ISIM только на одном узле Overview Center. Создание нового пакета регистрации отменяет подключение к предыдущему узлу регистрации.

► Чтобы создать пакет регистрации PT ISIM Overview Center:

1. В панели инструментов нажмите кнопку **Система** и в раскрывшемся меню выберите пункт **Создать пакет регистрации**.

Откроется окно **Создать пакет регистрации**.

Рисунок 53. Создание пакета регистрации

2. В поле **Адрес узла** введите IP-адрес или доменное имя регистрируемого узла ISIM.  
Данный адрес будет использоваться для подключения к регистрируемому узлу ISIM и перехода в его веб-интерфейс.
  3. В поле **Комментарий** опишите процедуру получения пароля к пакету регистрации.
  4. Выберите способ отправки пакета:
    - Для отправки пакета напрямую по сети выберите вариант **По сети**, в поле **Адрес узла регистрации** введите IP-адрес или доменное имя PT ISIM Overview Center, на котором требуется зарегистрировать ваш узел ISIM, и нажмите кнопку **Отправить пакет**. Пакет будет создан и автоматически отправлен на указанный адрес.
    - Для отправки пакета иным способом выберите вариант **Сохранить и отправить самостоятельно** и нажмите кнопку **Сохранить**. Пакет будет выгружен в виде JSON-файла. При этом варианте отправки потребуются самостоятельно загрузить узел в PT ISIM Overview Center, на котором вы хотите зарегистрировать свой узел.
- Откроется окно **Пароль пакета регистрации**.

5. Скопируйте пароль и передайте его получателю пакета регистрации.

6. Нажмите кнопку **Завершить**.

Пакет регистрации создан. Для подключения вашего узла необходимо активировать этот пакет на стороне узла регистрации.

## 7.4.8. Утилита резервного копирования

Утилита резервного копирования предназначена для сохранения и восстановления данных из PT ISIM Overview Center. При использовании утилиты на узлах PT ISIM Overview Center сохраняются данные об инцидентах и таблицы из базы данных PostgreSQL.

**Внимание!** Резервное копирование и восстановление данных должно выполняться на узлах PT ISIM Overview Center с абсолютно одинаковым номером версии и номером сборки. В противном случае данные могут быть потеряны.

### В этом разделе

[Выбор таблиц с инцидентами для резервного копирования \(см. раздел 7.4.8.1\)](#)

[Подключение к СУБД PostgreSQL \(см. раздел 7.4.8.2\)](#)

[Подключение к удаленному узлу по SSH \(см. раздел 7.4.8.3\)](#)

[Снятие резервной копии данных с локального узла Overview Center \(см. раздел 7.4.8.4\)](#)

[Снятие резервной копии данных с удаленного узла Overview Center \(см. раздел 7.4.8.5\)](#)

[Восстановление данных локального узла Overview Center из резервной копии \(см. раздел 7.4.8.6\)](#)

[Восстановление данных удаленного узла Overview Center из резервной копии \(см. раздел 7.4.8.7\)](#)

### 7.4.8.1. Выбор таблиц с инцидентами для резервного копирования

**Внимание!** В резервную копию всегда включаются таблицы `basis_user`, `basis_server`, `basis_overview`, `basis_sensor`, `basis_registration`, `management_licensetoken`, `management_managementsettings`, `overview_incidentdescription`, `overview_node`, `overview_incident`, `overview_overviewsettings`, `overview_violationinfo`, `overview_violation`. Не удаляйте эти стандартные таблицы из списка. Попытка снятия резервной копии данных и их последующее восстановление с неполным списком стандартных таблиц приведет к потере всех данных.

- ▶ Чтобы выбрать таблицы из базы данных PostgreSQL с инцидентами, которые будут включены в резервную копию:
  1. Запустите утилиту, выполнив команду `/opt/ptisim/bin/hammer`.
  2. Выберите **backup settings**.

Откроется меню выбора данных для резервного копирования.
  3. Выберите **setup postgresql**.

Откроется список таблиц с инцидентами, которые будут включены в резервную копию.
  4. Если требуется добавить таблицу в список, выберите **add table** и поочередно укажите значения параметров:
    - **Input name** — название таблицы из базы данных PostgreSQL;
    - **Input id** — индексный столбец таблицы из базы данных PostgreSQL.
  5. Если требуется удалить таблицу из списка, выберите **delete table** и введите номер таблицы в списке.

## 7.4.8.2. Подключение к СУБД PostgreSQL

Подключение утилиты резервного копирования к базе данных PostgreSQL используется для снятия резервной копии таблиц, содержащих в себе информацию об инцидентах, обнаруженных PT ISIM, пользователях PT ISIM и другую техническую информацию.

По умолчанию для подключения к СУБД PostgreSQL используются следующие параметры:

- имя базы данных — `overview`;
- IP-адрес сервера — `127.0.0.1`;
- пароль учетной записи — `ptisim`;
- логин учетной записи — `ptisim`;
- порт — `5432`.

- ▶ Чтобы изменить параметры для подключения к PostgreSQL:
  1. Запустите утилиту, выполнив команду `/opt/ptisim/bin/hammer`.
  2. Выберите **connection settings**.

Откроется меню настройки подключения.
  3. Выберите **postgresql**.
  4. Укажите параметры для подключения:
    - **db** — имя базы данных;
    - **host** — IP-адрес сервера;

- **password** — пароль учетной записи;
- **user** — логин учетной записи;
- **port** — порт.

### 7.4.8.3. Подключение к удаленному узлу по SSH

Подключение по SSH используется для снятия резервной копии данных с удаленного узла Overview Center и их восстановления на этом же удаленном узле.

- ▶ Чтобы настроить параметры подключения утилиты резервного копирования к удаленному узлу по SSH:

1. Запустите утилиту, выполнив команду `/opt/ptisim/bin/hammer`.

2. Выберите **connection settings**.

Откроется меню настройки подключения.

3. Выберите **ssh**.

4. Укажите параметры для подключения:

- **enabled** — состояние подключения утилиты к удаленному узлу (**True** — утилита подключена, **False** — отключена);

**Примечание.** Для работы с удаленным узлом необходимо указать значение **True**. Если будет указано значение **False**, то утилита резервного копирования будет использоваться локально.

- **login** — логин учетной записи;
- **password** — пароль учетной записи;
- **host** — IP-адрес сервера;
- **port** — порт.

5. Укажите порт для подключения к базе данных на удаленном сервере. Значение по умолчанию:

`postgresql_host_port: 5432`

6. Сгенерируйте пару из закрытого и открытого ключа на локальном компьютере, выполнив команду `ssh-keygen`.

7. В утилите введите адрес папки, в которую будет сохранен сгенерированный закрытый ключ.

**Примечание.** Вы можете сохранить закрытый ключ в папку по умолчанию `/home/username/.ssh/id_rsa`, нажав клавишу Enter.

8. В утилите установите пароль для закрытого ключа.

**Примечание.** Вы можете установить пустой пароль, нажав клавишу Enter.

9. Скопируйте открытый ключ на сервер:

```
ssh-copy-id <Логин учетной записи на удаленном сервере>@<IP-адрес удаленного сервера>
```

10. В утилите введите пароль пользователя.

Содержимое локального файла `~/.ssh/id_rsa.pub` будет скопировано в файл `~/.ssh/authorized_keys` домашнего каталога соответствующего пользователя на удаленном сервере.

11. Выполните тестовое подключение к удаленному серверу с помощью SSH-ключей:

```
ssh username@server
```

Откроется оболочка удаленного сервера.

Подключение к удаленному узлу по SSH настроено.

## 7.4.8.4. Снятие резервной копии данных с локального узла Overview Center

Для снятия резервной копии выбранных инцидентов с локального узла Overview Center необходимо сначала перевести узел Overview Center в сервисный режим работы, затем снять копию данных и после этого вернуть его в нормальный режим работы.

Сервисный режим работы PT ISIM Overview Center предназначен для остановки сервисов, которые отвечают за сбор и обработку данных и могут влиять на скорость получения данных из СУБД PostgreSQL. Сервисы, которые будут остановлены, перечислены в конфигурационном файле `hammer.yaml`, расположенном в каталоге `/opt/ptisim/etc/hammer/`.

**Внимание!** Если PT ISIM Overview Center установлен и на удаленном сервере, и на локальном компьютере, то перед снятием резервной копии данных необходимо отключить утилиту от удаленного узла Overview Center, выбрав для параметра **enabled** значение **False**.

- Чтобы снять резервную копию данных с локального узла Overview Center:

1. Запустите утилиту, выполнив команду `/opt/ptisim/bin/hammer`.
2. Выберите **service mode**.
3. Нажмите клавишу Y для подтверждения.

PT ISIM Overview Center будет переведен в сервисный режим работы.

```
Switch to service mode.
The following services will be stopped:
ptisim-overview-server

Continue: (y/n)? y
1. ptisim-overview-server stopped successfully
```

Рисунок 54. Перевод локального узла Overview Center в сервисный режим работы

4. Выберите **dump data**.

Начнется создание резервной копии. В зависимости от объема данных это может занять продолжительное время. Резервная копия данных будет размещена на локальном компьютере в каталоге `/opt/ptisim/data/hammer/dump` в виде отдельных файлов таблиц с инцидентами, нарушениями, пользователями и параметрами. Для каждой таблицы, копируемой из базы данных PostgreSQL, создается дополнительный файл с расширением `.columns`. В нем содержится список столбцов, данные из которых были скопированы.



Рисунок 55. Файлы резервной копии для PT ISIM Overview Center

5. Выберите **normal mode**.
6. Нажмите клавишу Y для подтверждения.

PT ISIM Overview Center будет переведен в нормальный режим работы.  
Резервная копия данных локального узла PT ISIM Overview Center создана.

## 7.4.8.5. Снятие резервной копии данных с удаленного узла Overview Center

Для снятия резервной копии выбранных инцидентов с удаленного узла Overview Center необходимо сначала перевести узел Overview Center в сервисный режим работы, затем снять копию данных и после этого вернуть его в нормальный режим работы.

Сервисный режим работы PT ISIM Overview Center предназначен для остановки сервисов, которые отвечают за сбор и обработку данных и могут влиять на скорость получения данных из СУБД PostgreSQL. Сервисы, которые будут остановлены, перечислены в конфигурационном файле `hammer.yaml`, расположенном в каталоге `/opt/ptisim/etc/hammer/`.

► Чтобы снять резервную копию данных с удаленного узла PT ISIM Overview Center:

1. Подключите утилиту к удаленному узлу Overview Center, выбрав для параметра **enabled** значение **True**.
2. Запустите утилиту, выполнив команду `/opt/ptisim/bin/hammer`.
3. Выберите **service mode**.
4. Нажмите клавишу Y для подтверждения.

PT ISIM Overview Center будет переведен в сервисный режим работы.

```
Switch to service mode.
Remote connection: ssh -p 22 root@10.20.135.212
NOTE: User should have superuser privileges.
The following services will be stopped:
ptisim-overview-server

continue: (y/n)? y
1. ptisim-overview-server stopped successfully
```

Рисунок 56. Перевод удаленного узла Overview Center в сервисный режим работы

5. Выберите **dump data**.

Начнется создание резервной копии. В зависимости от объема данных это может занять продолжительное время. Резервная копия данных будет размещена на локальном компьютере в папке `/opt/ptisim/data/hammer/dump` в виде отдельных файлов таблиц с инцидентами, нарушениями, пользователями и параметрами. Для каждой таблицы, копируемой из базы данных PostgreSQL, создается дополнительный файл с расширением `.columns`. В нем содержится список столбцов, данные из которых были скопированы.



Рисунок 57. Файлы резервной копии для PT ISIM Overview Center

6. Выберите **normal mode**.
7. Нажмите клавишу Y для подтверждения.

PT ISIM Overview Center будет переведен в нормальный режим работы.

Резервная копия данных удаленного узла Overview Center создана.

## 7.4.8.6. Восстановление данных локального узла Overview Center из резервной копии

Для восстановления данных локального PT ISIM Overview Center из резервной копии необходимо сначала перевести узел Overview Center в сервисный режим работы, затем восстановить данные из ранее снятой копии и после этого вернуть узел в нормальный режим работы. Ранее снятая копия данных должна находиться в папке `/opt/ptisim/data/hammer/dump`.

Сервисный режим работы PT ISIM Overview Center предназначен для остановки сервисов, которые отвечают за сбор и обработку данных и могут влиять на скорость получения данных из СУБД PostgreSQL. Сервисы, которые будут остановлены, перечислены в конфигурационном файле `hammer.yaml`, расположенном в каталоге `/opt/ptisim/etc/hammer/`.

**Внимание!** Если PT ISIM Overview Center установлен и на удаленном сервере, и на локальном компьютере, то перед восстановлением данных из резервной копии необходимо отключить утилиту от удаленного узла PT ISIM Overview Center, выбрав для параметра **enabled** значение `False`.

► Чтобы восстановить данные локального PT ISIM Overview Center из резервной копии:

1. Запустите утилиту, выполнив команду `/opt/ptisim/bin/hammer`.

2. Выберите **service mode**.

3. Нажмите клавишу Y для подтверждения.

PT ISIM Overview Center будет переведен в сервисный режим работы.

4. Выберите **restore data**.

Начнется восстановление данных из резервной копии.

5. Выберите **normal mode**.

6. Нажмите клавишу Y для подтверждения.

PT ISIM Overview Center будет переведен в нормальный режим работы.

Данные локального PT ISIM Overview Center восстановлены из резервной копии.

## 7.4.8.7. Восстановление данных удаленного узла Overview Center из резервной копии

Для восстановления данных удаленного PT ISIM Overview Center из резервной копии необходимо сначала перевести узел Overview Center в сервисный режим работы, затем восстановить данные из ранее снятой копии и после этого вернуть узел в нормальный режим работы. Ранее снятая копия данных должна находиться в папке `/opt/ptisim/data/hammer/dump`.

Сервисный режим работы PT ISIM Overview Center предназначен для остановки сервисов, которые отвечают за сбор и обработку данных и могут влиять на скорость получения данных из СУБД PostgreSQL. Сервисы, которые будут остановлены, перечислены в конфигурационном файле `hammer.yaml`, расположенном в каталоге `/opt/ptisim/etc/hammer/`.

► Чтобы восстановить данные удаленного PT ISIM Overview Center из резервной копии:

1. Подключите утилиту к удаленному узлу (см. раздел 7.4.8.3) Overview Center, выбрав для параметра **enabled** значение **True**.
2. Запустите утилиту, выполнив команду `/opt/ptisim/bin/hammer`.
3. Выберите **service mode**.
4. Нажмите клавишу Y для подтверждения.

PT ISIM Overview Center будет переведен в сервисный режим работы.

5. Выберите **restore data**.

Начнется восстановление данных из резервной копии.

6. Выберите **normal mode**.

7. Нажмите клавишу Y для подтверждения.

Узел PT ISIM будет переведен в нормальный режим работы.

Данные удаленного PT ISIM Overview Center восстановлены из резервной копии.

## 7.5. Администрирование PT ISIM Industrial Tablet

В этом разделе содержатся инструкции по администрированию PT ISIM Industrial Tablet.

### В этом разделе

[Настройка интерфейса PT ISIM Industrial Tablet \(см. раздел 7.5.1\)](#)

[Смена пароля для доступа в PT ISIM Industrial Tablet \(см. раздел 7.5.2\)](#)

[Изменение IP-адреса сервера для подключения PT ISIM Industrial Tablet к сенсору \(см. раздел 7.5.3\)](#)

### 7.5.1. Настройка интерфейса PT ISIM Industrial Tablet

Для настройки интерфейса PT ISIM Industrial Tablet в зависимости от наличия его связи с сенсором используются два конфигурационных файла, расположенных на сервере с PT ISIM View Sensor:

- `/opt/ptisim/etc/fullview/httpapi.conf.d/r4.yaml` — при наличии связи с сенсором;
- `/opt/ptisim/www/frontend/kiosk/config/config.json` — при отсутствии связи с сенсором.

В конфигурационных файлах вы можете настроить следующие параметры интерфейса PT ISIM Industrial Tablet:

- `lang` — язык интерфейса;
- `display_name` — название, отображаемое в левом верхнем углу экрана;

**Примечание.** Вы можете изменить это название только в файле `/opt/ptisim/www/frontend/kiosk/config/config.json`, используемом при отсутствии связи с сенсором. При наличии связи с сенсором в PT ISIM Industrial Tablet всегда отображается имя сенсора.

- `tech_support_number` — номер телефона техподдержки;
- `timezone` — часовой пояс в формате UTC;
- `sound_periodic_restore` — повторное включение звукового оповещения, принудительно отключенного пользователем, при автоматической перезагрузке экрана PT ISIM Industrial Tablet (`true` — звуковое оповещение будет снова включено после перезагрузки экрана планшета, которая происходит ежечасно или при обнаружении нового инцидента, а также при потере связи планшета с сенсором или с сетью, `false` — звуковое оповещение будет отключено до тех пор, пока не будет обнаружен инцидент с критическим уровнем опасности или не будет потеряна связь планшета с сенсором или с сетью).

**Примечание.** Вы можете настроить этот параметр только в файле `/opt/ptisim/www/frontend/kiosk/config/config.json`.

► Чтобы настроить интерфейс PT ISIM Industrial Tablet:

1. Откройте файл `/opt/ptisim/etc/fullview/httpapi.conf.d/r4.yaml`.
2. В файле измените значения параметров.
3. Перезапустите службу `ptisim-httpapi`:  

```
systemctl restart ptisim-httpapi.service
```
4. Откройте файл `/opt/ptisim/www/frontend/kiosk/config/config.json`.
5. В файле измените значения параметров.

Интерфейс PT ISIM Industrial Tablet настроен.

## 7.5.2. Смена пароля для доступа в PT ISIM Industrial Tablet

При работе с PT ISIM Industrial Tablet через веб-интерфейс или планшет оператор использует два пароля:

- пароль для входа — для доступа к главному экрану PT ISIM Industrial Tablet и просмотра информации о последнем инциденте, обнаруженном сенсором;
- пароль для доступа к списку инцидентов — для просмотра списка инцидентов, выгрузки данных инцидентов и выгрузки пакета диагностической информации.

Оба пароля по умолчанию — `12345678`. Вы можете сгенерировать новые пароли.

► Чтобы изменить пароль для доступа в PT ISIM Industrial Tablet:

1. В главном меню выберите  → **Доступ в PT ISIM Industrial Tablet**.

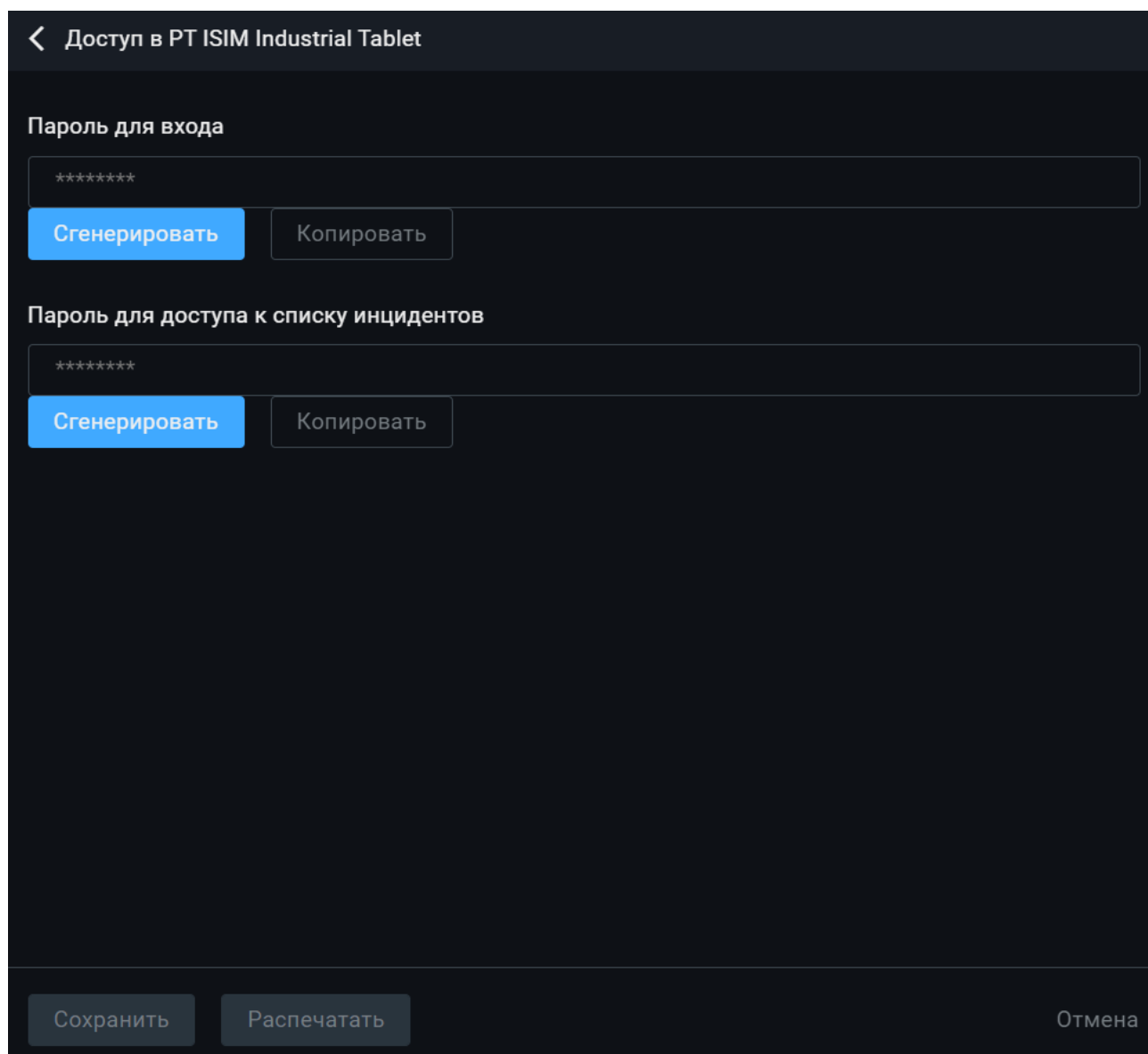


Рисунок 58. Смена пароля для доступа в PT ISIM Industrial Tablet

2. Под полем с нужным паролем нажмите **Сгенерировать**.
3. Нажмите **Сохранить**.

Пароль для доступа в PT ISIM Industrial Tablet изменен.

Вы можете сохранить пароль в буфер обмена, нажав **Копировать** под полем с нужным паролем, а также распечатать пароли.

## 7.5.3. Изменение IP-адреса сервера для подключения PT ISIM Industrial Tablet к сенсору

Если PT ISIM View Sensor был переустановлен или IP-адрес текущего сенсора был изменен, вы можете изменить IP-адрес сервера для подключения PT ISIM Industrial Tablet к сенсору двумя способами — с помощью скрипта или путем изменения конфигурационного файла.

- ▶ Чтобы изменить IP-адрес сервера для подключения PT ISIM Industrial Tablet к сенсору с помощью скрипта:

1. Запустите скрипт передачи нового IP-адреса сервера, на котором установлен PT ISIM Industrial Tablet:

```
sudo /opt/ptisim/bin/configure-kiosk-client.sh <Новый IP-адрес сенсора>
```

2. Перезапустите PT ISIM Industrial Tablet.

Когда связь с сенсором будет установлена, на экране отобразится окно входа в PT ISIM Industrial Tablet.

IP-адрес для подключения PT ISIM Industrial Tablet к PT ISIM View Sensor изменен.

- ▶ Чтобы изменить конфигурационный файл:

1. Откройте файл `/opt/ptisim/etc/kiosk_daemon.conf`, расположенный на сервере с PT ISIM Industrial Tablet.
2. В секции `kiosk` в параметре `remote_url` введите новый IP-адрес сервера, на котором установлен PT ISIM View Sensor.

IP-адрес для подключения PT ISIM Industrial Tablet к PT ISIM View Sensor изменен.

## 8. Удаление PT ISIM

В этом разделе содержатся инструкции по удалению компонентов PT ISIM.

### В этом разделе

[Удаление PT ISIM View Sensor \(см. раздел 8.1\)](#)

[Удаление PT ISIM Endpoint \(см. раздел 8.2\)](#)

[Удаление PT ISIM Collector \(см. раздел 8.3\)](#)

### 8.1. Удаление PT ISIM View Sensor

Вы можете удалить:

- компоненты PT ISIM View Sensor и их конфигурационные файлы;
- компоненты PT ISIM View Sensor и их конфигурационные файлы, а также пользовательские данные (события, инциденты, узлы).

- ▶ Чтобы удалить компоненты PT ISIM View Sensor и их конфигурационные файлы,

выполните команду:

```
sudo ptisim-uninstall-sensor
```

- ▶ Чтобы полностью удалить PT ISIM View Sensor, включая файлы компонентов продукта и пользовательские данные:

1. Запустите скрипт очистки баз данных:

```
sudo /opt/ptisim/bin/clean-localhost.sh
```

2. Удалите компоненты продукта и их конфигурационные файлы:

```
sudo ptisim-uninstall-sensor
```

3. Удалите каталоги с файлами:

```
sudo rm -rf /etc/ptisim/
```

```
sudo rm -rf /opt/ptisim/
```

```
sudo rm -rf /opt/ptsecurity/
```

### 8.2. Удаление PT ISIM Endpoint

- ▶ Чтобы удалить PT ISIM Endpoint,

на сервере с установленным PT ISIM Endpoint выполните команду `edr-purge` и подтвердите удаление.

## 8.3. Удаление PT ISIM Collector

В этом разделе приводятся инструкции по удалению коллектора на узле, вы также можете [удалить \(см. раздел 7.3.8\)](#) коллектор из PT ISIM View Sensor.

На узле вы можете удалить:

- компоненты PT ISIM Collector и их конфигурационные файлы;
- компоненты PT ISIM Collector и их конфигурационные файлы, а также пользовательские данные.

- ▶ Чтобы удалить компоненты PT ISIM Collector и их конфигурационные файлы,

выполните команду:

```
sudo ptisim-uninstall-collector
```

- ▶ Чтобы полностью удалить PT ISIM Collector, включая файлы компонентов продукта и пользовательские данные:

1. Удалите компоненты PT ISIM Collector и их конфигурационные файлы:

```
sudo ptisim-uninstall-collector
```

2. Удалите каталоги с файлами:

```
sudo rm -rf /etc/ptisim/
```

```
sudo rm -rf /opt/ptisim/
```

```
sudo rm -rf /opt/ptsecurity/
```

## 9. Решение проблем

Этот раздел содержит информацию для решения проблем при работе PT ISIM.

### В этом разделе

[Ошибка при обновлении из-за неразрешенных зависимостей \(см. раздел 9.1\)](#)

[Проблема с выявлением узлов сети \(см. раздел 9.2\)](#)

[Отсутствие событий в веб-интерфейсе \(см. раздел 9.3\)](#)

[Отсутствие данных в разделе Диагностика \(см. раздел 9.4\)](#)

[Ошибки при настройке сетевых интерфейсов \(см. раздел 9.5\)](#)

[Настройка ограничений GOOSE-событий \(см. раздел 9.6\)](#)

[Инцидент «Очистка очереди RabbitMQ» \(см. раздел 9.7\)](#)

[Чрезмерная загрузка диска запросами на запись статистики \(см. раздел 9.8\)](#)

[Большое потребление ресурсов сервера антивирусом \(см. раздел 9.9\)](#)

[Ошибка unable to resolve host \(см. раздел 9.10\)](#)

[Ошибка при установке Debian \(см. раздел 9.11\)](#)

[Установка PT ISIM прерывается на шаге Processing step rules \(см. раздел 9.12\)](#)

### 9.1. Ошибка при обновлении из-за неразрешенных зависимостей

#### Проблема

Попытка обновить PT ISIM завершается ошибкой, связанной с неразрешенными зависимостями. Проблема, как правило, актуальна для случаев, когда на сервере с PT ISIM есть доступ в интернет и между установкой прошлой версии и установкой новой версии продукта вы самостоятельно обновляли системные программы, например устанавливали обновления безопасности Debian.

#### Возможные причины

Во время [установки \(см. раздел 5.3.2\)](#) продукта автоматически перезаписывается список доступных источников пакетов: в `/etc/apt/sources.list.d/ptisim.list` прописывается путь до локального каталога с установочным комплектом PT ISIM, остальные источники пакетов на сервере удаляются. Если для обновления каких-либо программ на сервере вы самостоятельно изменяли список источников пакетов, при следующем обновлении PT ISIM этот список источников снова перезапишется. В этом случае может возникнуть конфликт

между версиями обновленных программ и версиями пакетов, требуемых для установки продукта, так как для установки теперь будут доступны только пакеты из установочного комплекта PT ISIM.

## Решение

Решением проблемы может быть обновление PT ISIM с сохранением текущего списка источников пакетов.

► Чтобы обновить PT ISIM с сохранением текущего списка источников пакетов:

1. Перенесите список источников пакетов из резервной копии в основной файл менеджера пакетов:

```
sudo mv /etc/apt/sources.list.<Дата и время>.save /etc/apt/sources.list
```

Например:

```
sudo mv /etc/apt/sources.list.2021-05-28_10-19-19.save /etc/apt/sources.list
```

2. В каталоге с установочным комплектом PT ISIM в файле `Manifest.pt` в параметре `hybrid` смените значение `false` на `true`.

При такой настройке текущий список источников пакетов не будет удаляться во время установки продукта.

3. Повторно запустите обновление PT ISIM:

```
sudo ./ptisim-install
```

## 9.2. Проблема с выявлением узлов сети

### Проблема

В веб-интерфейсе PT ISIM не отображаются новые узлы сети.

### Возможные причины

Если вы уверены, что в анализируемой сети происходит взаимодействие, но новые узлы не появляются на схеме сети и в таблице, возможны следующие причины проблемы:

- Не работают службы `ptdpi`, `ptisim-peony`, `ptisim-core`, `ptisim-model-service-ng`, `ptisim-httpapi`.
- PT ISIM не обнаруживает события.

## Решение

► Чтобы решить проблему:

1. Проверьте состояние указанных служб:

```
sudo systemctl status ptdpi ptisim-peony ptisim-core ptisim-model-service-ng ptisim-httpapi
```

Состояние каждой службы должно быть `Active: active (running)`.

2. Если состояние службы отличается, перезапустите ее:

```
sudo systemctl restart <Название службы>
```

3. Если службы запущены, но узлы не появляются в веб-интерфейсе, [проверьте наличие событий \(см. раздел 9.3\)](#).

Если службы запущены и новые события регистрируются в PT ISIM, причиной отсутствия узлов может быть неправильная работа службы моделирования. В этом случае рекомендуется обратиться в службу технической поддержки, приложив к запросу [пакет диагностический информации \(см. раздел 7.1.14.4\)](#).

## 9.3. Отсутствие событий в веб-интерфейсе

### Проблема

В веб-интерфейсе PT ISIM отсутствуют события.

### Возможные причины

Для определения причин и способов решения проблемы необходимо проверить наличие событий в базе данных.

► Чтобы проверить наличие событий в базе данных,

выполните команду:

```
clickhouse-client -n -q "select toDateTime(time/1000000), count() from isim.events group by time,class order by time desc"
```

Будет выведен список событий, сгруппированных по времени.

## Решение

Если события за определенный период присутствуют в базе данных, но отсутствуют в веб-интерфейсе, необходимо проверить службу `ptisim-httpapi` и перезапустить ее, если ее состояние отличается от `Active: active (running)`.

Если события отсутствуют в базе данных, необходимо создать [тестовые события \(см. раздел 5.3.5.3\)](#). Если тестовые события также не появляются в базе данных и в веб-интерфейсе, решение проблемы может состоять из нескольких этапов.

## Этап 1. Проверка часового пояса

Проверьте следующие параметры времени:

- На сервере с PT ISIM должен быть установлен часовой пояс UTC.
- Часовой пояс браузера, с помощью которого вы заходите в веб-интерфейс, должен быть таким же, как ваш реальный часовой пояс в формате UTC.

## Этап 2. Проверка состояния служб

Проверьте состояние служб (см. раздел 7.1.14.2). Все службы должны быть запущены (иметь статус «ОК»).

Если все службы запущены, но события по-прежнему отсутствуют в интерфейсе PT ISIM, перейдите к этапу 3.

## Этап 3. Проверка наличия трафика в сети

► Чтобы проверить наличие трафика в сети:

1. Выполните команду:

```
sudo tcpdump -nli bond0
```

2. Если на интерфейсе bond0 трафик не обнаружен, проверьте наличие трафика на интерфейсах, с которых необходимо перехватывать технологический трафик:

```
sudo tcpdump -nli <Название сетевого интерфейса>
```

**Примечание.** Проверить состояние сетевых интерфейсов вы также можете в веб-интерфейсе (см. раздел 7.1.14.1).

3. Если трафика на указанных интерфейсах не обнаружено, проверьте корректность подключения к коммутатору, трафик с которого необходимо перехватывать, исправность и подключение сетевого кабеля.
4. Если трафик обнаружен на указанных интерфейсах, но не обнаружен на интерфейсе bond0, перейдите к этапу 4.

## Этап 4. Настройка сетевых интерфейсов

Сетевые интерфейсы, с которых необходимо перехватывать технологический трафик, должны быть объединены в виртуальный интерфейс bond0.

Настройка сетевых интерфейсов, в том числе их объединение в bond0, осуществляется в процессе установки продукта.

► Чтобы проверить параметры сетевых интерфейсов,

выполните команду:

```
sudo ip addr show
```

В выводе команды должно быть указано, что виртуальный интерфейс bond0 включен (UP BROADCAST RUNNING MASTER), а сетевые интерфейсы, с которых необходимо перехватывать технологический трафик, включены и объединены в bond0 (UP BROADCAST RUNNING SLAVE).

► Чтобы объединить сетевые интерфейсы в bond0:

1. Откройте конфигуратор сетевых интерфейсов, запустив следующий сценарий:  
`/opt/ptisim/bin/configure-network.sh`
2. Нажмите клавишу 3 (add to bond).
3. В открывшемся списке интерфейсов выберите сетевой интерфейс, с которого требуется перехватывать технологический трафик, и нажмите соответствующую ему клавишу.
4. Нажмите клавишу 7 (exit).
5. Нажмите клавишу 1 (save and exit).
6. [Проверьте параметры сетевых интерфейсов \(см. раздел 9.3\).](#)
7. Проверьте наличие событий в веб-интерфейсе PT ISIM.

Если сетевые интерфейсы объединены в bond0 и пакеты на данном интерфейсе обнаружены, но события в веб-интерфейсе отсутствуют, обратитесь в службу технической поддержки.

## 9.4. Отсутствие данных в разделе Диагностика

### Проблема

В веб-интерфейсе PT ISIM на странице **Диагностика** выдается **Ошибка запроса**.

### Возможные причины

Не работает служба ptisim-httpapi.

### Решение

► Чтобы решить проблему,

перезапустите службу ptisim-httpapi:

```
sudo systemctl restart ptisim-httpapi.service.
```

После перезапуска состояние службы должно быть Active: active (running).

Состояние службы можно проверить с помощью команды `systemctl status ptisim-httpapi.service`.

## 9.5. Ошибки при настройке сетевых интерфейсов

Для настройки сетевых интерфейсов в PT ISIM предусмотрен специальный скрипт. Список интерфейсов, которые необходимо настроить, скрипт получает из файла `/etc/network/interfaces`. Если в файле указаны некорректные параметры, после запуска скрипта могут возникнуть ошибки.

Таблица 35. Ошибки при настройке сетевых интерфейсов

| Текст ошибки                                                        | Причина                                                                                                                                                                                  | Некорректные параметры                                                                                                     | Корректные параметры                                                                                                       |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Startup of non-configured interface                                 | В строке <code>auto</code> указан интерфейс, для которого не заданы никакие параметры                                                                                                    | <code>auto eth0</code><br><code>iface eth1 inet dhcp</code>                                                                | <code>auto eth0</code><br><code>iface eth0 inet dhcp</code>                                                                |
| Incorrect stanza beginning                                          | Строка с названием интерфейса начинается не с <code>iface</code> , <code>mapping</code> , <code>auto</code> , <code>allow</code> , <code>source</code> или <code>source-directory</code> | <code>face eth0 inet dhcp</code>                                                                                           | <code>iface eth0 inet dhcp</code>                                                                                          |
| Interface name may not start with #                                 | Имя интерфейса начинается с символа <code>#</code>                                                                                                                                       | <code>iface #eth1 inet dhcp</code>                                                                                         | <code>iface eth1 inet dhcp</code>                                                                                          |
| Duplicate declaration of <Имя интерфейса>                           | Интерфейс с одним и тем же названием задан дважды                                                                                                                                        | <code>auto eth2</code><br><code>iface eth2 inet dhcp</code><br><code>auto eth2</code><br><code>iface eth2 inet dhcp</code> | <code>auto eth1</code><br><code>iface eth1 inet dhcp</code><br><code>auto eth2</code><br><code>iface eth2 inet dhcp</code> |
| <code>bond0</code> is configured but does not have a "slaves" field | У интерфейса <code>bond0</code> нет <code>slave</code> -интерфейсов                                                                                                                      | <code>iface bond0 inet manual</code>                                                                                       | <code>iface bond0 inet manual</code><br><code>slaves eth1</code>                                                           |

## 9.6. Настройка ограничений GOOSE-событий

В результате неправильной настройки оборудования в анализируемой сети могут фиксироваться GOOSE-сообщения некорректного формата или содержания. При обнаружении таких сообщений PT ISIM может регистрировать события, сигнализирующие о нарушении последовательности номеров сообщений, некорректной метке времени или некорректном формате. Если оборудование вашей сети регулярно посылает такие сообщения, то количество событий может быть очень велико, и служба watchdog начнет постепенно удалять их [для поддержания свободного дискового пространства \(см. раздел 7.1.3\)](#). Если у вас нет возможности изменить параметры оборудования или если вы считаете, что такие сообщения не являются проблемными, вы можете ограничить количество создаваемых GOOSE-событий, чтобы не перегружать систему.

Ограничения событий за единицу времени указываются в конфигурационном файле компонента PT Peony и распространяются на каждый узел-источник, определяемый по его MAC-адресу.

► Чтобы ограничить количество GOOSE-событий:

1. Откройте конфигурационный файл PT Peony:  

```
sudo nano /opt/ptisim/etc/peony-host.conf
```
2. В секции `goose` в разделе `limits` для необходимых типов событий (`invalid_time`, `invalid_counters` или `invalid_parsing`) введите значения следующих параметров:
  - `enable` — включить ограничение (`true/false`);
  - `count` — максимальное количество сообщений от одного узла, при превышении которого события не будут создаваться;

**Примечание.** Вы также можете полностью отключить создание GOOSE-событий того или иного типа, указав для него 0 в параметре `count`.

  - `period_s` — период в секундах, за который отсчитывается ограничение, указанное в `count`.
3. Перезапустите компонент PT Peony:  

```
sudo systemctl restart ptisim-peony
```

Ниже приводится пример правила, при котором фиксируются только первые десять событий некорректного формата от одного узла в минуту, остальные сообщения (за эту же минуту от этого же узла) не приводят к созданию событий:

```
"goose": {
...
 "limits": {
...
 "invalid_parsing": {
 "enable": true,
 "count": 10,
 "period_s": 60
 }
 }
...
}
```

## 9.7. Инцидент «Очистка очереди RabbitMQ»

### Проблема

Зарегистрирован инцидент «Очистка очереди RabbitMQ».

### Возможные причины

Инцидент «Очистка очереди RabbitMQ» возникает в случае, если служба `ptisim-watchdog` для поддержания работоспособности продукта очистила очереди `coreq`, `modelq`, `incidentq` или `metricsq` в RabbitMQ. В результате очистки очереди происходит потеря данных, например событий, которые поступили в PT ISIM, но не были обработаны (очереди `coreq` и `modelq`), инцидентов (`incidentq`) или статистических данных (`metricsq`).

По умолчанию проверки `ptisim-watchdog`, в том числе проверки очередей, запускаются раз в минуту. Параметры очистки очередей указываются в следующих файлах:

- `/opt/ptisim/etc/watchdog.yaml` в параметре `queue_length` — предельный размер каждой очереди, при превышении которого происходит ее очищение;
- `/opt/ptisim/etc/watchdog.conf.d/watchdog-common.yaml` в параметре `queue_length` — предельный размер каждой очереди (общий параметр, который применяется, если значение не задано для конкретной очереди);
- `/usr/lib/systemd/system/ptisim-watchdog.timer` параметры `OnActiveSec` и `OnUnitInactiveSec` — частота запуска проверок `ptisim-watchdog` (задается в формате `systemd.timer`).

## Решение

Вы можете принять следующие меры:

- Текущая мера. Проверьте состояния служб, принимающих сообщения из RabbitMQ, и, если требуется, перезапустите их:  

```
systemctl status ptisim-core ptisim-model-service-ng ptisim-alerts ptisim-bucket
systemctl restart ptisim-core ptisim-model-service-ng ptisim-alerts ptisim-bucket
```
- Превентивная мера. В зависимости от аппаратных возможностей — увеличьте предельные размеры очередей.
- Восстановление. Копия поступившего трафика, в том числе не обработанного до уровня событий, инцидентов и статистических данных, хранится в формате PCAP в каталоге `/opt/ptsecurity/data/pcaps`. Вы можете использовать PCAP-файлы для анализа необработанных данных в сторонних системах.

**Примечание.** Доступность PCAP-файлов зависит от параметров хранения данных (см. раздел 7.1.3).

## 9.8. Чрезмерная загрузка диска запросами на запись статистики

### Проблема

Замедление работы PT ISIM вследствие большой загрузки дисковой системы запросами на запись статистических данных.

### Возможные причины

Служба `ptisim-bucket` формирует статистические данные для графиков на странице **Статистика**, используя базу `metrics` в PostgreSQL. Секции для этой базы по умолчанию создаются раз в сутки. При большом количестве статистических данных операции записи данных в базу `metrics` могут чрезмерно нагружать дисковую систему, что приводит к замедлению работы всей системы.

### Решение

Для уменьшения загрузки дисковой системы вы можете увеличить количество секций, создаваемых в сутки, и таким образом уменьшить объем данных, к которым обращается служба `ptisim-bucket` при записи. В качестве количества секций, создаваемых в сутки, вы можете указать любой делитель числа 24. Поскольку слишком большое число секций может привести к противоположному эффекту (чрезмерной загрузке дисковой системы операциями на чтение), рекомендуется указывать минимальное необходимое число секций в сутки.

Например, если дисковая система регулярно перегружается во второй половине дня, а в первой половине дня проблем с замедлением работы не наблюдается, то оптимальным будет создание секции базы два раза в сутки.

**Примечание.** Проверить текущую загрузку дисковой системы операциями на запись и чтение вы можете с помощью сторонних утилит мониторинга, таких как `iostat`.

► Чтобы изменить количество создаваемых секций для базы `metrics`:

1. Откройте конфигурационный файл службы сбора статистических данных:  
`sudo nano /opt/ptisim/etc/bucket/bucket.conf`
2. В параметре `storage` → `partitions_per_day` укажите, сколько секций в день требуется создавать, например `partitions_per_day: 2`.

Количество создаваемых секций изменено. Изменения вступят в силу с началом новых суток.

## 9.9. Большое потребление ресурсов сервера антивирусом

### Проблема

При работе PT ISIM чрезмерно нагружается центральный процессор сервера, возникают проблемы с производительностью, очереди `coreq`, `modelq`, `incidentq` или `metricsq` в RabbitMQ копятя и принудительно очищаются.

### Возможные причины

Антивирус Kaspersky Endpoint Security 12 проверяет все файлы системы, в связи с чем подаваемый на сенсор трафик не успевает корректно обрабатываться.

### Решение

Вы можете принять следующие меры:

- [Добавить в исключения антивируса](#) каталоги и файлы PT ISIM (ниже представлен обобщенный список каталогов Debian 10.12, Debian 12, Astra Linux 1.7.6 Special Edition, которые добавляются в систему после установки сенсора):
  - `/opt/ptisim/`
  - `/opt/ptisim-overview/`
  - `/etc/ptisim/`
  - `/opt/ptisim-common/`
  - `/var/log/ptisim/`

- `/etc/rsyslog.d/`
- `/etc/sudoers.d/`
- `/opt/ptsecurity/`
- `/etc/clickhouse-server/`
- `/etc/clickhouse-keeper/`
- `/etc/clickhouse-client/`
- `/etc/ld.so.conf.d/`
- `/etc/monit/`
- `/etc/network/`
- `/etc/nginx/`
- `/etc/sysctl.d/`
- `/etc/syslog-ng/`
- `/run/clickhouse-server/`
- `/run/blkid/`
- `/run/fail2ban/`
- `/run/containerd/`
- `/run/docker/`
- `/usr/libexec/`
- `/etc/init/`

— [Настроить оптимизацию потребления ресурсов антивирусом.](#)

## 9.10. Ошибка `unable to resolve host`

### Проблема

В терминале появляется сообщение вида `ptisim : unable to resolve host <имя узла>`.

### Возможные причины

Имя узла было изменено с помощью команды `hostnamectl set-hostname <Имя узла>`, а в файл `/etc/hosts` изменения внесены не были.

## Решение

Для решения проблемы потребуется добавить строку в файл `/etc/hosts`, сопоставив новое имя узла с `localhost`. Пример записи для нового имени узла `test-host`:

```
127.0.0.1 test-host
```

## 9.11. Ошибка при установке Debian

### Проблема

Установка Debian завершается неудачей.



Рисунок 59. Ошибка при установке Debian

### Возможные причины

Дефект в дистрибутиве Debian.

## Решение

Если установка Debian завершилась неудачей, отключите доступ в интернет на сервере, на котором необходимо установить операционную систему, и запустите установку повторно.

## 9.12. Установка PT ISIM прерывается на шаге Processing step rules

### Проблема

Установка PT ISIM прерывается на шаге Processing step rules.

### Возможные причины

PT ISIM устанавливается на один узел с антивирусом Kaspersky Endpoint Security 12. Антивирус в процессе установки определяет некоторые файлы как вредоносные и удаляет их.

### Решение

Перед запуском установки PT ISIM вы можете добавить в исключения антивируса каталог /opt/ptisim/lib/rules/, выполнив команду:

```
kesl-control --set-settings 1 --add-exclusion /opt/ptisim/lib/rules/**/*
```

Вы также можете добавить в исключения [другие каталоги и файлы \(см. раздел 9.9\)](#) PT ISIM. Подробнее работа с исключениями описана [в справке антивируса](#).

## 10. О технической поддержке

Гарантийная поддержка доступна для всех владельцев действующих лицензий на PT ISIM в течение периода предоставления обновлений и включает в себя следующий набор услуг.

### Предоставление доступа к обновленным версиям продукта

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies поставляет обновленные версии продукта в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта Positive Technologies.

Positive Technologies не производит установку обновлений продукта в рамках гарантийной поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продукта.

### Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

**Примечание.** Помощь оказывается при условии, что конечным пользователем продукта соблюдены все аппаратные, программные и иные требования и ограничения, описанные в документации к продукту.

### Устранение ошибок и дефектов в работе продукта в рамках выпуска обновленных версий

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

### Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы и сроки ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются [на портале технической поддержки](#).

## Портал технической поддержки

[На портале технической поддержки](#) вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к portalу технической поддержки нужно создать учетную запись, используя адрес электронной почты в официальном домене вашей организации. Вы можете указать другие адреса электронной почты в качестве дополнительных. Добавьте в профиль название вашей организации и контактный телефон — так нам будет проще с вами связаться.

Поддержка на портале предоставляется на русском и английском языках.

## Условия предоставления гарантийной поддержки

Для получения гарантийной поддержки необходимо оставить заявку [на портале технической поддержки](#) и предоставить следующие данные:

- номер лицензии на использование продукта;
- файлы журналов и наборы диагностических данных, которые требуются для анализа;
- снимки экрана.

Positive Technologies не берет на себя обязательств по оказанию услуг гарантийной поддержки в случае вашего отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по вашей инициативе при условии предоставления запрошенной ранее информации.

Услуги по гарантийной поддержке продукта не включают в себя услуги по переустановке продукта, решение проблем с операционной системой, инфраструктурой заказчика или сторонним программным обеспечением.

Заявки могут направлять уполномоченные сотрудники заказчика, владеющего продуктом на законном основании (включая наличие действующей лицензии). Специалисты заказчика должны иметь достаточно знаний и навыков для сбора и предоставления диагностической информации, необходимой для решения заявленной проблемы.

Услуги по гарантийной поддержке оказываются в отношении поддерживаемых версий продукта. Информация о поддерживаемых версиях содержится в «Политике поддержки версий программного обеспечения» и (или) иных информационных материалах, размещенных на официальном веб-сайте Positive Technologies.

## Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по ее обработке.

Время реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 36. Время реакции на заявку

| Уровень значимости заявки | Критерии значимости заявки                                                                                                                                              | Время реакции на заявку |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Критический               | Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие критически значимое влияние на бизнес заказчика | До 4 часов              |
| Высокий                   | Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика                                                       | До 8 часов              |
| Средний                   | Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес заказчика                                        | До 8 часов              |
| Низкий                    | Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта                                                                                       | До 8 часов              |

Указанные часы относятся к рабочему времени (рабочие дни с 9:00 до 18:00 UTC+3) специалистов технической поддержки. Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

## Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист службы поддержки сообщает вам:

- о ходе диагностики по заявленной проблеме и ее результатах;
- планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

- предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;
- заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

**Примечание.** Если продукт приобретался вместе с аппаратной платформой в виде программно-аппаратного комплекса (ПАК), решение заявок, связанных с ограничением или отсутствием работоспособности аппаратных компонентов, происходит согласно условиям и срокам, указанным в гарантийных обязательствах (гарантийных талонах) на такие аппаратные компоненты.

## Приложение А. Типы узлов

В PT ISIM View Sensor узлам присваиваются типы, которые обозначают роль узла в системе:

- AAA-служба;
- AD FS;
- CI/CD;
- DHCP-сервер;
- DNS-сервер;
- ERP-система;
- KVM-переключатель;
- OPC-сервер;
- RDG;
- VPN;
- WSUS;
- Антивирус;
- APM;
- APM оператора;
- Беспроводной доступ;
- Веб-сервер;
- Виртуализация;
- Гипервизор;
- Датчик;
- ИБП;
- Коммутатор;
- Контроллер домена;
- Контроллер ПАЗ;
- Маршрутизатор;
- Межсетевой экран;
- Модем;
- Панель HMI;
- ПЛК;

- Почтовый сервер;
- Преобразователь интерфейсов;
- Принтер;
- Прокси-сервер;
- Сервер SCADA;
- Сервер AB3;
- Сервер баз данных;
- Сервер времени GPS;
- Сервер исторических данных;
- Сервер приложений;
- Система контроля версий;
- Система мониторинга;
- Служба каталогов;
- Точка доступа;
- Устройство общего типа;
- Устройство РЗА;
- Файловая служба;
- Файловый сервер;

## Приложение Б. Формат syslog-сообщений об инцидентах

Формат и набор полей, из которых состоят сообщения об инцидентах, отправляемые PT ISIM в syslog (см. раздел 7.1.6.1), определяются с помощью шаблонов. Шаблоны хранятся в каталоге `/opt/ptisim/lib/ptisim-httpapi/templates/alerts/notify`. Каждому типу сообщений в этом каталоге соответствует свой шаблон:

- `alert_create_message/syslog` — уведомление об обнаружении нового инцидента;
- `alert_status_message/syslog` — уведомление о смене статуса инцидента;
- `alert_progress_message/syslog` — уведомление о том, что зафиксирован новый этап инцидента (для инцидентов, которые состоят из нескольких этапов, например «Возможное отключение PT ISIM от сети»).

Помимо полей, уже указанных в шаблонах, вы можете добавить в текст сообщений и другие поля, заключив их в двойные фигурные скобки `{{ ... }}`, например `{{ incident.status }}`. В таблице ниже приводится список основных параметров инцидентов, которые вы можете использовать в качестве полей syslog-сообщений. Полный список всех доступных полей приводится в файле `/opt/ptisim/etc/fullview/httpapi.conf.d/incidents-notify-fields.yaml`.

Таблица 37. Поля syslog-сообщений

| Поле                           | Тип данных | Описание                                                                                                                    |
|--------------------------------|------------|-----------------------------------------------------------------------------------------------------------------------------|
| <code>incident.id</code>       | UInt32     | Идентификатор инцидента                                                                                                     |
| <code>incident.type</code>     | String     | Тип инцидента                                                                                                               |
| <code>incident.status</code>   | String     | Текущий статус инцидента: <code>open</code> (открыт), <code>in_progress</code> (в работе), <code>closed</code> (закрыт)     |
| <code>incident.progress</code> | UInt32     | Текущий этап инцидента (для инцидентов, состоящих из нескольких этапов)                                                     |
| <code>incident.capacity</code> | UInt32     | Общее количество возможных этапов инцидента                                                                                 |
| <code>incident.events</code>   | String     | Список событий инцидента                                                                                                    |
| <code>incident.start</code>    | Timestamp  | Время заведения инцидента                                                                                                   |
| <code>incident.end</code>      | Timestamp  | Время последнего события инцидента. Может совпадать с <code>incident.start</code> , если инцидент состоит из одного события |

| Поле                    | Тип данных | Описание                                                                                                                                                      |
|-------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| change                  | Timestamp  | Время последнего изменения свойств инцидента. Изменениями считаются смена статуса, добавление в избранные, появление нового события, наступление нового этапа |
| incident.source         | String     | Идентификатор узла — источника инцидента                                                                                                                      |
| incident.destination    | String     | Идентификатор узла — цели инцидента                                                                                                                           |
| incident.model_state    | UInt32     | Идентификатор состояния модели на момент обнаружения инцидента                                                                                                |
| incident.src_ip         | String     | IP-адрес источника инцидента                                                                                                                                  |
| incident.src_mac        | String     | MAC-адрес источника инцидента                                                                                                                                 |
| incident.dst_ip         | String     | IP-адрес цели инцидента                                                                                                                                       |
| incident.dst_mac        | String     | MAC-адрес цели инцидента                                                                                                                                      |
| incident.group          | String     | Группа инцидентов                                                                                                                                             |
| incident.severity_level | String     | Уровень опасности инцидента: <i>high</i> (высокий), <i>medium</i> (средний), <i>low</i> (низкий), <i>info</i> (инфо)                                          |
| incident_url            | String     | Ссылка на инцидент в веб-интерфейсе                                                                                                                           |
| station_name            | String     | Название узла View Sensor                                                                                                                                     |
| now                     | String     | Текущее время                                                                                                                                                 |
| ip                      | String     | IP-адрес узла ISIM                                                                                                                                            |
| src_ip                  | String     | IP-адрес источника события                                                                                                                                    |
| dst_ip                  | String     | IP-адрес получателя события                                                                                                                                   |
| src_mac                 | String     | MAC-адрес источника события                                                                                                                                   |
| dst_mac                 | String     | MAC-адрес получателя события                                                                                                                                  |
| type                    | String     | Тип инцидента                                                                                                                                                 |
| incident.name.rus       | String     | Название инцидента на русском языке                                                                                                                           |
| incident.name.eng       | String     | Название инцидента на английском языке                                                                                                                        |

# Глоссарий

## PT ISTI

Экспертная база правил распознавания и разбора протоколов передачи данных, а также выявления инцидентов информационной безопасности, нарушений и аномалий в технологической сети, использующаяся в PT ISIM View Sensor.

## авторизованный узел

Сетевой элемент, который принадлежит анализируемой технологической сети или взаимодействие которого с узлами анализируемой сети считается допустимым. Узел может быть авторизован вручную или автоматически (в рамках режима обучения).

## атака

Попытка злоумышленника вывести узел из строя, например в случае DDoS-атаки, или получить несанкционированный доступ в сеть с целью изменить, удалить, получить данные или добавить нежелательные данные. Успех атаки зависит от степени уязвимости системы защиты и предпринимаемых контрмер.

## аудит

Режим сканирования, предназначенный для сбора и обновления данных о конечном узле с использованием учетных данных (методом белого ящика). Сканирование в этом режиме позволяет получить актуальную информацию о конфигурации узла, например о версии ОС, установленном ПО, аппаратном обеспечении, учетных записях и группах пользователей.

## инцидент (информационной безопасности)

Событие или цепочка событий, результатом которых может стать нарушение целостности, конфиденциальности или доступности данных.

## коллектор

Упрощенная версия PT ISIM View Sensor для установки в удаленных сегментах сети и передачи данных в PT ISIM View Sensor. Не имеет веб-интерфейса.

## контактное лицо

Лицо, имеющее доступ к объекту, на котором установлен PT ISIM View Sensor или PT ISIM Overview Center. Телефон и адрес электронной почты контактного лица являются частью пакета регистрации и могут потребоваться для получения информации о состоянии объекта и оперативного реагирования на инциденты.

## корреляционное событие

Событие, полученное в результате анализа нормализованных событий на соответствие правилу корреляции. Свидетельствует о нарушении информационной безопасности.

**нарушение**

Отклонение характеристик узла от рекомендованных значений. Нарушение может свидетельствовать о несоблюдении политик информационной безопасности (например, об использовании уязвимой версии протокола или слабого шифрования) или о сбое в работе (например, если узел не отвечает на ARP-запросы или на нем выявлена слишком высокая нагрузка на процессор).

**нормализованное событие**

Событие, приведенное к формату, позволяющему однозначно определить основные параметры события, отнести его к определенному узлу и устройству, а также провести дальнейший анализ события на основе значений отдельных полей.

**пакет регистрации**

Набор параметров узла PT ISIM View Sensor или PT ISIM Overview Center (название, сетевой адрес, геолокация и другие) для его регистрации в PT ISIM Overview Center. Пакет регистрации может быть отправлен по сети или передан в виде файла.

**правило корреляции**

Правило проверки потока событий на соответствие заданным закономерностям и условиям.

**разбираемый протокол**

Протокол, который PT ISIM View Sensor анализирует достаточно глубоко, чтобы получить из трафика интересующие атрибуты сообщений и их значения и использовать их в процессе корреляции. Одному такому протоколу соответствуют несколько типов инцидентов.

**разрешение**

Правило, которое описывает параметры соединений, допустимых в анализируемой сети: IP-адрес и MAC-адрес отправителя, IP-адрес, MAC-адрес и порт получателя и протокол. Если в сети обнаружено соединение, значения параметров которого соответствуют хотя бы одному из разрешений, система фиксирует такое соединение со статусом «Разрешенное». Если обнаружено соединение, которое не подходит ни под одно из разрешений, система фиксирует такое соединение как «Неразрешенное» и регистрирует инцидент.

**распознаваемый протокол**

Протокол, для которого PT ISIM View Sensor фиксирует каждый случай использования в сети в виде соединений и событий, но не различает типы инцидентов.

**редакция PT ISIM View Sensor**

Вариант поставки PT ISIM View Sensor с определенным набором функций: microView Sensor, netView Sensor или proView Sensor.

## **режим обучения**

Режим работы PT ISIM View Sensor, при котором все обнаруживаемые сущности, для которых предназначен режим, считаются авторизованными или разрешенными, а инциденты о появлении новых сущностей не заводятся. В PT ISIM View Sensor предусмотрено несколько режимов обучения. Все режимы обучения по умолчанию включены после установки продукта.

## **сервер обновлений**

Специальный сервер, который позволяет автоматически получать обновления PT ISIM View Sensor и экспертной базы PT ISTI.

## **сервисный интерфейс**

Сетевой интерфейс, предназначенный для предоставления пользователям доступа к веб-интерфейсу продукта (по HTTPS) и к его серверу (по SSH).

## **сетевой сканер**

Компонент PT ISIM View Sensor и PT ISIM Collector, который выполняет сбор данных с конечных узлов по сети. Сканер собирает события и данные о конфигурации узлов.

## **событие**

Зафиксированное состояние (или изменение состояния) элемента анализируемой системы.

## **соединение**

Процесс передачи данных от узла-отправителя узлу-получателю по определенному протоколу.

## **структура узлов PT ISIM**

Совокупность подключенных к PT ISIM Overview Center узлов, организованных в виде иерархии, в которой нижестоящие узлы (PT ISIM View Sensor или PT ISIM Overview Center) зарегистрированы на вышестоящих узлах PT ISIM Overview Center.

## **технологический интерфейс**

Сетевой интерфейс, принимающий зеркалируемый трафик технологической сети. PT ISIM анализирует такой трафик для обнаружения инцидентов и построения схемы сети.

## **технологический трафик**

Трафик между элементами сети АСУ ТП.

## **уровень опасности инцидента**

Параметр, который рассчитывается исходя из характера хакерской активности, потенциальной угрозы для инфраструктуры и возможных последствий атаки.

**уязвимость**

Недостаток вычислительной логики (например, в коде), обнаруженный в программном или аппаратном компоненте (например, в прошивке), использование которого может оказать негативное воздействие на конфиденциальность, целостность или доступность данных.

**фингерпринт**

Отпечаток аппаратных характеристик устройства, который используется для его идентификации, например при создании файла лицензии.

**цепочка инцидентов**

Инструмент для расследования атак, визуально представляющий последовательность возникновения инцидентов и их связи.



Positive Technologies — один из лидеров в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.