



Email Security

версия 5.37

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: 21.09.2026

Содержание

1.	Об этом документе.....	6
1.1.	Условные обозначения.....	6
1.2.	Другие источники информации о PT Email Security.....	7
2.	О PT Email Security.....	8
3.	Что нового в версии 5.37.....	11
4.	Компоненты PT Email Security.....	12
5.	Требования к рабочим станциям.....	13
6.	Настройка аутентификации.....	14
7.	Вход в PT Email Security.....	22
8.	Интерфейс PT Email Security.....	23
9.	Лицензирование.....	26
10.	Настройка средств проверки.....	29
10.1.	Настройка лимитов на размер извлекаемых файлов.....	29
10.2.	Настройка средств проверки Positive Technologies.....	30
10.3.	Настройка антивирусов.....	36
10.4.	Настройка поведенческого анализа.....	39
10.5.	Работа с пользовательскими YARA-правилами.....	40
11.	Настройка параметров PT Email Security.....	42
11.1.	Включение анонимной проверки объектов.....	43
11.2.	Настройка расписания обновления образов VM.....	43
11.3.	Настройка хранилища файлов.....	44
11.4.	Настройка карантина для писем.....	45
11.5.	Добавление IP-адресов службы публичного API.....	46
11.6.	Настройка времени отображения письма в очереди MTA.....	46
11.7.	Настройка почтовых уведомлений об угрозах.....	47
11.8.	Настройка параметров почтового шлюза безопасности.....	48
11.9.	Настройка хранения проверяемых файлов в оперативной памяти.....	49
12.	Работа с источниками.....	52
12.1.	Настройка источников.....	55
12.2.	Работа с токенами доступа.....	57
12.3.	Работа со списками адресов.....	59
12.3.1.	Списки адресов.....	59
12.3.2.	Адреса списка.....	62
12.4.	Работа с агентами почтового шлюза.....	67
12.5.	Настройка правил маршрутизации проверенных писем.....	70
12.6.	Отключение автоматической смены режимов проверки.....	73
13.	Подключение источников.....	74
13.1.	Служба Checkme.....	75
13.2.	Общая папка.....	76
13.3.	Папка-шлюз.....	79
13.4.	S3-хранилище.....	82
13.5.	Внешняя система как ICAP-клиент.....	84
13.6.	Внешняя система через API.....	87

13.7.	Почтовый шлюз безопасности.....	88
13.7.1.	Развертывание почтового шлюза безопасности	89
13.7.2.	Добавление агента почтового шлюза в PT Email Security	91
13.7.3.	Добавление источника в PT Email Security	91
13.7.4.	Подключение агента почтового шлюза к источнику	93
13.7.5.	Добавление правил маршрутизации проверенных писем	93
13.7.6.	Добавление доверенных сертификатов	95
13.7.7.	Включение проверки адресов получателей	96
13.8.	«Код безопасности», «Континент» 4.1.....	96
13.9.	Exim 4 в режиме фильтрации	100
13.10.	Exim 4 в режиме зеркалирования	107
13.11.	Microsoft Exchange 2010–2019 с установленным почтовым агентом	109
13.11.1.	Установка почтового агента	110
13.11.2.	Добавление источника в PT Email Security	112
13.12.	Microsoft Exchange 2010–2019 в режиме зеркалирования	112
13.13.	Postfix 3.2 в режиме фильтрации	115
13.14.	Postfix 3.2 в режиме зеркалирования	121
13.15.	PT Threat Analyzer 2.10 и выше	124
13.16.	RuPost 3.2, 4.1 в режиме фильтрации.....	125
13.16.1.	Добавление источника в PT Email Security	126
13.16.2.	Добавление правил маршрутизации проверенных писем	128
13.16.3.	Добавление доверенных сертификатов	130
13.16.4.	Включение проверки адресов получателей.....	131
13.16.5.	Настройка источника	131
13.17.	Squid 3 и выше	132
13.18.	UserGate NGFW 6, 7.1, 7.4	135
14.	Интеграция с внешними системами	139
14.1.	MaxPatrol EDR 6.0 и выше.....	139
14.2.	MaxPatrol SIEM 6.1 и выше.....	140
14.3.	PT AF 3, 4.2.1 и выше	142
14.4.	PT CS 1.1 и выше	144
14.5.	PT ISIM 5.2 и выше	146
14.6.	PT NAD 7.1 и выше.....	147
14.7.	PT NGFW 1.8 и выше	148
14.8.	PT Threat Analyzer 2.10 и выше.....	150
15.	Настройка обновления PT Email Security.....	152
16.	Просмотр конфигурации PT Email Security.....	156
17.	Мониторинг системных ресурсов в Grafana	160
18.	Смена IP-адреса узла PT Email Security	166
19.	Смена DNS-сервера	169
20.	Резервное копирование и восстановление параметров PT Email Security.....	170
21.	Обновление гипервизора Xen	172
22.	Удаление PT Email Security	175
23.	Диагностика и устранение неисправностей.....	176

24. О технической поддержке.....	179
Приложение. Сценарии отказов	183
Глоссарий.....	184

1. Об этом документе

Руководство администратора содержит справочную информацию и инструкции по настройке и администрированию Positive Technologies Email Security (далее также — PT Email Security). Руководство не содержит инструкций по использованию основных функций продукта.

Руководство адресовано специалистам, выполняющим настройку и администрирование PT Email Security.

Комплект документации PT Email Security включает в себя следующие документы:

- Этот документ.
- Руководство по внедрению — содержит информацию для внедрения продукта в инфраструктуре организации: от описания типовых конфигураций до инструкций по установке и первоначальной настройке продукта.
- Руководство специалиста по безопасности — содержит сценарии использования продукта для управления событиями информационной безопасности.
- Руководство пользователя — содержит инструкции по отправке файлов на проверку через интерфейс продукта или по электронной почте и просмотру результатов проверки.
- Руководство разработчика — содержит информацию для интеграции PT Email Security со сторонними системами.

В этом разделе

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

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

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 ОК	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом

Пример	Описание
Выполните команду <code>Stop-Service</code>	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
<code>Ctrl+Alt+Delete</code>	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о PT Email Security

Вы можете найти дополнительную информацию о PT Email Security на справочном портале help.ptsecurity.com и на [Позитивном портале](#). Через Позитивный портал вы также можете обратиться [в техническую поддержку \(см. раздел 24\)](#).

2. О PT Email Security

Positive Technologies Email Security (PT Email Security) — система многоуровневой защиты от угроз электронной почты с функциями почтового шлюза и почтового транспортного агента. В системе применяются различные средства статического и динамического анализа объектов, включая антифишинг- и антиспам-проверку, антивирусное сканирование, репутационный, ретроспективный и поведенческий анализ.

PT Email Security предназначен для выявления вредоносных объектов, предотвращения их проникновения и распространения в IT-инфраструктуре организации. Многоуровневая проверка позволяет повысить вероятность обнаружения объектов с угрозами.

PT Email Security может использоваться специалистами по информационной безопасности, администраторами и аналитиками SOC для анализа подозрительных объектов и расследования инцидентов информационной безопасности.

PT Email Security предоставляет следующие основные возможности:

- Инструменты для работы с письмами:
 - Почтовый шлюз безопасности с фильтрацией подключений.
 - Встроенный почтовый транспортный агент.
 - Обработка писем в зависимости от отправителя и получателей.
 - Обезвреживание писем с угрозами.
 - Карантин для подозрительных писем.
- Многоуровневая проверка объектов с использованием методов статического и динамического анализа:
 - Поведенческий анализ файлов в различных операционных системах.
 - Антивирусная проверка файлов.
 - Проверка файлов по YARA-правилам, разработанным специалистами экспертного центра Positive Technologies.
 - Проверка исполняемых файлов Windows с использованием машинного обучения.
 - Проверка файлов и ссылок по индикаторам компрометации.
 - Антифишинг- и антиспам-проверка писем.
 - Проверка адресов в письмах по спискам DNS-блокировок.
 - Ретроспективный анализ файлов в хранилище.

- Настраиваемые пользователем средства проверки:
 - Черный и белый списки файлов.
 - Проверка файлов по пользовательским YARA-правилам.
 - Пользовательские правила определения файлов и ссылок с угрозами.
- Экспертные инструменты для проверки объектов и расследования инцидентов:
 - Гибкий поиск заданий и объектов с использованием языка запросов QL.
 - Проверка объектов по базам VirusTotal и PT Fusion.
 - Поведенческий анализ файлов в интерактивном режиме.
 - Диаграммы поведенческого анализа.
- Быстрая проверка объектов через веб-интерфейс или по электронной почте.
- Поточковая проверка объектов, поступающих из различных источников:
 - Почтовый трафик серверов электронной почты с возможностью блокировки писем с угрозами.
 - Объекты от ICAP-клиентов с возможностью блокировки объектов с угрозами.
 - Объекты из файловых хранилищ и файловых шлюзов.
 - Объекты, передаваемые через публичный API PT Email Security.
- Интеграция с продуктами Positive Technologies:
 - MaxPatrol EDR.
 - MaxPatrol SIEM.
 - PT AF.
 - PT ISIM.
 - PT NAD.
 - PT NGFW.
 - PT Threat Analyzer.

PT Email Security также предоставляет дополнительные возможности:

- Мониторинг проверки объектов и обнаруженных угроз.
- Отправка почтовых уведомлений об угрозах.
- Управление очередью файлов, направляемых на поведенческий анализ.
- Управление приоритетами источников и типов файлов при поведенческом анализе.
- Формирование отчетов по заданиям и проверенным объектам.

- Скачивание проверенных файлов из хранилища.
- Мониторинг работы PT Email Security в Grafana с возможностью отправки почтовых уведомлений.

3. Что нового в версии 5.37

Ниже приводится список изменений, которые появились в PT Email Security.

Проверка исполняемых файлов с использованием машинного обучения

Теперь для проверки исполняемых PE-файлов Windows в PT Email Security используется средство проверки PT ML на основе технологии машинного обучения. Оно выявляет вредоносный код с помощью предварительно обученной модели ByteDog, разработанной специалистами Positive Technologies. Модель анализирует содержимое файла как последовательность байтов и выявляет закономерности, характерные для вредоносного кода. Это позволяет выявлять как известные, так и угрозы, которые не встречались в данных для обучения модели.

Создание собственных ролей пользователей PT Email Security

Теперь в PT MC вы можете создавать собственные роли для пользователей PT Email Security и настраивать их привилегии. Вы также можете копировать стандартные роли и изменять набор привилегий в созданных копиях.

Добавлена стандартная роль «Аудитор безопасности», которая позволяет просматривать действия других пользователей.

Списки для хранения адресов

Теперь в PT Email Security вы можете создавать списки для хранения адресов. В одном списке можно хранить IP-адреса, подсети, адреса электронной почты и домены. Список можно использовать в нескольких правилах приема и обработки писем, чтобы не перечислять адреса в каждом правиле. При изменении списка актуальный набор адресов автоматически применяется во всех правилах, где он используется.

Вы можете добавлять и удалять сразу несколько адресов, а также задавать срок их действия. После истечения срока адрес остается в списке, но больше не учитывается при применении правил. В истории изменений можно узнать, кто и когда изменил список или адреса, и просмотреть комментарии к этим действиям.

4. Компоненты PT Email Security

В состав PT Email Security входят следующие компоненты:

- Встроенный PT MC — компонент, отвечающий за аутентификацию и авторизацию пользователей PT Email Security (пользовательские данные хранятся в базе данных под управлением СУБД PostgreSQL).

Примечание. При использовании встроенного PT MC не рекомендуется интегрировать его с другими площадками в иерархии и не рекомендуется подключать к нему другие продукты.

Примечание. Встроенный PT MC может быть заменен на внешний экземпляр.

- Веб-интерфейс — компонент графического пользовательского интерфейса PT Email Security, доступный в браузере.
- Ядро проверки — компонент, который отправляет объекты на проверку и контролирует выполнение проверки.
- Модуль поведенческого анализа — компонент, отвечающий за проверку файлов методом поведенческого анализа.
- Хранилище файлов — компонент, отвечающий за хранение полученных извне файлов на жестком диске.
- База данных — компонент под управлением СУБД ClickHouse, который обеспечивает хранение данных о заданиях и файлах.
- API базы данных — компонент, который обеспечивает отображение информации из базы данных в веб-интерфейсе PT Email Security.
- Служба Updater — компонент, который обеспечивает скачивание и установку обновлений PT Email Security и образов VM. Включает в себя функции работы с лицензией продукта.
- Служба высокой доступности Keeralived — компонент, который обеспечивает доступность всех узлов отказоустойчивого кластера PT Email Security на одном IP-адресе.

5. Требования к рабочим станциям

К рабочим станциям администраторов PT Email Security, выдвигаются следующие аппаратные и программные требования:

- Разрешение монитора — Full HD (не менее 1920 × 1080 пикселей).
- Браузер — Google Chrome версии 148, Microsoft Edge 148, Mozilla Firefox 150, «Яндекс Браузер» 26.4 или более новых версий.
- На узле должны быть разрешены исходящие подключения к портам TCP 22, 80, 443, 3334.
- Если на узле установлен антивирус:
 - В исключения антивируса должны быть добавлены правила, которые разрешают доступ к основному узлу PT Email Security и используемым прокси-серверам по протоколам HTTP и HTTPS.
 - В PT Email Security должен быть установлен пользовательский SSL-сертификат, выпущенный доверенным центром сертификации.

6. Настройка аутентификации

Вход пользователей в PT Email Security выполняется через компонент PT MC, который обеспечивает единый механизм аутентификации пользователей в продуктах Positive Technologies. Для аутентификации может использоваться встроенный или внешний PT MC.

Для входа в PT MC используется адрес вида `https://<Адрес PT Email Security>:3334`.

При этом в качестве адреса PT Email Security необходимо указать:

- Если установлена конфигурация с отказоустойчивым кластером, — виртуальный IP-адрес службы Keeralived.
- Если используется другая конфигурация PT Email Security, — IP-адрес основного узла.

Для первого входа в PT MC используется стандартная учетная запись суперпользователя Administrator с паролем P@ssw0rd. Эта учетная запись предоставляет неограниченные права в PT Email Security и встроенном PT MC.

Внимание! В целях безопасности сразу после первого входа в PT MC вам необходимо сменить пароль учетной записи суперпользователя.

Учетные записи пользователей PT Email Security создаются в PT MC, там же пользователям назначаются роли. Для входа пользователей в PT Email Security могут использоваться локальные учетные записи PT MC, учетные записи из служб каталогов по протоколу LDAP, а также единый вход через сторонние SSO-системы по протоколу SAML 2.0. Для LDAP-аутентификации поддерживаются службы каталогов Microsoft Active Directory и FreeIPA.

Примечание. Инструкции по работе с пользователями и правами доступа в PT MC приведены [в технической документации компонента](#). Если вы используете встроенный PT MC, следуйте инструкциям для версии 101.20. Если подключен внешний PT MC, используйте инструкции для подключенной версии.

Настройка аутентификации по LDAP

В PT MC можно настроить вход в PT Email Security по протоколу LDAP. В этом случае логины и пароли пользователей хранятся в службе каталогов, а PT MC использует LDAP-подключение для проверки учетных данных. По умолчанию персональная и организационная информация также загружается из службы каталогов, но при необходимости ее можно указать или изменить в PT MC.

Для настройки LDAP-подключения следуйте инструкциям в технической документации PT MC. Вы можете подключить один или несколько LDAP-серверов и при необходимости настроить синхронизацию со службой каталогов.

Если вы используете встроенный PT MC и подключение к LDAP-серверу должно выполняться по защищенному соединению LDAPS, необходимо установить доверенный сертификат корневого центра сертификации этого сервера на основной узел PT Email Security. Сертификат можно получить у администратора службы каталогов.

Внимание! Необходимо использовать сертификат в виде файла X.509 в кодировке Base64.

- Чтобы установить доверенный сертификат для LDAPS,

выполните команду:

```
sudo ptmsctl auth use-local --ldaps-ca-crt <Путь к файлу сертификата>
```

Примечание. Повторное выполнение команды заменяет ранее установленный сертификат.

Например:

```
sudo ptmsctl auth use-local --ldaps-ca-crt /home/user/certificate_ca.crt
```

Доверенный сертификат для LDAPS установлен.

Роли пользователей

Для учетных записей пользователей PT Email Security используется ролевая модель управления доступом. Предусмотрены следующие стандартные роли: администратор, аудитор безопасности, пользователь и специалист по безопасности. Доступные для каждой роли привилегии указаны в таблице.

Вы можете создавать собственные роли и настраивать для них привилегии, необходимые для выполнения задач пользователей. Кроме того, можно копировать стандартные роли и изменять набор привилегий в созданных копиях.

Примечание. При создании учетной записи можно назначить ей одновременно несколько ролей. Например, вы можете создать еще одну учетную запись суперпользователя, назначив ей все четыре роли.

Таблица 2. Привилегии ролей пользователей

Привилегия	Роль пользователя			
	Админи-стратор	Аудитор безопасности	Пользователь	Специалист по безопасности
Мониторинг				
Просмотр страницы Сводка	Да	Да	—	Да
Просмотр страниц Компоненты, Узлы, Поды	Да	Да	—	Да
Просмотр дашбордов в Grafana	Да	Да	—	Да
Настройка дашбордов в Grafana	Да	—	—	—
Задания				
Просмотр карточек заданий и объектов	Да	Да	Да	Да

Привилегия	Роль пользователя			
	Администратор	Аудитор безопасности	Пользователь	Специалист по безопасности
Скачивание списка заданий в формате CSV	Да	Да	—	Да
Скачивание отчета по заданию в формате PDF	Да	Да	Да	Да
Просмотр страницы Задания	Да	Да	Да	Да
Объекты				
Просмотр содержимого письма	Да	Да	Да	Да
Просмотр заголовков письма	Да	Да	Да	Да
Просмотр содержимого артефактов поведенческого анализа	—	Да	—	Да
Скачивание списка объектов в формате CSV	Да	Да	—	Да
Скачивание диагностических данных и файлов задания	—	Да	—	Да
Скачивание файлов из хранилища	—	Да	—	Да
Скачивание результатов поведенческого анализа	—	Да	—	Да
Просмотр страницы Объекты	Да	Да	Да	Да
Очередь обработки писем МТА				
Просмотр карточки обработки письма МТА	Да	Да	—	Да
Повторная отправка недоставленного письма	Да	—	—	—
Просмотр страницы Очередь обработки МТА	Да	Да	—	Да
События по письмам				
Просмотр страницы События по письмам	Да	Да	—	Да
Карантин для писем				
Доступ к панели карантина в карточке задания	—	Да	—	Да

Привилегия	Роль пользователя			
	Администратор	Аудитор безопасности	Пользователь	Специалист по безопасности
Изменение статуса просмотра письма и комментария к письму в карантине	—	—	—	Да
Удаление письма из карантина	—	—	—	Да
Выпуск письма из карантина	—	—	—	Да
Переадресация письма из карантина	—	—	—	Да
Просмотр страницы Карантин	—	Да	—	Да
Средства проверки				
Просмотр страниц раздела Средства проверки	Да	Да	—	Да
Включение и отключение средства проверки	Да	—	—	Да
Изменение параметров средства проверки	Да	—	—	—
Изменение параметров проверки объектов	—	—	—	Да
Установка дополнительного антивируса	Да	—	—	—
Обновление лицензии дополнительного антивируса	Да	—	—	—
Удаление дополнительного антивируса	Да	—	—	—
Просмотр черного списка	—	—	—	Да
Изменение черного списка	—	—	—	Да
Импорт записей в черный список	—	—	—	Да
Экспорт записей из черного списка	—	—	—	Да
Очистка черного списка	—	—	—	Да
Просмотр белого списка	—	—	—	Да
Изменение белого списка	—	—	—	Да
Импорт записей в белый список	—	—	—	Да

Привилегия	Роль пользователя			
	Администратор	Аудитор безопасности	Пользователь	Специалист по безопасности
Экспорт записей из белого списка	—	—	—	Да
Очистка белого списка	—	—	—	Да
Перевод тестовых YARA-правил в действующие	—	—	—	Да
Поведенческий анализ				
Просмотр страницы Очередь файлов на анализ	Да	Да	—	Да
Изменение порядка файлов в очереди на анализ	—	—	—	Да
Очистка очереди файлов на анализ	—	—	—	Да
Добавление образа VM	Да	—	—	Да
Просмотр карточки образа VM	Да	Да	—	Да
Удаление образа VM	Да	—	—	Да
Скачивание образа VM	Да	—	—	Да
Просмотр страницы Управление образами VM	Да	Да	—	Да
Просмотр страницы Очередь обновления образов VM	Да	Да	—	Да
Изменение порядка образов VM в очереди на обновление	Да	—	—	Да
Источники				
Добавление источника	Да	—	—	—
Просмотр карточки источника	Да	Да	—	Да
Настройка параметров источника	Да	—	—	—
Настройка правил приема писем	Да	—	—	Да
Настройка параметров проверки объектов	—	—	—	Да
Настройка правил обработки писем	—	—	—	Да
Включение и отключение блокировки объектов	—	—	—	Да

Привилегия	Роль пользователя			
	Администратор	Аудитор безопасности	Пользователь	Специалист по безопасности
Удаление источника	Да	—	—	—
Скачивание файлов журнала источника	Да	Да	—	Да
Просмотр страницы Источники	Да	Да	—	Да
Параметры системы				
Просмотр страницы параметров Проверка объектов	Да	Да	—	Да
Просмотр страницы параметров поведенческого анализа Время хранения результатов	Да	Да	—	Да
Просмотр страницы параметров поведенческого анализа Приоритет файлов	Да	Да	—	Да
Просмотр страницы параметров поведенческого анализа Режим обновления образов VM	Да	Да	—	Да
Просмотр страницы параметров Хранилище	Да	Да	—	—
Просмотр страницы параметров Карантин	Да	Да	—	—
Просмотр страницы параметров Публичный API	Да	Да	—	—
Просмотр страницы параметров Очередь обработки писем MTA	Да	Да	—	—
Просмотр страницы параметров Уведомления	Да	Да	—	—
Просмотр страницы параметров Почтовый шлюз безопасности	Да	Да	—	—
Изменение параметров проверки объектов	Да	—	—	—
Изменение времени хранения результатов поведенческого анализа	—	—	—	Да

Привилегия	Роль пользователя			
	Администратор	Аудитор безопасности	Пользователь	Специалист по безопасности
Изменение правил определения приоритета файлов при поведенческом анализе	—	—	—	Да
Изменение режима и расписания обновления образов VM	Да	—	—	Да
Изменение параметров хранилища	Да	—	—	—
Изменение параметров карантина	Да	—	—	—
Изменение параметров публичного API	Да	—	—	—
Изменение параметров очереди обработки писем MTA	Да	—	—	—
Изменение параметров уведомлений	Да	—	—	—
Изменение параметров почтового шлюза безопасности	Да	—	—	—
Добавление агента почтового шлюза	Да	—	—	—
Изменение параметров агента почтового шлюза	Да	—	—	—
Удаление агента почтового шлюза	Да	—	—	—
Просмотр страницы Агенты почтового шлюза	Да	Да	—	—
Создание списка адресов	Да	—	—	Да
Просмотр адресов в списке	Да	Да	—	Да
Изменение списка адресов	Да	—	—	Да
Удаление списка адресов	Да	—	—	Да
Просмотр страницы Списки адресов	Да	Да	—	Да
Создание токена доступа к публичному API	Да	—	—	—
Добавление комментария к токenu доступа	Да	—	—	—

Привилегия	Роль пользователя			
	Администратор	Аудитор безопасности	Пользователь	Специалист по безопасности
Отзыв токена доступа	Да	—	—	—
Просмотр страницы Токены доступа	Да	Да	—	Да
Просмотр страницы Обновления	Да	Да	—	—
Настройка расписания обновления	Да	—	—	—
Ручной запуск обновления	Да	—	—	—
Просмотр страницы Лицензия	Да	Да	—	Да
Активация и замена лицензии	Да	—	—	—
Скачивание файлов системных журналов	Да	Да	—	Да
Веб-интерфейс				
Просмотр списка приложений, доступных через единый вход	Да	Да	—	Да
Просмотр уведомлений о проверке объектов	Да	Да	Да	Да
Просмотр системных уведомлений	Да	Да	—	Да
Проверка объектов через веб-интерфейс	Да	Да	Да	Да
Включение поведенческого анализа и выбор образа VM	Да	—	Да	Да
Изменение параметров поведенческого анализа	—	—	—	Да
Использование тестовых YARA-правил	—	—	—	Да
Доступ к заданиям				
Доступ ко всем заданиям	—	Да	—	Да
Доступ только к своим заданиям	Да	—	Да	—

7. Вход в PT Email Security

Вход в PT Email Security выполняется с помощью компонента PT MC, который обеспечивает единый механизм входа в продукты Positive Technologies.

Для входа в PT Email Security вам понадобится адрес веб-интерфейса PT Email Security и данные учетной записи.

► Чтобы войти в PT Email Security:

1. В адресной строке браузера введите адрес веб-интерфейса PT Email Security и нажмите клавишу Enter.

Откроется страница входа в PT Email Security или страница для анонимной проверки объектов.

2. Нажмите кнопку **Войти**.

Откроется страница входа в PT MC.

3. Если вы используете доменную учетную запись, выберите вкладку **LDAP**.

4. Введите данные учетной записи.

5. Нажмите кнопку **Войти**.

Откроется веб-интерфейс PT Email Security.

8. Интерфейс PT Email Security

Работа с PT Email Security выполняется через веб-интерфейс. Все передаваемые при работе данные защищаются при помощи HTTPS с использованием SSL-сертификата. Сертификат может быть как самоподписанным, так и выданным официальным центром сертификации.

Главное меню

Для доступа пользователей к страницам веб-интерфейса и основным функциям PT Email Security используется главное меню. В главном меню расположены следующие элементы управления.

 — кнопка для перехода между приложениями Positive Technologies, которые зарегистрированы в сервисе управления пользователями и доступом PT MC.

Разделы для перехода к страницам веб-интерфейса:

- **Задания** — для работы с заданиями на проверку объектов.
- **Объекты** — для работы с объектами в хранилище.
- **Средства проверки** — содержит пункты для перехода к следующим страницам:
 - **Экспертиза PT** — для работы со средствами проверки, которые разработаны специалистами Positive Technologies.
 - **Антивирусы** — для работы с антивирусами сторонних разработчиков, которые используются при проверке файлов.
 - **Пользовательские правила** — для работы со средством проверки объектов по пользовательским YARA-правилам.
- **Источники** — содержит пункты для перехода к следующим страницам:
 - **Управление источниками** — для работы с источниками, от которых поступают объекты на проверку.
 - **Агенты почтового шлюза** — для работы с агентами, которые обеспечивают передачу писем от почтовых шлюзов безопасности в PT Email Security на проверку.
 - **Токены доступа** — для работы с токенами для доступа к PT Email Security через публичный API.

— **Система** — содержит пункты для перехода к следующим страницам:

- **Параметры** — содержит пункты для перехода на страницы настройки PT Email Security.
- **Обновления** — для работы с обновлениями PT Email Security.
- **Конфигурация** — содержит пункты для перехода к страницам с информацией о настроенной конфигурации, компонентах, узлах и подах PT Email Security, а также для мониторинга системных ресурсов узлов с помощью средства визуализации и мониторинга данных Grafana.
- **Лицензия** — для работы с лицензией PT Email Security.

Проверить объекты — кнопка для проверки объектов через веб-интерфейс.

Также в главном меню расположены значки:



— для просмотра уведомлений о проверке объектов, отправленных вами через интерфейс. На значке отображается количество проверенных объектов. По ссылке в уведомлении вы можете открыть карточку задания, в котором проверен объект.



— для просмотра уведомлений о работе компонентов PT Email Security и доступных обновлениях. На значке отображается количество новых уведомлений. При нажатии на значок вы можете:

- Посмотреть версию PT Email Security.
- Скачать файлы журналов PT Email Security.
- Перейти на сайт технической поддержки Positive Technologies.



— для просмотра логина, под которым вы вошли в PT Email Security. При нажатии на значок вы можете:

- Сменить тему оформления и язык интерфейса.
- Выйти из PT Email Security.

Смена языка и темы оформления интерфейса

Интерфейс PT Email Security доступен на русском и английском языках в светлой и темной темах оформления. По умолчанию выбраны русский язык и светлая тема.

► Чтобы сменить язык интерфейса,

в главном меню выберите → **Язык** → **<Название языка>**.

► Чтобы сменить тему интерфейса,

в главном меню выберите → **Тема** → **<Название темы>**.

Примечание. Для выбора темы, соответствующей оформлению интерфейса ОС, вы можете выбрать **Системная**.

Аудит действий пользователей

В PT Email Security реализован аудит действий пользователей. Регистрируются события безопасности, связанные со следующими действиями пользователей:

- просмотр заданий;
- скачивание результатов проверки и файлов из хранилища;
- очистка очереди файлов на поведенческий анализ;
- просмотр и выпуск писем из карантина;
- изменение параметров проверки источников;
- работа с источниками (добавление, удаление, включение, отключение и изменение параметров);
- работа с антивирусами и (установка, удаление, включение и отключение);
- работа со средствами проверки Positive Technologies (включение, отключение и изменение параметров);
- работа с черным и белым списками (очистка, скачивание);
- работа с записями в черном и белом списках (добавление, удаление, перемещение между списками, добавление комментариев);
- работа с токенами доступа (создание, добавление комментария, привязка к источнику и отзыв);
- работа с образами виртуальных машин (добавление, удаление и скачивание);
- скачивание файлов журналов;
- изменение основных параметров PT Email Security;
- запуск обновления PT Email Security и изменение параметров автоматического обновления;
- замена лицензии PT Email Security.

Кроме того, регистрируются события безопасности, связанные со следующими автоматическими действиями PT Email Security:

- обновление PT Email Security по расписанию;
- обновление антивирусов, антивирусных баз, средств проверки Positive Technologies и их баз знаний.

Все зарегистрированные события отображаются в журнале действий PT MC.

9. Лицензирование

Чтобы использовать PT Email Security, вам нужно приобрести и активировать лицензию. Для приобретения лицензии или изменения параметров уже приобретенной лицензии вы можете обратиться в техническую поддержку Positive Technologies.

Если вы не вводили серийный номер лицензии при установке PT Email Security, вам нужно активировать лицензию после установки.

Чтобы активировать лицензию, приобретенную вашей организацией, вам нужно ввести серийный номер этой лицензии в интерфейсе PT Email Security. Серийный номер указывается в файле `serial number.txt` на установочном диске из комплекта поставки или высылается в электронном письме на адрес, указанный при заказе лицензии.

Замена лицензии может потребоваться в следующих случаях:

- Одна и та же лицензия была активирована в нескольких экземплярах PT Email Security. Поскольку одна лицензия может использоваться только в одном экземпляре продукта, вам нужно заменить лицензии так, чтобы в каждом экземпляре была активирована своя лицензия.

Примечание. При нехватке лицензий вашей организации нужно докупить их.

- Лицензия была активирована не в том экземпляре PT Email Security. Например, лицензия, которая позволяет проверять только почтовый трафик организации, была активирована в экземпляре, который вы устанавливали исключительно для самостоятельной проверки файлов пользователями.
- Конфигурация сервера с установленным PT Email Security менялась более трех раз (например, заменялись комплектующие сервера), вследствие чего лицензия стала недействительной. В таком случае вам нужно обратиться в техническую поддержку Positive Technologies для получения новой лицензии с теми же параметрами.

Управление лицензией осуществляется на странице **Система** → **Лицензия**.

↔ Заменить лицензию

↺ Проверить лицензию

Проверена 12 февраля, 10:58

Лицензия

№ 4 · Bn4s3M-*-OIAYBC**

✓ Действительна до 3 июня 2025

Образы VM

Доступные образы виртуальных машин для поведенческого анализа

win10-1803-x64

win7-sp1-x64

astralinux-orel-x64

win7-sp1-x64-ics

redos-murom-x64

astralinux-smolensk-x64

win10-22H2-x64

ubuntu-jammy-x64

Источники

Стандартные

Служба Checkme, веб-интерфейс для проверки файлов, расширенный API, API

Лимит обработки

∞

Электронная почта

Почтовый сервер в режиме фильтрации, почтовый сервер в режиме зеркалирования, почтовый сервер с установленным агентом

5 адресов

1 × 5

Сетевой трафик

ICAP-сервер, PT NAD

500 Мбит/с

1 × 500 Мбит/с

Сетевое хранилище

Общая папка, папка-шлюз

1

Рисунок 1. Страница **Лицензия**

В рабочей области страницы расположены:

- Кнопка **Заменить лицензию** для ввода серийного номера новой лицензии.
- Кнопка **Проверить лицензию** для обновления информации о параметрах текущей лицензии. Рядом с кнопкой также отображается дата последней проверки.

- Номер текущей лицензии и срок ее действия.
- Источники для проверки и лимит их обработки в рамках текущей лицензии.

▶ Чтобы активировать или заменить лицензию в веб-интерфейсе:

1. В главном меню выберите **Система** → **Лицензия**.
2. Нажмите кнопку **Заменить лицензию**.
3. Введите серийный номер лицензии и нажмите кнопку **Заменить**.

Примечание. Рекомендуется сравнить параметры лицензии, перечисленные на странице, с указанными при заказе лицензии. В случае несоответствия вам нужно обратиться в техническую поддержку Positive Technologies.

10. Настройка средств проверки

Через интерфейс PT Email Security вы можете настраивать средства статического и динамического анализа объектов. В зависимости от средства проверки возможности по настройке различаются. Вы можете:

- Включить или выключить средства проверки Positive Technologies, основные или дополнительные антивирусы, проверку через пользовательские YARA-правила.
- Выбрать источники индикаторов компрометации, который будет использоваться PT IoC для проверки файлов и ссылок.
- Выбрать способ проверки ссылок, который будет использоваться PT Crawler.
- Настроить отличный от основного прокси-сервер HTTP, который будет использоваться для проверки ссылок через PT Crawler.
- Установить и обновить дополнительные антивирусы.

Кроме того, вы можете настроить параметры поведенческого анализа с помощью консольных команд: отключить или включить проверку цифровой подписи кода приложений Windows и отключить или включить проверку артефактов поведенческого анализа для ОС семейства Linux.

В этом разделе

[Настройка лимитов на размер извлекаемых файлов \(см. раздел 10.1\)](#)

[Настройка средств проверки Positive Technologies \(см. раздел 10.2\)](#)

[Настройка антивирусов \(см. раздел 10.3\)](#)

[Настройка поведенческого анализа \(см. раздел 10.4\)](#)

[Работа с пользовательскими YARA-правилами \(см. раздел 10.5\)](#)

10.1. Настройка лимитов на размер извлекаемых файлов

С помощью консольных команд вы можете настроить максимальный размер извлекаемых дочерних файлов. Инструкции необходимо выполнять на основном узле.

Настройка лимитов распаковщика

Компонент Unpacker извлекает дочерние файлы из поступивших на проверку файлов. По умолчанию на размер дочернего файла установлено ограничение в 512 МБ. Если файл превышает этот размер, то извлекается фрагмент файла размером 512 МБ.

- Чтобы настроить максимальный размер файлов, извлекаемых Unpacker,

выполните команду:

```
sudo ptmsctl system components set -c unpacker -p max_unpacked_size=<Размер в байтах>
```

Например:

```
sudo ptmsctl system components set -c unpacker -p max_unpacked_size=268435456
```

Настройка лимитов средства проверки PT ESC

Средство проверки PT ESC при проверке файлов также извлекает и проверяет дочерние файлы. Ограничение на размер дочернего файла по умолчанию не установлено. Извлеченные дочерние файлы не отображаются в карточке задания.

Примечание. Ограничение на размер дочернего файла не распространяется на файлы PDF, извлекаемые OLE-объекты и изображения.

- ▶ Чтобы настроить максимальный размер файлов, извлекаемых PT ESC,

выполните команду:

```
sudo ptmsctl system components set -c ptesc -p max_unpack_file_size=<Размер в байтах>
```

Например:

```
sudo ptmsctl system components set -c ptesc -p max_unpack_file_size=<Размер в байтах>
```

- ▶ Чтобы снять ограничение на максимальный размер файлов, извлекаемых PT ESC,

выполните команду:

```
sudo ptmsctl system components set -c ptesc -p max_unpack_file_size=
```

10.2. Настройка средств проверки Positive Technologies

Для проверки объектов PT Email Security может использовать средства проверки, разработанные специалистами компании Positive Technologies. Для настройки таких средств проверки предназначена страница **Средства проверки** → **Экспертиза РТ**.

Статический анализ

PT ESC

Positive Technologies Expert Security Center

Версия 5.37.0.153025

Версия базы знаний 7.0.0.132 от 7 сен, 14:36

Проверяются Файлы, dropped файлы, дампы памяти, заголовки писем, AMSI-скрипты, DEX-дампы

PT IoC

Positive Technologies Indicators of Compromise

Версия 5.37.0.154997

Версия базы знаний 1.2.0.6054 от 7 сен, 15:07

Включенные источники Positive Technologies, ФСТЭК России

PT ML

Positive Technologies Machine Learning

Версия 5.37.0.154997

Версия базы знаний 4.0.0.82 от 7 сен, 14:34

Обработка ссылок

PT Crawler

Positive Technologies Crawler

Версия 5.37.0.154997

Способ проверки ссылок Простой

[Параметры](#)

PT Categorizer

Positive Technologies Categorizer

Версия 5.37.0.154997

Версия базы знаний 1.0.0.2376 от 7 сен, 14:14

Поведенческий анализ

PT ML

Positive Technologies Machine Learning

Версия 5.37.0.154997

Версия базы знаний 4.0.0.82 от 7 сен, 14:34

PT DPI

Positive Technologies Deep Packet Inspection

Версия 12.4.10321

Версия сетевых правил 2.1.0.7655 от 7 сен, 12:49

Защита от угроз в почте

PT Anti-Phishing and Anti-Spam

Positive Technologies Anti-Phishing and Anti-Spam

Версия 5.37.0.155324

Версия базы знаний 1.0.0.121 от 7 сен, 14:34

[Параметры](#)

Рисунок 2. Страница Экспертиза PT

В рабочей области страницы расположены панели с информацией о средствах проверки, разделенные с помощью заголовков на группы:

- **Статический анализ** — средства проверки, использующие методы проверки, относящиеся к статическому анализу:
 - PT ESC — средство статического анализа на основе YARA-правил. По ссылке **Параметры** вы можете выбрать типы проверяемых объектов.
 - PT IoC — средство обнаружения индикаторов компрометации в файлах и ссылках. По ссылке **Параметры** вы можете выбрать источники индикаторов компрометации.
 - PT ML — средство проверки на основе технологии машинного обучения. При статическом анализе используется для проверки исполняемых PE-файлов Windows.
- **Обработка ссылок** — средства проверки, предназначенные для работы со ссылками:
 - PT Crawler — средство динамической проверки ссылок. По ссылке **Параметры** вы можете выбрать способ проверки и указать прокси-сервер, который будет использоваться только при проверке ссылок.
 - PT Categorizer — средство категоризации ссылок. По ссылке **Параметры** вы можете указать имена доменов, исключаемых при категоризации ссылок. Ссылкам с такими доменами не будут присваиваться категории.
- **Поведенческий анализ** — средства проверки, использующие методы проверки, относящиеся к поведенческому анализу:
 - PT ML — средство проверки на основе технологии машинного обучения. При поведенческом анализе используется для анализа сетевого трафика.
 - PT DPI — средство поведенческого анализа сетевых пакетов.
- **Защита от угроз в почте** — средства проверки, предназначенные для проверки писем:
 - PT Anti-Phishing and Anti-Spam — средство проверки для выявления признаков фишинга и спама в письмах, а также для проверки найденных в письмах IP-адресов и имен доменов по спискам DNS-блокировок. По ссылке **Параметры** вы можете указать DNS-серверы для разрешения адресов.

Отключение и включение средства проверки Positive Technologies

Примечание. После включения средства проверки начнется обновление его базы знаний, что может занять продолжительное время. Средство проверки начнет работать только после завершения обновления.

- Чтобы отключить (включить) средство проверки:
 1. В главном меню выберите **Средства проверки** → **Экспертиза РТ**.
 2. В панели с информацией о средстве проверки отключите (включите) его.

Статус средства проверки изменится на **Отключен (Включен)**.

Выбор объектов для проверки PT ESC

► Чтобы выбрать объекты для проверки PT ESC:

1. В главном меню выберите **Средства проверки** → **Экспертиза РТ**.
2. В панели с информацией о PT ESC перейдите по ссылке **Параметры**.
3. В блоке параметров **Объекты для проверки** выберите объекты.
4. Нажмите кнопку **Сохранить**.

Выбор источников индикаторов компрометации для PT IoC

Для проверки файлов и ссылок по индикаторам компрометации можно использовать индикаторы из базы знаний Positive Technologies и индикаторы, полученные от ФСТЭК России.

► Чтобы выбрать источники индикаторов компрометации для PT IoC:

1. В главном меню выберите **Средства проверки** → **Экспертиза РТ**.
2. В панели с информацией о PT IoC перейдите по ссылке **Параметры**.
3. В блоке параметров **Источники индикаторов компрометации** выберите источники.
4. Нажмите кнопку **Сохранить**.

Добавление прокси-сервера для проверки ссылок

Вы можете добавить прокси-сервер, который будет использоваться PT Email Security только при проверке ссылок в объектах от источников.

Внимание! PT Email Security поддерживает подключение к прокси-серверу только по протоколу HTTP.

Для проверки ссылок можно использовать отдельный прокси-сервер или прокси-сервер, развернутый на основном узле PT Email Security. Если используется конфигурация с отказоустойчивым кластером, прокси-сервер необходимо развернуть и на резервных узлах аналогичным образом.

Для работы прокси-сервера на узле PT Email Security должен быть добавлен отдельный сетевой интерфейс с назначенным IP-адресом. Сетевой интерфейс должен быть настроен в отдельной подсети. В этой подсети должен быть зарезервирован диапазон не менее чем из двух IP-адресов для реплик прокси-сервера. В той же подсети должен быть доступен шлюз для обращения к внешним сетям.

Внимание! IP-адреса из указанного диапазона адресов подсети не должны использоваться другими узлами, сервисами или сетевыми устройствами.

- Чтобы установить прокси-сервер для проверки ссылок на узле,

выполните команду:

```
sudo ptmsctl system dirty-proxy add \
--node-name <Имя узла PT Email Security> \
--iface <Имя сетевого интерфейса> \
--subnet <Адрес подсети в формате CIDR> \
--ip-range-start <Первый IP-адрес диапазона> \
--ip-range-end <Последний IP-адрес диапазона> \
--gateway <IP-адрес шлюза> \
--nservers "<Список IP-адресов DNS-серверов>"
```

Например:

```
sudo ptmsctl system dirty-proxy add \
--node-name example-master \
--iface interface \
--subnet 198.51.100.0/24 \
--ip-range-start 198.51.100.20 \
--ip-range-end 198.51.100.21 \
--gateway 198.51.100.1 \
--nservers "192.0.2.53 203.0.113.53"
```

Прокси-сервер для проверки ссылок доступен по адресу <http://proxy:3333>. Для доступа к этому прокси-серверу аутентификация не требуется.

- Чтобы добавить прокси-сервер для проверки ссылок в PT Email Security:

1. В главном меню выберите **Средства проверки** → **Экспертиза РТ**.
2. В панели с информацией о PT Crawler перейдите по ссылке **Параметры**.
3. В блоке параметров **Прокси-сервер для проверки ссылок** в поле **URL-адрес** введите:
 - Если используется отдельный прокси-сервер, — адрес в формате <http://<Доменное имя или IP-адрес>:<Порт>>.
 - Если прокси-сервер развернут на узле PT Email Security, — <http://proxy:3333>.
4. Если для доступа к прокси-серверу требуется аутентификация, в поля **Логин** и **Пароль** введите учетные данные.
5. Нажмите кнопку **Сохранить**.

Выбор способа проверки ссылок

Предусмотрены простой и расширенный способы проверки ссылок. В обоих случаях контент по ссылкам скачивается с помощью HTTP/HTTPS-клиента. При расширенном способе проверки, если контент имеет формат HTML, после скачивания формируется полноценная веб-страница: загружаются все связанные ресурсы и выполняются сценарии JavaScript. Это позволяет выявлять динамически создаваемые элементы и потенциально вредоносные сценарии.

► Чтобы выбрать способ проверки ссылок:

1. В главном меню выберите **Средства проверки** → **Экспертиза РТ**.
2. В панели с информацией о PT Crawler перейдите по ссылке **Параметры**.
3. В блоке параметров **Способ проверки ссылок** выберите способ.
4. Нажмите кнопку **Сохранить**.

Настройка категоризации ссылок

При проверке ссылок PT Email Security выполняет категоризацию ссылок и устанавливает для них соответствующие метки. Вы можете указать имена доменов, исключаемых при категоризации ссылок. Ссылкам с такими доменами не будут присваиваться категории.

► Чтобы указать имена доменов, исключаемых при категоризации ссылок:

1. В главном меню выберите **Средства проверки** → **Экспертиза РТ**.
2. В панели с информацией о PT Categorizer перейдите по ссылке **Параметры**.
3. В поле **Исключаемые домены** введите имя домена или поддомена и нажмите клавишу Enter.

Примечание. При вводе имен вы можете использовать звездочку в качестве подстановочного знака.

4. Если требуется указать другие имена, введите их аналогичным образом.
5. Нажмите кнопку **Сохранить**.

Выбор DNS-сервера для разрешения адресов

Разрешение адресов выполняется при их проверке по DNS-спискам блокировок. По умолчанию используется DNS-сервер кластера Kubernetes, развернутого в PT Email Security. Вы можете указать DNS-серверы вашей организации, которые будут использоваться для разрешения адресов.

► Чтобы ввести адрес DNS-сервера:

1. В главном меню выберите **Средства проверки** → **Экспертиза РТ**.
2. В панели с информацией о PT Anti-Phishing and Anti-Spam перейдите по ссылке **Параметры**.
3. Выберите вариант **Указать DNS-серверы**.
4. Введите доменное имя или IP-адрес DNS-сервера.
5. Нажмите кнопку **Сохранить**.

10.3. Настройка антивирусов

Кроме средств проверки, разработанных специалистами Positive Technologies, для проверки объектов в PT Email Security используются антивирусы сторонних разработчиков. Для настройки антивирусов предназначена страница **Средства проверки** → **Антивирусы**.

Основные

Антивирусы и их базы обновляются автоматически с серверов Positive Technologies.

ClamAV ☒
Cisco Talos
Последнее обновление базы 23 июня, 14:34
Версия 0.103.8 от 20 мая, 13:30

PT AV ☒
Positive Technologies
Последнее обновление базы 23 июня, 14:00
Версия 5.3490.0 от 17 июня, 11:21

VBA32 ☐
«ВИРУСБЛОКАДА»

Дополнительные

Антивирусы нужно обновлять вручную. Их базы обновляются автоматически с серверов поставщиков.

Kaspersky Web Traffic Security ☒
«Лаборатория Касперского»
Последнее обновление базы 24 июня, 07:43
Версия продукта 6.1.0.4762
Версия ядра 6.1.0.4762
Установлен 24 июня, 09:44
Лицензия ☒ Действительна до 11 сентября
[⚙ Параметры](#)

Доступны к установке

Антивирусы нужно устанавливать вручную, используя дистрибутив.

Avast Core Security
AVAST Software
[⬇ Установить](#)

Рисунок 3. Страница **Антивирусы**

В рабочей области страницы расположены панели с информацией об антивирусах, разделенные с помощью заголовков на группы:

— **Основные** — входят в комплект поставки PT Email Security:

- ClamAV;
- PT AV;
- VBA32.

Примечание. Если вы используете PT Email Security в Республике Беларусь, вам доступен антивирус VBA32. В остальных случаях доступен антивирус PT AV.

Базы и лицензии этих антивирусов обновляются автоматически. Вы не можете удалить основные антивирусы, но при необходимости можете их отключить.

— **Дополнительные** — добавлены в PT Email Security после его установки.

Базы дополнительных антивирусов обновляются автоматически с серверов разработчиков или с указанных вами локальных серверов обновлений. Устанавливать новые версии и обновлять лицензии дополнительных антивирусов вам нужно самостоятельно. При необходимости вы можете отключить дополнительные антивирусы или удалить их.

Примечание. При поддержке PT Email Security новой версии дополнительного антивируса в блоке с информацией об этом антивирусе появится оповещение о новой версии. В этом случае вам необходимо самостоятельно обновить антивирус.

В панели каждого дополнительного антивируса расположена ссылка **Параметры** для загрузки файла лицензии и настройки сервера обновлений.

— **Доступны к установке** — антивирусы, которые можно приобрести и добавить в PT Email Security для повышения вероятности обнаружения угроз:

- Avast Core Security 3.0.3;
- Kaspersky Web Traffic Security 6.1.0.4762.

Внимание! В PT Email Security можно установить только указанные версии антивирусов; вы можете скачать их с сайтов разработчиков. Для получения дополнительной информации обратитесь в техническую поддержку Positive Technologies.

В панели каждого доступного для установки антивируса расположена ссылка **Установить** для загрузки файла дистрибутива, файла лицензии и настройки сервера обновлений.

Отключение и включение антивируса

Вы можете отключать проверку объектов отдельными антивирусами. Это может понадобиться, если антивирус показывает множество ложных результатов или требуется временно уменьшить нагрузку на информационную систему организации. Отключенный антивирус можно снова включить в любой момент.

► Чтобы отключить (включить) антивирус:

1. В главном меню выберите **Средства проверки** → **Антивирусы**.
2. В панели с информацией об антивирусе отключите (включите) его.

Статус антивируса изменится на **Отключен** (**Включен**).

Установка дополнительного антивируса

Для установки дополнительного антивируса вам понадобятся его дистрибутив и файл лицензии. Вам необходимо самостоятельно приобрести лицензию и установить ее в PT Email Security. Приобрести лицензию вы можете у поставщика антивируса. Лицензия должна быть рассчитана на использование антивируса на двух или более узлах. Требования к количеству пользователей не предъявляются.

Примечание. Если установка одного из поддерживаемых PT Email Security дополнительных антивирусов недоступна, обратитесь в техническую поддержку Positive Technologies.

► Чтобы установить дополнительный антивирус:

1. В главном меню выберите **Средства проверки** → **Антивирусы**.
2. В группе **Доступны к установке** в панели с информацией об антивирусе перейдите по ссылке **Установить**.
3. Перетащите в блок параметров **Загрузить дистрибутив** файл дистрибутива антивируса.
4. Перетащите в блок параметров **Загрузить файл лицензии** файл с лицензией антивируса.
5. Если для скачивания обновлений вы планируете использовать локальный сервер обновлений, включите использование такого сервера и в поле **URL-адрес** введите его адрес в формате <Протокол>://<Доменное имя или IP-адрес>.
6. Если для подключения к локальному серверу обновлений необходимо использовать прокси-сервер, установите флажок **Подключаться через прокси-сервер**.

Примечание. Необходимость использовать прокси-сервер может возникнуть, если сервер обновлений расположен вне закрытой локальной сети организации. В этом случае будет использоваться тот же прокси-сервер, который настроен в PT Email Security для доступа к внешним ресурсам.

7. Нажмите кнопку **Установить**.

По завершении установки в группе **Дополнительные** появится панель с информацией об антивирусе.

Обновление дополнительного антивируса

► Чтобы обновить дополнительный антивирус:

1. В главном меню выберите **Средства проверки** → **Антивирусы**.
2. В панели с информацией об антивирусе перейдите по ссылке **Параметры**.
3. Перетащите в блок параметров **Загрузить дистрибутив** файл дистрибутива антивируса.
4. Нажмите кнопку **Сохранить**.

Замена лицензии дополнительного антивируса

► Чтобы заменить лицензию дополнительного антивируса:

1. В главном меню выберите **Средства проверки** → **Антивирусы**.
2. В панели с информацией об антивирусе перейдите по ссылке **Параметры**.
3. Перетащите в блок параметров **Лицензия** файл с лицензией антивируса.
4. Нажмите кнопку **Сохранить**.

Удаление дополнительного антивируса

► Чтобы удалить дополнительный антивирус:

1. В главном меню выберите **Средства проверки** → **Антивирусы**.
2. В панели с информацией об антивирусе перейдите по ссылке **Параметры**.
3. Нажмите кнопку **Удалить антивирус** и подтвердите удаление.

10.4. Настройка поведенческого анализа

С помощью консольных команд вы можете настраивать некоторые параметры поведенческого анализа файлов.

Проверка цифровой подписи кода приложений Windows

В ходе поведенческого анализа файлов в образах виртуальных машин Windows выполняется проверка цифровой подписи кода приложений Windows (code signing) для файлов форматов DLL, EXE, MSI. Подтверждение цифровой подписи указывает на то, что файл не был изменен и что сертификат удостоверяющего центра не был отозван. Высока вероятность, что такой файл не является вредоносным, но окончательное решение о результате проверки выносится на основании всех используемых методов. Инструкции необходимо выполнять на основном узле.

- ▶ Чтобы отключить проверку цифровой подписи файлов,

выполните команду:

```
sudo ptmsctl system components set -c scan-machine -p check_sample_signature=false
```

- ▶ Чтобы включить проверку цифровой подписи,

выполните команду:

```
sudo ptmsctl system components set -c scan-machine -p check_sample_signature=true
```

10.5. Работа с пользовательскими YARA-правилами

В PT Email Security используется средство проверки объектов по пользовательским YARA-правилам. Вы можете отключать и включать это средство проверки.

Для работы с пользовательскими YARA-правилами предназначена страница **Средства проверки** → **Пользовательские правила**.

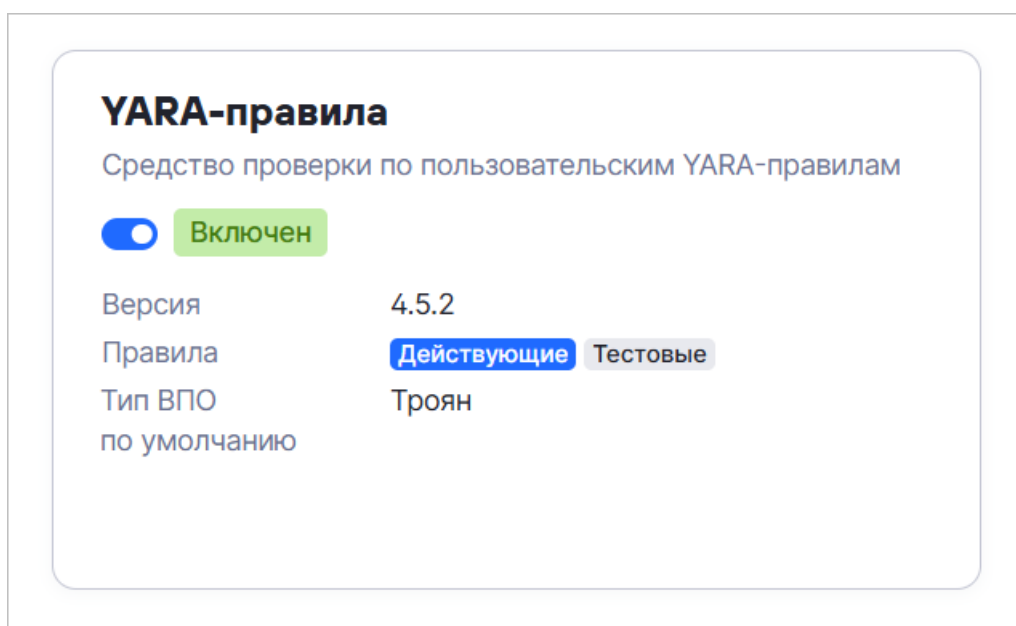


Рисунок 4. Страница **Пользовательские правила**

В рабочей области страницы расположена панель с информацией о средстве проверки по пользовательским YARA-правилам. В панели отображаются:

- Статус средства проверки. При необходимости вы можете отключать и включать средство проверки.
- Версия средства проверки.

- Статус добавленных правил: **Действующие** — результат проверки по таким правилам учитывается при вынесении вердикта; **Тестовые** — результат проверки отображается в карточке объекта, но не влияет на вердикт.
- Тип вредоносного ПО, который будет указан для объекта при вынесении вердикта, если тип не указан в правиле.

Отключение и включение средства проверки

- ▶ Чтобы отключить (включить) средства проверки по YARA-правилам:
 1. В главном меню выберите **Средства проверки** → **Пользовательские правила**.
 2. В панели **YARA-правила** отключите (включите) средство проверки.
Статус средства проверки изменится на **Отключен (Включен)**.

11. Настройка параметров PT Email Security

Настраивать параметры PT Email Security вы можете на страницах раздела **Система** → **Параметры**. Параметры сгруппированы в блоки по их назначению на отдельных страницах:

- Страница **Проверка объектов** содержит блок параметров **Анонимная проверка** для включения или отключения анонимной проверки объектов без входа в PT Email Security.
- Страница **Поведенческий анализ** → **Режим обновления образов ВМ** содержит блок параметров для настройки режима и расписания обновления образов виртуальных машин для поведенческого анализа файлов.
- Страница **Хранилище** содержит следующие блоки параметров:
 - **Хранилище** — для настройки размера хранилища файлов заданий.
 - **История проверок** — для изменения времени хранения информации о заданиях и проверенных файлах.
- Страница **Карантин** содержит блок параметров для настройки карантина для писем.
- Страница **Публичный API** содержит блок параметров **IP-адреса для подключения** для ввода дополнительных адресов службы публичного API PT Email Security.
- Страница **Очередь обработки писем МТА** содержит блок параметров для настройки времени отображения обработанных писем в очереди обработки писем.
- Страница **Уведомления** содержит следующие блоки параметров:
 - **Отправка сообщений в системный журнал по протоколу syslog** — для настройки отправки событий PT Email Security [во внешние системы в формате сообщений syslog \(см. раздел 14.2\)](#).
 - **Отправка данных в PT Threat Analyzer** — для настройки отправки данных об обнаруженных опасных и потенциально опасных объектах в программную платформу PT Threat Analyzer. Вы также можете настроить [отправку найденных в задании файлов с угрозами \(см. раздел 14.8\)](#).
 - **Отправка почтовых уведомлений об угрозах** — для настройки отправки уведомлений об обнаруженных файлах с угрозами по электронной почте.
- Страница **Почтовый шлюз безопасности** содержит блок параметров **Порты почтового шлюза** для настройки портов подключения агентов к PT Email Security.

В этом разделе

[Включение анонимной проверки объектов \(см. раздел 11.1\)](#)

[Настройка расписания обновления образов ВМ \(см. раздел 11.2\)](#)

[Настройка хранилища файлов \(см. раздел 11.3\)](#)

[Настройка карантина для писем \(см. раздел 11.4\)](#)

[Добавление IP-адресов службы публичного API \(см. раздел 11.5\)](#)

[Настройка времени отображения письма в очереди МТА \(см. раздел 11.6\)](#)

[Настройка почтовых уведомлений об угрозах \(см. раздел 11.7\)](#)

[Настройка параметров почтового шлюза безопасности \(см. раздел 11.8\)](#)

[Настройка хранения проверяемых файлов в оперативной памяти \(см. раздел 11.9\)](#)

11.1. Включение анонимной проверки объектов

По умолчанию пользователи не могут проверять объекты анонимно (без входа в PT Email Security). Если политика информационной безопасности организации разрешает анонимную проверку, вы можете включить ее.

► Чтобы включить анонимную проверку объектов:

1. В главном меню выберите **Система** → **Параметры** → **Проверка объектов**.
2. В блоке параметров **Анонимная проверка** включите проверку.
3. Нажмите кнопку **Сохранить**.

11.2. Настройка расписания обновления образов VM

Вы можете указать интервалы времени, в которые новые образы VM будут скачиваться с сервера Positive Technologies и устанавливаться на узлы PT Email Security с функцией поведенческого анализа.

► Чтобы настроить расписание обновления образов VM:

1. В главном меню выберите **Система** → **Параметры** → **Поведенческий анализ** → **Режим обновления образов VM**.
2. Нажмите кнопку **Параметры обновления образов**.
3. В блоке параметров **Режим обновления** выберите режим скачивания и установки образов.
4. Если вы выбрали обновление по расписанию, настройте интервалы времени для обновления:
 - Нажмите кнопку **Добавить**.
 - Введите время начала и время окончания интервала.
 - Если требуется, добавьте еще интервал аналогичным образом.
5. Нажмите кнопку **Сохранить**.

11.3. Настройка хранилища файлов

Вы можете настроить размер раздела хранилища для файлов заданий и срок хранения информации о заданиях и проверенных файлах.

Настройка хранилища для файлов заданий

Файлы всех заданий сохраняются в хранилище. Вы можете указать размер раздела хранилища, который будет зарезервирован для хранения файлов заданий. В этот раздел помещаются файлы, размер которых не превышает 1 ГБ или 1% от размера раздела.

Внимание! Уменьшение размера раздела для файлов заданий может привести к потере сохраненных файлов. Также не рекомендуется часто изменять размер раздела, это может приостановить проверку объектов и привести к задержкам при выполнении заданий.

Файлы заданий удаляются из раздела если: раздел заполнен на 90%; в разделе осталось менее 1 ГБ свободного места; количество файлов в разделе превысило 95% от количества, разрешенного файловой системой. Сперва удаляются самые старые файлы.

- ▶ Чтобы изменить размер раздела хранилища для файлов заданий:
 1. В главном меню выберите **Система** → **Параметры** → **Хранилище**.
 2. В блоке параметров **Хранилище** в строке **Файлы заданий** введите размер раздела в ГБ.
 3. Нажмите кнопку **Сохранить**.

Настройка срока хранения заданий

Задания на проверку сохраняются 3 года. Задания с истекшим сроком хранения удаляются блоками, содержащими данные за один календарный месяц. Например, если срок хранения задания истекает в середине месяца, оно будет удалено только по окончании этого месяца.

- ▶ Чтобы изменить срок хранения заданий:
 1. В главном меню выберите **Система** → **Параметры** → **Хранилище**.
 2. В блоке параметров **История проверок** в раскрывающемся списке выберите срок хранения заданий.
 3. Нажмите кнопку **Сохранить**.

11.4. Настройка карантина для писем

В карантин помещаются письма с угрозами, заблокированные в результате проверки. Специалист по безопасности может проанализировать содержимое письма в карантине и пропустить его в информационную систему, если признает письмо безопасным. При настройке карантина вы можете:

- Указать размер раздела хранилища, который будет зарезервирован для помещенных в карантин писем. В карантин могут помещаться письма, размер которых не превышает 1 ГБ. Письма удаляются из карантина если: раздел заполнен на 90%; в разделе осталось менее 1 ГБ свободного места; количество писем в разделе превысило 95% от количества, разрешенного файловой системой. Сперва удаляются самые старые письма, при этом помещение новых писем в карантин не ограничивается.
- Указать срок хранения писем в карантине. Письма с истекшим сроком хранения удаляются из карантина.
- Настроить резервный почтовый сервер для пересылки заблокированных писем. Если резервный сервер не настроен, используется почтовый сервер, указанный в параметрах источника.

Примечание. Резервный почтовый сервер всегда используется для источника с типом «Сервер Microsoft Exchange с установленным агентом». Для источника с типом «Почтовый сервер в режиме фильтрации» резервный почтовый сервер используется только если источник отключен или удален.

► Чтобы настроить карантин:

1. В главном меню выберите **Система** → **Параметры** → **Хранилище**.
2. В блоке параметров **Хранилище** в строке **Карантин** введите размер раздела в ГБ.
3. В главном меню выберите **Система** → **Параметры** → **Карантин**.
4. В блоке параметров **Карантин** в поле **Срок хранения в карантине** введите количество дней.
5. Если необходимо использовать резервные почтовые серверы для отправки заблокированных писем, включите их использование и настройте параметры:
 - В раскрывающемся списке **Доверенные сертификаты TLS-шифрования** выберите какой набор доверенных сертификатов будет использоваться для проверки сертификатов почтовых серверов.
 - В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
 - Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.
 - В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.

- Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
- Если в вашей организации используются несколько резервных почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.

6. Нажмите кнопку **Сохранить**.

11.5. Добавление IP-адресов службы публичного API

По умолчанию для подключения к публичному API используется IP-адрес основного узла PT Email Security.

- ▶ Чтобы добавить дополнительные адреса для подключения к службе публичного API:
 1. В блоке параметров **IP-адреса для подключения** введите дополнительные адреса.
 2. Нажмите кнопку **Сохранить**.

11.6. Настройка времени отображения письма в очереди МТА

По умолчанию письмо отображается в очереди не менее 28 дней. Вы можете изменить это время. Если обработка продлится дольше, письмо остается в очереди до ее завершения.

► Чтобы изменить время отображения письма в очереди МТА:

1. В главном меню выберите **Система** → **Параметры** → **Очередь обработки писем МТА**.
2. В поле **Время отображения писем в очереди** введите время в днях.
3. Нажмите кнопку **Сохранить**.

11.7. Настройка почтовых уведомлений об угрозах

Вы можете настроить отправку по электронной почте уведомлений об обнаруженных PT Email Security объектах с угрозами. Письма с уведомлениями отправляются для каждого задания при обнаружении первого опасного и первого потенциально опасного объекта. В теме письма указывается идентификатор задания, в котором обнаружен объект, а по кнопке в теле письма вы можете открыть карточку этого задания. В письме также указываются имя объекта с угрозой, класс обнаруженного вредоносного ПО, название и тип источника, с которого поступил файл, информация о том, откуда и куда был направлен объект.

► Чтобы настроить отправку почтовых уведомлений об угрозах:

1. В главном меню выберите **Система** → **Параметры** → **Уведомления**.
2. В блоке параметров **Отправка почтовых уведомлений об угрозах** включите отправку уведомлений.
3. В блоке параметров **Отправка уведомлений** выберите, в каких случаях требуется отправлять уведомления:
 - Если только при обнаружении опасных файлов, выберите **Только об опасных файлах**.
 - Если при обнаружении опасных и потенциально опасных файлов, выберите **Об опасных и потенциально опасных**.
4. В поле **Эл. адрес отправителя** введите адрес, который будет указан в письме с уведомлением в качестве отправителя.
5. В поле **Эл. адреса получателей** введите адреса, на которые будут отправляться письма с уведомлениями.
6. Если требуется изменить язык уведомления, в раскрывающемся списке **Язык уведомлений** выберите нужный язык.
7. В блоке параметров **SMTP-серверы** настройте параметры доступа к SMTP-серверу для отправки писем с уведомлениями:
 - В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
 - Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
- Если в вашей организации используются несколько SMTP-серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.

8. Нажмите кнопку **Сохранить**.

11.8. Настройка параметров почтового шлюза безопасности

Параметры применяются ко всем источникам типа «Почтовый шлюз безопасности».

Добавление IP-адресов SMTP-сервера

Для подключения агентов почтового шлюза к SMTP-серверу, созданному в PT Email Security, по умолчанию используется адрес основного узла PT Email Security.

► Чтобы добавить адрес SMTP-сервера:

1. В главном меню выберите **Система** → **Параметры** → **Почтовый шлюз безопасности**.
2. В поле **IP-адреса SMTP-сервера** введите IP-адрес.
3. Нажмите кнопку **Сохранить**.

Настройка портов почтового шлюза безопасности

Для передачи трафика от узлов, на которых установлен агент почтового шлюза безопасности, к основному узлу PT Email Security по умолчанию используются порты 50025 — для подключения к SMTP-серверу и 50052 — для управления агентом почтового шлюза.

Внимание! Указанные порты не должны использоваться другими источниками для проверки, службами или приложениями ОС.

► Чтобы изменить порты почтового шлюза безопасности:

1. В главном меню выберите **Система** → **Параметры** → **Почтовый шлюз безопасности**.
2. В поле **Порт SMTP** введите номер порта.
3. В поле **Порт управления** введите номер порта.
4. Нажмите кнопку **Сохранить**.

Фильтрация входящих подключений

По умолчанию SMTP-сервер принимает подключения только от узлов, на которых установлены агенты почтового шлюза. При отключении фильтрации сервер принимает подключения с любых IP-адресов.

► Чтобы отключить фильтрацию входящих подключений:

1. В главном меню выберите **Система** → **Параметры** → **Почтовый шлюз безопасности**.
2. Отключите фильтрацию входящих подключений.
3. Нажмите кнопку **Сохранить**.

11.9. Настройка хранения проверяемых файлов в оперативной памяти

По умолчанию PT Email Security хранит отправленные на проверку файлы на жестком диске. Для повышения скорости обработки и проверки файлов можно настроить их хранение в файловой системе tmpfs. Файловая система tmpfs использует оперативную память и, если в операционной системе настроено пространство подкачки, может использовать это пространство. За работу с файлами в PT Email Security отвечает компонент ScanFileManager версии 2 (SFMv2).

Включение хранения проверяемых файлов в оперативной памяти

Для включения хранения отправленных на проверку файлов в оперативной памяти необходимо создать каталог `/opt/ptms/var/files/fast` и смонтировать в него файловую систему tmpfs. После этого компонент SFMv2 автоматически обнаружит точку монтирования tmpfs.

Внимание! После перезагрузки узла содержимое tmpfs будет потеряно. Если в операционной системе не настроено автоматическое монтирование, tmpfs не будет смонтирована повторно.

Инструкцию необходимо выполнить на каждом узле PT Email Security.

Внимание! Перед включением хранения проверяемых файлов в оперативной памяти убедитесь, что на узле достаточно свободной оперативной памяти. Недостаток памяти или заполнение tmpfs могут привести к ошибкам проверки и нестабильной работе узла.

► Чтобы смонтировать tmpfs в каталог с файлами:

1. Определите размер tmpfs с учетом доступной оперативной памяти и максимального объема одновременно обрабатываемых файлов.
2. Создайте каталог `/opt/ptms/var/files/fast`.
3. Выполните команду, указав размер tmpfs в байтах или указав единицы измерения К, М, G:
`sudo mount -t tmpfs -o size=<Размер tmpfs> tmpfs /opt/ptms/var/files/fast`

Например:

```
sudo mount -t tmpfs -o size=2G tmpfs /opt/ptms/var/files/fast
```

4. Проверьте, что tmpfs смонтирована:

```
sudo findmnt --target /opt/ptms/var/files/fast --types tmpfs
```

При успешном монтировании отображается информация о tmpfs, точке монтирования и параметрах монтирования.

Отключение хранения проверяемых файлов в оперативной памяти

Для отключения хранения отправленных на проверку файлов в оперативной памяти необходимо отключить хранилища tmpfs в параметрах каждого экземпляра SFMv2, дождаться завершения обработки файлов, а затем размонтировать файловую систему tmpfs из каталога для хранения файлов.

Имя экземпляра SFMv2 зависит от назначения узла:

- `scan-file-manager-v2-<Имя узла>` — на основном и резервных узлах.
- `scan-file-manager-v2-sandbox-<Имя узла>` — на дополнительных узлах с функцией поведенческого анализа.

Инструкцию необходимо выполнить на основном узле для экземпляра SFMv2 каждого узла PT Email Security.

► Чтобы отключить хранилище tmpfs в параметрах экземпляра SFMv2,

выполните команду:

```
sudo ptmsctl system components set -c <Имя экземпляра SFMv2> -p fast_storage_enabled=false
```

Например:

```
sudo ptmsctl system components set -c scan-file-manager-v2-node01 -p
fast_storage_enabled=false
```

Инструкцию необходимо выполнить на каждом узле PT Email Security.

Внимание! После отключения хранилища tmpfs необходимо дождаться завершения обработки и проверки файлов. В противном случае размонтирование tmpfs может привести к потере хранящихся в ней файлов.

► Чтобы размонтировать tmpfs из каталога с файлами:

1. Выполните команду:

```
sudo umount /opt/ptms/var/files/fast
```

2. Проверьте, что tmpfs размонтирована:

```
sudo findmnt --mountpoint /opt/ptms/var/files/fast --types tmpfs
```

Если tmpfs размонтирована, команда не выводит сведения о точке монтирования.

12. Работа с источниками

Источник для проверки (источник) — интерфейс в информационной системе организации, с которого в PT Email Security поступают объекты на проверку.

Объекты могут поступать на проверку от встроенных источников, которые не требуется добавлять в PT Email Security, и от подключаемых внешних источников, которые необходимо добавлять в PT Email Security в соответствии с их типами.

Встроенные источники

В PT Email Security предусмотрены следующие встроенные источники:

- Веб-интерфейс — вы можете анонимно или после входа в PT Email Security отправить объекты на проверку через веб-интерфейс. Поддерживается проверка объектов размером до 1 ГБ.
- Хранилище файлов — после настройки параметров повторной проверки PT Email Security регулярно проверяет файлы в хранилище.
- API с передаваемыми параметрами проверки — внешняя система может передавать объекты на проверку через службу публичного API PT Email Security. Проверка выполняется с параметрами, переданными в запросе. Поддерживается проверка объектов размером до 1 ГБ.

Подключаемые источники

Источником объектов для PT Email Security может служить внешняя система, например почтовый сервер, межсетевой экран или папки на сетевом диске. При подключении внешней системы, как правило, требуется настроить саму систему для работы с PT Email Security и добавить эту систему в PT Email Security в качестве источника. Для подключения различных типов внешних систем предусмотрены следующие типы источников:

- Служба Checkme — служба для проверки объектов по электронной почте, обеспечивает взаимодействие PT Email Security с почтовым сервером вашей организации. После настройки этого источника для проверки объекта достаточно отправить его письмом на специальный адрес электронной почты. PT Email Security проверит само письмо, ссылки в тексте письма и вложенные в него файлы. Результат проверки отправляется в ответном письме. Поддерживается проверка писем размером до 1 ГБ.
- Общая папка — папка с настроенным общим доступом, все файлы которой проверяются PT Email Security. После проверки все файлы остаются в той же папке. Поддерживается проверка файлов размером до 5 ГБ.
- Папка-шлюз — папка с настроенным общим доступом, все файлы которой проверяются PT Email Security. По результатам проверки объекты из папки-шлюза переносятся в папку для безопасных объектов или папку карантина. Поддерживается проверка файлов размером до 5 ГБ.

- ICAP-сервер — позволяет принимать на проверку объекты по протоколу ICAP. Для этого в PT Email Security настраивается ICAP-сервер, а внешняя система выступает в качестве ICAP-клиента. Поддерживается проверка объектов размером до 1 ГБ.
- Почтовый шлюз безопасности — позволяет получать письма от SMTP-сервера, развернутого на внешнем узле. Такой сервер принимает письма от SMTP-клиентов и работает в качестве почтового шлюза. Поддерживается проверка писем размером до 20 МБ.
- Сервер Microsoft Exchange с установленным агентом — позволяет принимать почтовый трафик сервера Microsoft Exchange, перенаправляемый с помощью почтового агента PT Email Security. Почтовый агент устанавливается на сервер Microsoft Exchange, перехватывает все проходящие через сервер письма и отправляет их на проверку в PT Email Security, после чего возвращает проверенные письма обратно для доставки адресатам. Поддерживается проверка писем размером до 1 ГБ.
- Почтовый сервер в режиме фильтрации — позволяет принимать от почтового сервера, работающего в режиме фильтрации, письма для проверки в PT Email Security. Поддерживается проверка писем размером до 1 ГБ.

Режим фильтрации — режим работы почтового сервера, при котором PT Email Security может фильтровать почтовый трафик сервера. В зависимости от выбранного режима проверки PT Email Security либо сразу возвращает почтовому серверу отправленное на проверку письмо (пассивный режим), либо блокирует его до окончания проверки (блокирующий режим).

- Почтовый сервер в режиме фильтрации (MTA) — позволяет то же что и почтовый сервер в режиме фильтрации, но для работы с письмами используется встроенный в PT Email Security почтовый транспортный агент. Поддерживается проверка писем размером до 1 ГБ.
- Почтовый сервер в режиме зеркалирования — позволяет принимать от почтового сервера, работающего в режиме зеркалирования, скрытые копии писем для проверки в PT Email Security. Поддерживается проверка писем размером до 1 ГБ.

Режим зеркалирования — режим работы почтового сервера, при котором PT Email Security не влияет на почтовый трафик сервера. На проверку в PT Email Security отправляются копии писем.

- PT NAD — позволяет настроить интеграцию с PT NAD. После интеграции извлеченные из сетевого трафика файлы отправляются на проверку в PT Email Security. Поддерживается проверка файлов размером до 1 ГБ.
- MaxPatrol EDR — позволяет настроить интеграцию с MaxPatrol EDR. После интеграции извлеченные файлы конечных устройств отправляются на проверку в PT Email Security. Поддерживается проверка файлов размером до 1 ГБ.
- API с выбранными параметрами проверки — позволяет настроить интеграцию с внешними системами через сервис публичного API PT Email Security. Поддерживается проверка объектов размером до 1 ГБ.

Параметры проверки объектов, поступающих от источника, настраиваются индивидуально для каждого источника после его добавления в PT Email Security. Параметры проверки могут отличаться для источников разных типов.

Режимы проверки объектов, поступающих от источников

В зависимости от способа обработки объектов, поступающих на проверку в PT Email Security, предусмотрены следующие режимы проверки:

- Режим ожидания — режим проверки, при котором на проверку от источников в PT Email Security поступают копии объектов, а их распространение контролирует пользователь или сторонняя система.
- Пассивный режим — режим проверки, при котором поступившие на проверку объекты сразу пропускаются PT Email Security в информационную систему.
- Блокирующий режим — режим проверки, при котором поступившие на проверку объекты блокируются PT Email Security до окончания проверки. В зависимости от вынесенного вердикта объект пропускается в информационную систему или удаляется (или помещается в карантин).

Примечание. Использование блокирующего режима может быть ограничено лицензией.

Режимы проверки для каждого типа источника указаны в таблице. Для источников, поддерживающих несколько режимов проверки, выбор режима зависит от политики информационной безопасности вашей организации. Вы можете настроить режим проверки объектов для таких источников в параметрах проверки. Для источников с типом «ICAP-сервер» режим проверки настраивается в параметрах ICAP-клиента.

Таблица 3. Режимы проверки объектов, поступающих от источников

Тип источника	Режим ожидания	Пассивный режим	Блокирующий режим
Веб-интерфейс	Да	—	—
Хранилище файлов	Да	—	—
Служба Checkme	Да	—	—
Общая папка	—	Да	—
Папка-шлюз	—	Да	Да
ICAP-сервер	Да	Да	Да
Почтовый шлюз безопасности	—	Да	Да
Сервер Microsoft Exchange с установленным агентом	—	Да	Да
Почтовый сервер в режиме фильтрации	—	Да	Да

Тип источника	Режим ожидания	Пассивный режим	Блокирующий режим
Почтовый сервер в режиме фильтрации (MTA)	—	Да	Да
Почтовый сервер в режиме зеркалирования	—	Да	—
PT CS	Да	—	—
MaxPatrol EDR	Да	—	—
PT NAD	—	Да	—
API с выбранными параметрами проверки	Да	—	—
API с передаваемыми параметрами проверки	Да	—	—

В этом разделе

[Настройка источников \(см. раздел 12.1\)](#)

[Работа с токенами доступа \(см. раздел 12.2\)](#)

[Работа со списками адресов \(см. раздел 12.3\)](#)

[Работа с агентами почтового шлюза \(см. раздел 12.4\)](#)

[Настройка правил маршрутизации проверенных писем \(см. раздел 12.5\)](#)

[Отключение автоматической смены режимов проверки \(см. раздел 12.6\)](#)

12.1. Настройка источников

PT Email Security может проверять объекты, поступающие от пользователей или из внешних систем, подключенных в качестве источников объектов. Вы можете добавлять и удалять источники, изменять их параметры, временно отключать и включать. Для работы с источниками предназначена страница **Источники** → **Управление источниками**.

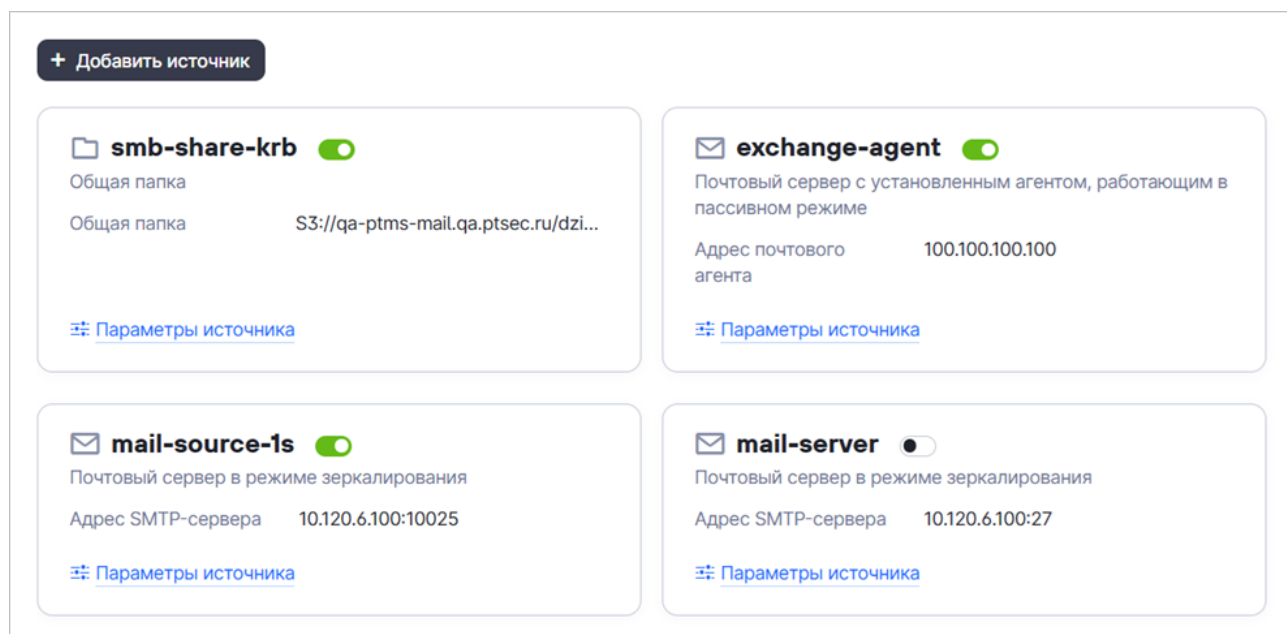


Рисунок 5. Страница **Управление источниками**

Вверху страницы расположена кнопка **Добавить источник** для добавления нового источника для проверки.

В рабочей области страницы расположены панели с информацией о добавленных источниках. При необходимости вы можете отключать источники. В каждой панели расположена ссылка **Параметры источника** для настройки параметров.

Добавление источника

Внимание! Количество подов на любом узле PT Email Security не должно превышать 150. При добавлении источника в PT Email Security на основном узле для его работы создаются два пода. Отслеживать текущее количество созданных подов вы можете на странице **Система** → **Конфигурация** → **Узлы**. Если требуется увеличить максимальное количество подов на узле, обратитесь в техническую поддержку Positive Technologies.

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите тип источника.

5. Укажите параметры подключения источника в зависимости от его типа.
6. Нажмите кнопку **Добавить источник**.

Изменение параметров источника

► Чтобы изменить параметры источника:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры источника**.
3. Измените параметры источника.

Примечание. Вы можете изменить любые параметры источника, кроме его названия и типа.

4. Нажмите кнопку **Сохранить**.

Отключение и включение источника

► Чтобы отключить (включить) источник:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. В панели с информацией об источнике отключите (включите) его.

Удаление источника

► Чтобы удалить источник:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры источника**.
3. Нажмите  и подтвердите удаление.

12.2. Работа с токенами доступа

Токен доступа — это уникальная последовательность символов, которая применяется для защиты PT Email Security от несанкционированного доступа через публичный API. Используется при подключении к PT Email Security внешних систем в качестве источников объектов.

Примечание. Доступ к результатам проверки объекта и информации о задании вы можете получить только с тем же токеном доступа, с которым объект был отправлен на проверку.

Вы можете работать с токенами доступа при помощи консольных команд или через веб-интерфейс PT Email Security. Работа с токенами доступа с помощью команд описана в Руководстве разработчика.

Работать с токенами доступа через веб-интерфейс PT Email Security можно на странице **Источники** → **Токены доступа**.

+ Создать токен доступа

[↶ Вернуться к фильтру по умолчанию](#)

Дата создания За все время	↓	Кто создал	Название	Связанный источник	Разрешенные действия	Комментарий
27 апр 2024, 13:49		Administrator	token-edr	edr-emakridi	Проверка с параметрами источника	
17 апр 2024, 16:59		Administrator	test		Проверка с передаваемыми параметрами, ...	
22 мар 2024, 15:32		Administrator	maxpatroledr		Проверка с параметрами источника	
14 мар 2024, 13:20		Administrator	maxpatroledrtoken		Проверка с параметрами источника	
6 мар 2024, 09:59		Administrator	oc-token	oc-entripoint	Проверка с параметрами источника	
6 мар 2024, 09:34		Administrator	oc-key		Проверка с передаваемыми параметрами	
21 фев 2024, 15:06		Administrator	api-entry-point-token	api-entry-point	Проверка с параметрами источника	
26 янв 2024, 05:06		Administrator	ptcs2avscanner	ptcs-av-scanner	Проверка с передаваемыми параметрами, ...	for PT CS

Всего 70

1
2
<
>

Рисунок 6. Страница **Токены доступа**

В панели инструментов страницы расположена кнопка **Создать токен доступа** для создания токена доступа.

В рабочей области страницы расположена таблица с информацией по всем созданным токенам доступа. При наведении курсора на строку таблицы отображаются значки:



— для изменения комментария к токenu.



— для отзыва токена доступа. Если токен привязан к источнику, то после его отзыва источник перестанет работать.

Ниже приведены инструкции по работе с токенами доступа.

Создание токена доступа

► Чтобы создать токен доступа:

1. В главном меню выберите **Источники** → **Токены доступа**.
2. Нажмите кнопку **Создать токен доступа**.
3. Введите название токена доступа. Оно будет отображаться на странице **Токены доступа**.
4. Выберите разрешенные действия, которые будут доступны при использовании токена.
5. Нажмите кнопку **Создать**.

Созданный токен доступа отобразится в окне **Токен доступа создан**.

6. Нажмите кнопку **Скопировать в буфер обмена и закрыть**, чтобы скопировать токен.

Внимание! После закрытия этого окна токен будет недоступен для просмотра и копирования.

Отзыв токена доступа

Вы можете отозвать токен доступа. Если токен доступа используется источником, то он перестанет работать после отзыва токена. Если токен доступа используется сторонней системой, то ее работа также может быть нарушена.

► Чтобы отозвать токен доступа:

1. В главном меню выберите **Источники** → **Токены доступа**.
2. В строке с токеном доступа нажмите .
3. Нажмите кнопку **Все равно отозвать**.

12.3. Работа со списками адресов

Список адресов — набор IP-адресов, подсетей, адресов электронной почты и доменов, объединенных под уникальным названием. Один список может содержать адреса разных типов. Для адресов вы можете ограничивать срок действия. После истечения срока адрес остается в списке, но не учитывается в правилах. Для списков и их адресов сохраняется история изменений: дата и время, действие, логин пользователя и комментарий.

При настройке правил обработки писем вы можете выбрать список вместо перечисления отдельных адресов. Изменение состава списка применяется во всех правилах, в которых он используется. Переименование списка сохраняет его связь с правилами.

В этом разделе

[Списки адресов \(см. раздел 12.3.1\)](#)

[Адреса списка \(см. раздел 12.3.2\)](#)

12.3.1. Списки адресов

Вы можете просматривать, создавать, изменять и удалять списки адресов, а также просматривать их историю и сведения об источниках и правилах, в которых они используются.

Для работы со списками предназначена страница **Источники** → **Списки адресов**.

+ Создать								
Название	↕	Типы адресов	Адреса	Источники	Дата изменения	↕		
Домены партнеров		Домены: 4	distributor.example.net, logistics.example.org, ...	1	9 сентября, 11:21			
Корпоративные почтовые серверы		Домены: 2 IP-адреса: 2 Подсети: 1	192.0.2.10, 192.0.2.11, 192.0.2.8/29, mail.examp...	1	9 сентября, 11:19			
Рабочие станции		Домены: 1 IP-адреса: 2 Подсети: 1	192.0.2.0/27, 192.0.2.21, 192.0.2.22, workstatio...		9 сентября, 11:19			
Системы отправки уведомлений		Домены: 2 Эл. адреса: 2 IP-адреса: 2 Подсети: 1	203.0.113.40, 203.0.113.40/29, 203.0.113.41, he...		9 сентября, 11:19			
Электронные адреса сотрудников		Эл. адреса: 5	admin@example.com, developer@example.co...	1	9 сентября, 11:20			
Всего 5				1	<	>		

Рисунок 7. Страница **Списки адресов**

В панели инструментов страницы расположены кнопки:

Создать — для создания списка.

↶ — для сброса фильтров таблицы.

⚙ — для выбора столбцов, которые должны отображаться в таблице.

В рабочей области страницы расположена таблица со списками адресов.

При наведении курсора на строку списка справа появляются кнопки:

✎ — для изменения названия и комментария.

🕒 — для просмотра истории списка.

🗑 — для удаления списка.

В зависимости от вашего выбора таблица может содержать следующие столбцы:

- **Название** — название списка. По ссылке с названием открывается страница с адресами списка.
- **Типы адресов** — типы адресов и количество адресов каждого типа в списке.
- **Адреса** — адреса, добавленные в список. Адреса с ограниченным сроком действия отмечаются значком 🕒, адреса с истекшим сроком — красным значком.
- **Источники** — количество источников, в которых используется список. При нажатии на число открываются сведения об источниках, группах правил и правилах, использующих список.
- **Дата изменения** — дата и время изменения списка.
- **Кто изменил** — логин пользователя, изменившего список.
- **Комментарий** — комментарий к изменению списка.

Вы можете фильтровать списки с помощью элементов в заголовках столбцов. При нажатии на заголовок **Адреса** открывается поле поиска. При поиске по адресу в таблице отображаются списки, содержащие адреса, соответствующие условию поиска. В столбце **Адреса** отображаются только найденные адреса.

Примечание. Поиск не проверяет вхождение IP-адреса в подсеть или принадлежность адреса электронной почты домену из списка.

С помощью кнопки  в заголовках **Название** и **Дата изменения** вы можете изменить порядок строк. Повторное нажатие меняет направление сортировки.

В нижней части таблицы отображаются количество списков и кнопки перехода между страницами таблицы.

Создание списка адресов

► Чтобы создать список адресов:

1. В главном меню выберите **Источники** → **Списки адресов**.
2. Нажмите кнопку **Создать**.
Откроется окно **Создание списка**.
3. В поле **Название** введите название списка.
Название должно быть уникальным среди всех списков.
4. Нажмите кнопку **Создать**.

Изменение названия списка адресов

Переименование сохраняет связь списка с правилами.

► Чтобы изменить название списка адресов:

1. В главном меню выберите **Источники** → **Списки адресов**.
2. Наведите курсор на строку списка и нажмите кнопку .
Откроется окно **Изменение списка**.
3. В поле **Название** введите новое название.
4. В поле **Комментарий** введите комментарий.
5. Нажмите кнопку **Изменить**.

Удаление списка адресов

Внимание! Если список используется источниками, после его удаления адреса из списка перестанут учитываться в правилах этих источников. Это может изменить обработку писем. Перед удалением замените список в правилах связанных источников или измените условия этих правил.

► Чтобы удалить список адресов:

1. В главном меню выберите **Источники** → **Списки адресов**.
2. Наведите курсор на строку списка и нажмите кнопку .
Откроется окно подтверждения.
3. В поле **Комментарий** введите комментарий и подтвердите удаление.

Просмотр истории списка адресов

История списка включает изменения самого списка и его адресов, в том числе удаленных. Для каждого события сохраняются дата и время, выполненное действие, сведения об изменении, логин пользователя и комментарий.

► Чтобы просмотреть историю списка:

1. В главном меню выберите **Источники** → **Списки адресов**.
2. Наведите курсор на строку списка и нажмите кнопку .
Откроется окно **История изменений**.

12.3.2. Адреса списка

Вы можете просматривать, добавлять, изменять и удалять адреса списка, устанавливать срок их действия и просматривать историю. Изменение срока действия и удаление доступны для одного или нескольких выбранных адресов.

Для работы с адресами предназначена страница с названием списка, которая открывается по ссылке с названием списка на странице **Источники** → **Списки адресов**.

Корпоративные почтовые серверы

История изменений

Типы адресов

Домены: 2 IP-адреса: 1 Подсети: 1

Источники

mail-agent 3 правила

+ Добавить

Изменить срок действия

Удалить

	Адрес	Тип адреса	Дата измен...	Кто изменил	Комментарий	Срок действия
☐	192.0.2.10	IP-адреса	11 сентября, 11:12	ivanov_spec	Резервный сервер	Истек
☐	192.0.2.11	IP-адреса	11 сентября, 11:11	ivanov_spec	Обслуживание сервера	14 ноября, 23:59
☐	192.0.2.8/29	Подсети	11 сентября, 11:11	ivanov_spec	Внутренняя подсеть	—
☒	mail.example.com	Домены	9 сентября, 11:19	ivanov_spec	Адреса корпоративных почтовых серверов	—
☐	smtp.example.com	Домены	9 сентября, 11:19	ivanov_spec	Адреса корпоративных почтовых серверов	—

Всего 5

1 < >

Рисунок 8. Страница с адресами в списке

В верхней части страницы отображается название списка. Справа расположены кнопки:

История изменений — для просмотра истории списка.



— для удаления списка.

Ниже расположена информационная панель. В ней отображаются типы адресов и связанные источники. Название источника является ссылкой на его параметры. Рядом указано количество правил, использующих список.

В панели инструментов таблицы расположены кнопки:

Добавить — для добавления адресов в список.

Изменить срок действия — для изменения срока действия всех выбранных адресов. Кнопка доступна после выбора адресов в таблице.

Удалить — для удаления всех выбранных адресов. Кнопка доступна после выбора адресов в таблице.



— для сброса фильтров таблицы.



— для выбора столбцов, которые должны отображаться в таблице.

В рабочей области страницы расположена таблица с адресами выбранного списка.

При наведении курсора на строку адреса справа появляются кнопки:



— для изменения адреса, срока действия и комментария.



— для просмотра истории адреса.



— для удаления адреса.

В зависимости от вашего выбора таблица может содержать следующие столбцы:

- Столбец для выбора нескольких адресов для массовых операций. Общий флажок в заголовке позволяет выбрать все адреса.
- **Адрес** — адрес, добавленный в список.
- **Тип адреса** — IP-адрес, подсеть, адрес электронной почты или домен.
- **Дата изменения** — дата и время изменения адреса.
- **Кто изменил** — логин пользователя, изменившего адрес.
- **Комментарий** — комментарий к изменению адреса.
- **Срок действия** — дата и время окончания срока действия адреса. Надпись **Истек** означает, что адрес больше не учитывается в правилах. Прочерк означает, что срок не ограничен.

Вы можете фильтровать адреса с помощью элементов в заголовках столбцов. При нажатии на заголовок **Адрес** открывается поле поиска. После фильтрации отображаются адреса, соответствующие условию.

С помощью кнопки  в заголовках **Дата изменения** и **Срок действия** вы можете изменить порядок адресов. Повторное нажатие меняет направление сортировки.

В нижней части таблицы отображаются количество адресов и кнопки перехода между страницами таблицы.

Добавление адресов в список

За одну операцию вы можете добавить несколько адресов разных типов с общим сроком действия и комментарием. По умолчанию срок действия не ограничен. Адрес должен быть уникальным в пределах списка.

► Чтобы добавить адреса в список:

1. В главном меню выберите **Источники** → **Списки адресов**.

2. Перейдите по ссылке с названием списка.

Откроется страница **<Название списка>**.

3. Нажмите кнопку **Добавить**.

Откроется окно **Добавление адресов**.

4. На вкладках введите адреса, подтверждая каждый нажатием клавиши Enter:

- На вкладке **Эл. адреса** введите адреса электронной почты, например `admin@example.com`.
- На вкладке **Домены** введите домены, например `mail.example.com`. Вы можете использовать маски с подстановочными знаками, например `*.example.com`.

- На вкладке **IP-адреса** введите адреса в формате IPv4, например 192.0.2.10.
 - На вкладке **Подсети** введите подсети в формате CIDR, например 198.51.100.0/24.
5. Если необходимо ограничить срок действия адресов:
 - Установите флажок **Ограничить срок действия**.
 - Введите дату и время.
 6. В поле **Комментарий** введите комментарий.
 7. Нажмите кнопку **Добавить**.

Изменение адреса в списке

- Чтобы изменить адрес в списке:
1. В главном меню выберите **Источники** → **Списки адресов**.
 2. Перейдите по ссылке с названием списка.
Откроется страница **<Название списка>**.
 3. Наведите курсор на строку адреса и нажмите кнопку .
Откроется окно **Изменение адреса**.
 4. В поле адреса введите новый адрес.
 5. В поле **Комментарий** введите комментарий.
 6. Нажмите кнопку **Изменить**.

Изменение срока действия адресов

Вы можете установить или изменить срок действия адресов, а также снять ограничение по сроку действия. Для выбранных адресов применяются общие дата и время окончания срока действия. Дата и время должны быть в будущем.

Если срок действия адреса уже истек, после установки будущей даты или снятия ограничения адрес снова учитывается в правилах.

- Чтобы изменить срок действия адресов:
1. В главном меню выберите **Источники** → **Списки адресов**.
 2. Перейдите по ссылке с названием списка.
Откроется страница **<Название списка>**.
 3. Выберите адреса.
 4. В панели инструментов нажмите кнопку **Изменить срок действия**.
Откроется окно изменения срока действия выбранных адресов.

5. Если необходимо установить или изменить дату окончания срока действия:
 - Выберите **Установить срок действия**.
 - Введите дату и время.
6. Если необходимо снять ограничение срока действия, выберите **Не ограничивать срок действия**.
7. В поле **Комментарий** введите комментарий.
8. Нажмите кнопку **Изменить**.

Удаление адресов из списка

- ▶ Чтобы удалить адреса из списка:
 1. В главном меню выберите **Источники** → **Списки адресов**.
 2. Перейдите по ссылке с названием списка.
Откроется страница **<Название списка>**.
 3. Выберите адреса.
 4. В панели инструментов нажмите кнопку **Удалить**.
Откроется окно подтверждения.
 5. В поле **Комментарий** введите комментарий и подтвердите удаление.

Просмотр истории отдельного адреса

История адреса содержит события его добавления и изменения, включая изменение срока действия и комментария. Для каждого события сохраняются дата и время, выполненное действие, сведения об изменении, логин пользователя и комментарий. После удаления адреса записи о связанных с ним событиях остаются в истории списка.

- ▶ Чтобы просмотреть историю адреса:
 1. В главном меню выберите **Источники** → **Списки адресов**.
 2. Перейдите по ссылке с названием списка.
Откроется страница **<Название списка>**.
 3. Наведите курсор на строку адреса и нажмите кнопку .

Откроется окно **История изменения адреса**.

12.4. Работа с агентами почтового шлюза

Агент почтового шлюза обеспечивает передачу писем, полученных почтовым шлюзом безопасности, на проверку в PT Email Security. При развертывании почтового шлюза безопасности [агент устанавливается на узле шлюза \(см. раздел 13.7\)](#).

Вы можете добавить установленный агент почтового шлюза в PT Email Security по IP-адресу узла шлюза, изменить IP-адрес добавленного агента или удалить агент. Управление агентами выполняется на странице **Источники** → **Агенты почтового шлюза**.

+ Добавить				
	IP-адрес	Писем на агенте	Источник	Прием писем
●	198.51.100.28	2	 mail-agent-mta	Включен
⌚	198.51.100.10		 mail-agent-mta	Включен
⌚	198.51.100.37		 fish-agent	Отключен
●	198.51.100.54	8	 test-mail-agent	Включен

Рисунок 9. Страница **Агенты почтового шлюза**

В панели инструментов страницы расположена кнопка **Добавить** для добавления агента почтового шлюза в PT Email Security.

В рабочей области страницы расположена таблица со списком добавленных агентов. При наведении курсора на строку таблицы отображаются значки:



— для изменения IP-адреса узла с агентом.



— для просмотра команды сопряжения агента с PT Email Security.



— для удаления агента.

Таблица содержит следующие столбцы с информацией об агенте:

- Статус подключения агента: ⌚ — требуется сопряжение; ● — доступен; ● — недоступен; ● — недоступен более 30 минут.
- **IP-адрес** — адрес узла с агентом.
- **Писем на агенте** — количество писем, которые получены агентом, но еще не переданы в PT Email Security.

- **Источник** — название источника, к которому подключен агент. По ссылке в названии источника вы можете открыть карточку источника.
- **Прием писем** — статус приема писем агентом. Если агент не подключен ни к одному источнику, он не принимает письма.

Примечание. Запускать и останавливать прием писем агентом вы можете в карточке источника, к которому он подключен.

Добавление агента в PT Email Security

Для добавления агента почтового шлюза в PT Email Security вам необходимо получить команду сопряжения агента почтового шлюза с PT Email Security и выполнить эту команду на узле с установленным агентом.

Инструкцию необходимо выполнить в интерфейсе PT Email Security.

- ▶ Чтобы получить команду для сопряжения агента почтового шлюза с PT Email Security:

1. В главном меню выберите **Источники** → **Агенты почтового шлюза**.

2. Нажмите кнопку **Добавить**.

Откроется окно **Добавление агента**.

3. В поле **IP-адрес узла с агентом** введите адрес узла.

4. Нажмите кнопку **Добавить**.

Откроется окно **Команда для сопряжения**.

5. Нажмите кнопку **Скопировать в буфер обмена и закрыть**.

Примечание. После закрытия окна вы сможете посмотреть команду сопряжения, нажав в строке агента .

Инструкцию необходимо выполнить на узле с установленным агентом почтового шлюза безопасности.

- ▶ Чтобы добавить агент почтового шлюза в PT Email Security,

выполните команду сопряжения, например:

```
sudo espa pair --key 89602a09-4b47-47b4-a02b-51216470be07 --grpc-port 50052 --server-ca "LS...Qo=" --ip 192.0.1.1 --smtp-port 50025
```

Подключение агента к источнику

Для подключения агента почтового шлюза к источнику агент должен быть добавлен в PT Email Security. К одному источнику можно подключить несколько агентов почтового шлюза.

► Чтобы подключить агент почтового шлюза к источнику:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите на панель с информацией об источнике с типом **Почтовый шлюз безопасности**.
3. Выберите вкладку **Агенты почтового шлюза**.
4. Нажмите кнопку **Подключить агент**.
Откроется окно **Подключение агента**.
5. Выберите агент в списке.
6. Нажмите кнопку **Подключить**.

Остановка и запуск приема писем агентом

► Чтобы остановить (запустить) прием писем агентом почтового шлюза:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите на панель с информацией об источнике с типом **Почтовый шлюз безопасности**.
3. Выберите вкладку **Агенты почтового шлюза**.
4. В строке агента отключите (включите) прием писем и подтвердите отключение.

Отключение агента от источника

Перед отключением агента почтового шлюза от источника необходимо остановить прием писем агентом и дождаться передачи всех принятых почтовым шлюзом писем в PT Email Security.

► Чтобы отключить агент почтового шлюза от источника:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите на панель с информацией об источнике с типом **Почтовый шлюз безопасности**.
3. Выберите вкладку **Агенты почтового шлюза**.
4. В строке агента нажмите кнопку **Отключить** и подтвердите отключение.

Удаление агента из PT Email Security

Если агент почтового шлюза подключен к источнику, перед удалением агента необходимо остановить прием писем агентом и отключить его от источника.

► Чтобы удалить агент почтового шлюза безопасности из PT Email Security:

1. В главном меню выберите **Источники** → **Агенты почтового шлюза**.
2. В строке агента нажмите  и подтвердите удаление.

12.5. Настройка правил маршрутизации проверенных писем

Если в вашей организации используются несколько почтовых серверов, вы можете настроить правила маршрутизации проверенных писем. В зависимости от домена, указанного в электронном адресе получателя письма, PT Email Security может отправлять письма и уведомления о результатах проверки на определенные почтовые серверы. В правиле маршрутизации вы можете выбрать один из способов маршрутизации: по MX-записям, имеющимся в DNS для почтового домена, или на указанные почтовые серверы (согласно их приоритету).

Настройка правил маршрутизации доступна для источников «Почтовый сервер в режиме фильтрации», «Почтовый сервер в режиме фильтрации (MTA)» и «Почтовый шлюз безопасности».

Правила маршрутизации настраиваются отдельно для каждого источника. Вы можете добавлять, изменять и удалять правила. Добавленное ранее правило вы можете скопировать для того же или другого источника.

Добавление правила маршрутизации

► Чтобы добавить правило маршрутизации:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры источника**.
3. В блоке параметров **Правила маршрутизации почтового трафика** нажмите кнопку **Добавить**.
4. В поле **Домен электронной почты получателя** введите доменную часть адреса электронной почты получателей, для которых необходимо настроить правило.

С помощью звездочки вы можете задать маску для доменной части адреса получателей писем, если доменная часть содержит поддомены третьего уровня или выше. Например, правило с маской *.example.com будет применяться и для адресов с доменной частью example.com, sub_1.example.com, sub_2.example.com, и для адресов с доменной частью, содержащей поддомены более высоких уровней.

Примечание. Если доменная часть адреса получателя соответствует нескольким правилам маршрутизации, будет использовано то правило, в котором указан наиболее точный адрес. При этом более высокий приоритет имеют правила, в которых не используются маски.

5. В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
6. Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.
7. Если необходимо перенаправлять письма согласно MX-записям, выберите способ маршрутизации **По MX-записям**.

Внимание! Письмо не будет отправлено, если в DNS отсутствует подходящая MX- или A-запись для указанного домена.

8. Если необходимо перенаправлять письма на определенный почтовый сервер, выберите способ маршрутизации **По адресам почтовых серверов** и укажите параметры сервера:

- В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
- Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
 - Если в вашей организации используется несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.
9. Нажмите кнопку **Добавить**.
 10. Нажмите кнопку **Сохранить**.
- Правило маршрутизации добавлено.

Копирование правила маршрутизации

► Чтобы скопировать правило маршрутизации:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.
3. В блоке параметров **Правила маршрутизации почтового трафика** в строке правила, которое вы хотите скопировать, нажмите .
4. Нажмите кнопку **Вставить правило**.
Откроется окно **Добавление правила**.
5. Нажмите кнопку **Добавить**.
6. Нажмите кнопку **Сохранить**.

Правило маршрутизации скопировано.

Изменение правила маршрутизации

► Чтобы изменить правило маршрутизации:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.
3. В блоке параметров **Правила маршрутизации почтового трафика** в строке правила, которое вы хотите изменить, нажмите .
4. Измените правило.
5. Нажмите кнопку **Изменить**.
6. Нажмите кнопку **Сохранить**.

Правило маршрутизации изменено.

Удаление правила маршрутизации

► Чтобы удалить правило маршрутизации:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.

3. В блоке параметров **Правила маршрутизации почтового трафика** в строке правила, которое вы хотите удалить, нажмите  и подтвердите удаление.

4. Нажмите кнопку **Сохранить**.

Правило маршрутизации удалено.

12.6. Отключение автоматической смены режимов проверки

Для источников с типами «Почтовый сервер в режиме фильтрации» и «Сервер Microsoft Exchange с установленным агентом» при большом количестве поступающих на проверку писем блокирующий режим проверки может автоматически меняться на пассивный. Это позволяет вовремя доставлять письма адресатам, но может привести к тому, что письма с угрозами попадут в информационную систему организации. После снижения нагрузки возвращается блокирующий режим проверки. Вы можете отключить для выбранных источников автоматическую смену режимов проверки. Инструкции необходимо выполнять на основном узле.

Внимание! После отключения автоматической смены режимов проверки для источника в случае нештатного прекращения проверки писем в PT Email Security письма от этого источника не будут доставляться адресатам.

► Чтобы отключить автоматическую смену режимов проверки для источника,

выполните команду:

```
sudo ptmsctl system components config patch --component <Название источника> --toml "[statistic]
enable_downgrade = false
"
```

► Чтобы включить автоматическую смену режимов проверки для источника,

выполните команду:

```
sudo ptmsctl system components config patch --component <Название источника> --toml "[statistic]
enable_downgrade = true
"
```

13. Подключение источников

В разделе описаны возможности подключения к PT Email Security источников объектов для проверки.

Внимание! Количество подов на любом узле PT Email Security не должно превышать 150. При добавлении источника в PT Email Security на основном узле для его работы создаются два пода. Отслеживать текущее количество созданных подов вы можете на странице **Система** → **Конфигурация** → **Узлы**. Если требуется увеличить максимальное количество подов на узле, обратитесь в техническую поддержку Positive Technologies.

Примечание. Если подключение источника какого-либо типа недоступно, обратитесь в техническую поддержку Positive Technologies.

В этом разделе

[Служба Checkme \(см. раздел 13.1\)](#)

[Общая папка \(см. раздел 13.2\)](#)

[Папка-шлюз \(см. раздел 13.3\)](#)

[S3-хранилище \(см. раздел 13.4\)](#)

[Внешняя система как ICAP-клиент \(см. раздел 13.5\)](#)

[Внешняя система через API \(см. раздел 13.6\)](#)

[Почтовый шлюз безопасности \(см. раздел 13.7\)](#)

[«Код безопасности», «Континент» 4.1 \(см. раздел 13.8\)](#)

[Exim 4 в режиме фильтрации \(см. раздел 13.9\)](#)

[Exim 4 в режиме зеркалирования \(см. раздел 13.10\)](#)

[Microsoft Exchange 2010–2019 с установленным почтовым агентом \(см. раздел 13.11\)](#)

[Microsoft Exchange 2010–2019 в режиме зеркалирования \(см. раздел 13.12\)](#)

[Postfix 3.2 в режиме фильтрации \(см. раздел 13.13\)](#)

[Postfix 3.2 в режиме зеркалирования \(см. раздел 13.14\)](#)

[PT Threat Analyzer 2.10 и выше \(см. раздел 13.15\)](#)

[RuPost 3.2, 4.1 в режиме фильтрации \(см. раздел 13.16\)](#)

[Squid 3 и выше \(см. раздел 13.17\)](#)

[UserGate NGFW 6, 7.1, 7.4 \(см. раздел 13.18\)](#)

13.1. Служба Checkme

PT Email Security может проверять письма и вложенные в них объекты, отправленные сотрудниками вашей организации на специальный электронный адрес. Результат проверки отправляется сотруднику в ответном письме. Служба Checkme обеспечивает взаимодействие PT Email Security с почтовым сервером вашей организации.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порты TCP 143, 587 или TCP 465, 993 (при подключении по SSL) от основного узла PT Email Security к почтовому серверу вашей организации.

Для создания и настройки службы Checkme необходимо:

- На почтовом сервере вашей организации создать электронный адрес для службы Checkme, например `checkme@example.com`.
- В PT Email Security добавить источник с типом **Служба Checkme** и указать для него параметры подключения к почтовому серверу вашей организации.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Служба Checkme**.
5. В блоке **Параметры подключения** настройте параметры IMAP-сервера для приема писем с вложениями для проверки:
 - В поле **Доменное имя или IP-адрес IMAP-сервера** введите адрес и порт сервера.
 - Если соединение с сервером устанавливается по протоколу SSL, установите флажок **Подключаться по SSL**.
 - В раскрывающемся списке **Тип аутентификации IMAP** выберите тип аутентификации при подключении к серверу.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- В полях **Логин** и **Пароль** введите учетные данные для подключения к серверу.
- 6. Если требуется, в блоке **Отправлять результат проверки в ответном письме** включите отправку писем с результатами проверки и настройте параметры SMTP-сервера для их отправки:
 - В поле **Доменное имя или IP-адрес SMTP-сервера** введите адрес и порт сервера.
 - В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
 - В раскрывающемся списке **Тип аутентификации IMAP** выберите тип аутентификации при подключении к серверу.
 - В полях **Логин** и **Пароль** введите учетные данные для подключения к серверу.
- 7. В поле **Эл. адрес службы Checkme** введите адрес, на который будут отправлять письма с вложениями для проверки, например `checkme@example.com`.
- 8. Нажмите кнопку **Добавить источник**.

13.2. Общая папка

Если для обмена файлами сотрудники вашей организации используют общую папку, с помощью PT Email Security вы можете организовать проверку файлов в этой папке. Проверяются все файлы в общей папке и вложенных в нее папках.

Для доступа к папке PT Email Security использует протоколы SMB версий 2 и 3 (с поддержкой DFS) или NFS версии 3.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порты TCP 139, 445 (SMB) или TCP 111, 2049 (NFS) от основного узла PT Email Security к узлу с общей папкой.

Для подключения общей папки необходимо:

- Создать папку и настроить общий доступ пользователей к этой папке.
- Предоставить PT Email Security право на чтение файлов в созданной папке и во всех вложенных папках.
- Добавить в PT Email Security источник с типом **Общая папка** с доступом к папке по протоколу SMB или NFS.

Алгоритм работы с общей папкой

PT Email Security проверяет общую папку на наличие в ней файлов, удовлетворяющих условиям:

- Новый файл, который никогда не проверялся.
- Задание на проверку файла завершилось с ошибкой более 1 часа назад.
- Задание на проверку файла завершилось успешно более 4 недель назад и хеш-сумма файла за это время изменилась.

Если файл в папке удовлетворяет хотя бы одному из условий выше, PT Email Security отслеживает его в течение 2 минут. По истечении этого времени:

- Если файл был изменен — отсчет времени начинается заново.
- Если не был изменен — создается задание на проверку.

Примечание. Одновременно PT Email Security может проверять не более 15 файлов из общей папки.

Повторная проверка общей папки выполняется через 5 минут после завершения предыдущей.

Добавление источника для протокола SMB

► Чтобы добавить источник с доступом к папке по протоколу SMB в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Общая папка**.
5. В полях блока **Доменное имя или IP-адрес узла с папкой** укажите параметры подключения к узлу с общей папкой:
 - Выберите протокол подключения **SMB**.
 - Введите доменное имя или IP-адрес узла.
 - Если для подключения используется нестандартный порт, укажите его.
6. Укажите параметры аутентификации:
 - В раскрывающемся списке **Тип аутентификации** выберите тип аутентификации.

- Если вы выбрали **Kerberos**, в поле **Доменное имя или IP-адрес контроллера домена** введите имя или адрес.
- В полях **Логин** и **Пароль** введите учетные данные для доступа к папке.

Если вы выбрали тип аутентификации Kerberos, логин необходимо указывать вместе с именем домена в формате <Имя домена>\<Логин>, например `yourdomain\ivanov`. Если вы выбрали NTLM, вы также можете указать имя домена в этом формате при необходимости.

7. В поле **Пути к папкам** введите пути к папкам для проверки на узле.

В качестве разделителя каталогов используйте косую черту `/`.

8. Если требуется исключить из проверки вложенные папки:

- Установите флажок **Не проверять указанные вложенные папки**.
- В поле ниже введите пути к вложенным папкам.

В качестве разделителя каталогов используйте косую черту `/`. Поддерживаются маски: `example/*` — для исключения всех вложенных папок, `*/example` — для исключения вложенной папки во всех добавленных папках.

9. Нажмите кнопку **Добавить источник**.

Добавление источника для протокола NFS

- Чтобы добавить источник с доступом к папке по протоколу NFS в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Общая папка**.
5. В полях блока **Доменное имя или IP-адрес узла с папкой** укажите параметры подключения к узлу с общей папкой:
 - Выберите протокол подключения **NFS**.
 - Введите доменное имя или IP-адрес узла.
 - Если для подключения используется нестандартный порт, укажите его.
6. В поле **Путь к папке** введите путь к общей папке.

В качестве разделителя каталогов используйте косую черту /.

7. Нажмите кнопку **Добавить источник**.

13.3. Папка-шлюз

Если для обмена файлами сотрудники вашей организации используют общую папку, с помощью PT Email Security вы можете настроить папку-шлюз. Проверяются все файлы в папке-шлюзе и вложенных в нее папках. По результатам проверки файлы из папки-шлюза переносятся в папку для безопасных файлов или папку карантина.

Для доступа к папкам PT Email Security использует протоколы SMB версий 2 и 3 (с поддержкой DFS) или NFS версии 3.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порты TCP 139, 445 (SMB) или TCP 111, 2049 (NFS) от основного узла PT Email Security к узлам, на которых расположены папка-шлюз, папка для безопасных файлов и папка карантина.

Для подключения папки-шлюза необходимо:

- Создать три папки и настроить общий доступ пользователей к этим папкам: папку-шлюз, папку для безопасных файлов и папку карантина. Папки могут располагаться на одном или на разных узлах.

Внимание! Папки не должны быть вложены друг в друга.

- Предоставить PT Email Security права на чтение, создание, изменение и удаление файлов и папок в созданных папках и во всех вложенных папках.
- Добавить в PT Email Security источник с типом **Папка-шлюз** с доступом к папкам по протоколу SMB или NFS.

Алгоритм работы с папкой-шлюзом

PT Email Security проверяет папку-шлюз на наличие новых файлов, которые никогда не проверялись, а также файлов, при проверке которых ранее произошла ошибка.

Если в папке есть такой файл, то PT Email Security отслеживает его в течение 2 минут. По истечении этого времени:

- Если файл был изменен — отсчет времени начинается заново.
- Если не был изменен — создается задание на проверку.

Примечание. Одновременно PT Email Security может проверять не более 30 файлов из папки-шлюза.

После завершения задания на проверку PT Email Security выполняет с файлом одно из действий:

- Если угроз не обнаружено, переносит файл в папку для безопасных файлов.
- Если файл представляет угрозу, переносит его в папку карантина.
- Если задание завершилось с ошибкой, оставляет файл в папке-шлюзе.

Повторная проверка папки-шлюза выполняется через 10 секунд после завершения предыдущей.

Добавление источника для протокола SMB

► Чтобы добавить источник с доступом к папкам по протоколу SMB в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.
4. В раскрывающемся списке **Тип** выберите **Папка-шлюз**.
5. В блоке параметров **Папка-шлюз** в полях блока **Доменное имя или IP-адрес узла с папкой** укажите параметры подключения к узлу с папкой-шлюзом:
 - Выберите протокол подключения **SMB**.
 - Введите доменное имя или IP-адрес узла.
 - Если для подключения используется нестандартный порт, укажите его.
6. Укажите параметры аутентификации:
 - В раскрывающемся списке **Тип аутентификации** выберите тип аутентификации.
 - Если вы выбрали **Kerberos**, в поле **Доменное имя или IP-адрес контроллера домена** введите имя или адрес.
 - В полях **Логин** и **Пароль** введите учетные данные для доступа к папке.

Если вы выбрали тип аутентификации Kerberos, логин необходимо указывать вместе с именем домена в формате <Имя домена>\<Логин>, например yourdomain\ivanov. Если вы выбрали NTLM, вы также можете указать имя домена в этом формате при необходимости.
7. В поле **Пути к папкам** введите пути к папкам для проверки на узле.

В качестве разделителя каталогов используйте косую черту /.

8. Если требуется исключить из проверки вложенные папки:
 - Установите флажок **Не проверять указанные вложенные папки**.
 - В поле ниже введите пути к вложенным папкам.
 В качестве разделителя каталогов используйте косую черту /. Поддерживаются маски: `example/*` — для исключения всех вложенных папок, `*/example` — для исключения вложенной папки во всех добавленных папках.
9. Если при перемещении проверенного файла в папку для безопасных файлов или папку карантина к пути файла требуется добавлять путь к исходной папке-шлюзу, установите флажок **Сохранять путь к папке-шлюзу**.
10. В блоке параметров **Папка для безопасных файлов** в полях блока **Доменное имя или IP-адрес узла с папкой** укажите параметры подключения к узлу с папкой для безопасных файлов:
 - Если папка расположена на том же узле, что и папка-шлюз, установите флажок **Такие же параметры, как у сервера папки-шлюза**.
 - Если папка расположена на другом узле, укажите параметры подключения к этому узлу.
11. В поле **Путь к папке** введите путь к папке на узле.
12. В блоке параметров **Папка карантина** в полях блока **Доменное имя или IP-адрес узла с папкой** укажите параметры подключения к узлу с папкой для файлов, представляющих угрозу:
 - Если папка расположена на том же узле, что и папка-шлюз, установите флажок **Такие же параметры, как у сервера папки-шлюза**.
 - Если папка расположена на другом узле, укажите параметры подключения к этому узлу.
13. В поле **Путь к папке** введите путь к папке на узле.
14. Нажмите кнопку **Добавить источник**.

Добавление источника для протокола NFS

- Чтобы добавить источник с доступом к папкам по протоколу NFS в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.
 Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.
4. В раскрывающемся списке **Тип** выберите **Папка-шлюз**.

5. В блоке параметров **Папка-шлюз** в полях блока **Доменное имя или IP-адрес узла с папкой** укажите параметры подключения к узлу с папкой-шлюзом:
 - Выберите протокол подключения **NFS**.
 - Введите доменное имя или IP-адрес узла.
 - Если для подключения используется нестандартный порт, укажите его.
6. В поле **Путь к папке** введите путь к папке-шлюзу на узле.
В качестве разделителя каталогов используйте косую черту /.
7. В блоке параметров **Папка для безопасных файлов** в полях блока **Доменное имя или IP-адрес узла с папкой** укажите параметры подключения к узлу с папкой для безопасных файлов:
 - Если папка расположена на том же узле, что и папка-шлюз, установите флажок **Такие же параметры, как у сервера папки-шлюза**.
 - Если папка расположена на другом узле, укажите параметры подключения к этому узлу.
8. В поле **Путь к папке** введите путь к папке на узле.
9. В блоке параметров **Папка карантина** в полях блока **Доменное имя или IP-адрес узла с папкой** укажите параметры подключения к узлу с папкой для файлов, представляющих угрозу:
 - Если папка расположена на том же узле, что и папка-шлюз, установите флажок **Такие же параметры, как у сервера папки-шлюза**.
 - Если папка расположена на другом узле, укажите параметры подключения к этому узлу.
10. В поле **Путь к папке** введите путь к папке на узле.
11. Нажмите кнопку **Добавить источник**.

13.4. S3-хранилище

Если для хранения файлов, писем и других объектов в вашей организации используется S3-хранилище, с помощью PT Email Security вы можете организовать проверку объектов в таком хранилище.

Внимание! Если провайдер S3-хранилища тарифицирует трафик или количество запросов, проверка объектов в PT Email Security может привести к дополнительным расходам.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 443 от узла источника к основному узлу PT Email Security.

Порядок подключения S3-хранилища зависит от провайдера. Как правило, для настройки доступа к хранилищу на сайте провайдера вам необходимо:

- Создать бакет (каталог верхнего уровня) для проверяемых объектов и указать для него название и регион, если предусмотрено провайдером.
- Создать сервисный аккаунт и предоставить ему право на чтение объектов бакета.
- Создать для сервисного аккаунта статический ключ доступа.

Примечание. Инструкции по настройке доступа к S3-хранилищу вы можете найти на сайте провайдера.

Для подключения S3-хранилища необходимо в PT Email Security добавить источник с типом **Общая папка** и протоколом подключения **S3**.

Алгоритм работы с S3-хранилищем

Сразу после добавления источника PT Email Security проверяет хранилище на наличие объектов, удовлетворяющих условиям:

- Новый объект, который никогда не проверялся.
- Задание на проверку объекта завершилось с ошибкой более 1 часа назад.
- Задание на проверку объекта завершилось успешно более 4 недель назад и хеш-сумма объекта за это время изменилась.

Если объект в хранилище удовлетворяет хотя бы одному из условий выше, PT Email Security отслеживает его в течение 2 минут. По истечении этого времени:

- Если объект был изменен — отсчет времени начинается заново.
- Если не был изменен — создается задание на проверку.

Примечание. Одновременно PT Email Security может проверять не более 15 объектов из хранилища.

Повторная проверка хранилища выполняется через 5 минут после завершения предыдущей.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Общая папка**.
5. В полях блока **Доменное имя или IP-адрес узла с папкой** укажите параметры подключения к S3-хранилищу:
 - Выберите протокол подключения **S3**.
 - Введите доменное имя или IP-адрес провайдера хранилища.
 - Если для подключения используется нестандартный порт, укажите его.
6. Если при подключении к хранилищу используется SSL, установите флажок **Использовать SSL**.
7. Если используется SSL и необходимо проверять используемый сертификат, установите флажок **Проверять подлинность SSL-сертификата**.
8. Если код региона отличается от `us-east-1`, в поле **Регион** введите код, предоставленный провайдером или указанный вами при создании бакета (например `ru-central-1`).
9. В полях **Логин** и **Пароль** введите данные статического ключа доступа, созданного для сервисного аккаунта.
10. В поле **Путь к папке** введите название бакета или объекта в бакете.
 Название бакета может содержать только буквы латинского алфавита, цифры, точку, дефис и символ подчеркивания. В качестве разделителя для названий объектов в бакете используйте косую черту `/`.
11. Нажмите кнопку **Добавить источник**.

13.5. Внешняя система как ICAP-клиент

PT Email Security может проверять объекты, поступающие от внешних систем по протоколу ICAP. Для этого в PT Email Security настраивается ICAP-сервер, а внешняя система выступает в качестве ICAP-клиента.

Примечание. Ответ ICAP-сервера с результатом проверки объекта формируется только на основании статического анализа, сразу после его завершения. Если настроен поведенческий анализ, его результаты не влияют на работу ICAP-клиента, но доступны в карточке задания.

В зависимости от приобретенной вами лицензии PT Email Security и выбранных параметров работы ICAP-сервера проверка может выполняться в блокирующем режиме, режиме ожидания или в пассивном режиме:

- В блокирующем режиме при обнаружении угрозы ICAP-сервер отправляет в ответе ICAP-клиенту уведомление о необходимости блокировки объекта. Если в течение установленного тайм-аута ICAP-сервер не отправляет ответ, объект считается безопасным.
- В режиме ожидания при обнаружении угрозы ICAP-сервер отправляет ICAP-клиенту ответ с кодом 204 и добавляет в заголовок ответа X-Virus-ID краткое описание обнаруженной угрозы. Если в течение установленного тайм-аута ICAP-сервер не отправляет ответ, объект считается безопасным. Этот режим может использоваться для интеграции со сторонними системами, которые самостоятельно принимают решение о блокировке объектов.
- В пассивном режиме объект сразу пропускается в информационную систему, а не задерживается ICAP-сервером на время проверки, как в других режимах. Результаты проверки не влияют на работу ICAP-клиента, но доступны в карточке задания.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 1344 от узла источника к основному узлу PT Email Security.

Для подключения внешней системы в PT Email Security необходимо добавить источник с типом **ICAP-сервер**.

Во внешней системе необходимо настроить ICAP-клиент для работы с ICAP-сервером, созданным при добавлении источника в PT Email Security:

- Необходимо указать ссылку для обращения к ICAP-серверу PT Email Security. Вид ссылки зависит от режима проверки объектов и режима работы ICAP-сервера.
- Если требуется отправлять IP-адрес пользователя, скачавшего файл, нужно настроить отправку поля заголовка X-Client-IP.
- Если требуется отправлять имя пользователя, скачавшего файл, нужно настроить отправку поля заголовка X-Client-Username.
- Если ICAP-клиент поддерживает режим ICAP Preview, рекомендуется отключить этот режим.

При настройке ICAP-клиента вам необходимо указать ссылку для обращения к ICAP-серверу PT Email Security. Вид ссылки зависит от режима проверки объектов и режима работы ICAP-сервера:

- Ссылки для проверки объектов в блокирующем режиме:
 - REQMOD: `icap://<IP-адрес>:<Порт>/scanrequest?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=<Тайм-аут>`
 - RESPMOD: `icap://<IP-адрес>:<Порт>/scanresponse?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=<Тайм-аут>`

Примечание. В параметре `block-unwanted` вы можете указать `y`, если необходимо блокировать потенциально опасные файлы, или `n` — если блокировать такие файлы не требуется (по умолчанию потенциально опасные файлы не блокируются). В параметре `timeout` вы можете указать тайм-аут ответа ICAP-сервера в секундах (по умолчанию 30 секунд).

- Ссылки для проверки объектов в режиме ожидания:
 - `REQMOD: icap://<IP-адрес>:<Порт>/scanrequest?modify=no&timeout=<Тайм-аут>`
 - `RESPMOD: icap://<IP-адрес>:<Порт>/scanresponse?modify=no&timeout=<Тайм-аут>`
- Ссылки для проверки объектов в пассивном режиме:
 - `REQMOD: icap://<IP-адрес>:<Порт>/bypass`
 - `RESPMOD: icap://<IP-адрес>:<Порт>/bypass`

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **ICAP-сервер**.
5. Если необходимо, в поле **IP-адреса ICAP-сервера** введите дополнительные адреса.

Примечание. В поле указан IP-адрес ICAP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.

6. Если необходимо, измените стандартный порт подключения к ICAP-серверу.

Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.

7. Если необходимо принимать объекты только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
8. Нажмите кнопку **Добавить источник**.

13.6. Внешняя система через API

PT Email Security может проверять объекты, поступающие от внешних систем через публичный API. Проверка выполняется в режиме ожидания.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 443 от узла источника к основному узлу PT Email Security.

Примечание. На размер файлов, поступающих на проверку в PT Email Security через публичный API, установлено ограничение в 1 ГБ. При необходимости вы можете изменить этот размер командой `sudo ptmsctl system components set -c nginx -p max_file_size=<Размер в МБ>`.

PT Email Security поддерживает два способа проверки объектов, поступающих от внешних систем через публичный API: когда параметры проверки передаются в запросе вместе с каждым объектом и когда объекты проверяются с общими параметрами проверки, добавленного в PT Email Security источника.

Для подключения внешней системы при проверке объектов с передаваемыми параметрами необходимо:

- В PT Email Security выпустить токен доступа к публичному API с разрешенным действием **Проверка с передаваемыми параметрами**.
- Во внешней системе настроить отправку объектов в PT Email Security через публичный API. Каждый запрос должен содержать в заголовке X-API-Key выпущенный токен доступа.

Для подключения внешней системы при проверке объектов с параметрами источника необходимо:

- В PT Email Security выпустить токен доступа к публичному API с разрешенным действием **Проверка с параметрами источника**.
- Добавить в PT Email Security источник с типом **API с выбранными параметрами проверки**.
- Во внешней системе настроить отправку объектов в PT Email Security через публичный API. Каждый запрос должен содержать в заголовке X-API-Key выпущенный токен доступа.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **API с выбранными параметрами проверки**.
5. В раскрывающемся списке **Токен доступа** выберите токен доступа к публичному API.
6. Нажмите кнопку **Добавить источник**.

13.7. Почтовый шлюз безопасности

При установке и подключении почтового шлюза безопасности письма от SMTP-клиентов принимаются шлюзом и отправляются на проверку в PT Email Security, после чего доставляются получателям через указанные в правилах маршрутизации почтовые серверы.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, необходимо настроить в них правила, разрешающие передачу трафика от почтового шлюза безопасности к основному узлу PT Email Security на порты 50025 и 50052.

Для подключения источника к PT Email Security необходимо:

1. Развернуть почтовый шлюз безопасности на отдельном узле.
2. Добавить в PT Email Security агент почтового шлюза безопасности, установленный на узле шлюза.
3. Если требуется, в PT Email Security [изменить параметры подключения почтового шлюза безопасности \(см. раздел 11.8\)](#).
4. Добавить в PT Email Security источник с типом **Почтовый шлюз безопасности**.
5. Подключить к источнику добавленный агент почтового шлюза безопасности.
6. Настроить в сетевой инфраструктуре организации маршрутизацию писем через почтовый шлюз безопасности.
7. Настроить в PT Email Security отправку проверенных писем:
 - Если используется несколько почтовых серверов, добавить правила маршрутизации.
 - Если используются непубличные почтовые серверы и требуется TLS-шифрование с проверкой сертификата, добавить корневой сертификат центра сертификации вашей организации.
 - Если на почтовых серверах поддерживается проверка адресов получателей, включить такую проверку для добавленного источника.

В этом разделе

[Развертывание почтового шлюза безопасности \(см. раздел 13.7.1\)](#)

[Добавление агента почтового шлюза в PT Email Security \(см. раздел 13.7.2\)](#)

[Добавление источника в PT Email Security \(см. раздел 13.7.3\)](#)

[Подключение агента почтового шлюза к источнику \(см. раздел 13.7.4\)](#)

[Добавление правил маршрутизации проверенных писем \(см. раздел 13.7.5\)](#)

[Добавление доверенных сертификатов \(см. раздел 13.7.6\)](#)

[Включение проверки адресов получателей \(см. раздел 13.7.7\)](#)

13.7.1. Развертывание почтового шлюза безопасности

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика от узлов SMTP-клиентов к узлу почтового шлюза безопасности на порт TCP 25.

Почтовый шлюз безопасности может быть развернут как на физическом сервере, так и в виртуальной среде. При развертывании почтового шлюза безопасности вам необходимо установить на узле агент почтового шлюза безопасности.

Аппаратные требования

Минимальные аппаратные требования к узлу для установки почтового шлюза безопасности указаны в таблице.

Таблица 4. Минимальные аппаратные требования к узлу

Компонент	Требование
Центральный процессор 2,2 ГГц, количество потоков	2
Память ОЗУ, ГБ	4
SSD, ГБ	40

Программные требования

Внимание! Каталог `/var` должен быть вынесен в отдельный раздел диска объемом не менее 30 ГБ.

Примечание. Для установки почтового шлюза безопасности в виртуальной среде необходимо использовать гипервизор VMware ESXi версии 6.0 или выше с аппаратным обеспечением версии 11 или выше.

Установка почтового шлюза безопасности возможна на узле с 64-разрядной операционной системой:

- Astra Linux Special Edition 1.8;
- Debian GNU/Linux 12;
- «ОСнова» 3.

К настройке операционной системы на узле для установки почтового шлюза безопасности выдвигаются следующие требования:

- Установлен и запущен почтовый транспортный агент Postfix.
- Установлена и запущена служба журналирования: rsyslog — для Debian и «ОСнова», syslog-ng — для Astra Linux.
- Установлено точное время и настроена синхронизация с NTP-сервером.
- Настроено подключение к DNS-серверу.
- Настроен менеджер пакетов APT.
- Установлена программа sudo. Пользователь, от имени которого выполняется установка, добавлен в группу sudo.

Установка агента почтового шлюза безопасности

Установочный пакет агента почтового шлюза безопасности входит в комплект поставки PT Email Security. После распаковки архива с установщиком PT Email Security установочный пакет агента будет доступен в каталоге `ptsb-installer/espa`.

► Чтобы установить на узле агент почтового шлюза безопасности:

1. Скопируйте установочный пакет в любой каталог на узле.
2. Перейдите в этот каталог.
3. Выполните команду:

```
sudo dpkg -i espa_<Версия>_amd64.deb
```

Изменение максимального размера проверяемых писем

По умолчанию почтовый шлюз безопасности поддерживает проверку писем размером до 20 МБ. При необходимости вы можете увеличить этот размер. Не рекомендуется устанавливать максимальный размер писем более 100 МБ.

► Чтобы изменить максимальный размер проверяемых писем:

1. Откройте файл `/etc/espa/config.toml`.
2. В секции `postfix` в параметре `message_size_limit` укажите максимальный размер письма в байтах:

```
message_size_limit = <Размер в байтах>
```

Например:

```
message_size_limit = 52428800
```

3. Сохраните изменения и закройте файл.
4. Перезапустите службу конфигуратора шлюза:

```
sudo systemctl restart espa-configurator
```

13.7.2. Добавление агента почтового шлюза в PT Email Security

Для добавления агента почтового шлюза в PT Email Security вам необходимо получить команду сопряжения агента почтового шлюза с PT Email Security и выполнить эту команду на узле с установленным агентом.

Инструкцию необходимо выполнить в интерфейсе PT Email Security.

- ▶ Чтобы получить команду для сопряжения агента почтового шлюза с PT Email Security:

1. В главном меню выберите **Источники** → **Агенты почтового шлюза**.
2. Нажмите кнопку **Добавить**.

Откроется окно **Добавление агента**.

3. В поле **IP-адрес узла с агентом** введите адрес узла.
4. Нажмите кнопку **Добавить**.

Откроется окно **Команда для сопряжения**.

5. Нажмите кнопку **Скопировать в буфер обмена и закрыть**.

Примечание. После закрытия окна вы сможете посмотреть команду сопряжения, нажав в строке агента .

Инструкцию необходимо выполнить на узле с установленным агентом почтового шлюза безопасности.

- ▶ Чтобы добавить агент почтового шлюза в PT Email Security,

выполните команду сопряжения, например:

```
sudo espa pair --key 89602a09-4b47-47b4-a02b-51216470be07 --grpc-port 50052 --server-ca "LS...Qo=" --ip 192.0.1.1 --smtp-port 50025
```

13.7.3. Добавление источника в PT Email Security

- ▶ Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.

3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Почтовый шлюз безопасности**.
5. Выберите для всех правил маршрутизации, какой набор доверенных сертификатов будет использоваться при проверке сертификатов серверов для проверенной почты:
 - Если только доверенные сертификаты из внутреннего хранилища PT Email Security, в раскрывающемся списке **Доверенные сертификаты TLS-шифрования** выберите **Пользовательские**.
 - Если сертификаты из внутреннего хранилища и глобальные сертификаты, доступные внутри Docker-контейнеров PT Email Security, выберите **Глобальные и пользовательские**.
6. Добавьте правило маршрутизации по умолчанию и укажите в нем параметры сервера для отправки писем и уведомлений о результатах проверки:
 - Нажмите кнопку **Добавить**.
 - В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
 - Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.
 - В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
 - Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.

- Если в вашей организации используется несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.
 - Нажмите кнопку **Добавить**.
7. Если необходимо пересылать скрытые копии проверенных писем дополнительным получателям:
 - В блоке параметров **Пересылать письма дополнительным получателям** включите пересылку писем.
 - В появившемся поле введите электронные адреса получателей.
 8. Нажмите кнопку **Добавить источник**.

13.7.4. Подключение агента почтового шлюза к источнику

Для подключения агента почтового шлюза к источнику агент должен быть добавлен в PT Email Security. К одному источнику можно подключить несколько агентов почтового шлюза.

- Чтобы подключить агент почтового шлюза к источнику:
1. В главном меню выберите **Источники** → **Управление источниками**.
 2. Нажмите на панель с информацией об источнике с типом **Почтовый шлюз безопасности**.
 3. Выберите вкладку **Агенты почтового шлюза**.
 4. Нажмите кнопку **Подключить агент**.
Откроется окно **Подключение агента**.
 5. Выберите агент в списке.
 6. Нажмите кнопку **Подключить**.

13.7.5. Добавление правил маршрутизации проверенных писем

Если необходимо использовать различные почтовые серверы в зависимости от домена в адресе электронной почты получателя, вы можете настроить в PT Email Security [правила маршрутизации проверенных писем](#) (см. раздел 12.5).

- Чтобы добавить правило маршрутизации:
1. В главном меню выберите **Источники** → **Управление источниками**.
 2. В панели с информацией об источнике перейдите по ссылке **Параметры источника**.

3. В блоке параметров **Правила маршрутизации почтового трафика** нажмите кнопку **Добавить**.

4. В поле **Домен электронной почты получателя** введите доменную часть адреса электронной почты получателей, для которых необходимо настроить правило.

С помощью звездочки вы можете задать маску для доменной части адреса получателей писем, если доменная часть содержит поддомены третьего уровня или выше. Например, правило с маской *.example.com будет применяться и для адресов с доменной частью example.com, sub_1.example.com, sub_2.example.com, и для адресов с доменной частью, содержащей поддомены более высоких уровней.

Примечание. Если доменная часть адреса получателя соответствует нескольким правилам маршрутизации, будет использовано то правило, в котором указан наиболее точный адрес. При этом более высокий приоритет имеют правила, в которых не используются маски.

5. В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
6. Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.
7. Если необходимо перенаправлять письма согласно MX-записям, выберите способ маршрутизации **По MX-записям**.

Внимание! Письмо не будет отправлено, если в DNS отсутствует подходящая MX- или A-запись для указанного домена.

8. Если необходимо перенаправлять письма на определенный почтовый сервер, выберите способ маршрутизации **По адресам почтовых серверов** и укажите параметры сервера:

- В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
- Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
- Если в вашей организации используется несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.

9. Нажмите кнопку **Добавить**.

10. Нажмите кнопку **Сохранить**.

Правило маршрутизации добавлено.

13.7.6. Добавление доверенных сертификатов

Если при отправке проверенных писем вы планируете использовать TLS-шифрование с проверкой сертификата, при проверке сертификатов почтовых серверов будут использоваться следующие сертификаты:

- Для публичных SMTP-серверов — сертификаты доверенных центров сертификации, доступные внутри Docker-контейнеров PT Email Security.
- Для непубличных SMTP-серверов вашей организации — доверенные сертификаты центров сертификации вашей организации. Корневые сертификаты этих центров необходимо добавить в PT Email Security.

Инструкции необходимо выполнять на основном узле PT Email Security. Поддерживаются только сертификаты формата PEM.

- Чтобы добавить сертификат в PT Email Security,

выполните команду:

```
sudo ptmsctl system trusted-certs add --name <Название сертификата> --path <Полный путь к файлу сертификата>
```

Например:

```
sudo ptmsctl system trusted-certs add --name example_cert --path /etc/tls/certs/rootCA.crt
```

- Чтобы просмотреть список добавленных в PT Email Security сертификатов,

выполните команду:

```
sudo ptmsctl system trusted-certs list
```

Примечание. Вы можете просмотреть информацию об отдельном сертификате, выполнив команду `sudo ptmsctl system trusted-certs view --name <Название сертификата>`.

- Чтобы удалить сертификат из PT Email Security,

выполните команду:

```
sudo ptmsctl system trusted-certs delete --name <Название сертификата>
```

Например:

```
sudo ptmsctl system trusted-certs delete --name example_cert
```

13.7.7. Включение проверки адресов получателей

Перед отправкой проверенных писем PT Email Security может проверять адреса получателей на принимающих почтовых серверах с помощью SMTP-команды **VRFY** (согласно спецификации RFC 5321). По умолчанию эта проверка отключена, поскольку на некоторых почтовых серверах выполнение этой команды может быть заблокировано по соображениям безопасности. Вы можете включить для источника проверку адресов получателей, если для него добавлено хотя бы одно правило маршрутизации или указано более одного почтового сервера. Инструкцию необходимо выполнить на основном узле PT Email Security.

- ▶ Чтобы включить проверку адресов получателей для источника,

выполните команду:

```
sudo ptmsctl system components config patch --component <Название источника> --toml "[smtp_client_config.verify_recipients]
enabled = true
"
```

13.8. «Код безопасности», «Континент» 4.1

При подключении источника объекты от межсетевого экрана «Континент» отправляются на проверку в PT Email Security по протоколу ICAP. В зависимости от приобретенной вами лицензии и выбранных параметров работы ICAP-сервера PT Email Security проверка может выполняться в режиме ожидания, в пассивном или блокирующем режиме.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 1344 от узла источника к основному узлу PT Email Security.

Для подключения источника к PT Email Security необходимо:

- Добавить в PT Email Security источник с типом **ICAP-сервер**.
- На межсетевом экране «Континент» настроить ICAP-клиент для работы с ICAP-сервером PT Email Security.

Добавление источника в PT Email Security

- ▶ Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.

3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **ICAP-сервер**.
5. Если необходимо, в поле **IP-адреса ICAP-сервера** введите дополнительные адреса.

Примечание. В поле указан IP-адрес ICAP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.

6. Если необходимо, измените стандартный порт подключения к ICAP-серверу.

Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.

7. Если необходимо принимать объекты только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
8. Нажмите кнопку **Добавить источник**.

Настройка источника

Для межсетевого экрана «Континент» необходимо настроить ICAP-клиент для работы с ICAP-сервером, созданным при добавлении источника в PT Email Security. Дополнительную информацию о настройке межсетевого экрана «Континент» вы можете получить на сайте securitycode.net.

При настройке ICAP-клиента вам необходимо указать ссылки для обращения к ICAP-серверу PT Email Security. Вид ссылки зависит от режима проверки объектов и режима работы ICAP-сервера:

- Ссылки для проверки объектов в блокирующем режиме:
 - REQMOD: /scanrequest?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=5
 - RESPMOD: /scanresponse?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=5

Примечание. В параметре `block-unwanted` вы можете указать `y`, если необходимо блокировать потенциально опасные файлы, или `n` — если блокировать такие файлы не требуется (по умолчанию потенциально опасные файлы не блокируются). В параметре `timeout` вы можете изменить тайм-аут ответа ICAP-сервера в секундах.

— Ссылки для проверки объектов в режиме ожидания:

- REQMOD: `/scanrequest?modify=no&timeout=5`
- RESPMOD: `/scanresponse?modify=no&timeout=5`

— Ссылки для проверки объектов в пассивном режиме:

- REQMOD: `/bypass`
- RESPMOD: `/bypass`

► Чтобы настроить ICAP-клиент:

1. Запустите «Менеджер конфигурации» межсетевого экрана «Континент».
2. Подключитесь к центру управления сетью (ЦУС) под учетной записью администратора.
3. В левой части окна нажмите кнопку **Контроль доступа**.
4. В панели **Навигация** выберите **Межсетевой экран** → **Группы Web/FTP-фильтров** → **ICAP-серверы**.
5. В панели инструментов нажмите кнопку **ICAP-сервер**.
Откроется окно **ICAP-сервер** на вкладке **Общие сведения**.
6. Укажите информацию об ICAP-сервере:

- В поле **Название** введите произвольное название ICAP-сервера.
- В поле **Адрес сервера** введите адрес ICAP-сервера PT Email Security.
- Если используемый порт отличается от 1344, в поле **Порт** введите номер порта.
- В поле **Тайм-аут опроса ICAP-сервера** введите 75.

Внимание! Тайм-аут опроса ICAP-сервера должен быть на 5–15 секунд больше значения параметра `timeout` в ссылке для обращения к ICAP-серверу PT Email Security.

- Если политика безопасности вашей организации позволяет пропускать непроверенные объекты, установите флажок **Пропускать при недоступности сервера**.
7. Выберите вкладку **Дополнительно**.
 8. Укажите ссылки для обращения к ICAP-серверу PT Email Security для выбранного вами режима проверки объектов:
 - Установите флажок **Режим модификации запроса** и в поле **Путь к службе** введите ссылку для REQMOD.
 - Установите флажок **Режим модификации ответа** и в поле **Путь к службе** введите ссылку на ICAP-сервер PT Email Security для RESPMOD.

- Установите флажок **Отправлять имя пользователя** и в поле **Заголовок** введите X-Client-Username.
 - Установите флажок **Отправлять IP-адрес** и в поле **Заголовок** введите X-Client-Ip.
9. Если требуется отправлять на проверку только определенные типы файлов, выберите вкладку **Фильтры** и по кнопке  добавьте MIME-типы файлов.
10. Нажмите кнопку **ОК**.
11. В панели **Навигация** выберите **Межсетевой экран** → **Группы Web/FTP-фильтров** → **Профили Web/FTP-фильтрации**.
12. Добавьте профиль для фильтрации HTTP-трафика:
- В панели инструментов нажмите кнопку **Профиль Web/FTP-фильтрации**.
 - В поле **Название** введите HTTP.
 - В раскрывающемся списке **Схема** выберите HTTP.
 - В меню кнопки  выберите **ICAP-серверы**.
 - В открывшемся окне выберите добавленный ранее ICAP-сервер.
 - После добавления сервера в списке **Группы Web/FTP-фильтров** в столбце **Действие** выберите режим проверки объектов.
 - Нажмите кнопку **ОК**.
13. Добавьте профиль для фильтрации HTTPS-трафика:
- В панели инструментов нажмите кнопку **Профиль Web/FTP-фильтрации**.
 - В поле **Название** введите HTTPS.
 - В раскрывающемся списке **Схема** выберите HTTPS.
 - В меню кнопки  выберите **ICAP-серверы**.
 - В открывшемся окне выберите добавленный ранее ICAP-сервер.
 - После добавления сервера в списке **Группы Web/FTP-фильтров** в столбце **Действие** выберите режим проверки объектов.
 - Нажмите кнопку **ОК**.
14. В панели **Навигация** выберите **Межсетевой экран**.
15. В панели инструментов нажмите кнопку **Установить**.
- ICAP-клиент настроен.

13.9. Exim 4 в режиме фильтрации

При подключении источника письма с сервера Exim отправляются на проверку в PT Email Security, после чего возвращаются обратно для дальнейшей доставки.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 25 от почтового сервера к основному узлу PT Email Security.

Для подключения источника к PT Email Security необходимо:

1. Добавить в PT Email Security источник с типом **Почтовый сервер в режиме фильтрации** или **Почтовый сервер в режиме фильтрации (MTA)**.
2. Настроить в PT Email Security отправку проверенных писем:
 - Если используется несколько почтовых серверов, добавить правила маршрутизации.
 - Если используются непубличные почтовые серверы и требуется TLS-шифрование с проверкой сертификата, добавить корневой сертификат центра сертификации вашей организации.
 - Если на почтовых серверах поддерживается проверка адресов получателей, включить такую проверку для добавленного источника.
3. На сервере Exim настроить маршрутизацию писем через PT Email Security.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите:
 - Если для работы с письмами от источника необходимо использовать встроенный в PT Email Security почтовый транспортный агент, выберите **Почтовый сервер в режиме фильтрации (MTA)**.
 - Если в этом нет необходимости, выберите **Почтовый сервер в режиме фильтрации**.

5. Если вы выбрали тип **Почтовый сервер в режиме фильтрации (MTA)**, в блоке параметров **Режим обработки писем** выберите режим:
 - Если хранение и доставку проверенных писем должен контролировать PT Email Security, выберите **Асинхронный**.
 - Если это должен делать почтовый сервер, выберите **Синхронный**.
6. В блоке **Параметры подключения** настройте параметры SMTP-сервера, создаваемого в PT Email Security для приема писем:
 - Если необходимо, в поле **IP-адреса SMTP-сервера** введите дополнительные адреса.

Примечание. В поле указан IP-адрес SMTP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.

- Если необходимо, измените стандартный порт подключения к серверу.
- Внимание!** Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.
- Если при подключении используется протокол SSL, установите флажок **Подключаться по SSL**.

Примечание. При снятом флажке передаваемые данные зашифровываются при помощи расширения STARTTLS. Если почтовый сервер организации не поддерживает STARTTLS, данные передаются без шифрования.

7. Если необходимо принимать письма только с определенных IP-адресов:
 - В блоке параметров **Фильтровать входящие подключения** включите фильтрацию.
 - В появившемся поле введите IP-адреса разрешенных узлов или подсетей.
8. Выберите для всех правил маршрутизации, какой набор доверенных сертификатов будет использоваться при проверке сертификатов серверов для проверенной почты:
 - Если только доверенные сертификаты из внутреннего хранилища PT Email Security, в раскрывающемся списке **Доверенные сертификаты TLS-шифрования** выберите **Пользовательские**.
 - Если сертификаты из внутреннего хранилища и глобальные сертификаты, доступные внутри Docker-контейнеров PT Email Security, выберите **Глобальные и пользовательские**.
9. Добавьте правило маршрутизации по умолчанию и укажите в нем параметры сервера для отправки писем и уведомлений о результатах проверки:
 - Нажмите кнопку **Добавить**.
 - В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
 - Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.

- В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
- Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
- Если в вашей организации используется несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.
- Нажмите кнопку **Добавить**.

10. Если необходимо пересылать скрытые копии проверенных писем дополнительным получателям:

- В блоке параметров **Пересылать письма дополнительным получателям** включите пересылку писем.
- В появившемся поле введите электронные адреса получателей.

11. Нажмите кнопку **Добавить источник**.

Добавление правила маршрутизации проверенных писем в PT Email Security

Если необходимо использовать различные почтовые серверы в зависимости от домена в адресе электронной почты получателя, вы можете настроить в PT Email Security [правила маршрутизации проверенных писем](#) (см. раздел 12.5).

► Чтобы добавить правило маршрутизации:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры источника**.

3. В блоке параметров **Правила маршрутизации почтового трафика** нажмите кнопку **Добавить**.

4. В поле **Домен электронной почты получателя** введите доменную часть адреса электронной почты получателей, для которых необходимо настроить правило.

С помощью звездочки вы можете задать маску для доменной части адреса получателей писем, если доменная часть содержит поддомены третьего уровня или выше. Например, правило с маской *.example.com будет применяться и для адресов с доменной частью example.com, sub_1.example.com, sub_2.example.com, и для адресов с доменной частью, содержащей поддомены более высоких уровней.

Примечание. Если доменная часть адреса получателя соответствует нескольким правилам маршрутизации, будет использовано то правило, в котором указан наиболее точный адрес. При этом более высокий приоритет имеют правила, в которых не используются маски.

5. В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
6. Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.
7. Если необходимо перенаправлять письма согласно MX-записям, выберите способ маршрутизации **По MX-записям**.

Внимание! Письмо не будет отправлено, если в DNS отсутствует подходящая MX- или A-запись для указанного домена.

8. Если необходимо перенаправлять письма на определенный почтовый сервер, выберите способ маршрутизации **По адресам почтовых серверов** и укажите параметры сервера:

- В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
- Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
- Если в вашей организации используется несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.

9. Нажмите кнопку **Добавить**.

10. Нажмите кнопку **Сохранить**.

Правило маршрутизации добавлено.

Добавление доверенных сертификатов в PT Email Security

Если при отправке проверенных писем вы планируете использовать TLS-шифрование с проверкой сертификата, при проверке сертификатов почтовых серверов будут использоваться следующие сертификаты:

- Для публичных SMTP-серверов — сертификаты доверенных центров сертификации, доступные внутри Docker-контейнеров PT Email Security.
- Для непубличных SMTP-серверов вашей организации — доверенные сертификаты центров сертификации вашей организации. Корневые сертификаты этих центров необходимо добавить в PT Email Security.

Инструкции необходимо выполнять на основном узле PT Email Security. Поддерживаются только сертификаты формата PEM.

- ▶ Чтобы добавить сертификат в PT Email Security,

выполните команду:

```
sudo ptmsctl system trusted-certs add --name <Название сертификата> --path <Полный путь к файлу сертификата>
```

Например:

```
sudo ptmsctl system trusted-certs add --name example_cert --path /etc/tls/certs/rootCA.crt
```

- ▶ Чтобы просмотреть список добавленных в PT Email Security сертификатов,

выполните команду:

```
sudo ptmsctl system trusted-certs list
```

Примечание. Вы можете просмотреть информацию об отдельном сертификате, выполнив команду `sudo ptmsctl system trusted-certs view --name <Название сертификата>`.

- ▶ Чтобы удалить сертификат из PT Email Security,

выполните команду:

```
sudo ptmsctl system trusted-certs delete --name <Название сертификата>
```

Например:

```
sudo ptmsctl system trusted-certs delete --name example_cert
```

Включение проверки адресов получателей

Перед отправкой проверенных писем PT Email Security может проверять адреса получателей на принимающих почтовых серверах с помощью SMTP-команды `VRFY` (согласно спецификации RFC 5321). По умолчанию эта проверка отключена, поскольку на некоторых почтовых серверах выполнение этой команды может быть заблокировано по соображениям безопасности. Вы можете включить для источника проверку адресов получателей, если для него добавлено хотя бы одно правило маршрутизации или указано более одного почтового сервера. Инструкцию необходимо выполнить на основном узле PT Email Security.

- ▶ Чтобы включить проверку адресов получателей для источника,

выполните команду:

```
sudo ptmsctl system components config patch --component <Название источника> --toml "[smtp_client_config.verify_recipients]
enabled = true
"
```

Настройка источника

На сервере Exim необходимо настроить маршрутизацию писем через PT Email Security.

Инструкция разработана для Exim версии 4 с отдельными файлами конфигурации. Если вы используете единый конфигурационный файл, указанные в инструкции строки необходимо добавлять в этот файл. Дополнительную информацию вы можете получить на сайте exim.org.

- ▶ Чтобы настроить маршрутизацию писем через PT Email Security:

1. Создайте транспорт `remote_smtp_check`:

- Создайте файл `45_exim4-config_remote_smtp_check`:

```
sudo nano etc/exim4/conf.d/transport/45_exim4-config_remote_smtp_check
```

- Добавьте в файл строки, указав порт SMTP-сервера PT Email Security:

```
remote_smtp_check:
  driver = smtp
  port = <Порт PT Email Security>
  delay_after_cutoff = false
```

- Если необходимо увеличить тайм-ауты SMTP-сессии, добавьте в файл в секцию `remote_smtp_check` строки:

```
command_timeout = 25m
final_timeout = 30m
```

Примечание. Тайм-ауты SMTP-сессии должны превышать время проверки письма в PT Email Security. Если в вашей организации разрешена отправка писем с вложениями большого размера (сотни мегабайт), рекомендуется увеличить тайм-ауты SMTP-сессии.

- Сохраните изменения и закройте файл.

2. Настройте правило маршрутизации почтового трафика Exim:

- Создайте файл `050_exim4-config_ptes`.

```
sudo nano /etc/exim4/conf.d/router/050_exim4-config_ptes
```

- Добавьте в файл строки, указав порт сервера Exim для проверенных писем и адрес SMTP-сервера PT Email Security:

```
send_to_check:
    driver = manualroute
    condition = ${if eq {$interface_port}{<Порт Exim>}{no}{yes}}
    transport = remote_smtp_check
    route_list = * <IP-адрес PT Email Security>
    address_test = false
```

- Сохраните изменения и закройте файл.

Внимание! Правило маршрутизации `send_to_check` должно иметь самый высокий приоритет. Для этого в каталоге `/etc/exim4/conf.d/router` файл `050_exim4-config_scanner` должен располагаться сразу после файла `00_exim4-config_header`.

3. Добавьте список контроля доступа (ACL) для писем от PT Email Security:

- Создайте файл `25_exim4-config_check_host`:

```
sudo nano /etc/exim4/conf.d/acl/25_exim4-config_check_host
```

- Добавьте в файл строки, указав порт Exim для проверенных писем и адрес SMTP-сервера PT Email Security:

```
acl_check_host:
    deny
        message = Untrusted sender host
        condition = ${if eq {$interface_port}{<Порт Exim>}{yes}{no}}
        condition = ${if match_ip{$sender_host_address}{<IP-адрес PT Email Security>}{no}{yes}}
    accept
```

- Сохраните изменения и закройте файл.

4. Добавьте в конфигурацию Exim созданный список контроля доступа:

- Создайте файл `02_exim4-config_acl_pre_options`:

```
sudo nano /etc/exim4/conf.d/main/02_exim4-config_acl_pre_options
```

- Добавьте в файл строку:
`acl_smtp_connect = acl_check_host`
- Если вы планируете использовать проверку адресов получателей, включите отправку положительного ответа 250 на команду проверки адреса, добавив в файл строку:
`acl_smtp_vrfy=accept`
- Если необходимо изменить максимальный размер письма, добавьте строку:
`MESSAGE_SIZE_LIMIT = "<Размер в МБ>М"`
- Сохраните изменения и закройте файл.

5. Настройте получение проверенной почты и уведомлений от PT Email Security:

- Откройте файл `update-exim4.conf.conf`:
`sudo nano /etc/exim4/update-exim4.conf.conf`
- Добавьте в файл строку, указав IP-адрес и порт Exim для проверенных писем:
`dc_local_interfaces='0.0.0.0 ; <IP-адрес Exim>.<Порт Exim>'`
- Разрешите пересылку уведомлений PT Email Security через Exim, добавив в файл строку с IP-адресом SMTP-сервера PT Email Security:
`dc_relay_nets='<IP-адрес PT Email Security>'`
- Сохраните изменения и закройте файл.

6. Сгенерируйте конфигурационный файл Exim:

```
sudo update-exim4.conf
```

7. Перезапустите службу Exim:

```
sudo service exim4 restart
```

Маршрутизация писем через PT Email Security настроена.

13.10. Exim 4 в режиме зеркалирования

При подключении источника скрытые копии писем с сервера Exim отправляются на проверку в PT Email Security. Проверка не влияет на доставку писем получателям.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 25 от почтового сервера к основному узлу PT Email Security.

Для подключения источника к PT Email Security необходимо:

- Добавить в PT Email Security источник с типом **Почтовый сервер в режиме зеркалирования**.
- На сервере Exim настроить отправку скрытых копий писем в PT Email Security.
- Если при обработке писем необходимо использовать адреса электронной почты конечных получателей, настроить на сервере Exim заполнение заголовков писем X-Original-Rcpt-To.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Почтовый сервер в режиме зеркалирования**.
5. Если необходимо, в поле **IP-адреса SMTP-сервера** введите дополнительные адреса.

Примечание. В поле указан IP-адрес SMTP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.

6. Если необходимо, измените стандартный порт подключения к серверу.

Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.

7. Если при подключении используется протокол SSL, установите флажок **Подключаться по SSL**.

Примечание. При снятом флажке передаваемые данные зашифровываются при помощи расширения STARTTLS. Если почтовый сервер организации не поддерживает STARTTLS, данные передаются без шифрования.

8. Если необходимо принимать письма только с определенных IP-адресов:
 - В блоке параметров **Фильтровать входящие подключения** включите фильтрацию.
 - В появившемся поле введите IP-адреса разрешенных узлов или подсетей.
9. Если необходимо, включите использование при электронных адресах конечных получателей.
10. Нажмите кнопку **Добавить источник**.

Настройка источника

На источнике необходимо настроить отправку скрытых копий писем на сервер, созданный при добавлении источника в PT Email Security.

Инструкция разработана для Exim версии 4 с отдельными файлами конфигурации. Если вы используете единый конфигурационный файл, указанные в инструкции строки необходимо добавлять в этот файл. Дополнительную информацию вы можете получить на сайте exim.org.

► Чтобы настроить отправку скрытых копий писем:

1. Создайте файл `03_exim4-config_redirect`:

```
sudo nano /etc/exim4/conf.d/router/03_exim4-config_redirect
```

2. Добавьте в файл строки:

```
bcc:
    driver = redirect
    data = bcc@sandbox.local
    unseen
```

3. Сохраните изменения и закройте файл.

4. Создайте файл `03_exim4-config_send`:

```
sudo nano /etc/exim4/conf.d/router/03_exim4-config_send
```

5. Добавьте в файл строки, указав IP-адрес и порт PT Email Security для отправки скрытых копий писем:

```
cmdfilter:
    driver = manualroute
    domains = sandbox.local
    transport = remote_smtp
    route_list = "* <IP-адрес>:<Порт>"
    self = send
```

6. Сохраните изменения и закройте файл.

7. Перезапустите службу Exim:

```
sudo service exim4 restart
```

Отправка скрытых копий писем настроена.

13.11. Microsoft Exchange 2010—2019 с установленным почтовым агентом

При подключении источника почтовый агент перехватывает все письма, проходящие через сервер Microsoft Exchange, и отправляет их на проверку в PT Email Security, после чего возвращает их обратно для дальнейшей доставки адресатам. В случае потери связи между почтовым агентом и PT Email Security письма доставляются без проверки.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 7536 от основного узла PT Email Security к узлу источника.

Для подключения источника к PT Email Security необходимо:

- На сервере Microsoft Exchange установить почтовый агент.
- Добавить в PT Email Security источник с типом **Сервер Microsoft Exchange с установленным агентом**.

В этом разделе

[Установка почтового агента \(см. раздел 13.11.1\)](#)

[Добавление источника в PT Email Security \(см. раздел 13.11.2\)](#)

13.11.1. Установка почтового агента

В схеме обработки писем Microsoft Exchange почтовый агент встраивается на уровне транспортного сервиса в качестве Routing Agent. Используя штатные средства Microsoft Exchange, вы можете отслеживать длину очереди из писем на почтовом агенте.

Инструкции по установке и удалению почтового агента необходимо выполнять от имени учетной записи, которая обладает правами локального администратора операционной системы и в Microsoft Exchange входит в группу ролей Organization Management.

Для получения архива с установщиком почтового агента вам необходимо обратиться в техническую поддержку Positive Technologies.

Аппаратные требования

Для установки почтового агента на узле Microsoft Exchange должны быть выделены дополнительные аппаратные ресурсы сверх минимальных требований операционной системы и Microsoft Exchange.

Таблица 5. Дополнительные аппаратные требования к узлу Microsoft Exchange

Компонент	Требование
Центральный процессор 2,2 ГГц, количество потоков	1
Память ОЗУ, ГБ	1
HDD или SSD, ГБ	2

Программные требования

Установка почтового агента возможна на узлах с операционной системой Windows Server версии 2012 или выше.

Почтовый агент поддерживает работу со следующими версиями Microsoft Exchange:

- Microsoft Exchange 2010 версии 14;
- Microsoft Exchange 2013 версии 15.0 (кроме 15.0.847.32);

- Microsoft Exchange 2016 версии 15.1;
- Microsoft Exchange 2019 версии 15.2.

На сервере Microsoft Exchange должна быть установлена роль Mailbox.

Установка почтового агента

► Чтобы установить почтовый агент:

1. На узле с Microsoft Exchange создайте папку для установки почтового агента.

Примечание. В этой же папке будут сохраняться файлы журналов почтового агента.

2. Скопируйте архив с установщиком почтового агента в созданную папку и распакуйте его.
3. Откройте интерфейс командной строки Windows от имени администратора.
4. Перейдите в папку с распакованным архивом.
5. Запустите установку почтового агента, выполнив одну из команд:

- Если используется стандартный сетевой интерфейс и порт 7536:

```
install.cmd
```

- Если для стандартного сетевого интерфейса необходимо указать порт:

```
install.cmd -BalancerEntryPointEndpoint "0.0.0.0:<Порт>"
```

- Если требуется указать сетевой интерфейс и порт:

```
install.cmd -BalancerEntryPointEndpoint "<IP-адрес>:<Порт>"
```

В процессе установки будет перезапущена служба MS Exchange Transport.

Почтовый агент установлен в папку, из которой была запущена установка.

Удаление почтового агента

► Чтобы удалить почтовый агент:

1. Откройте интерфейс командной строки Windows от имени администратора.
2. Перейдите в папку с почтовым агентом.
3. Запустите удаление почтового агента, выполнив команду:

```
install.cmd -Uninstall
```

В процессе удаления будет перезапущена служба MS Exchange Transport.

13.11.2. Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Сервер Microsoft Exchange с установленным агентом**.
5. В поле **Доменное имя или IP-адрес сервера** введите адрес сервера Microsoft Exchange.
6. Если необходимо, измените стандартный порт подключения к серверу.
7. Нажмите кнопку **Добавить источник**.

13.12. Microsoft Exchange 2010—2019 в режиме зеркалирования

При подключении источника скрытые копии писем с сервера Microsoft Exchange отправляются на проверку в PT Email Security. Проверка не влияет на доставку писем получателям.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 25 от почтового сервера к основному узлу PT Email Security.

Для подключения источника к PT Email Security необходимо:

- Добавить в PT Email Security источник с типом **Почтовый сервер в режиме зеркалирования**.
- На сервере Microsoft Exchange настроить отправку скрытых копий писем в PT Email Security.
- Если при обработке писем необходимо использовать адреса электронной почты конечных получателей, настроить на сервере Microsoft Exchange заполнение заголовков писем X-Original-Rcpt-To.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Почтовый сервер в режиме зеркалирования**.
5. Если необходимо, в поле **IP-адреса SMTP-сервера** введите дополнительные адреса.

Примечание. В поле указан IP-адрес SMTP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.

6. Если необходимо, измените стандартный порт подключения к серверу.

Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.

7. Если при подключении используется протокол SSL, установите флажок **Подключаться по SSL**.

Примечание. При снятом флажке передаваемые данные зашифровываются при помощи расширения STARTTLS. Если почтовый сервер организации не поддерживает STARTTLS, данные передаются без шифрования.

8. Если необходимо принимать письма только с определенных IP-адресов:
 - В блоке параметров **Фильтровать входящие подключения** включите фильтрацию.
 - В появившемся поле введите IP-адреса разрешенных узлов или подсетей.
9. Если необходимо, включите использование при электронных адресах конечных получателей.
10. Нажмите кнопку **Добавить источник**.

Настройка источника

На источнике необходимо настроить отправку скрытых копий писем на сервер, созданный при добавлении источника в PT Email Security.

Инструкция разработана для сервера Microsoft Exchange версии 2010 и выше. Инструкцию необходимо выполнять от имени учетной записи, которой в центре администрирования Exchange была назначена роль «Управление организацией». Подробную информацию вы можете получить на сайте technet.microsoft.com.

► Чтобы настроить отправку скрытых копий писем в PT Email Security:

1. Запустите центр администрирования Exchange.
2. В главном меню выберите раздел **поток обработки почты**.
Откроется страница **правила**.
3. Нажмите **+** и в раскрывшемся меню выберите **Создать новое правило**.
Откроется окно **новое правило**.
4. В поле **Имя** введите произвольное название правила, например PT Email Security.
5. В раскрывающемся списке **Применить это правило** выберите **Применить ко всем сообщениям**.
6. В раскрывающемся списке **Выполнить следующие действия** выберите **Отправить скрытую копию сообщения (СК)**.
Откроется окно **Выбрать членов**.
7. В поле **добавить** введите `bcc@sandbox.local`.
8. Нажмите кнопку **ОК**, затем кнопку **Сохранить**.
9. В панели инструментов нажмите **соединители отправки**.
Откроется страница **соединители**.
10. Нажмите **+**, чтобы добавить соединитель отправки.
Откроется мастер **новый соединитель отправки**.
11. Нажмите кнопку **далее**, оставив значения остальных параметров без изменений.
Откроется следующий шаг мастера.
12. Выберите вариант **Перенаправлять почту через промежуточные узлы**.
13. Нажмите **+**, чтобы добавить промежуточный узел.
Откроется страница **изменить промежуточный узел**.
14. В поле введите IP-адрес bcc-сервера PT Email Security. Если номер TCP-порта для SMTP отличается от стандартного (25), укажите его через двоеточие после IP-адреса.
15. Нажмите кнопку **Сохранить**.
Промежуточный узел будет создан. Откроется следующий шаг мастера.
16. Нажмите **+**, чтобы добавить адресное пространство.

Откроется страница **добавление домена**.

17. В поле **Полное доменное имя (FQDN)** введите `sandbox.local`.

18. Нажмите кнопку **Сохранить**, затем кнопку **Далее**, затем кнопку **Готово**.

Информация о новом соединителе отправки появится в таблице **соединители**.

Отправка скрытых копий писем настроена.

13.13. Postfix 3.2 в режиме фильтрации

При подключении источника письма с сервера Postfix отправляются на проверку в PT Email Security, после чего возвращаются обратно для дальнейшей доставки.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 25 от почтового сервера к основному узлу PT Email Security.

Для подключения источника к PT Email Security необходимо:

1. Добавить в PT Email Security источник с типом **Почтовый сервер в режиме фильтрации** или **Почтовый сервер в режиме фильтрации (MTA)**.
2. Настроить в PT Email Security отправку проверенных писем:
 - Если используется несколько почтовых серверов, добавить правила маршрутизации.
 - Если используются непубличные почтовые серверы и требуется TLS-шифрование с проверкой сертификата, добавить корневой сертификат центра сертификации вашей организации.
 - Если на почтовых серверах поддерживается проверка адресов получателей, включить такую проверку для добавленного источника.
3. На сервере Postfix настроить маршрутизацию писем через PT Email Security.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите:
 - Если для работы с письмами от источника необходимо использовать встроенный в PT Email Security почтовый транспортный агент, выберите **Почтовый сервер в режиме фильтрации (MTA)**.
 - Если в этом нет необходимости, выберите **Почтовый сервер в режиме фильтрации**.
5. Если вы выбрали тип **Почтовый сервер в режиме фильтрации (MTA)**, в блоке параметров **Режим обработки писем** выберите режим:
 - Если хранение и доставку проверенных писем должен контролировать PT Email Security, выберите **Асинхронный**.
 - Если это должен делать почтовый сервер, выберите **Синхронный**.
6. В блоке **Параметры подключения** настройте параметры SMTP-сервера, создаваемого в PT Email Security для приема писем:
 - Если необходимо, в поле **IP-адреса SMTP-сервера** введите дополнительные адреса.
Примечание. В поле указан IP-адрес SMTP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.
 - Если необходимо, измените стандартный порт подключения к серверу.
Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.
 - Если при подключении используется протокол SSL, установите флажок **Подключаться по SSL**.
Примечание. При снятом флажке передаваемые данные зашифровываются при помощи расширения STARTTLS. Если почтовый сервер организации не поддерживает STARTTLS, данные передаются без шифрования.
7. Если необходимо принимать письма только с определенных IP-адресов:
 - В блоке параметров **Фильтровать входящие подключения** включите фильтрацию.
 - В появившемся поле введите IP-адреса разрешенных узлов или подсетей.
8. Выберите для всех правил маршрутизации, какой набор доверенных сертификатов будет использоваться при проверке сертификатов серверов для проверенной почты:
 - Если только доверенные сертификаты из внутреннего хранилища PT Email Security, в раскрывающемся списке **Доверенные сертификаты TLS-шифрования** выберите **Пользовательские**.
 - Если сертификаты из внутреннего хранилища и глобальные сертификаты, доступные внутри Docker-контейнеров PT Email Security, выберите **Глобальные и пользовательские**.
9. Добавьте правило маршрутизации по умолчанию и укажите в нем параметры сервера для отправки писем и уведомлений о результатах проверки:

- Нажмите кнопку **Добавить**.
- В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
- Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.
- В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
- Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
- Если в вашей организации используется несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.
- Нажмите кнопку **Добавить**.

10. Если необходимо пересылать скрытые копии проверенных писем дополнительным получателям:

- В блоке параметров **Пересылать письма дополнительным получателям** включите пересылку писем.
- В появившемся поле введите электронные адреса получателей.

11. Нажмите кнопку **Добавить источник**.

Добавление правила маршрутизации проверенных писем в PT Email Security

Если необходимо использовать различные почтовые серверы в зависимости от домена в адресе электронной почты получателя, вы можете настроить в PT Email Security [правила маршрутизации проверенных писем](#) (см. раздел 12.5).

► Чтобы добавить правило маршрутизации:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры источника**.
3. В блоке параметров **Правила маршрутизации почтового трафика** нажмите кнопку **Добавить**.
4. В поле **Домен электронной почты получателя** введите доменную часть адреса электронной почты получателей, для которых необходимо настроить правило.

С помощью звездочки вы можете задать маску для доменной части адреса получателей писем, если доменная часть содержит поддомены третьего уровня или выше. Например, правило с маской *.example.com будет применяться и для адресов с доменной частью example.com, sub_1.example.com, sub_2.example.com, и для адресов с доменной частью, содержащей поддомены более высоких уровней.

Примечание. Если доменная часть адреса получателя соответствует нескольким правилам маршрутизации, будет использовано то правило, в котором указан наиболее точный адрес. При этом более высокий приоритет имеют правила, в которых не используются маски.

5. В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
6. Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.
7. Если необходимо перенаправлять письма согласно MX-записям, выберите способ маршрутизации **По MX-записям**.

Внимание! Письмо не будет отправлено, если в DNS отсутствует подходящая MX- или A-запись для указанного домена.

8. Если необходимо перенаправлять письма на определенный почтовый сервер, выберите способ маршрутизации **По адресам почтовых серверов** и укажите параметры сервера:

- В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
- Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.

- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
- Если в вашей организации используется несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.

9. Нажмите кнопку **Добавить**.

10. Нажмите кнопку **Сохранить**.

Правило маршрутизации добавлено.

Добавление доверенных сертификатов в PT Email Security

Если при отправке проверенных писем вы планируете использовать TLS-шифрование с проверкой сертификата, при проверке сертификатов почтовых серверов будут использоваться следующие сертификаты:

- Для публичных SMTP-серверов — сертификаты доверенных центров сертификации, доступные внутри Docker-контейнеров PT Email Security.
- Для непубличных SMTP-серверов вашей организации — доверенные сертификаты центров сертификации вашей организации. Корневые сертификаты этих центров необходимо добавить в PT Email Security.

Инструкции необходимо выполнять на основном узле PT Email Security. Поддерживаются только сертификаты формата PEM.

- Чтобы добавить сертификат в PT Email Security,

выполните команду:

```
sudo ptmsctl system trusted-certs add --name <Название сертификата> --path <Полный путь к файлу сертификата>
```

Например:

```
sudo ptmsctl system trusted-certs add --name example_cert --path /etc/tls/certs/rootCA.crt
```

- Чтобы просмотреть список добавленных в PT Email Security сертификатов,

выполните команду:

```
sudo ptmsctl system trusted-certs list
```

Примечание. Вы можете просмотреть информацию об отдельном сертификате, выполнив команду `sudo ptmsctl system trusted-certs view --name <Название сертификата>`.

- ▶ Чтобы удалить сертификат из PT Email Security,

выполните команду:

```
sudo ptmsctl system trusted-certs delete --name <Название сертификата>
```

Например:

```
sudo ptmsctl system trusted-certs delete --name example_cert
```

Включение проверки адресов получателей

Перед отправкой проверенных писем PT Email Security может проверять адреса получателей на принимающих почтовых серверах с помощью SMTP-команды VRFY (согласно спецификации RFC 5321). По умолчанию эта проверка отключена, поскольку на некоторых почтовых серверах выполнение этой команды может быть заблокировано по соображениям безопасности. Вы можете включить для источника проверку адресов получателей, если для него добавлено хотя бы одно правило маршрутизации или указано более одного почтового сервера. Инструкцию необходимо выполнить на основном узле PT Email Security.

- ▶ Чтобы включить проверку адресов получателей для источника,

выполните команду:

```
sudo ptmsctl system components config patch --component <Название источника> --toml "[smtp_client_config.verify_recipients]
enabled = true
"
```

Настройка источника

На сервере Postfix необходимо настроить маршрутизацию писем через PT Email Security.

- ▶ Чтобы настроить маршрутизацию писем через PT Email Security:

1. Откройте файл `/etc/postfix/main.cf`:

```
sudo nano /etc/postfix/main.cf
```
2. Добавьте в файл строки, указав IP-адрес и порт SMTP-сервера PT Email Security:

```
content_filter=scan:[<IP-адрес PT Email Security>]:<Порт PT Email Security>
receive_override_options=no_address_mappings
```
3. Сохраните изменения и закройте файл.
4. Откройте файл `/etc/postfix/master.cf`:

```
sudo nano /etc/postfix/master.cf
```
5. Добавьте в файл строки, указав IP-адрес и порт сервера Postfix для проверенных писем и IP-адрес SMTP-сервера PT Email Security:

```
scan unix - - n - 10 smtp
-o disable_dns_lookups=yes
-o smtp_data_done_timeout=1200
-o disable_mime_output_conversion=yes
-o max_use=8
```

```
<IP-адрес Postfix>:<Порт Postfix> inet n - n - 10 smtpd
-o mynetworks=<IP-адрес PT Email Security>
-o smtpd_client_restrictions=permit_mynetworks,reject
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o content_filter=
-o receive_override_options=no_unknown_recipient_checks,no_header_body_checks,no_milters
```

Примечание. Для проверки адресов получателей должна быть включена отправка положительного ответа 250 на команду проверки адреса, для параметра `disable_vrfy_command` должно быть указано значение `no`.

6. Сохраните изменения и закройте файл.

7. Перезапустите службу сервера Postfix:

```
service postfix restart
```

Маршрутизация писем через PT Email Security настроена.

13.14. Postfix 3.2 в режиме зеркалирования

При подключении источника скрытые копии писем с сервера Postfix отправляются на проверку в PT Email Security. Проверка не влияет на доставку писем получателям.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 25 от почтового сервера к основному узлу PT Email Security.

Для подключения источника к PT Email Security необходимо:

- Добавить в PT Email Security источник с типом **Почтовый сервер в режиме зеркалирования**.
- На сервере Postfix настроить отправку скрытых копий писем в PT Email Security.
- Если при обработке писем необходимо использовать адреса электронной почты конечных получателей, настроить на сервере Postfix заполнение заголовков писем `X-Original-Rcpt-To`.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Почтовый сервер в режиме зеркалирования**.
5. Если необходимо, в поле **IP-адреса SMTP-сервера** введите дополнительные адреса.
Примечание. В поле указан IP-адрес SMTP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.
6. Если необходимо, измените стандартный порт подключения к серверу.
Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.
7. Если при подключении используется протокол SSL, установите флажок **Подключаться по SSL**.
Примечание. При снятом флажке передаваемые данные зашифровываются при помощи расширения STARTTLS. Если почтовый сервер организации не поддерживает STARTTLS, данные передаются без шифрования.
8. Если необходимо принимать письма только с определенных IP-адресов:
 - В блоке параметров **Фильтровать входящие подключения** включите фильтрацию.
 - В появившемся поле введите IP-адреса разрешенных узлов или подсетей.
9. Если необходимо, включите использование при электронных адресах конечных получателей.
10. Нажмите кнопку **Добавить источник**.

Настройка источника

На сервере Postfix необходимо настроить отправку скрытых копий писем на сервер, созданный при добавлении источника в PT Email Security.

► Чтобы настроить отправку скрытых копий писем:

1. Создайте карту `transport` с описанием транспорта для отправки скрытых копий писем в PT Email Security:
 - Создайте файл `/etc/postfix/maps/transport`.
 - Добавьте в файл строку и укажите в ней IP-адрес и порт PT Email Security:
`bcc@sandbox.local smtp-bcc:[<IP-адрес>]:<Порт>`
 - Сохраните изменения и закройте файл.
2. Добавьте карту `transport` в конфигурацию сервера:

- Откройте файл `/etc/postfix/main.cf`.
 - Добавьте в файл строки:


```
always_bcc = bcc@sandbox.local
transport_maps = hash:/etc/postfix/maps/transport
```
 - Сохраните изменения и закройте файл.
3. Обновите файл соответствий:


```
sudo postmap /etc/postfix/maps/transport
```
 4. Добавьте транспорт `smtp-bcc` в конфигурацию сервера:
 - Откройте файл `/etc/postfix/master.cf`.
 - Добавьте в файл строку:


```
smtp-bcc unix - - y - - smtp
```
 - Сохраните изменения и закройте файл.
 5. Перезапустите службу сервера Postfix:


```
sudo systemctl restart postfix
```
- Отправка скрытых копий писем настроена.

Настройка заполнения заголовка X-Original-Rcpt-To

Если при обработке писем в PT Email Security планируется использовать электронные адреса конечных получателей, на сервере Postfix необходимо настроить заполнение заголовков писем X-Original-Rcpt-To.

- Чтобы настроить заполнение в письмах заголовка X-Original-Rcpt-To:
1. Создайте карту `detect_recipients` для добавления заголовка X-Original-Rcpt-To во все письма:
 - Создайте файл `/etc/postfix/maps/detect_recipients`.
 - Добавьте в файл строку:


```
/^(.+)$/ PREPEND X-Original-Rcpt-To: $1
```
 - Сохраните изменения и закройте файл.
 2. Добавьте карту `detect_recipients` в параметры обработки команды RCPT TO:
 - Откройте файл `/etc/postfix/main.cf`.
 - Добавьте в файл строку для параметра `smtpd_recipient_restrictions`:


```
smtpd_recipient_restrictions =
...
  check_recipient_access regexp:/etc/postfix/maps/detect_recipients
```
 - Сохраните изменения и закройте файл.
 3. Создайте карту `header_checks` для удаления заголовка X-Original-Rcpt-To из писем конечным получателям:

- Создайте файл `/etc/postfix/maps/header_checks`.
 - Добавьте в файл строку:
`/^X-Original-Rcpt-To:/ IGNORE`
 - Сохраните изменения и закройте файл.
4. Укажите карту `header_checks` в параметрах обработки заголовков писем для используемых транспортов:
- Откройте файл `/etc/postfix/master.cf`.
 - Если используется транспорт `smtp` (для пересылки писем на другие серверы), добавьте в файл строку для этого транспорта:

```
smtp unix - - y - - smtp
      -o smtp_header_checks=regex:/etc/postfix/maps/header_checks
```
 - Если используется транспорт `lmtp` (для локальной доставки писем), добавьте в файл строку для этого транспорта:

```
lmtp unix - - y - - lmtp
      -o lmtp_header_checks=regex:/etc/postfix/maps/header_checks
```
 - Сохраните изменения и закройте файл.
5. Перезапустите службу сервера Postfix:
- ```
sudo systemctl restart postfix
```
- Заполнение заголовка `X-Original-Rcpt-To` настроено.

## 13.15. PT Threat Analyzer 2.10 и выше

При подключении источника копии объектов из PT Threat Analyzer отправляются на проверку в PT Email Security через публичный API.

**Внимание!** Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 443 от узла источника к основному узлу PT Email Security.

Для подключения источника в PT Email Security необходимо:

- Выпустить токен доступа к публичному API с разрешенным действием **Проверка с параметрами источника**.
- Добавить в PT Email Security источник с типом **API с выбранными параметрами проверки**.

Для подключения источника в PT Threat Analyzer необходимо настроить отправку объектов в PT Email Security.

## Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.  
  
Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.
4. В раскрывающемся списке **Тип** выберите **API с выбранными параметрами проверки**.
5. В раскрывающемся списке **Токен доступа** выберите токен доступа к публичному API.
6. Нажмите кнопку **Добавить источник**.

## Настройка источника

На узле PT Threat Analyzer необходимо настроить отправку объектов на проверку в PT Email Security через публичный API.

► Чтобы настроить отправку объектов в PT Email Security:

1. Откройте конфигурационный файл `threat-analyzer-installer-<Версия>/group_vars/all/configuration.yml`.
2. В параметре `cybsi_pt_sb_host` укажите IP-адрес (доменное имя) основного узла PT Email Security.
3. В параметре `cybsi_pt_sb_api_key` укажите токен доступа к публичному API PT Email Security.
4. Сохраните изменения и закройте файл.

Отправка объектов в PT Email Security настроена.

## 13.16. RuPost 3.2, 4.1 в режиме фильтрации

При подключении источника письма с сервера RuPost отправляются на проверку в PT Email Security, после чего возвращаются обратно для дальнейшей доставки.

**Внимание!** Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, необходимо настроить в них правила, разрешающие передачу трафика от сервера RuPost к основному узлу PT Email Security на порт, указанный при добавлении источника.

Для подключения источника к PT Email Security необходимо:

1. Добавить в PT Email Security источник с типом **Почтовый сервер в режиме фильтрации** или **Почтовый сервер в режиме фильтрации (MTA)**.
2. Настроить в PT Email Security отправку проверенных писем:
  - Если используется несколько почтовых серверов, добавить правила маршрутизации.
  - Если используются непубличные почтовые серверы и требуется TLS-шифрование с проверкой сертификата, добавить корневой сертификат центра сертификации вашей организации.
  - Если на почтовых серверах поддерживается проверка адресов получателей, включить такую проверку для добавленного источника.
3. На сервере RuPost настроить маршрутизацию писем через PT Email Security.

## В этом разделе

[Добавление источника в PT Email Security \(см. раздел 13.16.1\)](#)

[Добавление правил маршрутизации проверенных писем \(см. раздел 13.16.2\)](#)

[Добавление доверенных сертификатов \(см. раздел 13.16.3\)](#)

[Включение проверки адресов получателей \(см. раздел 13.16.4\)](#)

[Настройка источника \(см. раздел 13.16.5\)](#)

## 13.16.1. Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.  
  
 Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.
4. В раскрывающемся списке **Тип** выберите:
  - Если для работы с письмами от источника необходимо использовать встроенный в PT Email Security почтовый транспортный агент, выберите **Почтовый сервер в режиме фильтрации (MTA)**.
  - Если в этом нет необходимости, выберите **Почтовый сервер в режиме фильтрации**.

5. Если вы выбрали тип **Почтовый сервер в режиме фильтрации (MTA)**, в блоке параметров **Режим обработки писем** выберите режим:
  - Если хранение и доставку проверенных писем должен контролировать PT Email Security, выберите **Асинхронный**.
  - Если это должен делать почтовый сервер, выберите **Синхронный**.
6. В блоке **Параметры подключения** настройте параметры SMTP-сервера, создаваемого в PT Email Security для приема писем:
  - Если необходимо, в поле **IP-адреса SMTP-сервера** введите дополнительные адреса.  
**Примечание.** В поле указан IP-адрес SMTP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.
  - Если необходимо, измените стандартный порт подключения к серверу.  
**Внимание!** Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.
7. Если необходимо принимать письма только с определенных IP-адресов:
  - В блоке параметров **Фильтровать входящие подключения** включите фильтрацию.
  - В появившемся поле введите IP-адреса разрешенных узлов или подсетей.
8. Выберите для всех правил маршрутизации, какой набор доверенных сертификатов будет использоваться при проверке сертификатов серверов для проверенной почты:
  - Если только доверенные сертификаты из внутреннего хранилища PT Email Security, в раскрывающемся списке **Доверенные сертификаты TLS-шифрования** выберите **Пользовательские**.
  - Если сертификаты из внутреннего хранилища и глобальные сертификаты, доступные внутри Docker-контейнеров PT Email Security, выберите **Глобальные и пользовательские**.
9. Добавьте правило маршрутизации по умолчанию и укажите в нем параметры сервера для отправки писем и уведомлений о результатах проверки:
  - Нажмите кнопку **Добавить**.
  - В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
  - Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.
  - В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
  - Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

**Примечание.** Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

**Примечание.** При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
  - Если в вашей организации используется несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.
  - Нажмите кнопку **Добавить**.
10. Если необходимо пересылать скрытые копии проверенных писем дополнительным получателям:
- В блоке параметров **Пересылать письма дополнительным получателям** включите пересылку писем.
  - В появившемся поле введите электронные адреса получателей.
11. Нажмите кнопку **Добавить источник**.

## 13.16.2. Добавление правил маршрутизации проверенных писем

Если необходимо использовать различные почтовые серверы в зависимости от домена в адресе электронной почты получателя, вы можете настроить в PT Email Security [правила маршрутизации проверенных писем](#) (см. раздел 12.5).

► Чтобы добавить правило маршрутизации:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры источника**.
3. В блоке параметров **Правила маршрутизации почтового трафика** нажмите кнопку **Добавить**.
4. В поле **Домен электронной почты получателя** введите доменную часть адреса электронной почты получателей, для которых необходимо настроить правило.

С помощью звездочки вы можете задать маску для доменной части адреса получателей писем, если доменная часть содержит поддомены третьего уровня или выше. Например, правило с маской \*.example.com будет применяться и для адресов с доменной частью example.com, sub\_1.example.com, sub\_2.example.com, и для адресов с доменной частью, содержащей поддомены более высоких уровней.

**Примечание.** Если доменная часть адреса получателя соответствует нескольким правилам маршрутизации, будет использовано то правило, в котором указан наиболее точный адрес. При этом более высокий приоритет имеют правила, в которых не используются маски.

5. В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
6. Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.
7. Если необходимо перенаправлять письма согласно MX-записям, выберите способ маршрутизации **По MX-записям**.

**Внимание!** Письмо не будет отправлено, если в DNS отсутствует подходящая MX- или A-запись для указанного домена.

8. Если необходимо перенаправлять письма на определенный почтовый сервер, выберите способ маршрутизации **По адресам почтовых серверов** и укажите параметры сервера:
  - В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
  - Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

**Примечание.** Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

**Примечание.** При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
- Если в вашей организации используется несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.

9. Нажмите кнопку **Добавить**.

10. Нажмите кнопку **Сохранить**.

Правило маршрутизации добавлено.

### 13.16.3. Добавление доверенных сертификатов

Если при отправке проверенных писем вы планируете использовать TLS-шифрование с проверкой сертификата, при проверке сертификатов почтовых серверов будут использоваться следующие сертификаты:

- Для публичных SMTP-серверов — сертификаты доверенных центров сертификации, доступные внутри Docker-контейнеров PT Email Security.
- Для непубличных SMTP-серверов вашей организации — доверенные сертификаты центров сертификации вашей организации. Корневые сертификаты этих центров необходимо добавить в PT Email Security.

Инструкции необходимо выполнять на основном узле PT Email Security. Поддерживаются только сертификаты формата PEM.

- ▶ Чтобы добавить сертификат в PT Email Security,

выполните команду:

```
sudo ptmsctl system trusted-certs add --name <Название сертификата> --path <Полный путь к файлу сертификата>
```

Например:

```
sudo ptmsctl system trusted-certs add --name example_cert --path /etc/tls/certs/rootCA.crt
```

- ▶ Чтобы просмотреть список добавленных в PT Email Security сертификатов,

выполните команду:

```
sudo ptmsctl system trusted-certs list
```

**Примечание.** Вы можете просмотреть информацию об отдельном сертификате, выполнив команду `sudo ptmsctl system trusted-certs view --name <Название сертификата>`.

- ▶ Чтобы удалить сертификат из PT Email Security,

выполните команду:

```
sudo ptmsctl system trusted-certs delete --name <Название сертификата>
```

Например:

```
sudo ptmsctl system trusted-certs delete --name example_cert
```

## 13.16.4. Включение проверки адресов получателей

Перед отправкой проверенных писем PT Email Security может проверять адреса получателей на принимающих почтовых серверах с помощью SMTP-команды **VRFY** (согласно спецификации RFC 5321). По умолчанию эта проверка отключена, поскольку на некоторых почтовых серверах выполнение этой команды может быть заблокировано по соображениям безопасности. Вы можете включить для источника проверку адресов получателей, если для него добавлено хотя бы одно правило маршрутизации или указано более одного почтового сервера. Инструкцию необходимо выполнить на основном узле PT Email Security.

- ▶ Чтобы включить проверку адресов получателей для источника,

выполните команду:

```
sudo ptmsctl system components config patch --component <Название источника> --toml "[smtp_client_config.verify_recipients]
enabled = true
"
```

## 13.16.5. Настройка источника

На сервере RuPost необходимо настроить маршрутизацию писем через PT Email Security. Инструкцию необходимо выполнять от имени учетной записи администратора RuPost.

- ▶ Чтобы настроить маршрутизацию писем через PT Email Security:

1. Откройте веб-интерфейс панели управления RuPost.
2. Введите учетные данные и нажмите кнопку **Войти**.
3. В главном меню выберите **Настройки** → **Конфигурации**.
4. Выберите вкладку **Создание конфигурации**.
5. Нажмите кнопку **Выбрать шаблон из библиотеки**.
6. Выберите шаблон **Интеграция RuPost с сервером PT Sandbox** и нажмите кнопку **Выбрать**.
7. Нажмите кнопку **Далее**.
8. В блоке параметров **Сервер PT SandBox** введите IP-адрес и порт SMTP-сервера PT Email Security, созданного при добавлении источника.
9. Если требуется проверять адреса получателей, в блоке параметров **Параметры SMTP-команды VRFY** введите **yes**.
10. Нажмите кнопку **Далее**.
11. В поле **Название конфигурации** введите название.
12. Нажмите кнопку **Применить конфигурацию**.

## 13.17. Squid 3 и выше

При подключении источника объекты с прокси-сервера Squid отправляются на проверку в PT Email Security по протоколу ICAP. В зависимости от приобретенной вами лицензии и выбранных параметров работы ICAP-сервера PT Email Security проверка может выполняться в режиме ожидания, в пассивном или блокирующем режиме.

**Внимание!** Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 1344 от узла источника к основному узлу PT Email Security.

Для подключения источника к PT Email Security необходимо:

- Добавить в PT Email Security источник с типом **ICAP-сервер**.
- На прокси-сервере Squid настроить ICAP-клиент для работы с ICAP-сервером PT Email Security.

### Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.  
  
Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.
4. В раскрывающемся списке **Тип** выберите **ICAP-сервер**.
5. Если необходимо, в поле **IP-адреса ICAP-сервера** введите дополнительные адреса.  
**Примечание.** В поле указан IP-адрес ICAP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.
6. Если необходимо, измените стандартный порт подключения к ICAP-серверу.  
**Внимание!** Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.
7. Если необходимо принимать объекты только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
8. Нажмите кнопку **Добавить источник**.

## Настройка источника

На узле прокси-сервера Squid необходимо настроить ICAP-клиент для работы с ICAP-сервером, созданным при добавлении источника в PT Email Security.

**Внимание!** Инструкция не содержит описания настройки аутентификации пользователей. Более подробную информацию о настройке Squid вы можете получить на сайте [squid-cache.org](http://squid-cache.org).

При настройке ICAP-клиента вам необходимо указать ссылку для обращения к ICAP-серверу PT Email Security. Вид ссылки зависит от режима проверки объектов и режима работы ICAP-сервера:

— Ссылки для проверки объектов в блокирующем режиме:

- REQMOD: `icap://<IP-адрес>:<Порт>/scanrequest?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=<Тайм-аут>`
- RESPMOD: `icap://<IP-адрес>:<Порт>/scanresponse?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=<Тайм-аут>`

**Примечание.** В параметре `block-unwanted` вы можете указать `y`, если необходимо блокировать потенциально опасные файлы, или `n` — если блокировать такие файлы не требуется (по умолчанию потенциально опасные файлы не блокируются). В параметре `timeout` вы можете указать тайм-аут ответа ICAP-сервера в секундах (по умолчанию 30 секунд).

— Ссылки для проверки объектов в режиме ожидания:

- REQMOD: `icap://<IP-адрес>:<Порт>/scanrequest?modify=no&timeout=<Тайм-аут>`
- RESPMOD: `icap://<IP-адрес>:<Порт>/scanresponse?modify=no&timeout=<Тайм-аут>`

— Ссылки для проверки объектов в пассивном режиме:

- REQMOD: `icap://<IP-адрес>:<Порт>/bypass`
- RESPMOD: `icap://<IP-адрес>:<Порт>/bypass`

► Чтобы настроить ICAP-клиент:

1. Создайте резервную копию конфигурационного файла `/etc/squid3/squid.conf`.

**Примечание.** Конфигурационный файл Squid также может располагаться в каталоге `/etc/squid/squid.conf` или `/usr/local/squid/etc/squid.conf`.

2. Откройте файл `/etc/squid3/squid.conf`:

```
sudo nano /etc/squid3/squid.conf
```

3. Добавьте в файл строку для включения модуля ICAP:

```
icap_enable on
```

4. Добавьте в файл строку для создания ICAP-службы Squid и укажите для нее ссылку на ICAP-сервер PT Email Security:

- Если используется режим REQMOD:  
`icap_service <Название ICAP-службы> reqmod_precache <Ссылка на ICAP-сервер для REQMOD>`
  - Если используется режим RESPMOD:  
`icap_service <Название ICAP-службы> respmod_precache <Ссылка на ICAP-сервер для RESPMOD>`
5. Если необходимо, укажите в той же строке дополнительные параметры ICAP-службы, разделяя их пробелами:
    - Если необходимо пересылать HTTP-клиенту сообщения, которые не были обработаны из-за ошибок или недоступности ICAP-сервера, добавьте параметр `bypass=1`. По умолчанию Squid передает HTTP-клиенту страницу с сообщением об ошибке.
    - Если необходимо переопределить максимальное число одновременных соединений с ICAP-сервером, добавьте параметра `max-conn=<Число соединений>`. По умолчанию установлено 128 соединений.
    - Если необходимо настроить поведение в случае превышения максимального числа соединений, добавьте параметр `on-overload=<Действие>`. Доступны следующие действия: `block` — отправить HTTP-клиенту страницу с сообщением об ошибке; `bypass` — игнорировать ICAP-службу (по умолчанию); `wait` — ожидать освобождения ICAP-соединения; `force` — игнорировать установленное максимальное число одновременных соединений.
  6. Добавьте в файл строку для настройки доступа к созданной ICAP-службе:  
`adaptation_access <Название ICAP-службы> <Параметры доступа>`  
 Например:  
`adaptation_access ptes_req allow all`  
`adaptation_access ptes_resp allow all`
  7. Если требуется отправлять поле заголовка X-Client-IP с IP-адресом пользователя, скачавшего файл, добавьте в файл строку:  
`adaptation_send_client_ip on`
  8. Если требуется отправлять поле заголовка X-Client-Username с именем пользователя, скачавшего файл, добавьте в файл строки:  
`adaptation_send_username on`  
`icap_client_username_header X-Client-Username`
  9. Сохраните изменения и закройте файл.
  10. Перезапустите прокси-сервер Squid:  
`sudo service squid3 reload`

**Примечание.** Для перезапуска прокси-сервера Squid также может использоваться команда `sudo service squid reload`.

ICAP-клиент настроен.

## 13.18. UserGate NGFW 6, 7.1, 7.4

При подключении источника объекты от межсетевого экрана UserGate отправляются на проверку в PT Email Security по протоколу ICAP. В зависимости от приобретенной вами лицензии и выбранных параметров работы ICAP-сервера PT Email Security проверка может выполняться в режиме ожидания, в пассивном или блокирующем режиме.

**Внимание!** Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 1344 от узла источника к основному узлу PT Email Security.

Для подключения источника к PT Email Security необходимо:

- Добавить в PT Email Security источник с типом **ICAP-сервер**.
- На межсетевом экране UserGate настроить ICAP-клиент для работы с ICAP-сервером PT Email Security.

### Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.  
  
Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.
4. В раскрывающемся списке **Тип** выберите **ICAP-сервер**.
5. Если необходимо, в поле **IP-адреса ICAP-сервера** введите дополнительные адреса.  
**Примечание.** В поле указан IP-адрес ICAP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.
6. Если необходимо, измените стандартный порт подключения к ICAP-серверу.  
**Внимание!** Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.
7. Если необходимо принимать объекты только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
8. Нажмите кнопку **Добавить источник**.

## Настройка источника

Для межсетевого экрана UserGate необходимо настроить ICAP-клиент для работы с ICAP-сервером, созданным при добавлении источника в PT Email Security. Дополнительную информацию о настройке UserGate вы можете получить на сайте [usergate.com](http://usergate.com).

Если UserGate у вас работает в качестве сетевого моста, для работы ICAP-клиента необходимо использовать режим моста Layer 3.

При настройке ICAP-клиента вам необходимо указать ссылку для обращения к ICAP-серверу PT Email Security. Вид ссылки зависит от режима проверки объектов и режима работы ICAP-сервера:

- Ссылки для проверки объектов в блокирующем режиме:
  - REQMOD: /scanrequest?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=5
  - RESPMOD: /scanresponse?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=5

**Примечание.** В параметре block-unwanted вы можете указать y, если необходимо блокировать потенциально опасные файлы, или n — если блокировать такие файлы не требуется (по умолчанию потенциально опасные файлы не блокируются). В параметре timeout вы можете изменить тайм-аут ответа ICAP-сервера в секундах.

- Ссылки для проверки объектов в режиме ожидания:
  - REQMOD: /scanrequest?modify=no&timeout=5
  - RESPMOD: /scanresponse?modify=no&timeout=5
- Ссылки для проверки объектов в пассивном режиме:
  - REQMOD: /bypass
  - RESPMOD: /bypass

► Чтобы настроить ICAP-клиент:

1. Откройте браузер и в адресной строке введите IP-адрес веб-интерфейса UserGate.  
Откроется веб-консоль UserGate.
2. Авторизуйтесь под учетной записью администратора UserGate.
3. В главном меню перейдите по ссылке **Настройки**.
4. В левой части страницы выберите раздел **Политики безопасности** → **ICAP-серверы**.
5. В панели инструментов нажмите кнопку **Добавить**.  
Откроется окно **Свойства ICAP-сервера**.
6. На вкладке **Общие** настройте параметры:
  - В поле **Название** введите название ICAP-сервера.

- В поле **Адрес сервера** введите адрес ICAP-сервера PT Email Security.
- Если используемый порт отличается от 1344, в поле **Порт** введите номер порта.
- Если необходимо изменить максимальный размер отправляемых на проверку файлов, в поле **Максимальный размер сообщения** укажите этот размер (размер по умолчанию — 512 КБ).

**Внимание!** Увеличение максимального размера отправляемых на проверку файлов приведет к увеличению объема используемой UserGate оперативной памяти. Объем используемой памяти вы можете отслеживать на дашборде **НОС** на виджете **Графики производительности**.

7. Выберите вкладку **Данные** и настройте параметры:

- В строке **Reqmod путь** установите флажок **Включено**, а в поле ниже введите ссылку на ICAP-сервер PT Email Security для REQMOD.

**Примечание.** Если вы увеличили максимальный размер отправляемых на проверку файлов, необходимо увеличить время проверки каждого файла в PT Email Security, указанное в параметре `timeout`.

- В строке **Respmoд путь** установите флажок **Включено**, а в поле ниже введите ссылку на ICAP-сервер PT Email Security для RESPMOD.

**Внимание!** Если вы увеличили время проверки файлов в PT Email Security, необходимо также увеличить тайм-аут ответа ICAP-сервера, оно должно быть на 5 секунд больше значения параметра `timeout`. Увеличение тайм-аута ответа ICAP-сервера приведет к увеличению объема используемой UserGate оперативной памяти.

**Примечание.** По умолчанию тайм-аут ответа ICAP-сервера составляет 10 секунд. Текущее значение тайм-аута вы можете узнать, выполнив на узле UserGate через интерфейс командной строки команду `proxu config -get icap_wait_timeout`. Изменить тайм-аут вы можете командой `proxu config -set icap_wait_timeout <Тайм-аут ответа ICAP-сервера>`.

- В строке **Посылать имя пользователя** установите флажки **Включено** и **Кодировать в base64**, а в поле ниже введите `X-Authenticated-User`.
- В строке **Посылать IP-адрес** установите флажок **Включено**, а в поле ниже введите `X-Client-IP`.

8. Нажмите кнопку **Сохранить**.

9. В левой части страницы выберите раздел **Политики безопасности** → **ICAP-правила**.

10. В панели инструментов нажмите кнопку **Добавить**.

Откроется окно **Свойства правила ICAP**.

11. На вкладке **Общие** настройте параметры:

- В поле **Название** введите название правила.

- В строке **Действие** по ссылке **Пропустить** откройте раскрывающийся список и выберите **Переслать**.

12. Выберите вкладку **ICAP-серверы**.

13. Нажмите кнопку **Добавить**.

Откроется окно **Выбор ICAP-сервера**.

14. Выберите в списке добавленный ранее ICAP-сервер и нажмите кнопку **Добавить**.

15. Нажмите кнопку **Заккрыть**.

ICAP-клиент настроен.

## 14. Интеграция с внешними системами

В разделе описаны возможности интеграции PT Email Security с внешними системами.

### В этом разделе

[MaxPatrol EDR 6.0 и выше \(см. раздел 14.1\)](#)

[MaxPatrol SIEM 6.1 и выше \(см. раздел 14.2\)](#)

[PT AF 3, 4.2.1 и выше \(см. раздел 14.3\)](#)

[PT CS 1.1 и выше \(см. раздел 14.4\)](#)

[PT ISIM 5.2 и выше \(см. раздел 14.5\)](#)

[PT NAD 7.1 и выше \(см. раздел 14.6\)](#)

[PT NGFW 1.8 и выше \(см. раздел 14.7\)](#)

[PT Threat Analyzer 2.10 и выше \(см. раздел 14.8\)](#)

### 14.1. MaxPatrol EDR 6.0 и выше

При интеграции продуктов пользователь MaxPatrol EDR с помощью агента на конечном устройстве может отправлять файлы на проверку в PT Email Security. Информация о проверенных файлах заносится в базы данных на агенте и на сервере MaxPatrol EDR. Получить эту информацию можно с помощью SQL-запроса.

**Внимание!** Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 443 от узла с сервером MaxPatrol EDR к основному узлу PT Email Security.

Интеграция осуществляется через публичный API PT Email Security. Для интеграции в MaxPatrol EDR используется модуль «Проверка файлов в PT Email Security».

**Примечание.** Инструкции по настройке MaxPatrol EDR приведены [в технической документации продукта](#).

Если вы настраиваете интеграцию с MaxPatrol EDR версии 8.0.1 и выше и при этом вы планируете настраивать параметры проверки через веб-интерфейс PT Email Security, вам необходимо:

- В PT Email Security выпустить токен доступа к публичному API с разрешенным действием **Проверка с параметрами источника**.
- Добавить в PT Email Security источник с типом **MaxPatrol EDR**.
- В MaxPatrol EDR настроить модуль «Проверка файлов в PT Email Security» (требуется модуль версии 2.0.0).

**Внимание!** При настройке модуля необходимо установить флажок **MaxPatrol EDR подключен как источник**.

Если вы настраиваете интеграцию с MaxPatrol EDR версии 8.0.1 и выше и при этом параметры проверки будут передаваться в запросе, вам необходимо:

- В PT Email Security выпустить токен доступа к публичному API с разрешенным действием **Проверка с передаваемыми параметрами**.
- В MaxPatrol EDR настроить модуль «Проверка файлов в PT Email Security» (требуется модуль версии 2.0.0).

**Примечание.** При настройке модуля флажок о подключении MaxPatrol EDR в качестве источника устанавливать не нужно.

Если вы настраиваете интеграцию с MaxPatrol EDR версий 6.0—8.0.0, вам необходимо:

- В PT Email Security выпустить токен доступа к публичному API с разрешенным действием **Проверка с передаваемыми параметрами**.
- В MaxPatrol EDR настроить модуль «Проверка файлов в PT Email Security».

## Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.  
  
Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.
4. В раскрывающемся списке **Тип** выберите **MaxPatrol EDR**.
5. В раскрывающемся списке **Токен доступа** выберите токен доступа к публичному API.
6. Нажмите кнопку **Добавить источник**.

## 14.2. MaxPatrol SIEM 6.1 и выше

При интеграции PT Email Security формирует сообщения в формате syslog и отправляет их на внешний syslog-сервер, в качестве которого выступает MaxPatrol SIEM. Например, формируются сообщения о начале и завершении работы с источником, о регистрации нового объекта, о результатах проверок объектов средствами проверки и о вынесении вердиктов по

объектам и заданиям. Подробная информация о сообщениях приведена в Руководстве разработчика. На основании полученных сообщений в MaxPatrol SIEM могут регистрироваться события ИБ.

**Внимание!** Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, необходимо настроить в них правила, разрешающие передачу трафика через порт UDP 514 или TCP 1468 от основного узла PT Email Security к узлу MaxPatrol SIEM.

Для передачи сообщений могут использоваться следующие протоколы:

- TCP — рекомендуется использовать, если важно снизить риск потери сообщений и сохранить порядок их передачи.
- UDP — рекомендуется использовать, если приоритетна скорость передачи и допустима потеря сообщений.

**Внимание!** При использовании протокола UDP доставка сообщений не гарантируется. Сообщения могут быть потеряны при большом объеме передаваемых данных, разрыве или перегрузке канала связи, а также при недоступности syslog-сервера. Кроме того, сообщения могут поступить на syslog-сервер не в том порядке, в котором были отправлены. Для протокола UDP не предусмотрены механизмы подтверждения доставки и повторной передачи потерянных данных.

Для настройки интеграции необходимо:

- В MaxPatrol SIEM создать и запустить задачу на сбор событий с профилем **SysLog**.
- В PT Email Security настроить отправку сообщений по протоколу syslog на внешний syslog-сервер.

**Примечание.** Инструкции по настройке MaxPatrol SIEM приведены [в технической документации продукта](#).

## Настройка PT Email Security для отправки сообщений syslog

- ▶ Чтобы настроить отправку сообщений по протоколу syslog на внешний syslog-сервер:
  1. В главном меню выберите **Система** → **Параметры** → **Уведомления**.
  2. В блоке параметров **Отправка сообщений по протоколу syslog** включите отправку сообщений.
  3. В полях **Доменное имя или IP-адрес syslog-сервера** введите адрес и порт внешнего syslog-сервера.
  4. Выберите транспортный протокол **TCP** или **UDP**.
  5. Если требуется, отключите отправку событий аудита PT Email Security.
  6. Нажмите кнопку **Сохранить**.

Изменения будут применены через несколько минут.

Отправка сообщений по протоколу syslog на внешний syslog-сервер настроена.

## 14.3. PT AF 3, 4.2.1 и выше

При интеграции продуктов PT AF отправляет извлеченные из трафика файлы на проверку в PT Email Security и в случае обнаружения угрозы получает результаты проверки.

**Внимание!** Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 1344 от узла PT AF к основному узлу PT Email Security.

Интеграция осуществляется по ICAP. При этом PT Email Security является ICAP-сервером, а PT AF — ICAP-клиентом, который отправляет извлеченные из трафика файлы на проверку и получает результаты проверки. В PT Email Security также отправляется дополнительная информация о файлах, например протокол, по которому перехвачен файл, и IP-адреса узлов, между которыми он передавался.

**Примечание.** Инструкции по настройке PT AF приведены [в технической документации продукта](#).

Если вы настраиваете интеграцию с PT AF версии 4.2.1 и выше, вам необходимо:

- Добавить в PT Email Security источник с типом **ICAP-сервер**.
- В PT AF добавить ICAP-сервер.
- В шаблоне политики безопасности PT AF настроить правило **Отправлять файлы на ICAP-серверы**.

Если вы настраиваете интеграцию с PT AF версии 3, вам необходимо:

- Добавить в PT Email Security источник с типом **ICAP-сервер**.
- В PT AF настроить работу со сторонними ICAP-службами.

При настройке ICAP-клиента вам необходимо указать ссылку для обращения к ICAP-серверу PT Email Security. Вид ссылки зависит от режима проверки объектов и режима работы ICAP-сервера:

- Ссылки для проверки объектов в блокирующем режиме:
  - REQMOD: `icap://<IP-адрес>:<Порт>/scanrequest?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=<Тайм-аут>`
  - RESPMOD: `icap://<IP-адрес>:<Порт>/scanresponse?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=<Тайм-аут>`

**Примечание.** В параметре `block-unwanted` вы можете указать `y`, если необходимо блокировать потенциально опасные файлы, или `n` — если блокировать такие файлы не требуется (по умолчанию потенциально опасные файлы не блокируются). В параметре `timeout` вы можете указать тайм-аут ответа ICAP-сервера в секундах (по умолчанию 30 секунд).

- Ссылки для проверки объектов в режиме ожидания:
  - `REQMOD: icap://<IP-адрес>:<Порт>/scanrequest?modify=no&timeout=<Тайм-аут>`
  - `RESPMOD: icap://<IP-адрес>:<Порт>/scanresponse?modify=no&timeout=<Тайм-аут>`
- Ссылки для проверки объектов в пассивном режиме:
  - `REQMOD: icap://<IP-адрес>:<Порт>/bypass`
  - `RESPMOD: icap://<IP-адрес>:<Порт>/bypass`

## Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **ICAP-сервер**.
5. Если необходимо, в поле **IP-адреса ICAP-сервера** введите дополнительные адреса.

**Примечание.** В поле указан IP-адрес ICAP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке интеграции в PT AF.

6. Если необходимо, измените стандартный порт подключения к ICAP-серверу.

**Внимание!** Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.

7. Если необходимо принимать объекты только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
8. Нажмите кнопку **Добавить источник**.

## 14.4. PT CS 1.1 и выше

При интеграции продуктов пользователь PT CS с помощью консольной утилиты `ptcs-cli` может отправлять образы контейнеров на проверку в PT Email Security. Информация о результатах проверки сохраняется в PT CS.

**Внимание!** Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 443 от узла с PT CS к основному узлу PT Email Security.

Для настройки интеграции в PT Email Security необходимо:

- Выпустить токен доступа к публичному API с разрешенным действием **Проверка с параметрами источника**.

**Примечание.** Созданный токен доступа нужно использовать в PT CS при запуске сканирования образа на ВПО с помощью утилиты командной строки `ptcs-cli` при добавлении источника PT CS.

- Добавить в PT Email Security источник с типом PT CS.

Для настройки интеграции в PT CS необходимо:

- Создать шаблоны уведомлений с типом **Сканирование образа на наличие ВПО**.
- Создать правила реагирования с типом **Сканирование образа на наличие ВПО**.

**Примечание.** Инструкции по настройке PT CS приведены [в технической документации продукта](#).

## Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите PT CS.
5. В раскрывающемся списке **Токен доступа** выберите существующий токен доступа или создайте новый, нажав ссылку **Создать токен доступа**.

**Примечание.** Вы можете привязать один токен доступа только к одному источнику.

6. Нажмите кнопку **Добавить источник**.

После добавления источника вам нужно настроить параметры проверки объектов, поступающих от источника.

## Настройка источника в PT Email Security

► Чтобы настроить параметры проверки объектов, поступающих от источника:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. В панели с информацией о добавленном источнике перейдите по ссылке **Параметры проверки**.
3. В поле **Максимальное время ожидания результатов проверки в синхронном режиме** введите 1200.
4. В поле **Максимальное время выполнения задания** введите 1600.
5. Отключите использование тестовых YARA-правил.
6. Выберите глубину распаковки архивов.

**Примечание.** Глубина распаковки архивов определяет максимальное количество вложенных друг в друга архивов, которые будут распаковываться при проверке. Если распаковывать архивы не требуется, вы можете выбрать **0**, тогда архивы будут проверяться как обычные файлы. Увеличение глубины распаковки архивов снижает скорость проверки.

7. Если архивы, для которых не удалось подобрать пароль, требуется определять как потенциально опасные, в блоке **Определять как потенциально опасные** установите флажок **Зашифрованные и нераспакованные архивы**.
8. Если архивы, вложенность которых превышает значение параметра **Глубина распаковки архивов**, требуется определять как потенциально опасные, в блоке **Определять как потенциально опасные** установите флажок **Архивы с превышенной глубиной распаковки**.
9. Отключите извлечение ссылок из объектов.
10. Отключите сохранение файлов без угроз.
11. Отключите поведенческий анализ.
12. Нажмите **Сохранить**.

## 14.5. PT ISIM 5.2 и выше

При интеграции продуктов PT ISIM отправляет извлеченные из сетевого трафика файлы на проверку в PT Email Security через публичный API. При выявлении опасных или потенциально опасных объектов в PT ISIM регистрируется событие информационной безопасности, которое будет доступно для анализа в цепочках инцидентов.

**Внимание!** Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 443 от узла PT ISIM к основному узлу PT Email Security.

**Примечание.** Инструкции по настройке PT ISIM приведены [в технической документации продукта](#).

Для настройки интеграции в PT Email Security необходимо:

- Выпустить токен доступа к публичному API с разрешенным действием **Проверка с параметрами источника**.
- Добавить в PT Email Security источник с типом **API с выбранными параметрами проверки**.

Для настройки интеграции в PT ISIM необходимо настроить отправку объектов в PT Email Security.

### Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **API с выбранными параметрами проверки**.
5. В раскрывающемся списке **Токен доступа** выберите токен доступа к публичному API.
6. Нажмите кнопку **Добавить источник**.

## 14.6. PT NAD 7.1 и выше

При интеграции продуктов PT NAD отправляет извлеченные из трафика файлы на проверку в PT Email Security и получает результаты проверки. Информация об обнаруженных угрозах отображается в карточках сессий и атак, а также в таблицах сессий и атак в столбце с метками репутации.

**Внимание!** Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 2344 от узла PT NAD к основному узлу PT Email Security.

Интеграция осуществляется по ICAP. При этом PT Email Security является ICAP-сервером. В качестве ICAP-клиента в PT NAD используется модуль `ptdpi-worker@icap`. Он отправляет извлеченные из трафика файлы на проверку и получает результаты проверки. В PT Email Security также отправляется дополнительная информация о файлах, например протокол, по которому перехвачен файл, и IP-адреса узлов, между которыми он передавался.

**Примечание.** Инструкции по настройке PT NAD приведены [в технической документации продукта](#).

Для настройки интеграции необходимо:

- В PT Email Security добавить источник с типом **PT NAD**.
- В центре управления PT NAD в параметрах интеграции с PT Email Security указать параметры созданного ICAP-сервера.

### Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **PT NAD**.
5. Если необходимо, в поле **IP-адреса ICAP-сервера** введите дополнительные адреса.

**Примечание.** В поле указан IP-адрес ICAP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке интеграции в PT NAD.

6. Если необходимо, измените стандартный порт подключения к ICAP-серверу.

**Внимание!** Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.

7. Если необходимо принимать объекты только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
8. Нажмите кнопку **Добавить источник**.

## 14.7. PT NGFW 1.8 и выше

При интеграции продуктов PT NGFW отправляет в PT Email Security извлеченные из трафика HTTP-сообщения и файлы для проверки. В случае выявления угрозы PT NGFW блокирует соответствующий трафик.

**Внимание!** Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 1344 от узла PT NGFW к основному узлу PT Email Security.

Интеграция осуществляется по протоколу ICAP. При этом PT Email Security является ICAP-сервером, а PT NGFW — ICAP-клиентом, который отправляет извлеченные из трафика HTTP-сообщения и файлы на проверку и получает результаты проверки.

Для настройки интеграции в PT Email Security необходимо добавить источник с типом **ICAP-сервер**.

**Примечание.** Инструкции по настройке PT NGFW приведены [в технической документации продукта](#).

Для настройки интеграции в PT NGFW необходимо:

- Добавить ICAP-сервер и указать в его профиле:
  - IP-адрес ICAP-сервера, созданного при добавлении источника в PT Email Security.
  - Ссылки для обращения к ICAP-серверу PT Email Security.
- Создать профиль ICAP и выбрать в нем профиль добавленного ICAP-сервера.
- В правиле безопасности указать созданный профиль ICAP в качестве профиля безопасности. На ICAP-сервер будет отправляться трафик, который соответствует этому правилу безопасности.

Вид ссылки для обращения к ICAP-серверу PT Email Security зависит от режима проверки объектов и режима работы ICAP-сервера:

- Ссылки для проверки объектов в блокирующем режиме:
  - REQMOD: /scanrequest?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=<Тайм-аут>
  - RESPMOD: /scanresponse?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=<Тайм-аут>

**Примечание.** В параметре `block-unwanted` вы можете указать `y`, если необходимо блокировать потенциально опасные файлы, или `n`, если блокировать такие файлы не требуется (по умолчанию потенциально опасные файлы не блокируются). В параметре `timeout` вы можете указать тайм-аут ответа ICAP-сервера в секундах (по умолчанию — 30 секунд).

- Ссылки для проверки объектов в режиме ожидания:
  - REQMOD: `/scanrequest?modify=no&timeout=<Тайм-аут>`
  - RESPMOD: `/scanresponse?modify=no&timeout=<Тайм-аут>`
- Ссылки для проверки объектов в пассивном режиме:
  - REQMOD: `/bypass`
  - RESPMOD: `/bypass`

## Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **ICAP-сервер**.
5. Если необходимо, в поле **IP-адреса ICAP-сервера** введите дополнительные адреса.

**Примечание.** В поле указан IP-адрес ICAP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке интеграции в PT NGFW.

6. Если необходимо, измените стандартный порт подключения к ICAP-серверу.
 

**Внимание!** Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.
7. Если необходимо принимать объекты только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
8. Нажмите кнопку **Добавить источник**.

## 14.8. PT Threat Analyzer 2.10 и выше

При интеграции продуктов PT Email Security отправляет в PT Threat Analyzer результаты заданий, в которых обнаружены опасные или потенциально опасные файлы. Вы также можете настроить отправку найденных в этих заданиях файлов с угрозами. На основе полученных результатов для каждого задания в PT Threat Analyzer формируется отдельный отчет. Интеграция осуществляется через публичный REST API PT Threat Analyzer.

**Внимание!** Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 443 от основного узла PT Email Security к узлу PT Threat Analyzer.

**Примечание.** Инструкции по настройке PT Threat Analyzer приведены [в технической документации продукта](#).

Для настройки интеграции в PT Threat Analyzer необходимо:

1. Создать учетную запись для PT Email Security.
2. Выпустить ключ API с привилегиями **Загрузка артефактов, Регистрация и изменение отчетов, Регистрация и изменение наблюдений, Просмотр задач обогащения, Создание задач обогащения** для доступа к REST API.
3. Добавить экземпляр источника с типом PT Email Security.
4. Привязать созданный источник к учетной записи PT Email Security.

Для настройки интеграции в PT Email Security необходимо настроить отправку данных для отчетов в PT Threat Analyzer.

### Настройка PT Email Security для отправки данных для отчетов

► Чтобы настроить отправку данных для отчетов в PT Threat Analyzer:

1. В главном меню выберите **Система** → **Параметры** → **Уведомления**.
2. В блоке параметров **Отправка данных в PT Threat Analyzer** включите отправку данных.
3. В поле **URL-адрес PT Threat Analyzer** введите адрес REST API PT Threat Analyzer в формате `https://<Доменное имя или IP-адрес>`.
4. В поле **Ключ API** введите ключ для доступа к REST API PT Threat Analyzer.
5. В раскрывающемся списке **Уровень доступа** выберите уровень доступа пользователя в PT Threat Analyzer, который необходим для доступа к отчету.
6. С помощью переключателя **Отправка файлов** настройте отправку файлов:
  - Если отправлять файлы не требуется, выберите **Не отправлять**.

- Если требуется отправлять только опасные и потенциально опасные файлы, выберите **Только файлы с угрозами**.
- Если требуется также отправлять файлы, в которых содержатся обнаруженные файлы с угрозами (например, архивы или письма), выберите **Файлы с угрозами и связанные с ними файлы**.

7. Нажмите кнопку **Сохранить**.

Отправка данных для отчетов в PT Threat Analyzer настроена.

## 15. Настройка обновления PT Email Security

Обновление PT Email Security включено по умолчанию, новые версии устанавливаются автоматически. Вы можете настроить автоматическое обновление или отключить его, чтобы запускать обновление вручную.

Новые версии PT Email Security бывают двух типов: с новыми функциями и с исправлениями. При обновлении до версии с новыми функциями в PT Email Security появляются новые возможности. Обновление до версии с исправлениями происходит в рамках текущей версии и предназначено для устранения ошибок. Вы можете настроить автоматическое обновление для версий обоих типов или автоматическое обновление только для версий с исправлениями.

Управлять обновлением можно на странице **Система** → **Обновления**. На этой странице вы можете просмотреть текущую версию PT Email Security, проверить наличие новых версий, запустить ручное обновление или перейти на страницу настройки автоматического обновления системы.

 Проверить наличие обновлений

Проверено 14 апреля, 13:40

**Доступна версия 5.22.0.110634**  
От 14 апреля  
**Обновить сейчас** Будет установлена автоматически 16 апреля (среда) в 20:33

**Доступна версия 5.22.0.110625**  
От 14 апреля  
**Обновить сейчас**

**Текущая версия**  
**5.22.0.110552**

☒ **Автоматическое обновление**  
[Изменить](#)  
**Версии с новыми функциями** **Включено**  
Не устанавливать версии, которым меньше 30 дней  
Расписание  
Суббота, 04:00  
**Версии с исправлениями** **Включено**  
Не устанавливать версии, которым меньше 24 часов  
Расписание  
Вторник, 04:00  
Среда, 04:00  
Пятница, 04:00

Рисунок 10. Страница **Обновления**

В рабочей области страницы расположены:

- Кнопка **Проверить наличие обновлений** для проверки доступных для установки версий.
- Блок с версией, которая доступна для установки. При наличии нескольких доступных версий каждая отображается в отдельном блоке. В блоке также отображается кнопка **Обновить сейчас** для установки версии вручную.
- Блок для настройки автоматического обновления. В блоке отображаются ссылка **Изменить**, настроенные параметры обновления и расписание автоматического обновления для версий с новыми функциями и версий с исправлениями.

## Настройка автоматического обновления

Вы можете настроить автоматическое обновление для всех новых версий: и для версий с новыми функциями, и для версий с исправлениями.

► Чтобы настроить автоматическое обновление:

1. В главном меню выберите **Система** → **Обновления**.
2. В блоке параметров **Автоматическое обновление** нажмите ссылку **Изменить**.
3. Включите автоматическое обновление в блоке **Версии с новыми функциями**.
4. Если вы хотите настроить минимальный срок, который должен пройти с момента выхода версии с новыми функциями:
  - В блоке **Версии с новыми функциями** установите флажок **Не устанавливать версии, которым меньше <количество> дней**.
  - Укажите количество дней, по истечении которого нужно установить обновление.
5. Если вы хотите настроить расписание обновления для версий с новыми функциями:
  - В блоке **Версии с новыми функциями** нажмите кнопку **Добавить**.
  - Выберите день недели и укажите время, в которые будут устанавливаться обновления.
6. Если вы хотите настроить минимальный срок, который должен пройти с момента выхода новой версии с исправлениями:
  - В блоке **Версии с исправлениями** установите флажок **Не устанавливать версии, которым меньше <количество> часов**.
  - Укажите количество часов, по истечении которого нужно установить обновление.
7. Если вы хотите настроить расписание обновления для версий с исправлениями:
  - В блоке **Версии с исправлениями** нажмите кнопку **Добавить**.
  - Выберите день недели и укажите время, в которые будут устанавливаться обновления.
8. Нажмите кнопку **Сохранить**.

## Настройка автоматического обновления только для версий с исправлениями

Вы можете настроить автоматическое обновление только для версий с исправлениями, отключив автоматическое обновление для версий с новыми функциями.

- ▶ Чтобы настроить автоматическое обновление только для версий с исправлениями:
  1. В главном меню выберите **Система** → **Обновления**.
  2. Нажмите ссылку **Изменить** в блоке **Автоматическое обновление**.
  3. Выключите автоматическое обновление в блоке **Версии с новыми функциями**.
  4. Если вы хотите настроить минимальный срок, который должен пройти с момента выхода новой версии с исправлениями:
    - В блоке **Версии с исправлениями** установите флажок **Не устанавливать версии, которым меньше <количество> часов**.
    - Укажите количество часов, по истечении которого нужно установить обновление.
  5. Если вы хотите настроить расписание обновления для версий с исправлениями:
    - В блоке **Версии с исправлениями** нажмите кнопку **Добавить**.
    - Выберите день недели и укажите время, в которые будут устанавливаться обновления.
  6. Нажмите кнопку **Сохранить**.

## Отключение автоматического обновления

- ▶ Чтобы отключить автоматическое обновление:
  1. В главном меню выберите **Система** → **Обновления**.
  2. В блоке параметров **Автоматическое обновление** выключите обновление.

## Запуск обновления вручную

- ▶ Чтобы запустить обновление вручную:
  1. В главном меню выберите **Система** → **Обновления**.
  2. Нажмите кнопку **Проверить наличие обновлений**.
  3. В оповещении о новой версии нажмите кнопку **Обновить сейчас**.

Во время обновления все функции PT Email Security будут доступны. По окончании обновления в меню информации о продукте отобразится уведомление об успешном обновлении.

## 16. Просмотр конфигурации PT Email Security

На страницах раздела **Система** → **Конфигурация** вы можете получить общее представление о настроенной конфигурации PT Email Security: об узлах, входящих в конфигурацию, их IP-адресах и ролях, о развернутых на узлах компонентах и подах. Вы также можете оценить работоспособность конфигурации, увидеть, какие из узлов, компонентов или подов не работают или работают частично, и принять решения по улучшению их работоспособности.

**Примечание.** В PT Email Security используется микросервисная архитектура и контейнеризация приложений на основе технологий containerd и Kubernetes (K8s). Для просмотра Docker-контейнеров и Docker-образов вы можете использовать утилиты `crictl` и `ctr`. Утилиты доступны на узлах PT Email Security.

В верхней части каждой страницы указаны:

- Статус отказоустойчивого кластера (отображается, если такой кластер настроен).
- Виртуальный IP-адрес отказоустойчивого кластера (отображается, если такой кластер настроен).
- Общее количество узлов для поведенческого анализа файлов и количество доступных узлов (отображается, если часть узлов недоступна).
- Общее количество виртуальных машин, которые можно запустить на всех узлах для поведенческого анализа файлов, и количество доступных для запуска виртуальных машин (отображается, если часть виртуальных машин недоступна).

Содержимое рабочей области зависит от выбранной страницы.

### Страница «Компоненты»

Для просмотра информации о компонентах PT Email Security предназначена страница **Система** → **Конфигурация** → **Компоненты**.

Отказоустойчивый кластер
**Настроен**

Адрес кластера
**10.120.10.120**

Узлы для поведенческого анализа
**1**

ВМ для поведенческого анализа
**2**

| Название           | ↓↑ | Тип                | ↓↑ | Узел                  | ↓↑ | Пространство имен | ↓↑ | Работающих подов | ↓↑ | Статус            | ↑ |
|--------------------|----|--------------------|----|-----------------------|----|-------------------|----|------------------|----|-------------------|---|
| vmagent            |    | Служба мониторинга |    | ptms-astra-all-qa4    |    | monitoring        |    | 0 из 1           |    | Не работает       |   |
| prometheus-adapter |    | Служба мониторинга |    | ptms-astra-all-qa4    |    | monitoring        |    | 11 из 12         |    | Работает частично |   |
| telemetry          |    | Служба интеграции  |    | ptms-astra-all-qa4    |    | ptms              |    | 2                |    | Работает          |   |
| ptioc              |    | Средство проверки  |    | ptms-astra-node3-q... |    | ptms              |    | 2                |    | Работает          |   |
| ptcategorizer      |    | Средство проверки  |    | ptms-astra-node3-q... |    | ptms              |    | 2                |    | Работает          |   |
| cluster-babysitter |    | Служба обновления  |    | ptms-astra-all-qa4    |    | ptms              |    | 1                |    | Работает          |   |
| av-nano            |    | Средство проверки  |    | ptms-astra-node3-q... |    | ptms              |    | 4                |    | Работает          |   |
| mc-licensing       |    | Служба             |    | ptms-astra-node3-q... |    | ptmc              |    | 1                |    | Работает          |   |
| kube-state-metrics |    | Служба мониторинга |    | ptms-astra-all-qa4    |    | monitoring        |    | 1                |    | Работает          |   |

Рисунок 11. Страница **Компоненты**

В рабочей области страницы расположена таблица с информацией о компонентах PT Email Security. По кнопке **↓↑** в заголовке любого столбца таблицы вы можете отсортировать компоненты по значениям в этом столбце. Нажимая на заголовок столбца, вы можете отфильтровать содержимое таблицы по значениям в столбце. Для каждого компонента в таблице указаны:

- **Название.**
- **Тип** — назначение компонента.
- **Узел** — название узла, на котором развернут компонент.
- **Пространство имен:**
  - **ptms** — PT Email Security.
  - **ptmc** — PT MC.
  - **monitoring** — подсистема мониторинга работы PT Email Security.
- **Работающих подов** — количество работающих подов и общее количество подов, используемых компонентом.
- **Статус** — один из статусов пода: **Работает**, **Работает частично** или **Не работает**.

## Страница «Узлы»

Для просмотра информации о входящих в конфигурацию PT Email Security узлах и ролях этих узлов предназначена страница **Система** → **Конфигурация** → **Узлы**.

Отказоустойчивый кластер

Настроен

Адрес кластера

10.120.10.120

Узлы для поведенческого анализа

1

ВМ для поведенческого анализа

2

ptms-astra-node3

Работает

scan-core

backend

persistent-data

control-plane

IP-адрес

ЦП

ОЗУ

ОС

containerd

Kubernetes

Поды

10.120.4.143

6 ядер

15,62 ГБ

Astra Linux

1.6.20

v1.26.4

30

ptms-astra-node2

Работает

scan-core

backend

persistent-data

control-plane

IP-адрес

ЦП

ОЗУ

ОС

containerd

Kubernetes

Поды

10.120.4.142

6 ядер

15,62 ГБ

Astra Linux

1.6.20

v1.26.4

22

ptms-astra-sandbox

Работает

sandbox

IP-адрес

ЦП

ОЗУ

ОС

containerd

Kubernetes

Xen

Поды

ВМ

10.120.4.149

16 ядер

26,47 ГБ

Astra Linux

1.6.20

v1.26.4

4.16.5

15

2

Рисунок 12. Страница **Узлы**

В рабочей области страницы расположены панели с информацией об узлах, входящих в конфигурацию PT Email Security. Для каждого узла указаны:

- Имя ноды Kubernetes и имя узла (если оно отличается от имени ноды).
- Роли узла. Могут быть настроены следующие роли:
  - **backend** — сервер приложений. На таком сервере могут быть установлены: встроенный PT MC, служба обновлений, служба публичного API и другие компоненты PT Email Security.
  - **control-plane** — основной или резервный узел с управляющей нодой Kubernetes.
  - **persistent-data** — хранилище файлов.
  - **sandbox** — узел для поведенческого анализа.
  - **scan-core** — ядро проверки PT Email Security.
- **IP-адрес** — IP-адрес узла.
- **ЦП** — количество ядер центрального процессора.
- **ОЗУ** — объем памяти.
- **ОС** — версия операционной системы.
- **containerd** — версия среды containerd.
- **Kubernetes** — версия Kubernetes.
- **Xen** — версия гипервизора Xen.

- **Поды** — количество подов, развернутых на узле.
- **ВМ** — количество виртуальных машин, которые можно запустить на узле для поведенческого анализа файлов.
- Статус узла: **Работает**, **Есть ошибки** или **Недоступен**.

## Страница «Поды»

Для просмотра информации о подах Kubernetes предназначена страница **Система** → **Конфигурация** → **Поды**.

| Отказоустойчивый кластер<br><b>Настроен</b> |                    | Адрес кластера<br><b>10.120.10.120</b> |              | Узлы для поведенческого анализа<br><b>1</b> |                       | ВМ для поведенческого анализа<br><b>2</b> |  |
|---------------------------------------------|--------------------|----------------------------------------|--------------|---------------------------------------------|-----------------------|-------------------------------------------|--|
| Имя пода                                    | Компонент          | Узел                                   | Перезапусков | Время работы                                | Работающих контейн... | Статус                                    |  |
| os-installer-xffsn                          | os-installer       | ptms-astra-node3                       | 2            | 2 д 4 ч                                     | 0                     | Не работает                               |  |
| prometheus-adapt...                         | prometheus-adapter | ptms-astra-node3                       | 2            | 3 нед 5 д                                   | 1                     | Работает                                  |  |
| trace2ml-6746f74c...                        | trace2ml           | ptms-astra-node4                       | 0            | 3 ч 1 мин                                   | 1                     | Работает                                  |  |
| trace2ml-6746f74c...                        | trace2ml           | ptms-astra-node3                       | 0            | 3 ч 1 мин                                   | 1                     | Работает                                  |  |
| ptioc-7cc7bb44bc-...                        | ptioc              | ptms-astra-node3                       | 0            | 3 ч 22 мин                                  | 1                     | Работает                                  |  |
| ptioc-7cc7bb44bc-...                        | ptioc              | ptms-astra-node3                       | 0            | 3 ч 21 мин                                  | 1                     | Работает                                  |  |
| ptcategorizer-c6d4...                       | ptcategorizer      | ptms-astra-node4                       | 0            | 3 ч 24 мин                                  | 1                     | Работает                                  |  |
| ptcategorizer-c6d4...                       | ptcategorizer      | ptms-astra-node3                       | 0            | 3 ч 23 мин                                  | 1                     | Работает                                  |  |
| cluster-babysitter-...                      | cluster-babysitter | ptms-astra-node4                       | 0            | 3 ч 26 мин                                  | 2                     | Работает                                  |  |

Рисунок 13. Страница **Поды**

В рабочей области страницы расположена таблица с информацией о подах Kubernetes. По кнопке  в заголовке любого столбца таблицы вы можете отсортировать поды по значениям в этом столбце. Нажимая на заголовок столбца, вы можете отфильтровать содержимое таблицы по значениям в столбце. Для каждого пода в таблице указаны:

- **Имя**.
- **Компонент** — название компонента, использующего под.
- **Узел** — название узла, на котором развернут под.
- **Перезапусков** — количество перезапусков пода.
- **Время работы** — общее время работы пода.
- **Работающих контейнеров** — количество контейнеров, работающих внутри пода.
- **Статус** — один из статусов пода: **Работает**, **Не работает**.

## 17. Мониторинг системных ресурсов в Grafana

Для визуализации данных об использовании системных ресурсов на узлах PT Email Security используется средство визуализации и мониторинга данных Grafana с набором стандартных дашбордов. Для работы с Grafana в главном меню вам необходимо выбрать раздел **Система** → **Конфигурация** → **Мониторинг**. Страница Grafana открывается в отдельной вкладке браузера. На странице отображается дашборд, выбранный основным. Работа Grafana одновременно на нескольких вкладках не поддерживается.

**Примечание.** По умолчанию установлена темная тема оформления интерфейса. Вы можете сменить тему оформления на светлую в параметрах профиля пользователя.

При работе с Grafana вы можете:

- Просматривать информацию на основном дашборде.
- Выбирать для просмотра другие стандартные дашборды.
- Копировать стандартные дашборды и при необходимости изменять их.
- Создавать и импортировать новые дашборды.
- Настраивать почтовые уведомления по событиям для любого дашборда.

**Внимание!** Для получения уведомлений от Grafana по электронной почте вам необходимо на основном узле PT Email Security настроить подключение к SMTP-серверу.

Инструкции по работе с Grafana вы можете найти в технической документации Grafana.

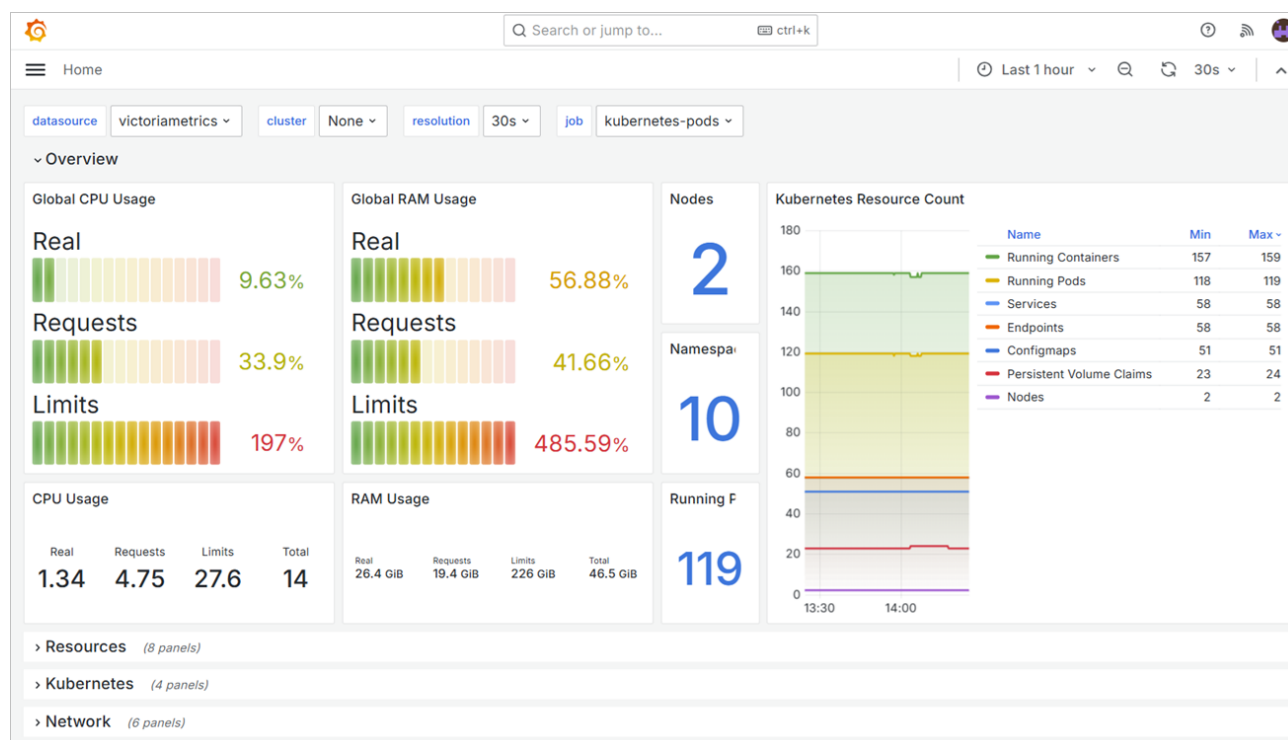


Рисунок 14. Мониторинг системных ресурсов в Grafana

В верхней части страницы расположена панель инструментов с кнопками:

☰ — для открытия боковой панели с главным меню. Используя разделы главного меню, вы можете переходить на страницы Grafana:

- **Home** — для просмотра домашней страницы с основным дашбордом.
- **Starred** — для выбора избранных дашбордов.
- **Dashboards** — для работы с дашбордами.
- **Explore** — для создания запросов к источникам данных.
- **Alerting** — для работы с уведомлениями.

🕒 — для выбора периода времени, за который отображаются данные на виджетах.

↻ — для обновления данных на виджетах.

⌵ — для настройки автоматического обновления данных на виджетах.

В рабочей области страницы отображаются виджеты выбранного вами дашборда. Виджеты сгруппированы в раскрывающиеся блоки.

## Назначение стандартных дашбордов

Для мониторинга обработки объектов в PT Email Security предназначены дашборды:

- **Product / Rabbitmq / Queues** — предоставляет детализированные данные об очередях сообщений компонента RabbitMQ, включая общее количество очередей, динамику изменения количества сообщений в очередях, а также скорость поступления, доставки и подтверждения сообщений.
- **Product / Gateway / BCC** — предназначен для мониторинга обработки писем от источников типа «Почтовый сервер в режиме фильтрации» и «Почтовый сервер в режиме зеркалирования».

В блоке **Current rates** отображается график изменения режимов работы источников во времени. Для каждого источника фиксируются переходы между блокирующим и пассивным режимами, что позволяет отследить стабильность их работы.

В блоке **Incoming Emails Stats** отображается статистика приема писем. Представлен график по времени, отражающий динамику изменения количества писем, полученных от каждого источника. Также представлены диаграммы, показывающие распределение общего количества писем по источникам и их типам.

В блоке **Processed Emails Stats** отображается статистика обработки писем.

Представлена гистограмма, показывающая распределение количества писем по времени их обработки, что позволяет оценить общую нагрузку и типичную продолжительность обработки письма.

Также представлены графики, отражающие динамику изменения во времени следующих показателей: количества писем, для которых выполнено определенное действие (пропущено, заблокировано), и количества писем, обработанных без таких действий; количества писем с определенными статусом, вердиктом и причиной вердикта (отдельные графики для пропущенных и заблокированных писем и для писем, обработанных без таких действий); количества обработанных писем от каждого источника.

**Примечание.** Письмо считается заблокированным, если оно заблокировано хотя бы для одного получателя. На графиках и диаграммах для писем, обработанных без выполнения каких-либо действий, учитываются письма только от источников типа «Почтовый сервер в режиме зеркалирования».

Кроме того, представлены диаграммы, показывающие распределение общего числа обработанных писем: по именам источников (отдельные диаграммы для пропущенных и заблокированных писем и для писем, обработанных без таких действий); по действиям (пропущено, заблокировано или обработано без таких действий); по статусам обработки (успешно или с ошибкой); отдельно для писем без задания на проверку — по действиям (пропущено или заблокировано).

В блоке **Errors Stats** отображается статистика ошибок при обработке писем.

Представлены графики, отражающие динамику изменения во времени количества ошибок с определенными типами и кодами. Также приведены диаграммы, показывающие распределение общего количества ошибок по типам и кодам. Даны отдельные графики и диаграммы для ошибок, возникших при попытке отправить письмо на внешний почтовый сервер, и ошибок, возвращенных удаленным сервером в ответ на отправку.

Для фильтрации данных в панели инструментов дашборда можно выбрать тип и название источника.

- **Product / MTA** — предназначен для мониторинга работы встроенного почтового транспортного агента. Дашборд позволяет отслеживать состояние очереди обработки писем, режимы работы источников, статистику приема и обработки писем, а также ошибки при взаимодействии с почтовыми серверами.

В блоке **Current Rates** отображается текущее состояние обработки писем. Представлен график изменения размера очереди писем во времени с разделением по статусам: ожидают обработки, обрабатываются и всего в очереди. Также отображается виджет с текущим количеством писем в очереди и график изменения режимов работы источников во времени. Для каждого источника фиксируются переходы между блокирующим и пассивным режимами.

В блоке **Incoming Emails Stats** отображается статистика приема писем. Представлены графики, отражающие динамику изменения количества оригинальных писем и дубликатов по идентификаторам источников. Также представлены диаграммы, показывающие распределение общего количества оригинальных писем и дубликатов по типам и идентификаторам источников.

В блоке **Processed Emails Stats** отображается статистика обработки писем. Представлена гистограмма, показывающая распределение количества писем по времени их обработки. Также представлены графики и диаграммы, отражающие динамику изменения во времени

следующих показателей: количества пропущенных и заблокированных писем по правилам, количества обработанных писем по действиям, количества обработанных писем по идентификаторам источников. Дополнительно отображается распределение обработанных писем по вердиктам, действиям, статусам обработки и решениям о пропуске или блокировке.

В блоке **Errors Stats** отображается статистика ошибок при приеме и доставке писем. Представлены графики и диаграммы ошибок при взаимодействии с SMTP-клиентами, от которых поступают письма, и с серверами для доставки проверенной почты. Ошибки группируются по типам и кодам. Эти данные позволяют выявлять проблемы, возникающие при приеме писем и передаче проверенных писем дальше по почтовому маршруту.

Для фильтрации данных в панели инструментов дашборда можно выбрать тип и название источника.

- **Product / BA Queue** — дашборд предназначен для мониторинга состояния и производительности модуля поведенческого анализа.

В блоке **Current queue size** отображаются текущее количество файлов в очереди на поведенческий анализ (добавленных и проверяемых), продолжительность анализа, количество запущенных для анализа VM, история изменения длины очереди и распределение накладных расходов по временным диапазонам.

Блок **Total stats** содержит статистику запусков поведенческого анализа за выбранный период: распределение по источникам, типам файлов и образам VM, количество ошибок и показатели эффективности кэширования.

В блоке **Rates in time** представлены графики по времени, отражающие динамику ошибок, накладных расходов, использования VM, запусков поведенческого анализа по источникам, типам файлов и образам VM, а также показатели активности кэша и количества успешно завершенных запусков.

Для фильтрации данных в панели инструментов дашборда можно выбрать источники, образы VM и типы файлов.

Для мониторинга узлов PT Email Security предназначен дашборд:

- **Node Exporter Full** — предоставляет детализированные данные о состоянии узлов PT Email Security, включая загрузку центрального процессора, использование памяти ОЗУ, состояние файловых систем и сетевой трафик.

Для мониторинга компонентов PT Email Security предназначены дашборды:

- **RabbitMQ-Overview** — дашборд предоставляет сводную информацию о работе компонента RabbitMQ, включая количество очередей, сообщений, соединений, каналов и узлов, а также скорость поступления, доставки, подтверждения и повторной отправки

сообщений. Кроме того, дашборд предоставляет данные об использовании компонентом системных ресурсов, включая память ОЗУ, дисковое пространство, файловые дескрипторы и сокеты.

- **VictoriaMetrics — cluster** — предоставляет информацию о загрузке центрального процессора, использовании памяти ОЗУ и дискового пространства в кластере системы VictoriaMetrics.
- **VictoriaMetrics — vmagent** — отображает информацию о работе агента сбора данных vmagent системы VictoriaMetrics, включая объем передаваемых данных и задержки их обработки.

В PT Email Security используется микросервисная архитектура и контейнеризация приложений на основе технологий containerd и Kubernetes. Для мониторинга работы кластера Kubernetes предназначены дашборды:

- **kube-state-metrics-v2** — отображает состояние объектов Kubernetes, включая узлы, поды, развертывания (Deployments), наборы подов с состоянием (Statefulset), контейнеры, автоскейлеры, задания и постоянные хранилища.
- **Kubernetes / System / API Server** — предназначен для мониторинга производительности API-сервера Kubernetes, включая нагрузку на обработку запросов и задержки операций.
- **Kubernetes / Views / Global** — предоставляет сводную информацию о загрузке ресурсов и состоянии всех компонентов кластера Kubernetes (основной дашборд по умолчанию).
- **Kubernetes / Views / Namespaces** — показывает использование ресурсов и количество активных подов в разрезе пространств имен.
- **Kubernetes / Views / Nodes** — отображает данные о производительности и загрузке узлов Kubernetes, включая центральный процессор, память ОЗУ и сетевые ресурсы.
- **Kubernetes / Views / Pods** — предоставляет информацию о статусе подов, использовании ими ресурсов и возможных причинах перезапусков.
- **Kubernetes Cluster Monitoring** — отображает данные о состоянии кластера Kubernetes, включая работу сервисов и использование вычислительных ресурсов.
- **Kubernetes Metrics — Deployments vs StatefulSets vs DaemonSets** — предназначен для просмотра информации об использовании ресурсов различных типов развертываний в Kubernetes, включая загрузку центрального процессора, использование памяти ОЗУ, дискового пространства, сетевого ввода-вывода и количество недоступных реплик.

## Настройка почтовых уведомлений

В Grafana предусмотрена отправка уведомлений по электронной почте для следующих стандартных событий:

- **sb\_component\_offline** — компонент PT Email Security не работает.
- **sb\_component\_partially\_unavailable** — компонент PT Email Security работает частично.
- **system\_update\_finished** — завершено обновление компонентов PT Email Security.

Для настройки отправки почтовых уведомлений от Grafana вам необходимо:

- На странице **Alerting** → **Contact points** добавить электронные адреса получателей уведомлений.
- На основном узле PT Email Security настроить подключение к SMTP-серверу.

Уведомления будут отправляться для всех событий на все добавленные адреса. При необходимости вы можете отключить отправку уведомлений для событий на странице **Alerting** → **Silences**.

- Чтобы настроить подключение к SMTP-серверу на основном узле PT Email Security,

выполните команду:

```
sudo ptmsctl system components set -c grafana -p grf-smtp-host=<Доменное имя или IP-адрес SMTP-сервера>:<Порт> -p grf-smtp-user=<Логин> -p grf-smtp-pass=<Пароль> -p grf-smtp-from-address=<Почтовый адрес отправителя>
```

Например:

```
sudo ptmsctl system components set -c grafana -p grf-smtp-host=hostname:587 -p grf-smtp-user=sandbox -p grf-smtp-pass=P@ssw0rd -p grf-smtp-from-address=sandbox@hostname.ru
```

Таблица 6. Параметры подключения к SMTP-серверу

| Параметр              | Тип данных | Описание                                                                      |
|-----------------------|------------|-------------------------------------------------------------------------------|
| grf-smtp-from-address | String     | Электронный адрес, который будет указан в уведомлении в качестве отправителя  |
| grf-smtp-host         | String     | IP-адрес или доменное имя SMTP-сервера в формате <Адрес> : <Порт>             |
| grf-smtp-pass         | String     | Пароль для аутентификации на SMTP-сервере                                     |
| grf-smtp-skip-tls     | Boolean    | Требуется ли проверять SSL/TLS-сертификат SMTP-сервера (по умолчанию — false) |
| grf-smtp-user         | String     | Логин для аутентификации на SMTP-сервере                                      |

## 18. Смена IP-адреса узла PT Email Security

Смена IP-адресов узлов не поддерживается в конфигурации PT Email Security с отказоустойчивым кластером.

Для смены IP-адреса основного узла в базовой конфигурации PT Email Security вам необходимо:

1. Изменить IP-адрес в ОС на основном узле.

**Внимание!** Сразу после смены IP-адреса в ОС необходимо на основном узле изменить IP-адрес в параметрах PT Email Security.

2. На основном узле изменить IP-адрес в параметрах PT Email Security.

Для смены IP-адреса основного узла в высоконагруженной конфигурации PT Email Security вам необходимо:

1. Изменить IP-адрес в ОС на основном узле.

**Внимание!** Сразу после смены IP-адреса в ОС необходимо на основном узле изменить IP-адрес в параметрах PT Email Security.

2. На основном узле изменить IP-адрес в параметрах PT Email Security.
3. На основном узле исключить каждый дополнительный узел из конфигурации PT Email Security.
4. Установить компоненты PT Email Security на каждый дополнительный узел.

**Примечание.** Если на дополнительном узле уже установлены компоненты PT Email Security, в процессе установки эти компоненты будут проверены и узел будет добавлен в конфигурацию PT Email Security.

Для смены IP-адреса дополнительного узла в высоконагруженной конфигурации PT Email Security вам необходимо:

1. Удалить компоненты PT Email Security с дополнительного узла (с сохранением гипервизора Xen и конфигурационных файлов PT Email Security).
2. Изменить IP-адрес в ОС на дополнительном узле.
3. Повторно установить компоненты PT Email Security на дополнительный узел.

### Изменение IP-адреса узла в ОС

► Чтобы изменить IP-адрес узла в ОС:

1. Откройте файл `/etc/hosts`.
2. Укажите в файле новый IP-адрес и сохраните изменения.
3. Откройте файл `/etc/network/interfaces`.

4. Укажите в файле новый IP-адрес и сохраните изменения.

5. Перезапустите службу `networking`:

```
sudo systemctl restart networking
```

**Примечание.** После перезапуска службы SSH-соединение с узлом будет разорвано. Для продолжения настройки подключитесь к узлу, используя новый IP-адрес.

## Изменение IP-адреса основного узла в параметрах PT Email Security

Инструкцию необходимо выполнять на основном узле PT Email Security. Перед сменой IP-адреса основного узла в параметрах PT Email Security необходимо изменить IP-адрес узла в ОС.

► Чтобы изменить IP-адрес основного узла в параметрах PT Email Security:

1. Перейдите в каталог со скриптами установщика PT Email Security:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт `change-master-node-ip.sh`:

```
sudo ./change-master-node-ip.sh
```

3. По завершении работы скрипта нажмите клавишу Enter.

Узел будет перезагружен.

## Исключение дополнительного узла из конфигурации PT Email Security

Инструкцию необходимо выполнять на основном узле PT Email Security.

► Чтобы исключить дополнительный узел из конфигурации PT Email Security:

1. Получите список узлов PT Email Security:

```
sudo kubectl --kubeconfig /etc/kubernetes/admin.conf get node
```

2. Если дополнительный узел указан в списке, исключите его из конфигурации:

```
sudo kubectl --kubeconfig /etc/kubernetes/admin.conf delete node <Имя дополнительного узла>
```

Появится сообщение об удалении дополнительного узла.

## Удаление компонентов PT Email Security с дополнительного узла

► Чтобы удалить компоненты PT Email Security с дополнительного узла:

1. Перейдите в каталог со скриптами установщика PT Email Security:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт `reset-kubernetes.sh`:

```
sudo ./reset-kubernetes.sh
```

**Примечание.** При таком удалении на узле сохраняются гипервизор Xen и конфигурационные файлы компонентов PT Email Security.

3. По завершении работы скрипта нажмите клавишу Enter.

Узел будет перезагружен.

## 19. Смена DNS-сервера

В случае изменения адреса DNS-сервера, например при смене подсети, вам необходимо:

- На всех узлах PT Email Security изменить адрес DNS-сервера средствами ОС.
- На основном узле PT Email Security перезапустить службу CoreDNS.

В зависимости от используемых на узле служб управления сетевыми параметрами для смены адреса DNS-сервера в ОС могут использоваться различные файлы, например файлы `/etc/network/interfaces` (параметр `dns-nameservers`) и `/etc/resolv.conf`. Для настройки адреса DNS-сервера в ОС следуйте документации используемых служб.

**Внимание!** Если файл `/etc/resolv.conf` используется службами ОС, содержимое файла обновляется автоматически. В этом случае все изменения, внесенные вами в этот файл вручную, будут потеряны, что может привести к неработоспособности PT Email Security.

- ▶ Чтобы перезапустить службу CoreDNS,

выполните команду:

```
sudo kubectl --kubeconfig /etc/kubernetes/admin.conf -n kube-system rollout restart
deploy/coredns
```

Появится сообщение:

```
deployment.apps/coredns restarted
```

Служба CoreDNS перезапущена.

## 20. Резервное копирование и восстановление параметров PT Email Security

Резервная копия параметров PT Email Security создается автоматически при каждом запуске скрипта `install.sh`, файлы резервной копии сохраняются в каталоге `/opt/ptms/var/configuration-backups`. Дополнительно вы можете вручную запустить создание резервной копии параметров. Рекомендуется создавать резервную копию параметров после каждого обновления версии PT Email Security.

При создании резервной копии параметров PT Email Security сохраняются:

- Основные параметры.
- Параметры, заданные с помощью команды `ptmsctl`.
- Параметры антивирусов и средств проверки Positive Technologies.
- Параметры источников и параметры проверки источников, кроме источников с типом «API с выбранными параметрами проверки».

При создании резервной копии не сохраняется лицензия. Если PT Email Security установлен в виртуальной среде, не сохраняются параметры виртуальной машины.

### Создание резервной копии параметров PT Email Security

Если вы планируете разворачивать PT Email Security на новом узле или удалять данные с жесткого диска, кроме создания резервной копии параметров вам необходимо:

- Через веб-интерфейс сохранить пользовательские YARA-правила и пользовательские образы ВМ (в случае удаления каталога `/opt/ptms/var/minio`).
- Сохранить данные из каталога `/opt/ptms/var/stolon/postgres`. В нем содержатся, например, данные черного и белого списков, информация о созданных токенах доступа, параметры источников с типом «API с выбранными параметрами проверки».

**Примечание.** При запуске скриптов для удаления PT Email Security данные из этих каталогов не удаляются.

После обновления версии PT Email Security рекомендуется использовать скрипт для создания резервной копии параметров новой версии. Для получения актуального скрипта вы можете обратиться в техническую поддержку Positive Technologies. Инструкцию необходимо выполнить на основном узле PT Email Security.

► Чтобы создать резервную копию параметров PT Email Security:

1. Перейдите в каталог со скриптами установщика PT Email Security:  
`cd /home/user/ptsb-installer`
2. Запустите скрипт `backup-config.sh`, указав полный путь к файлу для сохранения резервной копии параметров:  
`sudo ./backup-config.sh --backup-file <Путь к файлу резервной копии>`

Например:

```
sudo ./backup-config.sh --backup-file /opt/ptms/configuration/backup 11-12-2025.yaml
```

## Восстановление параметров PT Email Security из резервной копии

Резервную копию параметров можно использовать при переустановке или развертывании PT Email Security на новом узле.

**Внимание!** Для восстановления параметров из резервной копии имена узлов, версия и конфигурация PT Email Security должны совпадать с теми, для которых была создана резервная копия.

Инструкцию необходимо выполнить на основном узле после завершения развертывания PT Email Security. Для конфигурации с отказоустойчивым кластером должны быть развернуты все три узла кластера.

- Чтобы восстановить параметры PT Email Security из резервной копии:

1. Перейдите в каталог со скриптами установщика PT Email Security:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт `install.sh`, указав полный путь к файлу резервной копии параметров и серийный номер лицензии PT Email Security:

```
sudo ./install.sh --serial-number '<Серийный номер лицензии>' --backup-file <Путь к файлу резервной копии>
```

Например:

```
sudo ./install.sh --serial-number 'xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx' --backup-file /opt/ptms/var/configuration-backups/backup 11-12-2025.yaml
```

## 21. Обновление гипервизора Xen

Для обновления гипервизора Xen вам понадобится архив с установщиком PT Email Security.

**Примечание.** Для получения архива с установщиком актуальной версии PT Email Security вы можете обратиться в техническую поддержку Positive Technologies.

Для обновления гипервизора Xen необходимо:

1. Определить параметры установленного на узле гипервизора Xen.
2. Распаковать на узле архив с установщиком PT Email Security.
3. Если на узле установлен Xen версии 5.21 и ниже или в результате предыдущей попытки обновления произошла ошибка, удалить Xen.
4. Установить на узле новую версию гипервизора Xen.

### Определение параметров установленного гипервизора Xen

Перед обновлением вам необходимо определить параметры установленного гипервизора Xen: какое максимальное количество VM запускается на узлах с функцией поведенческого анализа и какой объема памяти выделяется гостевой операционной системе каждой виртуальной машины.

Инструкцию необходимо выполнять на основном узле PT Email Security.

► Чтобы определить параметры установленного гипервизора Xen:

1. Определите максимальное количество VM, запускаемых на узлах с функцией поведенческого анализа:

```
sudo ptmsctl sandbox status
```

Появится таблица со списком узлов и максимальным для них количеством VM.

2. Определите объема памяти, выделяемый гостевой операционной системе каждой виртуальной машины:

```
sudo ptmsctl system components show -c sandbox-creator -p vm_memory_max_mb
```

В столбце `value` появившейся таблицы будет указан объем выделяемой памяти в мегабайтах.

## Распаковка архива с установщиком

► Чтобы распаковать архив с установщиком:

1. Скопируйте архив с установщиком в любой каталог на узле.
2. Перейдите в каталог с архивом, например:  
`cd /home/user/ptsb-installer`
3. Распакуйте архив, например:  
`tar pxvf ptsb.installer.debian-12-amd64.5.37.0.177.tar.gz`

## Удаление гипервизора Xen

► Чтобы удалить с узла гипервизор Xen:

1. Перейдите в каталог с установщиком PT Email Security, например:  
`cd /home/user/ptsb-installer`
2. Запустите скрипт удаления гипервизора Xen:  
`sudo ./xen/purge.sh`
3. При запросе на очистку каталога `/opt/ptms/sandbox-images` введите `n` для отказа и нажмите клавишу `Enter`.
4. По завершении работы скрипта нажмите клавишу `Enter`.  
Узел будет перезагружен.
5. Если требуется, введите логин и пароль загрузчика.

## Установка гипервизора Xen

**Внимание!** При установке гипервизора Xen необходимо указать тот же объем оперативной памяти, выделяемый гостевой операционной системе каждой виртуальной машины, что и для установленного ранее гипервизора. При необходимости вы сможете изменить это значение после завершения обновления.

► Чтобы установить гипервизор Xen на узле:

1. Перейдите в каталог с установщиком PT Email Security, например:  
`cd /home/user/ptsb-installer`
2. Запустите скрипт установки гипервизора Xen:
  - Если вы устанавливаете гипервизор на основном узле:  
`sudo xen/install.sh --vm-count <Количество ВМ> --memory-per-vm <Объем памяти ОС в ГБ>`
  - Если вы устанавливаете гипервизор на дополнительном узле:  
`sudo xen/install.sh --slave --vm-count <Количество ВМ> --memory-per-vm <Объем памяти ОС в ГБ>`

Например:

```
sudo xen/install.sh --slave --vm-count 15 --memory-per-vm 2
```

3. По завершении работы скрипта нажмите клавишу Enter.

Узел будет перезагружен.

4. Если требуется, введите логин и пароль загрузчика.

## 22. Удаление PT Email Security

Вы можете удалить продукт полностью со всех узлов кластера, удалить продукт на определенном узле или функцию поведенческого анализа на определенном узле. Удаление производится с помощью скриптов, которые входят в комплект поставки системы.

► Чтобы удалить PT Email Security:

1. Перейдите в каталог с установщиком:

Например:

```
cd /home/user/ptsb-installer
```

2. Выполните подходящую команду:

- Если требуется удалить продукт вместе с узлами кластера, выполните на каждом узле команду:

```
sudo ./purge-all.sh
```

**Примечание.** При выполнении команды `sudo ./purge-all.sh` не удаляются данные из БД. Для удаления данных из БД обратитесь в техническую поддержку Positive Technologies.

- Если требуется удалить только продукт без удаления узлов, перейдите на любой основной узел и выполните команду:

```
sudo ./purge-product.sh
```

- Если требуется удалить продукт на определенном узле кластера, перейдите на этот узел и выполните команду:

```
sudo ./purge-kubernetes.sh
```

**Внимание!** После выполнения команды `sudo ./purge-kubernetes.sh` в односерверной конфигурации потребуется переустановка продукта, так как он перестанет работать.

- Если требуется удалить функцию поведенческого анализа, перейдите на узел, на котором установлена эта функция, и выполните команду:

```
sudo ./xen/purge.sh
```

**Примечание.** Если функция поведенческого анализа установлена на нескольких узлах, то после выполнения команды она удалится только на том узле, на котором была выполнена команда. Вы также можете отключить функцию поведенческого анализа.

3. Подтвердите удаление.

PT Email Security или функция поведенческого анализа удалены.

## 23. Диагностика и устранение неисправностей

В этом разделе описываются возможные проблемы в работе PT Email Security и варианты их решения.

### Проблемы с действующей лицензией

На странице **Лицензия** отображается сообщение о проблемах с лицензией. Объекты проверяются, но базы средств проверки не обновляются.

**Внимание!** Вам нужно решить проблему в течение двух недель с момента ее появления. В противном случае проверка объектов прекратится.

Проблема может возникать в следующих случаях:

- С основного узла PT Email Security нет доступа по HTTPS к серверам обслуживания Positive Technologies.
- Служба лицензирования PT Email Security работает некорректно или была остановлена (например, кто-то вручную принудительно завершил ее процесс через консоль ОС).
- Был удален или поврежден файл с информацией о лицензии.
- Изменилась конфигурация узла сервера PT Email Security (например, изменились комплектующие сервера).

Для решения проблемы:

- Проверьте доступ к серверам обслуживания Positive Technologies.
- Обновите информацию о параметрах лицензии на странице **Лицензия**.

Если вам не удалось решить проблему, скачайте файлы журналов PT Email Security и отправьте их в техническую поддержку Positive Technologies.

### Не удается заменить лицензию

После замены лицензии, информация о ней не отображается на странице **Лицензия**.

Проблема может возникать в следующих случаях:

- С основного узла PT Email Security нет доступа по HTTPS к серверам обслуживания Positive Technologies.
- Неверно сконфигурирована лицензия.

Для решения проблемы:

- Проверьте доступ к серверам обслуживания Positive Technologies.
- Повторите замену лицензии.

Если вам не удалось решить проблему, скачайте файлы журналов PT Email Security и отправьте их в техническую поддержку Positive Technologies.

## После замены лицензии недоступен образ VM

После замены лицензии в параметрах проверки источника стал недоступен образ VM.

Проблема может возникать в случае удаления образа VM из лицензии.

Для решения проблемы в параметрах проверки источника выберите другой образ.

Если вы считаете, что образ VM был удален по ошибке или вам нужно вернуть его в лицензию, обратитесь в техническую поддержку Positive Technologies.

## Домен не зарегистрирован

При попытке входа по IP-адресу интерфейс PT Email Security недоступен, отображается сообщение «Домен не зарегистрирован».

Проблема может возникать в следующих случаях:

- Было подключено доменное имя.
- Была настроена трансляция сетевых адресов (NAT).

Для решения проблемы:

- Просмотрите подключенное доменное имя и повторите попытку входа, но уже не по IP-адресу, а по доменному имени.
- Отключите доменное имя и повторите попытку входа по IP-адресу.

Если вам не удалось решить проблему, обратитесь в техническую поддержку Positive Technologies.

## Не удастся запустить поведенческий анализ в интерактивном режиме

При попытке запустить поведенческий анализ в интерактивном режиме появляется сообщение о разрыве соединения.

Проблема может возникать, если доступ к интерфейсу PT Email Security выполняется через обратный прокси-сервер (reverse proxy), и на сервере отключено проксирование WebSocket-соединений.

Для решения проблемы настройте на обратном прокси-сервере вашей организации проксирование WebSocket-соединений. Ниже приведен пример настройки для прокси-сервера nginx.

► Чтобы настроить проксирование WebSocket-соединений для обратного прокси-сервера nginx:

1. Откройте конфигурационный файл `/etc/nginx/nginx.conf`.
2. В секцию `location` добавьте строки:
 

```
proxy_http_version 1.1;
```

```
proxy_set_header Upgrade $http_upgrade;
proxy_set_header Connection "upgrade";
```

3. Сохраните изменения и закройте файл.
4. Проверьте конфигурацию и примените изменения:
 

```
sudo nginx -t
sudo systemctl reload nginx
```

## Скачивание файлов журналов PT Email Security

Скачать файлы журналов можно через интерфейс PT Email Security. При скачивании файлы журналов добавляются в ZIP-архив с названием `ptms-logs-<Дата и время скачивания>-<Период>.zip`.

- ▶ Чтобы скачать файлы журналов через интерфейс,

в главном меню выберите  → **Скачать файлы журналов** → **<Период>**.

Файлы журналов собраны, добавлены в архив и скачаны на ваш компьютер.

С помощью скрипта из комплекта поставки вы можете собрать файлы журналов и сохранить их локально. Инструкцию необходимо выполнять на основном узле.

- ▶ Чтобы собрать файлы журналов с помощью скрипта:

1. Перейдите в каталог со скриптами установщика PT Email Security:
 

```
cd /home/user/ptsb-installer
```
2. Запустите скрипт `collect-logs.sh`:
 

```
sudo ./collect-logs.sh
```

Файлы журналов собраны, добавлены в ZIP-архив и скачаны на ваш компьютер.

## Скачивание файлов журналов источника

Вы можете скачать файлы журналов отдельного источника через интерфейс PT Email Security. При скачивании файлы журналов добавляются в ZIP-архив с названием `ptms-logs-<Дата и время скачивания>-<Период>.zip`.

**Примечание.** Для источников типа «Почтовый шлюз безопасности» скачивание файлов журналов недоступно.

- ▶ Чтобы скачать файлы журналов источника:

1. В главном меню выберите **Источники** → **Управление источниками**.
2. Нажмите на панель источника.
3. Нажмите кнопку **Скачать файлы журналов** → **<Период>**.

Файлы журналов источника собраны, добавлены в ZIP-архив и скачаны на ваш компьютер.

## 24. О технической поддержке

Гарантийная поддержка доступна для всех владельцев действующих лицензий на PT Email Security 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 предоставляет 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 7. 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. Сценарии отказов

Если развернута конфигурация PT Email Security с отказоустойчивым кластером, при выходе из строя любого аппаратного компонента (например, жесткого диска или модуля ОЗУ), физического сервера или при потере сетевого доступа к одному из узлов PT Email Security продукт продолжит обрабатывать задания на проверку файлов в штатном режиме. Однако при возникновении неполадок может быть потеряна часть данных, на короткое время некоторые компоненты могут стать недоступными или может ухудшиться их производительность.

Таблица 8. Сценарии отказов компонентов PT Email Security

| Компонент                             | Следствие отказа                                                 |                                                                                                       |                                                  |
|---------------------------------------|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|--------------------------------------------------|
|                                       | Потерянные данные                                                | Недоступность компонентов и функций                                                                   | Ухудшение производительности                     |
| Служба высокой доступности Keeralived | Результаты проверки файлов, которые проверялись на момент отказа | ICAP-сервер, почтовый сервер в режиме зеркалирования, почтовый сервер в режиме фильтрации — 40 секунд | —                                                |
| Веб-интерфейс                         | —                                                                | Веб-интерфейс — до 5 минут                                                                            | —                                                |
| База данных                           | Завершенные задания                                              | Запись в базу данных — 20 секунд                                                                      | —                                                |
| API базы данных                       | Текущие задания в веб-интерфейсе                                 | Запись в базу данных — 90 секунд                                                                      | —                                                |
| Ядро проверки                         | Часть файлов у трети текущих заданий                             | —                                                                                                     | —                                                |
| Хранилище файлов                      | Файлы                                                            | —                                                                                                     | Модуль поведенческого анализа, скачивание файлов |
| Модуль поведенческого анализа         | —                                                                | —                                                                                                     | Модуль поведенческого анализа                    |

# Глоссарий

## Checkme

Служба для проверки объектов по электронной почте. Пользователь может отправить объект или переслать письмо на специальный электронный адрес и получить результат проверки в ответном письме.

## Keepalived

Служба, которая обеспечивает доступ к продукту по одному IP-адресу, независимо от того, какой из узлов отказоустойчивого кластера активен.

## блокирующий режим

Режим проверки, при котором поступившие на проверку объекты блокируются продуктом до окончания проверки. В зависимости от вынесенного вердикта объект пропускается в информационную систему или удаляется (или помещается в карантин).

## источник для проверки

Интерфейс в информационной системе организации, с которого в продукт поступают объекты на проверку.

## карантин

Изолированная часть хранилища файлов, позволяющая сохранять заблокированные файлы с угрозами для последующего анализа.

## пассивный режим

Режим проверки, при котором поступившие на проверку объекты сразу пропускаются продуктом в информационную систему.

## режим зеркалирования

Режим работы почтового сервера, при котором продукт не влияет на почтовый трафик сервера. На проверку в продукт отправляются копии писем.

## режим ожидания

Режим проверки, при котором на проверку от источников в продукт поступают копии объектов, а их распространение контролирует пользователь или сторонняя система.

## режим фильтрации

Режим работы почтового сервера, при котором продукт может фильтровать почтовый трафик сервера. В зависимости от выбранного режима проверки продукт либо сразу возвращает почтовому серверу отправленное на проверку письмо (пассивный режим), либо блокирует его до окончания проверки (блокирующий режим).



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.