

Версия 2.2

Версия 2.2

**POSITIVE TECHNOLOGIES**

© АО "Позитив Текнолоджиз", 2021.

Настоящий документ является собственностью АО "Позитив Текнолоджиз" (далее также — "Позитив Текнолоджиз") 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 "Позитив Текнолоджиз".

Документ может быть изменен без предварительного уведомления.

Positive Technologies, Positive Hack Days, PTSECURITY, MaxPatrol, XSpider, SurfPatrol, N-Scope, Positive Technologies Application Firewall, Positive Technologies Application Inspector, Positive Technologies MultiScanner, Positive Technologies Reporting Portal являются зарегистрированными товарными знаками либо товарными знаками "Позитив Текнолоджиз".

Иные товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям. "Позитив Текнолоджиз" не аффилировано с такими правообладателями и не производит продукцию, маркированную такими знаками.

Дата редакции документа: 23.04.2021

Содержание

1.	Об этом документе	8
1.1.	Условные обозначения	8
1.2.	Другие источники информации о PT Sandbox	9
2.	О PT Sandbox	10
3.	Что нового в версии 2.2	11
4.	Принцип работы PT Sandbox	12
4.1.	Методы проверки файлов	12
4.2.	Источники файлов и электронных писем, передаваемых на проверку	13
4.3.	Режимы проверки файлов и электронных писем	14
4.4.	Особенности работы PT Sandbox с архивами	16
4.5.	Безопасность данных при передаче и обработке	16
4.6.	Компоненты PT Sandbox	16
4.7.	Обеспечение отказоустойчивости PT Sandbox	17
5.	Аппаратные и программные требования	18
5.1.	Аппаратные требования	18
5.2.	Программные требования	20
6.	Лицензирование	22
7.	Проверка доступа к серверам обслуживания PT Sandbox	23
8.	Установка PT Sandbox	24
8.1.	Создание внешнего установочного носителя из ISO-файла	25
8.2.	Установка основного узла с функцией поведенческого анализа	26
8.2.1.	Установка ОС и основного узла с функцией поведенческого анализа	27
8.2.2.	Процедура установки основного узла с функцией поведенческого анализа в подготовленной ОС	31
8.2.2.1.	Распаковка архива для установки основного узла с функцией поведенческого анализа	32
8.2.2.2.	Настройка подключения к прокси-серверу для основного узла с функцией поведенческого анализа	32
8.2.2.3.	Установка виртуального окружения для основного узла	33
8.2.2.4.	Установка основного узла с функцией поведенческого анализа в подготовленной ОС	34
8.3.	Установка основного узла без функции поведенческого анализа	35
8.3.1.	Процедура установки ОС и основного узла без функции поведенческого анализа	35
8.3.1.1.	Установка ОС и основного узла без функции поведенческого анализа	36
8.3.1.2.	Установка службы высокой доступности для основного узла	39
8.3.2.	Процедура установки основного узла без функции поведенческого анализа в подготовленной ОС	40
8.3.2.1.	Распаковка архива для установки основного узла без функции поведенческого анализа	41
8.3.2.2.	Настройка подключения к прокси-серверу для основного узла без функции поведенческого анализа	41
8.3.2.3.	Установка службы высокой доступности для основного узла в подготовленной ОС	42
8.3.2.4.	Установка основного узла без функции поведенческого анализа в подготовленной ОС	42
8.4.	Установка дополнительных узлов	43
8.4.1.	Процедура установки ОС и дополнительных узлов с функцией поведенческого анализа	44

8.4.1.1.	Установка ОС и виртуального окружения для дополнительного узла	44
8.4.1.2.	Получение команды для установки дополнительных узлов с функцией поведенческого анализа	48
8.4.1.3.	Установка дополнительного узла с функцией поведенческого анализа	49
8.4.2.	Процедура установки дополнительных узлов с функцией поведенческого анализа в подготовленной ОС	49
8.4.2.1.	Распаковка архива для установки дополнительного узла с функцией поведенческого анализа	50
8.4.2.2.	Настройка подключения к прокси-серверу для дополнительного узла с функцией поведенческого анализа	51
8.4.2.3.	Установка виртуального окружения для дополнительного узла	51
8.4.2.4.	Получение команды для установки дополнительных узлов с функцией поведенческого анализа в подготовленной ОС	52
8.4.2.5.	Установка дополнительного узла с функцией поведенческого анализа в подготовленной ОС	53
8.4.3.	Процедура установки ОС и дополнительных узлов без функции поведенческого анализа	54
8.4.3.1.	Установка ОС для дополнительного узла	54
8.4.3.2.	Установка службы высокой доступности для дополнительного узла	58
8.4.3.3.	Получение команды для установки дополнительных узлов без функции поведенческого анализа	58
8.4.3.4.	Установка дополнительного узла без функции поведенческого анализа	59
8.4.4.	Процедура установки дополнительных узлов без функции поведенческого анализа в подготовленной ОС	59
8.4.4.1.	Распаковка архива для установки дополнительного узла без функции поведенческого анализа	60
8.4.4.2.	Настройка подключения к прокси-серверу для дополнительного узла без функции поведенческого анализа	61
8.4.4.3.	Установка службы высокой доступности для дополнительного узла в подготовленной ОС	61
8.4.4.4.	Получение команды для установки дополнительных узлов без функции поведенческого анализа в подготовленной ОС	62
8.4.4.5.	Установка дополнительного узла без функции поведенческого анализа в подготовленной ОС	63
8.5.	Резервное копирование и восстановление параметров PT Sandbox	63
8.5.1.	Создание файла резервной копии параметров PT Sandbox	64
8.5.2.	Восстановление параметров PT Sandbox из файла резервной копии	64
9.	Первоначальная настройка PT Sandbox	65
9.1.	Вход в PT IAM	65
9.2.	Смена пароля суперпользователя	66
9.3.	Создание учетной записи администратора PT Sandbox	66
9.4.	Активация приобретенной лицензии	67
9.5.	Активация функции поведенческого анализа	68
9.6.	Настройка обновлений PT Sandbox с локального зеркала	70
9.6.1.	Установка локального сервера обновлений	71
9.6.2.	Активация лицензии на локальном сервере обновлений в демилитаризованной зоне	72
9.6.3.	Ручной перенос обновлений PT Sandbox в закрытый сегмент сети	73
9.6.4.	Настройка автоматического переноса обновлений PT Sandbox в закрытый сегмент сети	74
9.6.5.	Смена источника обновлений PT Sandbox на локальное зеркало	75
9.7.	Настройка подключения к прокси-серверу	76
9.8.	Настройка подключения к прокси-серверу с SSL-инспекцией	76

10.	Вход в PT Sandbox	79
11.	Интерфейс PT Sandbox	80
11.1.	Главное меню	80
11.2.	Центр уведомлений	81
11.3.	Страница со списком образов виртуальных машин	82
11.4.	Страница управления антивирусами	84
12.	Просмотр информации о лицензии PT Sandbox	86
13.	Замена лицензии	87
14.	Добавление источников для проверки	89
14.1.	Создание и настройка службы Checkme	89
14.2.	Настройка проверки трафика, поступающего от ICAP-сервера	91
14.2.1.	Создание и настройка ICAP-сервера PT Sandbox	92
14.2.2.	Настройка ICAP-клиента для интеграции с PT Sandbox	93
14.2.2.1.	Настройка проверки посредством ICAP в блокирующем режиме	93
14.2.2.2.	Настройка проверки посредством ICAP в режиме ожидания	94
14.2.2.3.	Настройка проверки посредством ICAP в пассивном режиме	95
14.2.2.4.	Настройка ICAP-клиента на примере прокси-сервера Squid	96
14.3.	Настройка проверки почтового трафика организации	97
14.3.1.	Подключение к почтовому серверу при помощи агента	98
14.3.1.1.	Установка почтового агента с параметрами по умолчанию	98
14.3.1.2.	Установка почтового агента с переопределенными параметрами	99
14.3.1.3.	Подключение PT Sandbox к почтовому агенту	100
14.3.2.	Настройка зеркалирования почтового трафика с помощью bcc	101
14.3.2.1.	Создание bcc-сервера PT Sandbox	101
14.3.2.2.	Настройка зеркалирования трафика с Postfix	103
14.3.2.3.	Настройка зеркалирования трафика с Exim	103
14.3.2.4.	Настройка зеркалирования трафика с Microsoft Exchange	104
14.3.3.	Настройка фильтрации почтового трафика	105
14.3.3.1.	Добавление источника для фильтрации почтового трафика	106
14.3.3.2.	Настройка правил маршрутизации почтового трафика с сервера Postfix	109
14.3.3.3.	Настройка правил маршрутизации почтового трафика с сервера Exim	110
14.4.	Настройка проверки файлов в общей папке	113
14.5.	Настройка проверки файлов в папке-шлюзе	114
14.6.	Настройка проверки трафика организации при помощи модуля захвата трафика	117
14.7.	Настройка проверки трафика организации при помощи PT NAD	118
15.	Управление источниками для проверки	120
15.1.	Изменение параметров источника для проверки	120
15.2.	Отключение источника для проверки	120
15.3.	Удаление источника для проверки	121
16.	Проверка файлов в PT Sandbox	122
16.1.	Проверка файлов через интерфейс PT Sandbox	122
16.2.	Отправка файлов на проверку по электронной почте	124
17.	Работа с результатами проверки файлов	126
17.1.	Просмотр результатов проверки	126
17.2.	Поиск результатов проверки	126
17.2.1.	Поиск заданий по времени создания	127
17.2.2.	Поиск заданий по уровням опасности файлов	127

17.2.3.	Поиск заданий по результатам проверки.....	128
17.2.4.	Поиск заданий по проверенным в них файлам	129
17.2.5.	Поиск заданий по файлам, проверявшимся или не проверявшимся методом поведенческого анализа	129
18.	Просмотр пользовательских ролей и прав доступа	130
19.	Работа с антивирусами	132
19.1.	Просмотр сведений об антивирусах	132
19.2.	Включение и выключение антивируса	132
19.3.	Установка дополнительного антивируса	133
19.4.	Обновление лицензии дополнительного антивируса	134
19.5.	Удаление дополнительного антивируса	135
19.6.	Обновление дополнительного антивируса	135
20.	Включение записи событий в журнал аудита	137
21.	Изменение объема хранилища для файлов заданий	138
22.	Настройка карантина	139
23.	Изменение срока хранения заданий на проверку	140
24.	Настройка отправки сообщений в системный журнал по протоколу syslog	141
25.	Управление узлами в многосерверной конфигурации PT Sandbox	142
25.1.	Добавление узла в кластер PT Sandbox	142
25.2.	Отключение дополнительного узла	142
25.3.	Отключение функции поведенческого анализа на основном узле	143
26.	Удаление почтового агента	144
27.	Диагностика и устранение неисправностей	145
27.1.	Устранение проблем с действующей лицензией	145
27.2.	Устранение проблем при замене лицензии	146
27.3.	Недоступен образ VM	147
27.4.	Сбор файлов журналов для отправки в техническую поддержку	148
28.	Обращение в службу технической поддержки	149
28.1.	Техническая поддержка на портале	149
28.2.	Техническая поддержка по телефону	149
28.3.	Время работы службы технической поддержки	150
28.4.	Как служба технической поддержки работает с запросами	150
28.4.1.	Предоставление информации для технической поддержки	150
28.4.2.	Типы запросов	151
28.4.3.	Время реакции и приоритизация запросов	152
28.4.4.	Выполнение работ по запросу	153
Приложение А.	Сценарии отказов	154
Приложение Б.	Сообщения, отправляемые в системный журнал по протоколу syslog	155
Б.1.	Сообщения о сканировании файлов	155
Б.1.1.	Сообщения <Идентификатор типа источника для проверки>.start	158
Б.1.1.1.	Сообщение check_me.start	159
Б.1.1.2.	Сообщение dpi.start	165
Б.1.1.3.	Сообщение email.start	170
Б.1.1.4.	Сообщение mail_bcc.start	176
Б.1.1.5.	Сообщение mail_gateway.start	181
Б.1.1.6.	Сообщение files_inbox.start	187
Б.1.1.7.	Сообщение files_monitor.start	190

Б.1.1.8.	Сообщение icap.start	193
Б.1.1.9.	Сообщение user_scan.start	205
Б.1.2.	Сообщение new_artifact	208
Б.1.3.	Сообщение scan_machine.new_object	210
Б.1.4.	Сообщение scan_machine.file_result.av	218
Б.1.5.	Сообщение scan_machine.file_result.melded	224
Б.1.6.	Сообщение scan_machine.final_result	229
Б.1.7.	Сообщения <Идентификатор типа источника для проверки>.finish	233
Б.1.7.1.	Сообщение check_me.finish	233
Б.1.7.2.	Сообщение dpi.finish	234
Б.1.7.3.	Сообщение email.finish	235
Б.1.7.4.	Сообщение mail_bcc.finish	235
Б.1.7.5.	Сообщение mail_gateway.finish	236
Б.1.7.6.	Сообщение files_inbox.finish	237
Б.1.7.7.	Сообщение files_monitor.finish	239
Б.1.7.8.	Сообщение icap.finish	239
Б.1.8.	Идентификаторы типов источников для проверки	240
Б.2.	Сообщение av.update	241
Б.3.	Сообщение retro_scan.start	242
Б.4.	Сообщение retro.artifact_verdict_changed	244
Б.5.	Кодовые имена антивирусов	248
Предметный указатель		249
Глоссарий		252

1. Об этом документе

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

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

Комплект документации PT Sandbox включает в себя следующие документы:

- Этот документ.
- Руководство оператора 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.
- Справочное руководство по публичному API — содержит информацию о доступных функциях сервиса публичного API в продукте.

В этом разделе

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

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

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример текста с условным обозначением	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 кнопку ОК	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом

Пример текста с условным обозначением	Описание
Выполните команду Stop-Service	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о PT Sandbox

Вы можете найти дополнительную информацию о PT Sandbox на сайте ptsecurity.com и на портале технической поддержки support.ptsecurity.com.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов "Позитив Текнолоджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в [службу технической поддержки](#) (см. раздел 28).

2. О PT Sandbox

Positive Technologies Sandbox (PT Sandbox) — это программный комплекс, предназначенный для проверки файлов и электронных писем на предмет угрозы информационной безопасности. С помощью PT Sandbox пользователи и операторы безопасности могут получить оценку опасности, исходящей от файлов и электронных писем, поступающих в информационную систему извне, отправляемых за ее пределы или уже находящихся внутри нее.

Функции PT Sandbox:

- проверка файлов с помощью методов поведенческого и статического анализа;
- проверка файлов, поступающих в информационную систему извне, отправляемых за ее пределы или уже находящихся внутри нее;
- недопуск в информационную систему файлов и электронных писем, которые по результатам проверки представляют угрозу;
- автоматическое повторное сканирование файлов после обновления антивирусных баз;
- создание в интерфейсе PT Sandbox графических отчетов о результатах проверки.

PT Sandbox позволяет вам:

- добавлять источники для проверки файлов и настраивать подключение к ним;
- изменять объем хранилища файлов;
- настраивать отправку результатов проверки файлов на syslog-сервер;
- управлять антивирусами, которые используются PT Sandbox для сканирования файлов;
- просматривать информацию о лицензии PT Sandbox, добавлять и заменять ее.
- просматривать результаты проверки файлов.

3. Что нового в версии 2.2

Ниже приводится список изменений, которые появились в PT Sandbox версии 2.2.

Отображение статусов образов VM

В процессе работы продукта один и тот же образ может быть установлен на разных узлах. Теперь на странице **Образы VM** по ссылке **Статусы по узлам** вы можете отслеживать, на каких узлах образ VM загружается, устанавливается или обновляется, а на каких доступен для использования.

Подробное описание см. в разделе "[Страница со списком образов виртуальных машин \(см. раздел 11.3\)](#)" Руководства администратора.

Изменение логики информирования об окончании действия лицензии

Начиная с версии 2.2 информационное сообщение об истечении срока действия лицензии подсвечивается красным цветом за семь дней до окончания срока действия.

Мастер установки продукта в подготовленной операционной системе

Теперь установка продукта в подготовленной операционной системе выполняется с помощью мастера установки. Новый мастер установки помогает правильно указать источник обновления продукта и корректно ввести серийный номер лицензии.

4. Принцип работы PT Sandbox

PT Sandbox проверяет файлы следующим образом:

1. Файл поступает в PT Sandbox с одного из источников для проверки. Если на проверку поступает электронное письмо, PT Sandbox рассматривает его как файл-контейнер, содержащий файл с текстом письма и файлы вложений.
2. PT Sandbox обрабатывает файл:
 - вычисляет хеш-суммы файла (MD5, SHA-1 и SHA-256), которые позволяют однозначно идентифицировать файл;
 - подсчитывает размер файла;
 - определяет MIME-тип файла.

Если файл большой, обработка может занять продолжительное время. PT Sandbox отправляет файл на проверку только по завершении его обработки.

3. PT Sandbox проверяет файл и все файлы, которые были из него извлечены.
4. Если размер файла не превышает 1 ГБ и 1% от максимально допустимого объема хранилища файлов, PT Sandbox помещает его в хранилище.

Примечание. Извлеченные из архивов файлы и вложения электронных писем сохраняются в хранилище как отдельные файлы.

5. В зависимости от результатов, режима и параметров проверки PT Sandbox пропускает проверенные файл или электронное письмо в информационную систему или блокирует их распространение.

В этом разделе

[Методы проверки файлов \(см. раздел 4.1\)](#)

[Источники файлов и электронных писем, передаваемых на проверку \(см. раздел 4.2\)](#)

[Режимы проверки файлов и электронных писем \(см. раздел 4.3\)](#)

[Особенности работы PT Sandbox с архивами \(см. раздел 4.4\)](#)

[Безопасность данных при передаче и обработке \(см. раздел 4.5\)](#)

[Компоненты PT Sandbox \(см. раздел 4.6\)](#)

[Обеспечение отказоустойчивости PT Sandbox \(см. раздел 4.7\)](#)

4.1. Методы проверки файлов

Для получения информации об опасности файлов и электронных писем PT Sandbox проверяет их методами поведенческого и статического анализа.

Поведенческий анализ

В ходе поведенческого анализа PT Sandbox запускает файл в операционной системе на виртуальной машине и записывает его поведение, включая:

- запуск процессов;
- выполнение интернет-запросов;
- изменения системного реестра.

Для выявления опасного и потенциально опасного поведения файла PT Sandbox применяет правила из базы знаний экспертного центра "Позитив Текнолоджиз". Правила определяют вредоносное ПО по совокупности действий и признаков, которые могут указывать на попытки нарушения безопасности. Все созданные файлом артефакты в свою очередь сохраняются в хранилище файлов и подвергаются статическому анализу.

Статический анализ

В ходе статического анализа PT Sandbox выполняет антивирусное сканирование и экспертную оценку файлов.

Под антивирусным сканированием понимается многопоточный анализ файлов набором антивирусных программ сторонних разработчиков. В PT Sandbox существует функция автоматического повторного сканирования файлов после обновления антивирусных баз. Для повышения качества обнаружения угроз вы можете установить антивирусы в дополнение к стандартному набору.

Под экспертной оценкой понимается проверка файлов по технологии PT ESC, в основе которой лежат правила из базы знаний экспертного центра "Позитив Текнолоджиз".

4.2. Источники файлов и электронных писем, передаваемых на проверку

Источник для проверки — это интерфейс в информационной системе организации, с которого PT Sandbox получает файлы и (или) электронные письма для проверки.

В PT Sandbox предусмотрены источники следующих типов:

- Веб-интерфейс — компонент PT Sandbox, пользовательский графический веб-интерфейс, с помощью которого пользователи и операторы безопасности самостоятельно загружают на проверку файлы, сохраненные на их компьютерах, и получают результаты проверки.
- Checkme — служба PT Sandbox, с помощью которой сотрудники организации самостоятельно отправляют файлы на [проверку по электронной почте \(см. раздел 16.2\)](#) и получают результаты проверки в ответных письмах.
- Почтовый сервер с установленным агентом — сервер Microsoft Exchange с установленным на нем почтовым агентом PT Sandbox. Почтовый агент отвечает за передачу писем на проверку и за блокировку писем, представляющих угрозу.

- Почтовый сервер в режиме зеркалирования — почтовый сервер, который отправляет письма на проверку в PT Sandbox в виде скрытых копий.
- Почтовый сервер в режиме фильтрации — почтовый сервер Postfix или Exim, который отправляет письма на фильтрацию в PT Sandbox.
- Общая папка — папка с настроенным общим доступом.
- Папка-шлюз — общая папка, в которую операторы безопасности или сторонние системы помещают файлы для проверки в PT Sandbox. По результатам проверки PT Sandbox перемещает файлы из папки-шлюза в общую папку с безопасными файлами или в общую папку карантина.
- ICAP-сервер — компонент PT Sandbox, при помощи которого осуществляется интеграция с Positive Technologies Application Firewall (PT AF), системами обнаружения и предотвращения вторжений (IDS, IPS), прокси-серверами и другими средствами, поддерживающими ICAP.
- Модуль захвата трафика (DPI) — компонент PT Sandbox, который извлекает файлы из сетевого трафика организации.
- Positive Technologies Network Attack Discovery (PT NAD) — программно-аппаратный комплекс, который захватывает и анализирует сетевой трафик, чтобы выявлять аномальную сетевую активность и сложные целенаправленные атаки в сетевых взаимодействиях и блокировать такие взаимодействия.

По умолчанию файлы поступают для проверки только с веб-интерфейса PT Sandbox. Вы можете подключать источники других типов, а операторы безопасности — настраивать проверку файлов, поступающих с каждого отдельного источника.

См. также

[Добавление источников для проверки \(см. раздел 14\)](#)

[Управление источниками для проверки \(см. раздел 15\)](#)

4.3. Режимы проверки файлов и электронных писем

В зависимости от требований, предъявляемых службой информационной безопасности организации к PT Sandbox, проверка файлов и электронных писем может производиться в блокирующем режиме, режиме ожидания или пассивном режиме.

Блокирующий режим

В блокирующем режиме PT Sandbox ограничивает распространение файлов и электронных писем, передаваемых в информационную систему извне или внутри нее, на время их проверки. После проверки распространение всех файлов из одного задания блокируется, если хотя бы один файл в этом задании определяется как опасный.

Примечание. Использование блокирующего режима может быть ограничено [лицензией \(см. раздел 12\)](#).

Режим ожидания

В режиме ожидания PT Sandbox задерживает файлы и электронные письма на время их проверки, но не ограничивает их распространение в информационной системе. В этом режиме функцию пропуска или блокировки файлов выполняет сторонняя система на основании результатов проверки, полученных от PT Sandbox по ICAP. Также в этом режиме выполняется проверка файлов, которые уже находятся в информационной системе или отправляются на проверку пользователями и операторами безопасности.

Пассивный режим

В пассивном режиме файлы и электронные письма отправляются на проверку в PT Sandbox и одновременно пропускаются в информационную систему. Операторы безопасности могут затем проанализировать результаты проверки и запретить последующее распространение представляющих угрозу файлов.

Режим проверки настраивается оператором безопасности в зависимости от конкретного источника, на который поступил файл или письмо. Каждый тип источника поддерживает свой набор режимов проверки.

Таблица 2. Режимы проверки в зависимости от типа источника

Тип источника	Блокирующий режим	Режим ожидания	Пассивный режим
Веб-интерфейс	×	✓	×
Служба Checkme	×	✓	×
Почтовый сервер с установленным агентом	✓	×	✓
Почтовый сервер в режиме зеркалирования	×	×	✓
Почтовый сервер в режиме фильтрации	✓	×	✓
Общая папка	×	×	✓
Папка-шлюз	✓	×	×
ICAP-сервер	✓	✓	✓
Модуль захвата трафика	×	×	✓
PT NAD	×	×	✓

См. также

[Добавление источников для проверки \(см. раздел 14\)](#)

[Управление источниками для проверки \(см. раздел 15\)](#)

4.4. Особенности работы PT Sandbox с архивами

PT Sandbox извлекает файлы из архивов форматов RAR, 7z, ZIP и Tar.

По умолчанию PT Sandbox распаковывает архивы до второго уровня вложенности. Это означает, что если в отправленный на проверку архив вложены другие архивы, то они будут также распакованы с проверкой извлеченных из них файлов. Архивы последующих уровней вложенности PT Sandbox будет сохранять в хранилище файлов в нераспакованном виде, но отправлять на антивирусное сканирование запакованные в них файлы. Вы можете изменить стандартную глубину распаковки архивов при отправке файлов на проверку через интерфейс.

Для проверки зашифрованного архива необходим пароль. В PT Sandbox существует список стандартных паролей, который задается сотрудниками службы информационной безопасности. Если вы загружаете архив, зашифрованный нестандартным паролем, вы можете ввести этот пароль при загрузке файла через интерфейс или в теле письма при отправке файла по электронной почте. Архивы, которые PT Sandbox не удастся расшифровать, не проверяются и сохраняются в хранилище файлов без распаковки.

4.5. Безопасность данных при передаче и обработке

При работе с интерфейсом все передаваемые данные защищаются при помощи HTTPS с использованием SSL-сертификата. SSL-сертификат может быть как самоподписанным, так и выданным официальным центром сертификации.

Любые файлы, скачиваемые оператором безопасности из хранилища файлов, помещаются в ZIP-архивы с паролем infected.

4.6. Компоненты PT Sandbox

PT Sandbox состоит из следующих компонентов:

- Служба высокой доступности — компонент, который обеспечивает доступность всех узлов PT Sandbox на одном IP-адресе.
- Веб-интерфейс — компонент графического пользовательского интерфейса PT Sandbox, доступный в браузере.
- База данных — компонент под управлением СУБД PostgreSQL, который обеспечивает хранение данных о заданиях и файлах.
- API базы данных — компонент, который обеспечивает отображение информации из базы данных в веб-интерфейсе PT Sandbox.

- Ядро проверки — компонент, который отправляет файлы на сканирование антивирусами и передает файлы в виртуальные машины, а также контролирует выполнение проверки файлов.
- Хранилище файлов — компонент, отвечающий за хранение полученных извне файлов на жестком диске.
- Модуль поведенческого анализа — компонент, отвечающий за [проверку файлов методом поведенческого анализа \(см. раздел 4.1\)](#).

4.7. Обеспечение отказоустойчивости PT Sandbox

Для повышения надежности PT Sandbox, обеспечения сохранности данных и непрерывности работы в случае выхода из строя отдельных компонентов PT Sandbox продукт устанавливается на три узла, которыми могут быть виртуальные машины или физические серверы. 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 Sandbox продукт продолжит обрабатывать задачи на проверку файлов в штатном режиме.

5. Аппаратные и программные требования

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

В этом разделе

[Аппаратные требования \(см. раздел 5.1\)](#)

[Программные требования \(см. раздел 5.2\)](#)

5.1. Аппаратные требования

Аппаратные требования для работы PT Sandbox могут меняться в зависимости от желаемой производительности PT Sandbox, от максимального объема хранилища файлов и от планируемой нагрузки.

Таблица 3. Минимальные аппаратные требования¹

Параметр	Значение
Количество потоков процессора	16
Объем ОЗУ	32 ГБ
Свободное место	500 ГБ

Таблица 4. Рекомендуемые аппаратные требования²

Аппаратное обеспечение	Параметр	Значение
Процессоры	Количество	2 × Intel Xeon Platinum 8268
	Частота	2,9 ГГц
	Потоков	48
ОЗУ	Объем	128 ГБ
Жесткие диски	Объем	4 × 4 ТБ
	Скорость	7200 об/мин
	Интерфейс	NLSAS
	Уровень RAID	RAID 5
Твердотельные накопители	Объем	4 × 960 ГБ

¹ Рассчитаны для односерверной конфигурации, в которой для поведенческого анализа может быть развернуто не более двух одновременно работающих виртуальных машин и допустима только самостоятельная отправка файлов на проверку.

² Рассчитаны на выполнение поведенческого анализа в десяти одновременно работающих виртуальных машинах.

Аппаратное обеспечение	Параметр	Значение
	Интерфейс	SAS
	Уровень RAID	RAID 5
	Тип	Mixed Use
Сетевые платы	Количество	2 × Broadcom 5720, 2 × Broadcom 57416, 2 × Intel I350

Вы можете самостоятельно рассчитать минимальное необходимое количество оперативной памяти, потоков процессора и свободного места (см. таблицу 5). Расчет выполняется на основании:

- планируемой [конфигурации](#) (см. [раздел 8](#));
- количества образов виртуальных машин (ВМ), определенного лицензией;
- максимального количества одновременно работающих виртуальных машин для выполнения в них поведенческого анализа.

Примечание. В PT Sandbox может работать не более 15 виртуальных машин одновременно.

Таблица 5. Самостоятельный расчет аппаратных ресурсов

Конфигурация		ОЗУ, ГБ	Потоков процессора	Свободного места, ГБ
Односерверная		Кол-во ВМ × 4 + 19	Кол-во ВМ × 3 + 9	Кол-во образов ВМ × 28 + 352
Многосерверная	Узел без функции поведенческого анализа	15	6	Кол-во образов ВМ × 16 + 340
	Узел с функцией поведенческого анализа	Кол-во ВМ × 4 + 5	Кол-во ВМ × 3 + 4	Кол-во образов ВМ × 12 + 302

Требования для модуля захвата трафика

Модуль захвата трафика работает только на физическом сервере. Минимальные аппаратные требования для работы модуля:

- процессор с Advanced Vector Extensions (AVX);
- сетевая плата на чипе Intel, например Intel Ethernet I350 DP 1Gb или Intel X520 DP 10Gb.

Для захвата трафика со скоростью 1 Гбит/с модуль дополнительно требует минимум 8 потоков процессора и 32 ГБ ОЗУ.

Внимание! При использовании модуля захвата трафика недоступно создание [кластера высокой доступности \(см. раздел 4.7\)](#). В этом случае вы можете устанавливать дополнительные узлы PT Sandbox только для поведенческого анализа.

5.2. Программные требования

Общие программные требования:

- Есть доступ по HTTPS к поддоменам ptsecurity.com.
- Установлено точное время.
- Настроен статический IP-адрес.
- В многосерверной конфигурации PT Sandbox каждый узел должен иметь уникальное название (hostname).

Примечание. При установке PT Sandbox вместе с операционной системой основному узлу автоматически присваивается название ptsb, дополнительным узлам — ptsb-`<Хеш-сумма времени установки узла>`, например ptsb-271fec.

Требования к операционной системе

Вы можете установить PT Sandbox в подготовленной операционной системе. В этом случае операционной системой должна быть 64-разрядная версия Ubuntu Server 18.04.

При подготовке операционной системы нужно разметить дисковое пространство (см. таблицу 6). Разделы для операционной системы и программных модулей PT Sandbox рекомендуется создавать на твердотельном накопителе, а раздел для хранилища файлов — на жестком диске.

В подготовленной операционной системе не должно быть раздела или файла подкачки. Иначе PT Sandbox не может быть установлен.

Таблица 6. Рекомендуемая схема дисковой разметки

Назначение раздела	Точка монтирования	Минимальный размер, ГБ ³		Рекомендуемый размер, ГБ ⁴
		Узел с функцией поведенческого анализа	Узел без функции поведенческого анализа	
Операционная система	/	240		240
Программные модули PT Sandbox	/opt	Кол-во образов VM × 12 + 62	50	1024

³ Рассчитан для работы PT Sandbox под низкой нагрузкой: файлы отправляются на проверку только самостоятельно без их длительного хранения в хранилище.

⁴ Рассчитан для работы всех функций PT Sandbox.

Назначение раздела	Точка монтирования	Минимальный размер, ГБ ³		Рекомендуемый размер, ГБ ⁴
		Узел с функцией поведенческого анализа	Узел без функции поведенческого анализа	
Хранилище файлов	/opt/pt-ms/ var/ artifactory	Кол-во образов VM × 16 + 50		1024 и более
Пользовательские файлы	/home	—		100

Требования для функции поведенческого анализа

Сервер, на котором выполняется установка узла PT Sandbox с функцией поведенческого анализа, должен быть запущен с помощью BIOS. Запуск из-под UEFI в текущей версии не поддерживается.

Если узел устанавливается на физический сервер, в параметрах BIOS должна быть включена аппаратная поддержка виртуализации (например, Intel Virtualization Technology).

Если узел устанавливается на виртуальную машину, виртуальное окружение должно соответствовать следующим требованиям:

- гипервизор — VMware ESXi версии 6.0 или выше;
- аппаратная версия виртуальной машины — 11 или выше;
- в гостевой операционной системе включена аппаратная поддержка виртуализации.

Рекомендации по разрешению экрана и браузеру

Для работы с интерфейсом PT Sandbox рекомендуется использовать монитор с разрешением 1920 × 1080 пикселей и один из следующих браузеров:

- Google Chrome версии 49 или выше;
- Mozilla Firefox версии 45 или выше.

6. Лицензирование

Для работы PT Sandbox и его защиты от нелегального использования нужна действующая лицензия.

Чтобы использовать PT Sandbox, вам нужно указать серийный номер лицензии, приобретенной вашей организацией.

Примечание. Одна лицензия может быть активирована только в одном экземпляре PT Sandbox. В одном экземпляре PT Sandbox одновременно может действовать только одна лицензия.

Приобретенная лицензия определяет:

- доступную конфигурацию PT Sandbox, включая информацию о допустимом количестве дополнительных узлов и их типах;
- доступные типы [источников для проверки \(см. раздел 4.2\)](#), с информацией о лимите их производительности;
- доступные образы виртуальных машин.

При заказе лицензии устанавливается дата окончания срока ее действия. Начиная с этой даты предоставляется 30-дневный льготный период, в течение которого работают все функции PT Sandbox. По истечении льготного периода проверка отключается и файлы, представляющие угрозу, перестают блокироваться (если блокирующий режим был определен лицензией).

При необходимости параметры приобретенной лицензии могут быть изменены, например для продления срока работы PT Sandbox или добавления нового типа источника для проверки. Для этого нужно обратиться в службу технической поддержки "Позитив Текнолоджиз".

См. также

[Просмотр информации о лицензии PT Sandbox \(см. раздел 12\)](#)

[Активация приобретенной лицензии \(см. раздел 9.4\)](#)

[Замена лицензии \(см. раздел 13\)](#)

7. Проверка доступа к серверам обслуживания PT Sandbox

В процессе установки, обновления и проверки лицензии PT Sandbox может обращаться к серверам на разных поддоменах ptsecurity.com. Если в вашей организации используется ПО, ограничивающее сетевой доступ, вам необходимо убедиться, что со всех узлов с PT Sandbox разрешен доступ по HTTPS к любым поддоменам ptsecurity.com.

► Чтобы проверить доступ к серверам обслуживания PT Sandbox:

1. Проверьте подключение к поддоменам ptsecurity.com. Это можно сделать, проверив доступ к поддомену update.ptsecurity.com:

```
wget -Sq -O /dev/null https://update.ptsecurity.com
```

Результат выполнения команды будет начинаться со строки HTTP/1.1 403 Forbidden.

2. Проверьте подключение к update-registry-cloud4y.ptsecurity.com:

```
curl -iL https://update-registry-cloud4y.ptsecurity.com/v2
```

Результат выполнения команды будет начинаться со строки HTTP/1.1 301 Moved Permanently.

Если результат выполнения команд отличается от указанного выше, вам нужно обеспечить доступ, а затем проверить его повторно.

Внимание! Если в вашей организации используется ПО, ограничивающее сетевой доступ, убедитесь, что доступ обеспечен не только к update.ptsecurity.com, а к любым поддоменам ptsecurity.com.

8. Установка PT Sandbox

Установка PT Sandbox зависит от выбранной вами конфигурации PT Sandbox.

Существует два варианта конфигурации PT Sandbox:

- **Односерверная конфигурация.** PT Sandbox работает на одном узле, которым может быть физический сервер или виртуальная машина.

Односерверная конфигурация используется, если аппаратных ресурсов одного узла достаточно для проверки файлов со скоростью, приемлемой для службы информационной безопасности организации.

- **Многосерверная конфигурация.** PT Sandbox работает на нескольких узлах, которыми могут быть физические серверы или виртуальные машины. Узел, на котором изначально (впервые) устанавливался PT Sandbox, называется основным. Любой узел, который устанавливается после основного, называется дополнительным.

Многосерверная конфигурация может использоваться для ускорения поведенческого анализа. В этом случае сокращается время проведения поведенческого анализа благодаря увеличению количества потоков проверки. Увеличение количества потоков достигается за счет распределения задач поведенческого анализа между несколькими узлами, выделенными специально для этой цели.

Также многосерверная конфигурация может использоваться для [создания кластера высокой доступности \(см. раздел 4.7\)](#).

Для установки PT Sandbox вместе с операционной системой вам понадобится установочный ISO-файл, входящий в комплект поставки продукта. ISO-файл имеет название вида ptsb-2.2.<Версия сборки>-<Время создания сборки>.iso, например ptsb-2.2.0.136-20210111T080604.iso. Установка выполняется аналогично установке любой операционной системы — с помощью монтирования ISO-файла при настройке виртуальной машины или путем [создания внешнего установочного носителя из этого файла \(см. раздел 8.1\)](#).

Для установки PT Sandbox в подготовленной операционной системе нужно использовать архив с установщиком PT Sandbox. Архив имеет название ptsb.installer.<Версия продукта>.tar.gz, например ptsb.installer.2.2.0.6.tar.gz.

- Чтобы установить PT Sandbox в односерверной конфигурации,
[установите основной узел с функцией поведенческого анализа \(см. раздел 8.2\)](#).

- ▶ Чтобы установить PT Sandbox в многосерверной конфигурации без создания кластера высокой доступности:
 1. Если вы планируете устанавливать узлы PT Sandbox в подготовленных операционных системах, убедитесь, что названия узлов (hostnames) в этих операционных системах уникальны в разворачиваемом кластере PT Sandbox.
 2. Установите основной узел [с функцией поведенческого анализа \(см. раздел 8.2\)](#) или [без этой функции \(см. раздел 8.3\)](#).
 3. Установите необходимое количество дополнительных узлов с функцией поведенческого анализа [вместе с операционной системой \(см. раздел 8.4.1\)](#) или [в подготовленной операционной системе \(см. раздел 8.4.2\)](#).
- ▶ Чтобы установить PT Sandbox в многосерверной конфигурации для создания кластера высокой доступности:
 1. Если вы планируете устанавливать узлы PT Sandbox в подготовленных операционных системах, убедитесь, что названия узлов (hostnames) в этих операционных системах уникальны в разворачиваемом кластере PT Sandbox.
 2. [Установите основной узел без функции поведенческого анализа \(см. раздел 8.3\)](#).
 3. Установите первый дополнительный узел без функции поведенческого анализа [вместе с операционной системой \(см. раздел 8.4.3\)](#) или [в подготовленной операционной системе \(см. раздел 8.4.4\)](#).
 4. Установите второй дополнительный узел без функции поведенческого анализа [вместе с операционной системой \(см. раздел 8.4.3\)](#) или [в подготовленной операционной системе \(см. раздел 8.4.4\)](#).
 5. Установите необходимое количество дополнительных узлов с функцией поведенческого анализа [вместе с операционной системой \(см. раздел 8.4.1\)](#) или [в подготовленной операционной системе \(см. раздел 8.4.2\)](#).

В этом разделе

[Создание внешнего установочного носителя из ISO-файла \(см. раздел 8.1\)](#)

[Установка основного узла с функцией поведенческого анализа \(см. раздел 8.2\)](#)

[Установка основного узла без функции поведенческого анализа \(см. раздел 8.3\)](#)

[Установка дополнительных узлов \(см. раздел 8.4\)](#)

[Резервное копирование и восстановление параметров PT Sandbox \(см. раздел 8.5\)](#)

8.1. Создание внешнего установочного носителя из ISO-файла

В этом разделе приводятся инструкции по созданию внешнего установочного носителя из ISO-файла с установщиком PT Sandbox.

Внимание! Не рекомендуется создание установочного носителя способами, отличными от приведенных ниже, так как они не гарантируют последующую корректную установку продукта.

Вы можете создать установочный носитель в операционных системах Windows и Linux.

Для создания установочного носителя в операционной системе Windows рекомендуется использовать программу Win32 Disk Imager. Другие программы могут менять структуру файлов образа или конвертировать файловую систему носителя в FAT32, из-за чего установщик PT Sandbox не работает.

► Чтобы создать установочный носитель в операционной системе Linux:

1. Размонтируйте файловые системы подключенного внешнего носителя информации:

```
sudo umount <Название устройства, соответствующее внешнему носителю информации>
```

Например:

```
sudo umount /dev/sdf
```

Примечание. Вы можете получить список названий подключенных устройств по команде `lsblk`.

2. Запишите установщик продукта на внешний носитель:

```
sudo cp <Путь к установочному ISO-файлу> <Название устройства, соответствующее внешнему носителю информации>
```

Внимание! Все данные на устройстве будут уничтожены. Внимательно указывайте название устройства, потому что в случае ошибки вы можете потерять нужную вам информацию.

Например:

```
sudo cp /home/user/ptsb-2.2.0.136-20210111T080604.iso /dev/sdf
```

8.2. Установка основного узла с функцией поведенческого анализа

В этом разделе приводятся инструкции по установке основного узла PT Sandbox для выполнения на нем поведенческого анализа файлов. Вам нужно выбрать один из двух вариантов установки в зависимости от того, нужно ли вам установить основной узел вместе с операционной системой или установка должна выполняться в уже существующей операционной системе.

В этом разделе

[Установка ОС и основного узла с функцией поведенческого анализа \(см. раздел 8.2.1\)](#)

[Процедура установки основного узла с функцией поведенческого анализа в подготовленной ОС \(см. раздел 8.2.2\)](#)

8.2.1. Установка ОС и основного узла с функцией поведенческого анализа

Вы можете установить основной узел PT Sandbox на физический сервер или виртуальную машину без установленной операционной системы, чтобы этот узел выполнял поведенческий анализ файлов.

Для установки вам нужно использовать установочный ISO-файл, входящий в комплект поставки PT Sandbox. Файл имеет название вида `ptsb-2.2.<Версия сборки>-<Время создания сборки>.iso`, например `ptsb-2.2.0.136-20210111T080604.iso`. Установка выполняется аналогично установке любой операционной системы — путем [создания установочного носителя из ISO-файла \(см. раздел 8.1\)](#) или с помощью монтирования этого файла при настройке виртуальной машины. При запуске установки автоматически устанавливается и настраивается 64-разрядная версия Ubuntu Server 18.04, после чего настраивается виртуальное окружение для поведенческого анализа и устанавливается основной узел PT Sandbox.

Перед установкой нужно убедиться, что физический сервер или виртуальная машина, на которые вы планируете устанавливать PT Sandbox, соответствуют [аппаратным и программным требованиям \(см. раздел 5\)](#).

- Чтобы установить операционную систему и основной узел PT Sandbox с функцией поведенческого анализа:

1. Запустите виртуальную машину со смонтированным установочным ISO-файлом PT Sandbox или сервер с установочным носителем, созданным из этого ISO-файла.

Откроется главное меню установщика PT Sandbox.

2. Выберите пункт **Install new instance of PT Sandbox with behavioral analysis** и нажмите клавишу Enter.

Начнется загрузка установщика. По окончании загрузки установщик проверит сервер или виртуальную машину на соответствие минимальным системным требованиям для выполнения на них поведенческого анализа.

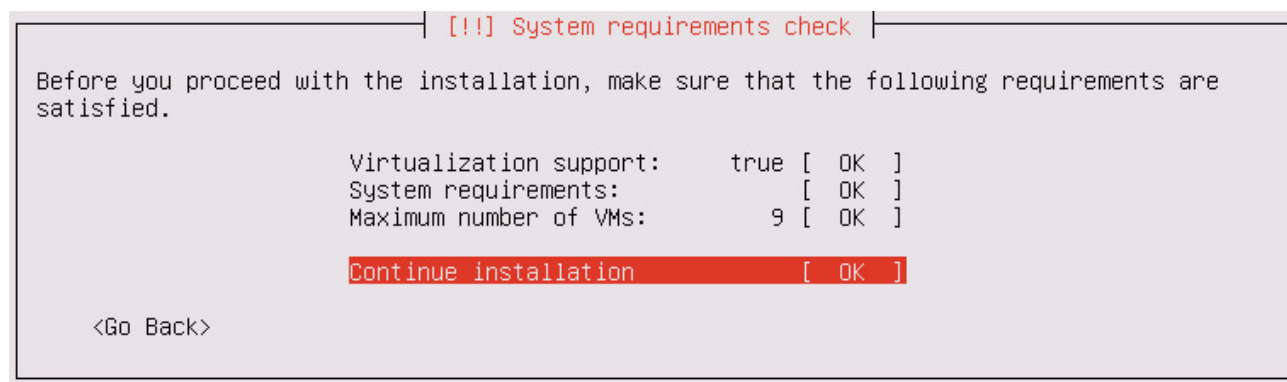


Рисунок 1. Проверка системных требований

В случае успешной проверки все пункты будут помечены словом "OK". При наличии хотя бы одного слова "FAILED" вы не сможете продолжить установку. Для получения подробной информации нужно выбрать соответствующий пункт.

3. Если вам нужно уменьшить максимальное количество одновременно работающих виртуальных машин, в которых выполняется поведенческий анализ, выберите пункт **Maximum number of VMs**, в появившемся поле введите новое число, после чего выберите вариант **Continue**.

Уменьшение может понадобиться, если вам нужно освободить часть аппаратных ресурсов под другие задачи.

Примечание. По умолчанию установщик указывает максимально допустимое значение, рассчитанное исходя из доступных аппаратных ресурсов.

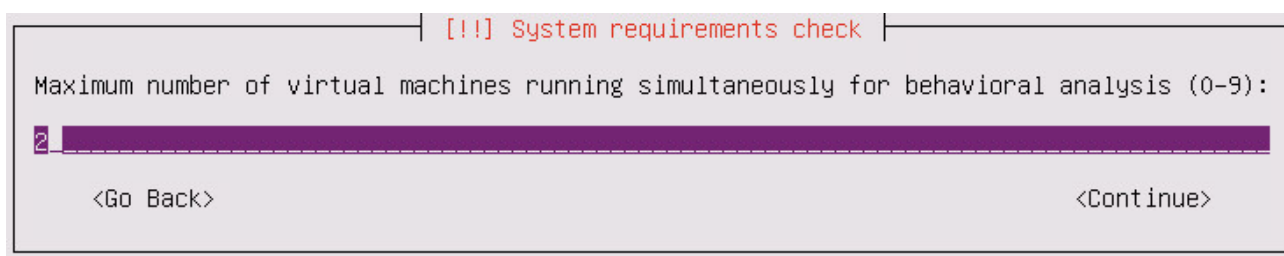


Рисунок 2. Изменение максимального количества виртуальных машин

4. Выберите вариант **Continue installation**.

Если физический сервер или виртуальная машина, на которые выполняется установка, не подключены к DHCP-серверу, установщик предложит вручную настроить сетевые параметры.



Рисунок 3. Сообщение о невозможности автоматической настройки сетевых параметров

5. Для ручной настройки сетевых параметров:

- Выберите пункт **Configure network manually** и нажмите клавишу Enter.

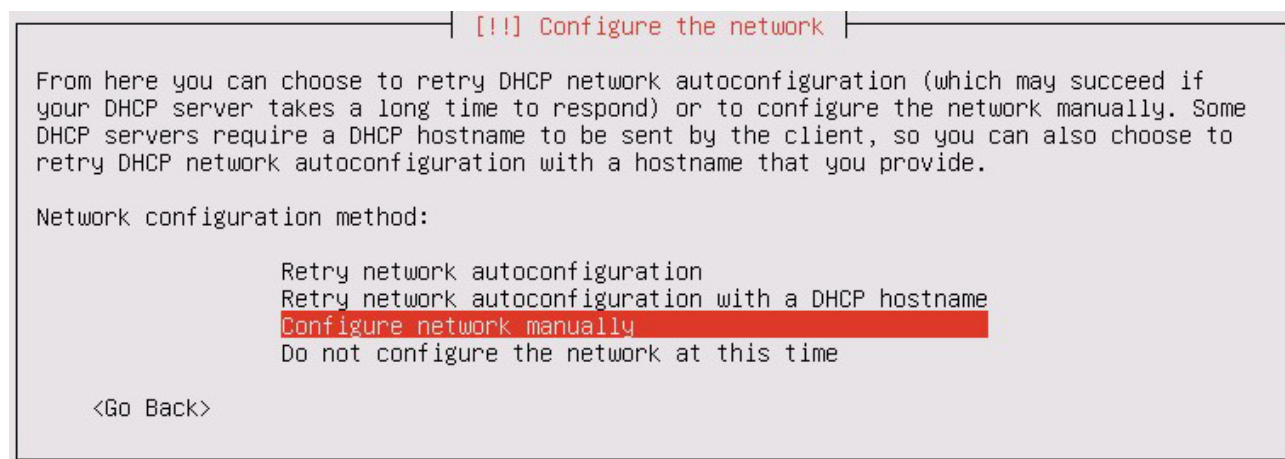


Рисунок 4. Ручная настройка сетевых параметров

- Введите IP-адрес физического сервера или виртуальной машины, на которые выполняется установка, и выберите вариант **Continue**.

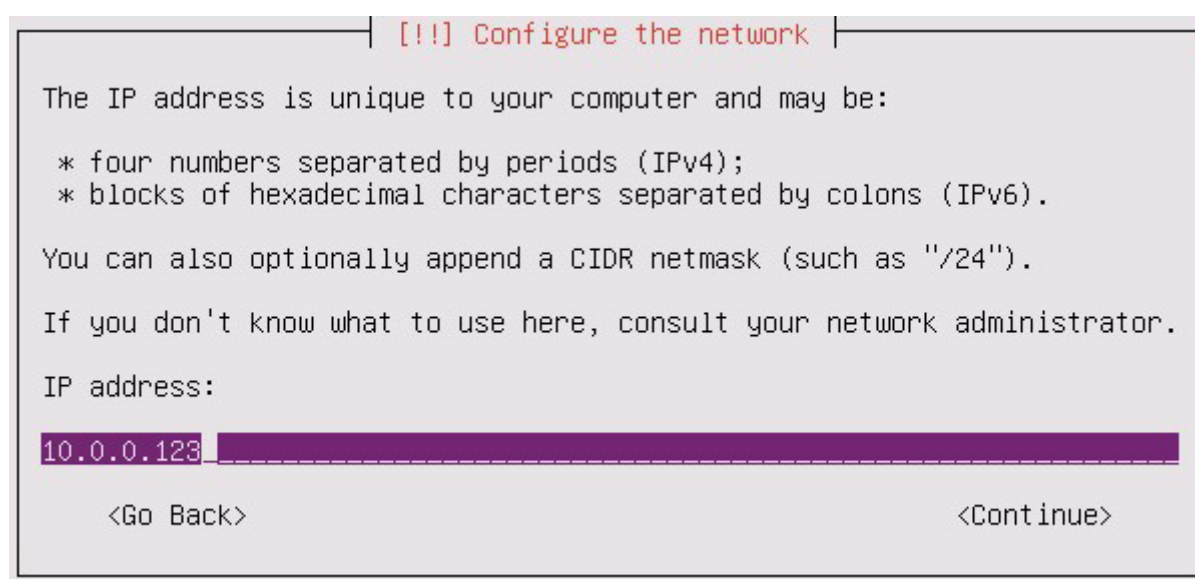


Рисунок 5. Ввод IP-адреса сервера или виртуальной машины

- Введите маску подсети и выберите вариант **Continue**.

[[!]] Configure the network

The netmask is used to determine which machines are local to your network. Consult your network administrator if you do not know the value. The netmask should be entered as four numbers separated by periods.

Netmask:

255.255.255.0

<Go Back> <Continue>

Рисунок 6. Ввод маски подсети

- Введите IP-адрес шлюза и выберите вариант **Continue**.

[[!]] Configure the network

The gateway is an IP address (four numbers separated by periods) that indicates the gateway router, also known as the default router. All traffic that goes outside your LAN (for instance, to the Internet) is sent through this router. In rare circumstances, you may have no router; in that case, you can leave this blank. If you don't know the proper answer to this question, consult your network administrator.

Gateway:

10.0.0.1

<Go Back> <Continue>

Рисунок 7. Ввод IP-адреса шлюза

- Через пробел введите IP-адреса DNS-серверов (до трех серверов) и выберите вариант **Continue**. Если вам не нужно использовать DNS-серверы, оставьте поле пустым и выберите вариант **Continue**.

[[!]] Configure the network

The name servers are used to look up host names on the network. Please enter the IP addresses (not host names) of up to 3 name servers, separated by spaces. Do not use commas. The first name server in the list will be the first to be queried. If you don't want to use any name server, just leave this field blank.

Name server addresses:

10.0.0.5 10.0.0.6

<Go Back> <Continue>

Рисунок 8. Ввод адресов DNS-серверов

Начнется установка Ubuntu Server 18.04. По окончании установки сервер или виртуальная машина, на которых выполнялась установка, будут перезагружены. Если виртуальный или физический носитель с установщиком PT Sandbox не был отключен, после перезагрузки снова откроется главное меню этого установщика. В таком случае вам нужно выйти из него, выбрав пункт **Exit**. Выход будет произведен автоматически, если не нажимать на клавиши клавиатуры в течение одной минуты.

После перезагрузки начнется загрузка Ubuntu Server 18.04. Когда система будет загружена, начнется установка PT Sandbox. По окончании установки появится сообщение `Version 2.2.<Номер сборки> successfully installed`.

6. Нажмите клавишу Enter.

Вам будет предложено ввести логин пользователя операционной системы.

7. Введите `administrator` и нажмите клавишу Enter.

Вам будет предложено ввести пароль пользователя операционной системы.

8. Введите `P0sitive` и нажмите клавишу Enter.

Появится приветственное сообщение операционной системы.

Основной узел PT Sandbox установлен.

Внимание! После установки основного узла PT Sandbox не изменяйте его название (hostname) в операционной системе. В противном случае вам придется переустанавливать основной узел PT Sandbox в этой операционной системе.

Внимание! После установки основного узла убедитесь, что он имеет [доступ к серверам обслуживания](#) (см. [раздел 7](#)).

8.2.2. Процедура установки основного узла с функцией поведенческого анализа в подготовленной ОС

В этом разделе приводится инструкция по установке основного узла PT Sandbox с функцией поведенческого анализа на физический сервер или виртуальную машину с уже установленной операционной системой.

Установка делится на следующие этапы:

1. Проверка физического сервера или виртуальной машины на соответствие [аппаратным и программным требованиям](#) (см. [раздел 5](#)).
2. Распаковка архива с установщиком PT Sandbox.
3. Настройка подключения к прокси-серверу (при необходимости).
4. Проверка [доступа к серверам обслуживания](#) (см. [раздел 7](#)).
5. Установка виртуального окружения.
6. Установка основного узла.

В этом разделе

Распаковка архива для установки основного узла с функцией поведенческого анализа (см. раздел 8.2.2.1)

Настройка подключения к прокси-серверу для основного узла с функцией поведенческого анализа (см. раздел 8.2.2.2)

Установка виртуального окружения для основного узла (см. раздел 8.2.2.3)

Установка основного узла с функцией поведенческого анализа в подготовленной ОС (см. раздел 8.2.2.4)

8.2.2.1. Распаковка архива для установки основного узла с функцией поведенческого анализа

► Чтобы распаковать архив с установщиком PT Sandbox:

1. Скопируйте архив с установщиком PT Sandbox, входящий в комплект поставки продукта, в любой каталог на сервере или виртуальной машине, на которые вы планируете устанавливать основной узел PT Sandbox с функцией поведенческого анализа.

Примечание. Архив имеет название `ptsb.installer.<Версия продукта>.tar.gz`, например `ptsb.installer.2.2.0.6.tar.gz`.

2. Перейдите в каталог со скопированным архивом.

Например:

```
cd /home/user/ptsb-installer
```

3. Распакуйте скопированный архив:

```
tar pxf ptsb.installer.<Версия продукта>.tar.gz
```

Например:

```
tar pxf ptsb.installer.2.2.0.6.tar.gz
```

Архив с установщиком PT Sandbox распакован.

8.2.2.2. Настройка подключения к прокси-серверу для основного узла с функцией поведенческого анализа

Если менеджер обновлений Ubuntu (APT) в операционной системе подключается к интернету через прокси-сервер, перед установкой основного узла PT Sandbox с функцией поведенческого анализа в этой операционной системе вам нужно указать параметры подключения к прокси-серверу.

► Чтобы настроить подключение к прокси-серверу:

1. Перейдите в каталог с [распакованным установщиком](#) (см. раздел 8.2.2.1).

Например:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт `setup-apt-proxy.sh`, указав параметры подключения к прокси-серверу:

```
sudo ./setup-apt-proxy.sh --proxy-addr <Адрес прокси-сервера>:<Порт> --proxy-user <Логин для подключения к прокси-серверу> --proxy-pass <Пароль для подключения к прокси-серверу>
```

Например:

```
sudo ./setup-apt-proxy.sh --proxy-addr http://192.0.2.108:3128 --proxy-user ivanov --proxy-pass P@ssw0rd
```

Подключение к прокси-серверу настроено.

Теперь вы можете перейти к [установке виртуального окружения \(см. раздел 8.2.2.3\)](#).

8.2.2.3. Установка виртуального окружения для основного узла

Перед установкой основного узла PT Sandbox с функцией поведенческого анализа в подготовленной операционной системе вам нужно установить виртуальное окружение в этой операционной системе.

- Чтобы установить виртуальное окружение:

1. Перейдите в каталог с [распакованным установщиком \(см. раздел 8.2.2.1\)](#).

Например:

```
cd /home/user/ptsb-installer
```

2. Проверьте ваш сервер или виртуальную машину на соответствие минимальным системным требованиям для выполнения на них поведенческого анализа:

```
sudo xen/check-system-requirements.sh
```

Начнется установка пакетов, необходимых для работы скрипта проверки требований. По окончании установки появится информация о конфигурации вашего сервера, параметрах установки и подробных требованиях для работы виртуального окружения. Если ваш сервер удовлетворяет этим требованиям, в конце вывода команды будет сообщение `CHECK STATUS: OK`.

Примечание. Вы можете узнать, сколько аппаратных ресурсов требуется для одновременной работы определенного количества виртуальных машин. Для этого нужно выполнить команду с параметром `--vm-count` <Количество виртуальных машин>, например `sudo xen/check-system-requirements.sh --vm-count 10`. Число не должно быть больше 15.

Примечание. Подробная справка доступна по команде `sudo xen/check-system-requirements.sh -h`.

3. Запустите скрипт установки виртуального окружения:

```
sudo xen/install.sh --vm-count <Количество виртуальных машин>
```

Например:

```
sudo xen/install.sh --vm-count 5
```

Примечание. Вы можете узнать, сколько виртуальных машин могут одновременно работать на вашем сервере исходя из его аппаратных ресурсов, выполнив команду `sudo xen/check-system-requirements.sh --get-max-vm`.

Примечание. Подробная справка доступна по команде `sudo xen/install.sh -h`.

По завершении работы скрипта появится сообщение `Press [Enter] to reboot`.

4. Нажмите клавишу Enter.

Физический сервер или виртуальная машина, на которых выполнялся скрипт, будут перезагружены.

Виртуальное окружение установлено.

Теперь вы можете перейти к [установке основного узла \(см. раздел 8.2.2.4\)](#).

8.2.2.4. Установка основного узла с функцией поведенческого анализа в подготовленной ОС

Перед выполнением инструкции вам нужно убедиться, что в подготовленной операционной системе [установлено виртуальное окружение \(см. раздел 8.2.2.3\)](#).

Внимание! Перед установкой убедитесь, что название узла (hostname) уникально в развертываемом кластере PT Sandbox. После установки основного узла PT Sandbox вы не сможете изменить его название без последующей переустановки.

Если вам нужно, чтобы PT Sandbox получал обновления из локального зеркала, перед установкой основного узла вам нужно [установить и настроить локальный сервер обновлений \(см. раздел 9.6\)](#).

Также перед установкой вам нужно подготовить серийный номер лицензии PT Sandbox, приобретенной вашей организацией. 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.

- Чтобы установить основной узел PT Sandbox с функцией поведенческого анализа в подготовленной операционной системе:

1. Перейдите в каталог с [распакованным установщиком \(см. раздел 8.2.2.1\)](#).

Например:

```
cd /home/user/ptsb-installer
```

2. Запустите мастер установки основного узла:

```
sudo ./wizard
```

3. Следуйте указаниям мастера.

На последнем шаге мастера начнется установка PT Sandbox. По завершении установки появится сообщение `Version <Версия PT Sandbox> successfully installed`.

Основной узел PT Sandbox установлен.

Внимание! После установки основного узла PT Sandbox не изменяйте его название (hostname) в операционной системе. В противном случае вам придется переустанавливать основной узел PT Sandbox в этой операционной системе.

8.3. Установка основного узла без функции поведенческого анализа

В этом разделе приводятся инструкции по установке основного узла PT Sandbox без функции поведенческого анализа. Вам нужно выбрать один из двух вариантов установки в зависимости от того, нужно ли вам установить основной узел вместе с операционной системой или установка должна выполняться в уже существующей операционной системе.

В этом разделе

[Процедура установки ОС и основного узла без функции поведенческого анализа \(см. раздел 8.3.1\)](#)

[Процедура установки основного узла без функции поведенческого анализа в подготовленной ОС \(см. раздел 8.3.2\)](#)

8.3.1. Процедура установки ОС и основного узла без функции поведенческого анализа

Вы можете установить основной узел PT Sandbox без функции поведенческого анализа на физический сервер или виртуальную машину без установленной операционной системы.

Установка делится на следующие этапы:

1. Проверка физического сервера или виртуальной машины на соответствие [аппаратным требованиям \(см. раздел 5.1\)](#).
2. Установка основного узла вместе с операционной системой.
3. Проверка [доступа к серверам обслуживания \(см. раздел 7\)](#).
4. Установка службы высокой доступности (если основной узел устанавливается для кластера высокой доступности).

В этом разделе

[Установка ОС и основного узла без функции поведенческого анализа \(см. раздел 8.3.1.1\)](#)

[Установка службы высокой доступности для основного узла \(см. раздел 8.3.1.2\)](#)

8.3.1.1. Установка ОС и основного узла без функции поведенческого анализа

Вы можете установить основной узел PT Sandbox без функции поведенческого анализа на физический сервер или виртуальную машину без установленной операционной системы.

Для установки вам нужно использовать установочный ISO-файл, входящий в комплект поставки PT Sandbox. Установка выполняется аналогично установке любой операционной системы — путем [создания установочного носителя из ISO-файла \(см. раздел 8.1\)](#) или с помощью монтирования этого файла при настройке виртуальной машины. Файл имеет название вида ptsb-2.2.<Версия сборки>-<Время создания сборки>.iso, например ptsb-2.2.0.136-20210111T080604.iso. При запуске установки автоматически устанавливается и настраивается 64-разрядная версия Ubuntu Server 18.04, после чего устанавливается основной узел PT Sandbox.

Перед установкой вам нужно убедиться, что физический сервер или виртуальная машина, на которые вы планируете устанавливать PT Sandbox, соответствуют [аппаратным требованиям \(см. раздел 5.1\)](#).

- Чтобы установить операционную систему и основной узел PT Sandbox без функции поведенческого анализа:
 1. Запустите виртуальную машину со смонтированным установочным ISO-файлом PT Sandbox или сервер с установочным носителем, созданным из этого ISO-файла.

Откроется главное меню установщика PT Sandbox.

2. Выберите пункт **Install new instance of PT Sandbox without behavioral analysis** и нажмите клавишу Enter.

Начнется загрузка установщика.

Если физический сервер или виртуальная машина, на которые выполняется установка, не подключены к DHCP-серверу, установщик предложит вручную настроить сетевые параметры.



Рисунок 9. Сообщение о невозможности автоматической настройки сетевых параметров

3. Для ручной настройки сетевых параметров:
 - Выберите пункт **Configure network manually** и нажмите клавишу Enter.

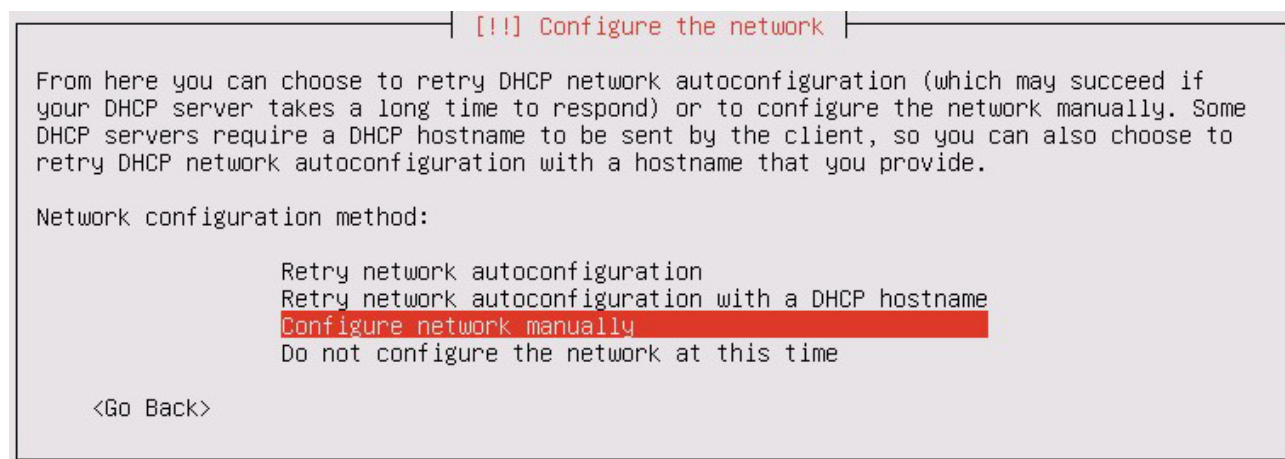


Рисунок 10. Ручная настройка сетевых параметров

- Введите IP-адрес физического сервера или виртуальной машины, на которые выполняется установка, и выберите вариант **Continue**.

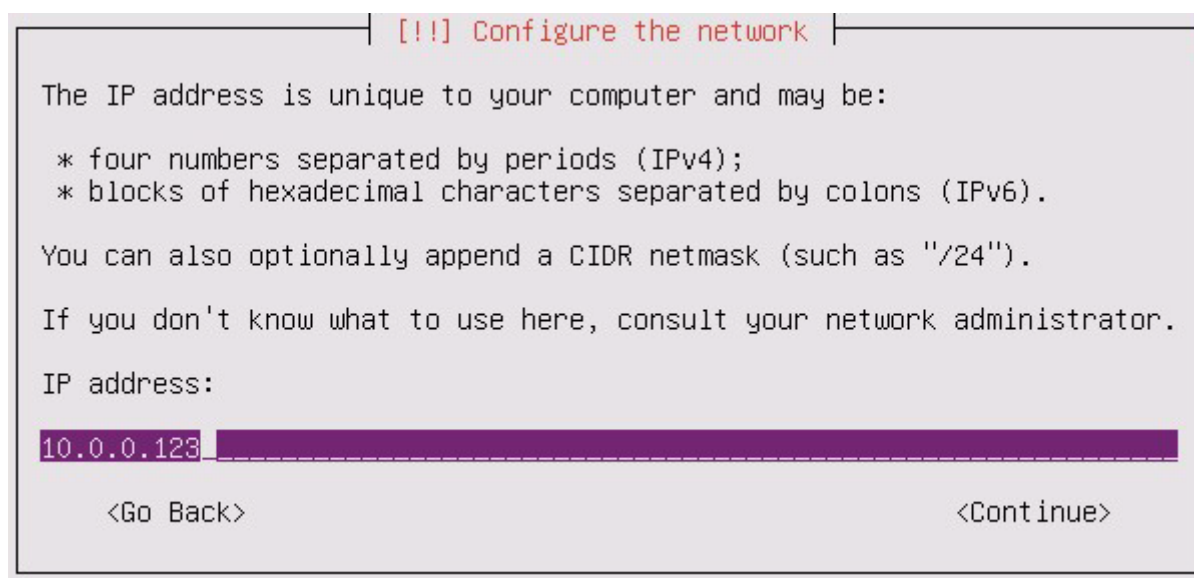


Рисунок 11. Ввод IP-адреса сервера или виртуальной машины

- Введите маску подсети и выберите вариант **Continue**.

[[!]] Configure the network

The netmask is used to determine which machines are local to your network. Consult your network administrator if you do not know the value. The netmask should be entered as four numbers separated by periods.

Netmask:

255.255.255.0

<Go Back> <Continue>

Рисунок 12. Ввод маски подсети

- Введите IP-адрес шлюза и выберите вариант **Continue**.

[[!]] Configure the network

The gateway is an IP address (four numbers separated by periods) that indicates the gateway router, also known as the default router. All traffic that goes outside your LAN (for instance, to the Internet) is sent through this router. In rare circumstances, you may have no router; in that case, you can leave this blank. If you don't know the proper answer to this question, consult your network administrator.

Gateway:

10.0.0.1

<Go Back> <Continue>

Рисунок 13. Ввод IP-адреса шлюза

- Через пробел введите IP-адреса DNS-серверов (до трех серверов) и выберите вариант **Continue**. Если вам не нужно использовать DNS-серверы, оставьте поле пустым и выберите вариант **Continue**.

[[!]] Configure the network

The name servers are used to look up host names on the network. Please enter the IP addresses (not host names) of up to 3 name servers, separated by spaces. Do not use commas. The first name server in the list will be the first to be queried. If you don't want to use any name server, just leave this field blank.

Name server addresses:

10.0.0.5 10.0.0.6

<Go Back> <Continue>

Рисунок 14. Ввод адресов DNS-серверов

Начнется установка Ubuntu Server 18.04. По окончании установки сервер или виртуальная машина, на которых выполнялась установка, будут перезагружены. Если виртуальный или физический носитель с установщиком PT Sandbox не был отключен, после перезагрузки снова откроется главное меню этого установщика. В таком случае вам нужно выйти из него, выбрав пункт **Exit**. Выход будет произведен автоматически, если не нажимать на клавиши клавиатуры в течение одной минуты.

После перезагрузки начнется загрузка Ubuntu Server 18.04. Когда система будет загружена, начнется установка PT Sandbox. По окончании установки появится сообщение `Version 2.2.<Номер сборки> successfully installed`.

4. Нажмите клавишу Enter.

Вам будет предложено ввести логин пользователя операционной системы.

5. Введите `administrator` и нажмите клавишу Enter.

Вам будет предложено ввести пароль пользователя операционной системы.

6. Введите `P0sitive` и нажмите клавишу Enter.

Появится приветственное сообщение операционной системы.

Основной узел PT Sandbox установлен.

Внимание! После установки основного узла PT Sandbox не изменяйте его название (hostname) в операционной системе. В противном случае вам придется переустанавливать основной узел PT Sandbox в этой операционной системе.

Если основной узел устанавливается для кластера высокой доступности, теперь вам нужно [установить на узле службу высокой доступности \(см. раздел 8.3.1.2\)](#).

8.3.1.2. Установка службы высокой доступности для основного узла

Если вы устанавливаете основной узел PT Sandbox для кластера высокой доступности, вам нужно установить службу высокой доступности в операционной системе, установленной вместе с основным узлом. Служба высокой доступности отвечает за работоспособность PT Sandbox в случае сбоя отдельных его компонентов или аппаратных частей на одном из физических серверов.

Перед выполнением инструкции вам нужно выделить в сетевой инфраструктуре организации IP-адрес для PT Sandbox. По этому IP-адресу, в частности, будет доступен веб-интерфейс продукта.

► Чтобы установить службу высокой доступности на основном узле:

1. Не менее чем через 3 минуты после входа в [установленную операционную систему \(см. раздел 8.3.1.1\)](#) перейдите в каталог со скриптами установщика PT Sandbox:

```
cd /home/administrator/installer
```

2. Запустите установку службы высокой доступности:

```
sudo ./install-keepalived.sh --virtual-ip <IP-адрес, выделенный для PT Sandbox> --  
interface <Название сетевого интерфейса этого IP-адреса>
```

Например:

```
sudo ./install-keepalived.sh --virtual-ip 192.0.2.55 --interface eth0
```

По окончании установки появится сообщение `Keepalived successfully installed`.

3. В конфигурационном файле Netplan пропишите IP-адрес, выделенный для PT Sandbox, и примените конфигурацию.

Примечание. Подробную инструкцию см. на [сайте Netplan](#).

4. Запустите скрипт для изменения IP-адреса в конфигурации PT Sandbox:

```
sudo ./change-master-node-ip.sh
```

После успешного выполнения скрипт запросит перезагрузку операционной системы.

Служба высокой доступности установлена на основном узле.

Теперь вы можете перейти к [установке дополнительных узлов \(см. раздел 8.4\)](#).

8.3.2. Процедура установки основного узла без функции поведенческого анализа в подготовленной ОС

В этом разделе приводится инструкция по установке основного узла PT Sandbox без функции поведенческого анализа на физический сервер или виртуальную машину с уже установленной операционной системой.

Установка делится на следующие этапы:

1. Проверка физического сервера или виртуальной машины на соответствие [аппаратным и программным требованиям \(см. раздел 5\)](#).
2. Распаковка архива с установщиком PT Sandbox.
3. Настройка подключения к прокси-серверу (при необходимости).
4. Проверка [доступа к серверам обслуживания \(см. раздел 7\)](#).
5. Установка службы высокой доступности (если основной узел устанавливается для кластера высокой доступности).
6. Установка основного узла.

В этом разделе

[Распаковка архива для установки основного узла без функции поведенческого анализа \(см. раздел 8.3.2.1\)](#)

[Настройка подключения к прокси-серверу для основного узла без функции поведенческого анализа \(см. раздел 8.3.2.2\)](#)

[Установка службы высокой доступности для основного узла в подготовленной ОС \(см. раздел 8.3.2.3\)](#)

[Установка основного узла без функции поведенческого анализа в подготовленной ОС \(см. раздел 8.3.2.4\)](#)

8.3.2.1. Распаковка архива для установки основного узла без функции поведенческого анализа

► Чтобы распаковать архив с установщиком PT Sandbox:

1. Скопируйте архив с установщиком PT Sandbox, входящий в комплект поставки продукта, в любой каталог на сервере или виртуальной машине, на которые вы планируете устанавливать основной узел PT Sandbox без функции поведенческого анализа.

Примечание. Архив имеет название `ptsb.installer.<Версия продукта>.tar.gz`, например `ptsb.installer.2.2.0.6.tar.gz`.

2. Перейдите в каталог со скопированным архивом.

Например:

```
cd /home/user/ptsb-installer
```

3. Распакуйте скопированный архив:

```
tar pxf ptsb.installer.<Версия продукта>.tar.gz
```

Например:

```
tar pxf ptsb.installer.2.2.0.6.tar.gz
```

Архив с установщиком PT Sandbox распакован.

8.3.2.2. Настройка подключения к прокси-серверу для основного узла без функции поведенческого анализа

Если менеджер обновлений Ubuntu (APT) в операционной системе подключается к интернету через прокси-сервер, перед установкой основного узла PT Sandbox без функции поведенческого анализа в этой операционной системе вам нужно указать параметры подключения к прокси-серверу.

► Чтобы настроить подключение к прокси-серверу:

1. Перейдите в каталог с [распакованным установщиком](#) (см. раздел 8.3.2.1).

Например:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт `setup-apt-proxy.sh`, указав параметры подключения к прокси-серверу:

```
sudo ./setup-apt-proxy.sh --proxy-addr <Адрес прокси-сервера>:<Порт> --proxy-user <Логин для подключения к прокси-серверу> --proxy-pass <Пароль для подключения к прокси-серверу>
```

Например:

```
sudo ./setup-apt-proxy.sh --proxy-addr http://192.0.2.108:3128 --proxy-user ivanov --proxy-pass P@ssw0rd
```

Подключение к прокси-серверу настроено.

8.3.2.3. Установка службы высокой доступности для основного узла в подготовленной ОС

Если вы устанавливаете основной узел PT Sandbox для кластера высокой доступности, вам нужно установить службу высокой доступности в операционной системе, подготовленной для установки основного узла. Служба высокой доступности отвечает за работоспособность PT Sandbox в случае сбоев отдельных его компонентов или аппаратных частей на одном из физических серверов.

Перед выполнением инструкции вам нужно выделить в сетевой инфраструктуре организации IP-адрес для PT Sandbox. По этому IP-адресу, в частности, будет доступен веб-интерфейс продукта.

► Чтобы установить службу высокой доступности:

1. Перейдите в каталог с [распакованным установщиком](#) (см. раздел 8.3.2.1).

Например:

```
cd /home/user/ptsb-installer
```

2. Запустите установку службы высокой доступности:

```
sudo ./install-keepalived.sh --virtual-ip <IP-адрес, выделенный для PT Sandbox> --  
interface <Название сетевого интерфейса этого IP-адреса>
```

Например:

```
sudo ./install-keepalived.sh --virtual-ip 192.0.2.55 --interface eth0
```

По окончании установки появится сообщение `Keepalived successfully installed`.

3. В конфигурационном файле Netplan пропишите IP-адрес, выделенный для PT Sandbox, и примените конфигурацию.

Примечание. Подробную инструкцию см. на [сайте Netplan](#).

4. Запустите скрипт для изменения IP-адреса в конфигурации PT Sandbox:

```
sudo ./change-master-node-ip.sh
```

После успешного выполнения скрипт запросит перезагрузку операционной системы.

Служба высокой доступности установлена.

Теперь вы можете перейти к [установке основного узла](#) (см. раздел 8.3.2.4).

8.3.2.4. Установка основного узла без функции поведенческого анализа в подготовленной ОС

Если основной узел PT Sandbox устанавливается для кластера высокой доступности, перед установкой узла в подготовленной операционной системе нужно [установить службу высокой доступности](#) (см. раздел 8.3.2.3).

Внимание! Перед установкой убедитесь, что название узла (hostname) уникально в развертываемом кластере PT Sandbox. После установки основного узла PT Sandbox вы не сможете изменить его название без последующей переустановки.

Если вам нужно, чтобы PT Sandbox получал обновления из локального зеркала, перед установкой основного узла вам нужно [установить и настроить локальный сервер обновлений \(см. раздел 9.6\)](#).

Также перед установкой вам нужно подготовить серийный номер лицензии PT Sandbox, приобретенной вашей организацией. 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.

- Чтобы установить основной узел PT Sandbox без функции поведенческого анализа в подготовленной операционной системе:

1. Перейдите в каталог с [распакованным установщиком \(см. раздел 8.3.2.1\)](#).

Например:

```
cd /home/user/ptsb-installer
```

2. Запустите мастер установки основного узла:

```
sudo ./wizard
```

3. Следуйте указаниям мастера.

На последнем шаге мастера начнется установка PT Sandbox. По завершении установки появится сообщение `Version <Версия PT Sandbox> successfully installed`.

Основной узел PT Sandbox установлен.

Внимание! После установки основного узла PT Sandbox не изменяйте его название (hostname) в операционной системе. В противном случае вам придется переустанавливать основной узел PT Sandbox в этой операционной системе.

8.4. Установка дополнительных узлов

В этом разделе приводятся инструкции по установке дополнительных узлов PT Sandbox. Вам нужно выбрать один из четырех вариантов установки в зависимости от того, нужно ли вам устанавливать дополнительный узел PT Sandbox вместе с операционной системой или установка должна выполняться в уже существующей операционной системе, и потребуется ли функция поведенческого анализа для проверки файлов с помощью этого узла.

В этом разделе

[Процедура установки ОС и дополнительных узлов с функцией поведенческого анализа \(см. раздел 8.4.1\)](#)

[Процедура установки дополнительных узлов с функцией поведенческого анализа в подготовленной ОС \(см. раздел 8.4.2\)](#)

[Процедура установки ОС и дополнительных узлов без функции поведенческого анализа \(см. раздел 8.4.3\)](#)

[Процедура установки дополнительных узлов без функции поведенческого анализа в подготовленной ОС \(см. раздел 8.4.4\)](#)

8.4.1. Процедура установки ОС и дополнительных узлов с функцией поведенческого анализа

В этом разделе приводится инструкция по установке дополнительного узла PT Sandbox вместе с операционной системой и функцией поведенческого анализа.

Установка делится на следующие этапы:

1. Проверка физического сервера или виртуальной машины на соответствие [аппаратным и программным требованиям](#) (см. раздел 5).
2. Установка операционной системы и виртуального окружения для выполнения поведенческого анализа.
3. Проверка [доступа к серверам обслуживания](#) (см. раздел 7).
4. Получение команды для установки дополнительного узла.
5. Установка дополнительного узла с помощью полученной команды.

В этом разделе

[Установка ОС и виртуального окружения для дополнительного узла](#) (см. раздел 8.4.1.1)

[Получение команды для установки дополнительных узлов с функцией поведенческого анализа](#) (см. раздел 8.4.1.2)

[Установка дополнительного узла с функцией поведенческого анализа](#) (см. раздел 8.4.1.3)

8.4.1.1. Установка ОС и виртуального окружения для дополнительного узла

Для установки вам нужно использовать установочный ISO-файл, входящий в комплект поставки PT Sandbox. Установка выполняется аналогично установке любой операционной системы — путем [создания установочного носителя из ISO-файла](#) (см. раздел 8.1) или с помощью монтирования этого файла при настройке виртуальной машины. Файл имеет название вида ptsb-2.2.<Версия сборки>-<Время создания сборки>.iso, например ptsb-2.2.0.136-20210111T080604.iso. При запуске установки автоматически устанавливается и настраивается 64-разрядная версия Ubuntu Server 18.04, после чего настраивается виртуальное окружение для поведенческого анализа.

Перед установкой нужно убедиться, что физический сервер или виртуальная машина, на которые вы планируете устанавливать PT Sandbox, соответствуют [аппаратным и программным требованиям](#) (см. раздел 5).

► Чтобы установить операционную систему и виртуальное окружение для дополнительного узла:

1. Запустите виртуальную машину со смонтированным установочным ISO-файлом PT Sandbox или сервер с установочным носителем, созданным из этого ISO-файла.

Откроется главное меню установщика PT Sandbox.

2. Выберите пункт **Install additional node for behavioral analysis** и нажмите клавишу Enter.

Начнется загрузка установщика. По окончании загрузки установщик проверит сервер или виртуальную машину на соответствие минимальным системным требованиям для выполнения на них поведенческого анализа.

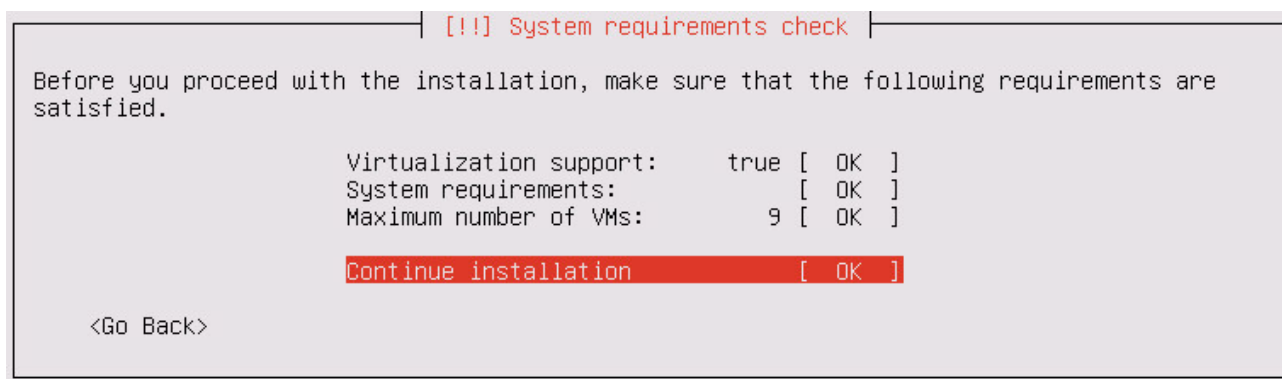


Рисунок 15. Проверка системных требований

В случае успешной проверки все пункты будут помечены словом "OK". При наличии хотя бы одного слова "FAILED" вы не сможете продолжить установку. Для получения подробной информации нужно выбрать соответствующий пункт.

3. Если вам нужно уменьшить максимальное количество одновременно работающих виртуальных машин, в которых выполняется поведенческий анализ, выберите пункт **Maximum number of VMs**, в появившемся поле введите новое число, после чего выберите вариант **Continue**.

Уменьшение может понадобиться, если вам нужно освободить часть аппаратных ресурсов под другие задачи.

Примечание. По умолчанию установщик указывает максимально допустимое значение, рассчитанное исходя из доступных аппаратных ресурсов.

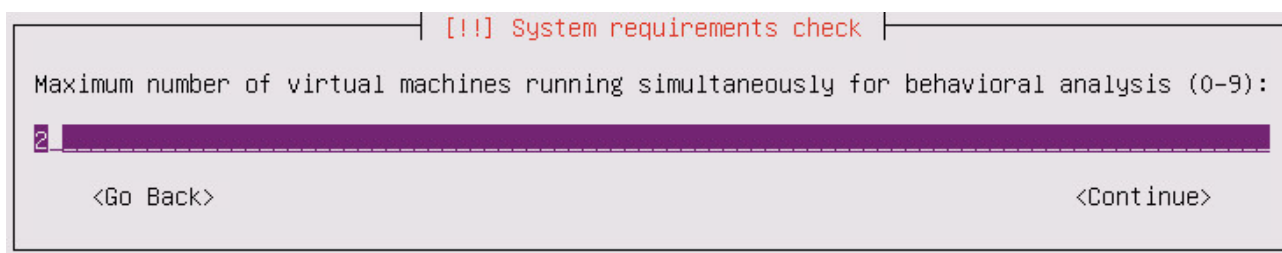


Рисунок 16. Изменение максимального количества виртуальных машин

4. Выберите вариант **Continue installation**.

Если физический сервер или виртуальная машина, на которые выполняется установка, не подключены к DHCP-серверу, установщик предложит вручную настроить сетевые параметры.



Рисунок 17. Сообщение о невозможности автоматической настройки сетевых параметров

5. Для ручной настройки сетевых параметров:

- Выберите пункт **Configure network manually** и нажмите клавишу Enter.

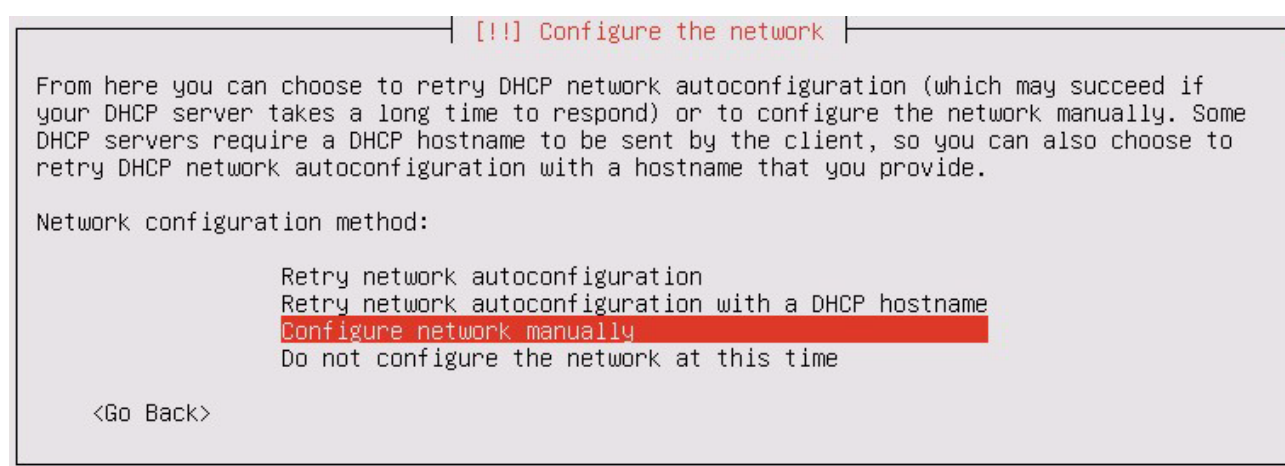


Рисунок 18. Ручная настройка сетевых параметров

- Введите IP-адрес физического сервера или виртуальной машины, на которые выполняется установка, и выберите вариант **Continue**.

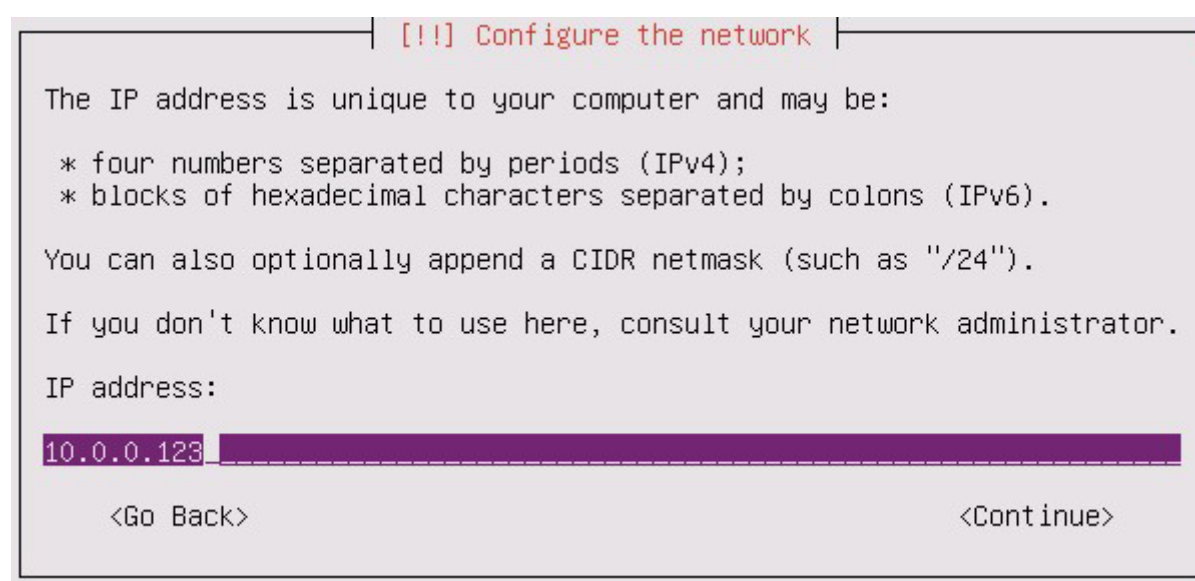


Рисунок 19. Ввод IP-адреса сервера или виртуальной машины

- Введите маску подсети и выберите вариант **Continue**.

!!! Configure the network

The netmask is used to determine which machines are local to your network. Consult your network administrator if you do not know the value. The netmask should be entered as four numbers separated by periods.

Netmask:

255.255.255.0

<Go Back><Continue>

Рисунок 20. Ввод маски подсети

- Введите IP-адрес шлюза и выберите вариант **Continue**.

!!! Configure the network

The gateway is an IP address (four numbers separated by periods) that indicates the gateway router, also known as the default router. All traffic that goes outside your LAN (for instance, to the Internet) is sent through this router. In rare circumstances, you may have no router; in that case, you can leave this blank. If you don't know the proper answer to this question, consult your network administrator.

Gateway:

10.0.0.1

<Go Back><Continue>

Рисунок 21. Ввод IP-адреса шлюза

- Через пробел введите IP-адреса DNS-серверов (до трех серверов) и выберите вариант **Continue**. Если вам не нужно использовать DNS-серверы, оставьте поле пустым и выберите вариант **Continue**.

!!! Configure the network

The name servers are used to look up host names on the network. Please enter the IP addresses (not host names) of up to 3 name servers, separated by spaces. Do not use commas. The first name server in the list will be the first to be queried. If you don't want to use any name server, just leave this field blank.

Name server addresses:

10.0.0.5 10.0.0.6

<Go Back><Continue>

Рисунок 22. Ввод адресов DNS-серверов

Начнется установка Ubuntu Server 18.04. По окончании установки сервер или виртуальная машина, на которых выполнялась установка, будут перезагружены. Если виртуальный или физический носитель с установщиком PT Sandbox не был отключен, после перезагрузки снова откроется главное меню этого установщика. В таком случае вам нужно выйти из него, выбрав пункт **Exit**. Выход будет произведен автоматически, если не нажимать на клавиши клавиатуры в течение одной минуты.

Начнется загрузка Ubuntu Server 18.04. Когда система будет загружена, начнется установка виртуального окружения. По окончании установки появится сообщение `Kubernetes successfully installed`.

6. Нажмите клавишу Enter.

Вам будет предложено ввести логин пользователя операционной системы.

7. Введите `administrator` и нажмите клавишу Enter.

Вам будет предложено ввести пароль пользователя операционной системы.

8. Введите `Positive` и нажмите клавишу Enter.

Появится приветственное сообщение операционной системы.

Операционная система и виртуальное окружение для дополнительного узла установлены.

Теперь вы можете перейти к [получению команды для установки дополнительных узлов \(см. раздел 8.4.1.2\)](#).

8.4.1.2. Получение команды для установки дополнительных узлов с функцией поведенческого анализа

Установка дополнительных узлов PT Sandbox выполняется при помощи специальной команды. Эту команду нужно получить на основном узле. Команда содержит токен, который действует два часа. По истечении срока действия токена вам нужно получить команду снова, так как предыдущая команда перестает работать.

- Чтобы получить команду для установки дополнительных узлов:

1. На основном узле перейдите в каталог со скриптами установщика PT Sandbox:

- Если основной узел устанавливался вместе с операционной системой (с помощью ISO-файла):

```
cd /home/administrator/installer
```

- Если основной узел устанавливался в подготовленной операционной системе (с помощью скрипта `install.sh`), перейдите в каталог с распакованным установщиком PT Sandbox, например:

```
cd /home/user/ptsb-installer
```

2. Сгенерируйте команду для установки дополнительных узлов:

```
sudo ./k8s-gen-token.sh
```


Внимание! Каждый последующий запуск скрипта `k8s-gen-token.sh` делает недействительной команду для установки, полученную при предыдущем его запуске.

Пример полученной команды для установки дополнительных узлов с функцией поведенческого анализа:

```
./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ijqr4l.vizd2...1vi66
```

Теперь вы можете перейти к [установке дополнительного узла с функцией поведенческого анализа \(см. раздел 8.4.1.3\)](#).

8.4.1.3. Установка дополнительного узла с функцией поведенческого анализа

Перед выполнением инструкции вам нужно [установить операционную систему и виртуальное окружение \(см. раздел 8.4.1.1\)](#), после чего [получить команду для установки дополнительных узлов \(см. раздел 8.4.1.2\)](#).

► Чтобы установить дополнительный узел с функцией поведенческого анализа:

1. Не менее чем через 3 минуты после входа в [установленную операционную систему \(см. раздел 8.4.1.1\)](#) перейдите в каталог со скриптами установщика PT Sandbox:

```
cd /home/administrator/installer
```

2. Выполните [команду для установки дополнительных узлов \(см. раздел 8.4.1.2\)](#) с правами root.

Например:

```
sudo ./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ijqr4l.vizd2...1vi66
```

Дополнительный узел с функцией поведенческого анализа установлен.

Внимание! После установки дополнительного узла PT Sandbox не изменяйте его название (hostname) в операционной системе. В противном случае вам придется переустанавливать дополнительный узел PT Sandbox в этой операционной системе.

8.4.2. Процедура установки дополнительных узлов с функцией поведенческого анализа в подготовленной ОС

В этом разделе приводится инструкция по установке дополнительного узла PT Sandbox с функцией поведенческого анализа в подготовленной операционной системе.

Установка делится на следующие этапы:

1. Проверка физического сервера или виртуальной машины на соответствие [аппаратным и программным требованиям \(см. раздел 5\)](#).
2. Распаковка архива с установщиком PT Sandbox.
3. Настройка подключения к прокси-серверу (при необходимости).
4. Проверка [доступа к серверам обслуживания \(см. раздел 7\)](#).

5. Установка виртуального окружения.
6. Получение команды для установки дополнительного узла.
7. Установка дополнительного узла с помощью полученной команды.

В этом разделе

Распаковка архива для установки дополнительного узла с функцией поведенческого анализа (см. раздел 8.4.2.1)

Настройка подключения к прокси-серверу для дополнительного узла с функцией поведенческого анализа (см. раздел 8.4.2.2)

Установка виртуального окружения для дополнительного узла (см. раздел 8.4.2.3)

Получение команды для установки дополнительных узлов с функцией поведенческого анализа в подготовленной ОС (см. раздел 8.4.2.4)

Установка дополнительного узла с функцией поведенческого анализа в подготовленной ОС (см. раздел 8.4.2.5)

8.4.2.1. Распаковка архива для установки дополнительного узла с функцией поведенческого анализа

► Чтобы распаковать архив с установщиком PT Sandbox:

1. Скопируйте архив с установщиком PT Sandbox, входящий в комплект поставки продукта, в любой каталог на сервере или виртуальной машине, на которые вы планируете устанавливать дополнительный узел PT Sandbox с функцией поведенческого анализа:

Примечание. Архив имеет название `ptsb.installer.<Версия продукта>.tar.gz`, например `ptsb.installer.2.2.0.6.tar.gz`.

2. Перейдите в каталог со скопированным архивом.

Например:

```
cd /home/user/ptsb-installer
```

3. Распакуйте скопированный архив:

```
tar pxf ptsb.installer.<Версия продукта>.tar.gz
```

Например:

```
tar pxf ptsb.installer.2.2.0.6.tar.gz
```

Архив с установщиком PT Sandbox распакован.

8.4.2.2. Настройка подключения к прокси-серверу для дополнительного узла с функцией поведенческого анализа

Если менеджер обновлений Ubuntu (APT) в операционной системе подключается к интернету через прокси-сервер, перед установкой дополнительного узла в этой операционной системе нужно указать параметры подключения к прокси-серверу.

► Чтобы настроить подключение к прокси-серверу:

1. Перейдите в каталог с [распакованным установщиком](#) (см. раздел 8.4.2.1).

Например:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт `setup-apt-proxy.sh`, указав параметры подключения к прокси-серверу:

```
sudo ./setup-apt-proxy.sh --proxy-addr <Адрес прокси-сервера>:<Порт> --proxy-user <Логин для подключения к прокси-серверу> --proxy-pass <Пароль для подключения к прокси-серверу>
```

Например:

```
sudo ./setup-apt-proxy.sh --proxy-addr http://192.0.2.108:3128 --proxy-user ivanov --proxy-pass P@ssw0rd
```

Подключение к прокси-серверу настроено.

Теперь вы можете перейти к [установке виртуального окружения](#) (см. раздел 8.4.2.3).

8.4.2.3. Установка виртуального окружения для дополнительного узла

Перед установкой дополнительного узла PT Sandbox с функцией поведенческого анализа в подготовленной операционной системе вам нужно установить виртуальное окружение в этой операционной системе.

► Чтобы установить виртуальное окружение:

1. Перейдите в каталог с [распакованным установщиком](#) (см. раздел 8.4.2.1).

Например:

```
cd /home/user/ptsb-installer
```

2. Проверьте ваш сервер или виртуальную машину на соответствие минимальным системным требованиям для выполнения на них поведенческого анализа:

```
sudo xen/check-system-requirements.sh --slave
```

Начнется установка пакетов, необходимых для работы скрипта проверки требований. По окончании установки появится информация о конфигурации вашего сервера, параметрах установки и подробных требованиях для работы виртуального окружения. Если ваш сервер удовлетворяет этим требованиям, в конце вывода команды будет сообщение `CHECK STATUS: OK`.

Примечание. Вы можете узнать, сколько аппаратных ресурсов требуется для одновременной работы определенного количества виртуальных машин. Для этого нужно выполнить команду с параметром `--vm-count` <Количество виртуальных машин>, например `sudo xen/check-system-requirements.sh --slave --vm-count 10`. Число не должно быть больше 15.

Примечание. Подробная справка доступна по команде `sudo xen/check-system-requirements.sh -h`.

3. Запустите скрипт установки виртуального окружения:

```
sudo xen/install.sh --slave --vm-count <Количество виртуальных машин>
```

Например:

```
sudo xen/install.sh --slave --vm-count 5
```

Примечание. Вы можете узнать, сколько виртуальных машин могут одновременно работать на вашем сервере исходя из его аппаратных ресурсов, выполнив команду `sudo xen/check-system-requirements.sh --slave --get-max-vm`.

Примечание. Подробная справка доступна по команде `sudo xen/install.sh -h`.

По завершении работы скрипта появится сообщение `Press [Enter] to reboot`.

4. Нажмите клавишу Enter.

Физический сервер или виртуальная машина, на которых выполнялся скрипт, будут перезагружены.

Виртуальное окружение установлено.

Теперь вы можете перейти к [получению команды для установки дополнительных узлов](#) (см. раздел 8.4.2.4).

8.4.2.4. Получение команды для установки дополнительных узлов с функцией поведенческого анализа в подготовленной ОС

Установка дополнительных узлов PT Sandbox выполняется при помощи специальной команды. Эту команду нужно получить на основном узле. Команда содержит токен, который действует два часа. По истечении срока действия токена вам нужно получить команду снова, так как предыдущая команда перестает работать.

- Чтобы получить команду для установки дополнительных узлов:

1. На основном узле перейдите в каталог со скриптами установщика PT Sandbox:

- Если основной узел устанавливался вместе с операционной системой (с помощью ISO-файла):

```
cd /home/administrator/installer
```

- Если основной узел устанавливался в подготовленной операционной системе (с помощью скрипта `install.sh`), перейдите в каталог с распакованным установщиком PT Sandbox, например:

```
cd /home/user/ptsb-installer
```

2. Сгенерируйте команду для установки дополнительных узлов:

```
sudo ./k8s-gen-token.sh
```

Внимание! Каждый последующий запуск скрипта `k8s-gen-token.sh` делает недействительной команду для установки, полученную при предыдущем его запуске.

Пример полученной команды для установки дополнительных узлов с функцией поведенческого анализа:

```
./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ijqr4l.vizd2...1vi66
```

Теперь вы можете перейти к [установке дополнительного узла с функцией поведенческого анализа \(см. раздел 8.4.2.5\)](#).

8.4.2.5. Установка дополнительного узла с функцией поведенческого анализа в подготовленной ОС

Перед выполнением инструкции убедитесь, что в подготовленной операционной системе [установлено виртуальное окружение \(см. раздел 8.4.2.3\)](#).

Внимание! Перед установкой убедитесь, что название узла (hostname) уникально в развертываемом кластере PT Sandbox. После установки дополнительного узла PT Sandbox вы не сможете изменить его название без последующей переустановки.

- Чтобы установить дополнительный узел с функцией поведенческого анализа:

1. Перейдите в каталог с [распакованным установщиком \(см. раздел 8.4.2.1\)](#).

Например:

```
cd /home/user/ptsb-installer
```

2. Выполните [команду для установки дополнительных узлов \(см. раздел 8.4.2.4\)](#) с правами root.

Например:

```
sudo ./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ijqr4l.vizd2...1vi66
```

Дополнительный узел с функцией поведенческого анализа установлен.

Внимание! После установки дополнительного узла PT Sandbox не изменяйте его название (hostname) в операционной системе. В противном случае вам придется переустанавливать дополнительный узел PT Sandbox в этой операционной системе.

8.4.3. Процедура установки ОС и дополнительных узлов без функции поведенческого анализа

В этом разделе приводится инструкция по установке дополнительного узла PT Sandbox без функции поведенческого анализа вместе с операционной системой.

Установка делится на следующие этапы:

1. Проверка физического сервера или виртуальной машины на соответствие [аппаратным требованиям \(см. раздел 5.1\)](#).
2. Установка операционной системы для дополнительного узла.
3. Проверка [доступа к серверам обслуживания \(см. раздел 7\)](#).
4. Установка службы высокой доступности.
5. Получение команды для установки дополнительного узла.
6. Установка дополнительного узла с помощью полученной команды.

В этом разделе

[Установка ОС для дополнительного узла \(см. раздел 8.4.3.1\)](#)

[Установка службы высокой доступности для дополнительного узла \(см. раздел 8.4.3.2\)](#)

[Получение команды для установки дополнительных узлов без функции поведенческого анализа \(см. раздел 8.4.3.3\)](#)

[Установка дополнительного узла без функции поведенческого анализа \(см. раздел 8.4.3.4\)](#)

8.4.3.1. Установка ОС для дополнительного узла

Для установки вам нужно использовать установочный ISO-файл, входящий в комплект поставки PT Sandbox. Установка выполняется аналогично установке любой операционной системы — [путем создания установочного носителя из ISO-файла \(см. раздел 8.1\)](#) или с помощью монтирования этого файла при настройке виртуальной машины. Файл имеет название вида ptsb-2.2.<Версия сборки>-<Время создания сборки>.iso, например ptsb-2.2.0.136-20210111T080604.iso. При запуске установки автоматически устанавливается и настраивается 64-разрядная версия Ubuntu Server 18.04, после чего копируется установщик PT Sandbox.

► Чтобы установить операционную систему для дополнительного узла:

1. Запустите виртуальную машину со смонтированным установочным ISO-файлом PT Sandbox или сервер с установочным носителем, созданным из этого ISO-файла.

Откроется главное меню установщика PT Sandbox.

2. Выберите пункт **Install additional node without behavioral analysis** и нажмите клавишу Enter.

Начнется загрузка установщика.

Если физический сервер или виртуальная машина, на которые выполняется установка, не подключены к DHCP-серверу, установщик предложит вручную настроить сетевые параметры.



Рисунок 23. Сообщение о невозможности автоматической настройки сетевых параметров

3. Для ручной настройки сетевых параметров:

- Выберите пункт **Configure network manually** и нажмите клавишу Enter.

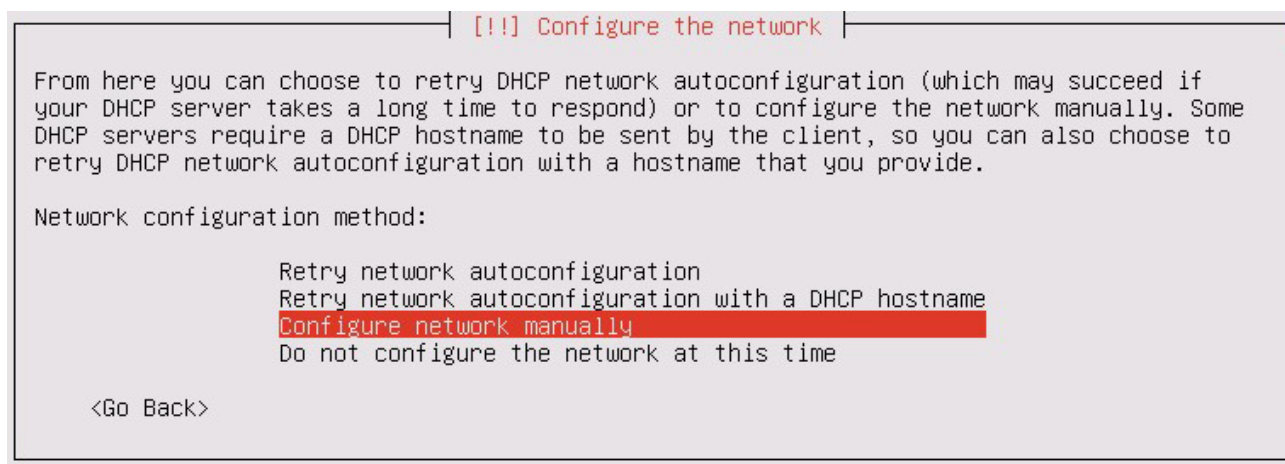


Рисунок 24. Ручная настройка сетевых параметров

- Введите IP-адрес физического сервера или виртуальной машины, на которые выполняется установка, и выберите вариант **Continue**.

!!! Configure the network

The IP address is unique to your computer and may be:

- * four numbers separated by periods (IPv4);
- * blocks of hexadecimal characters separated by colons (IPv6).

You can also optionally append a CIDR netmask (such as "/24").

If you don't know what to use here, consult your network administrator.

IP address:

10.0.0.123

<Go Back> <Continue>

Рисунок 25. Ввод IP-адреса сервера или виртуальной машины

- Введите маску подсети и выберите вариант **Continue**.

!!! Configure the network

The netmask is used to determine which machines are local to your network. Consult your network administrator if you do not know the value. The netmask should be entered as four numbers separated by periods.

Netmask:

255.255.255.0

<Go Back> <Continue>

Рисунок 26. Ввод маски подсети

- Введите IP-адрес шлюза и выберите вариант **Continue**.

!!! Configure the network

The gateway is an IP address (four numbers separated by periods) that indicates the gateway router, also known as the default router. All traffic that goes outside your LAN (for instance, to the Internet) is sent through this router. In rare circumstances, you may have no router; in that case, you can leave this blank. If you don't know the proper answer to this question, consult your network administrator.

Gateway:

10.0.0.1

<Go Back> <Continue>

Рисунок 27. Ввод IP-адреса шлюза

- Через пробел введите IP-адреса DNS-серверов (до трех серверов) и выберите вариант **Continue**. Если вам не нужно использовать DNS-серверы, оставьте поле пустым и выберите вариант **Continue**.

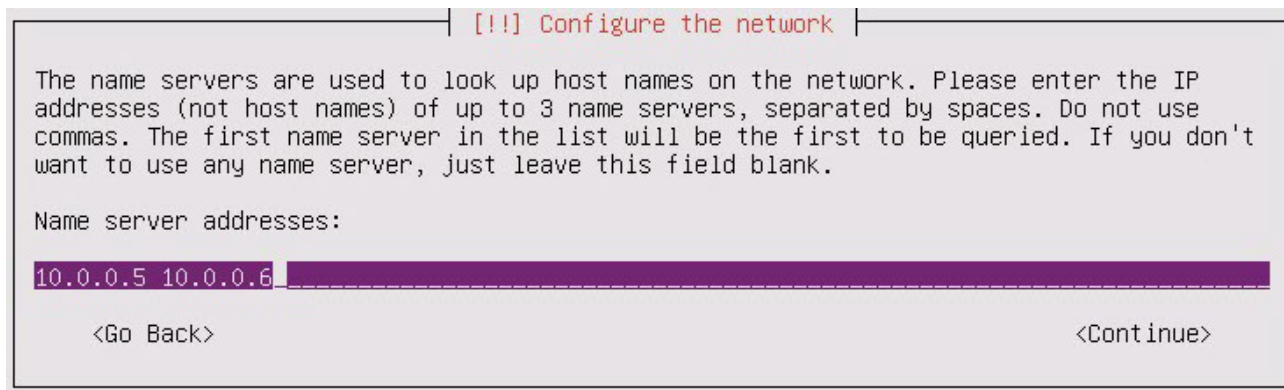


Рисунок 28. Ввод адресов DNS-серверов

Начнется установка Ubuntu Server 18.04. По окончании установки сервер или виртуальная машина, на которых выполнялась установка, будут перезагружены. Если виртуальный или физический носитель с установщиком PT Sandbox не был отключен, после перезагрузки снова откроется главное меню этого установщика. В таком случае вам нужно выйти из него, выбрав пункт **Exit**. Выход будет произведен автоматически, если не нажимать на клавиши клавиатуры в течение одной минуты.

Начнется загрузка Ubuntu Server 18.04. Когда система будет загружена, начнется копирование установщика PT Sandbox и подготовка к установке PT Sandbox. По окончании подготовки появится сообщение `Kubernetes successfully installed`.

4. Нажмите клавишу Enter.

Вам будет предложено ввести логин пользователя операционной системы.

5. Введите `administrator` и нажмите клавишу Enter.

Вам будет предложено ввести пароль пользователя операционной системы.

6. Введите `P0sitive` и нажмите клавишу Enter.

Появится приветственное сообщение операционной системы.

Операционная система для дополнительного узла установлена.

Теперь вы можете перейти к [установке службы высокой доступности \(см. раздел 8.4.3.2\)](#).

8.4.3.2. Установка службы высокой доступности для дополнительного узла

Перед установкой дополнительного узла PT Sandbox вам нужно установить службу высокой доступности в операционной системе, [установленной для дополнительного узла \(см. раздел 8.4.3.1\)](#). Служба высокой доступности отвечает за работоспособность PT Sandbox в случае сбоев отдельных его компонентов или аппаратных частей на одном из физических серверов.

► Чтобы установить службу высокой доступности для дополнительного узла:

1. Не менее чем через 3 минуты после входа в [установленную операционную систему \(см. раздел 8.4.3.1\)](#) перейдите в каталог со скриптами установщика PT Sandbox:

```
cd /home/administrator/installer
```

2. Запустите установку службы высокой доступности:

```
sudo ./install-keepalived.sh --virtual-ip <IP-адрес, выделенный для PT Sandbox> --  
interface <Название сетевого интерфейса этого IP-адреса>
```

Например:

```
sudo ./install-keepalived.sh --virtual-ip 192.0.2.55 --interface eth0
```

По окончании установки появится сообщение `Keepalived successfully installed`.

Служба высокой доступности для дополнительного узла установлена.

Теперь вы можете перейти к [получению команды для установки дополнительных узлов \(см. раздел 8.4.3.3\)](#).

8.4.3.3. Получение команды для установки дополнительных узлов без функции поведенческого анализа

Установка дополнительных узлов PT Sandbox выполняется при помощи специальной команды. Эту команду нужно получить на основном узле. Команда содержит токен, который действует два часа. По истечении срока действия токена вам нужно получить команду снова, так как предыдущая команда перестает работать.

► Чтобы получить команду для установки дополнительных узлов без функции поведенческого анализа:

1. На основном узле перейдите в каталог со скриптами установщика PT Sandbox:

- Если основной узел устанавливался вместе с операционной системой (с помощью ISO-файла):

```
cd /home/administrator/installer
```

- Если основной узел устанавливался в подготовленной операционной системе (с помощью скрипта `install.sh`), перейдите в каталог с распакованным установщиком PT Sandbox, например:

```
cd /home/user/ptsb-installer
```

2. Сгенерируйте команду для установки дополнительных узлов:

```
sudo ./k8s-gen-token.sh --with-master-role
```

Внимание! Каждый последующий запуск скрипта `k8s-gen-token.sh` делает недействительной команду для установки, полученную при предыдущем его запуске.

Пример полученной команды для установки дополнительных узлов кластера высокой доступности:

```
./k8s-join-node.sh --cluster-ip 192.0.2.15 --token ijqr3l.viz...i66 --with-master-role --certificate-key 7f3e58...14e2b3f
```

Теперь вы можете перейти к [установке дополнительного узла без функции поведенческого анализа \(см. раздел 8.4.3.4\)](#).

8.4.3.4. Установка дополнительного узла без функции поведенческого анализа

Перед установкой дополнительного узла PT Sandbox вам нужно [установить службу высокой доступности \(см. раздел 8.4.3.2\)](#) в операционной системе, установленной для этого узла.

- Чтобы установить дополнительный узел без функции поведенческого анализа:

1. Перейдите в каталог со скриптами установщика PT Sandbox:

```
cd /home/administrator/installer
```

2. Выполните [команду для установки дополнительных узлов \(см. раздел 8.4.3.3\)](#) с правами root.

Например:

```
sudo ./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ijqr4l.vizd2...1vi66 --with-master-role --certificate-key 7f3e58c0...e7e214e1b3f
```

Дополнительный узел без функции поведенческого анализа установлен.

Внимание! После установки дополнительного узла PT Sandbox не изменяйте его название (hostname) в операционной системе. В противном случае вам придется переустанавливать дополнительный узел PT Sandbox в этой операционной системе.

8.4.4. Процедура установки дополнительных узлов без функции поведенческого анализа в подготовленной ОС

В этом разделе приводится инструкция по установке дополнительного узла PT Sandbox без функции поведенческого анализа в подготовленной операционной системе.

Установка делится на следующие этапы:

1. Проверка физического сервера или виртуальной машины на соответствие [аппаратным и программным требованиям \(см. раздел 5\)](#).
2. Распаковка архива с установщиком PT Sandbox.
3. Настройка подключения к прокси-серверу (при необходимости).
4. Проверка [доступа к серверам обслуживания \(см. раздел 7\)](#).
5. Установка службы высокой доступности.
6. Получение команды для установки дополнительного узла.
7. Установка дополнительного узла с помощью полученной команды.

В этом разделе

[Распаковка архива для установки дополнительного узла без функции поведенческого анализа \(см. раздел 8.4.4.1\)](#)

[Настройка подключения к прокси-серверу для дополнительного узла без функции поведенческого анализа \(см. раздел 8.4.4.2\)](#)

[Установка службы высокой доступности для дополнительного узла в подготовленной ОС \(см. раздел 8.4.4.3\)](#)

[Получение команды для установки дополнительных узлов без функции поведенческого анализа в подготовленной ОС \(см. раздел 8.4.4.4\)](#)

[Установка дополнительного узла без функции поведенческого анализа в подготовленной ОС \(см. раздел 8.4.4.5\)](#)

8.4.4.1. Распаковка архива для установки дополнительного узла без функции поведенческого анализа

► Чтобы распаковать архив с установщиком PT Sandbox:

1. Скопируйте архив с установщиком PT Sandbox, входящий в комплект поставки продукта, в любой каталог на сервере или виртуальной машине, на которые вы планируете устанавливать дополнительный узел PT Sandbox без функции поведенческого анализа.

Примечание. Архив имеет название `ptsb.installer.<Версия продукта>.tar.gz`, например `ptsb.installer.2.2.0.6.tar.gz`.

2. Перейдите в каталог со скопированным архивом.

Например:

```
cd /home/user/ptsb-installer
```

3. Распакуйте скопированный архив:

```
tar xzf ptsb.installer.<Версия продукта>.tar.gz
```

Например:

```
tar pxf ptsb.installer.2.2.0.6.tar.gz
```

Архив с установщиком PT Sandbox распакован.

8.4.4.2. Настройка подключения к прокси-серверу для дополнительного узла без функции поведенческого анализа

Если менеджер обновлений Ubuntu (APT) в операционной системе подключается к интернету через прокси-сервер, перед установкой дополнительного узла в этой операционной системе нужно указать параметры подключения к прокси-серверу.

► Чтобы настроить подключение к прокси-серверу:

1. Перейдите в каталог с [распакованным установщиком](#) (см. раздел 8.4.4.1).

Например:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт `setup-apt-proxy.sh`, указав параметры подключения к прокси-серверу:

```
sudo ./setup-apt-proxy.sh --proxy-addr <Адрес прокси-сервера>:<Порт> --proxy-user <Логин для подключения к прокси-серверу> --proxy-pass <Пароль для подключения к прокси-серверу>
```

Например:

```
sudo ./setup-apt-proxy.sh --proxy-addr http://192.0.2.108:3128 --proxy-user ivanov --proxy-pass P@ssw0rd
```

Подключение к прокси-серверу настроено.

Теперь вы можете перейти к [установке службы высокой доступности](#) (см. раздел 8.4.4.3).

8.4.4.3. Установка службы высокой доступности для дополнительного узла в подготовленной ОС

Перед установкой дополнительного узла PT Sandbox вам нужно установить службу высокой доступности в операционной системе, подготовленной для этого узла. Служба высокой доступности отвечает за работоспособность PT Sandbox в случае сбоя отдельных его компонентов или аппаратных частей на одном из физических серверов.

► Чтобы установить службу высокой доступности для дополнительного узла:

1. Перейдите в каталог с [распакованным установщиком](#) (см. раздел 8.4.4.1).

Например:

```
cd /home/user/ptsb-installer
```

2. Запустите установку службы высокой доступности:

```
sudo ./install-keepalived.sh --virtual-ip <IP-адрес, выделенный для PT Sandbox> --interface <Название сетевого интерфейса этого IP-адреса>
```

Например:

```
sudo ./install-keepalived.sh --virtual-ip 192.0.2.55 --interface eth0
```

По окончании установки появится сообщение `Keepalived successfully installed`.

Служба высокой доступности для дополнительного узла установлена.

Теперь вы можете перейти к [получению команды для установки дополнительных узлов \(см. раздел 8.4.4.4\)](#).

8.4.4.4. Получение команды для установки дополнительных узлов без функции поведенческого анализа в подготовленной ОС

Установка дополнительных узлов PT Sandbox выполняется при помощи специальной команды. Эту команду нужно получить на основном узле. Команда содержит токен, который действует два часа. По истечении срока действия токена вам нужно получить команду снова, так как предыдущая команда перестает работать.

► Чтобы получить команду для установки дополнительных узлов:

1. На основном узле перейдите в каталог со скриптами установщика PT Sandbox:

- Если основной узел устанавливался вместе с операционной системой (с помощью ISO-файла):

```
cd /home/administrator/installer
```

- Если основной узел устанавливался в подготовленной операционной системе (с помощью скрипта `install.sh`), перейдите в каталог с распакованным установщиком PT Sandbox, например:

```
cd /home/user/ptsb-installer
```

2. Сгенерируйте команду для установки дополнительных узлов:

```
sudo ./k8s-gen-token.sh --with-master-role
```

Внимание! Каждый последующий запуск скрипта `k8s-gen-token.sh` делает недействительной команду для установки, полученную при предыдущем его запуске.

Пример полученной команды для установки дополнительных узлов кластера высокой доступности:

```
./k8s-join-node.sh --cluster-ip 192.0.2.15 --token ijqr3l.viz...i66 --with-master-role --certificate-key 7f3e58...14e2b3f
```

Теперь вы можете перейти к [установке дополнительного узла без функции поведенческого анализа \(см. раздел 8.4.4.5\)](#).

8.4.4.5. Установка дополнительного узла без функции поведенческого анализа в подготовленной ОС

Перед установкой дополнительного узла PT Sandbox вам нужно [установить службу высокой доступности \(см. раздел 8.4.4.3\)](#) в операционной системе, подготовленной для этого узла.

Внимание! Перед установкой убедитесь, что название узла (hostname) уникально в развертываемом кластере PT Sandbox. После установки дополнительного узла PT Sandbox вы не сможете изменить его название без последующей переустановки.

► Чтобы установить дополнительный узел без функции поведенческого анализа:

1. Перейдите в каталог с [распакованным установщиком \(см. раздел 8.4.4.1\)](#).

Например:

```
cd /home/user/ptsb-installer
```

2. Выполните [команду для установки дополнительных узлов \(см. раздел 8.4.4.4\)](#) с правами root.

Например:

```
sudo ./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ijqr4l.vizd2...1vi66 --with-master-role --certificate-key 7f3e58c0...e7e214e1b3f
```

Дополнительный узел без функции поведенческого анализа установлен.

Внимание! После установки дополнительного узла PT Sandbox не изменяйте его название (hostname) в операционной системе. В противном случае вам придется переустанавливать дополнительный узел PT Sandbox в этой операционной системе.

8.5. Резервное копирование и восстановление параметров PT Sandbox

В PT Sandbox вы можете создавать резервные копии параметров продукта. Резервная копия может понадобиться для восстановления параметров PT Sandbox. Например, в случае возникновения проблем с физическим сервером вы можете установить PT Sandbox на работающий сервер и восстановить параметры продукта. Или после удаления PT Sandbox и при повторной его установке.

Примечание. Если PT Sandbox установлен на виртуальной машине, резервная копия параметров продукта не содержит параметры виртуальной машины.

В этом разделе

[Создание файла резервной копии параметров PT Sandbox \(см. раздел 8.5.1\)](#)

[Восстановление параметров PT Sandbox из файла резервной копии \(см. раздел 8.5.2\)](#)

8.5.1. Создание файла резервной копии параметров PT Sandbox

Если PT Sandbox установлен и работает, файл резервной копии параметров продукта создается автоматически при каждом запуске команды `sudo ./install.sh` и сохраняется в каталоге `/opt/ptms/var/configuration-backups`. Чтобы создать файл резервной копии параметров продукта и сохранить его в другом каталоге, необходимо использовать отдельную команду.

- ▶ Чтобы создать файл резервной копии параметров PT Sandbox,

выполните команду:

```
sudo ./backup-config.sh --backup-file <Полный путь для сохранения файла резервной копии>
```

Например:

```
sudo ./backup-config.sh --backup-file /opt/ptms/configuration/backup_07-04-2020.yaml
```

8.5.2. Восстановление параметров PT Sandbox из файла резервной копии

- ▶ Чтобы восстановить параметры PT Sandbox из файла резервной копии,

выполните команду:

```
sudo ./install.sh --backup-file <Полный путь к файлу резервной копии>
```

Например:

```
sudo ./install.sh --backup-file /opt/ptms/var/configuration-backups/backup_07-04-2020.yaml
```

Примечание. Если PT Sandbox установлен и работает, при запуске команды `sudo ./install.sh` без указания пути к файлу резервной копии к продукту автоматически применятся параметры из последнего сохраненного ранее файла резервной копии.

Вы также можете восстановить параметры продукта в процессе повторной установки PT Sandbox, указав в команде установки параметр `--backup-file <Полный путь к файлу резервной копии>`.

9. Первоначальная настройка PT Sandbox

После установки PT Sandbox по умолчанию вам доступна только одна пользовательская учетная запись. Она предоставляет права доступа ко всем объектам в интерфейсе продукта (права суперпользователя) и нужна для создания первых пользовательских учетных записей продукта.

Сразу после установки PT Sandbox вам нужно:

1. Войти в сервис управления ролями и доступом (PT IAM).
2. В целях безопасности сменить стандартный пароль суперпользователя.
3. Создать учетную запись пользователя с правами администратора, который будет выполнять настройку и администрирование PT Sandbox.
4. Войти в PT Sandbox под учетной записью суперпользователя или администратора.
5. Активировать функцию поведенческого анализа.

Помимо обязательных действий при первоначальной настройке вы можете:

- Оценить объемы файлов, которые будут сканироваться. Возможно, вам нужно будет увеличить объемы хранилища файлов, а также карантина, где будут храниться заблокированные электронные письма. По умолчанию объемы хранилища файлов и карантина составляют по 3 ГБ.
- Настроить обновление с локального зеркала обновлений, если PT Sandbox работает в изолированном от интернета сегменте сети.

В этом разделе

[Вход в PT IAM \(см. раздел 9.1\)](#)

[Смена пароля суперпользователя \(см. раздел 9.2\)](#)

[Создание учетной записи администратора PT Sandbox \(см. раздел 9.3\)](#)

[Активация приобретенной лицензии \(см. раздел 9.4\)](#)

[Активация функции поведенческого анализа \(см. раздел 9.5\)](#)

[Настройка обновлений PT Sandbox с локального зеркала \(см. раздел 9.6\)](#)

[Настройка подключения к прокси-серверу \(см. раздел 9.7\)](#)

[Настройка подключения к прокси-серверу с SSL-инспекцией \(см. раздел 9.8\)](#)

9.1. Вход в PT IAM

Чтобы выполнить первоначальную настройку PT Sandbox, вам нужно войти в сервис управления пользователями и доступом Positive Technologies Identity and Access Management (PT IAM), который обеспечивает механизм единого входа (технология single sign-on) в приложения "Позитив Текнолоджиз".

► Чтобы войти в PT IAM:

1. В главном меню PT Sandbox нажмите  и в открывшемся меню выберите **Identity and Access Management**.

Откроется страница входа в PT IAM.

2. В поле **Логин** введите Administrator.
3. В поле **Пароль** введите P@ssw0rd.
4. Нажмите кнопку **Войти**.

Откроется страница управления учетными записями пользователей PT IAM.

9.2. Смена пароля суперпользователя

В целях безопасности сразу после установки продукта вам нужно сменить стандартный пароль для суперпользователя.

► Чтобы сменить пароль суперпользователя:

1. [Войдите в сервис управления ролями и доступом \(см. раздел 9.1\)](#).
2. В панели инструментов нажмите кнопку **Изменить данные**.

Откроется страница **Изменение данных пользователя**.

3. Нажмите на ссылку **Изменить**.
4. В поле **Пароль** введите новый безопасный пароль для суперпользователя.

Примечание. Пароль должен содержать не менее 8 символов: как минимум одну прописную и одну строчную латинскую букву, одну цифру и один спецсимвол. Вы можете создать безопасный пароль по кнопке **Сгенерировать**.

5. Нажмите кнопку **Сохранить**.

Пароль суперпользователя изменен.

9.3. Создание учетной записи администратора PT Sandbox

Вам нужно создать учетную запись пользователя с правами администратора, который будет выполнять настройку и администрирование PT Sandbox.

► Чтобы создать учетную запись администратора PT Sandbox:

1. [Войдите в сервис управления ролями и доступом \(см. раздел 9.1\)](#).
2. В панели инструментов нажмите кнопку **Добавить пользователя**.

Откроется страница **Новый пользователь**.

3. Заполните необходимые поля.
4. Нажмите на ссылку MultiScanner и в открывшемся окне установите флажок **Admin**.

5. Нажмите кнопку **Создать**.
6. При необходимости создайте другие учетные записи, например для операторов безопасности и обычных пользователей.

Учетная запись администратора PT Sandbox создана.

Теперь вы или другой сотрудник вашей организации можете [войти в продукт \(см. раздел 10\)](#), используя созданную учетную запись администратора, для дальнейшей настройки и администрирования продукта.

9.4. Активация приобретенной лицензии

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

Чтобы активировать лицензию, приобретенную вашей организацией, вам нужно ввести серийный номер этой лицензии в интерфейсе PT Sandbox. 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.

► Чтобы активировать лицензию:

1. В главном меню в разделе **Система** выберите пункт **Лицензия**.
Откроется страница **Система** на вкладке **Лицензия**.
2. Нажмите кнопку **Заменить лицензию**.
3. Во всплывающем окне введите серийный номер лицензии и нажмите кнопку **Заменить**.

Информация о приобретенной лицензии отобразится на странице.

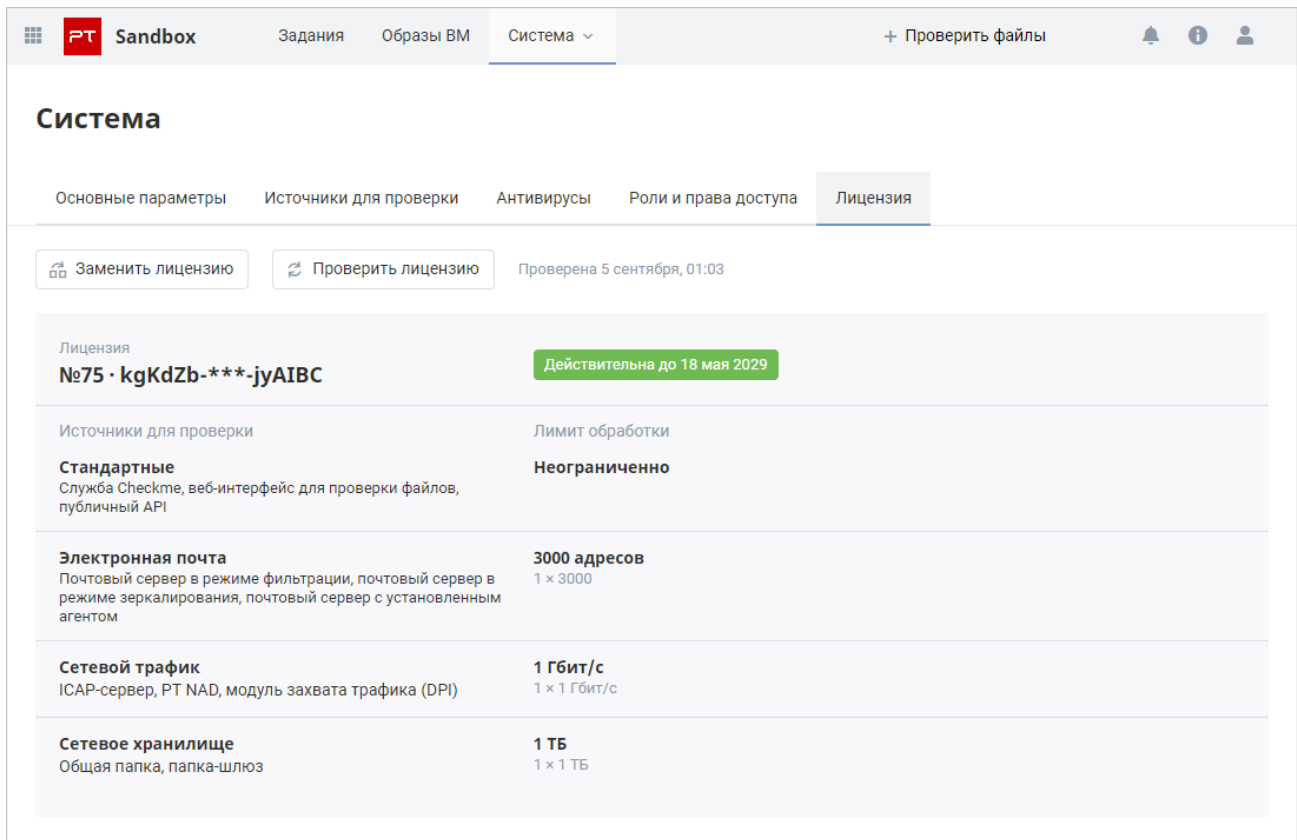


Рисунок 29. Просмотр информации о лицензии

Лицензия активирована.

Примечание. Рекомендуется сравнить параметры лицензии, перечисленные на странице, с указанными при заказе лицензии. В случае несоответствия вам нужно обратиться в службу технической поддержки "Позитив Текнолоджиз".

См. также

[Лицензирование \(см. раздел 6\)](#)

9.5. Активация функции поведенческого анализа

Чтобы PT Sandbox мог выполнять поведенческий анализ файлов, вам нужно активировать функцию поведенческого анализа на всех узлах PT Sandbox, кроме узлов кластера высокой доступности.

Все команды, упомянутые в этом разделе, выполняются на узле с установленным PT Sandbox (в случае многосерверной конфигурации — на основном узле кластера).

► Чтобы активировать функцию поведенческого анализа:

1. Получите список всех узлов PT Sandbox с информацией о готовности функции поведенческого анализа на каждом из них:

```
sudo /opt/ptms/sbin/ptmsctl sandbox nodes list
```

Появится список названий узлов PT Sandbox. Для каждого узла будет указано одно из следующих состояний функции поведенческого анализа:

- Behavioral analysis is enabled — функция поведенческого анализа на указанном узле активирована;
- Not ready for behavioral analysis to be enabled — виртуальное окружение было установлено на указанном узле, но функция поведенческого анализа на нем не была активирована;
- Behavioral analysis is disabled — узел не может выполнять задачи поведенческого анализа из-за того, что виртуальное окружение на нем не было установлено или было установлено некорректно.

После выполнения каждого из последующих шагов вы можете повторно получать список узлов при помощи вышеприведенной команды для проверки готовности функции поведенческого анализа.

2. Если для основного узла отображается состояние Behavioral analysis is disabled и вам нужно активировать на нем функцию поведенческого анализа, [установите на нем виртуальное окружение \(см. раздел 8.2.2.3\)](#).
3. На дополнительных узлах с состоянием Behavioral analysis is disabled, на которых вам нужно активировать функцию поведенческого анализа, [установите виртуальное окружение \(см. раздел 8.4.2.3\)](#).
4. Выполните команды для активации функции поведенческого анализа на нужных вам узлах:

```
sudo /opt/ptms/sbin/ptmsctl sandbox nodes acquire <Название узла (hostname)>, на котором  
нужно включить функцию поведенческого анализа
```

Например:

```
sudo /opt/ptms/sbin/ptmsctl sandbox nodes acquire host1  
sudo /opt/ptms/sbin/ptmsctl sandbox nodes acquire host5  
sudo /opt/ptms/sbin/ptmsctl sandbox nodes acquire host6
```

Появится сообщение Behavioral analysis is now enabled on the node "<Название узла>".

Примечание. Если вы по ошибке включили функцию поведенческого анализа не на том узле, вы можете выключить ее с помощью команды `sudo /opt/ptms/sbin/ptmsctl sandbox nodes release <Название узла, на котором нужно выключить функцию поведенческого анализа>`.

5. Запустите процесс скачивания и установки образов виртуальных машин:

```
sudo /opt/ptms/sbin/ptmsctl sandbox force-generate-images
```

Начнется скачивание и установка образов, предусмотренных лицензией. Это может занять продолжительное время. Вы можете отслеживать состояние установки образов в [интерфейсе продукта \(см. раздел 11.3\)](#).

Функция поведенческого анализа файлов активирована.

9.6. Настройка обновлений PT Sandbox с локального зеркала

Примечание. Вы можете обновлять PT Sandbox только до следующей по номеру версии. Например, с версии 0.9 до версии 1.0. Для обновления PT Sandbox с версии 0.9 до версии 1.1 необходимо сначала обновить продукт до версии 1.0, затем до версии 1.1.

PT Sandbox может проверять файлы и обновляться в изолированном от интернета сегменте сети. Если политика информационной безопасности организации запрещает доступ в интернет для PT Sandbox или если у сервера с PT Sandbox отсутствует канал связи с интернетом, вы можете установить локальное зеркало обновлений в демилитаризованной зоне (ДМЗ). Это зеркало будет загружать обновления с сайта "Позитив Текнолоджиз". Для передачи файлов обновлений с зеркала в PT Sandbox вы можете либо вручную копировать их при помощи внешнего носителя, либо настроить автоматическую передачу обновлений с локального зеркала в PT Sandbox.

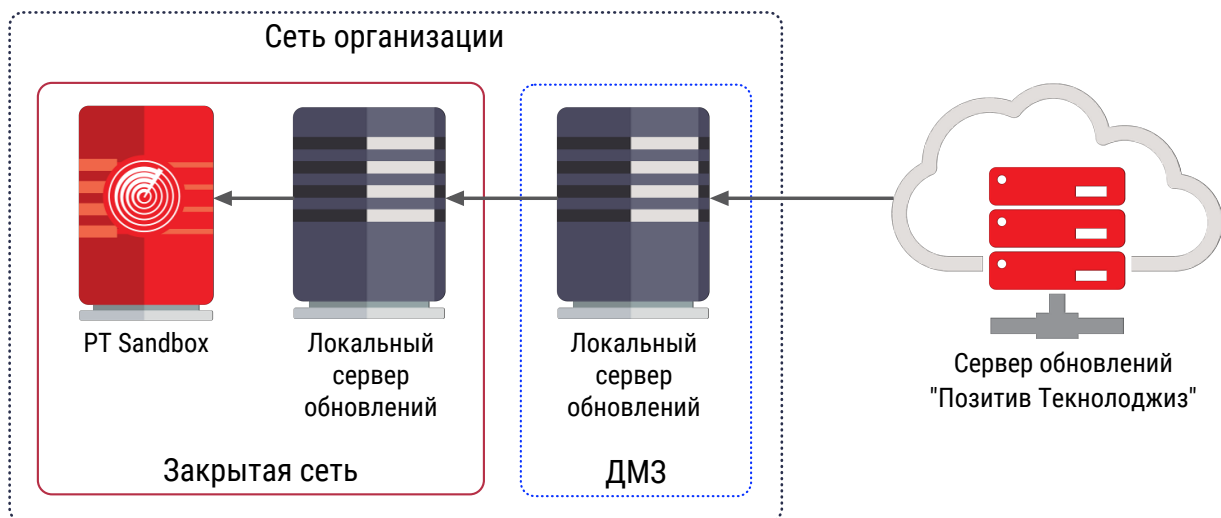


Рисунок 30. Обновление PT Sandbox в закрытом сегменте сети

Вы можете также реализовать схему обновления с одним локальным сервером обновлений, расположенным в демилитаризованной зоне. В этом разделе приводятся инструкции по настройке обновлений с использованием двух серверов.

Для настройки обновлений PT Sandbox с локального зеркала вам нужно:

1. Установить два локальных сервера обновлений: один в изолированном сегменте сети рядом с PT Sandbox, другой — в демилитаризованной зоне.
2. Активировать приобретенную вашей организацией лицензию на сервере обновлений, установленном в демилитаризованной зоне.

3. Если между локальными серверами обновлений есть сетевая связность и необходимо автоматизировать процедуру обновления, вам нужно настроить регулярные получение данных с публичного сервера обновлений "Позитив Текнолоджиз" локальным сервером обновлений в демилитаризованной зоне и передачу этих данных в PT Sandbox.
4. Сменить источник обновлений PT Sandbox с публичного сервера обновлений "Позитив Текнолоджиз" на локальный сервер обновлений, установленный в изолированном сегменте сети.

В этом разделе

[Установка локального сервера обновлений \(см. раздел 9.6.1\)](#)

[Активация лицензии на локальном сервере обновлений в демилитаризованной зоне \(см. раздел 9.6.2\)](#)

[Ручной перенос обновлений PT Sandbox в закрытый сегмент сети \(см. раздел 9.6.3\)](#)

[Настройка автоматического переноса обновлений PT Sandbox в закрытый сегмент сети \(см. раздел 9.6.4\)](#)

[Смена источника обновлений PT Sandbox на локальное зеркало \(см. раздел 9.6.5\)](#)

9.6.1. Установка локального сервера обновлений

В этом разделе приводится инструкция по установке локального сервера обновлений в закрытом сегменте сети или в демилитаризованной зоне. Установка сервера нужно выполнять в операционной системе Ubuntu.

Перед установкой локального сервера обновлений в демилитаризованной зоне вам нужно убедиться, что сервер или виртуальная машина, на которые вы планируете устанавливать локальный сервер обновлений, имеют доступ к серверам обслуживания.

- Чтобы установить локальный сервер обновлений в закрытом сегменте сети или в демилитаризованной зоне:
 1. Скопируйте архив с установщиком PT Sandbox, входящий в комплект поставки продукта, в любой каталог на сервере или виртуальной машине и перейдите в этот каталог.
 2. Распакуйте скопированный архив:

```
tar pxf ptsb.installer.<Версия продукта>.tar.gz
```

Например:

```
tar pxf ptsb.installer.2.2.0.6.tar.gz
```

3. Перейдите в каталог с распакованным установщиком PT Sandbox:

```
cd /home/user/ptsb-installer
```

4. Запустите установку локального сервера обновлений:

```
sudo ./update-mirror/install.sh
```

Локальный сервер обновлений установлен и запущен в виде службы подсистемы `systemd`. Вы можете проверять состояние сервера с помощью команды `systemctl status pt-update-mirror.service` и просматривать его журналы с помощью команды `journalctl -u pt-update-mirror.service`.

После установки локального сервера в демилитаризованной зоне вам нужно активировать на нем лицензию. Локальный сервер обновлений в закрытом сегменте сети не требует активации, поскольку не подключается к публичному серверу обновлений "Позитив Текнолоджиз".

9.6.2. Активация лицензии на локальном сервере обновлений в демилитаризованной зоне

После установки локального сервера обновлений в демилитаризованной зоне вам нужно активировать на нем лицензию, приобретенную вашей организацией. Лицензия нужна для аутентификации вашего сервера обновлений на публичном сервере обновлений "Позитив Текнолоджиз". Активация выполняется с помощью серийного номера лицензии, который указывается в файле `serial number.txt` на установочном диске из комплекта поставки или высылается в электронном письме на адрес, указанный при заказе лицензии.

- Чтобы активировать лицензию на локальном сервере обновлений в демилитаризованной зоне,

выполните команду:

- Если установленный локальный сервер обновлений должен иметь прямой доступ к публичному серверу обновлений "Позитив Текнолоджиз":

```
sudo /opt/ptms/bin/pt-update-mirror license activate --serial-number '<Серийный номер лицензии>'
```

- Если установленный локальный сервер обновлений должен подключаться к публичному серверу обновлений "Позитив Текнолоджиз" через прокси сервер:

```
sudo /opt/ptms/bin/pt-update-mirror license activate --serial-number '<Серийный номер лицензии>' --proxy <Адрес и порт прокси-сервера через двоеточие> --proxy-user <Логин для подключения к прокси-серверу> --proxy-password <Пароль для подключения к прокси-серверу>
```

Например:

```
sudo /opt/ptms/bin/pt-update-mirror license activate --serial-number 'XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXXXXXXXX' --proxy http://192.0.2.15:8080 --proxy-user Ivanov --proxy-password P@ssw0rd
```

Лицензия активирована.

9.6.3. Ручной перенос обновлений PT Sandbox в закрытый сегмент сети

Если между локальными серверами обновлений отсутствует сетевая связность, вам нужно вручную перенести обновления в закрытый сегмент сети для последующего обновления PT Sandbox.

► Чтобы вручную перенести обновления PT Sandbox в закрытый сегмент сети:

1. На локальном сервере обновлений в демилитаризованной зоне запустите получение обновлений с публичного сервера обновлений "Позитив Текнолоджиз":

```
sudo /opt/ptms/bin/pt-update-mirror repository update
```

Если сервер получит новые обновления, появится сообщение `New data available for update`.

2. Экспортируйте полученные обновления в файл экспорта-импорта обновлений:

- для экспорта как обновлений PT Sandbox, так и обновлений антивирусных баз:

```
sudo /opt/ptms/bin/pt-update-mirror repository export <Путь к архиву с его названием>
```

- для экспорта только обновлений антивирусных баз:

```
sudo /opt/ptms/bin/pt-update-mirror repository export --only-data-bases <Путь к архиву с его названием>
```

Например:

```
sudo /opt/ptms/bin/pt-update-mirror repository export --only-data-bases /home/user/tmp/update.tar.gz
```

В случае успешного импорта появится сообщение `Done`.

3. Скопируйте полученный файл экспорта-импорта на локальный сервер обновлений в закрытом сегменте сети с помощью внешнего носителя.

4. На локальном сервере обновлений в закрытом сегменте сети импортируйте обновления из скопированного файла экспорта-импорта:

```
sudo /opt/ptms/bin/pt-update-mirror repository import <Путь к архиву с его названием>
```

Например:

```
sudo /opt/ptms/bin/pt-update-mirror repository import /home/user/tmp/update.tar.gz
```

В случае успешного импорта появится сообщение `Done`.

Обновления PT Sandbox перенесены в закрытый сегмент сети.

Теперь вы можете [указать новый источник для обновлений в параметрах продукта \(см. раздел 9.6.5\)](#).

9.6.4. Настройка автоматического переноса обновлений PT Sandbox в закрытый сегмент сети

Если между локальными серверами обновлений есть сетевая связность, вы можете настроить автоматическую передачу обновлений с сайта "Позитив Текнолоджиз" в PT Sandbox через цепочку локальных серверов обновлений.

► Чтобы настроить автоматический перенос обновлений PT Sandbox в закрытый сегмент сети:

1. Настройте регулярное получение обновлений с публичного сервера обновлений "Позитив Текнолоджиз" локальным сервером обновлений, установленным в демилитаризованной зоне. Для этого нужно обеспечить автоматическое выполнение следующей команды (например, при помощи планировщика заданий):

```
sudo /opt/ptms/bin/pt-update-mirror repository update
```

2. На локальном сервере обновлений, установленном в демилитаризованной зоне, настройте автоматический экспорт загруженных обновлений в файл экспорта-импорта обновлений. Для этого нужно обеспечить автоматическое выполнение одной из следующих команд:

- для экспорта как обновлений PT Sandbox, так и обновлений антивирусных баз:

```
sudo /opt/ptms/bin/pt-update-mirror repository export <Путь к архиву с его названием>
```

- для экспорта только обновлений антивирусных баз:

```
sudo /opt/ptms/bin/pt-update-mirror repository export --only-data-bases <Путь к архиву с его названием>
```

Например:

```
sudo /opt/ptms/bin/pt-update-mirror repository export --only-data-bases /home/user/tmp/update.tar.gz
```

3. Настройте автоматическое копирование файла экспорта-импорта обновлений на локальный сервер обновлений, установленный в изолированном сегменте сети.
4. Настройте автоматический импорт данных из файла экспорта-импорта обновлений. Для этого на локальном сервере обновлений, установленном в изолированном сегменте сети, нужно обеспечить автоматическое выполнение следующей команды:

```
sudo -- bash -c 'yes | /opt/ptms/bin/pt-update-mirror repository import <Путь к архиву с его названием>'
```

Например:

```
sudo -- bash -c 'yes | /opt/ptms/bin/pt-update-mirror repository import /home/user/tmp/update.tar.gz'
```

Автоматический перенос обновлений PT Sandbox в закрытый сегмент сети настроен.

Теперь вы можете [указать новый источник для обновлений в параметрах продукта \(см. раздел 9.6.5\)](#).

9.6.5. Смена источника обновлений PT Sandbox на локальное зеркало

После установки локального сервера обновлений в закрытом сегменте сети вам нужно указать PT Sandbox, что он должен обновляться с этого сервера.

► Чтобы сменить источник обновлений PT Sandbox на локальное зеркало:

1. На сервере или виртуальной машине с PT Sandbox (в многосерверной конфигурации — на основном узле) укажите IP-адрес нового сервера обновлений:

```
sudo /opt/ptms/sbin/ptmsctl product settings apply --update-server http://<IP-адрес  
локального сервера обновлений, установленного в изолированном сегменте сети>:8553
```

Например:

```
sudo /opt/ptms/sbin/ptmsctl product settings apply --update-server  
http://203.0.113.220:8553
```

2. На сервере или виртуальной машине с PT Sandbox (в многосерверной конфигурации — на каждом узле PT Sandbox) откройте файл `/etc/docker/daemon.json`:

```
sudo nano /etc/docker/daemon.json
```

3. В открывшемся файле в JSON-объект добавьте параметр `insecure-registries` с IP-адресом локального сервера обновлений, установленного в изолированном сегменте сети, и портом 8553.

Например:

```
{  
  "insecure-registries": [ "203.0.113.220:8553" ],  
  "log-driver": "json-file",  
  "log-opts": {  
    "max-size": "25m",  
    "max-file": "4"  
  }  
}
```

4. Сохраните изменения в файле `daemon.json`.
5. Примените изменения, перезапустив службу `docker`. Для этого последовательно выполните команды:

```
sudo service docker stop  
sudo service docker start
```

Примечание. Вы можете получить состояние службы `docker` при помощи команды `sudo service docker status`.

Источник обновлений PT Sandbox изменен на локальное зеркало.

PT Sandbox готов к обновлению. Если вы отключили автоматическое обновление в PT Sandbox, вы можете вручную запустить процедуру обновления. Если вы не отключали автоматическое обновление, PT Sandbox запустит обновление автоматически в течение установленного периода проверки обновлений (по умолчанию — 12 часов).

9.7. Настройка подключения к прокси-серверу

В процессе работы PT Sandbox может обращаться к внешним ресурсам. Если для доступа к внешним ресурсам в сети организации используется прокси-сервер, необходимо после установки настроить подключение продукта к прокси-серверу.

PT Sandbox может взаимодействовать с прокси-серверами типа HTTP.

► Чтобы настроить подключение PT Sandbox к прокси-серверу:

1. На основном узле выполните команду:

```
sudo /opt/ptms/sbin/ptmsctl product settings apply --proxy-server 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Имя пользователя>' --proxy-password '<Пароль>'
```

Например:

```
sudo /opt/ptms/sbin/ptmsctl product settings apply --proxy-server http://192.0.2.108:3128
```

Появится сообщение `Settings applied`.

2. На каждом узле кластера перейдите в каталог с распакованным установщиком и выполните команду:

```
sudo ./utils/install-k8s.sh --no-checks --proxy-addr 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Имя пользователя>' --proxy-password '<Пароль>'
```

Например:

```
sudo ./utils/install-k8s.sh --no-checks --proxy-addr 'http://192.0.2.108:3128' --proxy-user 'User' --proxy-password 'Password'
```

Появится сообщение `Kubernetes successfully installed`.

► Чтобы удалить параметры прокси-сервера:

1. На основном узле выполните команду:

```
sudo /opt/ptms/sbin/ptmsctl product settings apply --proxy-server ""
```

Появится сообщение `Settings applied`.

2. На каждом узле кластера перейдите в каталог с распакованным установщиком и выполните команду:

```
sudo ./utils/install-k8s.sh --no-checks
```

Появится сообщение `Kubernetes successfully installed`.

9.8. Настройка подключения к прокси-серверу с SSL-инспекцией

Для анализа веб-трафика, защищенного протоколом HTTPS, может использоваться прокси-сервер с SSL-инспекцией. Прокси-сервер с SSL-инспекцией расшифровывает и зашифровывает трафик, используя динамически формируемые сертификаты. Эти сертификаты удостоверяются корневым сертификатом.

Если для доступа к внешним ресурсам в сети организации используется прокси-сервер с SSL-инспекцией, необходимо в параметры PT Sandbox добавить пользовательский корневой сертификат.

В контексте работы PT Sandbox пользовательский корневой сертификат может быть использован для автоматического обновления продукта.

Примечание. В параметры PT Sandbox можно добавлять корневой сертификат только формата PEM.

- ▶ Чтобы добавить пользовательский корневой сертификат на этапе установки PT Sandbox,

в команде установки продукта укажите параметр `--proxy-ca-crt` /<Полный путь к файлу корневого сертификата>/rootCA.crt.

Например, команда для установки PT Sandbox с указанием параметров обновления продукта и добавлением корневого сертификата:

```
sudo ./install.sh --update-server https://multiscanner.example/ --serial-number '...' --  
proxy-ca-crt /opt/ptms/user_serts/rootCA.crt --proxy-addr http://192.0.2.108:3128
```

Появится сообщение `Kubernetes successfully installed`.

- ▶ Чтобы добавить пользовательский корневой сертификат на этапе установки дополнительного узла PT Sandbox,

в команде установки дополнительного узла укажите параметр `--proxy-ca-crt` /<Полный путь к файлу корневого сертификата>/rootCA.crt.

Например, команда для установки дополнительного узла PT Sandbox с добавлением корневого сертификата:

```
sudo ./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ah93de.ulgb1oah2uofp1kj --with-  
master-role --certificate-key  
b4fcff115509d64088a8da5ff29fd43434a002ec9c17260c295533e96d80fa4c --proxy-ca-crt '/home/  
username/rootCA.crt' --proxy-addr 'http://192.0.2.108:3128'
```

Появится сообщение `Kubernetes initialized`.

Вы можете добавить пользовательский корневой сертификат после установки PT Sandbox, а также заменить его или изменить его параметры.

- ▶ Чтобы добавить, заменить пользовательский корневой сертификат или изменить его параметры после установки PT Sandbox:

1. На основном узле выполните команду:

```
sudo /opt/ptms/sbin/ptmsctl product settings apply --proxy-ca-crt /<Полный путь к файлу  
корневого сертификата>/rootCA.crt --proxy-server http://<IP-адрес прокси-сервера>:<Порт>
```

Например:

```
sudo /opt/ptms/sbin/ptmsctl product settings apply --proxy-ca-crt opt/ptms/user_serts/  
rootCA.crt --proxy-server http://192.0.2.108:3128
```

Внимание! Если не указан адрес прокси-сервера, пользовательский корневой сертификат не будет применен.

Появится сообщение `Settings applied`.

2. На каждом узле кластера перейдите в каталог с распакованным установщиком и выполните команду:

```
sudo ./utils/install-k8s.sh --no-checks --proxy-addr 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Имя пользователя>' --proxy-password '<Пароль>' --proxy-ca-crt '<Полный путь к файлу корневого сертификата>'
```

Например:

```
sudo ./utils/install-k8s.sh --no-checks --proxy-addr 'http://192.0.2.108:3128' --proxy-user 'User' --proxy-password 'Password' --proxy-ca-crt '/home/username/rootCA.crt'
```

Появится сообщение `Kubernetes successfully installed`.

Вы можете удалить пользовательский корневой сертификат и параметры прокси-сервера, например если параметры прокси-сервера изменились.

- Чтобы удалить пользовательский корневой сертификат,

выполните команду:

```
sudo /opt/ptms/sbin/ptmsctl product settings apply --without-proxy-ca-crt
```

Появится сообщение `Settings applied`.

10. Вход в PT Sandbox

Пользовательский интерфейс PT Sandbox доступен в браузере. Вход зарегистрированного пользователя в PT Sandbox выполняется через сервис управления пользователями и доступом PT Identity and Access Management (PT IAM), который обеспечивает механизм единого входа (технология single sign-on) в приложения "Позитив Текнолоджиз".

Для администрирования PT Sandbox вам нужно войти в его интерфейс, используя учетную запись с ролью администратора.

► Чтобы войти в PT Sandbox:

1. В адресной строке браузера введите ссылку вида `https://<IP-адрес сервера или виртуальной машины с установленным PT Sandbox>`.

Примечание. В случае установленного кластера высокой доступности вместо IP-адреса основного узла нужно указать IP-адрес службы высокой доступности.

Откроется страница входа в PT IAM.

2. В поле **Логин** введите логин вашей учетной записи.
3. В поле **Пароль** введите пароль вашей учетной записи.
4. Нажмите кнопку **Войти**.

Откроется [страница со списком источников для проверки \(см. раздел 15\)](#).

11. Интерфейс PT Sandbox

Все действия в PT Sandbox вы можете выполнять с помощью графического пользовательского интерфейса. В этом разделе приводится описание основных элементов интерфейса PT Sandbox, доступных после входа в PT Sandbox.

В этом разделе

[Главное меню \(см. раздел 11.1\)](#)

[Центр уведомлений \(см. раздел 11.2\)](#)

[Страница со списком образов виртуальных машин \(см. раздел 11.3\)](#)

[Страница управления антивирусами \(см. раздел 11.4\)](#)

11.1. Главное меню

В верхней части любой страницы интерфейса PT Sandbox расположено главное меню.

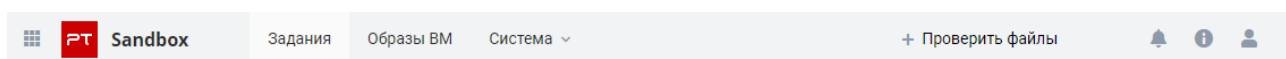



Рисунок 31. Главное меню

Главное меню PT Sandbox является ключевым элементом управления в интерфейсе PT Sandbox и обеспечивает доступ к основным функциям PT Sandbox.

Главное меню содержит разделы для перехода к страницам продукта:


- **Задания** — просмотр списка заданий на проверку файлов;
- **Образы ВМ** — просмотр информации о доступных для поведенческого анализа образах виртуальных машин;
- **Система** — управление и просмотр информации о PT Sandbox:
 - **Основные параметры** — управление записью событий в журнал аудита, изменение срока хранения истории проверок, настройка хранилища файлов, карантина и отправки сообщений в системный журнал по протоколу syslog;
 - **Источники для проверки** — добавление, удаление, управление источниками для проверки и настройка подключения к ним;
 - **Антивирусы** — управление антивирусами, используемыми PT Sandbox для сканирования файлов;
 - **Роли и права доступа** — просмотр списка ролей и соответствующих им прав доступа;
 - **Лицензия** — просмотр информации об активированной лицензии и ее замена.

В левой части главного меню находится кнопка  для перехода в другие приложения "Позитив Текнолоджиз", зарегистрированные в сервисе управления пользователями и доступом PT Identity and Access Management (PT IAM).

В правой части главного меню находятся элементы управления:

- Кнопка **Проверить файлы** для выборочной проверки файлов.
- Значок , по нажатию на который открывается [Центр уведомлений](#) (см. раздел 11.2).
На значке отображается количество уведомлений о результатах проверки файлов.
- Значок , по нажатию на который вы можете:
 - узнать версию PT Sandbox, установленную в организации;
 - получить информацию о состоянии компонентов PT Sandbox;
 - загрузить файлы журналов PT Sandbox на свой компьютер;
 - узнать контакты технической поддержки "Позитив Текнолоджиз".
- Значок , по нажатию на который вы можете просмотреть логин, с которым вы вошли в PT Sandbox, а также завершить работу под текущей учетной записью.

11.2. Центр уведомлений

По нажатию на значок  в главном меню открывается Центр уведомлений. Центр уведомлений — это всплывающее окно, в котором отображаются уведомления о проверке файлов, отправленных вами через интерфейс, а также уведомления об обновлении PT Sandbox.













Уведомления		Очистить 
installer.exe 21 мая, 16:25	Угроз не обнаружено	
archive.zip 21 мая, 16:26	Вирус   	
setup.exe 21 мая, 16:38	Рекламное ПО   	
package.zip 21 мая, 17:04	Троян   	
check.cmd 22 мая, 10:18	Угроз не обнаружено	
portable.zip 22 мая, 10:24	Проверяется 	

Рисунок 32. Центр уведомлений

В уведомлении о том, что файл проверяется (на белом фоне) отображаются имя файла и время начала проверки. Вы не можете удалять такие уведомления из Центра уведомлений, PT Sandbox удаляет их по завершении проверки.

В уведомлении о результате проверки файла отображаются название файла, информация о результате проверки файла и время завершения проверки. По нажатию на название файла в уведомлении открывается страница выполненного задания на проверку файла. Вы можете самостоятельно удалить уведомление по кнопке , которая появляется при наведении курсора мыши. Вы также можете удалить все уведомления по кнопке **Очистить**.

11.3. Страница со списком образов виртуальных машин

При выборе в главном меню раздела **Образы ВМ** открывается страница с информацией об образах виртуальных машин, которые используются для поведенческого анализа. Для каждого образа отображаются: имя, актуальная версия, дата установки версии, операционная система, статус образа.

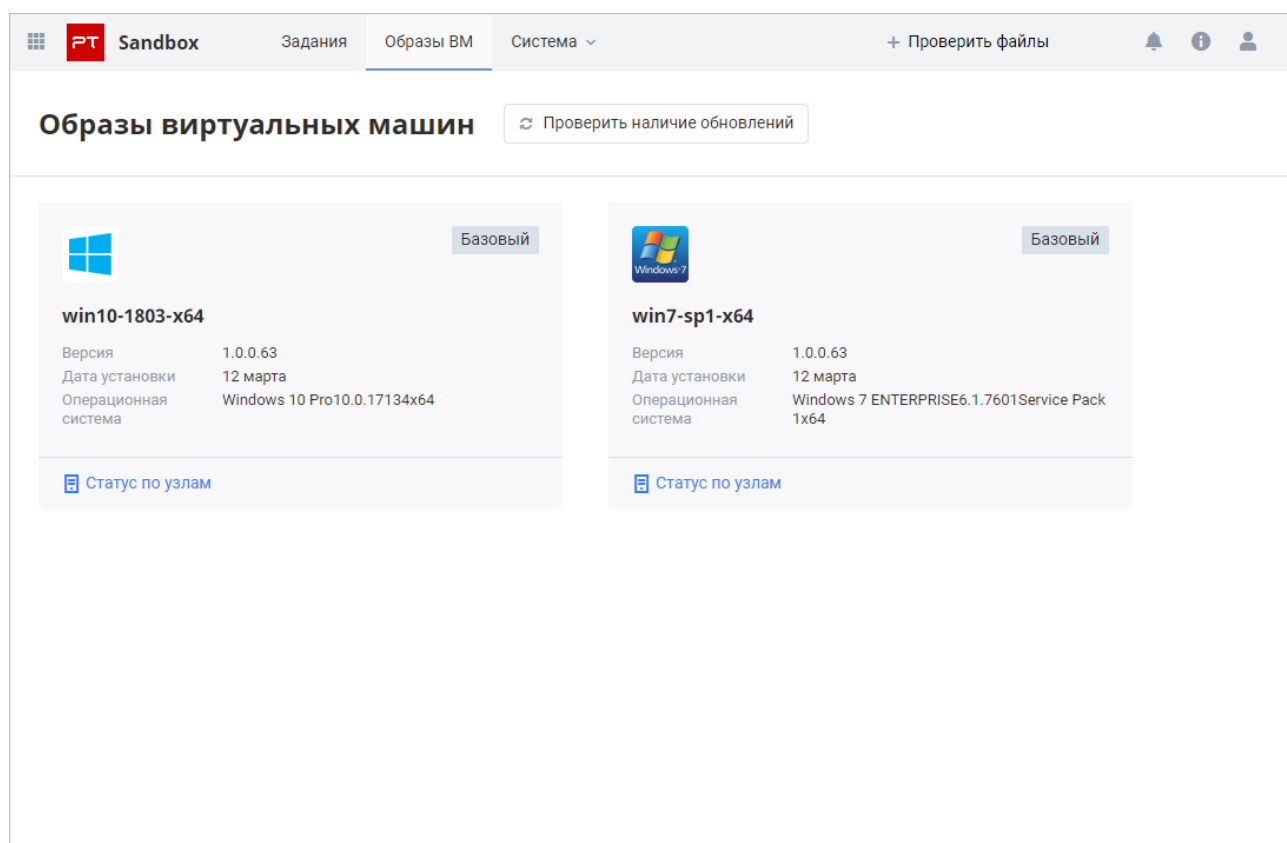


Рисунок 33. Образы виртуальных машин

Возможные статусы образов ВМ:

- **На все узлы установлена версия <Номер версии>** — образ последней доступной версии установлен на все узлы.
- **Устанавливается версия <Номер версии>** — образ последней доступной версии скачан в хранилище, но еще не установлен на все узлы.
- **Будет установлен образ версии <Номер версии>** — образ последней доступной версии доступен для скачивания или образ добавлен в лицензию.
- **Загружается версия <Номер версии>** — загрузка нового образа в хранилище для установки.

По ссылке **Статус по узлам** для каждого образа ВМ отображается информация об узлах, на которых образ установлен или устанавливается.

PT Sandbox периодически скачивает и устанавливает последние версии образов с сервера "Позитив Текнолоджиз". Вы можете самостоятельно проверить наличие новых версий на сервере по кнопке **Проверить наличие обновлений**.

11.4. Страница управления антивирусами

При выборе в главном меню в разделе **Система** пункта **Антивирусы** открывается страница с информацией об антивирусах, которые используются PT Sandbox для сканирования файлов.

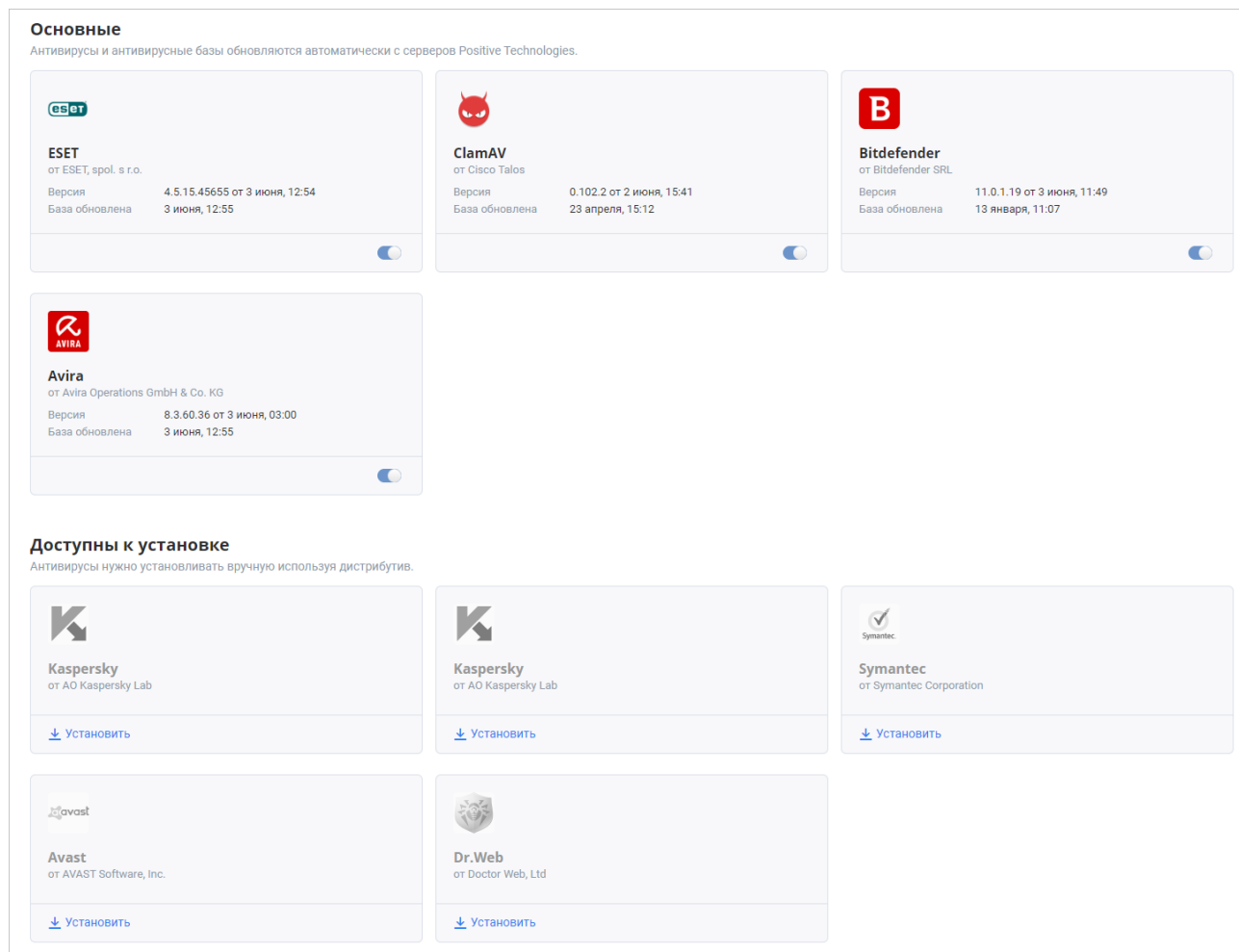


Рисунок 34. Просмотр информации об антивирусах

Информация об антивирусах включает в себя:

- название антивируса;
- название поставщика антивируса;
- версию антивируса;
- время, когда антивирус был впервые установлен или автоматически обновлен до указанной версии в PT Sandbox;
- время последнего обновления антивирусных баз.

Информация о выключенном антивирусе отображается в сером блоке.

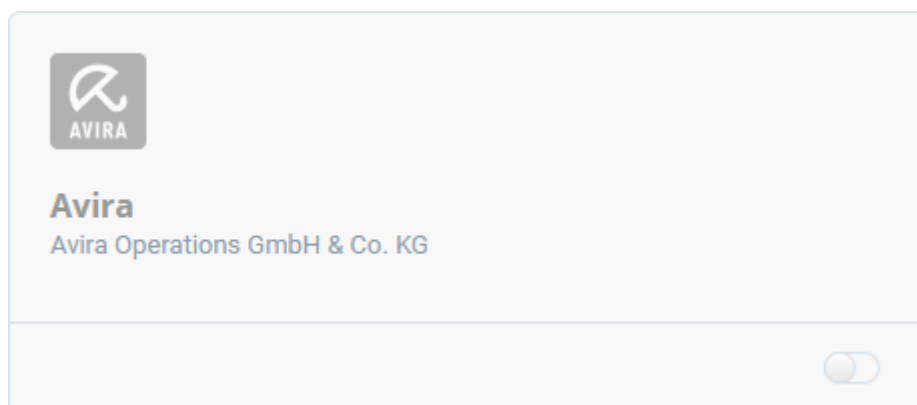


Рисунок 35. Информация о выключенном антивирусе

На этой странице вы также можете устанавливать, настраивать, обновлять и удалять дополнительные антивирусы, а также включать и выключать сканирование файлов любыми доступными вам антивирусами.

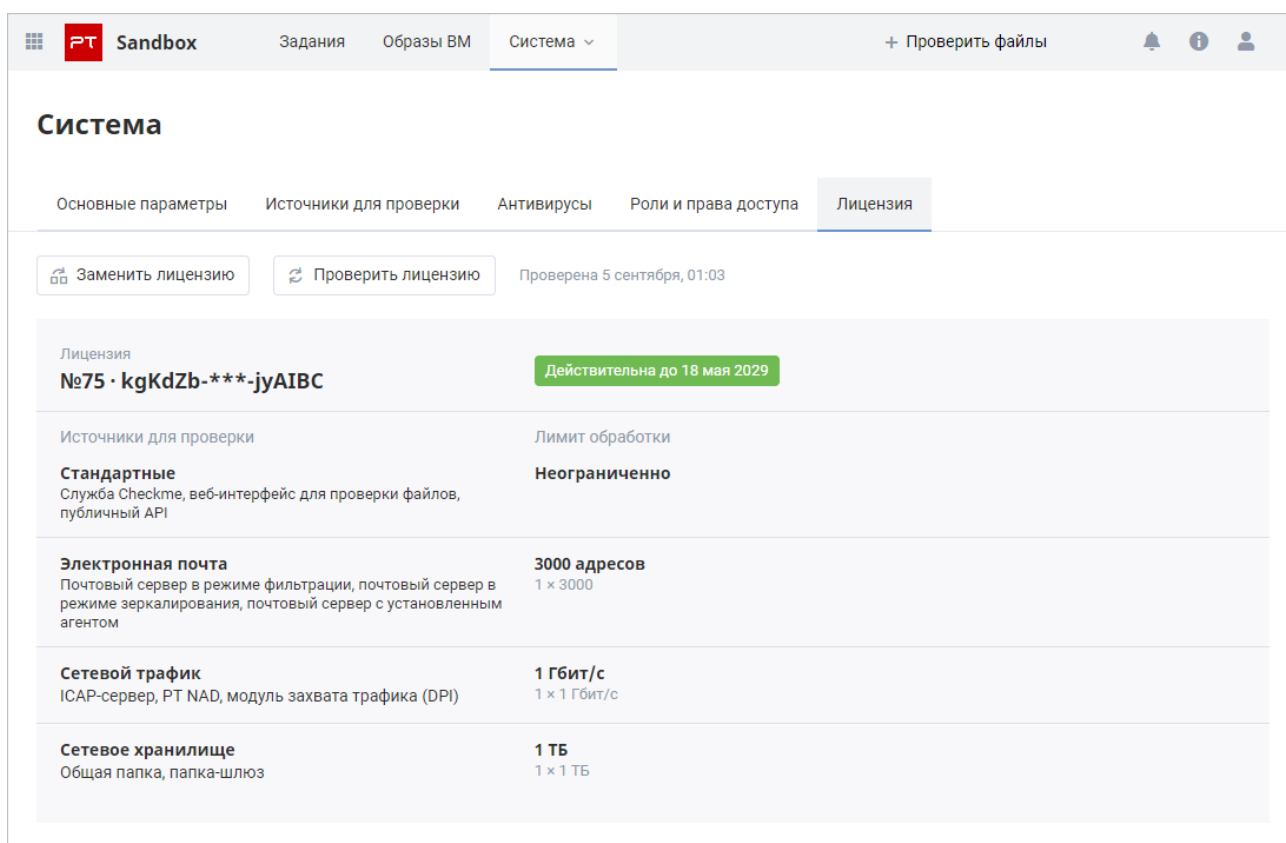
См. также

[Работа с антивирусами \(см. раздел 19\)](#)

12. Просмотр информации о лицензии PT Sandbox

Вы можете просмотреть параметры лицензии, в настоящий момент активированной в продукте.

- ▶ Чтобы просмотреть информацию о лицензии PT Sandbox, в главном меню в разделе **Система** выберите пункт **Лицензия**.
Откроется страница **Система** на вкладке **Лицензия**.



Система

Основные параметры Источники для проверки Антивирусы Роли и права доступа **Лицензия**

Заменить лицензию Проверить лицензию Проверена 5 сентября, 01:03

Лицензия №75 · kgKdZb-***-jyAIBC Действительна до 18 мая 2029	
Источники для проверки Стандартные Служба Checkme, веб-интерфейс для проверки файлов, публичный API	Лимит обработки Неограниченно
Электронная почта Почтовый сервер в режиме фильтрации, почтовый сервер в режиме зеркалирования, почтовый сервер с установленным агентом	3000 адресов 1 × 3000
Сетевой трафик ICAP-сервер, PT NAD, модуль захвата трафика (DPI)	1 Гбит/с 1 × 1 Гбит/с
Сетевое хранилище Общая папка, папка-шлюз	1 ТБ 1 × 1 ТБ

Рисунок 36. Просмотр информации о лицензии

См. также

[Лицензирование \(см. раздел 6\)](#)

13. Замена лицензии

Замена лицензии может потребоваться в следующих случаях:

- Одна и та же лицензия была активирована в нескольких экземплярах PT Sandbox. 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 Sandbox. 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 Sandbox менялась более трех раз (например, заменялись комплектующие сервера), вследствие чего лицензия стала недействительной. В таком случае вам нужно обратиться в службу технической поддержки "Позитив Текнолоджиз" для получения новой лицензии с теми же параметрами.

- Чтобы заменить лицензию:

1. В главном меню в разделе **Система** выберите пункт **Лицензия**.

Откроется страница **Система** на вкладке **Лицензия**.

2. Нажмите кнопку **Заменить лицензию**.

3. Во всплывающем окне введите серийный номер лицензии и нажмите кнопку **Заменить**.

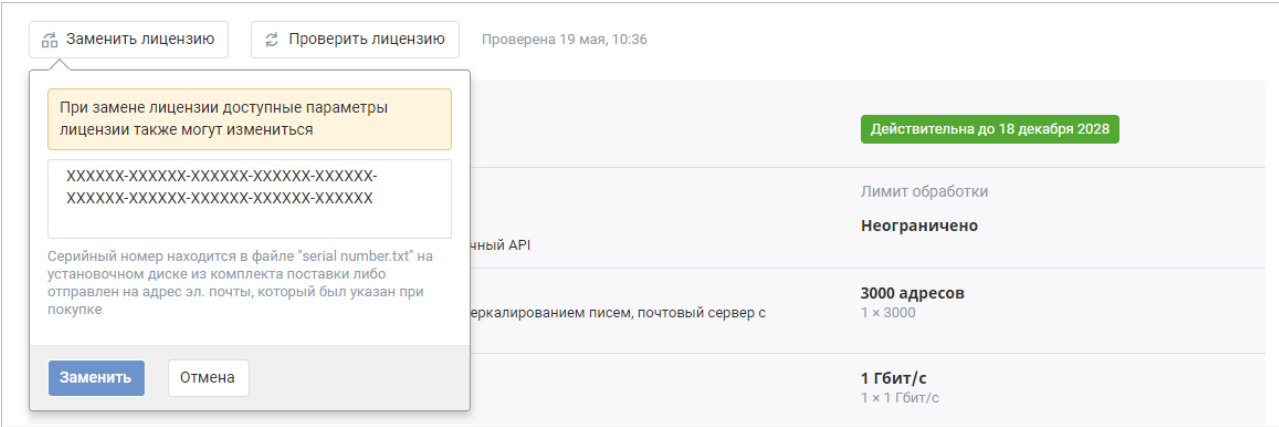


Рисунок 37. Замена лицензии

Информация о новой лицензии отобразится на странице.

Лицензия заменена.

Примечание. Рекомендуется сравнить параметры лицензии, перечисленные на странице, с указанными при заказе лицензии. В случае несоответствия вам нужно обратиться в службу технической поддержки "Позитив Текнолоджиз".

См. также

[Лицензирование \(см. раздел 6\)](#)

14. Добавление источников для проверки

Чтобы PT Sandbox мог получать файлы для проверки не только от пользователей через интерфейс, вам нужно добавить и настроить дополнительные источники для проверки.

В этом разделе

[Создание и настройка службы Checkme \(см. раздел 14.1\)](#)

[Настройка проверки трафика, поступающего от ICAP-сервера \(см. раздел 14.2\)](#)

[Настройка проверки почтового трафика организации \(см. раздел 14.3\)](#)

[Настройка проверки файлов в общей папке \(см. раздел 14.4\)](#)

[Настройка проверки файлов в папке-шлюзе \(см. раздел 14.5\)](#)

[Настройка проверки трафика организации при помощи модуля захвата трафика \(см. раздел 14.6\)](#)

[Настройка проверки трафика организации при помощи PT NAD \(см. раздел 14.7\)](#)

См. также

[Источники файлов и электронных писем, передаваемых на проверку \(см. раздел 4.2\)](#)

[Управление источниками для проверки \(см. раздел 15\)](#)

[Режимы проверки файлов и электронных писем \(см. раздел 4.3\)](#)

14.1. Создание и настройка службы Checkme

Служба Checkme позволяет пользователям самостоятельно отправлять файлы на проверку во вложениях писем на специальный корпоративный почтовый ящик.

Для создания и настройки службы Checkme вам нужно создать адрес электронной почты (например, `checkme@example.com`) на почтовом сервере вашей организации. На этот адрес сотрудники вашей организации смогут отправлять файлы для проверки в PT Sandbox. Чтобы PT Sandbox мог получать письма из этого ящика и отправлять результаты проверки в ответных письмах, вам нужно добавить и настроить источник для проверки, указав в его параметрах данные для доступа к адресу электронной почты службы Checkme: логин и пароль ящика, а также адреса и порты серверов IMAP и SMTP.

- Чтобы добавить и настроить источник для проверки писем и файлов, отправленных на адрес электронной почты службы Checkme:

1. В главном меню в разделе **Система** выберите пункт **Источники для проверки**.

Откроется страница **Система** на вкладке **Источники для проверки**.

2. Нажмите кнопку **Добавить источник**.

Откроется страница **Новый источник для проверки**.

3. В поле **Название** введите название источника, позволяющего проверять электронные письма и файлы, отправленные на адрес электронной почты службы Checkme.

Введенное название будет отображаться для операторов безопасности среди информации об электронных письмах и файлах, полученных от службы Checkme.

Примечание. Название должно содержать не менее пяти символов, среди которых могут быть только строчные буквы латинского алфавита, цифры и дефис. Первым и последним символами могут быть только буквы. Название должно быть уникальным среди названий источников любых типов в экземпляре PT Sandbox, в том числе среди названий удаленных источников.

4. В раскрывающемся списке **Тип** выберите **Checkme**.

На странице отобразятся параметры службы Checkme.

Название и тип	Название <input type="text" value="checkme"/> Тип <input type="text" value="Checkme"/>
Параметры соединения	Адрес IMAP-сервера <input type="text" value="198.51.100.44"/> : <input type="text" value="993"/> <input checked="" type="checkbox"/> Подключаться по SSL Адрес SMTP-сервера <input type="text" value="198.51.100.31"/> : <input type="text" value="465"/> <input checked="" type="checkbox"/> Подключаться по SSL
Аутентификация	Тип аутентификации IMAP <input type="text" value="Выбирать автоматически"/> Тип аутентификации SMTP <input type="text" value="Выбирать автоматически"/> Логин: <input type="text" value="username"/> Пароль: <input type="password" value="....."/>
Адрес службы Checkme	Электронная почта <input type="text" value="checkme@example.com"/> <small>Адрес электронной почты для отправки файлов пользователями на проверку</small>

Рисунок 38. Настройка службы Checkme

5. В полях **Адрес IMAP-сервера** и **Адрес SMTP-сервера** введите IP-адреса и порты IMAP-сервера (для получения писем с вложениями для проверки) и SMTP-сервера (для отправки пользователям ответных писем с результатами проверки).
6. Если соединение с указанными серверами устанавливается по протоколу SSL, установите флажки **Подключаться по SSL** под соответствующими полями.

7. В блоке параметров **Аутентификация** настройте аутентификацию для подключения к IMAP- и SMTP-серверам:
 - Если политика информационной безопасности вашей организации или указанные серверы допускают только определенный тип аутентификации, выберите его в раскрывающихся списках **Тип аутентификации IMAP** и **Тип аутентификации SMTP**.

Примечание. По умолчанию PT Sandbox автоматически выбирает наиболее безопасный тип аутентификации из предложенных удаленным почтовым сервером.

 - В полях **Логин** и **Пароль** введите логин и пароль для доступа к указанным серверам.
8. В поле **Электронная почта** введите адрес электронной почты службы Checkme, например checkme@example.com.
9. Нажмите кнопку **Добавить**.

Источник добавлен и настроен.

См. также

[Отправка файлов на проверку по электронной почте \(см. раздел 16.2\)](#)

14.2. Настройка проверки трафика, поступающего от ICAP-сервера

Вы можете настроить перехват интернет-трафика в организации и уведомления службы ИБ об угрозах, обнаруженных в этом трафике. Для этого PT Sandbox интегрируется с системами обнаружения и предотвращения вторжений (IDS, IPS), прокси-серверами и другими средствами, поддерживающими ICAP. Интеграция позволит настроить проверку всех файлов, загруженных из внешних подсетей, в автоматическом режиме.

Также вы можете настроить контроль важнейших каталогов веб-приложений и порталов организации. Для этого вам нужно интегрировать PT Sandbox с решениями для защиты веб-приложений (web application firewalls, WAF), например с Positive Technologies Application Firewall (PT AF), посредством ICAP. Такая интеграция позволяет проверять загружаемый контент антивирусами и дополнительно защищать веб-приложение от внешних угроз при помощи межсетевого экрана.

В зависимости от приобретенной вами лицензии на продукт PT Sandbox может блокировать файлы, представляющие угрозу, или только проверять файлы, поступающие на проверку по ICAP.

В этом разделе

[Создание и настройка ICAP-сервера PT Sandbox \(см. раздел 14.2.1\)](#)

[Настройка ICAP-клиента для интеграции с PT Sandbox \(см. раздел 14.2.2\)](#)

14.2.1. Создание и настройка ICAP-сервера PT Sandbox

Для интеграции PT Sandbox с PT AF или с системами обнаружения и предотвращения вторжений (IDS, IPS) вам нужно создать и настроить ICAP-сервер.

► Чтобы создать и настроить ICAP-сервер:

1. В главном меню в разделе **Система** выберите пункт **Источники для проверки**.

Откроется страница **Система** на вкладке **Источники для проверки**.

2. Нажмите кнопку **Добавить источник**.

Откроется страница **Новый источник для проверки**.

3. В поле **Название** введите название ICAP-сервера.

Название ICAP-сервера будет отображаться для операторов безопасности среди информации о файлах, поступивших на проверку от этого сервера.

Примечание. Название должно содержать не менее пяти символов, среди которых могут быть только строчные буквы латинского алфавита, цифры и дефис. Первым и последним символами могут быть только буквы. Название должно быть уникальным среди названий источников любых типов в экземпляре PT Sandbox, в том числе среди названий удаленных источников.

4. В раскрывающемся списке **Тип** выберите **ICAP-сервер**.

На странице отобразятся параметры ICAP-сервера.

Название и тип	<p>Название</p> <input type="text" value="icap-server"/> <p>Тип</p> <input type="text" value="ICAP-сервер"/>
Параметры соединения Установите на своем прокси-сервере данные параметры соединения	<p>Адрес сервера</p> <input type="text" value="198.51.100.22"/> : <input type="text" value="1344"/> <p>Не забудьте настроить на ICAP-клиенте режим блокировки файлов и время ожидания поведенческого анализа.</p>

Рисунок 39. Настройка параметров ICAP-сервера

5. При необходимости в поле **Адрес сервера** измените стандартный TCP-порт (1344) для подключения к ICAP-серверу.

6. Нажмите кнопку **Добавить**.

ICAP-сервер создан и настроен.

Теперь вам нужно настроить внешний ICAP-клиент, который будет взаимодействовать с ICAP-сервером PT Sandbox. Если в качестве ICAP-клиента выступает PT AF, вам или администратору PT AF нужно выполнить настройку этого продукта (подробнее см. в разделе об интеграции с продуктами "Позитив Текнолоджиз" в Руководстве администратора PT AF).

14.2.2. Настройка ICAP-клиента для интеграции с PT Sandbox

Для того чтобы обеспечить взаимодействие стороннего ICAP-клиента с ICAP-сервером PT Sandbox, в параметрах ICAP-клиента вам нужно настроить:

- доступ к ICAP-службам PT Sandbox;
- URI для отправки запросов на ICAP-сервер PT Sandbox и получения ответов от него;
- отправку поля заголовка X-Client-IP с IP-адресом пользователя, который получил контент или отправил HTTP-запрос (при необходимости записи этой информации в результаты проверки).

ICAP-сервер PT Sandbox поддерживает следующие методы запросов:

- REQMOD — используется для проверки трафика, передаваемого за пределы информационной системы вашей организации;
- RESPMOD — используется для проверки трафика, передаваемого извне в информационную систему вашей организации;
- OPTIONS — используется для запроса ICAP-клиентом конфигурации ICAP-сервера.

В этом разделе приводятся инструкции по настройке ICAP-клиента в зависимости от режима проверки трафика, поступающего по ICAP.

В этом разделе

[Настройка проверки посредством ICAP в блокирующем режиме \(см. раздел 14.2.2.1\)](#)

[Настройка проверки посредством ICAP в режиме ожидания \(см. раздел 14.2.2.2\)](#)

[Настройка проверки посредством ICAP в пассивном режиме \(см. раздел 14.2.2.3\)](#)

[Настройка ICAP-клиента на примере прокси-сервера Squid \(см. раздел 14.2.2.4\)](#)

14.2.2.1. Настройка проверки посредством ICAP в блокирующем режиме

В блокирующем режиме файлы, поступившие на проверку от ICAP-сервера, не пропускаются продуктом в информационную систему организации, если по результатам проверки они представляют угрозу.

Внимание! При блокирующем режиме проверки файлов максимальный размер файла, передаваемого ICAP-серверу PT Sandbox, не должен превышать 1 ГБ. Иначе файл может не быть передан его получателю.

Примечание. Использование блокирующего режима может быть ограничено [лицензией](#) (см. раздел 12).

Настройка выполняется в параметрах стороннего ICAP-клиента, например [прокси-сервера Squid](#) (см. раздел 14.2.2.4). Перед настройкой ICAP-клиента вам нужно [добавить в список источников ICAP-сервер](#) (см. раздел 14.2.1).

► Чтобы настроить проверку по ICAP в блокирующем режиме:

1. Настройте доступ к ICAP-серверу PT Sandbox, используя URI в следующем формате:

`icap://<IP-адрес ICAP-сервера>:<Порт ICAP>/<Режим ICAP>?timeout=<Тайм-аут сканирования>`

где:

- Вместо <IP-адрес ICAP-сервера> и <Порт ICAP> укажите IP-адрес и порт из [параметров ICAP-сервера](#) (см. раздел 14.2.1).
- Вместо <Режим ICAP> укажите `scan-request` для режима REQMOD или `scan-response` для режима RESPMOD.
- Вместо <Тайм-аут сканирования> укажите тайм-аут сканирования в секундах, по превышении которого контент передается как есть.

Примечание. По умолчанию тайм-аут равен 30 секундам.

Примеры URI:

`icap://198.51.100.32:1344/scan-request`

`icap://198.51.100.32:1344/scan-response`

`icap://198.51.100.32:1344/scan-response?timeout=90`

2. Настройте отправку поля заголовка X-Client-IP с IP-адресом пользователя, скачавшего или отправившего файл (при необходимости записи этой информации в результаты проверки).

Проверка по ICAP в блокирующем режиме настроена.

14.2.2.2. Настройка проверки посредством ICAP в режиме ожидания

В режиме ожидания при обнаружении угрозы ICAP-сервер PT Sandbox не изменяет проверенный контент, а только добавляет в заголовок ответа 204 поле X-Virus-ID с кратким описанием обнаруженной угрозы. Таким образом, режим ожидания может использоваться для интеграции PT Sandbox со сторонними системами, самостоятельно принимающими решения о блокировке контента, например с PT AF.

Если вам нужно проверять, но пропускать весь трафик в информационную систему организации, [настройте проверку в пассивном режиме](#) (см. раздел 14.2.2.3).

Настройка выполняется в параметрах стороннего ICAP-клиента, например [прокси-сервера Squid](#) (см. раздел 14.2.2.4). Перед настройкой ICAP-клиента вам нужно [добавить в список источников ICAP-сервер](#) (см. раздел 14.2.1).

► Чтобы настроить проверку по ICAP в режиме ожидания:

1. Настройте доступ к ICAP-серверу PT Sandbox, используя URI в следующем формате:

```
icap://<IP-адрес ICAP-сервера>:<Порт ICAP>/<Режим ICAP>?modify=no&timeout=<Тайм-аут сканирования>
```

где:

- Вместо <IP-адрес ICAP-сервера> и <Порт ICAP> укажите IP-адрес и порт из [параметров ICAP-сервера \(см. раздел 14.2.1\)](#).
- Вместо <Режим ICAP> укажите scan-request для режима REQMOD или scan-response для режима RESPMOD.
- Вместо <Тайм-аут сканирования> укажите тайм-аут сканирования в секундах, по превышении которого контент передается как есть.

Примечание. По умолчанию тайм-аут равен 30 секундам.

Примеры URI:

```
icap://198.51.100.32:1344/scan-request?modify=no
```

```
icap://198.51.100.32:1344/scan-response?modify=no
```

```
icap://198.51.100.32:1344/scan-response?modify=no&timeout=90
```

2. Настройте отправку поля заголовка X-Client-IP с IP-адресом пользователя, скачавшего или отправившего файл (при необходимости записи этой информации в результаты проверки).

Проверка по ICAP в режиме ожидания настроена.

14.2.2.3. Настройка проверки посредством ICAP в пассивном режиме

В пассивном режиме весь трафик, проходящий через ICAP-сервер продукта, пропускается в информационную систему вашей организации или за ее пределы. В отличие от режима ожидания, в пассивном режиме трафик не задерживается на время сканирования, а пропускается в инфраструктуру одновременно с передачей в антивирусы.

Настройка выполняется в параметрах стороннего ICAP-клиента, например [прокси-сервера Squid \(см. раздел 14.2.2.4\)](#). Перед настройкой ICAP-клиента вам нужно [добавить в список источников ICAP-сервер \(см. раздел 14.2.1\)](#).

► Чтобы настроить проверку по ICAP в пассивном режиме:

1. Настройте доступ к ICAP-серверу PT Sandbox, используя URI в следующем формате:

```
icap://<IP-адрес ICAP-сервера>:<Порт ICAP>/bypass
```

где вместо <IP-адрес ICAP-сервера> и <Порт ICAP> укажите IP-адрес и порт из [параметров ICAP-сервера \(см. раздел 14.2.1\)](#).

Например:

```
icap://198.51.100.32:1344/bypass
```

Примечание. Для настройки проверки в пассивном режиме нужно использовать указанный формат URI как для метода REQMOD, так и для RESPMOD.

2. Настройте отправку поля заголовка X-Client-IP с IP-адресом пользователя, скачавшего или отправившего файл (при необходимости записи этой информации в результаты проверки).

Проверка по ICAP в пассивном режиме настроена.

14.2.2.4. Настройка ICAP-клиента на примере прокси-сервера Squid

Ниже приводится инструкция по настройке ICAP-клиента для проверки файлов в блокирующем режиме на примере прокси-сервера Squid без описания настройки аутентификации пользователей. Более подробную информацию о настройке Squid вы можете получить на [сайте производителя](#).

► Чтобы настроить прокси-сервер Squid:

1. В любом редакторе простых текстовых файлов откройте файл `/etc/squid3/squid.conf`, расположенный на сервере или виртуальной машине с установленным прокси-сервером Squid.

Например:

```
sudo nano /etc/squid3/squid.conf
```

Внимание! Перед изменением файла сделайте его резервную копию.

Примечание. В некоторых версиях Squid файл `squid.conf` может находиться в каталоге `/etc/squid` или `/usr/local/squid/etc`.

2. Включите модуль ICAP. Для этого добавьте в любое место в файле следующую строку:

```
icap_enable on
```

3. Настройте подключение к ICAP-серверу PT Sandbox:

- Чтобы на ICAP-сервер поступал трафик, который передается от пользователя на внешний ресурс за прокси-сервером Squid, добавьте в любое место в файле следующую строку:

```
icap_service <Произвольное название ICAP-службы> reqmod_precache icap://<IP-адрес ICAP-сервера>:<Порт ICAP>/scan-request
```

- Чтобы на ICAP-сервер поступал трафик, который передается от внешнего ресурса пользователю за прокси-сервером Squid, добавьте в любое место в файле следующую строку:

```
icap_service <Произвольное название ICAP-службы> respmod_precache icap://<IP-адрес ICAP-сервера>:<Порт ICAP>/scan-response
```

Вместо `<IP-адрес ICAP-сервера>` и `<Порт ICAP>` в обеих строках укажите IP-адрес и порт из [параметров ICAP-сервера \(см. раздел 14.2.1\)](#).

Например:

```
icap_service ptsb_req reqmod_precache icap://198.51.100.32:1344/scan-request
icap_service ptsb_resp respmod_precache icap://198.51.100.32:1344/scan-response
```

Примечание. По умолчанию в случае ошибок или недоступности ICAP-служб PT Sandbox прокси-сервер Squid передает HTTP-клиенту страницу с сообщением об ошибке. Если вам нужно настроить обязательную пересылку сообщений, которые не были обработаны из-за ошибок или недоступности ICAP-сервера PT Sandbox, вам нужно добавить в конец строки `icap_service` параметр `bypass=1`. Например:
`icap_service ptsb_resp respmod_precache icap://198.51.100.32:1344/scan-response bypass=1`.

Примечание. По умолчанию Squid игнорирует ICAP-службу PT Sandbox, если одновременных соединений с ней больше 128. Вы можете переопределить это число при помощи параметра `max-conn` и настроить поведение Squid в случае перегрузок при помощи параметра `on-overload`.

4. Настройте доступ к ICAP-службам, указанным на предыдущем шаге. Для этого добавьте в любое место в файле строки в следующем формате:

```
adaptation_access <Название ICAP-службы> <Параметры доступа>
```

Например:

```
adaptation_access ptsb_req allow all
adaptation_access ptsb_resp allow all
```

5. Чтобы Squid отправлял поле заголовка X-Client-IP с IP-адресом пользователя, скачавшего файл, добавьте в любое место в файле строку:

```
adaptation_send_client_ip on
```

6. Чтобы Squid отправлял поле заголовка X-Client-Username с именем пользователя, скачавшего файл, добавьте в любое место в файле две следующие строки:

```
adaptation_send_username on
icap_client_username_header X-Client-Username
```

7. Сохраните изменения в файле `squid.conf`.

8. Чтобы изменения вступили в силу, перезапустите процесс прокси-сервера Squid:

```
sudo service squid3 reload
```

Примечание. В некоторых версиях Squid перезапуск процесса осуществляется командой `sudo service squid reload`.

Прокси-сервер Squid настроен.

14.3. Настройка проверки почтового трафика организации

PT Sandbox позволяет автоматически обнаруживать угрозы в почтовом трафике организации. Для этого PT Sandbox интегрируется с одним или несколькими почтовыми серверами организации. PT Sandbox проверяет, представляют ли угрозу письма и почтовые вложения, в том числе архивированные, разделенные на части и защищенные паролями.

В этом разделе

[Подключение к почтовому серверу при помощи агента \(см. раздел 14.3.1\)](#)

[Настройка зеркалирования почтового трафика с помощью bcc \(см. раздел 14.3.2\)](#)

[Настройка фильтрации почтового трафика \(см. раздел 14.3.3\)](#)

14.3.1. Подключение к почтовому серверу при помощи агента

Если в вашей организации используется почтовый сервер Microsoft Exchange 2010, 2013 или 2016, вы можете организовать проверку почтового трафика при помощи почтового агента. В отличие от настройки отправки скрытых копий (bcc) интеграция с почтовым сервером с помощью агента является более простым и надежным вариантом интеграции с Microsoft Exchange и позволяет операторам безопасности настраивать блокировку писем, представляющих угрозу безопасности.

Чтобы подключить PT Sandbox к почтовому серверу при помощи агента, вам нужно:

1. Установить почтовый агент PT Sandbox на сервере Microsoft Exchange.
2. Добавить источник для проверки с параметрами установленного почтового агента в интерфейсе PT Sandbox.

Почтовый агент PT Sandbox будет перехватывать все письма, проходящие через сервер Microsoft Exchange организации, и отправлять их на проверку.

В этом разделе

[Установка почтового агента с параметрами по умолчанию \(см. раздел 14.3.1.1\)](#)

[Установка почтового агента с переопределенными параметрами \(см. раздел 14.3.1.2\)](#)

[Подключение PT Sandbox к почтовому агенту \(см. раздел 14.3.1.3\)](#)

14.3.1.1. Установка почтового агента с параметрами по умолчанию

В этом разделе описывается простая установка почтового агента без указания сетевого интерфейса для перехвата писем и без изменения стандартного TCP-порта (7536).

Перед установкой почтового агента вам нужно проверить версию Microsoft Exchange, установленную в вашей организации. Почтовый агент работает:

- с Microsoft Exchange 2010 (версия 14);
- Microsoft Exchange 2013 (версия 15.0, кроме 15.0.847.32);
- Microsoft Exchange 2016 (версия 15.1, она же 15.01).

► Чтобы установить почтовый агент с параметрами по умолчанию:

1. Скопируйте архив с установщиком почтового агента на узел с Microsoft Exchange.
2. Распакуйте скопированный архив в любую папку и откройте эту папку.
3. В контекстном меню файла `install.cmd` выберите пункт **Run as administrator**.

Откроется окно интерфейса командной строки. Начнется установка почтового агента. По завершении установки окно закроется.

Почтовый агент установлен с параметрами по умолчанию.

Теперь вы можете перейти к [подключению почтового агента \(см. раздел 14.3.1.3\)](#) в интерфейсе PT Sandbox.

14.3.1.2. Установка почтового агента с переопределенными параметрами

Если на узле с Microsoft Exchange работает несколько сетевых интерфейсов, то для установки почтового агента вам нужно указать IP-адрес конкретного интерфейса, с которого должен перехватываться почтовый трафик. Также вы можете переопределить стандартный TCP-порт агента (7536), если этот порт уже используется для других целей или по какой-то причине запрещен.

Перед установкой почтового агента вам нужно проверить версию Microsoft Exchange, установленную в вашей организации. Почтовый агент работает:

- с Microsoft Exchange 2010 (версия 14);
- Microsoft Exchange 2013 (версия 15.0, кроме 15.0.847.32);
- Microsoft Exchange 2016 (версия 15.1, она же 15.01).

► Чтобы установить почтовый агент с переопределенными параметрами:

1. Скопируйте архив с установщиком почтового агента на узел с Microsoft Exchange.
2. Распакуйте скопированный архив в любую папку.
3. Запустите Windows PowerShell от имени администратора.
4. В окне Windows PowerShell перейдите в каталог с распакованным архивом.

Например:

```
cd D:\exchange-mta
```

5. Запустите установку почтового агента, указав IP-адрес сетевого интерфейса и порт:


```
.\install.ps1 -BalancerEndpoint "<IP-адрес сетевого интерфейса>:<TCP-порт>"
```

Например:

```
.\install.ps1 -BalancerEndpoint "203.0.113.11:7936"
```

Примечание. Для указания стандартного IP-адреса сетевого интерфейса введите `0.0.0.0`.

Начнется установка почтового агента. По окончании установки появится сообщение `Installation completed`.

Почтовый агент установлен с переопределенными параметрами.

Теперь вы можете перейти к [подключению почтового агента \(см. раздел 14.3.1.3\)](#) в интерфейсе PT Sandbox.

14.3.1.3. Подключение PT Sandbox к почтовому агенту

После установки почтового агента с параметрами по умолчанию или переопределенными параметрами вам нужно настроить его в интерфейсе PT Sandbox.

- Чтобы подключить почтовый агент к PT Sandbox:
- В главном меню в разделе **Система** выберите пункт **Источники для проверки**.
Откроется страница **Система** на вкладке **Источники для проверки**.
 - Нажмите кнопку **Добавить источник**.
Откроется страница **Новый источник для проверки**.
 - В поле **Название** введите название почтового агента.
Название агента будет отображаться для операторов безопасности среди информации об электронных письмах и файлах, поступивших на проверку от этого агента.
Примечание. Название должно содержать не менее пяти символов, среди которых могут быть только строчные буквы латинского алфавита, цифры и дефис. Первым и последним символами могут быть только буквы. Название должно быть уникальным среди названий источников любых типов в экземпляре PT Sandbox, в том числе среди названий удаленных источников.
 - В раскрывающемся списке **Тип** выберите **Почтовый сервер с установленным агентом**.
На странице отобразятся параметры подключения к почтовому агенту.

Название и тип	Название
	<input type="text" value="mail-agent"/>
	Тип
	<div>Почтовый сервер с установленным агентом</div>
Параметры соединения	Адрес сервера
	<div><input type="text" value="198.51.100.97"/> : <input type="text" value="7536"/></div>

Рисунок 40. Настройка подключения к почтовому агенту

5. В поле **Адрес сервера** введите IP-адрес сервера Microsoft Exchange и укажите TCP-порт почтового агента (по умолчанию — 7536).
6. Нажмите кнопку **Добавить**.

Почтовый агент подключен к PT Sandbox.

14.3.2. Настройка зеркалирования почтового трафика с помощью bcc

Вы можете настроить отправку скрытых копий (bcc) всех писем, которые поступают и отправляются с почтового сервера организации, на проверку в PT Sandbox в пассивном режиме. В отличие от зеркалирования с помощью почтового агента отправка скрытых копий может быть настроена практически с любого почтового сервера. Также зеркалирование с помощью bcc может пригодиться, если вы против интеграции сторонних расширений в сервер Microsoft Exchange.

Для отправки скрытых копий в PT Sandbox вам нужно добавить источник с типом "Почтовый сервер в режиме зеркалирования" в интерфейсе PT Sandbox и указать в параметрах почтового сервера адрес и порт сервера из параметров этого источника при настройке bcc.

В этом разделе приводятся примеры настройки почтовых серверов различных производителей для интеграции с PT Sandbox.

В этом разделе

[Создание bcc-сервера PT Sandbox \(см. раздел 14.3.2.1\)](#)

[Настройка зеркалирования трафика с Postfix \(см. раздел 14.3.2.2\)](#)

[Настройка зеркалирования трафика с Exim \(см. раздел 14.3.2.3\)](#)

[Настройка зеркалирования трафика с Microsoft Exchange \(см. раздел 14.3.2.4\)](#)

14.3.2.1. Создание bcc-сервера PT Sandbox

Перед тем как начать настраивать отправку скрытых копий на почтовом сервере организации, вам нужно создать bcc-сервер в интерфейсе PT Sandbox. На адрес созданного сервера будут отправляться скрытые копии писем.

► Чтобы создать bcc-сервер PT Sandbox:

1. В главном меню в разделе **Система** выберите пункт **Источники для проверки**.
Откроется страница **Система** на вкладке **Источники для проверки**.
2. Нажмите кнопку **Добавить источник**.
Откроется страница **Новый источник для проверки**.
3. В поле **Название** введите название bcc-сервера PT Sandbox.

Название бсс-сервера будет отображаться для операторов безопасности среди информации о письмах и файлах, поступивших на проверку от этого сервера.

Примечание. Название должно содержать не менее пяти символов, среди которых могут быть только строчные буквы латинского алфавита, цифры и дефис. Первым и последним символами могут быть только буквы. Название должно быть уникальным среди названий источников любых типов в экземпляре PT Sandbox, в том числе среди названий удаленных источников.

4. В раскрывающемся списке **Тип** выберите **Почтовый сервер в режиме зеркалирования**.

На странице отобразятся параметры бсс-сервера.

Название и тип	Название <input type="text" value="mail-bcc"/> Тип <input type="text" value="Почтовый сервер в режиме зеркалирования"/>
Параметры соединения Настройте отправку копий всех писем в PT Sandbox для проверки. Используйте указанные параметры на вашем почтовом сервере.	Адрес сервера <input type="text" value="198.51.100.22"/> : <input type="text" value="25"/> <input checked="" type="checkbox"/> Требовать подключение по SSL

Рисунок 41. Настройка параметров бсс-сервера PT Sandbox

5. Если вам нужно, чтобы почтовый сервер отправлял скрытые копии по TCP-порту, отличному от 25, в поле **Адрес сервера** измените номер порта.
6. Если подключение к почтовому серверу осуществляется по защищенному протоколу (SMTP по SSL), установите флажок **Требовать подключение по SSL**.

Примечание. Если флажок снят, данные, передаваемые на бсс-сервер, будут зашифровываться при помощи расширения STARTTLS. Если флажок снят, а почтовый сервер организации не поддерживает STARTTLS, данные будут передаваться без шифрования.

7. Нажмите кнопку **Добавить**.

Бсс-сервер PT Sandbox создан.

Теперь вы можете приступить к настройке почтового сервера вашей организации для отправки скрытых копий всех писем на созданный бсс-сервер.

См. также

[Настройка зеркалирования трафика с Microsoft Exchange \(см. раздел 14.3.2.4\)](#)

[Настройка зеркалирования трафика с Postfix \(см. раздел 14.3.2.2\)](#)

[Настройка зеркалирования трафика с Exim \(см. раздел 14.3.2.3\)](#)

14.3.2.2. Настройка зеркалирования трафика с Postfix

Инструкция актуальна для агента пересылки почтовых сообщений Postfix версии 3.2.

Перед началом настройки вам нужно [создать бсс-сервер](#) (см. раздел 14.3.2.1).

► Чтобы настроить зеркалирование трафика с Postfix:

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

```
sudo nano /etc/postfix/main.cf
```
2. Добавьте в любое место в файле две строки:

```
always_bcc = bcc@sandbox.local
transport_maps = hash:/etc/postfix/transport
```
3. Сохраните изменения в файле `main.cf`.
4. Создайте файл `/etc/postfix/transport`:

```
sudo nano /etc/postfix/transport
```
5. Добавьте в файл строку в следующем формате:

```
bcc@sandbox.local smtp:[<IP-адрес бсс-сервера PT Sandbox>]:<Номер TCP-порта для SMTP, если отличается от 25>
```


 Например:

```
bcc@sandbox.local smtp:[203.0.113.203]
```
6. Сохраните файл `transport`.
7. Обновите файл соответствий:

```
sudo postmap /etc/postfix/transport
```
8. Чтобы изменения вступили в силу, перезапустите Postfix:

```
sudo systemctl restart postfix
```

Зеркалирование трафика с Postfix настроено.

14.3.2.3. Настройка зеркалирования трафика с Exim

Инструкция актуальна для агента пересылки почтовых сообщений Exim версии 4 с отдельными файлами конфигурации. Если в вашей организации все параметры Exim хранятся в едином конфигурационном файле, вам нужно добавлять указанные в инструкции строки в этот файл. Подробную информацию о настройке Exim вы можете получить на сайте exim.org.

Перед началом настройки вам нужно [создать бсс-сервер](#) (см. раздел 14.3.2.1).

► Чтобы настроить зеркалирование трафика с Exim:

1. Создайте файл `/etc/exim4/conf.d/router/03_exim4-config_redirect`:

```
sudo nano /etc/exim4/conf.d/router/03_exim4-config_redirect
```
2. Добавьте в файл следующее содержимое и сохраните изменения:

```
bcc:
    driver = redirect
```

```
data = bcc@sandbox.local
unseen
```

3. Создайте файл /etc/exim4/conf.d/router/03_exim4-config_send:

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

4. Добавьте в файл строки в следующем формате:

```
cmdfilter:
    driver = manualroute
    domains = sandbox.local
    transport = remote_smtp
    route_list = "*" <IP-адрес bcc-сервера PT Sandbox>:<Номер TCP-порта для SMTP, если
отличается от 25>"
    self = send
```

Например:

```
cmdfilter:
    driver = manualroute
    domains = sandbox.local
    transport = remote_smtp
    route_list = "*" 203.0.113.203"
    self = send
```

5. Сохраните изменения в файле 03_exim4-config_send.
6. Чтобы изменения вступили в силу, перезапустите Exim:

```
sudo service exim4 restart
```

Зеркалирование трафика с Exim настроено.

14.3.2.4. Настройка зеркалирования трафика с Microsoft Exchange

Инструкция актуальна для почтового сервера Microsoft Exchange версии 2010 и выше.

Настройка выполняется в центре администрирования Exchange. Для входа в центр администрирования вам нужно использовать учетную запись, которой была назначена роль "Управление организацией". Подробную информацию вы можете получить на сайте technet.microsoft.com.

Перед началом настройки вам нужно [создать bcc-сервер \(см. раздел 14.3.2.1\)](#).

- Чтобы настроить зеркалирование трафика с Microsoft Exchange:

1. В главном меню центра администрирования Exchange выберите раздел **поток обработки почты**.

Откроется страница **правила**.

2. Нажмите **+** и в раскрывшемся меню выберите **Создать новое правило**.

Откроется окно **новое правило**.

3. В поле **Имя** введите произвольное название правила, например Sandbox.

4. В раскрывающемся списке **Применить это правило** выберите **Применить ко всем сообщениям**.
5. В раскрывающемся списке **Выполнить следующие действия** выберите **Отправить скрытую копию сообщения (СК)**.
Откроется окно **Выбрать членов**.
6. В поле **добавить** введите `bcc@sandbox.local`.
7. Нажмите кнопку **ОК**, затем кнопку **Сохранить**.
8. В панели инструментов нажмите **соединители отправки**.
Откроется страница **соединители**.
9. Нажмите **+**, чтобы добавить соединитель отправки.
Откроется мастер **новый соединитель отправки**.
10. Нажмите кнопку **далее**, оставив значения остальных параметров без изменений.
Откроется следующий шаг мастера.
11. Выберите вариант **Перенаправлять почту через промежуточные узлы**.
12. Нажмите **+**, чтобы добавить промежуточный узел.
Откроется страница **изменить промежуточный узел**.
13. В поле введите IP-адрес бсс-сервера PT Sandbox. Если номер TCP-порта для SMTP отличается от стандартного (25), укажите его через двоеточие после IP-адреса.
14. Нажмите кнопку **Сохранить**.
Промежуточный узел будет создан. Откроется следующий шаг мастера.
15. Нажмите **+**, чтобы добавить адресное пространство.
Откроется страница **добавление домена**.
16. В поле **Полное доменное имя (FQDN)** введите `sandbox.local`.
17. Нажмите кнопку **Сохранить**, затем кнопку **Далее**, затем кнопку **Готово**.
Информация о новом соединителе отправки появится в таблице **соединители**.
Зеркалирование трафика с Microsoft Exchange настроено.

14.3.3. Настройка фильтрации почтового трафика

Вы можете настроить фильтрацию почтового трафика с сервера Postfix или Exim: почтовый сервер организации передает письма на проверку в PT Sandbox и, в зависимости от режима проверки почтового трафика, PT Sandbox сразу пересылает письма обратно на сервер (пассивный режим) или задерживает письма до получения результатов проверки и блокирует угрозы (блокирующий режим).

Внимание! Письма, размер которых превышает 1 ГБ, PT Sandbox пропускает без проверки.

Для настройки фильтрации почтового трафика с сервера Postfix или Exim вам нужно:

1. В интерфейсе PT Sandbox добавить источник для фильтрации почтового трафика.
2. Настроить правила маршрутизации почтового трафика с сервера Postfix или Exim в конфигурационных файлах сервера.

В этом разделе

[Добавление источника для фильтрации почтового трафика \(см. раздел 14.3.3.1\)](#)

[Настройка правил маршрутизации почтового трафика с сервера Postfix \(см. раздел 14.3.3.2\)](#)

[Настройка правил маршрутизации почтового трафика с сервера Exim \(см. раздел 14.3.3.3\)](#)

14.3.3.1. Добавление источника для фильтрации почтового трафика

► Чтобы добавить источник для фильтрации почтового трафика:

1. В главном меню в разделе **Система** выберите пункт **Источники для проверки**.

Откроется страница **Система** на вкладке **Источники для проверки**.

2. Нажмите кнопку **Добавить источник**.

Откроется страница **Новый источник для проверки**.

3. В поле **Название** введите название почтового сервера организации.

Название почтового сервера будет отображаться для операторов безопасности среди информации об электронных письмах и файлах, поступивших на проверку от этого сервера.

Примечание. Название должно содержать не менее пяти символов, среди которых могут быть только строчные буквы латинского алфавита, цифры и дефис. Первым и последним символами могут быть только буквы. Название должно быть уникальным среди названий источников любых типов в экземпляре PT Sandbox, в том числе среди названий удаленных источников.

4. В раскрывающемся списке **Тип** выберите **Почтовый сервер в режиме фильтрации**.

На странице отобразятся параметры подключения к SMTP-серверу PT Sandbox и почтовому серверу для проверенной почты.

Рисунок 42. Добавление источника "Почтовый сервер в режиме фильтрации"

5. При необходимости в поле **Адрес SMTP-сервера PT Sandbox** измените стандартный порт (25) для подключения к SMTP-серверу.
6. Укажите параметры доступа к почтовому серверу для проверенной почты:
 - В полях **Адрес почтового сервера для проверенной почты** введите IP-адрес или доменное имя и порт сервера.
 - Если соединение с сервером устанавливается по протоколу SSL, установите флажок **Подключаться по SSL**.
 - Если сервер или политика информационной безопасности вашей организации допускают только определенный тип аутентификации, выберите его в раскрывающемся списке **Тип аутентификации**.
7. Нажмите кнопку **Добавить**.

Источник для фильтрации почтового трафика добавлен.

Теперь вы можете перейти к настройке правил маршрутизации на почтовом сервере организации.

См. также

[Настройка правил маршрутизации почтового трафика с сервера Postfix \(см. раздел 14.3.3.2\)](#)

[Настройка правил маршрутизации почтового трафика с сервера Exim \(см. раздел 14.3.3.3\)](#)

14.3.3.2. Настройка правил маршрутизации почтового трафика с сервера Postfix

Перед началом настройки вам нужно [добавить источник для фильтрации почтового трафика](#) (см. раздел 14.3.3.1).

► Чтобы настроить правила маршрутизации почтового трафика с сервера Postfix:

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

```
sudo nano /etc/postfix/main.cf
```

2. Добавьте в любое место в файле две строки:

```
content_filter=scan:[<IP-адрес сервера PT Sandbox, на котором работает источник "Почтовый сервер в режиме фильтрации">]:<Номер TCP-порта для сервера PT Sandbox, если отличается от 25>
receive_override_options=no_address_mappings
```

3. Сохраните изменения в файле `main.cf`.

4. Откройте файл `/etc/postfix/master.cf`:

```
sudo nano /etc/postfix/master.cf
```

5. Добавьте в любое место в файле строки:

```
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 интерфейса почтового сервера, через который осуществляется прием проверенных писем>: <Номер TCP-порта интерфейса почтового сервера, через который осуществляется прием проверенных писем> inet n - n - 10 smtpd
```

```
-o mynetworks=<IP-адрес сервера PT Sandbox>
```

```
-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
```

6. Чтобы изменения вступили в силу, перезапустите Postfix:

```
service postfix restart
```

Правила маршрутизации почтового трафика с сервера Postfix настроены.

14.3.3.3. Настройка правил маршрутизации почтового трафика с сервера Exim

Инструкция актуальна для агента пересылки почтовых сообщений Exim версии 4 с отдельными файлами конфигурации. Если в вашей организации все параметры Exim хранятся в едином конфигурационном файле, вам нужно добавлять указанные в инструкции строки в этот файл. Подробную информацию о настройке Exim вы можете получить на сайте exim.org.

Перед началом настройки вам нужно [добавить источник для фильтрации почтового трафика](#) (см. раздел 14.3.3.1).

- Чтобы настроить правила маршрутизации почтового трафика с сервера Exim:

1. Создайте транспорт `remote_smtp_check` для отправки почтового трафика с сервера Exim на проверку в PT Sandbox. Для этого создайте файл `/etc/exim4/conf.d/transport/45_exim4-config_remote_smtp_check` и добавьте в него следующие строки:

```
remote_smtp_check:  
  driver = smtp  
  port = <Порт для приема почты на SMTP-сервере PT Sandbox>  
  delay_after_cutoff = false
```

2. Если в организации разрешена отправка писем с вложениями большого размера (сотни мегабайт), во избежание принудительного завершения SMTP-сессий сервером Exim по причине долгой проверки подобных писем в PT Sandbox увеличьте тайм-ауты SMTP-сессии, добавив в секцию `remote_smtp_check` следующие строки:

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

3. Сохраните файл `45_exim4-config_remote_smtp_check`.

4. Настройте новое правило маршрутизации почтового трафика. Для этого создайте файл `/etc/exim4/conf.d/router/050_exim4-config_ptsb` и добавьте в него следующие строки:

```
send_to_check:
    driver = manualroute
    condition = ${if eq {$interface_port}{<Порт для приема проверенных писем>}{no}{yes}}
    transport = remote_smtp_check
    route_list = * <IP-адрес PT Sandbox>
    address_test = false
```

Внимание! Добавленное правило маршрутизации `send_to_check` должно иметь наивысший приоритет. Чтобы это проверить, убедитесь, что в каталоге `/etc/exim4/conf.d/router` файл `050_exim4-config_scanner` идет первым по алфавиту после файла `00_exim4-config_header`.

5. Сохраните файл `050_exim4-config_ptsb`.
6. Добавьте список контроля доступа (ACL) для ограничения доступа к точке приема проверенной почты. Для этого создайте файл `/etc/exim4/conf.d/acl/25_exim4-config_check_host` и добавьте в него следующие строки:

```
acl_check_host:
    deny
        message = Untrusted sender host
        condition = ${if eq {$interface_port}{<Порт для приема проверенных писем>}{yes}{no}}
        condition = ${if match_ip{$sender_host_address}{<IP-адрес PT Sandbox>}{no}{yes}}

    accept
```

Сервер Exim будет отклонять почту, поступающую не с PT Sandbox.

7. Сохраните файл `25_exim4-config_check_host`.
8. Привяжите к конфигурации созданный список контроля доступа. Для этого создайте файл `/etc/exim4/conf.d/main/02_exim4-config_acl_pre_options` и добавьте в него следующую строку:

```
acl_smtp_connect = acl_check_host
```

9. Если вам нужно изменить максимальный размер письма, добавьте также следующую строку:

```
MESSAGE_SIZE_LIMIT = "<Максимальный размер письма в МБ>М"
```

10. Сохраните файл `02_exim4-config_acl_pre_options`.

11. Откройте файл `/etc/exim4/update-exim4.conf.conf`:

```
sudo nano /etc/exim4/update-exim4.conf.conf
```

12. Настройте точку входа проверенной почты, добавив в файл следующую строку:

```
dc_local_interfaces='0.0.0.0 ; <IP-адрес сервера для приема проверенной почты>.<Порт для приема проверенной почты>'
```

13. Добавьте IP-адрес PT Sandbox в список сетей, с которых разрешена пересылка сообщений электронной почты, добавив в файл следующую строку:

```
dc_relay_nets='<IP-адрес PT Sandbox>'
```

Эта строка обеспечит отправку уведомлений PT Sandbox адресатам из доменов, не обслуживаемых почтовым сервером Exim.

14. Сохраните файл `update-exim4.conf.conf`.

15. Сгенерируйте рабочий конфигурационный файл почтового сервера Exim:

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

16. Чтобы изменения вступили в силу, перезапустите Exim:

```
sudo service exim4 restart
```

Правила маршрутизации почтового трафика с сервера Exim настроены.

14.4. Настройка проверки файлов в общей папке

Если в информационной системе вашей организации для работы с файлами используются общие папки, вы можете организовать проверку файлов в этих папках с помощью PT Sandbox.

Внимание! Перед настройкой убедитесь, что PT Sandbox имеет доступ на чтение файлов в общей папке.

Для доступа к общей папке поддерживаются протоколы SMB версий 2 и 3 и NFS версий 3 и 4.

В подключенной к PT Sandbox общей папке будут проверяться все файлы, размер которых не превышает 5 ГБ.

Примечание. Если вы используете DFS, на сервере с установленным PT Sandbox необходимо указать IP-адрес DNS-сервера организации и домен организации в конфигурации Netplan и применить изменения. Подробную инструкцию см. на [сайте Netplan](#).

► Чтобы добавить и настроить источник для проверки файлов из общей папки:

1. В главном меню в разделе **Система** выберите пункт **Источники для проверки**.

Откроется страница **Система** на вкладке **Источники для проверки**.

2. Нажмите кнопку **Добавить источник**.

Откроется страница **Новый источник для проверки**.

3. В поле **Название** введите название источника, позволяющего проверять файлы в общей папке.

Введенное название будет отображаться для операторов безопасности среди информации о файлах, загруженных из общей папки.

Примечание. Название должно содержать не менее пяти символов, среди которых могут быть только строчные буквы латинского алфавита, цифры и дефис. Первым и последним символами могут быть только буквы. Название должно быть уникальным среди названий источников любых типов в экземпляре PT Sandbox, в том числе среди названий удаленных источников.

4. В раскрывающемся списке **Тип** выберите **Общая папка**.

На странице отобразятся параметры подключения к общей папке.

Название и тип	Название <input type="text" value="shared-folder"/> Тип <input type="text" value="Общая папка"/>
Параметры доступа к общей папке PT Sandbox проверяет все файлы в общей папке и уведомляет об опасностях. Не забудьте настроить для PT Sandbox доступ для чтения к этой папке.	Адрес сервера <div> <input type="text" value="NFS"/> <input type="text" value="198.51.100.101"/> <input type="text" value=":"/> <input type="text"/> </div> Укажите доменное имя или IP-адрес сервера и его порт, если он нестандартный. Стандартный порт указывать не нужно Путь к папке <input type="text" value="/Common/Shared"/> Используйте косую черту / в качестве разделителя каталогов в пути к общей папке

Рисунок 43. Настройка проверки файлов в общей папке

5. Укажите параметры доступа к общей папке:

- В раскрывающемся списке **Адрес сервера** выберите протокол для подключения к общей папке.
- В полях **Адрес сервера** укажите доменное имя или IP-адрес сервера и его порт, если он нестандартный. Стандартный порт указывать не нужно.
- В поле **Путь к папке** введите путь к общей папке.
- Если вы выбрали протокол SMB, в полях **Логин** и **Пароль** введите логин и пароль для подключения к общей папке.

Примечание. При настройке доступа по протоколу SMB вместе с логином вы можете указать и доменное имя. Для этого в поле **Логин** введите данные в формате <Доменное имя>\<Логин>, например yourdomain\ivanov.

6. Нажмите кнопку **Добавить**.


Источник добавлен и настроен.

14.5. Настройка проверки файлов в папке-шлюзе

Папка-шлюз — это папка в информационной системе организации с настроенным общим доступом. Сотрудники организации помещают в папку-шлюз файлы для проверки в PT Sandbox.

Чтобы настроить проверку файлов в папке-шлюзе, вам нужно создать или выделить для этой цели три папки с настроенным общим доступом: папку-шлюз, папку для безопасных файлов и папку карантина:

- В папку-шлюз сотрудники вашей организации помещают файлы для проверки в PT Sandbox.
- В папку для безопасных файлов по результатам проверки PT Sandbox перемещает файлы, не представляющие угрозы.

Примечание. В эту же папку перемещаются обработанные файлы, которые по какой-либо причине не удалось отсканировать в течение часа. В результатах проверки такие файлы помечаются значком .

- В папку карантина по результатам проверки PT Sandbox перемещает файлы, представляющие угрозу.

Этими тремя папками могут быть как отдельные папки, так и вложенные папки в одной папке. Вы также можете разместить папки на разных серверах.

Внимание! Папки не должны быть вложены друг в друга, иначе может произойти заикливание сканирования.

Поддерживаемые протоколы для общего доступа к папкам:

- SMB версии 2.1;
- NFS версии 3.

После создания папок вам нужно добавить и настроить источник с типом "Папка-шлюз", указав в его параметрах доступ к созданным папкам.

Внимание! Перед настройкой убедитесь, что PT Sandbox имеет доступ на чтение, запись и удаление файлов в папках с настроенным общим доступом.

Примечание. Если вы используете DFS, на сервере с установленным PT Sandbox необходимо указать IP-адрес DNS-сервера организации и домен организации в конфигурации Netplan и применить изменения. Подробную инструкцию см. на [сайте Netplan](#).

- Чтобы добавить и настроить источник для проверки файлов в папке-шлюзе:

1. В главном меню в разделе **Система** выберите пункт **Источники для проверки**.

Откроется страница **Система** на вкладке **Источники для проверки**.

2. Нажмите кнопку **Добавить источник**.

Откроется страница **Новый источник для проверки**.

3. В поле **Название** введите название папки-шлюза.

Название папки-шлюза будет отображаться для операторов безопасности среди информации о файлах, загруженных из этой папки.

Примечание. Название должно содержать не менее пяти символов, среди которых могут быть только строчные буквы латинского алфавита, цифры и дефис. Первым и последним символами могут быть только буквы. Название должно быть уникальным среди названий источников любых типов в экземпляре PT Sandbox, в том числе среди названий удаленных источников.

4. В раскрывающемся списке **Тип** выберите **Папка-шлюз**.

На странице отобразятся параметры подключения к общим папкам.

Название и тип	Название <input type="text" value="gateway-folder"/> Тип <input type="text" value="Папка-шлюз"/>
Параметры доступа к общим папкам PT Sandbox проверяет файлы, поступающие в папку-шлюз, и в зависимости от результата проверки перемещает их в другие папки. Файлы, при сканировании которых произошла ошибка, останутся в папке-шлюзе. Не забудьте настроить для PT Sandbox доступ к этим папкам на чтение, запись и удаление файлов.	Адрес сервера папки-шлюза <div> <input type="text" value="NFS"/> <input type="text" value="198.51.100.100"/> <input type="text" value=":"/> <input type="text"/> </div> Укажите доменное имя или IP-адрес сервера и его порт, если он нестандартный. Стандартный порт указывать не нужно Путь к папке <input type="text" value="/files/inbox"/> Используйте косую черту / в качестве разделителя каталогов в пути к общей папке Адрес сервера папки для безопасных файлов <div> <input type="text" value="NFS"/> <input type="text" value="198.51.100.100"/> <input type="text" value=":"/> <input type="text"/> </div> Укажите доменное имя или IP-адрес сервера и его порт, если он нестандартный. Стандартный порт указывать не нужно Путь к папке <input type="text" value="/files/safe"/> Используйте косую черту / в качестве разделителя каталогов в пути к общей папке Адрес сервера папки карантина <div> <input type="text" value="NFS"/> <input type="text" value="198.51.100.100"/> <input type="text" value=":"/> <input type="text"/> </div> Укажите доменное имя или IP-адрес сервера и его порт, если он нестандартный. Стандартный порт указывать не нужно Путь к папке <input type="text" value="/files/qt"/> Используйте косую черту / в качестве разделителя каталогов в пути к общей папке

Рисунок 44. Настройка проверки файлов в папке-шлюзе

5. Укажите параметры доступа к папке-шлюзу:

- В раскрывающемся списке **Адрес сервера папки-шлюза** выберите протокол для подключения к папке-шлюзу.
- В полях **Адрес сервера папки-шлюза** укажите доменное имя или IP-адрес сервера и его порт, если он нестандартный. Стандартный порт указывать не нужно.
- В поле **Путь к папке** введите путь к папке-шлюзу.
- Если вы выбрали протокол SMB, в полях **Логин** и **Пароль** введите логин и пароль для подключения к папке-шлюзу.

Примечание. При настройке доступа по протоколу SMB вместе с логином вы можете указать и доменное имя. Для этого в поле **Логин** введите данные в формате <Доменное имя>\<Логин>, например yourdomain\ivanov.

6. Укажите параметры доступа к папке для безопасных файлов:

- В раскрывающемся списке **Адрес сервера папки для безопасных файлов** выберите протокол для подключения к папке для безопасных файлов.

- В полях **Адрес сервера папки для безопасных файлов** укажите доменное имя или IP-адрес сервера и его порт, если он нестандартный. Стандартный порт указывать не нужно.
- В поле **Путь к папке** введите путь к папке для безопасных файлов.
- Если вы выбрали протокол SMB, в полях **Логин** и **Пароль** введите логин и пароль для подключения к папке для безопасных файлов.

Примечание. При настройке доступа по протоколу SMB вместе с логином вы можете указать и доменное имя. Для этого в поле **Логин** введите данные в формате <Доменное имя>\<Логин>, например yourdomain\ivanov.

7. В блоке параметров **Папка карантина** укажите параметры доступа к папке для файлов, представляющих угрозу.

В раскрывающемся списке **Адрес сервера папки карантина** выберите протокол для подключения к папке карантина.

- В полях **Адрес сервера папки карантина** укажите доменное имя или IP-адрес сервера и его порт, если он нестандартный. Стандартный порт указывать не нужно.
- В поле **Адрес сервера папки карантина** введите путь к папке карантина.
- Если вы выбрали протокол SMB, в полях **Логин** и **Пароль** введите логин и пароль для подключения к папке карантина.

Примечание. При настройке доступа по протоколу SMB вместе с логином вы можете указать и доменное имя. Для этого в поле **Логин** введите данные в формате <Доменное имя>\<Логин>, например yourdomain\ivanov.

8. Нажмите кнопку **Добавить**.

Источник для проверки файлов в папке-шлюзе добавлен и настроен.

14.6. Настройка проверки трафика организации при помощи модуля захвата трафика

Вы можете настроить проверку сетевого трафика организации при помощи модуля захвата трафика PT Sandbox. Для этого вам нужно обеспечить зеркалирование трафика на определенный сетевой интерфейс сервера или виртуальной машины с установленным PT Sandbox. После этого вам нужно добавить и настроить источник с типом "Модуль захвата трафика (DPI)", указав в его параметрах название этого сетевого интерфейса. Модуль захвата трафика будет извлекать файлы из сетевого трафика на указанном интерфейсе и отправлять их на проверку.

- Чтобы добавить и настроить источник для проверки файлов, полученных от модуля захвата трафика:
 1. В главном меню в разделе **Система** выберите пункт **Источники для проверки**.
Откроется страница **Система** на вкладке **Источники для проверки**.
 2. Нажмите кнопку **Добавить источник**.

Откроется страница **Новый источник для проверки**.

3. В поле **Название** введите название источника файлов, полученных от модуля захвата трафика.

Название источника будет отображаться для операторов безопасности среди информации о файлах, полученных от модуля захвата трафика.

Примечание. Название должно содержать не менее пяти символов, среди которых могут быть только строчные буквы латинского алфавита, цифры и дефис. Первым и последним символами могут быть только буквы. Название должно быть уникальным среди названий источников любых типов в экземпляре PT Sandbox, в том числе среди названий удаленных источников.

4. В раскрывающемся списке **Тип** выберите **Модуль захвата трафика (DPI)**.

На странице отобразится параметр источника выбранного типа.

Название и тип	<p>Название</p> <input type="text" value="dpi-module"/> <p>Тип</p> <div>Модуль захвата трафика (DPI) ▾</div>
Параметры соединения PT Sandbox анализирует весь трафик, проходящий через выбранный сетевой интерфейс, и проверяет файлы, которые удалось извлечь.	<p>Сетевой интерфейс</p> <input type="text" value="eth0"/> <p><small>Может содержать только буквы латинского алфавита, цифры, точку, дефис и символ подчеркивания</small></p>

Рисунок 45. Настройка проверки файлов, полученных от модуля захвата трафика

5. В поле **Сетевой интерфейс** введите название сетевого интерфейса для захвата трафика.

6. Нажмите кнопку **Добавить**.

Источник для проверки файлов, полученных от модуля захвата трафика, добавлен и настроен.

14.7. Настройка проверки трафика организации при помощи PT NAD

Если в информационной системе вашей организации установлен Positive Technologies Network Attack Discovery (PT NAD), вы можете настроить отправку файлов, извлеченных этим продуктом из сетевого трафика, на проверку в PT Sandbox. Для этого вам нужно добавить источник для проверки файлов, извлеченных PT NAD.

- Чтобы добавить источник для проверки файлов, извлеченных PT NAD:

1. В главном меню в разделе **Система** выберите пункт **Источники для проверки**.

Откроется страница **Система** на вкладке **Источники для проверки**.

2. Нажмите кнопку **Добавить источник**.

Откроется страница **Новый источник для проверки**.

3. В поле **Название** введите название экземпляра PT NAD.

Название экземпляра PT NAD будет отображаться для операторов безопасности среди информации о файлах, извлеченных экземпляром этого продукта.

Примечание. Название должно содержать не менее пяти символов, среди которых могут быть только строчные буквы латинского алфавита, цифры и дефис. Первым и последним символами могут быть только буквы. Название должно быть уникальным среди названий источников любых типов в экземпляре PT Sandbox, в том числе среди названий удаленных источников.

4. В раскрывающемся списке **Тип** выберите **PT NAD**.

На странице отобразятся параметры подключения к папке с файлами, извлеченными PT NAD из сетевого трафика.

Название и тип	<p>Название</p> <input type="text" value="ptnad"/> <p>Тип</p> <div>PT NAD ▾</div>
Параметры соединения Установите в конфигурации PT NAD указанные параметры подключения модуля ptdpi-icar-worker к PT Sandbox	<p>Адрес сервера</p> <div> <input type="text" value="203.0.113.34"/> : <input type="text" value="2344"/> </div>

Рисунок 46. Настройка проверки файлов, извлекаемых PT NAD

5. Нажмите кнопку **Добавить**.

Источник для проверки файлов, извлеченных PT NAD, добавлен.

Теперь вам нужно в PT NAD установить и настроить модуль ptdpi-worker@icar. Этот модуль является ICAP-клиентом, который отправляет извлеченные файлы ICAP-серверу PT Sandbox и получает от него результаты сканирования. В отличие от источника "ICAP-сервер", источник "PT NAD" позволяет отправлять в PT Sandbox дополнительную информацию о проверяемых файлах. Например, IP-адреса компьютеров, между которыми передавался файл, перехваченный PT NAD; название протокола, по которому PT NAD перехватил файл.

Информация о настройке модуля ptdpi-worker@icar приведена в Руководстве администратора для PT NAD версии 7.1 и выше.

15. Управление источниками для проверки

Вы можете управлять добавленными источниками для проверки: настраивать, отключать и удалять их.

В этом разделе

[Изменение параметров источника для проверки \(см. раздел 15.1\)](#)

[Отключение источника для проверки \(см. раздел 15.2\)](#)

[Удаление источника для проверки \(см. раздел 15.3\)](#)

См. также

[Добавление источников для проверки \(см. раздел 14\)](#)

[Источники файлов и электронных писем, передаваемых на проверку \(см. раздел 4.2\)](#)

[Режимы проверки файлов и электронных писем \(см. раздел 4.3\)](#)

15.1. Изменение параметров источника для проверки

Вы можете изменять параметры источников для проверки, кроме их названий и типов.

- ▶ Чтобы изменить параметры источника для проверки:
 1. В главном меню в разделе **Система** выберите пункт **Источники для проверки**.
Откроется страница **Система** на вкладке **Источники для проверки**.
 2. В блоке с информацией об источнике перейдите по ссылке **Настроить источник**.
Откроется страница с параметрами выбранного источника.
 3. Измените параметры источника по своему усмотрению.
 4. Нажмите кнопку **Сохранить изменения**.
Параметры источника для проверки изменены.

15.2. Отключение источника для проверки

Вы можете временно отключить источник для проверки, например для уменьшения нагрузки на информационную систему вашей организации.

Примечание. Стандартный источник (веб-интерфейс) не может быть отключен.

- ▶ Чтобы отключить источник для проверки:
 1. В главном меню в разделе **Система** выберите пункт **Источники для проверки**.

Откроется страница **Система** на вкладке **Источники для проверки**.

2. Отключите источник для проверки.

Блок с информацией об источнике для проверки сменит цвет с зеленого на серый.

Источник для проверки отключен.

15.3. Удаление источника для проверки

Вы можете удалить источник для проверки, который был добавлен по ошибке или перестал существовать. Если вам нужно приостановить работу источника на какое-то время, не удаляйте его, а [отключите \(см. раздел 15.2\)](#).

Примечание. Стандартный источник (веб-интерфейс) не может быть удален.

- Чтобы удалить источник для проверки:

1. В главном меню в разделе **Система** выберите пункт **Источники для проверки**.

Откроется страница **Система** на вкладке **Источники для проверки**.

2. В блоке с информацией об источнике, который вам нужно удалить, перейдите по ссылке **Параметры**.

Откроется страница с параметрами выбранного источника.

3. Нажмите кнопку **Удалить источник для проверки** и подтвердите удаление.

Источник для проверки удален.

16. Проверка файлов в PT Sandbox

После настройки источников для самостоятельной проверки вы можете отправлять файлы и письма на проверку с помощью интерфейса PT Sandbox или по электронной почте.

В этом разделе

[Проверка файлов через интерфейс PT Sandbox \(см. раздел 16.1\)](#)

[Отправка файлов на проверку по электронной почте \(см. раздел 16.2\)](#)

См. также

[Создание и настройка службы Checkme \(см. раздел 14.1\)](#)

16.1. Проверка файлов через интерфейс PT Sandbox


Для проверки работоспособности PT Sandbox после его установки вы можете отправить файл на проверку через его интерфейс. Максимальный размер файла, который вы можете отправить на проверку через интерфейс PT Sandbox, — 1 ГБ.

► Чтобы проверить файлы через интерфейс PT Sandbox:

1. Перетащите файлы в окно браузера в область **Загрузка файлов на проверку**, которая появится на открытой странице в процессе перетаскивания.

В окне появится информация о загруженных файлах.

Примечание. Вы также можете открыть окно загрузки файлов по кнопке **Проверить файлы** в главном меню.

Примечание. Вы можете отменить отправку файла на проверку по кнопке  и добавить другие файлы, перетащив их в область загрузки файлов или по ссылке **выберите**.

Загрузка файлов на проверку

📁 Перетащите сюда или [выберите](#)

Загружен 1 файл

Файл	Размер	Результат
archive.zip	2.81 МБ	📁 Загружено

Далее
Отмена

Рисунок 47. Загрузка файлов на проверку

2. Нажмите кнопку **Далее**.
3. Если вам нужно проверить файлы только методом статического анализа, выключите поведенческий анализ.
4. Если вам нужно проверить файлы методом поведенческого анализа:

- В раскрывающемся списке **Образ виртуальной машины** выберите название образа операционной системы с набором программ и предустановленной конфигурацией виртуального окружения.

Выбранный образ будет использоваться для развертывания виртуальной машины, в которой PT Sandbox будет запускать файлы для анализа их поведения.

- В поле **Продолжительность наблюдения за файлом** введите максимальную продолжительность проверки каждого файла в виртуальной машине.

По истечении этого времени проверка файла будет прервана с сохранением полученных результатов проверки.

- Если вам нужно отключить подмену сертификатов при анализе защищенного трафика в виртуальной машине, снимите флажок **Расшифровывать и анализировать HTTPS-трафик**.

Отключение этого параметра может понадобиться для выявления вредоносного ПО, которое проверяет свойства сертификата и перестает работать, обнаружив его подмену. Если флажок установлен, PT Sandbox подменяет сертификат своим для расшифровки и анализа защищенного трафика.

5. Если среди загруженных файлов есть архивы, защищенные известными вам паролями, введите эти пароли в поле **Пароли для архивов**.

6. В поле **Глубина распаковки архивов** укажите глубину распаковки архивов, вложенных в архивы.
7. Нажмите кнопку **Проверить**.
 Файлы будут отправлены на проверку. Для проверки каждого файла будет создано отдельное задание.
 По окончании проверки каждого файла в Центре уведомлений появляется уведомление, информирующее о результате проверки файла, типе обнаруженной угрозы и времени завершения проверки.
8. В главном меню нажмите  .
 Откроется Центр уведомлений.
9. В уведомлении нажмите на название проверенного файла.
 Откроется страница с результатами проверки файла.

16.2. Отправка файлов на проверку по электронной почте

После настройки службы Checkme вы можете проверить ее работоспособность, отправив по электронной почте файлы и письма на проверку.

► Чтобы проверить файлы по электронной почте:

1. В вашей почтовой программе откройте форму создания письма.
2. В поле получателя введите адрес электронной почты для проверки файлов.
Внимание! Не добавляйте других адресатов, иначе письмо не будет доставлено в PT Sandbox.
3. Если предназначенные для проверки файлы запакованы в архивы и защищены известными вам паролями, в тексте письма введите по одному уникальному паролю в каждой строке.

Примечание. Если вы не знаете пароль к архиву, PT Sandbox попытается распаковать архив, используя список стандартных паролей, который задается оператором безопасности PT Sandbox.

4. Прикрепите к письму файлы, которые вам нужно проверить.
5. Отправьте письмо.

PT Sandbox проверит как текст письма, так и его вложения. По окончании проверки PT Sandbox отправит вам ответное письмо с ее результатами.

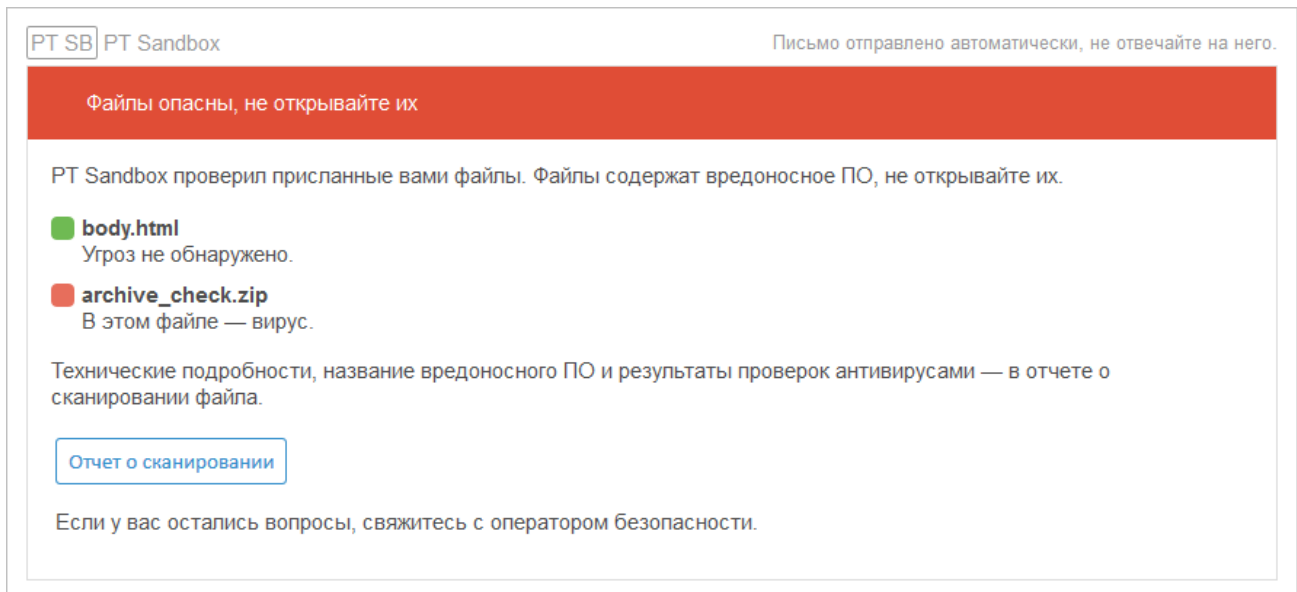


Рисунок 48. Ответное письмо с результатами проверки

6. В полученном письме нажмите кнопку **Отчет о сканировании**, чтобы просмотреть в интерфейсе PT Sandbox результаты проверки отправленного вами письма с вложениями.

См. также

Создание и настройка службы Checkme (см. раздел 14.1)

17. Работа с результатами проверки файлов

После завершения проверки файлов PT Sandbox генерирует отчет с результатами проверки. Если вы отправляли файлы на проверку через интерфейс, уведомление об окончании проверки со ссылкой на отчет появится в [Центре уведомлений](#) (см. раздел 11.2). Если вы отправляли файлы на проверку по электронной почте, ссылка на отчет придет в ответном письме.

В этом разделе

[Просмотр результатов проверки](#) (см. раздел 17.1)

[Поиск результатов проверки](#) (см. раздел 17.2)

17.1. Просмотр результатов проверки

Вы можете просматривать информацию о результатах проверки файлов, отправленных вами в PT Sandbox с помощью его интерфейса.

► Чтобы просмотреть результат проверки:

1. В главном меню выберите раздел **Задания**.

Откроется страница **Задания** со списком ваших заданий на проверку.

2. В списке найдите задание, в котором хранится нужный вам результат проверки.
3. Выберите задание в списке.

Откроется страница, содержащая результат и время проверки файла, название источника, с которого файл поступил на проверку, а также информацию об отправителе файла.

4. В панели слева выберите название проверенного файла.

На странице отобразятся результаты проверки и свойства файла.

Примечание. Если при проверке зашифрованный архив был распакован с использованием пароля, то этот пароль отображается в свойствах файла.

17.2. Поиск результатов проверки

В этом разделе приводятся инструкции по поиску заданий с результатами проверки файлов, отправленных вами через интерфейс. Вы можете совмещать критерии поиска.

В этом разделе

[Поиск заданий по времени создания](#) (см. раздел 17.2.1)

[Поиск заданий по уровням опасности файлов](#) (см. раздел 17.2.2)

[Поиск заданий по результатам проверки](#) (см. раздел 17.2.3)

Поиск заданий по проверенным в них файлам (см. раздел 17.2.4)

Поиск заданий по файлам, проверявшимся или не проверявшимся методом поведенческого анализа (см. раздел 17.2.5)

17.2.1. Поиск заданий по времени создания

► Чтобы найти задания по времени создания:

1. В главном меню выберите раздел **Задания**.

Откроется страница **Задания** со списком всех заданий на проверку.

2. В панели фильтрации нажмите ссылку с текущим выбранным периодом.

3. Во всплывающем окне выберите предустановленный период или настройте свой.

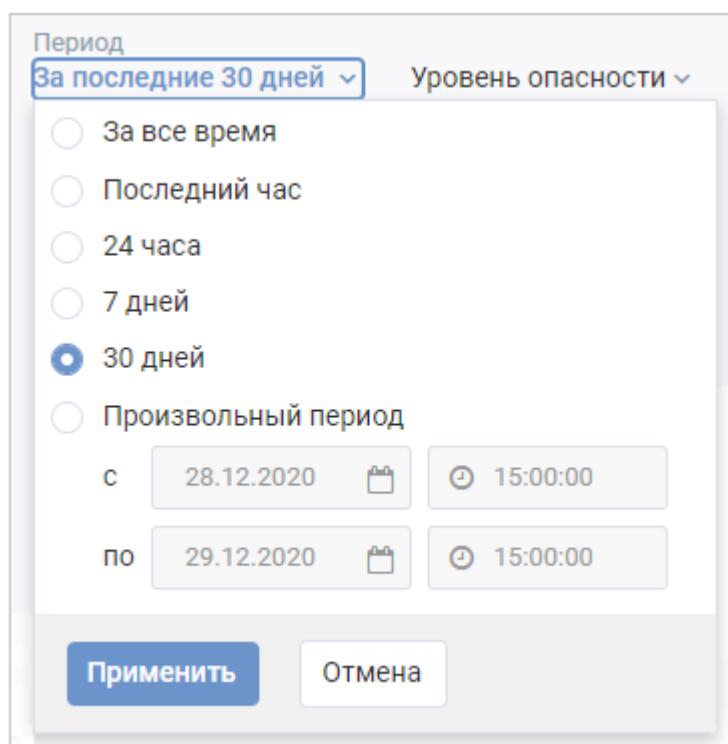


Рисунок 49. Поиск заданий по времени создания

4. Нажмите кнопку **Применить**.

PT Sandbox отобразит в списке только те задания, которые были созданы за выбранный вами период.

17.2.2. Поиск заданий по уровням опасности файлов

Вы можете отфильтровать список заданий по уровням опасности файлов, для проверки которых PT Sandbox создавал эти задания.

- Чтобы найти задания по уровням опасности файлов:

1. В главном меню выберите раздел **Задания**.

Откроется страница **Задания** со списком всех заданий на проверку.

2. В панели фильтрации в раскрывающемся списке **Уровень опасности** установите флажки напротив нужных вам уровней.

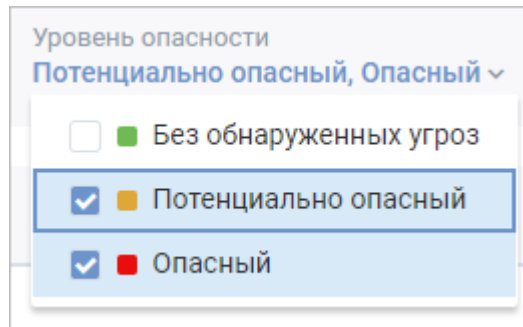


Рисунок 50. Выбор уровней опасности файлов

PT Sandbox отобразит в списке задания с выбранными вами уровнями опасности файлов.

17.2.3. Поиск заданий по результатам проверки

Вы можете отфильтровать список заданий по результатам проверки файлов, для проверки которых PT Sandbox создавал эти задания.

- Чтобы найти задания по результатам проверки:

1. В главном меню выберите раздел **Задания**.

Откроется страница **Задания** со списком всех заданий на проверку.

2. В панели фильтрации в раскрывающемся списке **Результат проверки** установите флажки напротив нужных вам типов ПО, обнаруженного в результате проверки.

Вы можете искать типы ПО с помощью поля поиска в этом раскрывающемся списке.

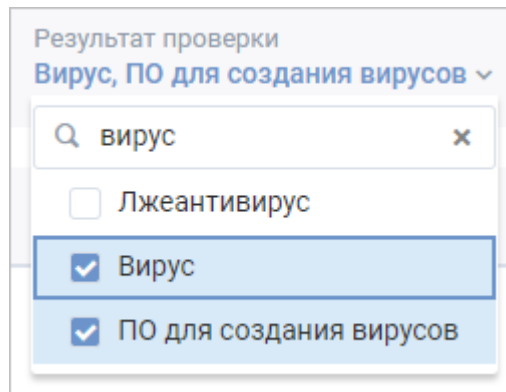


Рисунок 51. Выбор типов ПО

PT Sandbox отобразит в списке задания с выбранными вами результатами проверки.

17.2.4. Поиск заданий по проверенным в них файлам

- Чтобы найти задания по проверенным в них файлам:

1. В главном меню выберите раздел **Задания**.

Откроется страница **Задания** со списком всех заданий на проверку.

2. В поле поиска введите название файла или его хеш-сумму (MD5, SHA-1 или SHA-256).
3. Нажмите клавишу Enter.

PT Sandbox отобразит в списке задания, в процессе обработки которых были проверены файлы с указанными вами названием или хеш-суммой.

17.2.5. Поиск заданий по файлам, проверявшимся или не проверявшимся методом поведенческого анализа

Для проверки работы поведенческого анализа вы можете отфильтровать список заданий для показа только тех заданий, в ходе которых был завершен или не проводился поведенческий анализ файлов.

- Чтобы найти задания по файлам, для проверки которых проводился или не проводился метод поведенческого анализа:

1. В главном меню выберите раздел **Задания**.

Откроется страница **Задания** со списком всех заданий на проверку.

2. В панели фильтрации в раскрывающемся списке **Поведенческий анализ** выберите пункт **Завершен** или **Не проводился**.

18. Просмотр пользовательских ролей и прав доступа

Вы можете просматривать список разрешенных действий для ролей, которые присваиваются учетным записям пользователей PT Sandbox.

Примечание. Создание учетных записей пользователей и назначение ролей этим записям осуществляется в сервисе PT IAM.

- ▶ Чтобы просмотреть список пользовательских ролей и прав доступа,
в главном меню в разделе **Система** выберите пункт **Роли и права доступа**.
Откроется страница **Система** на вкладке **Роли и права доступа**.

<div> <div> <div></div> <div>РТ Sandbox</div> </div> <div> <div>Задания</div> <div>Образы VM</div> <div>Система ▾</div> </div> <div> <div>+ Проверить файлы</div> <div></div> <div></div> <div></div> </div> </div>				
Система				
<div> <div>Основные параметры</div> <div>Источники для проверки</div> <div>Антивирусы</div> <div>Роли и права доступа</div> <div>Лицензия</div> </div>				
Разрешенное действие	Администратор	Оператор безопасности	Пользователь	Анонимный пользователь
Мониторинг				
Просмотр сводки и списка угроз		✓		
Проверка файлов				
Доступ к своим результатам проверки	✓	✓	✓	
Доступ ко всем результатам проверки		✓		
Создание заданий на проверку	✓	✓	✓	✓
Файлы				
Просмотр истории проверки файла		✓		
Просмотр списка всех файлов		✓		
Просмотр информации о файле	✓	✓	✓	
Скачивание файлов		✓		
Антивирусы				
Просмотр информации об антивирусах	✓	✓		
Параметры системы				
Изменение параметров системы	✓			
Изменение параметров проверки		✓		
Другое				
Мониторинг текущего состояния системы	✓	✓		
Доверенный пользователь	✓	✓	✓	

Рисунок 52. Просмотр ролей и прав доступа

19. Работа с антивирусами

Для сканирования файлов PT Sandbox использует антивирусы сторонних разработчиков.

Антивирусы, с которыми работает PT Sandbox, делятся на основные и дополнительные.

Основные антивирусы входят в комплект поставки PT Sandbox. Основные антивирусы, их базы и лицензии обновляются автоматически. Вы не можете удалять основные антивирусы, а только выключать сканирование ими.

В дополнение к основным антивирусам вы можете самостоятельно устанавливать антивирусы из разрешенного набора. Такие антивирусы называются дополнительными. Базы дополнительных антивирусов обновляются автоматически с серверов поставщиков или с указанных вами локальных источников обновлений. Обновление дополнительных антивирусов до новых версий и замену лицензий по истечении их срока действия нужно выполнять самостоятельно.

В этом разделе

[Просмотр сведений об антивирусах \(см. раздел 19.1\)](#)

[Включение и выключение антивируса \(см. раздел 19.2\)](#)

[Установка дополнительного антивируса \(см. раздел 19.3\)](#)

[Обновление лицензии дополнительного антивируса \(см. раздел 19.4\)](#)

[Удаление дополнительного антивируса \(см. раздел 19.5\)](#)

[Обновление дополнительного антивируса \(см. раздел 19.6\)](#)

19.1. Просмотр сведений об антивирусах

Вы можете просмотреть сведения об антивирусах, установленных в PT Sandbox.

- Чтобы просмотреть сведения об антивирусах,
 - в главном меню в разделе **Система** выберите пункт **Антивирусы**.
 - Откроется страница **Система** на вкладке **Антивирусы**.

См. также

[Страница управления антивирусами \(см. раздел 11.4\)](#)

19.2. Включение и выключение антивируса

Вы можете выключить сканирование файлов отдельными антивирусами. Выключение может понадобиться, если антивирус показывает множество ложных результатов или требуется временно уменьшить нагрузку на информационную систему организации. Выключенный антивирус можно снова включить в любой момент.

► Чтобы включить или выключить антивирус:

1. В главном меню в разделе **Система** выберите пункт **Антивирусы**.

Откроется страница **Система** на вкладке **Антивирусы**.

2. В блоке с информацией об антивирусе включите или выключите антивирус.

Если антивирус выключен, блок с информацией об антивирусе будет выделен серым цветом.

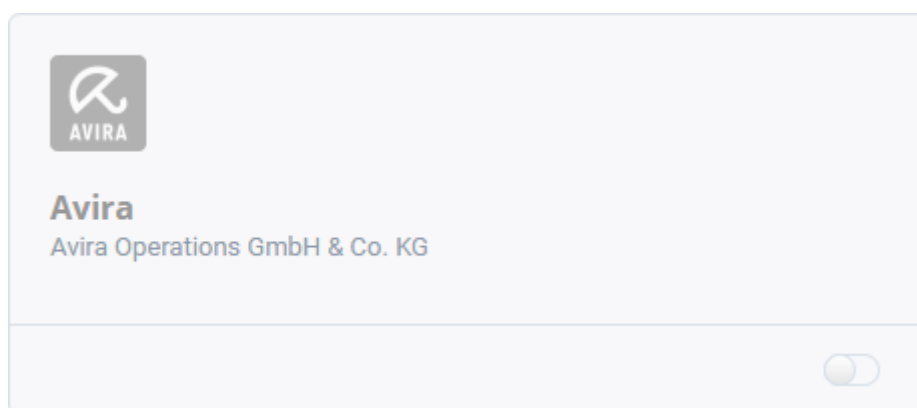


Рисунок 53. Выключение антивируса

Включение или выключение антивируса может занять некоторое время.

19.3. Установка дополнительного антивируса

Для повышения качества обнаружения угроз в дополнение к антивирусам, включенным в комплект поставки PT Sandbox, ваша организация может купить и самостоятельно установить следующие антивирусы:

- Kaspersky for Proxy Server 5.5.86;
- Kaspersky Web Traffic Security 6.1.0.4762;
- Avast Core Security 3.0;
- Symantec Protection Engine for Network Attached Storage 7.9.1.12;
- Dr.Web Server Security Suite 11.1.

Примечание. Установка дополнительного антивируса может быть ограничена [лицензией \(см. раздел 12\)](#).

Для установки дополнительного антивируса вам понадобятся его дистрибутив и файл лицензии.

► Чтобы установить дополнительный антивирус:

1. В главном меню в разделе **Система** выберите пункт **Антивирусы**.

Откроется страница **Система** на вкладке **Антивирусы**.

- В секции **Доступны к установке** в блоке с названием антивируса нажмите кнопку **Установить**.

На странице отобразится форма установки дополнительного антивируса.





Дистрибутив	<div>  Загрузить дистрибутив </div> <div>  По вопросам совместимости дистрибутива — обратитесь в техническую поддержку </div>
Лицензия	<div>  Загрузить файл лицензии </div> <div> <small>Файл с расширением .key</small> </div> <div>  По вопросам совместимости лицензии антивируса — обратитесь в техническую поддержку </div>
Зеркало обновлений	<div> <small>Адрес сервера</small> <input type="text"/> </div> <div> <small>Оставьте поле пустым для использования зеркала по умолчанию</small> </div> <div> <input type="checkbox"/> Подключаться через прокси-сервер </div>

Рисунок 54. Установка дополнительного антивируса

- По кнопке **Загрузить дистрибутив** загрузите файл дистрибутива антивируса.
- По кнопке **Загрузить файл лицензии** загрузите файл с лицензией антивируса.
- Если вам нужно, чтобы антивирус получал обновления своих баз из локального источника, укажите адрес этого источника в поле **Зеркало обновлений**.
- Если вам нужно, чтобы при подключении к зеркалу обновлений использовался прокси-сервер, который указывался при установке PT Sandbox (например, если зеркало обновлений находится не в информационной системе организации), установите флажок **Подключаться через прокси-сервер**.
- Нажмите кнопку **Установить**.

Начнется установка антивируса. По завершении установки на [странице со списком антивирусов \(см. раздел 11.4\)](#) появится информация об установленном антивирусе.

Дополнительный антивирус установлен.

Базы дополнительного антивируса обновляются автоматически с сервера поставщика или с указанного вами зеркала обновлений. Первое обновление баз начинается сразу после установки антивируса.

19.4. Обновление лицензии дополнительного антивируса

Если срок действия лицензии дополнительного антивируса истек, вам нужно обновить ее, чтобы PT Sandbox мог снова использовать антивирус для сканирования файлов.

- Чтобы обновить лицензию дополнительного антивируса:

- В главном меню в разделе **Система** выберите пункт **Антивирусы**.

Откроется страница **Система** на вкладке **Антивирусы**.

2. В блоке с информацией об антивирусе нажмите кнопку **Параметры**.

На странице отобразятся параметры дополнительного антивируса.

3. По кнопке **Заменить файл лицензии** загрузите файл новой лицензии.

4. Нажмите кнопку **Сохранить изменения**.

Начнется обновление лицензии дополнительного антивируса, которое может занять некоторое время. По окончании обновления информация о новой лицензии отобразится на странице с параметрами антивируса.

19.5. Удаление дополнительного антивируса

Вы можете удалить дополнительный антивирус, например чтобы затем установить его более новую версию. Если вам нужно приостановить сканирование файлов антивирусом на какое-то время, не удаляйте его, а [выключите \(см. раздел 19.2\)](#).

- Чтобы удалить дополнительный антивирус:

1. В главном меню в разделе **Система** выберите пункт **Антивирусы**.

Откроется страница **Система** на вкладке **Антивирусы**.

2. В блоке с информацией об антивирусе нажмите кнопку **Параметры**.

На странице отобразятся параметры дополнительного антивируса.

3. Нажмите кнопку **Удалить антивирус** и подтвердите удаление.

Дополнительный антивирус удален.

19.6. Обновление дополнительного антивируса

Если доступно обновление дополнительного антивируса, на странице **Антивирусы сторонних разработчиков** в блоке с информацией об антивирусе появится оповещение о выпуске новой версии. В этом случае вам необходимо обновить используемый дополнительный антивирус. Если не обновить антивирусы после оповещения, они могут быть отключены при следующих обновлениях PT Sandbox.

- Чтобы обновить дополнительный антивирус:

1. В главном меню в разделе **Система** выберите пункт **Антивирусы**.

2. В блоке с информацией об антивирусе нажмите кнопку **Параметры**.

На странице отобразятся параметры дополнительного антивируса.

3. По кнопке **Загрузить дистрибутив** загрузите файл дистрибутива антивируса.

Начнется передача файла дистрибутива антивируса на сервер.

4. По завершении передачи файла нажмите кнопку **Сохранить**.

Начнется обновление дополнительного антивируса. По завершении обновления на странице со списком антивирусов появится информация об обновленном антивирусе.

Дополнительный антивирус обновлен.

20. Включение записи событий в журнал аудита

Журнал аудита представляет собой базу данных, в которую записываются следующие события:

- включение и выключение записи событий в журнал аудита;
- обновление антивирусов;
- обновление антивирусных баз.

По умолчанию запись событий в журнал аудита выключена.

► Чтобы включить запись событий в журнал аудита:

1. В главном меню в разделе **Система** выберите пункт **Основные параметры**.

Откроется страница **Система** на вкладке **Основные параметры**.

2. Включите запись событий в журнал аудита.

3. Нажмите кнопку **Сохранить**.

Запись событий в журнал аудита включена.

Записи из журнала аудита отображаются в журнале действий PT IAM (доступен оператору PT Sandbox).

21. Изменение объема хранилища для файлов заданий

Любой отправляемый на проверку файл, размер которого не превышает 1 ГБ и не превышает 1% от максимального объема хранилища файлов, помещается в хранилище файлов.

PT Sandbox начинает удалять самые старые файлы из хранилища при выполнении хотя бы одного из условий:

- заполнено 90% от максимального объема файлов заданий, который указан в параметрах PT Sandbox;
- до полного заполнения объема файлов заданий остался 1 ГБ свободного места;
- в хранилище помещено 95% от максимально допустимого количества файлов заданий.

Чем больше выделенный объем для файлов заданий, тем дольше хранятся файлы для их повторного сканирования. Увеличение объема для файлов заданий может понадобиться, например, если на сервере с PT Sandbox был добавлен жесткий диск и вам нужно увеличить количество файлов, доступных для повторного сканирования. Уменьшение объема для файлов заданий может понадобиться, чтобы освободить место на диске для других целей.

При расчете объема, доступного для файлов заданий, PT Sandbox учитывает объемы, выделенные для операционной системы, работы PT Sandbox, образов виртуальных машин и карантина.

Внимание! Не изменяйте объем для файлов заданий часто. Во время применения изменений могут перестать проверяться файлы или могут возникнуть задержки в их обработке. Изменение объема в меньшую сторону может привести к потере файлов в хранилище.

► Чтобы изменить объем для файлов заданий:

1. В главном меню в разделе **Система** выберите пункт **Основные параметры**.

Откроется страница **Система** на вкладке **Основные параметры**.

2. В блоке **Файлы заданий** введите объем, который будет зарезервирован для файлов заданий.

3. Нажмите кнопку **Сохранить**.

Изменения будут применены через некоторое время.

22. Настройка карантина

Письмо, заблокированное в результате проверки, размер которого не превышает 1 ГБ, вместо удаления можно перемещать в карантин. Пока письмо находится в карантине, оператор безопасности может проанализировать его содержимое и, если признает его неопасным, переслать письмо адресатам.

PT Sandbox начинает удалять письма из карантина при выполнении хотя бы одного из условий:

- истек срок хранения писем в карантине, который указан в параметрах PT Sandbox;
- заполнено 90% от максимального объема карантина, который указан в параметрах PT Sandbox;
- до полного заполнения объема карантина остался 1 ГБ свободного места;
- в карантин помещено 95% от максимально допустимого количества файлов.

Удаляются самые старые письма, при этом помещение новых писем в карантин не ограничивается.

► Чтобы настроить карантин:

1. В главном меню в разделе **Система** выберите пункт **Основные параметры**.

Откроется страница **Система** на вкладке **Основные параметры**.

Примечание. При расчете объема, доступного для карантина, PT Sandbox учитывает объемы, выделенные для операционной системы, работы PT Sandbox, образов виртуальных машин и файлов заданий.

2. В блоке **Карантин** в поле **Срок хранения в карантине** укажите количество дней, в течение которых письма будут храниться в карантине и будут доступны для пересылки адресатам.
3. Если требуется, включите резервный почтовый сервер и укажите его параметры.

Резервный почтовый сервер всегда используется для пересылки заблокированных писем от источника "Почтовый сервер с установленным агентом" и в случае отключения или удаления источника "Почтовый сервер в режиме фильтрации". Если источник "Почтовый сервер в режиме фильтрации" включен, письма от этого источника пересылаются с помощью почтового сервера, указанного в параметрах источника.

4. Нажмите кнопку **Сохранить**.

Карантин настроен.

23. Изменение срока хранения заданий на проверку

На странице **Задания**, доступной в главном меню PT Sandbox, отображается информация о заданиях на проверку. Вы можете изменить срок хранения этой информации в интерфейсе продукта.

- ▶ Чтобы изменить срок хранения заданий на проверку:
 1. В главном меню в разделе **Система** выберите пункт **Основные параметры**.
Откроется страница **Система** на вкладке **Основные параметры**.
 2. В блоке **История проверок** выберите срок хранения заданий на проверку.
 3. Нажмите кнопку **Сохранить**.
- Срок хранения заданий на проверку изменен.

24. Настройка отправки сообщений в системный журнал по протоколу syslog

PT Sandbox может выступать в качестве источника [сообщений для системного журнала](#) (см. приложение Б). Для отправки сообщений в системный журнал PT Sandbox использует протокол syslog.

► Чтобы настроить отправку сообщений в системный журнал по протоколу syslog:

1. В главном меню в разделе **Система** выберите пункт **Основные параметры**.
Откроется страница **Система** на вкладке **Основные параметры**.
2. В блоке параметров **Отправка сообщений в системный журнал по протоколу syslog** включите отправку сообщений.
3. В полях **Syslog-сервер** введите IP-адрес или доменное имя и порт syslog-сервера, на который PT Sandbox должен отправлять сообщения.
4. Выберите транспортный протокол (TCP или UDP) для передачи сообщений на syslog-сервер.
5. Нажмите кнопку **Сохранить**.

Изменения будут применены через несколько минут.

Отправка сообщений в системный журнал по протоколу syslog настроена.

25. Управление узлами в многосерверной конфигурации PT Sandbox

В этом разделе приводятся инструкции по управлению узлами в многосерверной конфигурации PT Sandbox.

В этом разделе

[Добавление узла в кластер PT Sandbox \(см. раздел 25.1\)](#)

[Отключение дополнительного узла \(см. раздел 25.2\)](#)

[Отключение функции поведенческого анализа на основном узле \(см. раздел 25.3\)](#)

25.1. Добавление узла в кластер PT Sandbox

Если PT Sandbox, установленный в организации, не справляется с задачами поведенческого анализа и вам нужно уменьшить время проверки файлов с использованием этого метода, вы можете добавить физические серверы или виртуальные машины в кластер PT Sandbox. При этом, если в кластере был всего один узел с PT Sandbox, он становится основным после добавления нового узла.

► Чтобы добавить узел в кластер PT Sandbox:

1. Если название нового узла (hostname) совпадает с названием ранее добавленного узла в кластере, измените название нового узла на уникальное.
2. Установите PT Sandbox на новом сервере или виртуальной машине вместе с операционной системой или в подготовленной операционной системе.
3. [Активируйте функцию поведенческого анализа на новом узле \(см. раздел 9.5\)](#).

Узел добавлен в кластер.

Теперь вы можете [отключить поведенческий анализ на основном узле \(см. раздел 25.3\)](#).

25.2. Отключение дополнительного узла

Если физический сервер с дополнительным узлом вышел из строя или вы планируете удалить PT Sandbox с этого сервера, вам нужно отключить этот дополнительный узел.

► Чтобы отключить дополнительный узел,

на основном узле последовательно выполните следующие команды:

```
sudo -i
export KUBECONFIG=/etc/kubernetes/admin.conf
kubectl delete node <Название дополнительного узла>
```

В случае успешного выполнения последней команды появится сообщение node "**<Название дополнительного узла>**" deleted.

Примечание. Вы можете получить список названий всех узлов PT Sandbox, выполнив на основном узле команду `sudo /opt/ptms/sbin/ptmsctl sandbox nodes list`. После отключения дополнительного узла его название должно пропасть из этого списка.

Дополнительный узел отключен.

Теперь вы можете удалить PT Sandbox вместе с операционной системой с этого сервера.

25.3. Отключение функции поведенческого анализа на основном узле

Если вы добавили в кластер дополнительные узлы для выполнения поведенческого анализа, вы можете отключить выполнение поведенческого анализа на основном узле, чтобы освободить его аппаратные ресурсы.

- ▶ Чтобы отключить функцию поведенческого анализа на основном узле,

выполните команду:

```
sudo /opt/ptms/sbin/ptmsctl sandbox nodes release <Название основного узла>
```

Например:

```
sudo /opt/ptms/sbin/ptmsctl sandbox nodes release ptms-host-main
```

Функция поведенческого анализа отключена на основном узле.

26. Удаление почтового агента

Вы можете удалить почтовый агент с сервера Microsoft Exchange. В процессе удаления будет перезапущена служба MS Exchange Transport.

► Чтобы удалить почтовый агент:

1. Войдите с правами администратора в операционную систему Windows, в которой работает Microsoft Exchange с установленным почтовым агентом.
2. В командной строке Windows перейдите в каталог с установщиком почтового агента.

Например:

```
cd C:\exchange-mta
```

Примечание. Если этот каталог был удален, вам нужно скопировать архив с установщиком почтового агента в любой каталог, распаковать его и перейти в каталог с распакованным установщиком.

3. Запустите процедуру удаления почтового агента:

```
install.cmd -Uninstall
```

Начнется процесс удаления почтового агента. По окончании процесса появится сообщение `Uninstallation completed`.

Почтовый агент удален.

27. Диагностика и устранение неисправностей

В этом разделе описываются возможные проблемы в работе PT Sandbox, варианты их решения, а также приводится инструкция по сбору файлов журналов для их отправки в службу технической поддержки.

В этом разделе

[Устранение проблем с действующей лицензией \(см. раздел 27.1\)](#)

[Устранение проблем при замене лицензии \(см. раздел 27.2\)](#)

[Недоступен образ ВМ \(см. раздел 27.3\)](#)

[Сбор файлов журналов для отправки в техническую поддержку \(см. раздел 27.4\)](#)

27.1. Устранение проблем с действующей лицензией

Проблема

На странице с [информацией о лицензии \(см. раздел 12\)](#) отображается сообщение о проблемах с лицензией. Файлы проверяются, но PT Sandbox и антивирусные базы не обновляются.

Внимание! Вам нужно решить проблему в течение двух недель с момента ее появления. В противном случае сканирование отключится и файлы, представляющие угрозу, перестанут блокироваться (если блокирующий режим был определен лицензией).

Возможные причины

Проблема может возникать в следующих случаях:

- Изменилась конфигурация сервера с установленным PT Sandbox (например, изменились комплектующие сервера).
- На сервере с установленным PT Sandbox был удален или поврежден файл, содержащий информацию о лицензии (например, кто-то вручную удалил каталог, содержащий этот файл).
- Служба лицензирования PT Sandbox работает некорректно или была остановлена (например, кто-то вручную принудительно завершил ее процесс через консоль ОС).
- У сервера с установленным PT Sandbox нет доступа по HTTPS к поддоменам ptsecurity.com.

Решение

► Чтобы решить проблему:

1. В главном меню в разделе **Система** выберите пункт **Лицензия**.

Откроется страница **Система** на вкладке **Лицензия**.

2. Нажмите кнопку **Проверить лицензию**.

Начнется проверка добавленной лицензии с использованием службы лицензирования.

3. Если сообщение о проблеме с лицензией не исчезло, на сервере с установленным PT Sandbox проверьте доступ к поддоменам ptsecurity.com по HTTPS. Это можно сделать, проверив доступ к поддомену update.ptsecurity.com:

```
wget -Sq -O /dev/null https://update.ptsecurity.com
```

Если доступ к указанным адресам есть, результаты выполнения команд будут начинаться со строки HTTP/1.1 403 Forbidden.

4. Если доступ к указанным адресам отсутствует, восстановите его, после чего еще раз нажмите кнопку **Проверить лицензию**.

Начнется проверка добавленной лицензии с использованием службы лицензирования.

5. Если сообщение о проблемах с лицензией не исчезло, [соберите файлы журналов \(см. раздел 27.4\)](#) и отправьте их в службу технической поддержки "Позитив Текнолоджиз" для дальнейшего анализа.

См. также

[Лицензирование \(см. раздел 6\)](#)

27.2. Устранение проблем при замене лицензии

Проблема

Если при замене лицензии возникла проблема, информация о ней отображается на странице с [информацией о лицензии \(см. раздел 12\)](#).

Возможные причины

Проблема может возникать в следующих случаях:

- Недоступен сервер, на котором проверяются лицензии.
- Лицензия сконфигурирована неверно.

Решение

► Чтобы решить проблему:

1. Повторите попытку [замены лицензии \(см. раздел 13\)](#).
2. Если сообщение о проблеме с лицензией не исчезло, на сервере с установленным PT Sandbox проверьте доступ к поддоменам ptsecurity.com по HTTPS. Это можно сделать, проверив доступ к поддомену update.ptsecurity.com:

```
wget -Sq -O /dev/null https://update.ptsecurity.com
```

Если доступ к указанному адресу есть, результат выполнения команды будет начинаться со строки HTTP/1.1 403 Forbidden.

Внимание! Если в вашей организации используется ПО, ограничивающее сетевой доступ, убедитесь, что доступ обеспечен не только к update.ptsecurity.com, а к любым поддоменам ptsecurity.com.

3. Если доступ к указанному адресу отсутствует, восстановите его, после чего еще раз повторите попытку [замены лицензии \(см. раздел 13\)](#).
4. Если сообщение о проблеме с лицензией не исчезло, [соберите файлы журналов \(см. раздел 27.4\)](#) и отправьте их в службу технической поддержки "Позитив Текнолоджиз" для дальнейшего анализа.

27.3. Недоступен образ ВМ

Если образ ВМ, выбранный в параметрах источника для проверки, стал недоступен после обновления лицензии, уведомление о недоступности образа отобразится в меню информации о продукте (значок ⓘ в главном меню). Причиной недоступности образа может быть удаление его из лицензии.

► Чтобы решить проблему:

1. В главном меню в разделе **Система** выберите пункт **Источники для проверки**.
Откроется страница **Система** на вкладке **Источники для проверки**.
2. Проверьте, какие источники используют для проверки удаленный образ.
3. Если удаление образа из лицензии было предусмотрено, замените его на другие образы ВМ для всех источников, которые его использовали.
4. Если вы считаете, что образ ВМ был удален по ошибке или вам нужно вернуть его в лицензию, обратитесь в службу технической поддержки "Позитив Текнолоджиз".

См. также

[Страница со списком образов виртуальных машин \(см. раздел 11.3\)](#)

[Изменение параметров источника для проверки \(см. раздел 15.1\)](#)

27.4. Сбор файлов журналов для отправки в техническую поддержку

Если вам не удалось решить проблему в работе продукта самостоятельно, вы можете собрать файлы журналов PT Sandbox и отправить их в службу технической поддержки "Позитив Текнолоджиз" для дальнейшего анализа.

- ▶ Чтобы собрать файлы журналов,

в главном меню нажмите ⓘ и во всплывающем окне нажмите кнопку **Скачать файлы журналов**.

PT Sandbox начнет собирать файлы журналов продукта. Этот процесс может занять несколько минут в зависимости от общего размера файлов журналов, а также от аппаратных ресурсов сервера или виртуальной машины с установленным PT Sandbox. По окончании сбора архив `ptms-logs-ГГГГ-ММ-ДД_чч-мм-сс.zip` будет сохранен на вашем компьютере (время в названии архива — в UTC).

Файлы журналов собраны.

28. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;
- диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;
- разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;
- устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале support.ptsecurity.com или по телефону. Запросы на портале — основной способ обращений за технической поддержкой.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

[Техническая поддержка на портале \(см. раздел 28.1\)](#)

[Техническая поддержка по телефону \(см. раздел 28.2\)](#)

[Время работы службы технической поддержки \(см. раздел 28.3\)](#)

[Как служба технической поддержки работает с запросами \(см. раздел 28.4\)](#)

28.1. Техническая поддержка на портале

Портал support.ptsecurity.com предоставляет вам возможность создавать запросы на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов "Позитив Текнолджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Техническая поддержка на портале предоставляется на русском и английском языках.

28.2. Техническая поддержка по телефону

Вы можете связаться со службой технической поддержки по телефону +7 495 744 01 44.

Техническая поддержка по телефону предоставляется на русском и английском языках.

Сотрудники технической поддержки по телефону могут выполнить оперативную диагностику, ответить на простые вопросы или уточнить текущий статус работ по ранее созданному запросу.

Если решить вопрос по телефону в разумное время (15–20 минут) невозможно, создайте запрос на портале support.ptsecurity.com. Запрос на портале, созданный и обновляемый по рекомендациям специалиста технической поддержки, гарантирует дальнейшие работы по вашему обращению.

28.3. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний. Сотрудники технической поддержки работают по имеющимся запросам и принимают обращения по телефону с понедельника по пятницу с 9:00 до 19:00 UTC+3.

28.4. Как служба технической поддержки работает с запросами

При получении вашего запроса специалист службы технической поддержки классифицирует его (присваивает запросу тип и уровень значимости) и выполняет дальнейшие шаги по выполнению запроса.

В этом разделе

[Предоставление информации для технической поддержки \(см. раздел 28.4.1\)](#)

[Типы запросов \(см. раздел 28.4.2\)](#)

[Время реакции и приоритизация запросов \(см. раздел 28.4.3\)](#)

[Выполнение работ по запросу \(см. раздел 28.4.4\)](#)

28.4.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста "Позитив Текнолоджиз" нужно предоставить:

- номер лицензии на использование продукта;
- файлы журналов и другие наборы диагностических данных, хранящихся в продукте;
- снимки экрана;
- результаты выполнения рекомендаций специалиста технической поддержки;
- каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

"Позитив Текнолоджиз" не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть запрос.

28.4.2. Типы запросов

Специалист технической поддержки относит ваш запрос к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист "Позитив Текнолоджиз" оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). "Позитив Текнолоджиз" не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

"Позитив Текнолоджиз" предоставляет пакеты обновления продукта в течение срока действия лицензии на продукт.

"Позитив Текнолоджиз" не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, "Позитив Текнолоджиз" обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

28.4.3. Время реакции и приоритизация запросов

Время реакции на запрос рассчитывается с момента получения запроса до первичного ответа специалиста технической поддержки с уведомлением о взятии запроса в работу.

Время обработки запроса рассчитывается с момента отправки уведомления о взятии вашего запроса в работу до предоставления описания дальнейших шагов по устранению проблемы либо классификации вопроса, указанного в запросе, как дефекта ПО и передачи запроса ответственным лицам для исправления дефекта.

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 7).

Специалист службы технической поддержки оставляет за собой право переопределять уровень значимости запроса по приведенным ниже критериям. Указанные сроки являются целевыми и подразумевают стремление и разумные усилия исполнителя для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 7. Время реакции на запрос и время его обработки

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 4 часов	Не ограничено
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 24 часов	Не ограничено
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес	До 24 часов	Не ограничено

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки запроса).

28.4.4. Выполнение работ по запросу

По мере выполнения работ по вашему запросу специалист технической поддержки сообщает вам:

- о диагностике проблемы и ее результатах;
- о поиске решения или возможности обойти причины возникновения проблемы;
- о планировании и выпуске обновления продукта (если требуется для устранения проблемы).

Если по итогам обработки запроса необходимо внести изменения в продукт, "Позитив Текнолоджиз" включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по запросу считаются выполненными, если:

- предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- проблема вызвана программными продуктами или оборудованием сторонних производителей, не подпадающих под гарантийные обязательства по продукту;
- проблема классифицирована как неподдерживаемая.

Приложение А. Сценарии отказов

Если PT Sandbox развернут в кластере высокой доступности, 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 Sandbox 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 Sandbox

Компонент	Следствие отказа		
	Потерянные данные	Недоступность компонентов и функций	Ухудшение производительности
Служба высокой доступности	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, повторное сканирование, скачивание файлов
Модуль поведенческого анализа	—	—	Модуль поведенческого анализа

См. также

[Обеспечение отказоустойчивости PT Sandbox \(см. раздел 4.7\)](#)

[Компоненты PT Sandbox \(см. раздел 4.6\)](#)

Приложение Б. Сообщения, отправляемые в системный журнал по протоколу syslog

PT Sandbox может отправлять на сервер системного журнала по протоколу syslog:

- сообщения о ходе сканирования файлов антивирусами, включая информацию о файлах и источниках их получения, распаковке архивов и обнаруженных угрозах;
- уведомления об обновлении антивирусов или их баз;
- информацию о результатах повторного сканирования файлов.

Вы можете включить и настроить отправку сообщений по протоколу syslog в интерфейсе PT Sandbox для централизованного сбора и анализа событий ИБ в информационной системе вашей организации.

PT Sandbox формирует тело сообщения в формате JSON, а заголовок сообщения в формате, описанном в [RFC 5424](#). Тип сообщения записывается в части MSGID заголовка. Значение приоритета, которое указывается в части PRI заголовка, для всех отправляемых сообщений равно 100.

В этом разделе

[Сообщения о сканировании файлов \(см. раздел Б.1\)](#)

[Сообщение av.update \(см. раздел Б.2\)](#)

[Сообщение retro_scan.start \(см. раздел Б.3\)](#)

[Сообщение retro.artifact_verdict_changed \(см. раздел Б.4\)](#)

[Кодовые имена антивирусов \(см. раздел Б.5\)](#)

См. также

[Настройка отправки сообщений в системный журнал по протоколу syslog \(см. раздел 24\)](#)

Б.1. Сообщения о сканировании файлов

Алгоритм отправки сообщений об обработке задания на проверку файлов представлен на рисунке ниже, где в зеленых блоках — названия типов сообщений.

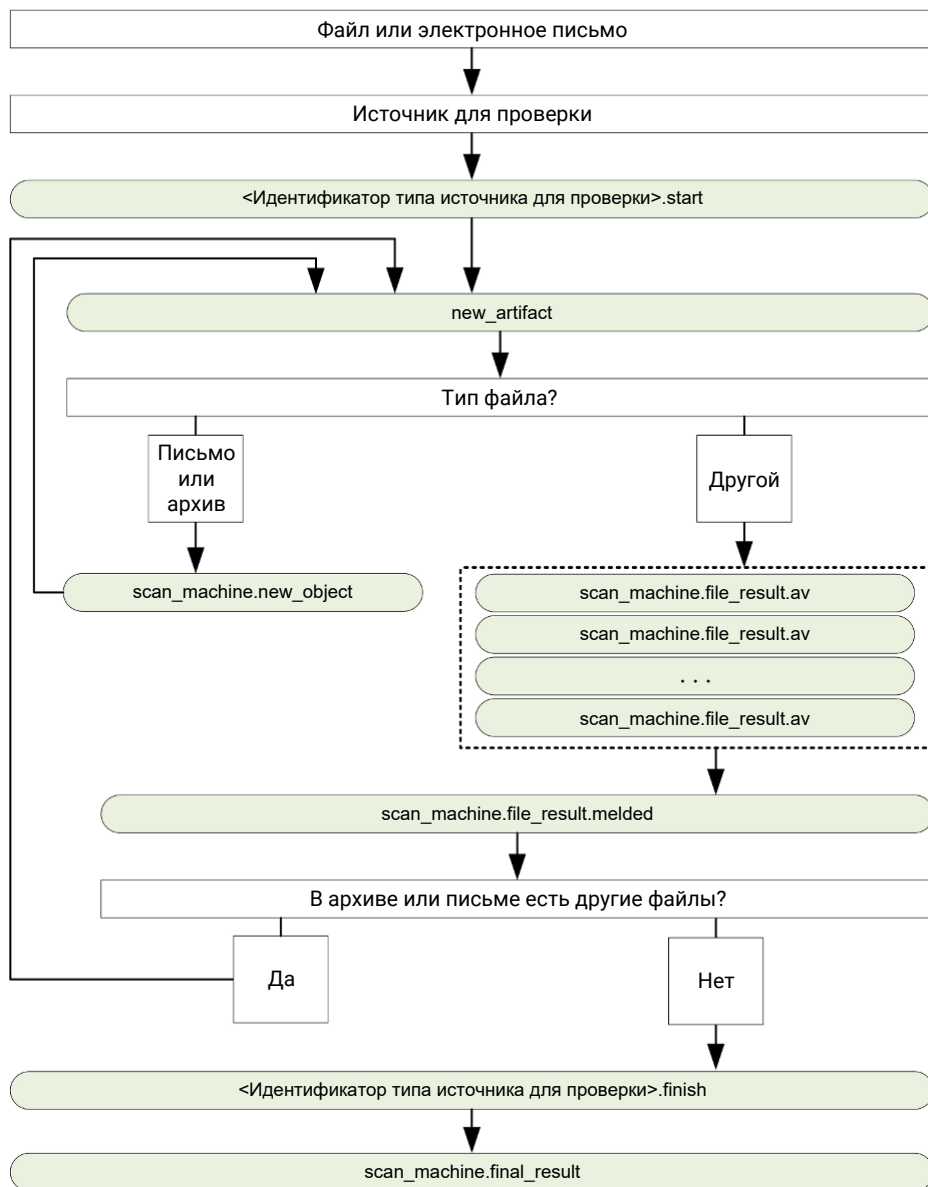


Рисунок 55. Алгоритм отправки сообщений о сканировании в syslog

Подробное описание алгоритма:

1. PT Sandbox получает файл или электронное письмо на одну из своих точек входа — [источников для проверки \(см. раздел 4.2\)](#).
2. PT Sandbox отправляет сообщение типа <Идентификатор типа источника для проверки>.start (например, email.start).

Это сообщение информирует о начале обработки файла и содержит уникальный идентификатор задания на проверку файла, информацию о файле и о том, как он был получен.

3. PT Sandbox отправляет сообщение типа new_artifact.

В этом сообщении содержатся информация о файле и идентификатор задания, в ходе которого этот файл был получен.

4. Если файл из задания является архивом или письмом, PT Sandbox попытается извлечь файлы из этого архива или письма. При извлечении файла PT Sandbox отправляет в системный журнал сообщение с типом `scan_machine.new_object`.

В этом сообщении содержатся информация об извлеченных файлах, информация об архиве или письме, из которого были извлечены файлы, а также идентификатор задания.

Примечание. При извлечении каждого файла в свою очередь отправляется отдельное сообщение типа `new_artifact` (см. предыдущий пункт) с указанием родительского файла.

5. После сканирования файла антивирусом PT Sandbox отправляет сообщение с типом `scan_machine.file_result.av`.

В этом сообщении содержатся информация о файле, идентификатор задания, в ходе которого этот файл был получен, а также результаты сканирования файла конкретным антивирусом.

6. Получив результаты сканирования файла от всех антивирусов, PT Sandbox отправляет в системный журнал сообщение типа `scan_machine.file_result.melded`.

В этом сообщении содержатся информация о файле, идентификатор задания, в ходе которого этот файл был получен, а также общий результат сканирования файла всеми антивирусами.

7. По завершении сканирования всех файлов задания PT Sandbox отправляет в системный журнал сообщение типа `scan_machine.final_result`.

В этом сообщении содержатся идентификатор задания и итоговый результат сканирования по этому заданию.

8. PT Sandbox отправляет в системный журнал сообщение с типом `<Идентификатор типа источника для проверки>.finish` (например, `email.finish`).

Это сообщение информирует об окончании обработки задания и содержит уникальный идентификатор задания и признак успешности обработки задания.

Примечание. Если файл поступал на сканирование через веб-интерфейс, сообщение об окончании обработки задания не отправляется.

В этом разделе

Сообщения `<Идентификатор типа источника для проверки>.start` (см. раздел Б.1.1)

Сообщение `new_artifact` (см. раздел Б.1.2)

Сообщение `scan_machine.new_object` (см. раздел Б.1.3)

Сообщение `scan_machine.file_result.av` (см. раздел Б.1.4)

Сообщение `scan_machine.file_result.melded` (см. раздел Б.1.5)

Сообщение `scan_machine.final_result` (см. раздел Б.1.6)

Сообщения <Идентификатор типа источника для проверки>.finish (см. раздел Б.1.7)

Идентификаторы типов источников для проверки (см. раздел Б.1.8)

Б.1.1. Сообщения <Идентификатор типа источника для проверки>.start

При создании задания на проверку PT Sandbox отправляет в системный журнал сообщение типа <Идентификатор типа источника для проверки>.start (например, email.start). Это сообщение информирует о начале обработки файлов из задания и содержит уникальный идентификатор задания, информацию о файлах в задании и о том, как они были получены.

В зависимости от типа источника, от которого были получены файлы, сообщения имеют разную структуру и содержание.

В этом разделе

Сообщение check_me.start (см. раздел Б.1.1.1)

Сообщение dpi.start (см. раздел Б.1.1.2)

Сообщение email.start (см. раздел Б.1.1.3)

Сообщение mail_bcc.start (см. раздел Б.1.1.4)

Сообщение mail_gateway.start (см. раздел Б.1.1.5)

Сообщение files_inbox.start (см. раздел Б.1.1.6)

Сообщение files_monitor.start (см. раздел Б.1.1.7)

Сообщение icap.start (см. раздел Б.1.1.8)

Сообщение user_scan.start (см. раздел Б.1.1.9)

См. также

Идентификаторы типов источников для проверки (см. раздел Б.1.8)

Б.1.1.1. Сообщение check_me.start

В таблице ниже описываются поля и объекты в сообщении check_me.start о начале обработки задания на проверку письма, полученного службой Checkme.

Таблица 9. Поля в сообщении check_me.start

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
scan_id	—	—	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
entry_point_id	—	—	Название источника для проверки в интерфейсе PT Sandbox	Строка
email	—	id from_address to_list cc_list bcc_list subject references reply_to files	Блок данных о письме	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
id	email	—	Поле заголовка Message-ID	Строка
from_address	email	address name	Блок данных об отправителе письма	Объект
to_list	email	Словари с полями address и name	Блок данных о получателях письма	Массив
cc_list	email	Словари с полями address и name	Блок данных о получателях копии письма	Массив
bcc_list	email	Словари с полями address и name	Блок данных о получателях скрытой копии письма	Массив
address	from_address to_list cc_list bcc_list	—	Адрес электронной почты	Строка
name	from_address to_list cc_list bcc_list	—	Имя отправителя (получателя) письма	Строка
subject	email	—	Тема письма	Строка
references	email	—	Идентификационное поле заголовка references согласно RFC 5322	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
reply_to	email	—	Идентификационное поле заголовка in-reply-to согласно RFC 5322	Строка
files	email	Словари с полями: — mime_type — md5 — sha1 — sha256 — size — name	Блок данных о файлах, прикрепленных к письму	Массив
mime_type	files	—	MIME-тип файла	Строка
md5	files	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка
sha1	files	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	files	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	files	—	Размер файла в байтах	64-разрядное беззнаковое целое число
name	files	—	Имя файла	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
envelope	—	from_address recipients	Блок данных из части Envelope электронного письма	Объект
from_address	envelope	—	Адрес электронной почты отправителя письма	Строка
recipients	envelope	Строки	Блок данных о получателях письма	Массив
received	—	—	UNIX-время формирования задания на проверку	Число с плавающей точкой

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - check_me.start - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "entry_point_id": "checkme-service",
  "email": {
    "id": "<name@58d4cf987f-chlq>",
    "from_address": {
```

```
"address": "ivanov@example.org",  
"name": "Alexander Ivanov"  
},  
"to_list": [  
  {  
    "address": "checkme@example.org",  
    "name": ""  
  }  
],  
"cc_list": [  
  {  
    "address": "username@example.org",  
    "name": "Ivan Ivanov"  
  }  
],  
"bcc_list": [  
  {  
    "address": "admin@example.org",  
    "name": ""  
  }  
],  
"subject": "Проверка файла",
```

```
"references": "user@example.org",
"reply_to": "",
"files": [
  {
    "mime_type": "application/x-dosexec; charset=binary",
    "md5": "11aced0fd6535f6e...1495ba1c7be00",
    "sha1": "45e50e2af429e44...6f59e46b18b60",
    "sha256": "23ef04408bb2c...7928e7caf3d7f",
    "size": 64000,
    "name": "software.exe"
  }
],
"envelope": {
  "from_address": "ivanov@example.org",
  "recipients": ["checkme@example.org", "username@example.org", "admin@example.org"]
},
"received": 1511421762.957363
}
```

См. также

[Сообщение check_me.finish \(см. раздел Б.1.7.1\)](#)

[Создание и настройка службы Checkme \(см. раздел 14.1\)](#)

Б.1.1.2. Сообщение dpi.start

В таблице ниже описываются поля и объекты в сообщении dpi.start о начале обработки задания на проверку файла, полученного от модуля захвата трафика или PT NAD.

Таблица 10. Поля в сообщении dpi.start

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
scan_id	—	—	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
entry_point_id	—	—	Название источника для проверки в интерфейсе PT Sandbox	Строка
meta	—	src dst filename magic file_id	Блок данных о файле, полученного от модуля захвата трафика или PT NAD	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
		proto state один из двух объектов: http или smtp		
src	meta	ip port	Блок данных об отправителе файла	Объект
dst	meta	ip port	Блок данных о получателе файла	Объект
ip	src dst	—	IP-адрес	Строка
port	src dst	—	Номер сетевого порта	32-разрядное без- знаковое целое число
filename	meta	—	Имя файла	Строка
magic	meta	—	Текстовое описание автоматически определенного формата файла	Строка
file_id	meta	—	Идентификатор файла, полученный от модуля захвата трафика или PT NAD	Строка
proto	meta	—	Прикладной протокол, который исполь- зовался для передачи файла	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
state	meta	—	Состояние записи файла. Возможные значения: <ul style="list-style-type: none"> — "UNKNOWN" — состояние неизвестно; — "COMPLETED" — файл записан; — "TRUNCATED" — файл записан не полностью, но данных больше нет; — "ERROR" — ошибка записи (при получении ошибки файл удаляется). PT Sandbox отправляет на проверку файлы с состоянием COMPLETED	Строка
http	meta	referer user_agent host uri	Блок данных с информацией о файле, относящейся к HTTP	Объект
referer	http	—	Адрес предыдущей веб-страницы, с которой был осуществлен данный HTTP-запрос	Строка
user_agent	http	—	Название и версия браузера	Строка
host	http	—	HTTP-адрес узла, с которого был скачан файл	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
uri	http	—	URI файла	Строка
file	—	mime_type md5 sha1 sha256 size name	Блок данных о файле	Объект
mime_type	file	—	MIME-тип файла	Строка
md5	file	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка
sha1	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	file	—	Размер файла в байтах	64-разрядное беззнаковое целое число
name	file	—	Имя файла	Строка
received	—	—	UNIX-время формирования задания на проверку	Число с плавающей точкой

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - dpi.start - {  
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",  
  "created": 1511421763.3728465,  
  "entry_point_id": "dpi-module",  
  "meta": {  
    "src": {  
      "ip": "203.0.113.43",  
      "port": 8080  
    },  
    "dst": {  
      "ip": "203.0.113.11",  
      "port": 8080  
    },  
    "filename": "example",  
    "magic": "ASCII text, with very long lines",  
    "file_id": "10007",  
    "proto": "HTTP",  
    "state": "COMPLETED",  
    "http": {  
      "referer": "<unknown>",  
      "user_agent": "Wget/1.15 (linux-gnu)",
```

```
    "host": "203.0.113.43",  
    "uri": "/test"  
  },  
  "file": {  
    "mime_type": "application/x-dosexec; charset=binary",  
    "md5": "11aced0fd6535f6e...1495ba1c7be00",  
    "sha1": "45e50e2af429e44...6f59e46b18b60",  
    "sha256": "23ef04408bb2c...7928e7caf3d7f",  
    "size": 64000,  
    "name": "software.exe"  
  },  
  "received": 1511421762.957363  
}
```

См. также

[Сообщение dpi.finish \(см. раздел Б.1.7.2\)](#)

[Настройка проверки трафика организации при помощи модуля захвата трафика \(см. раздел 14.6\)](#)

Б.1.1.3. Сообщение email.start

В таблице ниже описываются поля и объекты в сообщении `email.start` о начале обработки задания на проверку письма, полученного почтовым агентом от сервера Microsoft Exchange организации.

Таблица 11. Поля в сообщении email.start

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
scan_id	—	—	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
entry_point_id	—	—	Название источника для проверки в интерфейсе PT Sandbox	Строка
email	—	id from_address to_list cc_list bcc_list subject references reply_to files	Блок данных о письме	Объект
id	email	—	Поле заголовка Message-ID	Строка
from_address	email	address name	Блок данных об отправителе письма	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
to_list	email	Словари с полями address и name	Блок данных о получателях письма	Массив
cc_list	email	Словари с полями address и name	Блок данных о получателях копии письма	Массив
bcc_list	email	Словари с полями address и name	Блок данных о получателях скрытой копии письма	Массив
address	from_address to_list cc_list bcc_list	—	Адрес электронной почты	Строка
name	from_address to_list cc_list bcc_list	—	Имя отправителя (получателя) письма	Строка
subject	email	—	Тема письма	Строка
references	email	—	Идентификационное поле заголовка references согласно RFC 5322	Строка
reply_to	email	—	Идентификационное поле заголовка in-reply-to согласно RFC 5322	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
files	email	Словари с полями: — mime_type — md5 — sha1 — sha256 — size — name	Блок данных о файлах, прикрепленных к письму	Массив
mime_type	files	—	MIME-тип файла	Строка
md5	files	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка
sha1	files	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	files	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	files	—	Размер файла в байтах	64-разрядное беззнаковое целое число
name	files	—	Имя файла	Строка
envelope	—	from_address recipients	Блок данных из части Envelope электронного письма	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
from_address	envelope	—	Адрес электронной почты отправителя письма	Строка
recipients	envelope	Строки	Блок данных о получателях письма	Массив
received	—	—	UNIX-время формирования задания на проверку	Число с плавающей точкой

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - email.start - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "entry_point_id": "mail-agent",
  "email": {
    "id": "<6fee62f024e0@example.com>",
    "from_address": {
      "address": "ivanov@example.org",
      "name": "Ivan Ivanov"
    },
    "to_list": [ {
      "address": "username@example.com",
      "name": "Ivan Ivanov"
    }
  ]
}
```

```
    }  
  ],  
  "subject": "Последняя версия моей программы",  
  "references": "",  
  "reply_to": "",  
  "files": [{  
    "mime_type": "application/x-dosexec; charset=binary",  
    "md5": "11aced0fd6535f6e...1495ba1c7be00",  
    "sha1": "45e50e2af429e44...6f59e46b18b60",  
    "sha256": "23ef04408bb2c...7928e7caf3d7f",  
    "size": 64000,  
    "name": "software.exe"  
  }  
]  
},  
"envelope": {  
  "from_address": "ivanov@example.org",  
  "recipients": ["checkme@example.org", "username@example.org", "admin@example.org"]  
},  
"received": 1511421762.957363  
}
```

См. также

[Сообщение email.finish \(см. раздел Б.1.7.3\)](#)

[Подключение к почтовому серверу при помощи агента \(см. раздел 14.3.1\)](#)

Б.1.1.4. Сообщение mail_bcc.start

В таблице ниже описываются поля и объекты в сообщении `mail_bcc.start` о начале обработки задания на проверку письма, полученного от почтового сервера организации в виде скрытой копии.

Таблица 12. Поля в сообщении mail_bcc.start

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
scan_id	—	—	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
entry_point_id	—	—	Название источника для проверки в интерфейсе PT Sandbox	Строка
client	—	ip	Блок данных с информацией об SMTP-клиенте	Объект
ip	client	—	IP-адрес SMTP-клиента	Строка
email	—	id from_address	Блок данных о письме	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
		to_list cc_list subject references reply_to files		
id	email	—	Поле заголовка Message-ID	Строка
from_address	email	address name	Блок данных об отправителе письма	Объект
to_list	email	Словари с полями address и name	Блок данных о получателях письма	Массив
cc_list	email	Словари с полями address и name	Блок данных о получателях копии письма	Массив
address	from_address to_list cc_list	—	Адрес электронной почты	Строка
name	from_address to_list cc_list	—	Имя отправителя (получателя) письма	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
subject	email	—	Тема письма	Строка
references	email	—	Идентификационное поле заголовка references согласно RFC 5322	Строка
reply_to	email	—	Идентификационное поле заголовка in-reply-to согласно RFC 5322	Строка
files	email	Словари с полями: — mime_type — md5 — sha1 — sha256 — size — name	Блок данных о файлах, прикрепленных к письму	Массив
envelope	—	from_address recipients	Блок данных из части Envelope электронного письма	Объект
from_address	envelope	—	Адрес электронной почты отправителя письма	Строка
recipients	envelope	Строки	Блок данных о получателях письма	Массив
received	—	—	UNIX-время формирования задания на проверку	Число с плавающей точкой

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - mail_bcc.start - {  
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",  
  "created": 1511421763.3728465,  
  "entry_point_id": "mail-bcc",  
  "client": {  
    "ip": "203.0.113.33"  
  },  
  "email": {  
    "id": "<6fee62f024e0@example.com>",  
    "from_address": {  
      "address": "ivanov@example.org",  
      "name": "Ivan Ivanov"  
    },  
    "to_list": [ {  
      "address": "username@example.com",  
      "name": "Ivan Ivanov"  
    }  
  ],  
  "subject": "Последняя версия моей программы",  
  "references": "",  
  "reply_to": "",
```

```
"files": [{
  "mime_type": "application/x-dosexec; charset=binary",
  "md5": "11aced0fd6535f6e...1495ba1c7be00",
  "sha1": "45e50e2af429e44...6f59e46b18b60",
  "sha256": "23ef04408bb2c...7928e7caf3d7f",
  "size": 64000,
  "name": "software.exe"
}]
},
"envelope": {
  "from_address": "ivanov@example.org",
  "recipients": ["bcc@multiscanner.local"]
},
"received": 1511421762.957363
}
```

См. также

[Сообщение mail_bcc.finish \(см. раздел Б.1.7.4\)](#)

[Настройка зеркалирования почтового трафика с помощью bcc \(см. раздел 14.3.2\)](#)

Б.1.1.5. Сообщение mail_gateway.start

В таблице ниже описываются поля и объекты в сообщении `mail_gateway.start` о начале обработки задания на проверку письма, полученного от почтового сервера Postfix или Exim в режиме фильтрации.

Таблица 13. Поля в сообщении mail_gateway.start

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
scan_id	—	—	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
entry_point_id	—	—	Название источника для проверки в интерфейсе PT Sandbox	Строка
client	—	ip	Блок данных с информацией об SMTP-клиенте	Объект
ip	client	—	IP-адрес SMTP-клиента	Строка
email	—	id from_address to_list cc_list bcc_list subject	Блок данных о письме	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
		references reply_to files		
id	email	—	Поле заголовка Message-ID	Строка
from_address	email	address name	Блок данных об отправителе письма	Объект
to_list	email	Словари с полями address и name	Блок данных о получателях письма	Массив
cc_list	email	Словари с полями address и name	Блок данных о получателях копии письма	Массив
bcc_list	email	Словари с полями address и name	Блок данных о получателях скрытой копии письма	Массив
address	from_address to_list cc_list bcc_list	—	Адрес электронной почты	Строка
name	from_address to_list cc_list	—	Имя отправителя (получателя) письма	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
	bcc_list			
subject	email	—	Тема письма	Строка
references	email	—	Идентификационное поле заголовка references согласно RFC 5322	Строка
reply_to	email	—	Идентификационное поле заголовка in-reply-to согласно RFC 5322	Строка
files	email	Словари с полями: — mime_type — md5 — sha1 — sha256 — size — name	Блок данных о файлах, прикрепленных к письму	Массив
mime_type	files	—	MIME-тип файла	Строка
md5	files	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка
sha1	files	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	files	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
size	files	—	Размер файла в байтах	64-разрядное без- знаковое целое число
name	files	—	Имя файла	Строка
envelope	—	from_address recipients	Блок данных из части Envelope элек- тронного письма	Объект
from_address	envelope	—	Адрес электронной почты отправителя письма	Строка
recipients	envelope	Строки	Блок данных о получателях письма	Массив
received	—	—	UNIX-время формирования задания на проверку	Число с плавающей точкой

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - mail_gateway.start - {  
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",  
  "created": 1511421763.3728465,  
  "entry_point_id": "mail-gateway",  
  "client": {  
    "ip": "203.0.113.33"  
  },  
  "email": {  
    "id": "<6fee62f024e0@example.com>",  
    "from_address": {  
      "address": "ivanov@example.org",  
      "name": "Ivan Ivanov"  
    },  
    "to_list": [ {  
      "address": "username@example.com",  
      "name": "Ivan Ivanov"  
    }  
  ],  
  "subject": "Последняя версия моей программы",  
  "references": "",  
  "reply_to": "",
```

```
"files": [{
  "mime_type": "application/x-dosexec; charset=binary",
  "md5": "11aced0fd6535f6e...1495ba1c7be00",
  "sha1": "45e50e2af429e44...6f59e46b18b60",
  "sha256": "23ef04408bb2c...7928e7caf3d7f",
  "size": 64000,
  "name": "software.exe"
}]
},
"envelope": {
  "from_address": "ivanov@example.org",
  "recipients": ["username@example.com"]
},
"received": 1511421762.957363
}
```

См. также

[Сообщение mail_gateway.finish \(см. раздел Б.1.7.5\)](#)

[Настройка фильтрации почтового трафика \(см. раздел 14.3.3\)](#)

Б.1.1.6. Сообщение files_inbox.start

В таблице ниже описываются поля и объекты в сообщении files_inbox.start о начале обработки задания на проверку файла, обнаруженного в папке-шлюзе.

Таблица 14. Поля в сообщении files_inbox.start

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
scan_id	—	—	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
entry_point_id	—	—	Название источника для проверки в интерфейсе PT Sandbox	Строка
src_file_info	—	url	Блок данных с информацией о файле в папке-шлюзе	Объект
url	src_file_info	—	Путь до файла в папке-шлюзе	Строка
file	—	mime_type md5 sha1 sha256 size name	Блок данных о файле	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
mime_type	file	—	MIME-тип файла	Строка
md5	file	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка
sha1	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	file	—	Размер файла в байтах	64-разрядное беззнаковое целое число
name	file	—	Имя файла	Строка
received	—	—	UNIX-время формирования задания на проверку	Число с плавающей точкой

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - files_inbox.start - {  
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",  
  "created": 1511421763.3728465,  
  "entry_point_id": "gateway-folder",  
  "src_file_info": {  
    "url": "smb://example.org/share/inbox/software.exe"  
  },  
  "file": {  
    "mime_type": "application/x-dosexec; charset=binary",  
    "md5": "11aced0fd6535f6e...1495ba1c7be00",  
    "sha1": "45e50e2af429e44...6f59e46b18b60",  
    "sha256": "23ef04408bb2c...7928e7caf3d7f",  
    "size": 64000,  
    "name": "software.exe"  
  },  
  "received": 1511421762.957363  
}
```

См. также

[Сообщение files_inbox.finish \(см. раздел Б.1.7.6\)](#)

[Настройка проверки файлов в папке-шлюзе \(см. раздел 14.5\)](#)

Б.1.1.7. Сообщение files_monitor.start

В таблице ниже описываются поля и объекты в сообщении files_monitor.start о начале обработки задания на проверку файла, обнаруженного в общей папке.

Таблица 15. Поля в сообщении files_monitor.start

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
scan_id	—	—	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
entry_point_id	—	—	Название источника для проверки в интерфейсе PT Sandbox	Строка
src_file_info	—	url	Блок данных с информацией о файле в общей папке	Объект
url	src_file_info	—	Путь до файла в общей папке	Строка
file	—	mime_type md5 sha1 sha256 size name	Блок данных о файле	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
mime_type	file	—	MIME-тип файла	Строка
md5	file	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка
sha1	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	file	—	Размер файла в байтах	64-разрядное беззнаковое целое число
received	—	—	UNIX-время формирования задания на проверку	Число с плавающей точкой

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - files_monitor.start - {  
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",  
  "created": 1511421763.3728465,  
  "entry_point_id": "shared-folder",  
  "src_file_info": {  
    "url": "smb://example.org/share/software.exe"  
  },  
  "file": {  
    "mime_type": "application/x-dosexec; charset=binary",  
    "md5": "11aced0fd6535f6e...1495ba1c7be00",  
    "sha1": "45e50e2af429e44...6f59e46b18b60",  
    "sha256": "23ef04408bb2c...7928e7caf3d7f",  
    "size": 64000,  
    "name": "software.exe"  
  },  
  "received": 1511421762.957363  
}
```

См. также

[Сообщение files_monitor.finish \(см. раздел Б.1.7.7\)](#)

[Настройка проверки файлов в общей папке \(см. раздел 14.4\)](#)

Б.1.1.8. Сообщение icap.start

В таблице ниже описываются поля и объекты в сообщении `icap.start` о начале обработки задания на проверку контента, полученного по ICAP.

Таблица 16. Поля в сообщении `icap.start`

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
<code>scan_id</code>	—	—	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
<code>created</code>	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
<code>entry_point_id</code>	—	—	Название источника для проверки в интерфейсе PT Sandbox	Строка
<code>request</code>	—	<code>method</code> <code>url</code> <code>version</code> <code>client_ip</code> <code>client_username</code> один из двух объектов: <code>http</code> (в случае HTTP-запроса) или <code>file</code> (в случае файла)	Блок данных о запросе	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
method	request	—	Метод запроса. Возможные значения: "REQMOD" (запрос на изменение HTTP REQUEST) или "RESPMOD" (запрос на изменение HTTP RESPONSE)	Строка
url	request	—	URL ICAP, по которому идет обращение к PT Sandbox	Строка
version	request	—	Версия протокола ICAP-клиента	Строка
client_ip	request	—	IP-адрес пользователя, который получил контент или отправил HTTP-запрос (значение извлекается из поля X-Client-IP заголовка HTTP-запроса)	Строка
client_username	request	—	Имя пользователя, прошедшего аутентификацию на прокси-сервере (значение извлекается из поля X-Client-Username заголовка HTTP-запроса)	Строка
http	request	direction http_request http_response	Блок данных с информацией о файле, относящейся к HTTP	Объект
direction	http	—	Направление сообщения. Возможные значения: "REQUEST" (запрос к удаленному узлу за прокси-сервером) или "RESPONSE" (ответ от удаленного узла за прокси-сервером)	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
http_request	http	method url version files host date referer user_agent content_type content_length content_location content_disposition	Блок данных с информацией об HTTP-запросе. Записывается в случае запроса к удаленному узлу за прокси-сервером, в остальных случаях может отсутствовать или содержать незаполненные поля	Объект
method	http_request	—	Метод HTTP-запроса. Возможные значения: "get" или "post"	Строка
url	http_request	—	URL HTTP-запроса	Строка
version	http_request	—	Версия HTTP	Строка
files	http_request	mime_type md5	Блок данных о файлах, полученных в HTTP-запросе	Массив

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
		sha1 sha256 size name		
mime_type	file	—	MIME-тип файла	Строка
mime_type	files	—	MIME-тип файла	Строка
md5	files	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка
sha1	files	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	files	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	files	—	Размер файла в байтах	64-разрядное беззнаковое целое число
name	files	—	Имя файла	Строка
host	http_request	—	Доменное имя сервера, которому был адресован HTTP-запрос	Строка
date	http_request	—	UNIX-время генерации HTTP-отклика	Число с плавающей точкой

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
referer	http_request	—	Адрес предыдущей веб-страницы, с которой был осуществлен данный HTTP-запрос	Строка
user_agent	http_request	—	Название пользовательского приложения (например, браузера), с которого был осуществлен HTTP-запрос	Строка
content_type	http_request	mime_type charset name boundary	Блок данных с содержимым поля заголовка Content-Type	Объект
mime_type	content_type	—	MIME-тип файла согласно полю Content-Type заголовка HTTP-сообщения	Строка
charset	content_type	—	Кодировка веб-страницы	Строка
name	content_type	—	Значение параметра name в поле Content-Type заголовка HTTP-сообщения	Строка
boundary	content_type	—	Значение параметра boundary в поле Content-Type заголовка HTTP-сообщения	Строка
content_length	http_request	—	Содержимое поля заголовка Content-Length	32-разрядное беззнаковое целое число

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
content_location	http_request	—	Содержимое поля заголовка Content-Location	Строка
content_disposition	http_request	type filename	Блок данных с содержимым поля заголовка Content-Disposition	Объект
type	content_disposition	—	Тип файла согласно полю Content-Disposition заголовка HTTP-сообщения	Строка
filename	content_disposition	—	Имя файла согласно полю Content-Disposition заголовка HTTP-сообщения	Строка
http_response	http	version code reason files	Блок данных с информацией об HTTP-ответе. Записывается только в случае ответа от удаленного узла за прокси-сервером	Объект
version	http_response	—	Версия HTTP	Строка
code	http_response	—	Код ответа	32-разрядное беззнаковое целое число
reason	http_response	—	Описание ответа (Reason-Phrase)	Строка
files	http_response	mime_type md5 sha1	Блок данных о файлах, полученных с HTTP-ответом	Массив

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
		sha256		
mime_type	files	—	MIME-тип файла	Строка
md5	files	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка
sha1	files	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	files	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	files	—	Размер файла в байтах	64-разрядное беззнаковое целое число
name	files	—	Имя файла	Строка
server	http_response	—	Название и версия веб-сервера, от которого был получен HTTP-ответ	Строка
date	http_response	—	UNIX-время генерации HTTP-отклика	Число с плавающей точкой
content_type	http_response	mime_type charset name boundary	Блок данных с содержимым поля заголовка Content-Type	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
mime_type	content_type	—	MIME-тип файла согласно полю Content-Type заголовка HTTP-сообщения	Строка
charset	content_type	—	Кодировка веб-страницы	Строка
name	content_type	—	Значение параметра name в поле Content-Type заголовка HTTP-сообщения	Строка
boundary	content_type	—	Значение параметра boundary в поле Content-Type заголовка HTTP-сообщения	Строка
content_length	http_response	—	Содержимое поля заголовка Content-Length	32-разрядное беззнаковое целое число
content_location	http_response	—	Содержимое поля заголовка Content-Location	Строка
content_disposition	http_response	type filename	Блок данных с содержимым поля заголовка Content-Disposition	Объект
type	content_disposition	—	Тип файла согласно полю Content-Disposition заголовка HTTP-сообщения	Строка
filename	content_disposition	—	Имя файла согласно полю Content-Disposition заголовка HTTP-сообщения	Строка
file	request	mime_type md5	Блок данных о файле	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
		sha1 sha256 size name		
md5	file	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка
sha1	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	file	—	Размер файла в байтах	64-разрядное беззнаковое целое число
name	file	—	Имя файла	Строка
client	—	address port	Блок данных об ICAP-клиенте, который обращается к ICAP-серверу PT Sandbox	Объект
address	client	—	URL ICAP-клиента	Строка
port	client	—	Номер ICAP-порта	32-разрядное беззнаковое целое число

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - icap.start - {  
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",  
  "created": 1511421763.3728465,  
  "entry_point_id": "icap",  
  "request": {  
    "method": "RESPMOD",  
    "url": "icap://198.51.100.12:1344/scan-response",  
    "version": "1.0",  
    "client_ip": "198.51.100.22",  
    "client_username": "",  
    "http": {  
      "direction": "RESPONSE",  
      "http_response": {  
        "version": "1.1",  
        "code": 200,  
        "reason": "OK",  
        "files": [{  
          "mime_type": "",  
          "md5": "9627e80903cbf...77327f6ae1",  
          "sha1": "756569700b98...3c65185a19",  
          "sha256": "b385294dc4...68c3967b64",
```

```
        "size": 9322,  
        "name": "body"  
    }  
},  
"server": "nginx/1.13.4",  
"date": 1511164896.0,  
"content_type": {  
    "mime_type": "image/png",  
    "charset": "",  
    "name": "",  
    "boundary": ""  
},  
"content_length": 9322,  
"content_location": "",  
"content_disposition": {  
    "type": "",  
    "filename": ""  
}  
}
```

```
    }  
  }  
},  
"client": {  
  "address": "198.51.100.13",  
  "port": 55892  
}  
}
```

См. также

[Сообщение icap.finish \(см. раздел Б.1.7.8\)](#)

[Настройка проверки трафика, поступающего от ICAP-сервера \(см. раздел 14.2\)](#)

Б.1.1.9. Сообщение user_scan.start

В таблице ниже описываются поля и объекты в сообщении user_scan.start о начале обработки задания на проверку файлов, отправленных пользователем через веб-интерфейс.

Таблица 17. Поля в сообщении user_scan.start

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
scan_id	—	—	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
user	—	id name login	Блок данных о пользователе, загрузившем файлы в продукт	Объект
id	user	—	Идентификатор пользователя в продукте	32-разрядное беззнаковое целое число
name	user	—	Фамилия, имя и отчество пользователя	Строка
login	user	—	Логин пользователя	Строка
http	—	client_ip user_agent	Блок данных об HTTP-запросе браузера при загрузке файла в продукт	Объект
client_ip	http	—	IP-адрес клиента, с помощью которого был осуществлен запрос	Строка
user_agent	http	—	Название и версия браузера	Строка
files	—	mime_type md5 sha1 sha256 size name	Блок данных о файлах, загруженных пользователем для сканирования	Объект

Поле (объект)	Родительский объект	Вложенные по- ля (объекты)	Описание	Тип данных
mime_type	files	—	MIME-тип файла	Строка
md5	files	—	Хеш-сумма файла, вы- численная по алгоритму MD5	Строка
sha1	files	—	Хеш-сумма файла, вы- численная по алгоритму SHA-1	Строка
sha256	files	—	Хеш-сумма файла, вы- численная по алгоритму SHA-256	Строка
size	files	—	Размер файла в байтах	64-разряд- ное беззна- ковое целое число
name	files	—	Имя файла	Строка
received	—	—	UNIX-время формирова- ния задания на проверку	Число с плавающей точкой

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - user_scan.start - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "user": {
    "id": 534333,
```

```
    "name": "Ivan Ivanov",
    "login": "username"
  },
  "http": {
    "client_ip": "192.0.2.32",
    "user_agent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
    Gecko) Chrome/51.0.2704.103 Safari/537.36"
  },
  "files": [
    {
      "mime_type": "application/x-dosexec; charset=binary",
      "md5": "11aced0fd6535f6e...1495ba1c7be00",
      "sha1": "45e50e2af429e44...6f59e46b18b60",
      "sha256": "23ef04408bb2c...7928e7caf3d7f",
      "size": 64000,
      "name": "software.exe"
    }
  ],
  "received": 1511421762.957363
}
```

Б.1.2. Сообщение new_artifact

В таблице ниже описываются поля и объекты в сообщении new_artifact об обнаружении файла в задании на проверку, в архиве или письме.

Таблица 18. Поля в сообщении new_artifact

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
scan_id	—	—	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
new_artifact	—	file	Блок данных о файле, поступившем на проверку	Объект
parent	—	file	Блок данных о родительском файле, например письме или архиве, из которого был извлечен файл, поступивший на проверку	Объект
file	new_artifact или parent	mime_type md5 sha1 sha256 size name	Блок данных о файле	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
mime_type	file	—	MIME-тип файла (не заполняется)	Строка
md5	file	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка
sha1	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	file	—	Размер файла в байтах	64-разрядное беззнаковое целое число
name	file	—	Имя файла	Строка

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - new_artifact - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "new_artifact": {
    "file": {
      "mime_type": "",
      "md5": "11aced0fd6535f6e...1495ba1c7be00",
      "sha1": "45e50e2af429e44...6f59e46b18b60",
      "sha256": "23ef04408bb2c...7928e7caf3d7f",
```

```
    "size": 64000,  
    "name": "software.exe"  
  }  
}  
}
```

Б.1.3. Сообщение scan_machine.new_object

В таблице ниже описываются поля и объекты в сообщении scan_machine.new_object с результатами извлечения файлов из архива или письма, поступившего на проверку.

Таблица 19. Поля в сообщении scan_machine.new_object

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
scan_id	—	—	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
origin_file	—	mime_type md5 sha1 sha256 size	Блок данных о файле, из которого были извлечены файлы	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
mime_type	origin_file	—	MIME-тип файла	Строка
md5	origin_file	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка
sha1	origin_file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	origin_file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	origin_file	—	Размер файла в байтах	64-разрядное беззнаковое целое число
recognized_object	—	Один из объектов: file, email, archive или compressed_file	Блок данных об извлеченных файлах	Объект
file	recognized_object	mime_type md5 sha1 sha256 size	Блок данных о файле	Объект
mime_type	file	—	MIME-тип файла	Строка
md5	file	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
sha1	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	file	—	Размер файла в байтах	64-разрядное беззнаковое целое число
email	recognized_object	id from_address to_list cc_list bcc_list subject references reply_to files	Блок данных о письме	Объект
id	email	—	Поле заголовка Message-ID	Строка
from_address	email	address name	Блок данных об отправителе письма	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
to_list	email	Словари с полями address и name	Блок данных о получателях письма	Массив
cc_list	email	Словари с полями address и name	Блок данных о получателях копии письма	Массив
bcc_list	email	Словари с полями address и name	Блок данных о получателях скрытой копии письма	Массив
address	from_address to_list cc_list bcc_list	—	Адрес электронной почты	Строка
name	from_address to_list cc_list bcc_list	—	Имя отправителя (получателя) письма	Строка
subject	email	—	Тема письма	Строка
references	email	—	Идентификационное поле заголовка references согласно RFC 5322	Строка
reply_to	email	—	Идентификационное поле заголовка in-reply-to согласно RFC 5322	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
files	email	Словари с полями: — mime_type — md5 — sha1 — sha256 — size — name	Блок данных о файлах, прикрепленных к письму	Массив
archive	recognized_object	mime_type files	Блок данных об архиве	Объект
mime_type	archive	—	MIME-тип архива	Строка
files	archive	mime_type md5 sha1 sha256 size name relative_path	Массив данных о файлах в архиве	Массив
mime_type	files	—	MIME-тип файла	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
md5	files	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка
sha1	files	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	files	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	files	—	Размер файла в байтах	64-разрядное беззнаковое целое число
name	files	—	Имя файла	Строка
relative_path	files	—	Относительный путь к файлу в архиве	Строка
compressed_file	recognized_object	mime_type file	Блок данных о сжатом файле	Объект
mime_type	compressed_file	—	MIME-тип сжатого файла	Строка
file	compressed_file	mime_type md5 sha1 sha256 size	Блок данных о файле, который был сжат	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
		name		
md5	file	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка
sha1	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	file	—	Размер файла в байтах	64-разрядное беззнаковое целое число
name	file	—	Имя файла	Строка

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - scan_machine.new_object - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "origin_file": {
    "mime_type": "",
    "md5": "b53173def106ad...0ea30e504ec860f",
    "sha1": "c73c71d7858b7...de0272ce1125e01",
```



```
"sha256": "d523708fe3b...e8f9a41b25f3c8d",
"size": 792
},
"recognized_object": {
  "archive": {
    "mime_type": "application/zip; charset=binary",
    "files": [{
      "mime_type": "text/plain; charset=us-ascii",
      "md5": "44d88612fea8a...6de82e1278abb02f",
      "sha1": "3395856ce81f...02f798b642f14140",
      "sha256": "275a021bbf...c4538aabf651fd0f",
      "size": 68,
      "name": "eicar.com",
      "relative_path": "test/eicar.com"
    }, {
      "mime_type": "text/plain; charset=us-ascii",
      "md5": "eb733a00c0c9...6e65691a37ab54293",
      "sha1": "f48dd853820...d0f584dc863327a7c",
      "sha256": "916f0027a...92da1a577bf2335f9",
      "size": 9,
      "name": "file_name",
      "relative_path": "test/file_name"
```

```
    }, {  
      "mime_type": "text/plain; charset=us-ascii",  
      "md5": "eb733a00c0c9...6e65691a37ab54293",  
      "sha1": "f48dd853820...d0f584dc863327a7c",  
      "sha256": "916f0027a...92da1a577bf2335f9",  
      "size": 9,  
      "name": "another_file_name",  
      "relative_path": "test/another_file_name"  
    }  
  }  
}  
}
```

Б.1.4. Сообщение scan_machine.file_result.av

В таблице ниже описываются поля и объекты в сообщении scan_machine.file_result.av с результатом сканирования файла или письма конкретным антивирусом.

Таблица 20. Поля в сообщении scan_machine.file_result.av

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
scan_id	—	—	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
created	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
file	—	mime_type md5 sha1 sha256 size	Блок данных о файле	Объект
mime_type	file	—	MIME-тип файла	Строка
md5	file	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка
sha1	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	file	—	Размер файла в байтах	64-разрядное беззнаковое целое число
av_code_name	—	—	Кодовое имя антивируса (см. раздел Б.5) , который сканировал файл	Строка
engine_version	—	—	Версия антивируса, который сканировал файл	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
database_time	—	—	UNIX-время последнего обновления баз антивируса, который сканировал файл	Число с плавающей точкой
duration	—	—	Продолжительность сканирования файла антивирусом в секундах	Число с плавающей точкой
result	—	verdict errors state raw_detections	Блок данных с результатом сканирования, ошибками сканирования и состоянием сканирования	Объект
verdict	result	threat_level threat accuracy	Блок данных с результатом сканирования	Объект
threat_level	verdict	—	<p>Результат сканирования. Возможные значения:</p> <ul style="list-style-type: none"> — "UNKNOWN" — результат сканирования неизвестен; — "CLEAN" — файл без обнаруженных угроз; — "UNWANTED" — потенциально опасный файл; — "DANGEROUS" — опасный файл 	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
threat	verdict	classification family	Информация об обнаруженной угрозе	Объект
classification	threat	—	Тип обнаруженной угрозы. Если угроза не была обнаружена, в это поле записывается "UNKNOWN"	Строка
family	threat	—	Семейство, к которому принадлежит обнаруженный вирус	Строка
accuracy	verdict	—	Точность результата сканирования	Число с плавающей точкой
errors	result	internal corrupted encrypted max_depth_exceeded	Блок данных с информацией об ошибках сканирования	Объект
internal	errors	—	Внутренняя ошибка при сканировании	Логический
corrupted	errors	—	Файл поврежден	Логический
encrypted	errors	—	Файл зашифрован паролем, который неизвестен продукту	Логический
max_depth_exceeded	errors	—	Превышен максимально допустимый уровень вложенности архивов в архивы	Логический

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
state	result	—	Состояние сканирования. Возможные значения: <ul style="list-style-type: none"> — "UNSCANNED" — файл не был сканирован из-за ошибки; — "PARTIAL" — файл был сканирован частично; — "FULL" — файл был сканирован полностью 	Строка
raw_detections	result	—	Необработанный результат сканирования (в исходном виде, полученном от антивируса)	Массив

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - scan_machine.file_result.av - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "file": {
    "mime_type": "application/x-dosexec; charset=binary",
    "md5": "11aced0fd6535f6e...1495ba1c7be00",
    "sha1": "45e50e2af429e44...6f59e46b18b60",
```

```
"sha256": "Хеш-сумма файла, вычисленная по алгоритму SHA-256",  
"size": 64000  
},  
"av_code_name": "clamav",  
"engine_version": "0.99.2",  
"database_time": 1510892498.0,  
"duration": 0.1300000,  
"result": {  
  "verdict": {  
    "threat_level": "CLEAN",  
    "threat": {  
      "classification": "UNKNOWN",  
      "family": ""  
    },  
    "accuracy": 1.0  
  },  
  "errors": {  
    "internal": false,  
    "corrupted": false,
```

```
    "encrypted": false,
    "max_depth_exceeded": false
  },
  "state": "FULL",
  "raw_detections": []
}
```

Б.1.5. Сообщение scan_machine.file_result.melded

В таблице ниже описываются поля и объекты в сообщении scan_machine.file_result.melded с результатами сканирования файла или письма всеми антивирусами.

Таблица 21. Поля в сообщении scan_machine.file_result.melded

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
scan_id	—	—	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
file	—	mime_type md5 sha1	Блок данных о файле	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
		sha256 size		
mime_type	file	—	MIME-тип файла	Строка
md5	file	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка
sha1	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	file	—	Размер файла в байтах	64-разрядное беззнаковое целое число
result	—	verdict errors state	Блок данных с итоговым результатом сканирования файла, ошибками сканирования и состоянием сканирования	Объект
verdict	result	threat_level threat accuracy	Блок данных с результатом сканирования	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
threat_level	verdict	—	Результат сканирования. Возможные значения: — "UNKNOWN" — результат сканирования неизвестен; — "CLEAN" — файл без обнаруженных угроз; — "UNWANTED" — потенциально опасный файл; — "DANGEROUS" — опасный файл	Строка
threat	verdict	classification family	Информация об обнаруженной угрозе	Объект
classification	threat	—	Тип обнаруженной угрозы. Если угроза не была обнаружена, в это поле записывается "UNKNOWN"	Строка
family	threat	—	Семейство, к которому принадлежит обнаруженный вирус	Строка
accuracy	verdict	—	Точность результата сканирования	Число с плавающей точкой
errors	result	internal corrupted encrypted	Блок данных с информацией об ошибках сканирования	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
		max_depth_exceeded		
internal	errors	—	Внутренняя ошибка при сканировании	Логический
corrupted	errors	—	Файл поврежден	Логический
encrypted	errors	—	Файл зашифрован паролем, который неизвестен продукту	Логический
max_depth_exceeded	errors	—	Превышен максимально допустимый уровень вложенности архивов в архивы	Логический
state	result	—	Состояние сканирования. Возможные значения: <ul style="list-style-type: none"> — "UNSCANNED" — файл не был сканирован из-за ошибки; — "PARTIAL" — файл был сканирован частично; — "FULL" — файл был сканирован полностью 	Строка

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - scan_machine.file_result.melded - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "file": {
    "mime_type": "application/x-dosexec; charset=binary",
    "md5": "11aced0fd6535f6e...1495ba1c7be00",
    "sha1": "45e50e2af429e44...6f59e46b18b60",
    "sha256": "23ef04408bb2c...7928e7caf3d7f",
    "size": 64000
  },
  "result": {
    "verdict": {
      "threat_level": "CLEAN",
      "threat": {
        "classification": "UNKNOWN",
        "family": ""
      },
    },
    "accuracy": 1.0
  },
  "errors": {
    "internal": false,
```

```
    "corrupted": false,
    "encrypted": false,
    "max_depth_exceeded": false
  },
  "state": "FULL"
}
```

Б.1.6. Сообщение scan_machine.final_result

В таблице ниже описываются поля и объекты в сообщении scan_machine.final_result с итоговым результатом сканирования всех файлов задания всеми антивирусами.

Таблица 22. Поля в сообщении scan_machine.final_result

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
scan_id	—	—	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
result	—	verdict errors state	Блок данных с итоговым результатом сканирования файлов задания, ошибками сканирования и состоянием сканирования	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
verdict	result	threat_level threat accuracy	Блок данных с результатом сканирования	Объект
threat_level	verdict	—	Результат сканирования задания. Возможные значения: — "UNKNOWN" — результат сканирования неизвестен; — "CLEAN" — в файлах задания угроз не обнаружено; — "UNWANTED" — задание содержит потенциально опасные файлы; — "DANGEROUS" — задание содержит опасные файлы	Строка
threat	verdict	classification family	Блок с информацией об обнаруженной угрозе в задании. Если в задании было обнаружено несколько угроз, в это поле записывается самая опасная из них	Объект
classification	threat	—	Тип обнаруженной угрозы. Если угроза не была обнаружена, в это поле записывается "UNKNOWN"	Строка
family	threat	—	Семейство, к которому принадлежит обнаруженный вирус	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
accuracy	verdict	—	Точность результата сканирования	Число с плавающей точкой
errors	result	internal corrupted encrypted max_depth_exceeded	Блок данных с информацией об ошибках сканирования	Объект
internal	errors	—	Внутренняя ошибка при сканировании	Логический
corrupted	errors	—	В задании есть поврежденные файлы	Логический
encrypted	errors	—	В задании есть файлы, зашифрованные паролем, который неизвестен продукту	Логический
max_depth_exceeded	errors	—	При обработке файлов задания был превышен максимально допустимый уровень вложенности архивов в архивы	Логический
state	result	—	Состояние сканирования файлов задания. Возможные значения: <ul style="list-style-type: none"> — "UNSCANNED" — файлы задания не были сканированы из-за ошибки; — "PARTIAL" — были сканированы только некоторые файлы в задании; — "FULL" — все файлы в задании были сканированы полностью 	Строка

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - scan_machine.final_result - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "result": {
    "verdict": {
      "threat_level": "CLEAN",
      "threat": {
        "classification": "UNKNOWN",
        "family": ""
      },
      "accuracy": 1.0
    },
    "errors": {
      "internal": false,
      "corrupted": false,
      "encrypted": false,
      "max_depth_exceeded": false
    },
    "state": "FULL"
  }
}
```


Б.1.7. Сообщения <Идентификатор типа источника для проверки>.finish

Сообщение с типом <Идентификатор типа источника для проверки>.finish (например, email.finish) информирует об окончании обработки задания на проверку и содержит уникальный идентификатор задания, признак успешности обработки задания.

В этом разделе

[Сообщение check_me.finish \(см. раздел Б.1.7.1\)](#)

[Сообщение dpi.finish \(см. раздел Б.1.7.2\)](#)

[Сообщение email.finish \(см. раздел Б.1.7.3\)](#)

[Сообщение mail_bcc.finish \(см. раздел Б.1.7.4\)](#)

[Сообщение mail_gateway.finish \(см. раздел Б.1.7.5\)](#)

[Сообщение files_inbox.finish \(см. раздел Б.1.7.6\)](#)

[Сообщение files_monitor.finish \(см. раздел Б.1.7.7\)](#)

[Сообщение icap.finish \(см. раздел Б.1.7.8\)](#)

См. также

[Идентификаторы типов источников для проверки \(см. раздел Б.1.8\)](#)

Б.1.7.1. Сообщение check_me.finish

В таблице ниже описываются поля в сообщении типа check_me.finish о завершении обработки задания на проверку файлов, полученных службой Checkme.

Таблица 23. Поля в сообщении check_me.finish

Поле	Описание	Тип данных
scan_id	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	UNIX-время генерации сообщения	Число с плавающей точкой
status	Признак успешности обработки задания на проверку. Возможные значения: "SUCCESS" (задание обработано успешно) или "FAIL" (обработка задания завершилась с ошибкой)	Строка

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - check_me.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS"
}
```

См. также

- [Сообщение check_me.start \(см. раздел Б.1.1.1\)](#)
- [Создание и настройка службы Checkme \(см. раздел 14.1\)](#)

Б.1.7.2. Сообщение dpi.finish

В таблице ниже описываются поля в сообщении типа dpi.finish о завершении обработки задания на проверку файла, полученного от модуля захвата трафика или PT NAD.

Таблица 24. Поля в сообщении dpi.finish

Поле	Описание	Тип данных
scan_id	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	UNIX-время генерации сообщения	Число с плавающей точкой
status	Признак успешности обработки задания на проверку. Возможные значения: "SUCCESS" (задание обработано успешно) или "FAIL" (обработка задания завершилась с ошибкой)	Строка

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - dpi.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS"
}
```

См. также

- [Сообщение dpi.start \(см. раздел Б.1.1.2\)](#)
- [Настройка проверки трафика организации при помощи модуля захвата трафика \(см. раздел 14.6\)](#)

Б.1.7.3. Сообщение email.finish

В таблице ниже описываются поля в сообщении типа `email.finish` о завершении обработки задания на проверку файлов, полученных почтовым агентом.

Таблица 25. Поля в сообщении email.finish

Поле	Описание	Тип данных
scan_id	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	UNIX-время генерации сообщения	Число с плавающей точкой
action	<p>Действие, которое PT Sandbox выполнил с письмом, обработанным в задании. Возможные значения:</p> <ul style="list-style-type: none"> — "UNKNOWN" — действие неизвестно; — "PASS" — письмо пропущено в информационную систему вместе с вложениями; — "BLOCK" — распространение письма было заблокировано; — "MODIFY" — письмо было пропущено в информационную систему с удалением файлов, представляющих угрозу 	Строка

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - email.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "action": "BLOCK"
}
```

См. также

[Сообщение email.start \(см. раздел Б.1.1.3\)](#)

[Подключение к почтовому серверу при помощи агента \(см. раздел 14.3.1\)](#)

Б.1.7.4. Сообщение mail_bcc.finish

В таблице ниже описываются поля в сообщении типа `mail_bcc.finish` о завершении обработки задания на проверку письма, полученного от почтового сервера организации в виде скрытой копии.

Таблица 26. Поля в сообщении mail_bcc.finish

Поле	Описание	Тип данных
scan_id	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	UNIX-время генерации сообщения	Число с плавающей точкой
status	Признак успешности обработки задания на проверку. Возможные значения: "SUCCESS" (задание обработано успешно) или "FAIL" (обработка задания завершилась с ошибкой)	Строка

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - mail_bcc.finish - {  
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",  
  "created": 1511421763.3728465,  
  "status": "SUCCESS"  
}
```

См. также

[Сообщение mail_bcc.start \(см. раздел Б.1.1.4\)](#)

[Настройка зеркалирования почтового трафика с помощью bcc \(см. раздел 14.3.2\)](#)

Б.1.7.5. Сообщение mail_gateway.finish

В таблице ниже описываются поля в сообщении mail_gateway.finish о завершении обработки задания на проверку письма, полученного от почтового сервера Postfix или Exim в режиме фильтрации.

Таблица 27. Поля в сообщении mail_gateway.finish

Поле	Описание	Тип данных
scan_id	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	UNIX-время генерации сообщения	Число с плавающей точкой
status	Признак успешности обработки задания на проверку. Возможные значения: "SUCCESS" (задание обработано успешно) или "FAIL" (обработка задания завершилась с ошибкой)	Строка

Поле	Описание	Тип данных
action	<p>Действие, которое PT Sandbox выполнил с письмом, обработанным в задании. Возможные значения:</p> <ul style="list-style-type: none"> — "PASS" — письмо пропущено в информационную систему вместе с вложениями; — "BLOCK" — распространение письма было заблокировано; — "MODIFY" — письмо было пропущено в информационную систему с удалением файлов, представляющих угрозу 	Строка

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - mail_gateway.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS",
  "action": "BLOCK"
}
```

См. также

[Сообщение mail_gateway.start \(см. раздел Б.1.1.5\)](#)

[Настройка фильтрации почтового трафика \(см. раздел 14.3.3\)](#)

Б.1.7.6. Сообщение files_inbox.finish

В таблице ниже описываются поля и объекты в сообщении типа files_inbox.finish о завершении обработки задания на проверку файла, обнаруженного в папке-шлюзе.

Таблица 28. Поля в сообщении files_inbox.finish

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
scan_id	—	—	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
created	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
status	—	—	Признак успешности обработки задания на проверку. Возможные значения:	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
			ния: "SUCCESS" (задание обработано успешно) или "FAIL" (обработка задания завершилась с ошибкой)	
action	—	—	Общая папка, в которую PT Sandbox переместил файл по результатам проверки. Возможные значения: — "NOTHING" — файл не был перемещен из папки-шлюза; — "DESTINATION" — файл был перемещен в папку для безопасных файлов; — "QUARANTINE" — файл был перемещен в папку карантина	Строка
dst_file_info	—	url	Блок данных о перемещенном файле	Объект
url	dst_file_info	—	Путь к перемещенному файлу в папке для безопасных файлов или в папке карантина	Строка

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - files_inbox.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS"
  "action": "DESTINATION",
  "dst_file_info": {
    "url": "smb://host/share/safe/software.exe"
  }
}
```

См. также

[Сообщение files_inbox.start \(см. раздел Б.1.1.6\)](#)

[Настройка проверки файлов в папке-шлюзе \(см. раздел 14.5\)](#)

Б.1.7.7. Сообщение files_monitor.finish

В таблице ниже описываются поля в сообщении типа `files_monitor.finish` о завершении обработки задания на проверку файла, обнаруженного в общей папке.

Таблица 29. Поля в сообщении `files_monitor.finish`

Поле	Описание	Тип данных
<code>scan_id</code>	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
<code>created</code>	UNIX-время генерации сообщения	Число с плавающей точкой
<code>status</code>	Признак успешности обработки задания на проверку. Возможные значения: "SUCCESS" (задание обработано успешно) или "FAIL" (обработка задания завершилась с ошибкой)	Строка

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - files_monitor.finish - {  
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",  
  "created": 1511421763.3728465,  
  "status": "SUCCESS"  
}
```

См. также

[Сообщение files_monitor.start \(см. раздел Б.1.1.7\)](#)

[Настройка проверки файлов в общей папке \(см. раздел 14.4\)](#)

Б.1.7.8. Сообщение icap.finish

В таблице ниже описываются поля в сообщении типа `icap.finish` о завершении обработки задания на проверку контента, полученного от ICAP-сервера PT Sandbox.

Таблица 30. Поля в сообщении `icap.finish`

Поле	Описание	Тип данных
<code>scan_id</code>	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка

Поле	Описание	Тип данных
created	UNIX-время генерации сообщения	Число с плавающей точкой
action	<p>Действие, которое PT Sandbox выполнил с контентом, обработанным в задании. Возможные значения:</p> <ul style="list-style-type: none"> — "UNKNOWN" — действие неизвестно; — "PASS" — контент пропущен в информационную систему; — "BLOCK" — распространение контента было заблокировано; — "MODIFY" — контент пропущен в информационную систему с указанием типа обнаруженной угрозы в поле X-Virus-ID ответного запроса 	Строка

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - icap.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "action": "BLOCK"
}
```

См. также

[Сообщение icap.start \(см. раздел Б.1.1.8\)](#)

[Настройка проверки трафика, поступающего от ICAP-сервера \(см. раздел 14.2\)](#)

Б.1.8. Идентификаторы типов источников для проверки

Идентификаторами типа источника для проверки могут быть:

- check_me — служба Checkme;
- dpi — модуль захвата трафика или PT NAD;
- email — Microsoft Exchange Server с установленным почтовым агентом PT Sandbox;
- file_inbox — папка-шлюз;
- files_monitor — общая папка;
- icap — ICAP-сервер;
- mail-bcc — почтовый сервер организации, отправляющий скрытые копии писем в PT Sandbox;

- `mail-gateway` — почтовый сервер Postfix или Exim, отправляющий письма на фильтрацию в PT Sandbox;
- `user_scan` — веб-интерфейс.

См. также

[Источники файлов и электронных писем, передаваемых на проверку \(см. раздел 4.2\)](#)

Б.2. Сообщение `av.update`

В таблице ниже описываются поля в сообщении `av.update`, которое формируется при обновлении антивируса и (или) его базы.

Таблица 31. Поля в сообщении `av.update`

Поле	Описание	Тип данных
<code>created</code>	UNIX-время формирования сообщения	Число с плавающей точкой
<code>av_code_name</code>	Кодовое имя антивируса (см. раздел Б.5)	Строка
<code>engine_version</code>	Версия антивируса	Строка
<code>database_time</code>	UNIX-время выпуска антивирусной базы	Число с плавающей точкой

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - av.update - {  
  "created": 1520866088.3110101,  
  "av_code_name": "bitdefender",  
  "engine_version": "11.0.1.18",  
  "database_time": 1520862339.0  
}
```

Б.3. Сообщение retro_scan.start

При создании задания на повторное сканирование PT Sandbox отправляет в системный журнал сообщение типа `retro_scan.start`. Это сообщение информирует о начале обработки файла из задания и содержит уникальный идентификатор задания и информацию о файле в нем.

В таблице ниже описываются поля и объекты в сообщении `retro_scan.start`.

Таблица 32. Поля в сообщении `retro_scan.start`

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
<code>scan_id</code>	—	—	Хеш-сумма задания на проверку, вычисленная по алгоритму продукта	Строка
<code>created</code>	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
<code>file</code>	—	<code>mime_type</code> <code>md5</code> <code>sha1</code> <code>sha256</code> <code>size</code> <code>name</code>	Блок данных о файле	Объект
<code>mime_type</code>	<code>file</code>	—	MIME-тип файла	Строка
<code>md5</code>	<code>file</code>	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
sha1	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	file	—	Размер файла в байтах	64-разрядное беззнаковое целое число
name	file	—	Имя файла	Строка
received	—	—	UNIX-время формирования задания на проверку	Число с плавающей точкой

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - retro_scan.start - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "file": {
    "mime_type": "application/x-dosexec; charset=binary",
    "md5": "11aced0fd6535f6e...1495ba1c7be00",
    "sha1": "45e50e2af429e44...6f59e46b18b60",
    "sha256": "23ef04408bb2c...7928e7caf3d7f",
```

```
"size": 64000,  
"name": "software.exe"  
},  
"received": 1511421762.957363  
}
```

Б.4. Сообщение retro.artifact_verdict_changed

Если результат повторного сканирования оказался отличным от предыдущего результата сканирования, PT Sandbox отправляет в системный журнал сообщение с типом retro.artifact_verdict_changed. Это сообщение содержит информацию о файле, его прошлый и последний результаты сканирования.

В таблице ниже описываются поля и объекты в сообщении retro.artifact_verdict_changed.

Таблица 33. Поля в сообщении retro.artifact_verdict_changed

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
created	—	—	UNIX-время генерации сообщения	Число с плавающей точкой
file	—	mime_type md5 sha1 sha256 size	Блок данных о файле	Объект

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
		name		
mime_type	file	—	MIME-тип файла	Строка
md5	file	—	Хеш-сумма файла, вычисленная по алгоритму MD5	Строка
sha1	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-1	Строка
sha256	file	—	Хеш-сумма файла, вычисленная по алгоритму SHA-256	Строка
size	file	—	Размер файла в байтах	64-разрядное без- знаковое целое число
name	file	—	Имя файла	Строка
old_verdict	—	threat_level threat	Блок данных с информацией о предыдущем сканировании	Объект
verdict	—	threat_level threat	Блок данных с информацией о последнем повторном сканировании	Объект
threat_level	old_verdict и verdict	—	Результат сканирования. Возможные значения: — "UNKNOWN" — результат сканирования неизвестен; — "CLEAN" — файл без обнаруженных угроз; — "UNWANTED" — потенциально опасный файл; — "DANGEROUS" — опасный файл	Строка

Поле (объект)	Родительский объект	Вложенные поля (объекты)	Описание	Тип данных
threat	old_verdict и verdict	classification	Информация об обнаруженной угрозе	Объект
classification	threat	—	Тип обнаруженной угрозы. Если угроза не была обнаружена, в это поле записывается "UNKNOWN"	Строка

Пример сообщения:

```
<100>1 2017-11-23T07:22:44.018041Z host1-example sandbox - retro.artifact_verdict_changed - {
  "created": 1511264056.5231795,
  "file": {
    "mime_type": "application/x-dosexec; charset=binary",
    "md5": "11aced0fd6535f6e...1495ba1c7be00",
    "sha1": "45e50e2af429e44...6f59e46b18b60",
    "sha256": "23ef04408bb2c...7928e7caf3d7f",
    "size": 64000,
    "name": "software.exe"
  },
  "old_verdict": {
    "threat_level": "CLEAN",
    "threat": {
```

```
    "classification": "UNKNOWN"
  },
  "verdict": {
    "threat_level": "DANGEROUS",
    "threat": {
      "classification": "VIRUS"
    }
  }
}
```

Б.5. Кодовые имена антивирусов

В таблице ниже приводится список кодовых имен антивирусов. Кодовое имя используется для обозначения антивируса в сообщениях `av.update` и `scan_machine.file_result.av`.

Таблица 34. Кодовые имена антивирусов

Антивирус	Кодовое имя
Avira	avira
Bitdefender	bitdefender
ClamAV	clamav
ESET	eset
Kaspersky for Proxy Server	kaspersky
Avast Core Security	avast
Symantec Protection Engine for Network Attached Storage	symantec
Dr.Web Server Security Suite	drweb

См. также

[Просмотр сведений об антивирусах \(см. раздел 19.1\)](#)

Предметный указатель

В

bcc 101

I

ICAP

настройка клиента 93

настройка сервера 92

P

PT IAM 79

вход 65

запись в журнал аудита 137

назначение 65

переход из PT Sandbox 130

PT Sandbox 10

S

Squid 96

SSL-сертификат 16

SSO

см. PT IAM 65

syslog

см. системный журнал 141

A

администратор 66

антивирусное сканирование 13

антивирусные базы 132

антивирусы

дополнительные 132, 133, 134, 135

основные 132

просмотр сведений 84

архивы

вложенные в архивы 16

зашифрованные паролями 16

поддерживаемые форматы 16

В

вход в PT Sandbox 79

Д

диагностика 145

дополнительный антивирус

включение 133

выключение 133

обновление 135

обновление лицензии 134

просмотр сведений 132

удаление 135

установка 133

дополнительный узел 24

добавление 142

отключение 142

установка 43

Е

единый вход	
см. PT IAM	65

И

интеграция с продуктами PT	
PT AF	91, 94
PT NAD	118
интерфейс PT Sandbox	
главное меню	80
страница с информацией об антивирусах	84
страница с информацией об образах виртуальных машин	82
Центр уведомлений	81
источники для проверки	
ICAP-сервер	14, 92
PT NAD	14, 118
веб-интерфейс	13
добавление	89
изменение параметров	120
модуль захвата трафика	14, 117
общая папка	14, 113
отключение	120
папка-шлюз	14, 114
почтовый сервер	13, 97
служба Checkme	13, 89
удаление	121

К

карантин	139
----------	-----

компоненты PT Sandbox	16
API базы данных	16
база данных	16
веб-интерфейс	16
модуль поведенческого анализа	17
служба высокой доступности	16, 39, 42, 58, 61
хранилище файлов	17
ядро проверки	17

конфигурация PT Sandbox

многосерверная	24, 142
односерверная	24

Л

лицензия	22
активация	67
замена	87
просмотр	86
льготный период	22

М

методы проверки	
поведенческий анализ	13
статический анализ	13

О

образы виртуальных машин	82
основной антивирус	
включение	133
выключение	133
просмотр сведений	132
основной узел	24

отключение поведенческого анализа	143
установка	26, 35
отказоустойчивость	17

П

почтовый агент	
удаление	144
установка	98, 99
почтовый сервер	
Exim	103, 110
Microsoft Exchange	98, 104
Postfix	103, 109
права доступа	130
принцип работы PT Sandbox	12
проверка	
архива, зашифрованного паролем	16, 124
файлов по электронной почте	124
проверка файлов	
методы	12
режимы	14
результаты	126

Р

режимы проверки	
блокирующий	14, 93, 98
ожидания	15, 94
пассивный	15, 95
резервное копирование и восстановление	63

результаты проверки	
просмотр	126
роли пользователей	130

С

серийный номер	22, 67
системный журнал	141
суперпользователь	
назначение	65
смена пароля	66

У

установка	24
устранение неисправностей	145

Ф

файлы журналов	148
----------------	-----

Х

хранилище файлов	138
------------------	-----

Э

экспертная оценка	13
-------------------	----

Глоссарий

Всс-сервер

Компонент продукта, на который отправляются скрытые копии писем с почтового сервера организации.

ICAP-сервер

Компонент продукта, обеспечивающий взаимодействие системы с PT AF или другими программами, работающими по ICAP.

вредоносное ПО

Программное обеспечение, которое разрабатывается для получения несанкционированного доступа к вычислительным ресурсам компьютера или к информации, которая на нем хранятся. Такие программы предназначены для несанкционированного использования ресурсов компьютера или нанесения ущерба владельцу информации или компьютера путем копирования, искажения, удаления или подмены информации.

дополнительный антивирус

Антивирус, самостоятельно устанавливаемый администратором в дополнение к антивирусам из основного набора.

дополнительный узел

Физический сервер или виртуальная машина с установленным продуктом, на которых выполняется только поведенческий анализ, или которые используются для обеспечения отказоустойчивости продукта.

источник для проверки

Интерфейс в информационной системе организации, с которого продукт получает файлы и (или) электронные письма для проверки.

карантин

Функция временного удержания в хранилище файлов тех электронных писем, которые по результатам проверки представляют угрозу информационной безопасности.

многосерверная конфигурация

Вариант установки продукта, при котором продукт устанавливается на несколько узлов, которыми могут быть физические сервера или виртуальные машины.

модуль захвата трафика

Компонент системы, отвечающий за захват сетевого корпоративного трафика.

общая папка

Папка в информационной системе организации с общим сетевым доступом, настроенным с помощью протокола SMB или NFS.

односерверная конфигурация

Вариант установки, при котором продукт устанавливается на единственный узел, которым может быть физический сервер или виртуальная машина.

основной антивирус

Антивирус, входящий в комплект поставки продукта.

основной узел

Физический сервер или виртуальная машина с продуктом, который был установлен первым из всех узлов кластера.

папка карантина

Общая папка, в которую из папки-шлюза перемещаются файлы, представляющие угрозу.

папка-шлюз

Общая папка с файлами для проверки. В зависимости от результатов проверки файлы перемещаются из папки-шлюза либо в папку для безопасных файлов, либо в папку карантина.

почтовый агент

Компонент продукта, который используется для интеграции продукта с Microsoft Exchange и позволяет операторам безопасности настраивать блокировку писем, представляющих угрозу безопасности.

проверка

Поиск угроз в файле, письме или веб-контенте с использованием методов статического и поведенческого анализа.

режим зеркалирования

Режим работы почтового сервера организации, при котором на проверку отправляются копии писем.

режим фильтрации

Режим интеграции продукта с почтовым сервером Postfix или Exim организации, при котором почтовый сервер отправляет письма на проверку согласно правилам маршрутизации, настроенным администратором. В зависимости от режима проверки трафика продукт возвращает письма почтовому серверу сразу или задерживает их до получения результатов проверки.

результат проверки

Тип самого опасного программного обеспечения, обнаруженного в файле или электронном письме.

хранилище файлов

Компонент продукта, отвечающий за хранение полученных извне файлов на жестком диске.

О компании

"Позитив Текнолоджиз" уже 19 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявить, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга "Эксперт-400".