Sandbox версия 5.7

Руководство администратора

Дата редакции документа: 18.01.2024

Содержание

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 специалиста по безопасности — содержит сценарии использования продукта для управления событиями информационной безопасности.

— Руководство пользователя — содержит инструкции по отправке файлов на проверку через интерфейс продукта или по электронной почте и просмотру результатов проверки.

— Руководство разработчика — содержит информацию для интеграции PT Sandbox со сторонними системами.

В этом разделе

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите кнопку **OK**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом

Пример	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 портале технической поддержки.

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, 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 30).

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 специалисты по 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;

— 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.

— проверять ссылки, ведущие на файлы;

— просматривать результаты проверки файлов.

3. Что нового в версии 5.7

Ниже приводится список изменений, которые появились в PT Sandbox.

Уведомления о прекращении технической поддержки PT Sandbox

Теперь за месяц до прекращения технической поддержки установленной у вас версии PT Sandbox будет появляться системное уведомление о планируемом прекращении поддержки. Если у вас установлена версия PT Sandbox, для которой техническая поддержка уже прекращена, соответствующее системное уведомление будет также показано.

> **Примечание.** Техническая поддержка PT Sandbox осуществляется для всех версий, выпущенных за последние три месяца, для последней минорной версии и для последней сертифицированной ФСТЭК версии.

4. Принципы работы PT Sandbox

Раздел содержит основную информацию о принципах работы PT Sandbox.

В этом разделе

4.1. 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 специалистом по безопасности из хранилища файлов, помещаются в ZIP-архивы с паролем infected.

При взаимодействии PT Sandbox с сервисом управления пользователями и доступом PT Management and Configuration (PT MC) все данные передаются в зашифрованном виде.

4.2. Компоненты PT Sandbox

В состав PT Sandbox входят следующие компоненты:

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

  Примечание. Встроенный PT MC может быть заменен на внешний экземпляр (см. раздел 12.4).

— Веб-интерфейс — компонент графического пользовательского интерфейса PT Sandbox, доступный в браузере.

— Ядро проверки — компонент, который отправляет объекты на проверку и контролирует выполнение проверки.

— Модуль поведенческого анализа — компонент, отвечающий за проверку файлов методом поведенческого анализа.

— Хранилище файлов — компонент, отвечающий за хранение полученных извне файлов на жестком диске.

— База данных — компонент под управлением СУБД ClickHouse, который обеспечивает хранение данных о заданиях и файлах.

— API базы данных — компонент, который обеспечивает отображение информации из базы данных в веб-интерфейсе PT Sandbox.

— Служба Updater — компонент, который обеспечивает скачивание и установку обновлений PT Sandbox и образов ВМ. Включает в себя функции работы с лицензией продукта.

— Служба высокой доступности Keepalived — компонент, который обеспечивает доступность всех узлов отказоустойчивого кластера PT Sandbox на одном IP-адресе.

4.3. Обеспечение отказоустойчивости PT Sandbox

Для повышения надежности PT Sandbox, обеспечения сохранности данных и непрерывности работы в случае выхода из строя отдельных компонентов вы можете настроить отказоустойчивый кластер. В этом случае PT Sandbox 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 продолжит обрабатывать задачи на проверку файлов в штатном режиме (см. приложение).

4.4. Алгоритм работы PT Sandbox

Проверка объектов в PT Sandbox выполняется согласно следующему алгоритму:

1. Объект поступает на проверку в PT Sandbox от одного из настроенных источников или через веб-интерфейс. Для объекта создается задание на проверку, карточка задания. В карточку задания добавляется карточка исходного объекта.
2. Выполняются определение типа объекта и выделение дочерних объектов:
   - Если объект является письмом, из него выделяются тело письма, файлы вложений, выполняется поиск ссылок и скачивание файлов по этим ссылкам.
   - Если объект является архивом, выполняется декомпрессия или распаковка файлов. Для зашифрованных архивов выполняется подбор пароля.
   - Если объект является ссылкой, скачивается файл по этой ссылке.

   В карточку задания добавляются отдельные карточки для объектов, связанных с исходным объектом.
3. Собираются данные об объектах задания и заносятся в карточки объектов. Например, для файла указываются хеш-суммы (MD5, SHA-1 и SHA-256), размер и MIME-тип.

4. Каждый объект задания проверяется с помощью различных методов проверки в соответствии с заданными параметрами проверки, результаты проверок заносятся в карточку объекта. На основании результатов проверок принимается решении о наличии или отсутствии угрозы в объекте — выносится вердикт по объекту.
5. На основании вердиктов по отдельным объектам выносится вердикт о наличии или отсутствии угрозы в исходном объекте, поступившем на проверку.
6. Файлы задания сохраняются в хранилище файлов. Извлеченные из архивов файлы и вложения электронных писем сохраняются в хранилище как отдельные файлы. Если файл имеет размер больше 1 ГБ или занимает больше 1% от объема хранилища, он удаляется.
7. Если для источника настроен блокирующий режим работы, в зависимости от вердикта проверенный файл или электронное письмо пропускается в информационную систему или блокируется.

4.5. Методы проверки объектов

Для получения информации об опасности объектов PT Sandbox проверяет их методами статического и динамического анализа.

Статический анализ

К статическому анализу относятся следующие методы проверки:

— Антивирусное сканирование файлов. Проверка файлов в многопоточном режиме с помощью антивирусов сторонних разработчиков.

— Экспертная оценка файлов. Проверка файлов с помощью YARA-правил из базы знаний средства проверки PT ESC, разработанного специалистами экспертного центра Positive Technologies.

— Проверка файлов по спискам. Проверка хеш-сумм файлов по черному и белому спискам, составленным специалистами по информационной безопасности вашей организации.

— Проверка файлов и ссылок по индикаторам компрометации с помощью средства проверки PT IoC. Индикатор компрометации — это объект или свойство объекта, которые указывают на подозрительную или вредоносную активность в информационной системе. Индикаторами компрометации для файлов могут быть хеш-суммы, для ссылок — URL, IP-адреса и имена доменов.

— Ретроспективный анализ файлов. Регулярная повторная проверка файлов из хранилища с использованием обновленных антивирусных баз и обновленной базы знаний средства проверки PT ESC.

Динамический анализ

К динамическому анализу относятся следующие методы проверки:

— Поведенческий анализ файлов. Анализ поведения файлов в изолированной виртуальной среде.

  Файл запускается в специально подготовленном образе ОС, в котором анализируется его поведение. Образ может содержать специальные файлы-приманки, которые выглядят привлекательной мишенью и провоцируют вредоносное ПО на попытки получить к ним доступ. При этом отслеживаются следующие действия файла: создание файлов (артефактов), запуск процессов, выполнение интернет-запросов, изменение оперативной памяти, изменение системного реестра.

  Для выявления вредоносного ПО используются правила из базы знаний экспертного центра Positive Technologies. Эти правила определяют признаки опасного и потенциально опасного поведения файла. Все полученные в ходе анализа артефакты сохраняются в хранилище файлов и проверяются методами статического анализа.

— Анализ файлов с использованием машинного обучения. Анализ поведения файлов в изолированной виртуальной среде с помощью средства проверки PT ML, разработанного специалистами экспертного центра Positive Technologies на основе технологии машинного обучения.

— Анализ ссылок. Поиск и скачивание контента по ссылкам с помощью средства проверки PT Crawler и механизма curl. Скачанные файлы сохраняются в хранилище файлов и проверяются методами статического анализа.

4.6. Источники для проверки

Источник для проверки — это интерфейс в информационной системе организации, с которого в PT Sandbox поступают объекты на проверку.

Доступны источники для проверки следующих типов:

— Веб-интерфейс — компонент PT Sandbox, пользовательский графический веб-интерфейс, с помощью которого пользователи и специалисты по безопасности самостоятельно загружают на проверку файлы, указывают ссылки, которые нужно проверить, и получают результаты проверки.

— Checkme — служба PT Sandbox, с помощью которой сотрудники организации самостоятельно отправляют файлы на проверку по электронной почте (см. раздел 20.3) 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 специалисты по 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.

— 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.

— Публичный API — сервис PT Sandbox, предоставляющий возможность взаимодействия сторонних приложений с PT Sandbox по HTTP и HTTPS.

— Хранилище — компонент PT Sandbox, отвечающий за хранение полученных извне файлов на жестком диске. PT Sandbox отправляет файлы из хранилища на повторную проверку, если она была настроена.

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

4.7. Режимы проверки объектов

В зависимости от типа источника для проверки и требований службы информационной безопасности организации PT Sandbox может проверять поступающие на проверку объекты в режиме ожидания, пассивном режиме или блокирующем режиме.

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 специалистами по безопасности.

Пассивный режим

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

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.

Режим проверки настраивается специалистом по 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	Режим ожидания	Пассивный режим	Блокирующий режим
Веб-интерфейс	Да	—	—
Служба Checkme	Да	—	—
Хранилище файлов	Да	—	—
Публичный API	Да	—	—
Почтовый сервер с установленным агентом	—	Да	Да
Почтовый сервер в режиме фильтрации	—	Да	Да
Почтовый сервер в режиме зеркалирования	—	Да	—
ICAP-сервер	Да	Да	Да
Папка-шлюз	—	—	Да
Общая папка	—	Да	—
PT NAD	—	Да	—

5. Выбор конфигурации PT Sandbox

Предусмотрены несколько конфигураций для развертывания PT Sandbox:

— **Базовая конфигурация.** Используется, если аппаратных ресурсов одного узла достаточно для проверки файлов со скоростью, приемлемой для службы информационной безопасности организации. Базовая конфигурация PT Sandbox (All-in-One) состоит из одного основного узла с функцией поведенческого анализа.

— **Высоконагруженная конфигурация.** Используется, если необходимо увеличить скорость проверки файлов методом поведенческого анализа. Задания на поведенческий анализ распределяются между несколькими специально выделенными для этого дополнительными узлами. Высоконагруженная конфигурация PT Sandbox состоит из основного узла (без функции поведенческого анализа) и одного или нескольких дополнительных узлов для поведенческого анализа файлов.

— **Отказоустойчивый кластер для высоконагруженной конфигурации.** Используется, если необходимо обеспечить бесперебойную работу PT Sandbox при высокой скорости проверки файлов. Отказоустойчивый кластер для высоконагруженной конфигурации состоит из основного узла (без функции поведенческого анализа), двух резервных узлов и одного или нескольких дополнительных узлов для поведенческого анализа файлов.

Для развертывания любой из конфигураций вы можете использовать ISO-файл или установщик из комплекта поставки PT Sandbox.

6. Требования к рабочим станциям

Для узла, с которого выполняется вход в веб-интерфейс PT Sandbox, выдвигаются следующие аппаратные и программные требования:

— Разрешение монитора —Full HD (не менее 1920 × 1080 пикселей).

— Браузер — Google Chrome версии 49 и выше или Mozilla Firefox версии 45 и выше.

— На рабочей станции администратора должны быть разрешены исходящие подключения к порту TCP 22.

— Если на узле установлен антивирус:

  - В исключения антивируса должны быть добавлены правила, которые разрешают доступ к основному узлу PT Sandbox и используемым прокси-серверам по протоколам HTTP и HTTPS.
  - В PT Sandbox должен быть установлен пользовательский SSL-сертификат, выпущенный доверенным центром сертификации (см. раздел 13.4).

7. Требования к узлам PT Sandbox

В разделе указаны аппаратные и программные требования к узлам для развертывания PT Sandbox, а также требования к сетевой инфраструктуре. Количество узлов, а также выдвигаемые к ним аппаратные и программные требования зависят от выбранной вами конфигурации PT Sandbox. Узлы PT Sandbox могут быть развернуты как на физических серверах, так и в виртуальной среде.

Внимание! Не рекомендуется устанавливать узлы с функцией поведенческого анализа в виртуальной среде.

В этом разделе

7.1. Аппаратные требования

Аппаратные требования к узлам для развертывания PT Sandbox зависят от планируемой нагрузки, от количества одновременно работающих виртуальных машин для поведенческого анализа файлов и от планируемого объема хранилища файлов.

> **Внимание!** На одном узле PT Sandbox с функцией поведенческого анализа одновременно может работать не более 15 виртуальных машин. Если на узле установлена защищенная операционная система Astra Linux Special Edition релиза «Орел» 1.7, при указанных аппаратных требованиях число одновременно работающих виртуальных машин может быть меньше.

Основной узел с функцией поведенческого анализа

В таблице указаны минимальные аппаратные требования к физическому серверу для развертывания основного узла PT Sandbox с функцией поведенческого анализа в зависимости от планируемого количества виртуальных машин.

> **Примечание.** Вы можете самостоятельно рассчитать количество потоков центрального процессора в зависимости от планируемого количества виртуальных машинах по формуле $N_П = 3\ N_{ВМ} + 9$. Для расчета памяти ОЗУ вы можете использовать формулу $V_{ОЗУ} = 4\ N_{ВМ} + 19$. Вы получите объем памяти в ГиБ. Для перевода в ГБ умножьте его на 1,074.

Таблица 3. Минимальные аппаратные требования для основного узла с функцией поведенческого анализа

Параметр	Количество виртуальных машин			
	2	**5**	**10**	**15**
Центральный процессор 2,2 ГГц, количество потоков	15	24	39	54
Память ОЗУ, ГБ	29	42	64	85
SSD для ОС и компонентов PT Sandbox, ГБ	225	1240	1240	1240
HDD для хранилища файлов, ГБ	75	От 1100	От 1100	От 1100

Основной или резервный узел без функции поведенческого анализа

В таблице указаны минимальные аппаратные требования к физическому серверу для развертывания основного и резервных узлов PT Sandbox без функции поведенческого анализа в зависимости от планируемого количества создаваемых за час заданий на проверку объектов. При этом учтено потребление аппаратных ресурсов на получение объектов, на создание и обработку указанного количества заданий, а также на проверку объектов с помощью доступных средств проверки Positive Technologies и антивирусов.

Примечание. При оценке аппаратных требований учтено, что набор поступающих на проверку объектов зависит от типа источника. Если источником файлов выступает сетевой трафик, набор обычно содержит следующие типы файлов: 60% — документы (DOC, DOCX, ODT, ODS, PDF, XLS), 20% — исполняемые файлы (EXE), 15% — графические файлы (PNG, JPG) и 5% — архивы (ZIP, RAR, 7Z). Для почтовых серверов набор содержит письма с вложенными файлами следующих типов: 40% — графические файлы, 35% — документы, 15% — исполняемые файлы и 10% — архивы.

Таблица 4. Минимальные аппаратные требования для основного и резервных узлов без функции поведенческого анализа

Параметр	Нагрузка (заданий/час)			
	100	**1000**	**5000**	**10000**
Центральный процессор 2,2 ГГц, количество потоков	4	6	10	15
Память ОЗУ, ГБ	16	32	32	32
SSD для ОС и компонентов PT Sandbox, ГБ	215	1240	1240	1240
HDD для хранилища файлов, ГБ	65	От 1000	От 1100	От 1100

Дополнительный узел

В таблице указаны минимальные аппаратные требования к физическому серверу для развертывания дополнительного узла PT Sandbox с функцией поведенческого анализа в зависимости от планируемого количества виртуальных машин.

> **Примечание.** Вы можете самостоятельно рассчитать количество потоков центрального процессора в зависимости от планируемого количества виртуальных машин по формуле $N_П = 3\ N_{ВМ} + 4$. Для расчета памяти ОЗУ вы можете использовать формулу $V_{ОЗУ} = 4\ N_{ВМ} + 5$. Вы получите объем памяти в ГиБ. Для перевода в ГБ умножьте его на 1,074.

Таблица 5. Минимальные аппаратные требования для дополнительного узла

Параметр	**Количество виртуальных машин**			
	2	**5**	**10**	**15**
Центральный процессор 2,2 ГГц, количество потоков	10	19	34	49
Память ОЗУ, ГБ	14	27	49	70
SSD для ОС и компонентов PT Sandbox, ГБ	175	560	560	560

Примеры аппаратных конфигураций

В таблице приведены примеры аппаратных конфигураций для основного узла с функцией поведенческого анализа и для дополнительного узла.

Таблица 6. Примеры аппаратных конфигураций

Параметр	**Основной узел с функцией поведенческого анализа**	**Дополнительный узел**
Центральный процессор		
Количество	2 × Intel Xeon Gold 6230R	
Частота	2,1 ГГц	
Потоки	52	
Память ОЗУ		
Объем	256 ГБ	192 ГБ
Твердотельные накопители (SSD)		
Количество и объем	4 × 960 ГБ	
Интерфейс	SAS	
Уровень RAID	RAID 5 или RAID 10	

Параметр	Основной узел с функцией поведенческого анализа	Дополнительный узел
Тип	Mixed Use	
Жесткие диски (HDD)		
Количество и объем	6 × 8 ТБ	—
Скорость	7200 об/мин	—
Интерфейс	NL SAS	—
Уровень RAID	RAID 5 или RAID 10	—
Сетевые платы		
Количество и скорость сетевых портов для доступа к веб-интерфейсу	2 × 1 Гбит/с, 2 × 10 Гбит/с	

7.2. Программные требования

Общие программные требования к узлам для развертывания PT Sandbox:

- Для узла настроен статический IP-адрес.
- Узлу присвоено уникальное название (hostname) в рамках конфигурации PT Sandbox.
- На узле установлено точное время и обеспечено подключение к NTP-серверам организации для его синхронизации.
- С узла есть доступ к серверам обслуживания Positive Technologies по протоколу HTTPS.
- На узле в параметрах BIOS или UEFI отключен режим энергосбережения.
- На узлах с функцией поведенческого анализа в параметрах BIOS или UEFI включена аппаратная поддержка виртуализации (например, Intel Virtualization Technology).
- В операционной системе на узле отсутствуют антивирусы, работающие отдельно от PT Sandbox.

В этом разделе

7.2.1. Требования к ОС для развертывания с помощью установщика

Установка PT Sandbox с помощью установщика возможна на узлах с 64-разрядной операционной системой Astra Linux Special Edition релиза «Орел» 1.7 или Debian GNU/Linux 11 Bullseye.

> **Внимание!** При установке операционной системы Astra Linux в окне **Дополнительные настройки ОС** должны быть сняты флажки **Мандатный контроль целостности** и **Мандатное управление доступом**.

В операционной системе не должно быть раздела или файла подкачки, иначе PT Sandbox не сможет быть установлен.

В операционной системе должен быть настроен менеджер пакетов APT с корректным индексом пакетов. Менеджер пакетов используется при установке и обновлении PT Sandbox.

> **Примечание.** Вы можете проверить корректность индексов пакетов, запустив на узле команду `sudo apt-get check`.

Подсистемы безопасности Astra Linux, в частности `auditd` — служба регистрации событий безопасности, могут влиять на производительность PT Sandbox. Вы можете повысить производительность PT Sandbox, настроив или отключив службу `auditd` и перезагрузив ОС.

> **Внимание!** Полное отключение службы `auditd` может повлиять на функцию аудита в ОС. Изменяйте параметры службы `auditd` или отключайте ее в Astra Linux только в том случае, если это допускается сертификационными требованиями и политиками безопасности вашей организации.

7.2.2. Требования к разметке жесткого диска

При установке операционной системы на узлах PT Sandbox необходимо разметить дисковое пространство. В таблицах ниже указаны размеры разделов для файлов операционной системы, программных модулей PT Sandbox, хранилища файлов заданий и пользовательских данных.

> **Внимание!** Разделы для системных файлов и программных модулей PT Sandbox рекомендуется создавать на твердотельном накопителе, а разделы для хранилища файлов и пользовательских данных — на жестком диске.

Минимальные требования к размеру разделов рассчитаны для работы PT Sandbox под низкой нагрузкой, когда за час создается не более ста заданий на проверку объектов и для поведенческого анализа используется не более двух образов виртуальных машин.

Основной узел с функцией поведенческого анализа

В таблице указаны минимальный и рекомендуемый размеры разделов дисков на основном узле PT Sandbox с функцией поведенческого анализа.

Таблица 7. Разметка диска на основном узле с функцией поведенческого анализа

Тип данных	Точка монтирования	Размер[1], ГиБ / ГБ	
		Минимальный	Рекомендуемый
Системные файлы	`/`	120 / 140	220 / 240
Программные модули PT Sandbox	`/opt`	75 / 85	900 / 1000
Хранилище файлов	`/opt/ptms/var/minio`	66 / 75	От 900 / 1000
Пользовательские	`/home`	—	От 90 / 100

Основной или резервный узел без функции поведенческого анализа

В таблице указаны минимальный и рекомендуемый размеры разделов дисков на основном и резервных узлах PT Sandbox без функции поведенческого анализа.

Таблица 8. Разметка диска на основном и резервных узлах без функции поведенческого анализа

Тип данных	Точка монтирования	Размер[1], ГиБ / ГБ	
		Минимальный	Рекомендуемый размер
Системные файлы	`/`	110 / 130	220 / 240
Программные модули PT Sandbox	`/opt`	75 / 85	900 / 1000
Хранилище файлов	`/opt/ptms/var/minio`	55 / 65	От 900 / 1000
Пользовательские	`/home`	—	От 90 / 100

Дополнительный узел

В таблице указаны минимальный и рекомендуемый размеры разделов диска на дополнительном узле PT Sandbox с функцией поведенческого анализа.

1 Первое значение — размер файловой системы в ГиБ. Этот размер проверяется при установке компонентов PT Sandbox. Второе значение — размер раздела диска в ГБ. На этот размер вы можете ориентироваться при разметке диска.

Таблица 9. Разметка диска на дополнительном узле

Тип данных	Точка монтирования	Размер[1], ГиБ / ГБ	
		Минимальный	Рекомендуемый
Системные файлы	`/`	120 / 140	220 / 240
Программные модули PT Sandbox	`/opt`	30 / 35	200 / 220
Пользовательские	`/home`	—	От 90 / 100

7.2.3. Особенности развертывания в виртуальной среде

Внимание! Не рекомендуется устанавливать узлы с функцией поведенческого анализа в виртуальной среде. Использование вложенной виртуализации (nested virtualization) может привести к значительному снижению производительности PT Sandbox.

Для развертывания узлов PT Sandbox в виртуальной среде необходимо использовать гипервизор VMware ESXi версии 6.0 или выше с аппаратным обеспечением версии 11 или выше.

При установке узла PT Sandbox в виртуальной среде:

- Не поддерживается использование снапшотов. Восстановление состояния гостевой ОС из снапшота может привести к неработоспособности узла.
- Не поддерживается использование дисков с емкостью, выделяемой по требованию (технология thin provisioning).

При установке в виртуальной среде узла PT Sandbox с функцией поведенческого анализа:

- Для гостевой ОС должна быть включена аппаратная поддержка виртуализации.
- Если узел запускается при помощи UEFI, в его параметрах должна быть отключена функция Secure Boot.

7.3. Требования к сетевой инфраструктуре

В процессе установки, обновления и проверки лицензии PT Sandbox может обращаться к серверам Positive Technologies на поддоменах сайта `ptsecurity.com`. Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, необходимо обеспечить доступ к серверам Positive Technologies по протоколу HTTPS со всех узлов PT Sandbox.

Порты взаимодействия PT Sandbox

Для сетевого взаимодействия PT Sandbox с другими компонентами информационной системы на узлах PT Sandbox должны быть разрешены входящие и исходящие подключения к портам, указанным в таблице.

> **Примечание.** На рабочей станции администратора должны быть разрешены исходящие подключения к порту TCP 22.

Таблица 10. Порты взаимодействия основного и резервных узлов с компонентами информационной системы

Компонент	Протокол и порт	Направление подключений	Назначение
Рабочая станция администратора	SSH (TCP 22)	Входящие	Подключение по протоколу SSH для взаимодействия с ОС на узле PT Sandbox
	HTTPS (TCP 80, 443)	Входящие	Доступ к интерфейсу PT Sandbox и к сервису публичного API
	HTTPS (TCP 3334, 8703, 8704)	Входящие	Подключение к PT MC для аутентификации
Рабочие станции операторов	HTTPS (TCP 80, 443)	Входящие	Доступ к интерфейсу PT Sandbox
	HTTPS (TCP 3334, 8703, 8704)	Входящие	Подключение к PT MC для аутентификации
Другие узлы PT Sandbox	TCP 2379, 2380, 6443, 10250, 10251, 10252	Входящие, исходящие	Обмен данными через внутренний API
	TCP 179, 5473 и UDP 4789	Входящие, исходящие	Работа внутренней виртуальной сети
	VRRP	Входящие, исходящие	Работа службы Keepalived
Сервер Positive Technologies	HTTPS (TCP 443)	Исходящие	Загрузка обновлений и активация лицензии PT Sandbox с серверов `update.ptsecurity.com` и `update-registry.ptsecurity.com`
Внешний PT MC	HTTPS (TCP 3334, 8703, 8704)	Исходящие	Подключение к внешнему PT MC для аутентификации пользователей

Компонент	Протокол и порт	Направление подключений	Назначение
Локальный сервер обновлений	HTTP (TCP 8553) или HTTPS (TCP 8743)	Исходящие	Загрузка обновлений PT Sandbox
Источник для проверки объектов через API	HTTPS (TCP 80, 443)	Входящие	Доступ к интерфейсу и к сервису публичного API
Источник для проверки, работающий в блокирующем режиме	SMTP (TCP 587, 10025)	Исходящие	Отправка писем из карантина. Номер порта задается в параметрах источника
Сервер обновлений дополнительных антивирусов	HTTP (TCP) или HTTPS (TCP)	Исходящие	Обновление антивирусов. Номер порта зависит от антивируса
DNS-сервер	DNS (TCP 53, UDP 53)	Исходящие	Подключение к DNS-серверу
Syslog-сервер	SYSLOG (TCP 1468 или UDP 514)	Исходящие	Отправка сообщений стандарта syslog в MaxPatrol SIEM или другие системы для централизованного сбора и анализа событий ИБ. Номер порта и протокол задаются в основных параметрах PT Sandbox

На дополнительных узлах PT Sandbox должны быть разрешены входящие и исходящие подключения к портам, указанным в таблице.

Таблица 11. Порты взаимодействия дополнительных узлов с компонентами информационной системы

Компонент	Протокол и порт	Направление подключений	Назначение
Рабочая станция администратора	SSH (TCP 22)	Входящие	Подключение по протоколу SSH для взаимодействия с ОС узла
Другие узлы PT Sandbox	TCP 10250	Входящие, исходящие	Обмен данными через внутренний API

Компонент	Протокол и порт	Направление подключений	Назначение
	TCP 12345	Входящие	Подключение к сервису анализатора сетевого трафика виртуальных машин
	TCP 179, 5473 и UDP 4789	Входящие, исходящие	Работа внутренней виртуальной сети
Сервер Positive Technologies	HTTPS (TCP 443)	Исходящие	Загрузка обновлений и активация лицензии PT Sandbox с серверов `update.ptsecurity.com` и `update-registry.ptsecurity.com`
Локальный сервер обновлений	HTTP (TCP 8553) или HTTPS (TCP 8743)	Исходящие	Обновление PT Sandbox
DNS-сервер	DNS (TCP 53, UDP 53)	Исходящие	Подключение к DNS-серверу

Порты взаимодействия PT Sandbox с источниками для проверки файлов

Для сетевого взаимодействия PT Sandbox с источниками для проверки файлов на узлах PT Sandbox должны быть разрешены входящие и исходящие подключения к портам, указанным в таблице.

Внимание! Порт, указанный в параметрах источника, не должен использоваться другими источниками, службами или приложениями ОС.

Таблица 12. Порты взаимодействия узла PT Sandbox с источниками для проверки файлов

Источник для проверки	Порт и протокол	Направление подключений	Примечание
ICAP-сервер	ICAP (TCP 1344)	Входящие	Вы можете изменить номер порта в параметрах источника или через интерфейс командной строки
Почтовый сервер в режиме зеркалирования	SMTP (TCP 25)	Входящие	
Почтовый сервер в режиме фильтрации	SMTP (TCP 25 или TCP 2525)	Входящие	
PT NAD	ICAP (TCP 2344)	Входящие	

Источник для проверки	Порт и протокол	Направление подключений	Примечание
Checkme	IMAP (TCP 143), SMTP (TCP 587)	Исходящие	Вы можете указать или изменить номер порта в параметрах источника
Почтовый сервер с установленным агентом	TCP 7536	Исходящие	
Почтовый сервер в режиме фильтрации	SMTP (TCP 10025)	Исходящие	
Общая папка и папка-шлюз	NFS (TCP 111 и TCP 2049), SMB (TCP 139 и TCP 445)	Исходящие	

8. Лицензирование

Чтобы использовать PT Sandbox, вам нужно приобрести и активировать лицензию. Для приобретения лицензии или изменения параметров уже приобретенной лицензии вы можете обратиться в службу технической поддержки Positive Technologies. Лицензия может быть бессрочной или с ограниченным сроком действия. Приобретенная лицензия определяет:

— доступную конфигурацию PT Sandbox (включая информацию о допустимом количестве дополнительных узлов и их типах);

— доступные типы источников для проверки (включая информацию о лимите их производительности и использовании режима блокировки);

— доступные образы виртуальных машин.

Примечание. Одна лицензия может быть активирована только на одном экземпляре PT Sandbox.

Бессрочная лицензия

При покупке такой лицензии дополнительно определяется период предоставления обновлений. В рамках лицензии вы можете использовать все функции PT Sandbox неограниченное время, в том числе проверять объекты средствами проверки Positive Technologies и методом поведенческого анализа. После окончания периода предоставления обновлений прекратится обновление PT Sandbox, образов виртуальных машин, средств проверки Positive Technologies и их баз знаний, но сохранится возможность использования уже установленных версий. Сроки работы и обновления антивирусов определяются их лицензиями.

Лицензия с ограниченным сроком действия

При покупке такой лицензии дополнительно определяются срок ее действия и льготный период. В рамках лицензии вы можете использовать все функции PT Sandbox на протяжении всего срока действия лицензии. Сразу после окончания этого срока наступает льготный период, который предназначен для приобретения новой лицензии. В течение льготного периода также работают все функции PT Sandbox. Во время срока действия лицензии и льготного периода выполняется обновление PT Sandbox, образов виртуальных машин, средств проверки Positive Technologies и их баз знаний. После окончания льготного периода проверка объектов и обновления будут недоступны. Сроки работы и обновления антивирусов определяются их лицензиями.

См. также

Страница «Лицензия» (см. раздел 15.9.4)

Активация приобретенной лицензии (см. раздел 13.1)

Замена лицензии PT Sandbox (см. раздел 25)

9. Настройка локального сервера обновлений

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 Positive Technologies. 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.

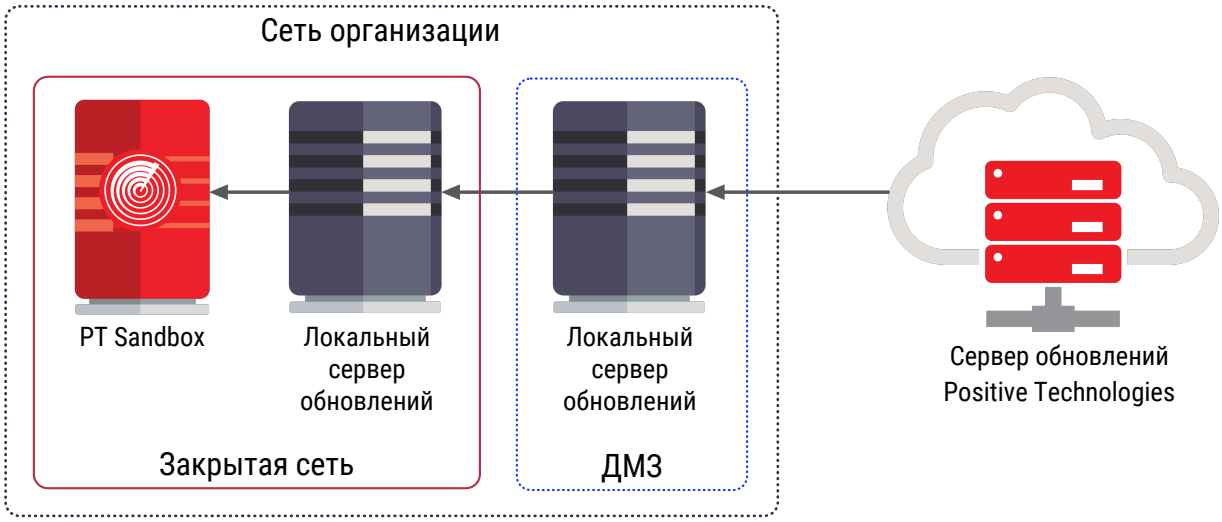

Рисунок 1. Обновление PT Sandbox в закрытом сегменте сети

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 синхронизации системного времени и для обращения к серверам обновлений необходимо обеспечить подключение к DNS- и NTP-серверам организации. Также должны быть заданы порты HTTP и (или) HTTPS для доступа к APT-репозиториям операционной системы.

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 Positive Technologies локальным сервером обновлений в демилитаризованной зоне и передачу этих данных в PT Sandbox.
4. Сменить источник обновлений PT Sandbox с публичного сервера обновлений Positive Technologies на локальный сервер обновлений, установленный в изолированном сегменте сети.

В этом разделе

9.1. Аппаратные и программные требования для локального сервера обновлений

Локальный сервер обновлений может быть установлен как на физическом сервере, так и в виртуальной среде.

Аппаратные требования

Для работы локального сервера обновлений потребуются следующие минимальные аппаратные ресурсы:

— 2 ядра процессора;

— 4 ГБ оперативной памяти;

— свободное место на диске, которое можно рассчитать с помощью формулы $V = 200 + 30 \times N$, где V — минимальный объем свободного места на диске в гигабайтах, а N — количество образов виртуальных машин, определенное вашей лицензией. Например, если лицензия позволяет использовать пять образов виртуальных машин, локальный сервер обновлений потребует минимум $200 + 30 \times 5 = 350$ ГБ свободного места на диске.

Программные требования

Локальный сервер обновлений рекомендуется устанавливать на чистую 64-разрядную серверную версию Ubuntu 18.04, Debian 10 или Debian 11.

9.2. Распаковка архива с установщиком локального сервера обновлений

► Чтобы распаковать архив с установщиком локального сервера обновлений:

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 локальный сервер обновлений.

   Примечание. Архив имеет название `ptsb.installer.<Версия ОС>.<Версия продукта>.tar.gz`, например `ptsb.installer.astra-1.7-amd64.5.7.0.177.tar.gz` или `ptsb.installer.debian-11-amd64.5.7.0.177.tar.gz`.

2. Перейдите в каталог со скопированным архивом.

   Например:

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

3. Распакуйте скопированный архив:

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

   Например:

   ```
   tar pxf ptsb.installer.astra-1.7-amd64.5.7.0.177.tar.gz
   ```

Архив с установщиком локального сервера обновлений распакован.

9.3. Установка локального сервера обновлений

В этом разделе приводится инструкция по установке локального сервера обновлений в закрытом сегменте сети или в демилитаризованной зоне.

Перед выполнением инструкции нужно:

— Убедиться, что физический сервер или виртуальная машина, на которые вы планируете устанавливать локальный сервер обновлений, удовлетворяет аппаратным и программным требованиям (см. раздел 9.1).

— Если вы устанавливаете локальный сервер обновлений в демилитаризованной зоне, убедиться, что сервер или виртуальная машина, на которые вы планируете устанавливать локальный сервер обновлений, имеет доступ к серверам обслуживания (см. раздел 10.5.4).

— Распаковать архив с установщиком локального сервера обновлений (см. раздел 9.2).

► Чтобы установить локальный сервер обновлений:

1. Перейдите в каталог с распакованным установщиком локального сервера обновлений:
   `cd /home/user/ptsb-installer`
2. Запустите установку локального сервера обновлений:
   `sudo ./pt-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 Positive Technologies.

9.4. 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 Positive Technologies. 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 Positive Technologies:
  ```
  sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --serial-number '<Серийный номер лицензии>'
  ```
- Если установленный локальный сервер обновлений должен подключаться к публичному серверу обновлений Positive Technologies через прокси сервер:
  ```
  sudo /opt/pt/pt-update-mirror/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/pt/pt-update-mirror/bin/pt-update-mirror license activate --serial-number 'XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXXXXXXXX' --proxy http://192.0.2.15:8080 --proxy-user Ivanov --proxy-password P@ssw0rd
  ```

Лицензия активирована.

9.5. Ручной перенос обновлений 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 Positive Technologies:

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

   Если сервер получит информацию о доступных обновлениях, появится сообщение `New data available for update`.

2. На этом же сервере экспортируйте полученные обновления в файл экспорта-импорта обновлений:

   - Если требуется экспортировать обновления и лицензию PT Sandbox, а также обновления баз средств проверки:

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

   - Если требуется экспортировать только лицензию PT Sandbox:

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

   - Если требуется экспортировать только обновления баз средств проверки:

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

     Например:

     ```
     sudo /opt/pt/pt-update-mirror/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:

   - Если требуется импортировать лицензию PT Sandbox:

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

   - Если из файла требуется импортировать все:

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

Например:

```
sudo /opt/pt/pt-update-mirror/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 вам нужно выбрать локальное зеркало в качестве источника обновлений.

9.6. Настройка автоматического переноса обновлений в закрытый сегмент сети

Если между локальными серверами обновлений есть сетевая связность, вы можете настроить автоматическую передачу обновлений с сайта Positive Technologies 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 Positive Technologies локальным сервером обновлений, установленным в демилитаризованной зоне.

   Для этого нужно обеспечить автоматическое выполнение следующей команды (например, при помощи планировщика заданий):

   ```
   sudo /opt/pt/pt-update-mirror/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:

   - Если требуется экспортировать обновления и лицензию PT Sandbox, а также обновления баз средств проверки:

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

   - Если требуется экспортировать только лицензию PT Sandbox:

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

   - Если требуется экспортировать только обновления баз средств проверки:

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

     Например:

     ```
     sudo /opt/pt/pt-update-mirror/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:

   - Если требуется импортировать лицензию PT Sandbox:
     ```
     sudo -- bash -c 'yes | /opt/pt/pt-update-mirror/bin/pt-update-mirror repository import --only-licenses <Путь к архиву с его названием>'
     ```
   - Если из файла требуется импортировать все:
     ```
     sudo -- bash -c 'yes | /opt/pt/pt-update-mirror/bin/pt-update-mirror repository import <Путь к архиву с его названием>'
     ```

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

Автоматический перенос обновлений PT Sandbox в закрытый сегмент сети настроен.

Теперь вам нужно выбрать локальное зеркало в качестве источника обновлений.

9.7. Выбор локального зеркала в качестве источника обновлений

Для выбора локального зеркала в качестве источника обновлений PT Sandbox необходимо:

— На основном узле указать локальное зеркало в качестве сервера обновлений.

— На каждом узле PT Sandbox указать IP-адрес или FQDN локального зеркала в параметрах среды containerd.

► Чтобы указать локальное зеркало в качестве сервера обновлений PT Sandbox,

на основном узле выполните команду:
```
sudo ptmsctl product settings apply --update-server http://<IP-адрес или FQDN локального зеркала>:8553
```

В качестве сервера обновлений PT Sandbox указано локальное зеркало.

Инструкцию необходимо выполнить на каждом узле PT Sandbox.

► Чтобы указать адрес локального зеркала в параметрах среды containerd:

1. Если у вас было настроено локальное зеркало для обновления PT Sandbox версий 5.0—5.1, выполните следующие действия:

   - Замените содержимое файла `/etc/containerd/config.toml` следующими строками:
     ```
     version = 2
     [plugins."io.containerd.grpc.v1.cri".containerd.runtimes.runc]
       runtime_type = "io.containerd.runc.v2"
     ```

```
  [plugins."io.containerd.grpc.v1.cri".containerd.runtimes.runc.options]
    systemdCgroup = true
[plugins."io.containerd.grpc.v1.cri".registry]
  config_path = "/etc/containerd/certs.d"
```

- Сохраните файл.

2. Настройте параметры в файле `hosts.toml`:

   - Создайте на узле каталог `/etc/containerd/certs.d/<IP-адрес или FQDN локального зеркала>:8553`.
   - Создайте в этом каталоге файл `hosts.toml`.
   - Добавьте в файл строки:

     ```
     server = "http://<IP-адрес или FQDN локального зеркала>:8553"
     [host."http://<IP-адрес или FQDN локального зеркала>:8553"]
       capabilities = ["pull", "resolve"]
     ```

   - Сохраните файл.

3. Перезапустите службу `containerd`:

   ```
   sudo systemctl restart containerd
   ```

   Примечание. Вы можете узнать состояние службы, выполнив команду `sudo service containerd status`.

В параметрах среды containerd указан адрес локального зеркала.

10. Развертывание PT Sandbox с помощью ISO-файла

В разделе приведены инструкции по развертыванию различных конфигураций PT Sandbox с помощью ISO-файла.

Внимание! Если для обновления PT Sandbox вы планируете использовать локальное зеркало обновлений, перед развертыванием любой из конфигураций необходимо установить и настроить локальный сервер обновлений.

Примечание. В PT Sandbox используется микросервисная архитектура и контейнеризация приложений на основе технологий containerd и Kubernetes (K8s). Для просмотра докер-контейнеров и докер-образов, созданных при развертывании, вы можете использовать утилиты crictl и ctr. Утилиты будут доступны на узлах после установки компонентов PT Sandbox.

В этом разделе

10.1. Создание внешнего установочного носителя из ISO-файла

Для создания внешнего установочного носителя с установщиком PT Sandbox вам нужно использовать ISO-файл, входящий в комплект поставки PT Sandbox. Файл имеет название формата `ptsb.<Версия ОС>.<Версия PT Sandbox>.<Версия ISO-файла>.iso`, например `ptsb.debian-11-amd64.5.7.0.4242.333.iso`.

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

Создание установочного носителя в Windows

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, в результате чего установщик PT Sandbox не будет работать.

Создание установочного носителя в ОС семейства Linux

► Чтобы создать установочный носитель:

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 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.debian-11-amd64.5.7.0.4242.333.iso /dev/sdf
   ```

10.2. Базовая конфигурация

Базовая конфигурация PT Sandbox (All-in-One) состоит из одного основного узла с функцией поведенческого анализа. Для развертывания базовой конфигурации вам необходимо:

1. Создать внешний установочный носитель.
2. Установить на основной узел ОС, гипервизор Xen и компоненты PT Sandbox.
3. Активировать на основном узле функцию поведенческого анализа.
4. Проверить доступ с узла к серверам обслуживания Positive Technologies.

Основному узлу будет присвоено название `ptsb`. Вы можете изменить его в процессе установки.

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.

► Чтобы установить ОС, гипервизор Xen и компоненты PT Sandbox на основной узел:

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.

```
┤ [!!] System requirements check ├

Before you proceed with the installation, make sure that the following requirements are
satisfied.

                    Virtualization support:      true [  OK  ]
                    System requirements:              [  OK  ]
                    Maximum number of VMs:           1 [  OK  ]
                    Partitioning mode:             ask [  OK  ]

                    Continue installation             [  OK  ]

   <Go Back>
```

Рисунок 2. 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, на 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.

```
┤ [!!] System requirements check ├

Maximum number of virtual machines running simultaneously for behavioral analysis (0-9):

2

   <Go Back>                                                    <Continue>
```

Рисунок 3. Изменение максимального количества виртуальных машин

4. Если вам нужно изменить режим разметки дисков, выберите пункт **Partitioning mode** и затем один из вариантов:

   - **auto** — установщик разметит дисковое пространство согласно рекомендуемой схеме (см. раздел 7.2.2), после чего продолжит установку;

- **ask** — установщик разметит дисковое пространство согласно рекомендуемой схеме (см. раздел 7.2.2), после чего предложит вам подтвердить или изменить автоматически созданную таблицу разметки перед продолжением установки;
- **manual** — разметка дискового пространства выполняется вручную (при необходимости вы сможете запустить автоматическую разметку на этапе ручной разметки).

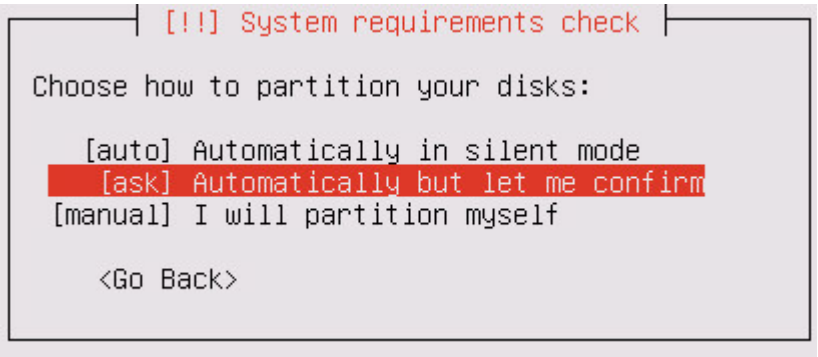

Рисунок 4. Выбор режима разметки дисков

5. В меню **System requirements check** выберите вариант **Continue installation**.

   Если устанавливаемой операционной системе доступно несколько сетевых интерфейсов, установщик предложит выбрать один из них.

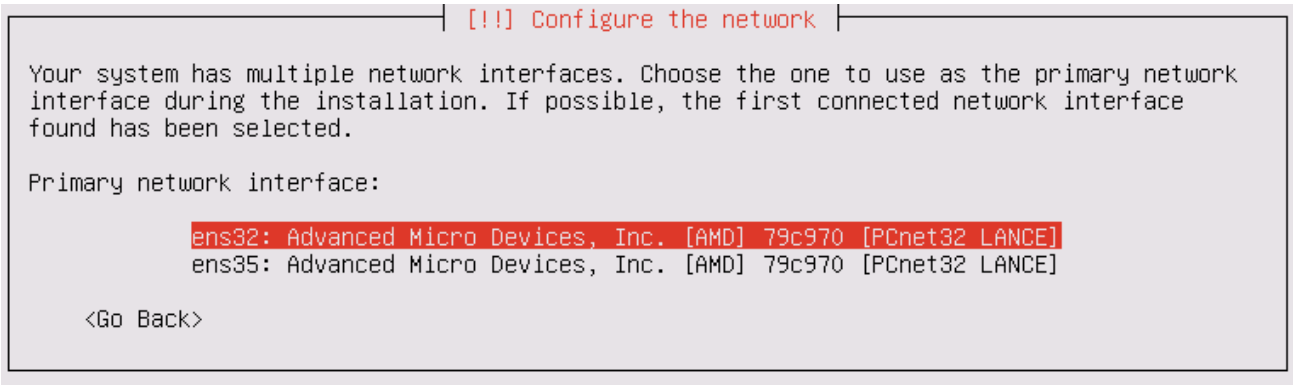

Рисунок 5. Выбор сетевого интерфейса

   Если физический сервер или виртуальная машина, на которые выполняется установка, не подключены к DHCP-серверу, установщик предложит вручную настроить сетевые параметры (см. раздел 10.5.2).

Рисунок 6. Сообщение о невозможности автоматической настройки сетевых параметров

6. Если вам нужно изменить предустановленное название узла, введите новое название в поле **Hostname** и выберите вариант **Continue**.

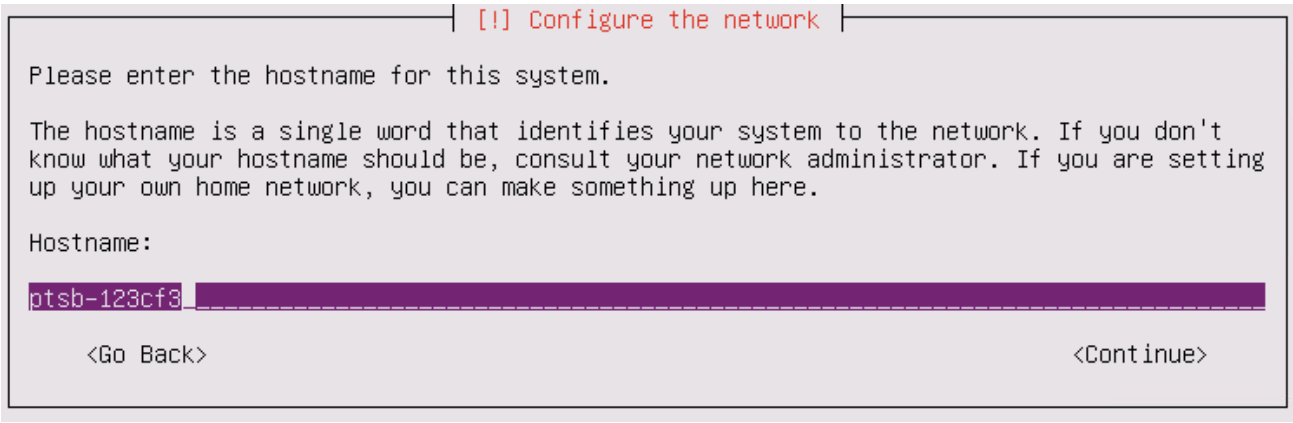

Рисунок 7. Изменение названия узла

Если на этапе **System requirements check** в качестве режима разметки (**Partitioning mode**) вы выбрали вариант **ask** или **manual**, после настройки сетевых параметров откроется меню **Partition disks** для разметки дискового пространства (см. раздел 10.5.1).

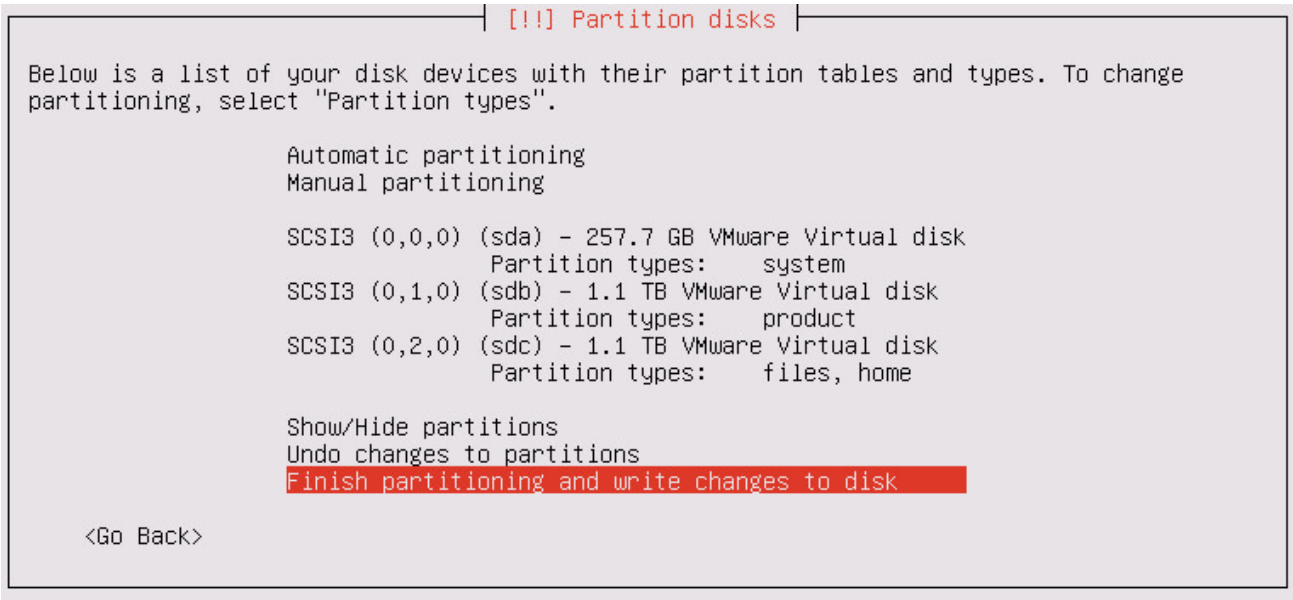

Рисунок 8. Разметка дискового пространства

После разметки дискового пространства начнется установка ОС. По окончании установки сервер или виртуальная машина, на которые 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 клавиши клавиатуры в течение одной минуты.

После перезагрузки начнется загрузка ОС. Когда система будет загружена, начнется установка PT Sandbox. По окончании установки появится сообщение `Version 5.7.<Номер сборки> successfully installed`.

7. Нажмите клавишу Enter.

   Вам будет предложено ввести логин пользователя операционной системы.

8. Введите `administrator` и нажмите клавишу Enter.

   Вам будет предложено ввести пароль пользователя операционной системы.

9. Введите `P0sitive` и нажмите клавишу Enter.

   Появится приветственное сообщение операционной системы.

На основной узел установлены ОС, гипервизор Xen и компоненты PT Sandbox.

См. также

Активация функции поведенческого анализа (см. раздел 10.5.3)

Проверка доступа к серверам обслуживания (см. раздел 10.5.4)

10.3. Высоконагруженная конфигурация

Высоконагруженная конфигурация PT Sandbox состоит из основного узла (без функции поведенческого анализа) и одного или нескольких дополнительных узлов для поведенческого анализа файлов. Для развертывания высоконагруженной конфигурации PT Sandbox вам необходимо:

1. Создать внешний установочный носитель.
2. Развернуть основной узел (без функции поведенческого анализа):
   - Установить на основной узел ОС и компоненты PT Sandbox.
   - Проверить доступ с основного узла к серверам обслуживания Positive Technologies.
3. Развернуть дополнительные узлы:
   - Установить на каждый дополнительный узел ОС и гипервизор Xen.
   - Установить на каждый дополнительный узел компоненты PT Sandbox.
   - Проверить доступ с каждого дополнительного узла к серверам обслуживания Positive Technologies.
4. Активировать на дополнительных узлах функцию поведенческого анализа.

В этом разделе

См. также

Активация функции поведенческого анализа (см. раздел 10.5.3)

Проверка доступа к серверам обслуживания (см. раздел 10.5.4)

10.3.1. Установка ОС и компонентов PT Sandbox на основной узел

Основному узлу будет присвоено название `ptsb`. Вы можете изменить его в процессе установки.

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.

► Чтобы установить ОС и компоненты PT Sandbox на основной узел:

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 устанавливаемой операционной системе доступно несколько сетевых интерфейсов, установщик предложит выбрать один из них.

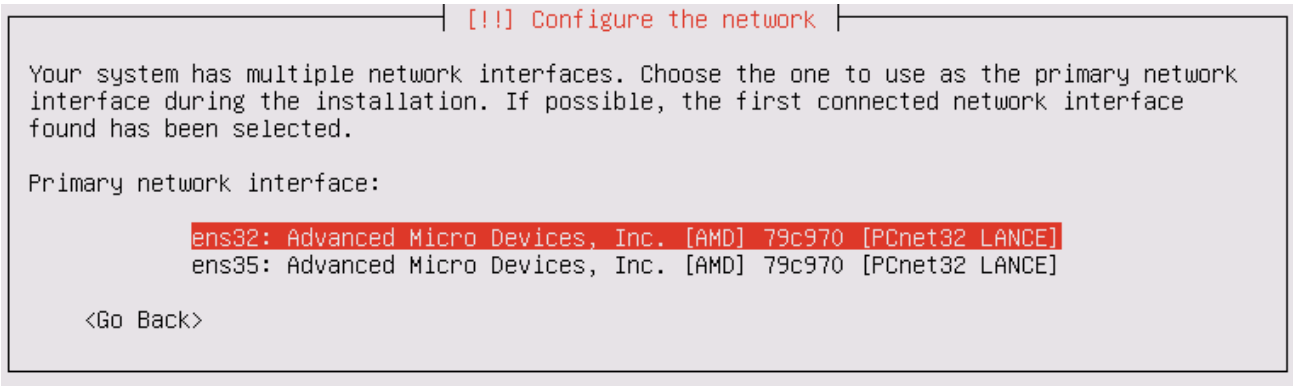

Рисунок 9. Выбор сетевого интерфейса

   Если физический сервер или виртуальная машина, на которые выполняется установка, не подключены к DHCP-серверу, установщик предложит вручную настроить сетевые параметры (см. раздел 10.5.2).

Рисунок 10. Сообщение о невозможности автоматической настройки сетевых параметров

3. Если вам нужно изменить предустановленное название узла, введите новое название в поле **Hostname** и выберите вариант **Continue**.

```
[!] Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't
know what your hostname should be, consult your network administrator. If you are setting
up your own home network, you can make something up here.

Hostname:

ptsb-123cf3

    <Go Back>                                                    <Continue>
```

Рисунок 11. Изменение названия узла

После настройки сетевых параметров откроется меню **Partition disks** для работы с разметкой дискового пространства (см. раздел 10.5.1).

```
[!!] Partition disks

Below is a list of your disk devices with their partition tables and types. To change
partitioning, select "Partition types".

                    Automatic partitioning
                    Manual partitioning

                    SCSI3 (0,0,0) (sda) - 257.7 GB VMware Virtual disk
                                   Partition types:    system
                    SCSI3 (0,1,0) (sdb) - 1.1 TB VMware Virtual disk
                                   Partition types:    product
                    SCSI3 (0,2,0) (sdc) - 1.1 TB VMware Virtual disk
                                   Partition types:    files, home

                    Show/Hide partitions
                    Undo changes to partitions
                    Finish partitioning and write changes to disk

    <Go Back>
```

Рисунок 12. Разметка дискового пространства

После разметки дискового пространства начнется установка ОС. По окончании установки сервер или виртуальная машина, на которые 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 клавиши клавиатуры в течение одной минуты.

После перезагрузки начнется загрузка ОС. Когда система будет загружена, начнется установка PT Sandbox. По окончании установки появится сообщение `Version 5.7.<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.

На основной узел установлены ОС и компоненты PT Sandbox.

10.3.2. Установка ОС и гипервизора Xen на дополнительный узел

Дополнительному узлу будет присвоено название `ptsb-<Хеш-сумма времени установки узла>`, например `ptsb-271fec`. Вы можете изменить его в процессе установки.

Внимание! Имя узла в операционной системе (hostname) должно отличаться от имен других узлов PT Sandbox в рамках одной конфигурации. Изменение имени узла после установки компонентов PT Sandbox приведет к неработоспособности компонентов PT Sandbox на этом узле.

► Чтобы установить на дополнительный узел ОС и гипервизор Xen:

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.

```
┤ [!!] System requirements check ├

Before you proceed with the installation, make sure that the following requirements are
satisfied.

                    Virtualization support:      true [  OK  ]
                    System requirements:              [  OK  ]
                    Maximum number of VMs:           1 [  OK  ]
                    Partitioning mode:             ask [  OK  ]

                    Continue installation             [  OK  ]

   <Go Back>
```

Рисунок 13. 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, на 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.

```
┤ [!!] System requirements check ├

Maximum number of virtual machines running simultaneously for behavioral analysis (0-9):

2

   <Go Back>                                                    <Continue>
```

Рисунок 14. Изменение максимального количества виртуальных машин

4. Если вам нужно изменить режим разметки дисков, выберите пункт **Partitioning mode** и затем один из вариантов:

   - **auto** — установщик разметит дисковое пространство согласно рекомендуемой схеме (см. раздел 7.2.2), после чего продолжит установку;
   - **ask** — установщик разметит дисковое пространство согласно рекомендуемой схеме (см. раздел 7.2.2), после чего предложит вам подтвердить или изменить автоматически созданную таблицу разметки перед продолжением установки;
   - **manual** — разметка дискового пространства выполняется вручную (при необходимости вы сможете запустить автоматическую разметку на этапе ручной разметки).

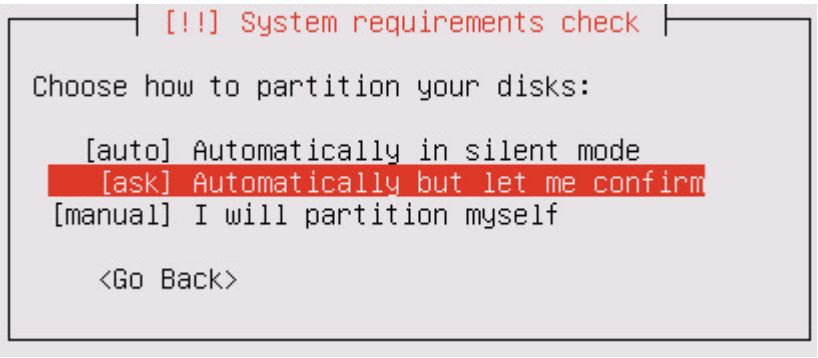

Рисунок 15. Выбор режима разметки дисков

5. В меню **System requirements check** выберите вариант **Continue installation**.

   Если устанавливаемой операционной системе доступно несколько сетевых интерфейсов, установщик предложит выбрать один из них.

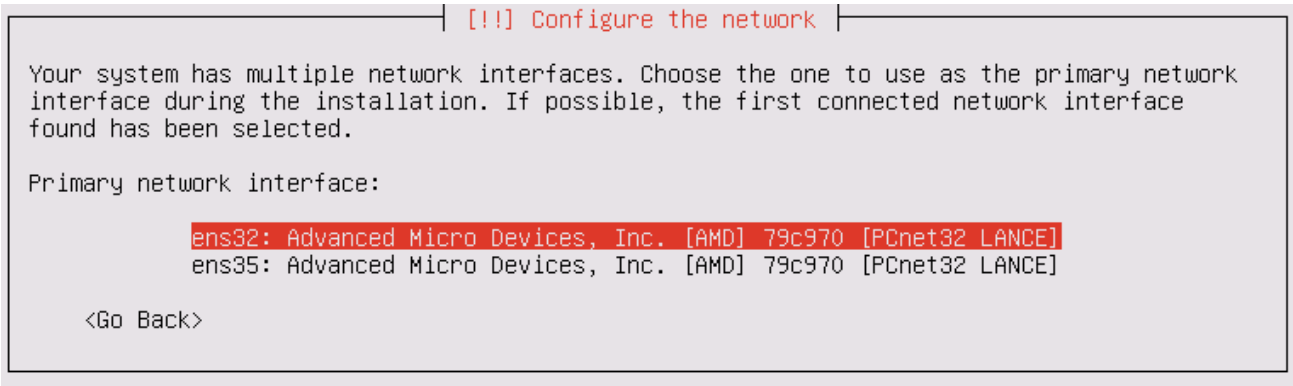

Рисунок 16. Выбор сетевого интерфейса

   Если физический сервер или виртуальная машина, на которые выполняется установка, не подключены к DHCP-серверу, установщик предложит вручную настроить сетевые параметры (см. раздел 10.5.2).

Рисунок 17. Сообщение о невозможности автоматической настройки сетевых параметров

6. Если вам нужно изменить предустановленное название узла, введите новое название в поле **Hostname** и выберите вариант **Continue**.

```
[!] Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't
know what your hostname should be, consult your network administrator. If you are setting
up your own home network, you can make something up here.

Hostname:

ptsb-123cf3

    <Go Back>                                                    <Continue>
```

Рисунок 18. Изменение названия узла

Если на этапе **System requirements check** в качестве режима разметки (**Partitioning mode**) вы выбрали вариант **ask** или **manual**, после настройки сетевых параметров откроется меню **Partition disks** для разметки дискового пространства (см. раздел 10.5.1).

```
[!!] Partition disks

Below is a list of your disk devices with their partition tables and types. To change
partitioning, select "Partition types".

                    Automatic partitioning
                    Manual partitioning

                    SCSI3 (0,0,0) (sda) - 257.7 GB VMware Virtual disk
                                   Partition types:    system
                    SCSI3 (0,1,0) (sdb) - 1.1 TB VMware Virtual disk
                                   Partition types:    product
                    SCSI3 (0,2,0) (sdc) - 1.1 TB VMware Virtual disk
                                   Partition types:    files, home

                    Show/Hide partitions
                    Undo changes to partitions
                    Finish partitioning and write changes to disk

    <Go Back>
```

Рисунок 19. Разметка дискового пространства

После разметки дискового пространства начнется установка ОС. По окончании установки сервер или виртуальная машина, на которые 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 клавиши клавиатуры в течение одной минуты.

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

7. Нажмите клавишу Enter.

   Вам будет предложено ввести логин пользователя операционной системы.

8. Введите `administrator` и нажмите клавишу Enter.

   Вам будет предложено ввести пароль пользователя операционной системы.

9. Введите `P0sitive` и нажмите клавишу Enter.

   Появится приветственное сообщение операционной системы.

На дополнительный узел установлены ОС и гипервизор Xen.

10.3.3. Установка компонентов PT Sandbox на дополнительный узел

Установка компонентов PT Sandbox на дополнительный узел выполняется при помощи специальной команды. Эту команду нужно сгенерировать на основном узле и затем запустить на дополнительном.

Генерация команды для установки компонентов PT Sandbox

Инструкцию необходимо выполнять на основном узле.

Внимание! Команда действует два часа. Повторная генерация команды делает недействительной ранее сгенерированную команду.

► Чтобы получить команду для установки компонентов PT Sandbox:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   ```
   cd /home/administrator/installer
   ```
2. Запустите скрипт для генерации команды:
   ```
   sudo ./k8s-gen-token.sh
   ```
   Пример сгенерированной команды:
   ```
   ./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ijqr4l.vizd2...1vi66
   ```

Запуск команды для установки компонентов PT Sandbox

Инструкцию необходимо выполнять на дополнительном узле от имени суперпользователя (root).

► Чтобы установить компоненты PT Sandbox:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   `cd /home/user/ptsb-installer`
2. Выполните полученную ранее команду, например:
   `sudo ./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ijqr4l.vizd2...1vi66`

   Примечание. Если для доступа к внешним ресурсам в сети организации используется прокси-сервер, в команду для установки дополнительных узлов необходимо добавить параметры `--proxy-addr 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Логин>' --proxy-password '<Пароль>'`.

Компоненты PT Sandbox установлены.

10.4. Отказоустойчивый кластер для высоконагруженной конфигурации

Отказоустойчивый кластер для высоконагруженной конфигурации PT Sandbox состоит из основного узла (без функции поведенческого анализа), двух резервных узлов и одного или нескольких дополнительных узлов для поведенческого анализа файлов. Для развертывания отказоустойчивого кластера для высоконагруженной конфигурации PT Sandbox вам необходимо:

1. Создать внешний установочный носитель.
2. Развернуть основной узел (без функции поведенческого анализа):
   - Установить на основной узел ОС и компоненты PT Sandbox.
   - Проверить доступ с основного узла к серверам обслуживания Positive Technologies.
   - Установить на основной узел службу Keepalived.
3. Развернуть два резервных узла:
   - Установить на оба резервных узла ОС.
   - Установить на оба резервных узла компоненты PT Sandbox.
   - Проверить доступ с обоих резервных узлов к серверам обслуживания Positive Technologies.
   - Установить на оба резервных узла службу Keepalived.

4. Развернуть дополнительные узлы:
   - Установить на каждый дополнительный узел ОС и гипервизор Xen.
   - Установить на каждый дополнительный узел компоненты PT Sandbox.
   - Проверить доступ с каждого дополнительного узла к серверам обслуживания Positive Technologies.
5. Активировать на дополнительных узлах функцию поведенческого анализа.

В этом разделе

См. также

10.4.1. Установка ОС и компонентов PT Sandbox на основной узел

Основному узлу будет присвоено название `ptsb`. Вы можете изменить его в процессе установки.

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.

► Чтобы установить ОС и компоненты PT Sandbox на основной узел:

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 устанавливаемой операционной системе доступно несколько сетевых интерфейсов, установщик предложит выбрать один из них.

```
[!!] Configure the network

Your system has multiple network interfaces. Choose the one to use as the primary network
interface during the installation. If possible, the first connected network interface
found has been selected.

Primary network interface:

        ens32: Advanced Micro Devices, Inc. [AMD] 79c970 [PCnet32 LANCE]
        ens35: Advanced Micro Devices, Inc. [AMD] 79c970 [PCnet32 LANCE]

    <Go Back>
```

Рисунок 20. Выбор сетевого интерфейса

Если физический сервер или виртуальная машина, на которые выполняется установка, не подключены к DHCP-серверу, установщик предложит вручную настроить сетевые параметры (см. раздел 10.5.2).

```
[!!] Configure the network

                    Network autoconfiguration failed
Your network is probably not using the DHCP protocol. Alternatively, the DHCP server may
be slow or some network hardware is not working properly.

                          <Continue>
```

Рисунок 21. Сообщение о невозможности автоматической настройки сетевых параметров

3. Если вам нужно изменить предустановленное название узла, введите новое название в поле **Hostname** и выберите вариант **Continue**.

```
[!] Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't
know what your hostname should be, consult your network administrator. If you are setting
up your own home network, you can make something up here.

Hostname:

ptsb-123cf3_____________________________________________________________

    <Go Back>                                                <Continue>
```

Рисунок 22. Изменение названия узла

После настройки сетевых параметров откроется меню **Partition disks** для работы с разметкой дискового пространства (см. раздел 10.5.1).

```
┤ [!!] Partition disks ├

Below is a list of your disk devices with their partition tables and types. To change
partitioning, select "Partition types".

                    Automatic partitioning
                    Manual partitioning

                    SCSI3 (0,0,0) (sda) - 257.7 GB VMware Virtual disk
                                   Partition types:    system
                    SCSI3 (0,1,0) (sdb) - 1.1 TB VMware Virtual disk
                                   Partition types:    product
                    SCSI3 (0,2,0) (sdc) - 1.1 TB VMware Virtual disk
                                   Partition types:    files, home

                    Show/Hide partitions
                    Undo changes to partitions
                    Finish partitioning and write changes to disk

    <Go Back>
```

Рисунок 23. Разметка дискового пространства

После разметки дискового пространства начнется установка ОС. По окончании установки сервер или виртуальная машина, на которые 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 клавиши клавиатуры в течение одной минуты.

После перезагрузки начнется загрузка ОС. Когда система будет загружена, начнется установка PT Sandbox. По окончании установки появится сообщение `Version 5.7.<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.

На основной узел установлены ОС и компоненты PT Sandbox.

10.4.2. Установка службы Keepalived на основной или резервный узел

Служба Keepalived обеспечивает работоспособность PT Sandbox в случае сбоев его отдельных компонентов или узлов.

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

Внимание! Виртуальный IP-адрес должен отличаться от IP-адресов других узлов PT Sandbox.

► Чтобы установить службу Keepalived:

1. Не менее чем через три минуты после входа в установленную ОС перейдите в каталог с установщиком PT Sandbox, например:

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

2. Запустите скрипт для установки службы Keepalived:

   ```
   sudo ./install-keepalived.sh --virtual-ip <Виртуальный 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 завершении работы скрипта появится сообщение об успешной установке службы.

Служба Keepalived установлена.

10.4.3. Установка ОС на резервный узел

Резервному узлу будет присвоено название `ptsb-<Хеш-сумма времени установки узла>`, например `ptsb-271fec`. Вы можете изменить его в процессе установки.

Внимание! Имя узла в операционной системе (hostname) должно отличаться от имен других узлов PT Sandbox в рамках одной конфигурации. Изменение имени узла после установки компонентов PT Sandbox приведет к неработоспособности компонентов PT Sandbox на этом узле.

► Чтобы установить ОС на резервный узел:

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 устанавливаемой операционной системе доступно несколько сетевых интерфейсов, установщик предложит выбрать один из них.

```
[!!] Configure the network

Your system has multiple network interfaces. Choose the one to use as the primary network
interface during the installation. If possible, the first connected network interface
found has been selected.

Primary network interface:

        ens32: Advanced Micro Devices, Inc. [AMD] 79c970 [PCnet32 LANCE]
        ens35: Advanced Micro Devices, Inc. [AMD] 79c970 [PCnet32 LANCE]

    <Go Back>
```

Рисунок 24. Выбор сетевого интерфейса

Если физический сервер или виртуальная машина, на которые выполняется установка, не подключены к DHCP-серверу, установщик предложит вручную настроить сетевые параметры (см. раздел 10.5.2).

```
[!!] Configure the network

                    Network autoconfiguration failed
Your network is probably not using the DHCP protocol. Alternatively, the DHCP server may
be slow or some network hardware is not working properly.

                          <Continue>
```

Рисунок 25. Сообщение о невозможности автоматической настройки сетевых параметров

3. Если вам нужно изменить предустановленное название узла, введите новое название в поле **Hostname** и выберите вариант **Continue**.

```
[!] Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't
know what your hostname should be, consult your network administrator. If you are setting
up your own home network, you can make something up here.

Hostname:

ptsb-123cf3_____________________________________________________________

    <Go Back>                                                <Continue>
```

Рисунок 26. Изменение названия узла

После настройки сетевых параметров откроется меню **Partition disks** для работы с разметкой дискового пространства (см. раздел 10.5.1).

```
┤ [!!] Partition disks ├

Below is a list of your disk devices with their partition tables and types. To change
partitioning, select "Partition types".

                    Automatic partitioning
                    Manual partitioning

                    SCSI3 (0,0,0) (sda) - 257.7 GB VMware Virtual disk
                                   Partition types:    system
                    SCSI3 (0,1,0) (sdb) - 1.1 TB VMware Virtual disk
                                   Partition types:    product
                    SCSI3 (0,2,0) (sdc) - 1.1 TB VMware Virtual disk
                                   Partition types:    files, home

                    Show/Hide partitions
                    Undo changes to partitions
                    Finish partitioning and write changes to disk

    <Go Back>
```

Рисунок 27. Разметка дискового пространства

После разметки дискового пространства начнется установка ОС. По окончании установки сервер или виртуальная машина, на которые 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 клавиши клавиатуры в течение одной минуты.

Начнется загрузка ОС. 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.

ОС установлена на резервный узел.

10.4.4. Установка компонентов PT Sandbox на резервный узел

Установка компонентов PT Sandbox на резервный узел выполняется при помощи специальной команды. Эту команду нужно сгенерировать на основном узле и затем запустить на резервном.

Генерация команды для установки компонентов PT Sandbox

Внимание! Команда действует два часа. Повторная генерация команды делает недействительной ранее сгенерированную команду.

Инструкцию необходимо выполнять на основном узле.

► Чтобы получить команду для установки компонентов PT Sandbox:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   ```
   cd /home/administrator/installer
   ```
2. Запустите скрипт для генерации команды:
   ```
   sudo ./k8s-gen-token.sh --with-master-role
   ```

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

Запуск команды для установки компонентов PT Sandbox

Инструкцию необходимо выполнять на резервном узле от имени суперпользователя (root).

► Чтобы установить компоненты PT Sandbox:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   ```
   cd /home/administrator/installer
   ```
2. Выполните полученную ранее команду, например:
   ```
   ./k8s-join-node.sh --cluster-ip 192.0.2.15 --token ijqr3l.viz...i66 --with-master-role --
   certificate-key 7f3e58...14e2b3f
   ```

   Примечание. Если для доступа к внешним ресурсам в сети организации используется прокси-сервер, в команду для установки дополнительных узлов необходимо добавить параметры `--proxy-addr 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Логин>' --proxy-password '<Пароль>'`.

Компоненты PT Sandbox установлены.

10.4.5. Установка ОС и гипервизора Xen на дополнительный узел

Дополнительному узлу будет присвоено название `ptsb-<Хеш-сумма времени установки узла>`, например `ptsb-271fec`. Вы можете изменить его в процессе установки.

Внимание! Имя узла в операционной системе (hostname) должно отличаться от имен других узлов PT Sandbox в рамках одной конфигурации. Изменение имени узла после установки компонентов PT Sandbox приведет к неработоспособности компонентов PT Sandbox на этом узле.

► Чтобы установить на дополнительный узел ОС и гипервизор Xen:

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.

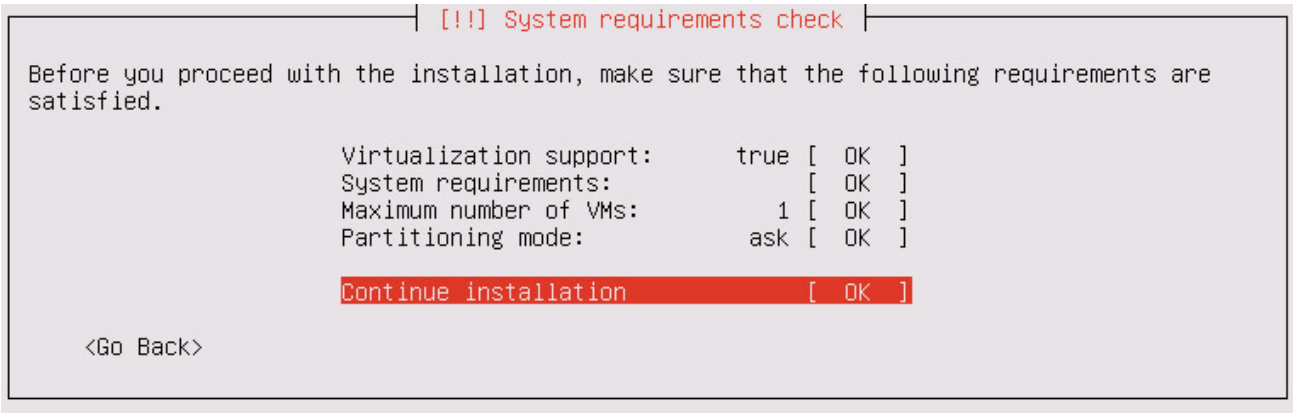

Рисунок 28. Проверка системных требований

   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, на 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.

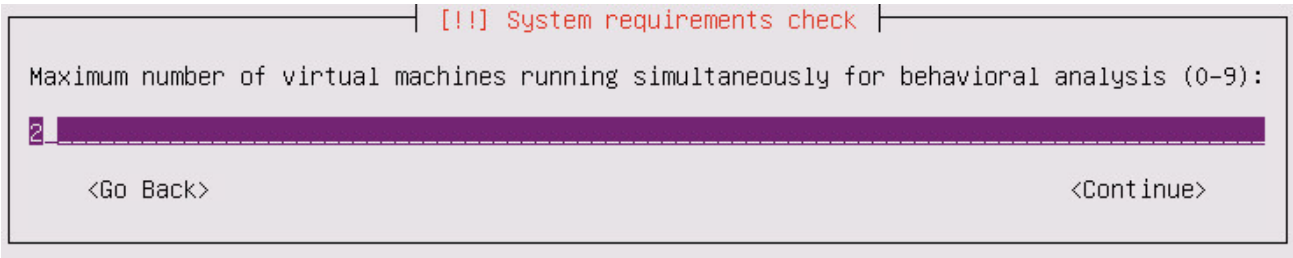

Рисунок 29. Изменение максимального количества виртуальных машин

4. Если вам нужно изменить режим разметки дисков, выберите пункт **Partitioning mode** и затем один из вариантов:

   - **auto** — установщик разметит дисковое пространство согласно рекомендуемой схеме (см. раздел 7.2.2), после чего продолжит установку;
   - **ask** — установщик разметит дисковое пространство согласно рекомендуемой схеме (см. раздел 7.2.2), после чего предложит вам подтвердить или изменить автоматически созданную таблицу разметки перед продолжением установки;
   - **manual** — разметка дискового пространства выполняется вручную (при необходимости вы сможете запустить автоматическую разметку на этапе ручной разметки).

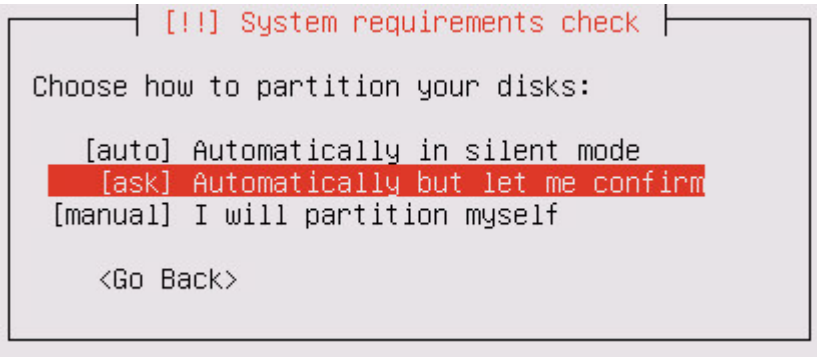

Рисунок 30. Выбор режима разметки дисков

5. В меню **System requirements check** выберите вариант **Continue installation**.

   Если устанавливаемой операционной системе доступно несколько сетевых интерфейсов, установщик предложит выбрать один из них.

```
[!!] Configure the network

Your system has multiple network interfaces. Choose the one to use as the primary network
interface during the installation. If possible, the first connected network interface
found has been selected.

Primary network interface:

        ens32: Advanced Micro Devices, Inc. [AMD] 79c970 [PCnet32 LANCE]
        ens35: Advanced Micro Devices, Inc. [AMD] 79c970 [PCnet32 LANCE]

    <Go Back>
```

Рисунок 31. Выбор сетевого интерфейса

Если физический сервер или виртуальная машина, на которые выполняется установка, не подключены к DHCP-серверу, установщик предложит вручную настроить сетевые параметры (см. раздел 10.5.2).

```
[!!] Configure the network

                    Network autoconfiguration failed
Your network is probably not using the DHCP protocol. Alternatively, the DHCP server may
be slow or some network hardware is not working properly.

                              <Continue>
```

Рисунок 32. Сообщение о невозможности автоматической настройки сетевых параметров

6. Если вам нужно изменить предустановленное название узла, введите новое название в поле **Hostname** и выберите вариант **Continue**.

```
[!] Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't
know what your hostname should be, consult your network administrator. If you are setting
up your own home network, you can make something up here.

Hostname:

ptsb-123cf3_____________________________________________________________

    <Go Back>                                                <Continue>
```

Рисунок 33. Изменение названия узла

Если на этапе **System requirements check** в качестве режима разметки (**Partitioning mode**) вы выбрали вариант **ask** или **manual**, после настройки сетевых параметров откроется меню **Partition disks** для разметки дискового пространства (см. раздел 10.5.1).

```
┤ [!!] Partition disks ├

Below is a list of your disk devices with their partition tables and types. To change
partitioning, select "Partition types".

                    Automatic partitioning
                    Manual partitioning

                    SCSI3 (0,0,0) (sda) - 257.7 GB VMware Virtual disk
                                   Partition types:    system
                    SCSI3 (0,1,0) (sdb) - 1.1 TB VMware Virtual disk
                                   Partition types:    product
                    SCSI3 (0,2,0) (sdc) - 1.1 TB VMware Virtual disk
                                   Partition types:    files, home

                    Show/Hide partitions
                    Undo changes to partitions
                    Finish partitioning and write changes to disk

    <Go Back>
```

Рисунок 34. Разметка дискового пространства

После разметки дискового пространства начнется установка ОС. По окончании установки сервер или виртуальная машина, на которые 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 клавиши клавиатуры в течение одной минуты.

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

7. Нажмите клавишу Enter.

   Вам будет предложено ввести логин пользователя операционной системы.

8. Введите `administrator` и нажмите клавишу Enter.

   Вам будет предложено ввести пароль пользователя операционной системы.

9. Введите `P0sitive` и нажмите клавишу Enter.

   Появится приветственное сообщение операционной системы.

На дополнительный узел установлены ОС и гипервизор Xen.

10.4.6. Установка компонентов PT Sandbox на дополнительный узел

Установка компонентов PT Sandbox на дополнительный узел выполняется при помощи специальной команды. Эту команду нужно сгенерировать на основном узле и затем запустить на дополнительном.

Генерация команды для установки компонентов PT Sandbox

Инструкцию необходимо выполнять на основном узле.

Внимание! Команда действует два часа. Повторная генерация команды делает недействительной ранее сгенерированную команду.

► Чтобы получить команду для установки компонентов PT Sandbox:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   `cd /home/administrator/installer`
2. Запустите скрипт для генерации команды:
   `sudo ./k8s-gen-token.sh`

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

Запуск команды для установки компонентов PT Sandbox

Инструкцию необходимо выполнять на дополнительном узле от имени суперпользователя (root).

► Чтобы установить компоненты PT Sandbox:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   `cd /home/user/ptsb-installer`
2. Выполните полученную ранее команду, например:
   `sudo ./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ijqr4l.vizd2...1vi66`

   Примечание. Если для доступа к внешним ресурсам в сети организации используется прокси-сервер, в команду для установки дополнительных узлов необходимо добавить параметры `--proxy-addr 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Логин>' --proxy-password '<Пароль>'`.

Компоненты PT Sandbox установлены.

10.5. Дополнительные действия при развертывании

Раздел содержит инструкции для выполнения дополнительных действий, которые могут потребоваться при развертывании PT Sandbox.

В этом разделе

10.5.1. Разметка дискового пространства при установке с помощью ISO-файла

При установке PT Sandbox вместе с операционной системой (с помощью ISO-файла) установщик попытается автоматически разметить дисковое пространство по рекомендуемой схеме (см. раздел 7.2.2). Результат разметки отображается в меню **Partition disks**.

> **Примечание.** Меню **Partition disks** не открывается, если при установке основного узла на шаге **System requirements check** мастера установки вы выбрали вариант **auto** в качестве режима разметки (**Partitioning mode**).

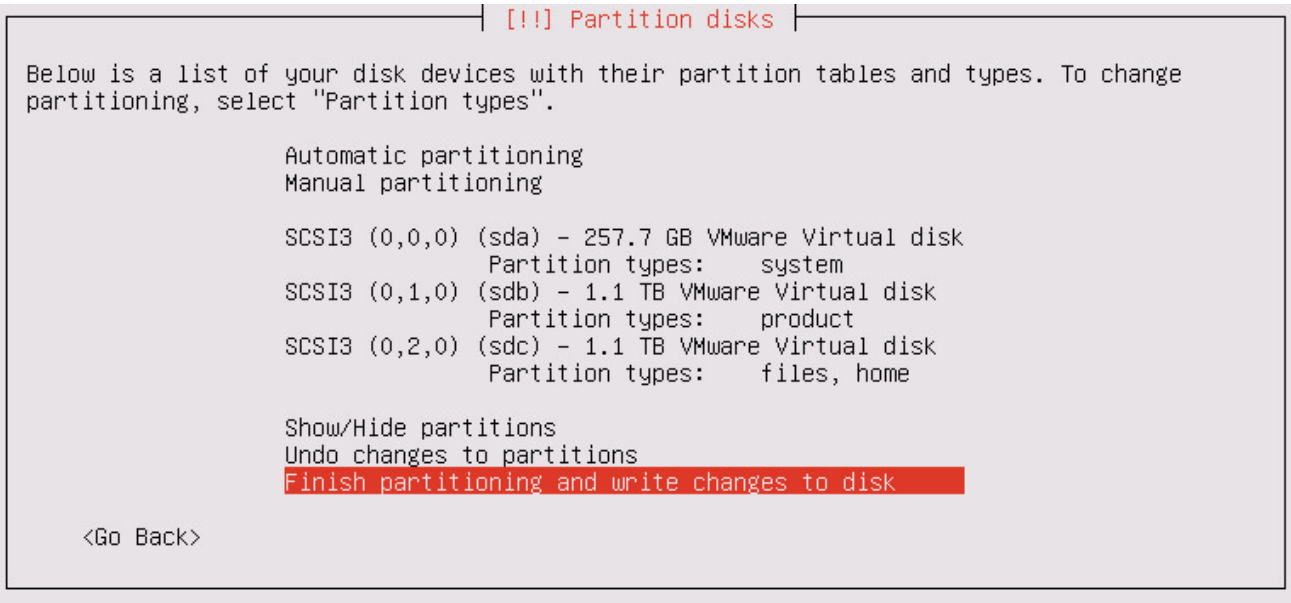

Рисунок 35. Разметка дискового пространства

Меню содержит список доступных запоминающих устройств (жестких дисков и SSD). В режиме **ask** или после выбора пункта **Automatic partitioning** под каждым устройством отображаются назначенные ему типы разделов. Типы разделов определяют, какие данные установщик будет записывать на устройство и какие таблицы разметки для этих данных будет создавать.

С помощью пунктов меню **Partition disks** вы можете ознакомиться с результатами автоматической разметки дисков, изменить или подтвердить таблицу разметки.

Таблица 13. Пункты меню Partition disks

Пункт	Что делает
Automatic partitioning	Выполняет автоматическую разметку дискового пространства по рекомендуемой схеме
Manual partitioning	Открывает меню, аналогичное тому, которое используется в стандартном установщике операционной системы Debian для ручной разметки дискового пространства. **Примечание.** Ручная разметка сбрасывает назначенные устройствам типы разделов
Partition types	Открывает меню, которое позволяет переназначить типы разделов для конкретного запоминающего устройства: — `system` — операционная система; — `product` — программные модули PT Sandbox; — `files` — файловое хранилище; — `home` — пользовательские файлы (точка монтирования `/home`) Каждый тип может быть назначен только одному устройству. Одному устройству могут быть назначены несколько типов
Show/Hide partitions	Показывает или скрывает разделы и точки монтирования
Undo changes to partitions	Отменяет изменения, которые были внесены в таблицу разметки
Finish partitioning and write changes to disk	Запускает проверку таблицы разметки. Если таблица разметки не содержит ошибок, установщик запишет изменения на диск и продолжит установку

10.5.2. Ручная настройка сетевых параметров при установке с помощью ISO-файла

При установке PT Sandbox вместе с операционной системой (с помощью ISO-файла) установщик попытается автоматически настроить сетевые параметры: определить IP-адреса узла, шлюза и DNS-серверов. Если физический сервер или виртуальная машина, на которые выполняется установка, не подключены к DHCP-серверу, установщик предложит настроить сетевые параметры вручную.

► Чтобы вручную настроить сетевые параметры:

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

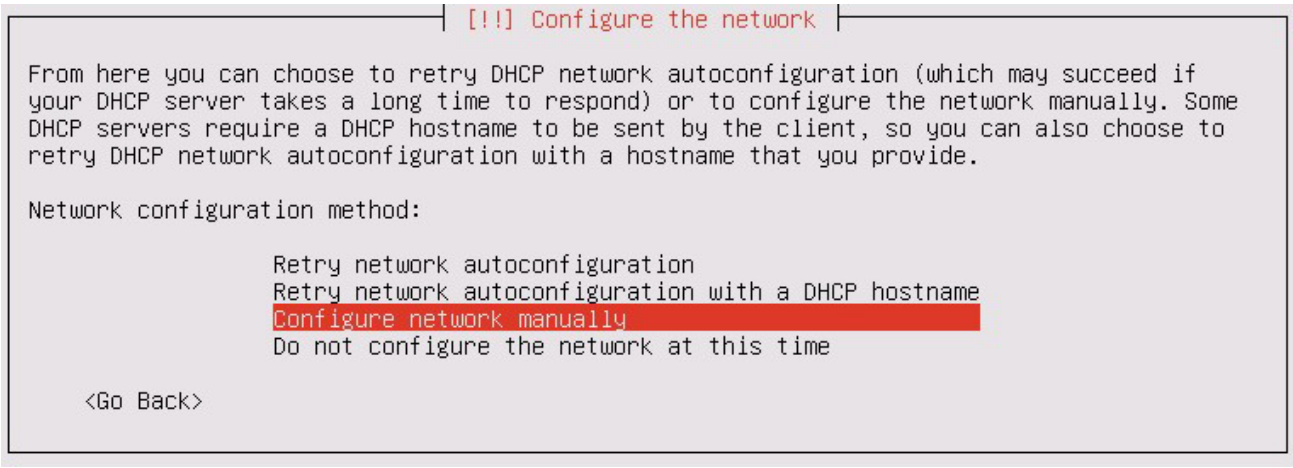

Рисунок 36. Ручная настройка сетевых параметров

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

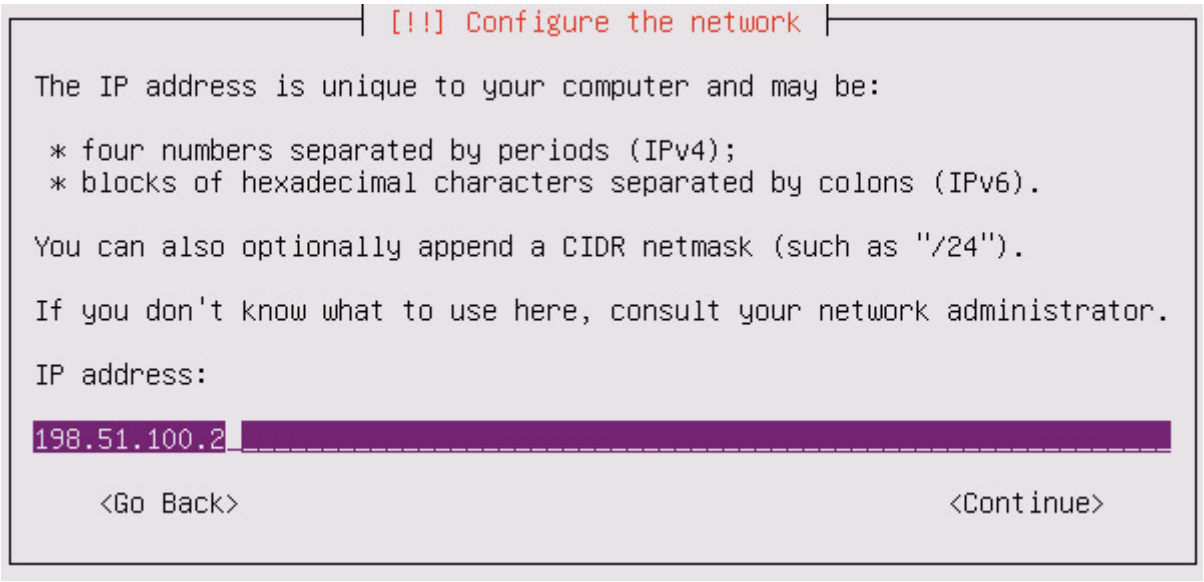

Рисунок 37. Ввод IP-адреса физического сервера или виртуальной машины

3. 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 38. Ввод маски подсети

4. 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:

198.51.100.43

    <Go Back>                                                    <Continue>
```

Рисунок 39. Ввод IP-адреса шлюза

5. Если вам нужно использовать DNS-серверы, через пробел введите IP-адреса DNS-серверов (до трех серверов) 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:

192.0.2.1 192.0.2.2

    <Go Back>                                                    <Continue>
```

Рисунок 40. Ввод адресов DNS-серверов

Установка будет продолжена.

6. Если вам не нужно использовать DNS-серверы, оставьте поле пустым и выберите вариант **Continue**.

   Установка будет продолжена.

Сетевые параметры настроены.

10.5.3. Активация функции поведенческого анализа

После развертывания узлов конфигурации PT Sandbox необходимо указать, какие из узлов будут использоваться для поведенческого анализа. Для этого на них необходимо активировать функцию поведенческого анализа.

Инструкцию необходимо выполнять на основном узле.

► Чтобы активировать функцию поведенческого анализа на узлах PT Sandbox:

1. Получите список узлов, на которых установлены компоненты PT Sandbox:

   ```
   sudo ptmsctl sandbox nodes list
   ```

   Появится список узлов со статусом функции поведенческого анализа:

   - `Behavioral analysis is enabled` — узел уже используется для поведенческого анализа;
   - `Behavioral analysis is disabled` — узел не используется для поведенческого анализа;
   - `Not ready for behavioral analysis to be enabled` — узел не может быть использован для поведенческого анализа (не установлен гипервизор Xen).

2. Последовательно активируйте функцию поведенческого анализа на узлах в соответствии с конфигурацией PT Sandbox:

   ```
   sudo ptmsctl sandbox nodes acquire <Имя узла>
   ```

   Например:

   ```
   sudo ptmsctl sandbox nodes acquire hostname1
   sudo ptmsctl sandbox nodes acquire hostname5
   sudo ptmsctl sandbox nodes acquire hostname6
   ```

   Примечание. Вы можете повторно проверить статус функции поведенческого анализа на узлах командой `sudo ptmsctl sandbox nodes list`. Если вы по ошибке активировали функцию не на том узле, вы можете отключить ее командой `sudo ptmsctl sandbox nodes release <Имя узла>`.

3. Запустите скачивание и установку образов ВМ на узлы с функцией поведенческого анализа:

   ```
   sudo ptmsctl sandbox force-generate-images
   ```

Примечание. Скачивание и установка образов ВМ может занять продолжительное время. Вы можете отслеживать состояние установки в интерфейсе PT Sandbox.

Функция поведенческого анализа активирована на узлах PT Sandbox.

10.5.4. Проверка доступа к серверам обслуживания

В процессе установки, обновления и проверки лицензии PT Sandbox может обращаться к серверам Positive Technologies на поддоменах сайта `ptsecurity.com`. Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, необходимо обеспечить доступ к серверам Positive Technologies по протоколу HTTPS со всех узлов PT Sandbox.

► Чтобы проверить доступ к серверам обслуживания PT Sandbox:

1. Проверьте подключение к поддомену update:
   ```
   wget -Sq -O /dev/null https://update.ptsecurity.com/test
   ```
2. Проверьте подключение к поддомену update-registry:
   ```
   wget -Sq -O /dev/null https://update-registry.ptsecurity.com/test
   ```
3. Если код ответа на любую из команд отличается от 200 OK, настройте доступ и проверьте подключение повторно.

11. Развертывание PT Sandbox с помощью установщика

В разделе приведены инструкции по развертыванию различных конфигураций PT Sandbox с помощью установщика.

Внимание! Если для обновления PT Sandbox вы планируете использовать локальное зеркало обновлений, перед развертыванием любой из конфигураций необходимо установить и настроить локальный сервер обновлений.

Примечание. В PT Sandbox используется микросервисная архитектура и контейнеризация приложений на основе технологий containerd и Kubernetes (K8s). Для просмотра докер-контейнеров и докер-образов, созданных при развертывании, вы можете использовать утилиты crictl и ctr. Утилиты будут доступны на узлах после установки компонентов PT Sandbox.

В этом разделе

11.1. Подготовка к развертыванию

Перед развертыванием вам необходимо подготовить каждый узел выбранной конфигурации, на который будут устанавливаться компоненты PT Sandbox:

1. Установить на узле одну из ОС, рекомендованных в программных требованиях PT Sandbox.
2. Скопировать на каждый узел архив с установщиком и распаковать его.
3. Если в вашей информационной системе для доступа в интернет используется прокси-сервер, настроить подключение менеджера обновлений ОС к этому прокси-серверу.
4. Проверить доступ с узла к серверам обслуживания Positive Technologies.

В этом разделе

11.1.1. Проверка доступа к серверам обслуживания

В процессе установки, обновления и проверки лицензии PT Sandbox может обращаться к серверам Positive Technologies на поддоменах сайта `ptsecurity.com`. Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, необходимо обеспечить доступ к серверам Positive Technologies по протоколу HTTPS со всех узлов PT Sandbox.

► Чтобы проверить доступ к серверам обслуживания PT Sandbox:

1. Проверьте подключение к поддомену update:
   ```
   wget -Sq -O /dev/null https://update.ptsecurity.com/test
   ```
2. Проверьте подключение к поддомену update-registry:
   ```
   wget -Sq -O /dev/null https://update-registry.ptsecurity.com/test
   ```
3. Если код ответа на любую из команд отличается от 200 OK, настройте доступ и проверьте подключение повторно.

11.1.2. Распаковка архива с установщиком

Архив с установщиком входит в комплект поставки PT Sandbox и имеет название в формате `ptsb.installer.<Версия ОС>.<Версия продукта>.tar.gz`, например `ptsb.installer.astra-1.7-amd64.5.7.0.177.tar.gz` или `ptsb.installer.debian-11-amd64.5.7.0.177.tar.gz`.

► Чтобы распаковать архив с установщиком PT Sandbox:

1. Скопируйте архив с установщиком в любой каталог на узле.
2. Перейдите в каталог с архивом, например:
   ```
   cd /home/user/ptsb-installer
   ```
3. Распакуйте архив, например:
   ```
   tar pxf ptsb.installer.astra-1.7-amd64.5.7.0.177.tar.gz
   ```

Архив с установщиком PT Sandbox распакован.

11.1.3. Настройка подключения менеджера обновлений ОС к прокси-серверу

Если в вашей информационной системе подключение к интернету выполняется через прокси-сервер, вам нужно настроить подключение менеджера обновлений ОС к прокси-серверу.

► Чтобы настроить подключение менеджера обновлений ОС к прокси-серверу:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   ```
   cd /home/user/ptsb-installer
   ```
2. Запустите скрипт для настройки, 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 менеджера обновлений ОС к прокси-серверу настроено.

11.2. Базовая конфигурация

Базовая конфигурация PT Sandbox (All-in-One) состоит из одного основного узла с функцией поведенческого анализа. Для развертывания базовой конфигурации вам необходимо:

1. Подготовить основной узел к установке.
2. Установить на основной узел гипервизор Xen.
3. Установить на основной узел компоненты PT Sandbox.
4. Активировать на основном узле функцию поведенческого анализа.

В этом разделе

11.2.1. Установка гипервизора Xen на основной узел

Для выполнения поведенческого анализа на узле необходимо установить гипервизор Xen. Требования к аппаратным ресурсам узла зависят от количества одновременно запускаемых в гипервизоре виртуальных машин.

Определение требований к аппаратным ресурсам

► Чтобы определить требования к аппаратным ресурсам узла:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   ```
   cd /home/user/ptsb-installer
   ```
2. Запустите скрипт для определения требований к аппаратным ресурсам узла:

- Если необходимо определить, сколько виртуальных машин могут одновременно работать на узле исходя из его аппаратных ресурсов:
  `sudo xen/check-system-requirements.sh --get-max-vm`
- Если необходимо определить, сколько аппаратных ресурсов требуется для одновременной работы определенного количества виртуальных машин (не более 15):
  `sudo xen/check-system-requirements.sh --vm-count <Количество виртуальных машин>`

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

Установка гипервизора Xen

► Чтобы установить гипервизор Xen:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   `cd /home/user/ptsb-installer`
2. Запустите скрипт для проверки соответствия узла аппаратным требованиям:
   `sudo xen/check-system-requirements.sh`
3. Если узел соответствует аппаратным требованиям, запустите скрипт установки гипервизора:
   `sudo xen/install.sh --vm-count <Количество виртуальных машин>`

   Примечание. Подробная справка доступна по команде `sudo xen/install.sh -h`.
4. По завершении работы скрипта нажмите клавишу Enter.

   Узел будет перезагружен.
5. Если требуется, введите логин и пароль загрузчика.

Гипервизор Xen установлен.

11.2.2. Установка компонентов PT Sandbox на основной узел

Внимание! Имя узла в операционной системе (hostname) должно отличаться от имен других узлов PT Sandbox в рамках одной конфигурации. Изменение имени узла после установки компонентов PT Sandbox приведет к неработоспособности компонентов PT Sandbox на этом узле.

Для выполнения инструкции вам понадобится серийный номер лицензии PT Sandbox, приобретенной вашей организацией. Серийный номер высылается на адрес электронной почты, указанный при заказе лицензии, или указывается в файле `serial number.txt` на установочном диске из комплекта поставки.

► Чтобы установить компоненты PT Sandbox на основной узел:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   `cd /home/user/ptsb-installer`
2. Запустите мастер установки PT Sandbox:
   `sudo ./wizard`
3. Выберите язык мастера установки и нажмите клавишу Enter.
4. Выберите метод скачивания обновлений PT Sandbox с сайта Positive Technologies и нажмите клавишу Enter.

   Примечание. Вы можете выбрать скачивание напрямую с сайта Positive Technologies, через прокси-сервер или через локальное зеркало обновлений.
5. Если вы выбрали вариант скачивания через прокси-сервер:
   - Введите IP-адрес прокси-сервера и нажмите клавишу Enter.
   - Последовательно введите логин и пароль учетной записи для доступа к серверу, подтверждая ввод клавишей Enter.
6. Если вы выбрали вариант скачивания через локальное зеркало обновлений, введите его IP-адрес и нажмите клавишу Enter.
7. Введите серийный номер лицензии (без кавычек) и нажмите клавишу Enter.
8. Если вы планируете настраивать отказоустойчивый кластер, укажите его виртуальный адрес и нажмите клавишу Enter.
9. Введите `y` и нажмите клавишу Enter.

   Начнется установка PT Sandbox. По завершении появится сообщение об успешной установке.

Компоненты PT Sandbox установлены на основной узел.

11.2.3. Активация функции поведенческого анализа

После развертывания узлов конфигурации PT Sandbox необходимо указать, какие из узлов будут использоваться для поведенческого анализа. Для этого на них необходимо активировать функцию поведенческого анализа.

Инструкцию необходимо выполнять на основном узле.

► Чтобы активировать функцию поведенческого анализа на узлах PT Sandbox:

1. Получите список узлов, на которых установлены компоненты PT Sandbox:
   `sudo ptmsctl sandbox nodes list`

   Появится список узлов со статусом функции поведенческого анализа:
   - `Behavioral analysis is enabled` — узел уже используется для поведенческого анализа;

- `Behavioral analysis is disabled` — узел не используется для поведенческого анализа;
- `Not ready for behavioral analysis to be enabled` — узел не может быть использован для поведенческого анализа (не установлен гипервизор Xen).

2. Последовательно активируйте функцию поведенческого анализа на узлах в соответствии с конфигурацией PT Sandbox:

   ```
   sudo ptmsctl sandbox nodes acquire <Имя узла>
   ```

   Например:

   ```
   sudo ptmsctl sandbox nodes acquire hostname1
   sudo ptmsctl sandbox nodes acquire hostname5
   sudo ptmsctl sandbox nodes acquire hostname6
   ```

   Примечание. Вы можете повторно проверить статус функции поведенческого анализа на узлах командой `sudo ptmsctl sandbox nodes list`. Если вы по ошибке активировали функцию не на том узле, вы можете отключить ее командой `sudo ptmsctl sandbox nodes release <Имя узла>`.

3. Запустите скачивание и установку образов ВМ на узлы с функцией поведенческого анализа:

   ```
   sudo ptmsctl sandbox force-generate-images
   ```

   Примечание. Скачивание и установка образов ВМ может занять продолжительное время. Вы можете отслеживать состояние установки в интерфейсе PT Sandbox.

Функция поведенческого анализа активирована на узлах PT Sandbox.

11.3. Высоконагруженная конфигурация

Высоконагруженная конфигурация PT Sandbox состоит из основного узла (без функции поведенческого анализа) и одного или нескольких дополнительных узлов для поведенческого анализа файлов. Для развертывания высоконагруженной конфигурации PT Sandbox вам необходимо:

1. Развернуть основной узел (без функции поведенческого анализа):
   - Подготовить основной узел к установке.
   - Установить на основной узел компоненты PT Sandbox.
2. Развернуть дополнительные узлы:
   - Подготовить каждый дополнительный узел к установке.
   - Установить на каждый дополнительный узел гипервизор Xen.
   - Установить на каждый дополнительный узел компоненты PT Sandbox.
3. Активировать на дополнительных узлах функцию поведенческого анализа.

В этом разделе

11.3.1. Установка компонентов PT Sandbox на основной узел

Внимание! Имя узла в операционной системе (hostname) должно отличаться от имен других узлов PT Sandbox в рамках одной конфигурации. Изменение имени узла после установки компонентов PT Sandbox приведет к неработоспособности компонентов PT Sandbox на этом узле.

Для выполнения инструкции вам понадобится серийный номер лицензии PT Sandbox, приобретенной вашей организацией. Серийный номер высылается на адрес электронной почты, указанный при заказе лицензии, или указывается в файле `serial number.txt` на установочном диске из комплекта поставки.

► Чтобы установить компоненты PT Sandbox на основной узел:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   `cd /home/user/ptsb-installer`
2. Запустите мастер установки PT Sandbox:
   `sudo ./wizard`
3. Выберите язык мастера установки и нажмите клавишу Enter.
4. Выберите метод скачивания обновлений PT Sandbox с сайта Positive Technologies и нажмите клавишу Enter.

   Примечание. Вы можете выбрать скачивание напрямую с сайта Positive Technologies, через прокси-сервер или через локальное зеркало обновлений.
5. Если вы выбрали вариант скачивания через прокси-сервер:
   - Введите IP-адрес прокси-сервера и нажмите клавишу Enter.
   - Последовательно введите логин и пароль учетной записи для доступа к серверу, подтверждая ввод клавишей Enter.
6. Если вы выбрали вариант скачивания через локальное зеркало обновлений, введите его IP-адрес и нажмите клавишу Enter.
7. Введите серийный номер лицензии (без кавычек) и нажмите клавишу Enter.

8. Если вы планируете настраивать отказоустойчивый кластер, укажите его виртуальный адрес и нажмите клавишу Enter.
9. Введите `y` и нажмите клавишу Enter.

   Начнется установка PT Sandbox. По завершении появится сообщение об успешной установке.

Компоненты PT Sandbox установлены на основной узел.

11.3.2. Установка гипервизора Xen на дополнительный узел

Для выполнения поведенческого анализа на узле необходимо установить гипервизор Xen. Требования к аппаратным ресурсам узла зависят от количества одновременно запускаемых в гипервизоре виртуальных машин.

Определение требований к аппаратным ресурсам

► Чтобы определить требования к аппаратным ресурсам узла:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   ```
   cd /home/user/ptsb-installer
   ```
2. Запустите скрипт для определения требований к аппаратным ресурсам узла:
   - Если необходимо определить, сколько виртуальных машин могут одновременно работать на узле исходя из его аппаратных ресурсов:
     ```
     sudo xen/check-system-requirements.sh --slave --get-max-vm
     ```
   - Если необходимо определить, сколько аппаратных ресурсов требуется для одновременной работы определенного количества виртуальных машин (не более 15):
     ```
     sudo xen/check-system-requirements.sh --slave --vm-count <Количество виртуальных машин>
     ```

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

Установка гипервизора Xen

► Чтобы установить гипервизор Xen:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   ```
   cd /home/user/ptsb-installer
   ```
2. Запустите скрипт для проверки соответствия узла аппаратным требованиям:
   ```
   sudo xen/check-system-requirements.sh --slave
   ```

3. Если узел соответствует аппаратным требованиям, запустите скрипт установки гипервизора:

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

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

4. По завершении работы скрипта нажмите клавишу Enter.

   Узел будет перезагружен.

5. Если требуется, введите логин и пароль загрузчика.

Гипервизор Xen установлен.

11.3.3. Установка компонентов PT Sandbox на дополнительный узел

Внимание! Имя узла в операционной системе (hostname) должно отличаться от имен других узлов PT Sandbox в рамках одной конфигурации. Изменение имени узла после установки компонентов PT Sandbox приведет к неработоспособности компонентов PT Sandbox на этом узле.

Установка компонентов PT Sandbox на дополнительный узел выполняется при помощи специальной команды. Эту команду нужно сгенерировать на основном узле и затем запустить на дополнительном.

Генерация команды для установки компонентов PT Sandbox

Инструкцию необходимо выполнять на основном узле.

Внимание! Команда действует два часа. Повторная генерация команды делает недействительной ранее сгенерированную команду.

► Чтобы получить команду для установки компонентов PT Sandbox:

1. Перейдите в каталог с установщиком PT Sandbox, например:

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

2. Запустите скрипт для генерации команды:

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

   Пример сгенерированной команды:

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

Запуск команды для установки компонентов PT Sandbox

Инструкцию необходимо выполнять на дополнительном узле от имени суперпользователя (root).

► Чтобы установить компоненты PT Sandbox:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   ```
   cd /home/user/ptsb-installer
   ```
2. Выполните полученную ранее команду, например:
   ```
   sudo ./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ijqr4l.vizd2...1vi66
   ```

   Примечание. Если для доступа к внешним ресурсам в сети организации используется прокси-сервер, в команду для установки дополнительных узлов необходимо добавить параметры `--proxy-addr 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Логин>' --proxy-password '<Пароль>'`.

Компоненты PT Sandbox установлены.

11.3.4. Активация функции поведенческого анализа

После развертывания узлов конфигурации PT Sandbox необходимо указать, какие из узлов будут использоваться для поведенческого анализа. Для этого на них необходимо активировать функцию поведенческого анализа.

Инструкцию необходимо выполнять на основном узле.

► Чтобы активировать функцию поведенческого анализа на узлах PT Sandbox:

1. Получите список узлов, на которых установлены компоненты PT Sandbox:
   ```
   sudo ptmsctl sandbox nodes list
   ```

   Появится список узлов со статусом функции поведенческого анализа:

   - `Behavioral analysis is enabled` — узел уже используется для поведенческого анализа;
   - `Behavioral analysis is disabled` — узел не используется для поведенческого анализа;
   - `Not ready for behavioral analysis to be enabled` — узел не может быть использован для поведенческого анализа (не установлен гипервизор Xen).
2. Последовательно активируйте функцию поведенческого анализа на узлах в соответствии с конфигурацией PT Sandbox:
   ```
   sudo ptmsctl sandbox nodes acquire <Имя узла>
   ```

   Например:
   ```
   sudo ptmsctl sandbox nodes acquire hostname1
   sudo ptmsctl sandbox nodes acquire hostname5
   sudo ptmsctl sandbox nodes acquire hostname6
   ```

Примечание. Вы можете повторно проверить статус функции поведенческого анализа на узлах командой `sudo ptmsctl sandbox nodes list`. Если вы по ошибке активировали функцию не на том узле, вы можете отключить ее командой `sudo ptmsctl sandbox nodes release <Имя узла>`.

3. Запустите скачивание и установку образов ВМ на узлы с функцией поведенческого анализа:

   ```
   sudo ptmsctl sandbox force-generate-images
   ```

   Примечание. Скачивание и установка образов ВМ может занять продолжительное время. Вы можете отслеживать состояние установки в интерфейсе PT Sandbox.

Функция поведенческого анализа активирована на узлах PT Sandbox.

11.4. Отказоустойчивый кластер для высоконагруженной конфигурации

Отказоустойчивый кластер для высоконагруженной конфигурации PT Sandbox состоит из основного узла (без функции поведенческого анализа), двух резервных узлов и одного или нескольких дополнительных узлов для поведенческого анализа файлов. Для развертывания отказоустойчивого кластера для высоконагруженной конфигурации PT Sandbox вам необходимо:

1. Развернуть основной узел (без функции поведенческого анализа):
   - Подготовить основной узел к установке.
   - Установить на основной узел службу Keepalived.
   - Установить на основной узел компоненты PT Sandbox.
2. Развернуть два резервных узла:
   - Подготовить оба резервных узла к установке.
   - Установить на оба резервных узла службу Keepalived.
   - Установить на оба резервных узла компоненты PT Sandbox.
3. Развернуть дополнительные узлы:
   - Подготовить каждый дополнительный узел к установке.
   - Установить на каждый дополнительный узел гипервизор Xen.
   - Установить на каждый дополнительный узел компоненты PT Sandbox.
4. Активировать на дополнительных узлах функцию поведенческого анализа.

В этом разделе

11.4.1. Установка службы Keepalived на основной или резервный узел

Служба Keepalived обеспечивает работоспособность PT Sandbox в случае сбоев его отдельных компонентов или узлов.

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

Внимание! Виртуальный IP-адрес должен отличаться от IP-адресов других узлов PT Sandbox.

► Чтобы установить службу Keepalived:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   ```
   cd /home/user/ptsb-installer
   ```
2. Запустите скрипт для установки службы Keepalived:
   ```
   sudo ./install-keepalived.sh --virtual-ip <Виртуальный 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 завершении работы скрипта появится сообщение об успешной установке службы.

Служба Keepalived установлена.

11.4.2. Установка компонентов PT Sandbox на основной узел

Внимание! Имя узла в операционной системе (hostname) должно отличаться от имен других узлов PT Sandbox в рамках одной конфигурации. Изменение имени узла после установки компонентов PT Sandbox приведет к неработоспособности компонентов PT Sandbox на этом узле.

Для выполнения инструкции вам понадобится серийный номер лицензии PT Sandbox, приобретенной вашей организацией. Серийный номер высылается на адрес электронной почты, указанный при заказе лицензии, или указывается в файле `serial number.txt` на установочном диске из комплекта поставки.

► Чтобы установить компоненты PT Sandbox на основной узел:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   `cd /home/user/ptsb-installer`
2. Запустите мастер установки PT Sandbox:
   `sudo ./wizard`
3. Выберите язык мастера установки и нажмите клавишу Enter.
4. Выберите метод скачивания обновлений PT Sandbox с сайта Positive Technologies и нажмите клавишу Enter.

   Примечание. Вы можете выбрать скачивание напрямую с сайта Positive Technologies, через прокси-сервер или через локальное зеркало обновлений.
5. Если вы выбрали вариант скачивания через прокси-сервер:
   - Введите IP-адрес прокси-сервера и нажмите клавишу Enter.
   - Последовательно введите логин и пароль учетной записи для доступа к серверу, подтверждая ввод клавишей Enter.
6. Если вы выбрали вариант скачивания через локальное зеркало обновлений, введите его IP-адрес и нажмите клавишу Enter.
7. Введите серийный номер лицензии (без кавычек) и нажмите клавишу Enter.
8. Если вы планируете настраивать отказоустойчивый кластер, укажите его виртуальный адрес и нажмите клавишу Enter.
9. Введите `y` и нажмите клавишу Enter.

   Начнется установка PT Sandbox. По завершении появится сообщение об успешной установке.

Компоненты PT Sandbox установлены на основной узел.

11.4.3. Установка компонентов PT Sandbox на резервный узел

Внимание! Имя узла в операционной системе (hostname) должно отличаться от имен других узлов PT Sandbox в рамках одной конфигурации. Изменение имени узла после установки компонентов PT Sandbox приведет к неработоспособности компонентов PT Sandbox на этом узле.

Установка компонентов PT Sandbox на резервный узел выполняется при помощи специальной команды. Эту команду нужно сгенерировать на основном узле и затем запустить на резервном.

Генерация команды для установки компонентов PT Sandbox

Внимание! Команда действует два часа. Повторная генерация команды делает недействительной ранее сгенерированную команду.

Инструкцию необходимо выполнять на основном узле.

► Чтобы получить команду для установки компонентов PT Sandbox:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   `cd /home/user/ptsb-installer`
2. Запустите скрипт для генерации команды:
   `sudo ./k8s-gen-token.sh --with-master-role`

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

Запуск команды для установки компонентов PT Sandbox

Инструкцию необходимо выполнять на резервном узле от имени суперпользователя (root).

► Чтобы установить компоненты PT Sandbox:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   `cd /home/user/ptsb-installer`
2. Выполните полученную ранее команду, например:
   `./k8s-join-node.sh --cluster-ip 192.0.2.15 --token ijqr3l.viz...i66 --with-master-role --certificate-key 7f3e58...14e2b3f`

   Примечание. Если для доступа к внешним ресурсам в сети организации используется прокси-сервер, в команду для установки дополнительных узлов необходимо добавить параметры `--proxy-addr 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Логин>' --proxy-password '<Пароль>'`.

Компоненты PT Sandbox установлены.

11.4.4. Установка гипервизора Xen на дополнительный узел

Для выполнения поведенческого анализа на узле необходимо установить гипервизор Xen. Требования к аппаратным ресурсам узла зависят от количества одновременно запускаемых в гипервизоре виртуальных машин.

Определение требований к аппаратным ресурсам

► Чтобы определить требования к аппаратным ресурсам узла:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   `cd /home/user/ptsb-installer`
2. Запустите скрипт для определения требований к аппаратным ресурсам узла:
   - Если необходимо определить, сколько виртуальных машин могут одновременно работать на узле исходя из его аппаратных ресурсов:
     `sudo xen/check-system-requirements.sh --slave --get-max-vm`
   - Если необходимо определить, сколько аппаратных ресурсов требуется для одновременной работы определенного количества виртуальных машин (не более 15):
     `sudo xen/check-system-requirements.sh --slave --vm-count <Количество виртуальных машин>`

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

Установка гипервизора Xen

► Чтобы установить гипервизор Xen:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   `cd /home/user/ptsb-installer`
2. Запустите скрипт для проверки соответствия узла аппаратным требованиям:
   `sudo xen/check-system-requirements.sh --slave`
3. Если узел соответствует аппаратным требованиям, запустите скрипт установки гипервизора:
   `sudo xen/install.sh --slave --vm-count <Количество виртуальных машин>`

   Примечание. Подробная справка доступна по команде `sudo xen/install.sh -h`.
4. По завершении работы скрипта нажмите клавишу Enter.

   Узел будет перезагружен.
5. Если требуется, введите логин и пароль загрузчика.

Гипервизор Xen установлен.

11.4.5. Установка компонентов PT Sandbox на дополнительный узел

Внимание! Имя узла в операционной системе (hostname) должно отличаться от имен других узлов PT Sandbox в рамках одной конфигурации. Изменение имени узла после установки компонентов PT Sandbox приведет к неработоспособности компонентов PT Sandbox на этом узле.

Установка компонентов PT Sandbox на дополнительный узел выполняется при помощи специальной команды. Эту команду нужно сгенерировать на основном узле и затем запустить на дополнительном.

Генерация команды для установки компонентов PT Sandbox

Инструкцию необходимо выполнять на основном узле.

Внимание! Команда действует два часа. Повторная генерация команды делает недействительной ранее сгенерированную команду.

► Чтобы получить команду для установки компонентов PT Sandbox:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   `cd /home/user/ptsb-installer`
2. Запустите скрипт для генерации команды:
   `sudo ./k8s-gen-token.sh`

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

Запуск команды для установки компонентов PT Sandbox

Инструкцию необходимо выполнять на дополнительном узле от имени суперпользователя (root).

► Чтобы установить компоненты PT Sandbox:

1. Перейдите в каталог с установщиком PT Sandbox, например:
   `cd /home/user/ptsb-installer`
2. Выполните полученную ранее команду, например:
   `sudo ./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ijqr4l.vizd2...1vi66`

   Примечание. Если для доступа к внешним ресурсам в сети организации используется прокси-сервер, в команду для установки дополнительных узлов необходимо добавить параметры `--proxy-addr 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Логин>' --proxy-password '<Пароль>'`.

Компоненты PT Sandbox установлены.

11.4.6. Активация функции поведенческого анализа

После развертывания узлов конфигурации PT Sandbox необходимо указать, какие из узлов будут использоваться для поведенческого анализа. Для этого на них необходимо активировать функцию поведенческого анализа.

Инструкцию необходимо выполнять на основном узле.

► Чтобы активировать функцию поведенческого анализа на узлах PT Sandbox:

1. Получите список узлов, на которых установлены компоненты PT Sandbox:

   ```
   sudo ptmsctl sandbox nodes list
   ```

   Появится список узлов со статусом функции поведенческого анализа:

   - `Behavioral analysis is enabled` — узел уже используется для поведенческого анализа;
   - `Behavioral analysis is disabled` — узел не используется для поведенческого анализа;
   - `Not ready for behavioral analysis to be enabled` — узел не может быть использован для поведенческого анализа (не установлен гипервизор Xen).

2. Последовательно активируйте функцию поведенческого анализа на узлах в соответствии с конфигурацией PT Sandbox:

   ```
   sudo ptmsctl sandbox nodes acquire <Имя узла>
   ```

   Например:

   ```
   sudo ptmsctl sandbox nodes acquire hostname1
   sudo ptmsctl sandbox nodes acquire hostname5
   sudo ptmsctl sandbox nodes acquire hostname6
   ```

   Примечание. Вы можете повторно проверить статус функции поведенческого анализа на узлах командой `sudo ptmsctl sandbox nodes list`. Если вы по ошибке активировали функцию не на том узле, вы можете отключить ее командой `sudo ptmsctl sandbox nodes release <Имя узла>`.

3. Запустите скачивание и установку образов ВМ на узлы с функцией поведенческого анализа:

   ```
   sudo ptmsctl sandbox force-generate-images
   ```

   Примечание. Скачивание и установка образов ВМ может занять продолжительное время. Вы можете отслеживать состояние установки в интерфейсе PT Sandbox.

Функция поведенческого анализа активирована на узлах PT Sandbox.

12. Настройка аутентификации

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

После установки PT Sandbox вам необходимо:

1. Сменить язык интерфейса сервиса управления ролями и доступом (PT MC).
2. Войти в сервис управления ролями и доступом (PT MC).
3. В целях безопасности сменить стандартный пароль суперпользователя.
4. При необходимости создать учетную запись администратора, который будет выполнять только настройку и администрирование PT Sandbox.
5. Войти в PT Sandbox под учетной записью суперпользователя или администратора.
6. Настроить аутентификацию пользователей в продукте.

В этом разделе

12.1. Смена языка интерфейса PT MC

Сервис управления пользователями и доступом PT Management and Configuration (PT MC) обеспечивает механизм единого входа (технология single sign-on) в продукты Positive Technologies. PT MC поставляется с двумя языками интерфейса — русским (по умолчанию) и английским.

► Чтобы сменить язык интерфейса PT MC,

выполните команду:

```
ptmsctl auth use-local --locale <Новый язык интерфейса: ru-RU или en-US>
```

Например:

```
sudo ptmsctl auth use-local --locale en-US
```

Параметры будут применены, появится сообщение `Please wait a few minutes while the system components are restarted`.

12.2. Вход в PT MC

Чтобы выполнить первоначальную настройку PT Sandbox, вам нужно войти в сервис управления пользователями и доступом PT Management and Configuration (PT MC), который обеспечивает механизм единого входа (технология single sign-on) в продукты Positive Technologies.

Примечание. Все аутентификационные данные передаются в зашифрованном виде.

Перед выполнением инструкции нужно подготовить адрес PT MC. Если используется встроенный PT MC, его адресом будет IP-адрес основного узла PT Sandbox или виртуальный IP-адрес службы Keepalived (для конфигурации с отказоустойчивым кластером). Если настроен внешний сервис аутентификации (см. раздел 12.4), адресом PT MC будет IP-адрес или доменное внешнего сервиса.

► Чтобы войти в PT MC:

1. В адресной строке браузера введите ссылку вида `https://<Адрес PT MC>:3334`.

   Например:
   `https://198.51.100.22:3334`

   Откроется страница входа в PT MC.
2. В поле **Логин** введите `Administrator`.
3. В поле **Пароль** введите `P@ssw0rd`.
4. Нажмите кнопку **Войти**.

   Откроется страница управления учетными записями пользователей PT MC.

12.3. 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 пользователями и доступом (см. раздел 12.2).
2. В панели инструментов нажмите кнопку **Изменить данные**.

   Откроется страница **Редактировать информацию о пользователе**.
3. Нажмите 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.

12.4. Настройка аутентификации с помощью внешнего PT MC

По умолчанию для аутентификации пользователей PT Sandbox используется встроенный PT MC: он устанавливается вместе с PT Sandbox и работает с ним на одном сервере. Если до установки PT Sandbox в организации уже был PT MC (например, как часть системы MaxPatrol 10), вы можете использовать его вместо встроенного PT MC. Таким образом будет обеспечиваться единый механизм входа в продукты Positive Technologies.

Перед выполнением инструкции вам нужно получить корневой сертификат, которым подписан сертификат сервера с внешним PT MC, у администратора внешнего PT MC. Полученный сертификат нужно скопировать в виде файла с расширением .crt на сервер с PT Sandbox (в многосерверной конфигурации — на основной узел PT Sandbox).

► Чтобы настроить аутентификацию с помощью внешнего PT MC,

зарегистрируйте PT Sandbox в PT MC:

```
sudo ptmsctl auth use-remote \
--tenant-internal-url https://<Адрес PT MC>:8703 \
--iam-internal-url https://<Адрес PT MC>:3334 \
--ca-crt <Путь до сертификата PT MC> \
--ms-name '<Название экземпляра PT Sandbox>'
```

Например:

```
sudo ptmsctl auth use-remote \
--tenant-internal-url https://ptmc.example:8703 \
--iam-internal-url https://ptmc.example:3334 \
--ca-crt /home/user/MC_RootCA.crt \
--ms-name 'PT Sandbox'
```

Примечание. Если в организации установлен один экземпляр PT Sandbox, вы можете не указывать параметр `ms-name`. При регистрации нескольких экземпляров PT Sandbox значение параметра `ms-name` должно быть уникальным.

Параметры будут применены, появится сообщение `Please wait a few minutes while the system components are restarted`.

Аутентификация с помощью внешнего PT MC настроена.

Для возврата встроенного PT MC в качестве механизма аутентификации пользователей нужно выполнить команду `sudo ptmsctl auth use-local`.

12.5. Настройка аутентификации пользователей по LDAP

В PT MC есть два типа аутентификации: локальный и по протоколу LDAP. При использовании локальной аутентификации все данные о пользователях, включая их логины и пароли, хранятся в PT MC. При использовании LDAP логины и пароли пользователей хранятся в Microsoft Active Directory. Персональная и организационная информация по умолчанию также загружается из Microsoft Active Directory, но может быть указана и изменена в PT MC.

По умолчанию используется только локальная аутентификация пользователей. Дополнительно вы можете настроить LDAP-аутентификацию. При этом PT MC может содержать учетные записи пользователей с разными типами аутентификации. Для каждого пользователя может быть выбран свой тип аутентификации.

Для настройки LDAP-аутентификации нужно настроить подключение к одному или нескольким LDAP-серверам организации. Если вы используете стандартный (встроенный в продукт) PT MC и связь с LDAP-сервером должна осуществляться через зашифрованное соединение (LDAP по SSL, или LDAPS), дополнительно нужно установить доверенный сертификат корневого центра сертификации, используемый этим LDAP-сервером. При необходимости вы также можете настроить синхронизацию с Microsoft Active Directory.

В этом разделе

12.5.1. Установка доверенного сертификата для LDAPS

Если встроенный в продукт PT MC должен подключаться к LDAP-серверу по протоколу SSL (LDAPS), перед настройкой такого подключения вам нужно установить на сервер PT Sandbox доверенный сертификат корневого центра сертификации, используемый этим LDAP-сервером.

Внимание! Перед выполнением инструкции вам нужно получить у администратора контроллера домена необходимый сертификат в виде файла X.509 в кодировке Base64.

Примечание. В случае многосерверной конфигурации сертификат должен устанавливаться на основной узел PT Sandbox.

► Чтобы установить доверенный сертификат для LDAPS,

выполните команду:

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

Например:

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

Параметры будут применены, появится сообщение `Please wait a few minutes while the system components are restarted`.

Примечание. Повторное выполнение команды заменяет ранее установленный сертификат.

Доверенный сертификат для LDAPS установлен.

Теперь вы можете перейти к настройке подключения к LDAP-серверу.

12.5.2. Настройка подключения к LDAP-серверу

Если вы используете стандартный (встроенный в продукт) PT MC и связь с LDAP-сервером должна осуществляться через зашифрованное соединение (LDAPS), перед выполнением инструкции нужно установить доверенный сертификат корневого центра сертификации (см. раздел 12.5.1), используемый этим LDAP-сервером.

► Чтобы настроить подключение к LDAP-серверу:

1. Войдите в сервис управления пользователями и доступом (см. раздел 12.2).
2. В главном меню в разделе **Пользователи** выберите пункт **Настройка LDAP-подключений**.

   Откроется страница **Настройка LDAP-подключений**.
3. В панели инструментов нажмите кнопку **Добавить подключение**.

   Откроется страница **Новое LDAP-подключение**.
4. В поле **Название** введите название LDAP-подключения.
5. В блоке параметров **Серверы** в поле **Адрес** введите IP-адрес или полное доменное имя (FQDN) LDAP-сервера.

   Примечание. Если требуется устанавливать защищенное соединение с LDAP-сервером, адрес необходимо вводить в зависимости от типа доверенного сертификата (он выпускается или для IP-адреса, или для полного доменного имени (FQDN)).
6. В поле **Порт** введите номер порта.
7. Если требуется устанавливать защищенное соединение с LDAP-сервером, установите флажок **SSL**.

   Примечание. Вы можете добавлять дополнительные серверы по кнопке +. При потере соединения с одним сервером запрос аутентификации может быть обработан другим сервером.
8. В поле **Домены** введите DNS-имя домена, NetBIOS-имя домена или UPN-суффикс.

Примечание. Вы можете автоматически загрузить имена доменов и параметры базы поиска, нажав кнопку **Запросить данные с сервера** и указав данные учетной записи с правами доступа на чтение данных о пользователях.

9. Если вам нужно проверить соединение с указанными вами LDAP-серверами, нажмите кнопку **Проверить соединение**.
10. Нажмите кнопку **Добавить**.

Подключение к LDAP-серверу настроено.

12.5.3. Настройка синхронизации с Microsoft Active Directory

PT MC может создавать учетную запись пользователя при его первом успешном входе в продукт. Для включения этой возможности нужно после настройки LDAP-подключения настроить синхронизацию с Microsoft Active Directory. Логин, пароль, а также группы пользователя, соответствующие его ролям, хранятся в Microsoft Active Directory и не могут быть изменены в PT MC. Персональная и организационная информация также по умолчанию загружается из Microsoft Active Directory, но может быть указана в PT MC для каждого пользователя отдельно.

Перед настройкой синхронизации необходимо создать в Microsoft Active Directory учетную запись с правами на чтение данных о пользователях и группах пользователей.

► Чтобы настроить синхронизацию с Microsoft Active Directory:

1. Войдите в сервис управления пользователями и доступом (см. раздел 12.2).
2. В главном меню в разделе **Пользователи** выберите пункт **Настройка LDAP-подключений**.

   Откроется страница **Настройка LDAP-подключений**.
3. Выберите LDAP-подключение.
4. В панели инструментов нажмите кнопку **Изменить параметры**.

   Откроется страница **Изменение параметров LDAP-подключения**.
5. Включите синхронизацию с Active Directory.
6. Если необходимо, включите синхронизацию по расписанию и по ссылке настройте расписание.

   Примечание. Синхронизация также может быть запущена вручную на странице **Настройка LDAP-подключений**.
7. В блоке параметров **Соответствие ролей и групп** нажмите кнопку **Получить список групп** и в раскрывающихся списках выберите группы Microsoft Active Directory, соответствующие ролям пользователей.
8. Нажмите кнопку **Сохранить**.

Синхронизация с Microsoft Active Directory настроена.

12.6. Роли пользователей

В PT Sandbox используется ролевая модель управления доступом. Доступны следующие роли пользователей: администратор, специалист по безопасности и пользователь. При создании учетной записи можно назначить ей одновременно несколько ролей. Например, вы можете создать еще одну учетную запись суперпользователя, назначив ей все три роли.

Таблица 14. Доступные для пользователей страницы и привилегии

Страницы и привилегии	**Роль пользователя**		
	Администратор	**Специалист по безопасности**	**Пользователь**
Получение системных уведомлений	Да	—	—
Получение уведомлений безопасности	—	Да	—
Страница **Сводка**	—	Да	—
Просмотр сводки	—	Да	—
Страница **Задания**	Да	Да	Да
Создание заданий на проверку	Да	Да	Да
Доступ к своим результатам проверки	Да	Да	Да
Доступ ко всем результатам проверки	—	Да	—
Страница **Объекты**	Да	Да	Да
Просмотр информации о файле	Да	Да	Да
Управление метками и комментариями файлов	Да	Да	Да
Просмотр списка всех файлов	—	Да	—
Просмотр истории проверки файла	—	Да	—
Скачивание файлов	—	Да	—
Страница **Экспертиза PT**	Да	Да	—
Страница **Антивирусы**	Да	Да	—
Просмотр информации об антивирусах	Да [2]	Да	—
Просмотр статистики антивирусов	—	Да	—
Страница **Образы ВМ**	—	Да	—

2 Доступна установка дополнительных средств проверки.

Страницы и привилегии	Роль пользователя		
	Администратор	Специалист по безопасности	Пользователь
Страница **Черный список**	—	Да	—
Страница **Белый список**	—	Да	—
Страница **Источники**	Да	Да	—
Изменение параметров проверки	—	Да	—
Страница **Основные параметры**	Да	Да	—
Мониторинг текущего состояния системы	Да	Да	—
Изменение параметров системы	Да	—	—
Страница **Токены доступа**	Да	Да	—
Страница **Обновления**	Да	—	—
Страница **Лицензия**	Да	—	—

12.7. 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 пользователями и доступом (см. раздел 12.2).
2. В панели инструментов нажмите кнопку **Добавить пользователя**.

   Откроется страница **Новый пользователь**.
3. Заполните необходимые поля.
4. В блоке параметров **Роли в приложениях** в раскрывающемся списке с названием PT Sandbox выберите **Admin**.
5. Нажмите кнопку **Создать**.

Учетная запись администратора PT Sandbox создана.

13. Первоначальная настройка PT Sandbox

После развертывания PT Sandbox вы можете выполнить дополнительные действия для первоначальной настройке продукта.

В этом разделе

13.1. 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.

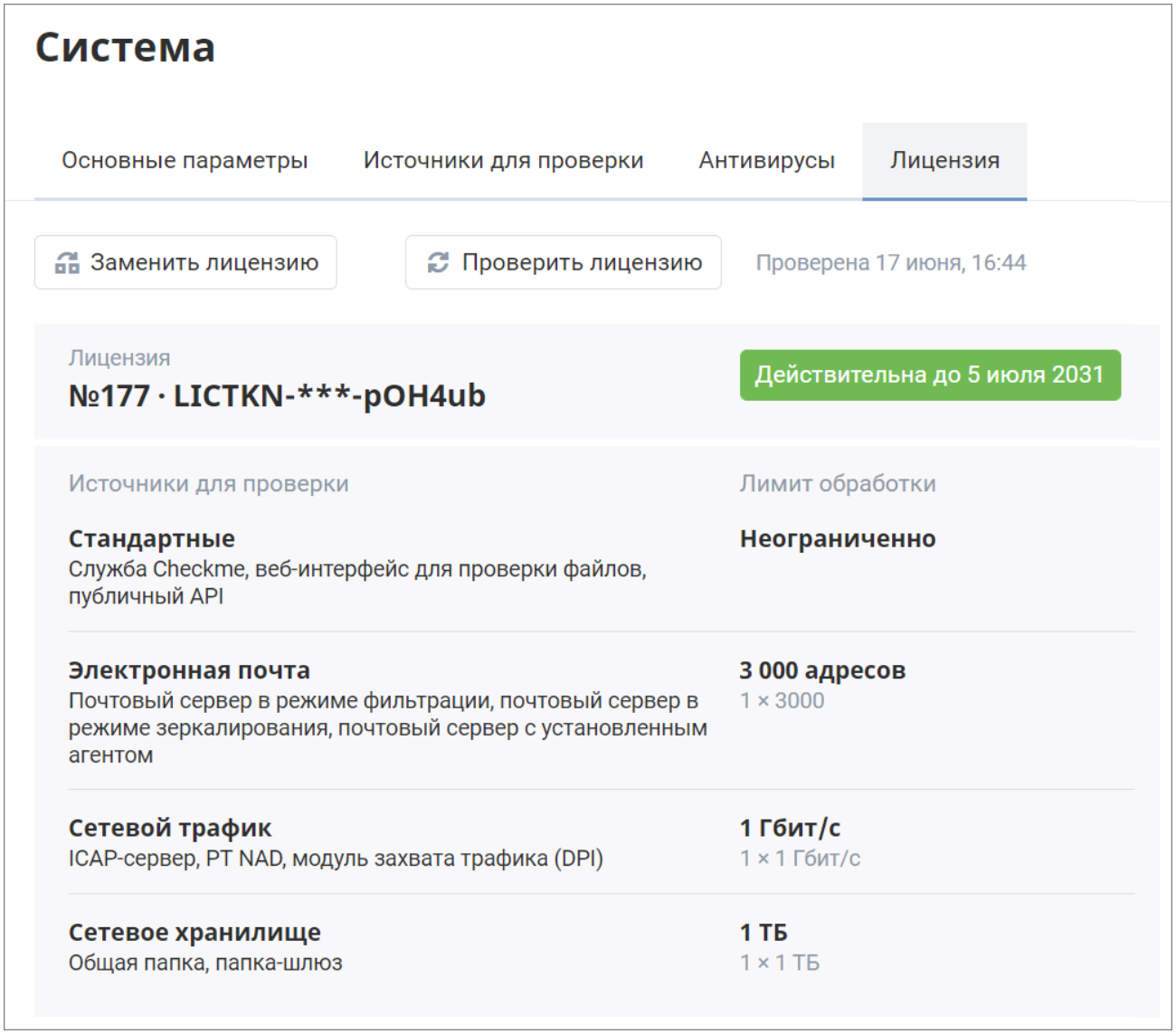

Рисунок 41. Просмотр информации о лицензии

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 Positive Technologies.

Если веб-интерфейс недоступен, вы можете активировать лицензию в консоли на узле с PT Sandbox (в многосерверной конфигурации — на основном узле).

► Чтобы активировать лицензию с помощью консоли,

выполните команду:

```
sudo ptmsctl license apply --serial-number '<Серийный номер лицензии>'
```

Например:

```
sudo ptmsctl license apply --serial-number 'xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-
xxxxxx-xxxxxx-xxxxxx-xxxxxx'
```

Появится сообщение `License was successfully replaced`.

Лицензия активирована.

Для проверки лицензии в консоли можно использовать команду `sudo ptmsctl license info`.

13.2. 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 ptmsctl product settings apply --proxy-server 'http://<IP-адрес прокси-
   сервера>:<Порт>' --proxy-user '<Логин>' --proxy-password '<Пароль>'
   ```

   Например:

   ```
   sudo 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:

   - Если вы настраиваете основной узел:

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

   - Если вы настраиваете дополнительный узел:

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

     Появится сообщение `Kubernetes successfully installed`.

► Чтобы удалить параметры прокси-сервера:

1. На основном узле выполните команду:

   ```
   sudo ptmsctl product settings apply --proxy-server ""
   ```

   Появится сообщение `Settings applied`.

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

   - Если вы настраиваете основной узел:

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

- Если вы настраиваете дополнительный узел:

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

  Появится сообщение `Kubernetes successfully installed`.

13.3. 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://sandbox.example/ --serial-number '...' --proxy-ca-crt /opt/ptms/user_certs/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 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 ptmsctl product settings apply --proxy-ca-crt /opt/ptms/user_certs/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 '<Логин>' --proxy-pass '<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-pass '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 ptmsctl product settings apply --without-proxy-ca-crt
```

Появится сообщение `Settings applied`.

13.4. Установка SSL-сертификата

Чтобы пользователи PT Sandbox имели доступ к его веб-интерфейсу через HTTPS-соединение, вам нужно установить в PT Sandbox SSL-сертификат, который должен соответствовать следующим требованиям:

— использует алгоритм подписи SHA-256;

— использует алгоритм RSA для шифрования ключей;

— длина закрытого ключа — не менее 2048 бит;

— включает область применения сертификата Digital Signature или Key Encipherment;

— в расширении Subject Alternative Name (SAN) содержит запись о доменном имени или IP-адресе сервера с установленным веб-интерфейсом PT Sandbox.

Установка SSL-сертификата выполняется на основном узле (на первом из узлов, на которых установлен PT Sandbox). Перед установкой вам нужно убедиться, что на этом узле есть:

— файл SSL-сертификата открытого ключа;

— файл закрытого ключа, который расшифрован без SSL-сертификата в нем;

— файл .pem сертификата издателя, выпустившего SSL-сертификат.

► Чтобы установить SSL-сертификат,

выполните команду:

```
sudo ptmsctl web-interface https-certs apply --crt <Файл SSL-сертификата открытого ключа>
--key <Файл закрытого ключа> --ca-bundle <Файл сертификата издателя>
```

Например:

```
sudo ptmsctl web-interface https-certs apply --crt /home/user/your_company.crt --key /
home/user/your_company.key --ca-bundle /etc/ssl/certs/root_ca.pem
```

Параметры будут применены, появится сообщение `Please wait a few minutes while the system components are restarted`.

SSL-сертификат установлен.

13.5. Подключение доменного имени к PT Sandbox

После подключения доменного имени веб-интерфейс PT Sandbox будет доступен не только по IP-адресу, но и по доменному имени.

Перед выполнением инструкции вам нужно настроить в сетевой инфраструктуре организации сопоставление выбранного доменного имени с IP-адресом основного узла PT Sandbox или с виртуальным IP-адресом службы Keepalived (для конфигураций с отказоустойчивым кластером).

► Чтобы подключить доменное имя к PT Sandbox,

выполните команду:

```
sudo ptmsctl web-interface domain-name apply <Доменное имя>
```

Например:

```
sudo ptmsctl web-interface domain-name apply sandbox.example.org
```

Параметры будут применены, появится сообщение `Please wait a few minutes while the system components are restarted`.

Доменное имя подключено к PT Sandbox.

13.6. Отключение передачи информации о работе PT Sandbox

PT Sandbox собирает и передает в Positive Technologies следующую информацию о заданиях на проверку объектов:

- Идентификаторы заданий.
- Данные о поступивших на проверку файлах (имя, размер, MIME-тип, хеш-суммы).
- Информацию об используемых средствах проверки и антивирусах (название, версия, примененное правило).
- Информацию об используемых при проверке образах виртуальных машин.
- Результат проверки (название и класс обнаруженного вредоносного ПО).

Эта информация необходима для повышения качества экспертизы и дальнейшего развития PT Sandbox. Вся информация передается в обезличенном и зашифрованном виде.

Если политика информационной безопасности вашей организации запрещает передачу такой информации в сторонние компании, вы можете отключить передачу информации. Для получения инструкций обратитесь в техническую поддержку Positive Technologies.

13.7. Проверка цифровой подписи при поведенческом анализе файлов

При проверке файлов форматов CAB, DLL, EXE, MSI методом поведенческого анализа PT Sandbox может проверять их цифровые подписи. Подтверждение цифровой подписи указывает на то, что файл не был изменен и сертификат удостоверяющего центра не был отозван. Высока вероятность, что такой файл не является вредоносным, но окончательное решение о результате проверки выносится на основании всех используемых методов. Проверка цифровой подписи файлов может выполняться в образах виртуальных машин Windows, но по умолчанию отключена.

► Чтобы включить проверку цифровой подписи при поведенческом анализе файлов,

выполните команду:

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

Проверка цифровой подписи включена.

► Чтобы отключить проверку цифровой подписи файлов при поведенческом анализе,

выполните команду:

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

Проверка цифровой подписи отключена.

14. 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 Management and Configuration (PT MC), который обеспечивает механизм единого входа (технология single sign-on) в продукты Positive Technologies.

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. Если вы используете конфигурацию PT Sandbox с отказоустойчивым кластером, вместо IP-адреса основного узла нужно ввести виртуальный IP-адрес службы Keepalived.

   Откроется страница входа в PT Sandbox.

   Примечание. Если разрешена анонимная проверка файлов, откроется страница для такой проверки.

2. Нажмите кнопку **Войти**.

   Откроется страница входа в PT MC.

3. Выполните одно из следующих действий:

   - Если вы входите под локальной учетной записью, то на вкладке **Локальный** укажите логин локальной учетной записи.
   - Если вы входите под доменной учетной записью, то на вкладке **LDAP** укажите логин доменной учетной записи.

4. В поле **Пароль** введите пароль вашей учетной записи.

5. Нажмите кнопку **Войти**.

   Откроется страница **Задания**.

   Примечание. Если вы выполняете первый вход после обновления версии PT Sandbox, откроется страница для принятия лицензионного соглашения.

15. 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

15.1. Главное меню

В верхней части любой страницы интерфейса PT Sandbox расположено главное меню. Главное меню PT Sandbox является ключевым элементом управления в интерфейсе PT Sandbox и обеспечивает доступ к основным функциям PT Sandbox.

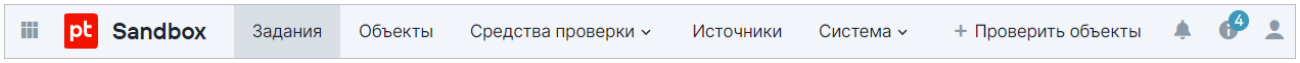

Рисунок 42. Главное меню

В левой части главного меню находится кнопка для перехода в другие приложения Positive Technologies, зарегистрированные в сервисе управления пользователями и доступом PT Management and Configuration (PT MC).

Главное меню содержит разделы для перехода к страницам интерфейса:

— **Задания** — переход к странице со списком заданий на проверку;

— **Объекты** — доступ к хранилищу объектов;

— **Средства проверки** — просмотр и управление средствами, используемыми PT Sandbox для проверки объектов:

  - **Экспертиза PT** — переход к странице для просмотра средств проверки, которые разработаны специалистами компании Positive Technologies;
  - **Антивирусы** — переход к странице для управления антивирусами сторонних разработчиков, которые используются при проверке файлов.

— **Источники** — просмотр и управление источниками, с которых объекты поступают на проверку;

— **Система** — управление и просмотр информации о PT Sandbox:

  - **Основные параметры** — переход к странице для настройки основных параметров работы PT Sandbox.
  - **Обновления** — просмотр информации о текущей версии PT Sandbox и ее обновление;
  - **Лицензия** — просмотр информации об активированной лицензии и ее замена.

В правой части главного меню расположены:

— Кнопка **Проверить объекты** для выборочной проверки объектов.

— Значок , по нажатию на который открывается Центр уведомлений (см. раздел 15.2).

  На значке отображается количество уведомлений о результатах проверки файлов и ссылок.

— Значок , по нажатию на который вы можете увидеть установленную версию PT Sandbox и версии, доступные для установки, получить информацию о состоянии компонентов PT Sandbox, скачать файлы журналов, перейти на сайт технической поддержки Positive Technologies.

— Значок , по нажатию на который вы можете просмотреть логин, с которым вы вошли в PT Sandbox, сменить тему оформления и язык интерфейса, а также завершить работу под текущей учетной записью.

15.2. 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.

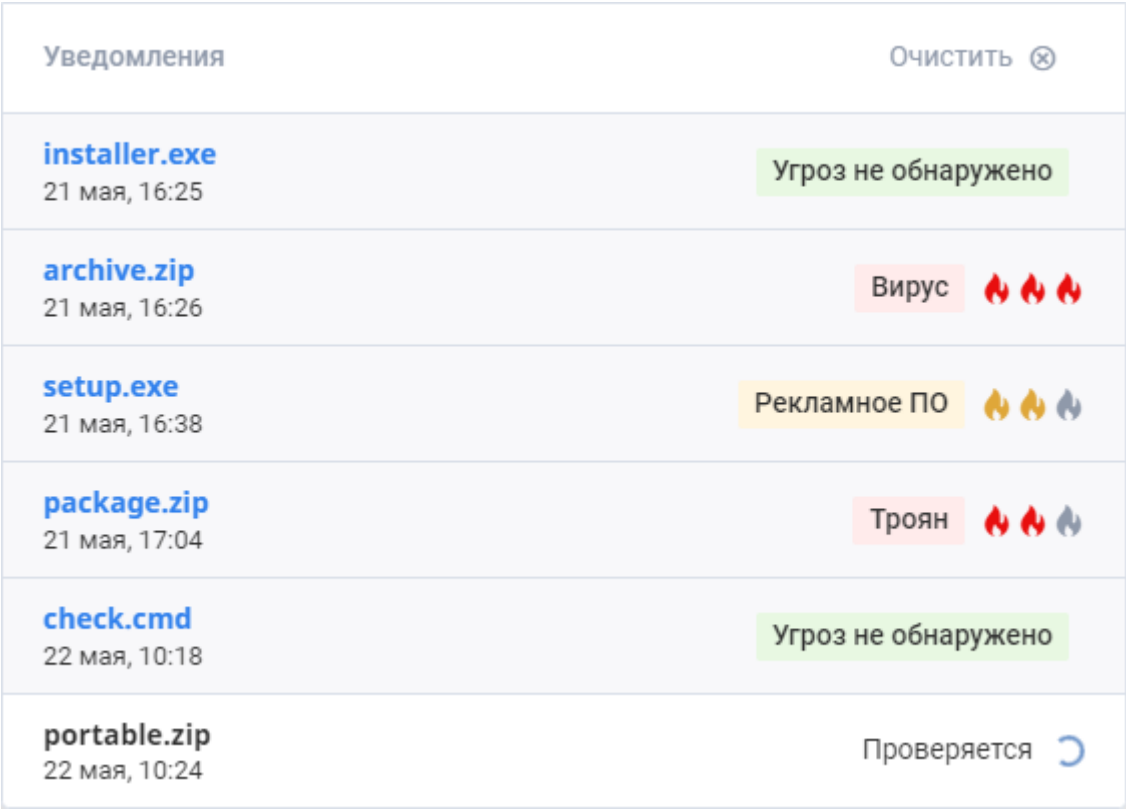

Рисунок 43. Центр уведомлений

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**.

15.3. Страница «Задания»

При выборе в главном меню раздела **Задания** открывается страница со списком заданий на проверку объектов.

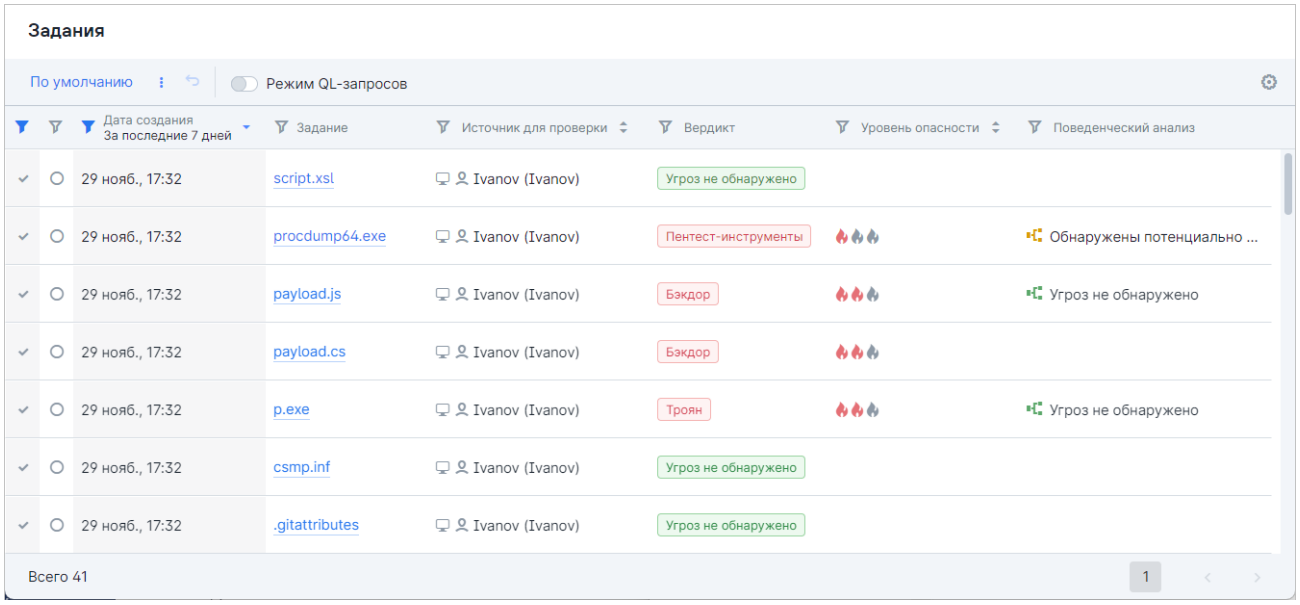

Рисунок 44. Список заданий на проверку

В панели инструментов страницы расположены:

— Кнопка **<Название фильтра>** для выбора фильтра. По кнопке раскрывается меню, в котором вы можете выбрать один из сохраненных фильтров или фильтр по умолчанию. В верхней части меню доступно поле для быстрого поиска фильтра.

— Кнопка ⋮ для выбора дополнительных действий с фильтром. После настройки параметров фильтрации по этой кнопке вы можете сохранить их как новый фильтр или сбросить все изменения. После изменения параметров созданного ранее фильтра по этой кнопке вы можете сохранить для него измененные параметры фильтрации, сохранить параметры фильтрации как новый фильтр, сбросить все изменения, переименовать фильтр или удалить его.

— Кнопка ↩ для выбора фильтра по умолчанию.

— Переключатель **Режим QL-запросов** для создания фильтра с помощью языка запросов QL. В этом режиме появляется поле для ввода QL-запросов, кнопки ‹ и › для выбора предыдущего или следующего запроса и кнопка 🕘 для просмотра списка выполненных ранее запросов.

— Кнопка ⚙ для выбора столбцов таблицы.

В рабочей области страницы расположена таблица со списком заданий на проверку. По ссылке в строке задания вы можете открыть карточку задания. В зависимости от вашего выбора, таблица может содержать следующие столбцы с информацией о задании:

— **Статус проверки** — в столбце отображается значок статуса проверки задания:

● — проверка не выполнена;

◔ — проверка выполнена частично;

— проверка завершена;

— выполняется проверка.

— **Действие** — в столбце отображается значок, показывающий, был ли файл пропущен в информационную систему организации:

— заблокировано;

— пропущено;

— действие не совершено.

— **Карантин** — в столбце отображается значок, показывающий, был ли файл помещен в карантин:

— в карантине;

— удалено из карантина;

Отсутствие значка указывает на то, что файл не помещался в карантин.

— **Дата создания** — в столбце указаны дата и время добавления задания. По умолчанию в таблице отображаются задания за последние 7 дней.

— **Задание** — в столбце указано название проверяемого объекта.

— **Источник для проверки** — в столбце указан источник, от которого объект поступил на проверку:

Веб-интерфейс — имя пользователя, который отправил объект на проверку через веб-интерфейс PT Sandbox, и логин его учетной записи;

Хранилище (повторная проверка) — хранилище объектов при повторной проверке объектов из хранилища;

— почтовый сервер или служба Checkme;

— ICAP-сервер или PT NAD;

— общая папка или папка-шлюз;

API — стороннее приложение через API.

— **Вердикт** — в столбце указан вердикт по заданию и, если обнаружены объекты с вредоносным ПО, тип обнаруженного ПО.

— **Уровень опасности** — в столбце отображается значок, показывающий уровень опасности обнаруженного вредоносного ПО. Выделяются три уровня для опасного ПО — и три уровня для потенциально опасного ПО — .

— **Поведенческий анализ** — в столбце отображается значок, показывающий результат поведенческого анализа:

— обнаружены опасные файлы;

— обнаружены потенциально опасные файлы;

— поведенческий анализ выполнен частично или с ошибками;

— угроз не обнаружено;

Отсутствие значка указывает на то, что поведенческий анализ не проводился.

— **Откуда > Куда** — в столбце указана информация об отправителе объекта:

- Если объект отправлен через веб-интерфейс PT Sandbox, в столбце указан логин учетной записи пользователя.
- Если объект поступил на проверку через службу Checkme, — адрес электронной почты, с которого пришло письмо.
- Если объект поступил с почтового сервера, — адреса электронной почты отправителя и получателя письма.

Для других источников информация в столбце не указывается.

15.4. Страница «Объекты»

При выборе в главном меню раздела **Объекты** открывается страница со списком объектов заданий.

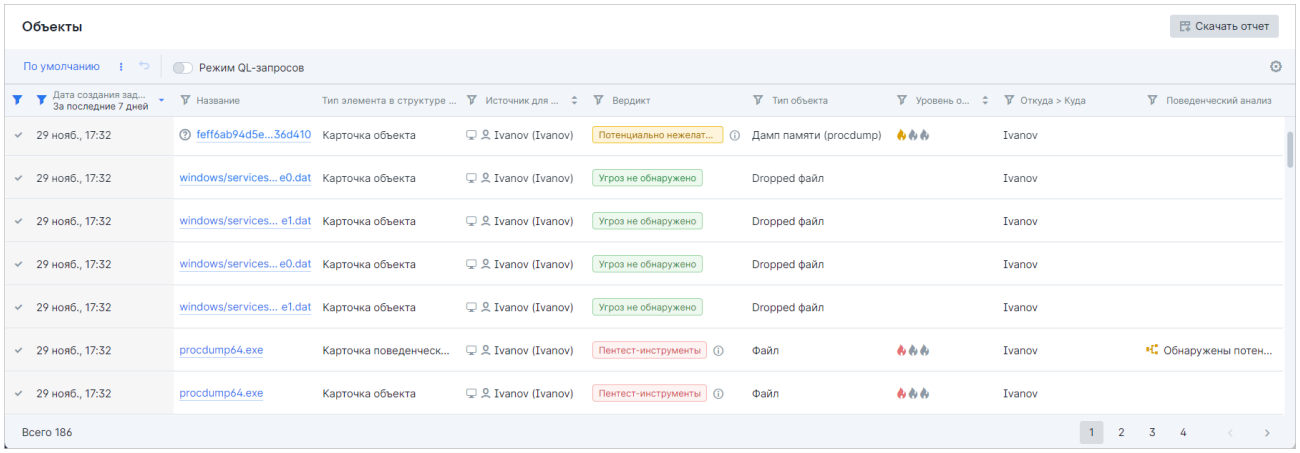

Рисунок 45. Список проверенных объектов

Вверху страницы расположена кнопка **Скачать отчет** для сохранения списка проверенных объектов в файле формата CSV.

В панели инструментов страницы расположены:

— Кнопка **<Название фильтра>** для выбора фильтра. По кнопке раскрывается меню, в котором вы можете выбрать один из сохраненных фильтров или фильтр по умолчанию. В верхней части меню доступно поле для быстрого поиска фильтра.

— Кнопка ⋮ для выбора дополнительных действий с фильтром. После настройки параметров фильтрации по этой кнопке вы можете сохранить их как новый фильтр или сбросить все изменения. После изменения параметров созданного ранее фильтра по этой кнопке вы можете сохранить для него измененные параметры фильтрации, сохранить параметры фильтрации как новый фильтр, сбросить все изменения, переименовать фильтр или удалить его.

— Кнопка ↩ для выбора фильтра по умолчанию.

— Переключатель **Режим QL-запросов** для создания фильтра с помощью языка запросов QL. В этом режиме появляется поле для ввода QL-запросов, кнопки < и > для выбора предыдущего или следующего запроса и кнопка 🕘 для просмотра списка выполненных ранее запросов.

— Кнопка ⚙ для выбора столбцов таблицы.

В рабочей области страницы расположена таблица со списком проверенных объектов. По ссылке в строке объекта вы можете открыть карточку объекта. В зависимости от вашего выбора таблица может содержать следующие столбцы с информацией об объектах:

— **Статус проверки** — в столбце отображается значок статуса проверки объекта:

■ — проверка не выполнена;

— проверка выполнена частично;

✓ — проверка завершена;

⌛ — выполняется проверка.

— **Дата создания задания** — в столбце указаны дата и время добавления задания на проверку объекта. По умолчанию в таблице отображаются объекты заданий, созданных за последние 7 дней.

— **Название** — в столбце указано название объекта, с которым он впервые поступил на проверку.

— **Тип элемента в структуре задания** — в столбце указано, является ли этот элемент карточкой объекта или карточкой поведенческого анализа.

— **Источник для проверки** — в столбце указан источник, от которого объект поступил на проверку:

Веб-интерфейс — имя пользователя, который отправил объект на проверку через веб-интерфейс PT Sandbox, и логин его учетной записи;

Хранилище (повторная проверка) — хранилище объектов при повторной проверке объектов из хранилища;

— почтовый сервер или служба Checkme;

— ICAP-сервер или PT NAD;

— общая папка или папка-шлюз;

API — стороннее приложение через API.

— **Вердикт** — в столбце указан вердикт по объекту. Если в объекте обнаружено вредоносное ПО, указан его тип. По кнопке ⓘ вы можете посмотреть, какими средствами проверки вредоносное ПО было обнаружено.

— **Тип объекта** — в столбце указан тип объекта.

— **Уровень опасности** — в столбце отображается значок, показывающий уровень опасности обнаруженного вредоносного ПО. Выделяются три уровня для опасного ПО — и три уровня для потенциально опасного ПО — .

— **Откуда > Куда** — в столбце указана информация об отправителе объекта:

- Если объект отправлен через веб-интерфейс PT Sandbox, в столбце указан логин учетной записи пользователя.
- Если объект поступил на проверку через службу Checkme, — адрес электронной почты, с которого пришло письмо.
- Если объект поступил с почтового сервера, — адреса электронной почты отправителя и получателя письма.

Для других источников информация в столбце не указывается.

— **Поведенческий анализ** — в столбце отображается значок, показывающий результат поведенческого анализа:

— обнаружены опасные файлы;

— обнаружены потенциально опасные файлы;

— поведенческий анализ выполнен частично или с ошибками;

— угроз не обнаружено;

Отсутствие значка указывает на то, что поведенческий анализ не проводился.

— **Идентификатор задания** — в столбце указан идентификатор задания, по которому проверен объект.

— **Объект получен** — в столбце указано, откуда получен объект:

- **От источника** — объект поступил на проверку от источника.
- **Из архива** — файл получен в результате распаковки архива.

- **Из письма** — файл является телом или вложением письма.
- **Из тела письма** — ссылка извлечена из тела письма.
- **Из файла** — ссылка извлечена из файла, тела письма или вложения.
- **По ссылке** — файл скачан по ссылке.
- **Из HTTP-сообщения** — файл получен в результате HTTP-запроса.
- **В результате ПА** — объект является артефактом поведенческого анализа.

— **Причина вердикта** — для объектов с угрозами в столбце указаны средства проверки, которыми эта угроза была обнаружена. Если указано **Наследуемый вердикт**, то причиной вердикта стал результат проверки дочерних объектов.

— **MIME-тип** — в столбце указан формат файла, записанный в виде MIME-типа.

— **SHA-256**, **SHA-1**, **MD5** — в столбцах указана хеш-сумма файла в различных форматах.

— **Метки** — в столбце указаны особенности объекта.

— **Черный и белый списки** — в столбце указано, находился ли файл в черном или белом списке на момент проверки:

В черном списке;

В белом списке;

Если ничего не указано, то файл на момент проверки отсутствовал в списках.

— **Название образа ВМ** — в столбце указано название образа ВМ, на котором выполнялся поведенческий анализ файла.

— **Продолжительность анализа** — в столбце указано время выполнения поведенческого анализа файла в минутах.

— **Поведенческий анализ (результат проверки)** — в столбце указан тип вредоносного ПО, обнаруженного при поведенческом анализе..

— **Поведенческий анализ (обнаруженное ВПО)** — в столбце указано название вредоносного ПО, обнаруженного при поведенческом анализе.

— **Потенциально опасное поведение** — в столбце указана информация о подозрительном поведении файла, обнаруженном при поведенческом анализе.

— **Анализ с перезагрузкой ОС** — в столбце указан режим поведенческого анализа файла.

— **Родительский процесс** — в столбце указано название родительского процесса, связанного с вредоносным ПО, которое было обнаружено при поведенческом анализе.

— **<Средство проверки> (результат проверки)** — в столбце указан тип вредоносного ПО, обнаруженного этим средством проверки.

— **<Средство проверки> (обнаруженное ВПО)** — в столбце указано название вредоносного ПО, обнаруженного этим средством проверки.

15.5. Карточка задания и карточки объектов

Страница карточки задания открывается по нажатию на строку таблицы на странице **Задания**. Карточка задания содержит карточки отдельных объектов, проверенных в ходе выполнения этого задания. Страница карточки объекта открывается из карточки задания или по нажатию на строку таблицы на странице **Объекты**.

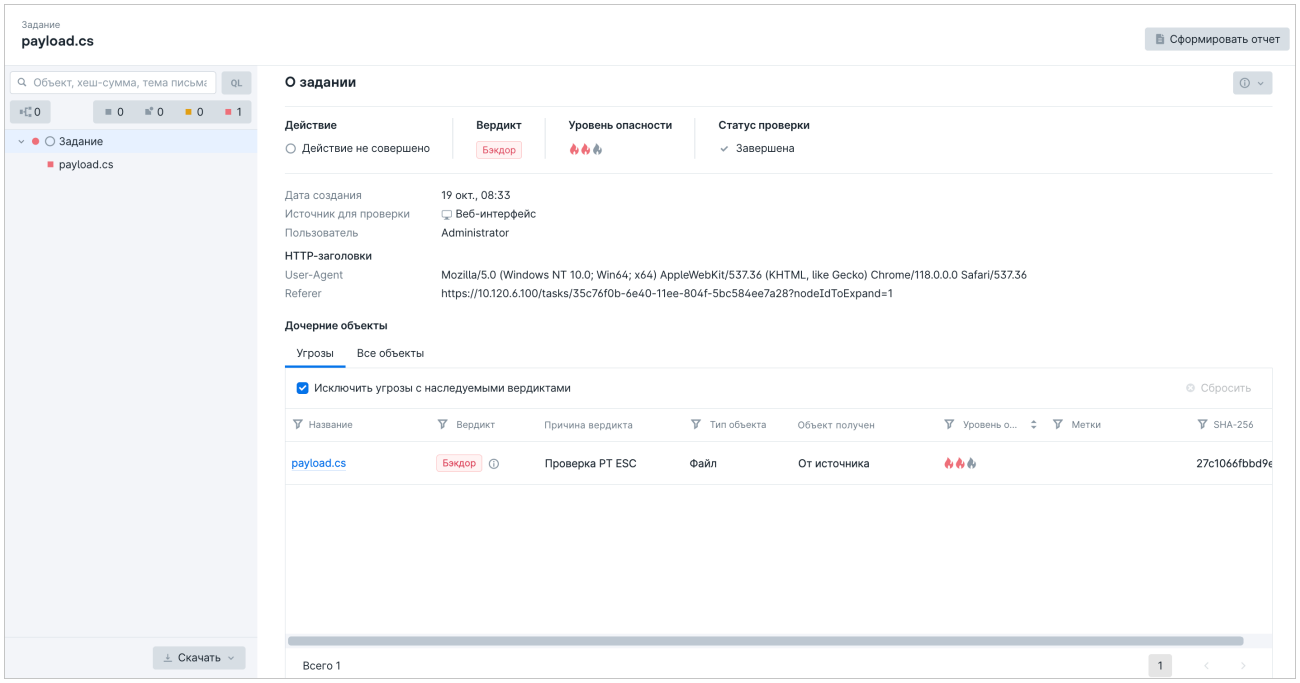

Рисунок 46. Карточка задания

В верхней части страницы с карточкой задания или карточкой объекта указывается название задания и находится кнопка **Сформировать отчет** для выпуска отчета по заданию. В левой части страницы расположена панель для выбора объектов задания. В панели расположены:

— Блок поиска и фильтрации. В этом блоке вы можете искать объекты через обычный поиск или с помощью языка запросов. Здесь вы также можете отфильтровать объекты, используя следующие кнопки:

  - Показать только объекты поведенческого анализа;
  - Показать непроверенные объекты;
  - Показать частично проверенные объекты;
  - Показать потенциально опасные объекты;
  - Показать опасные объекты.

— Иерархический список файлов задания и объектов поведенческого анализа.

— Кнопка **Скачать**, которая позволяет скачать из хранилища файлы, связанные с заданием на проверку.

Наполнение рабочей области зависит от элемента, выбранного в списке.

Задание

При выборе в иерархическом списке задания в рабочей области отображаются:

— Кнопка ⓘ с раскрывающимся списком для скачивания диагностической информации для анализа ложных срабатываний.

— Результат проверки задания: действие, вердикт по всему заданию, который выносится на основании вердиктов по каждому объекту задания, присвоенный уровень опасности и статус проверки.

— Общая информация о задании: дата создания задания, источник, с которого была инициирована проверка, пользователь, который запустил проверку.

— Дополнительная информация по источнику для проверки:

- HTTP-заголовки (при проверке через веб-интерфейс PT Sandbox);
- SMTP-адреса (при проверке через почтовые источники).

— Таблица с дочерними объектами. Вы можете отфильтровать объекты в таблице, а также посмотреть информацию о вердикте, нажав ⓘ. В таблице отображаются:

- все объекты с угрозами на вкладке **Угрозы**. Если требуется, вы можете отключить отображение угроз с наследуемыми вердиктами, установив соответствующий флажок. При нажатии на название объекта открывается его карточка, в которой вы можете посмотреть информацию о проверке объекта.
- все объекты задания на вкладке **Все объекты**. Если требуется, вы можете включить отображение только дочерних объектов первого уровня, установив соответствующий флажок. При нажатии на название объекта открывается его карточка, в которой вы можете посмотреть информацию о проверке объекта.

При выборе задания, содержащего письмо от почтовых источников «Почтовый сервер с установленным агентом» и «Почтовый сервер в режиме фильтрации» в рабочей области задания также отображается ссылка **Показать детали доставки**, по которой открывается боковая панель с информацией о доставке письма SMTP-сервером.

Файл

При выборе файла в иерархическом списке в рабочей области отображаются:

— Кнопка **Перепроверить** для повторной проверки файла.

— Кнопка ⓘ с раскрывающимся списком для скачивания диагностической информации для анализа ложных срабатываний.

— Свойства файла.

— Ссылка **Найти этот объект в других заданиях**, по которой открывается новая вкладка браузера с разделом **Объекты** главного меню — списком заданий, в которых проверялся объект.

— Ссылка **Проверить объект по базе VirusTotal**, по которой открывается новая вкладка с результатами проверки объекта в сторонней базе.

— Вердикт по файлу и статус проверки.

— Информация о том, находились ли хеш-суммы файла в черном или белом списке на момент проверки. Нажав на ссылку **Найти файл в списках**, вы можете обновить информацию о нахождении файла в списках, а также добавить его в черный или белый список.

— Результаты статического и поведенческого анализа файла.

— Результаты проверки в соответствии с дополнительными критериями определения потенциально опасных файлов.

— Таблица с дочерними объектами. Вы можете отфильтровать объекты в таблице, а также посмотреть информацию о вердикте, нажав ⓘ. В таблице отображаются:

- все объекты с угрозами на вкладке **Угрозы**. Если требуется, вы можете отключить отображение угроз с наследуемыми вердиктами, установив соответствующий флажок. При нажатии на название объекта открывается его карточка, в которой вы можете посмотреть информацию о проверке объекта.
- все объекты задания на вкладке **Все объекты**. Если требуется, вы можете включить отображение только дочерних объектов первого уровня, установив соответствующий флажок. При нажатии на название объекта открывается его карточка, в которой вы можете посмотреть информацию о проверке объекта.

Письмо

При выборе в иерархическом списке письма в рабочей области отображаются:

— Кнопка **Перепроверить** для повторной проверки письма и всех его вложений.

— Свойства письма.

— Тема и текст сообщения письма. Для текста сообщения письма отображаются ссылки **Показать** и **Скрыть**, которые позволяют управлять отображением содержимого, и ссылка **HTML-версия**, по которой сообщение письма открывается в HTML-формате (при наличии).

— Ссылка **Найти этот объект в других заданиях**, по которой открывается новая вкладка браузера с разделом **Объекты** главного меню—списком заданий, в которых проверялся объект.

— Ссылка **Проверить объект по базе VirusTotal**, по которой открывается новая вкладка с результатами проверки объекта в сторонней базе.

— Вердикт по файлу и статус проверки.

— Результат статического анализа файла.

— Информация о том, находились ли хеш-суммы файла письма в черном или белом списке на момент проверки. Нажав на ссылку **Найти файл в списках**, вы можете обновить информацию о нахождении файла письма в списках, а также добавить его в черный или белый список.

— Результаты проверки в соответствии с дополнительными критериями определения потенциально опасных файлов.

— Таблица с дочерними объектами. Вы можете отфильтровать объекты в таблице, а также посмотреть информацию о вердикте, нажав ⓘ. В таблице отображаются:

- все объекты с угрозами на вкладке **Угрозы**. Если требуется, вы можете отключить отображение угроз с наследуемыми вердиктами, установив соответствующий флажок. При нажатии на название объекта открывается его карточка, в которой вы можете посмотреть информацию о проверке объекта.
- все объекты задания на вкладке **Все объекты**. Если требуется, вы можете включить отображение только дочерних объектов первого уровня, установив соответствующий флажок. При нажатии на название объекта открывается его карточка, в которой вы можете посмотреть информацию о проверке объекта.

Ссылка

При выборе в иерархическом списке ссылки в рабочей области отображаются:

— Кнопка **Перепроверить** для повторной проверки ссылки.

— Кнопка **Скопировать** для копирования ссылки — объекта проверки.

— Свойства ссылки: исходная ссылка и средство проверки, с помощью которого она была обработана.

— Ссылка **Найти этот объект в других заданиях**, по которой открывается новая вкладка браузера с разделом **Объекты** главного меню — списком заданий, в которых проверялся объект.

— Вердикт по ссылке и статус проверки.

— Таблица с дочерними объектами. Вы можете отфильтровать объекты в таблице, а также посмотреть информацию о вердикте, нажав ⓘ. В таблице отображаются:

- все объекты с угрозами на вкладке **Угрозы**. Если требуется, вы можете отключить отображение угроз с наследуемыми вердиктами, установив соответствующий флажок. При нажатии на название объекта открывается его карточка, в которой вы можете посмотреть информацию о проверке объекта.
- все объекты задания на вкладке **Все объекты**. Если требуется, вы можете включить отображение только дочерних объектов первого уровня, установив соответствующий флажок. При нажатии на название объекта открывается его карточка, в которой вы можете посмотреть информацию о проверке объекта.

См. также

Страница «Задания» (см. раздел 15.3)

Страница «Объекты» (см. раздел 15.4)

15.6. Карточка поведенческого анализа

В карточке собрана вся информация и артефакты, которые были сформированы в ходе поведенческого анализа. В карточке вы можете найти и отфильтровать объекты поведенческого анализа, посмотреть диаграмму поведения файла и узнать результат поведенческого анализа. Открыть карточку поведенческого анализа можно через раздел **Объекты** главного меню, выбрав в столбце **Тип элемента в структуре задания** значение **Карточка поведенческого анализа**, или через раздел **Задания**, выбрав задание, для которого был проведен поведенческий анализ.

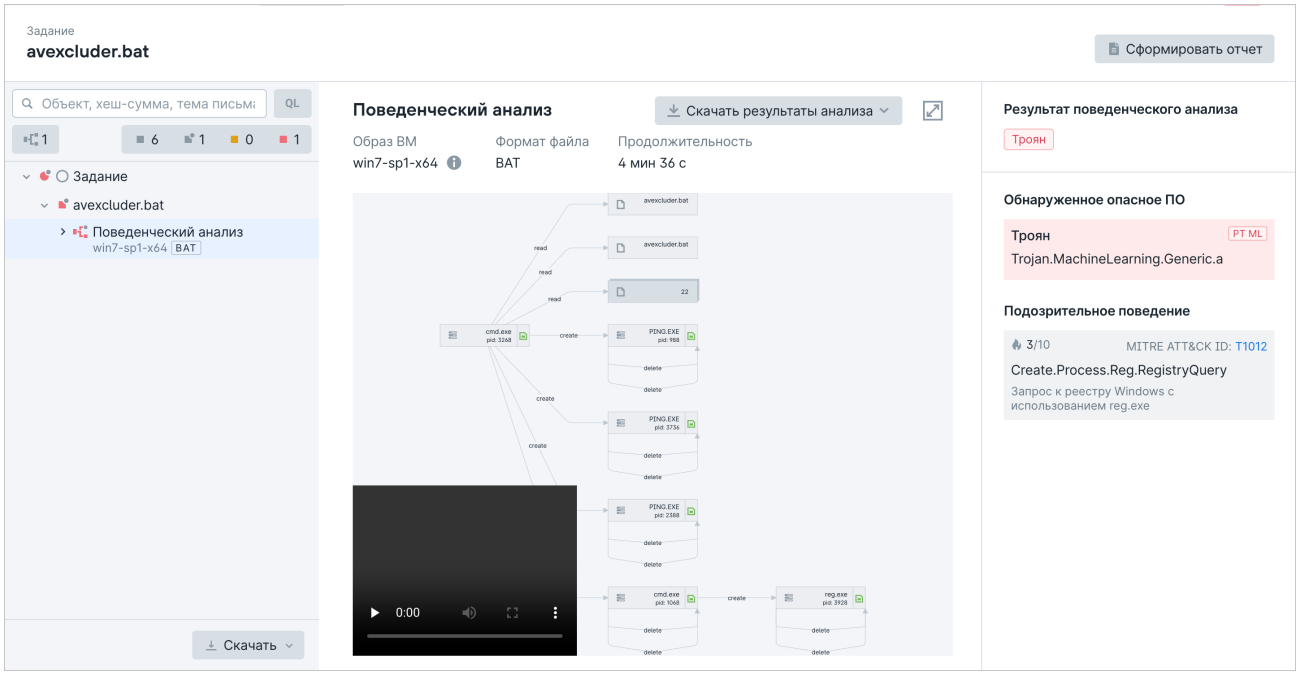

Рисунок 47. Карточка поведенческого анализа

Вверху страницы справа отображается кнопка **Сформировать отчет**, нажав которую можно создать отчет по проверенным объектам (см. раздел 21.2). Рабочая область карточки разделена на три панели.

В панели слева вы можете выбрать объекты поведенческого анализа. Эта панель состоит из следующих элементов:

— Блок поиска и фильтрации. В этом блоке вы можете искать объекты через обычный поиск или с помощью языка запросов. Здесь вы также можете отфильтровать объекты, используя следующие кнопки:

  - Показать только объекты поведенческого анализа;
  - Показать непроверенные объекты;
  - Показать частично проверенные объекты;
  - Показать потенциально опасные объекты;
  - Показать опасные объекты.

— Иерархический список файлов задания и объектов поведенческого анализа.

— Кнопка **Скачать**, которая позволяет скачать из хранилища файлы, связанные с заданием на проверку.

В центральной панели отображается информация об образе ВМ, формате файла, продолжительности наблюдения за файлом. В панели также расположены следующие элементы:

— Кнопка **Скачать результаты анализа**, нажав которую, вы можете выбрать, какие файлы нужно скачать.

— Диаграмма поведения файла. На диаграмме поведения файла отображаются объекты, которые обозначены прямоугольниками, и стрелки, которые показывают связи между объектами: создание, изменение, чтение данных или удаление. При нажатии на прямоугольник в правой панели страницы отображается информация об объекте. На диаграмме могут отображаться следующие типы объектов:

  — процесс (если для процесса проверялся дамп памяти, то для объекта также отображается значок);

  — файл или группа файлов;

  — обращение к реестру или группе реестров;

  — служба;

  IP — IP;

  — сокет;

  URL —сервер или гиперссылка;

  — сетевой пакет;

  — мьютекс;

  — именованный канал;

  —точка соединения, жесткая ссылка или символическая ссылка.

— Окно для просмотра видеозаписи поведения файла в ОС, если при проверке объекта не была отключена запись видео.

  Примечание. Вы можете увеличить масштаб диаграммы двойным щелчком мыши и управлять масштабом диаграммы колесом мыши. По нажатию кнопки вы можете расширить область диаграммы для удобства просмотра. При этом левая и правая панели страницы будут скрыты. Вы можете восстановить их, повторно нажав кнопку .

В правой панели страницы вы можете просмотреть информацию о выбранном объекте диаграммы. Если объект на диаграмме не выбран, то отображается информация о результате поведенческого анализа, которая разделена на следующие блоки:

— Блок **Результат поведенческого анализа**. В этом блоке отображается конечный результат поведенческого анализа — тип обнаруженной угрозы.

— Блок **Обнаруженное опасное ПО**. Блок отображается, если в ходе поведенческого анализа было обнаружено такое ПО. В карточке по каждому опасному ПО отображается его название и метод, с помощью которого оно было обнаружено при проверке.

  Примечание. Вы можете скопировать название обнаруженного вредоносного ПО, нажав кнопку .

— Блок **Подозрительное поведение**. В этом блоке по каждому обнаруженному подозрительному поведению отображается его описание, уровень опасности и идентификатор техники MITRE ATT&CK, при нажатии на который открывается страница с информацией о технике на сайте MITRE ATT&CK.

15.7. Страницы раздела «Средства проверки»

Используя пункты раздела **Средства проверки** главного меню, вы можете просматривать и настраивать различные средства, которые используются при проверке объектов в PT Sandbox.

В этом разделе

15.7.1. Страница «Экспертиза PT»

Для проверки объектов PT Sandbox может использовать средства проверки, разработанные специалистами компании Positive Technologies. Страница **Экспертиза PT** предназначена для просмотра информации о таких средствах проверки. Страница открывается при выборе в главном меню в разделе **Средства проверки** пункта **Экспертиза PT**.

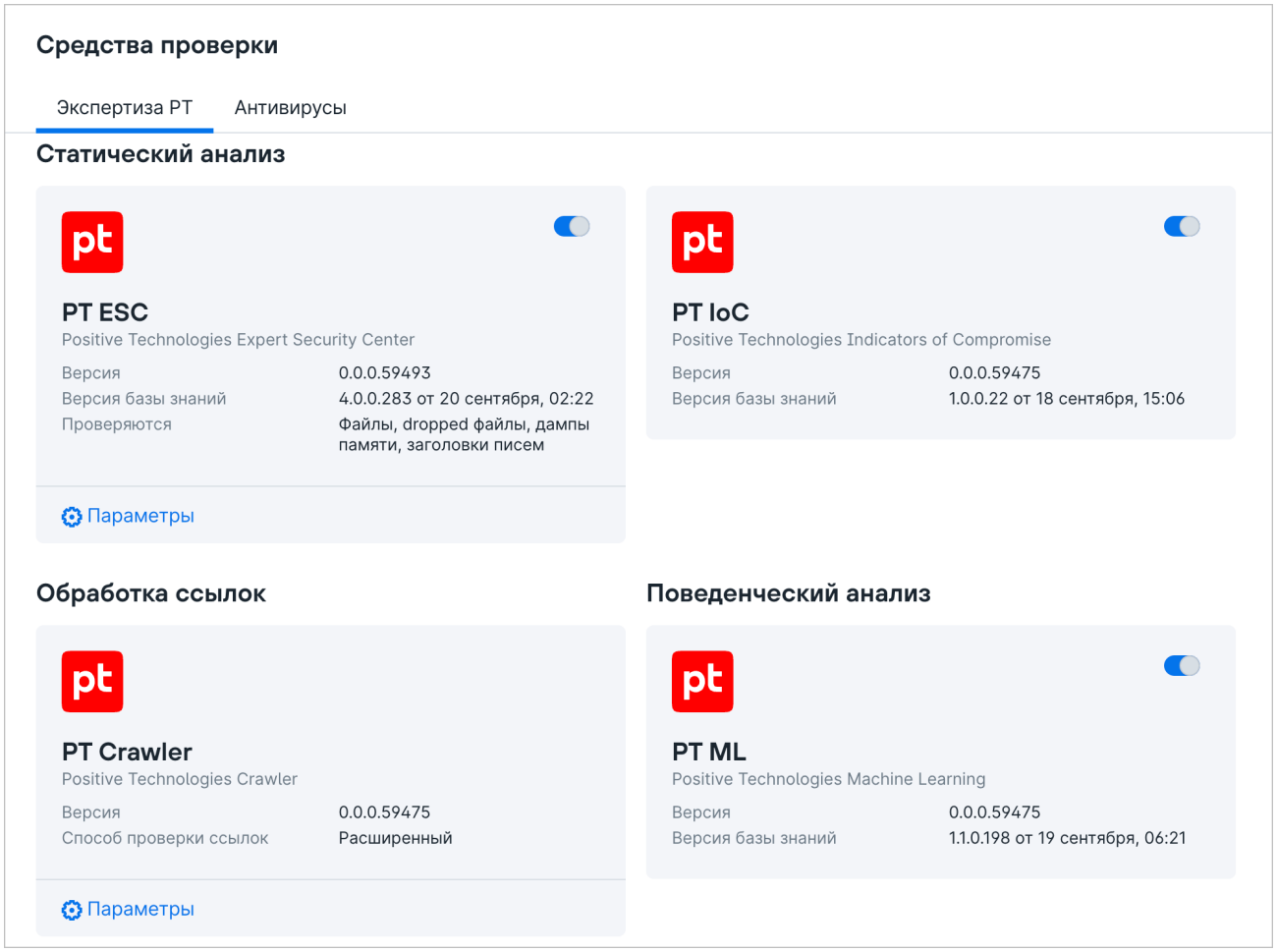

Рисунок 48. Страница **Экспертиза PT**

В рабочей области страницы расположены панели с информацией о средствах проверки:

- PT ESC — средство статического анализа на основе YARA-правил. База знаний PT ESC обновляется автоматически.
- PT IoC — средство обнаружения индикаторов компрометации в файлах и ссылках. База знаний PT IoC обновляется автоматически.
- PT ML — средство поведенческого анализа на основе технологии машинного обучения. База знаний PT ML обновляется автоматически.
- PT Crawler — средство динамической проверки ссылок.

При необходимости вы можете отключить средство проверки, если в его панели отображается переключатель. Панель отключенного средства проверки будет выделена серым цветом. В панели средств проверки PT ESC и PT Crawler расположена ссылка **Параметры**, которая в PT ESC используется для выбора типов проверяемых объектов, а в PT Crawler — для настройки работы средства проверки.

15.7.2. Страница «Антивирусы»

Для проверки объектов PT Sandbox может использовать антивирусы сторонних разработчиков. Страница **Антивирусы** предназначена для просмотра информации о доступных антивирусах. Страница открывается при выборе в главном меню в разделе **Средства проверки** пункта **Антивирусы**.

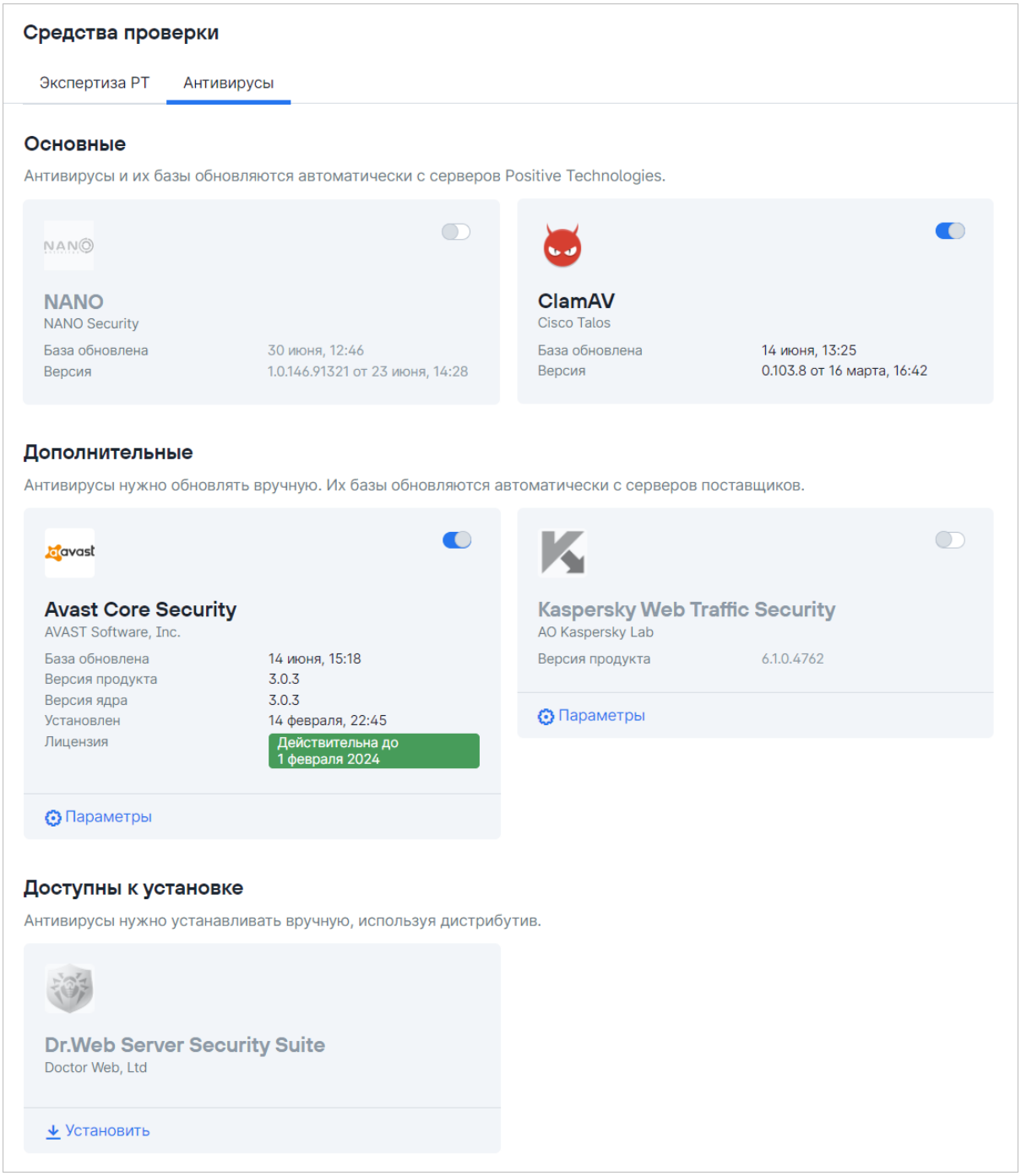

Рисунок 49. Страница **Антивирусы**

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

— **Основные** — входят в комплект поставки PT Sandbox. При необходимости любой из основных антивирусов можно отключить. Базы и лицензии этих антивирусов обновляются автоматически.

— **Дополнительные** — добавлены в PT Sandbox после его установки. При необходимости любой из дополнительных антивирусов можно отключить. Базы дополнительных антивирусов обновляются автоматически. Устанавливать новые версии и обновлять лицензии вам нужно самостоятельно.

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

— **Доступны к установке** — антивирусы, которые можно добавить в PT Sandbox.

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

Панели отключенных или неустановленных антивирусов выделены серым цветом.

См. также

Настройка антивирусов (см. раздел 16)

15.8. Страница «Источники»

PT Sandbox может проверять объекты, поступающие из различных источников. Страница **Источники** предназначена для добавления и управления источниками. Страница открывается при выборе в главном меню раздела **Источники**.

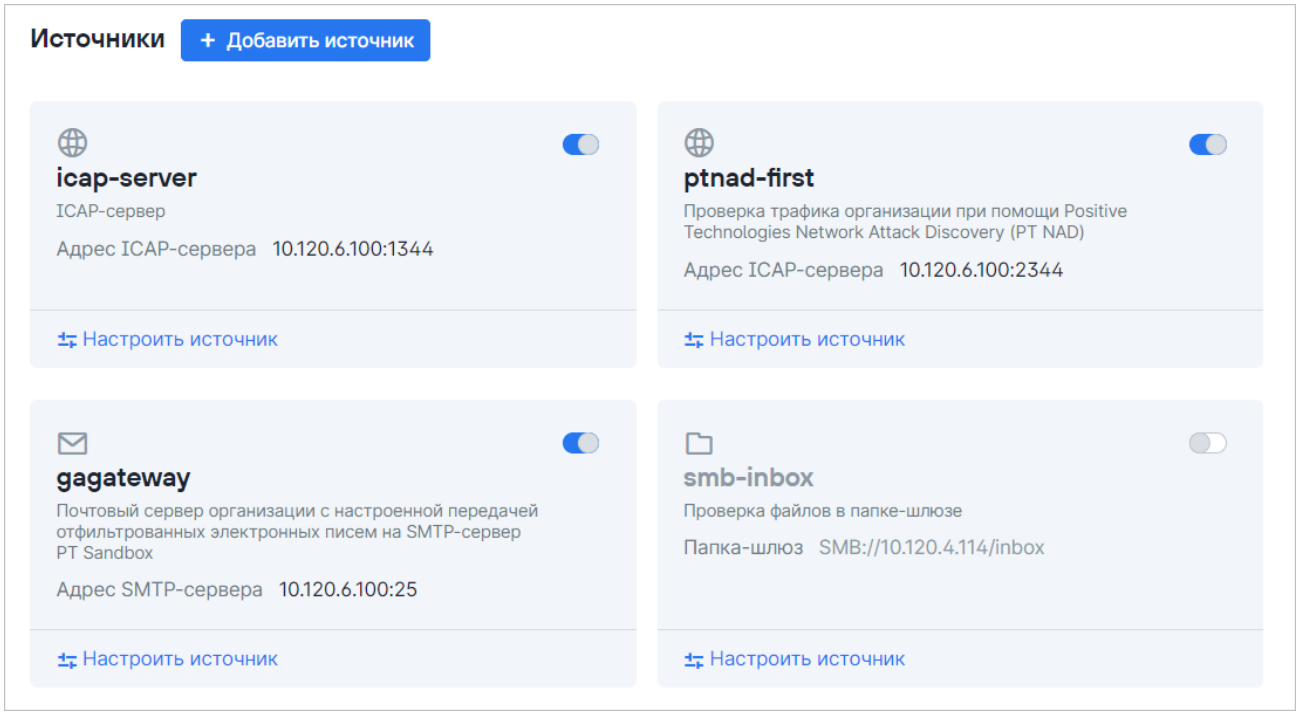

Рисунок 50. Страница **Источники**

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

В рабочей области страницы расположены панели с информацией о добавленных источниках. При необходимости вы можете отключить источник, тогда его панель будет выделена серым цветом. В каждой панели расположена кнопка **Настроить источник** для настройки параметров источника.

15.9. Страницы раздела «Система»

Используя пункты раздела **Система** главного меню, вы можете настраивать основные параметры PT Sandbox, управлять обновлением, лицензией и токенами доступа.

В этом разделе

15.9.1. Страница «Основные параметры»

Странице **Основные параметры** предназначена для настройки параметров PT Sandbox.

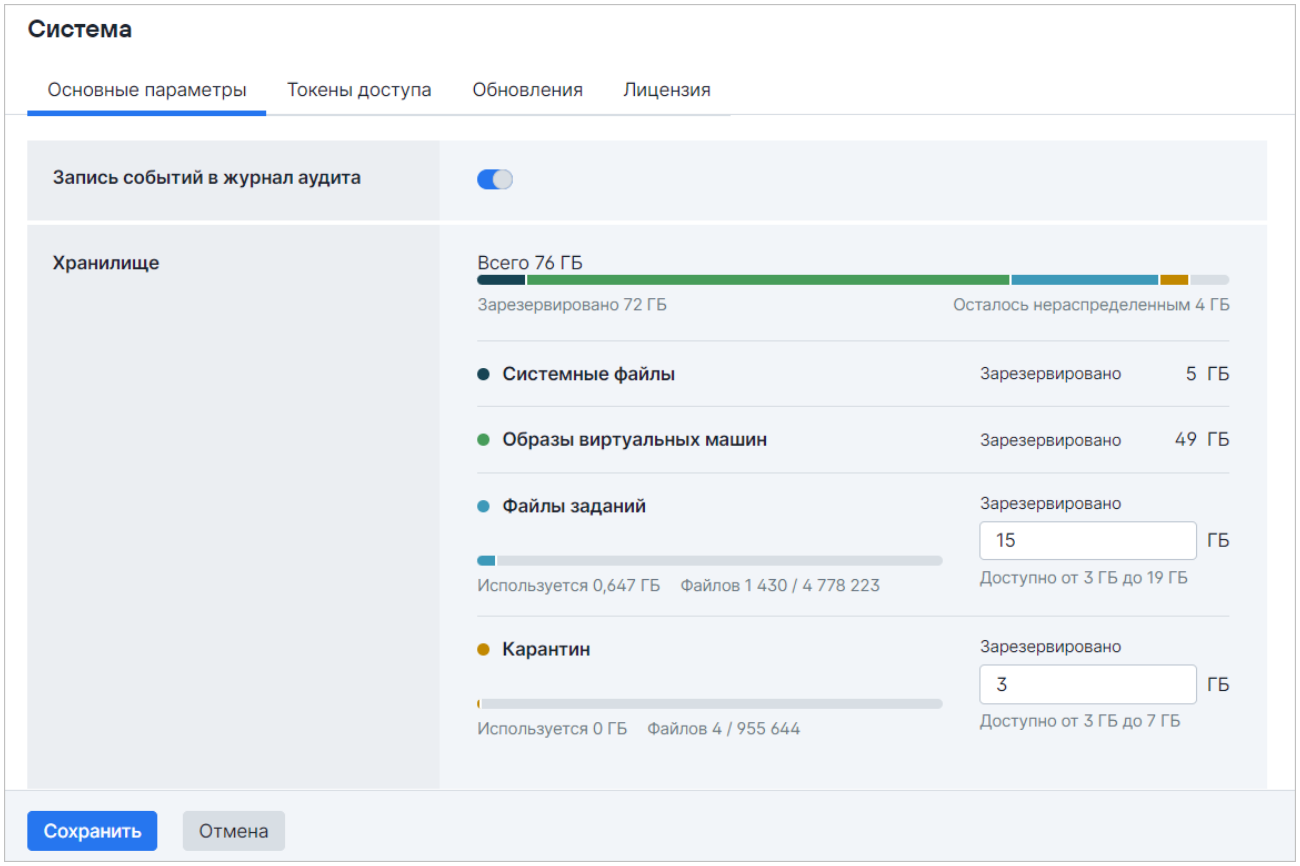

Рисунок 51. Страница **Основные параметры**

В рабочей области страницы расположены следующие блоки параметров:

- **Запись событий в журнал аудита** — для включения записи в журнал аудита событий об обновлении антивирусов и антивирусных баз и о фактах включения и отключения записи (см. раздел 19.1).
- **Хранилище** — для настройки объема хранилища для файлов заданий (см. раздел 19.2).
- **Карантин** — для настройки срока хранения заблокированных писем в карантине (см. раздел 19.3).
- **История проверок** — для изменения времени хранения информации о заданиях и проверенных объектах (см. раздел 19.4).
- **Повторная проверка** — для настройки повторной проверки файлов из хранилища.
- **Стандартные пароли** — для ввода паролей, которые будут использоваться при распаковке архивов.
- **Отправка сообщений в системный журнал по протоколу syslog** — для настройки отправки событий PT Sandbox во внешние системы в формате сообщений syslog (см. раздел 19.5).

— **Отправка данных в PT Threat Analyzer** — для настройки отправки данных об обнаруженных опасных и потенциально опасных объектах в программную платформу PT Threat Analyzer. Вы также можете настроить отправку найденных в задании файлов с угрозами (см. раздел 19.6).

— **Уведомления об угрозах** — для настройки отправки уведомлений об обнаруженных файлах с угрозами по электронной почте (см. раздел 19.7).

— **Анонимная проверка** — для предоставления пользователям возможности анонимно (см. раздел 19.8)проверять файлы и ссылки.

В нижней части страницы расположены кнопки **Сохранить** и **Отменить** для применения или отмены внесенных изменений.

15.9.2. Страница «Токены доступа»

При выборе в главном меню в разделе **Система** пункта **Токены доступа** открывается страница со всеми созданными токенами для доступа к PT Sandbox по API. Созданные токены используются при добавлении источника «API с выбранными параметрами проверки».

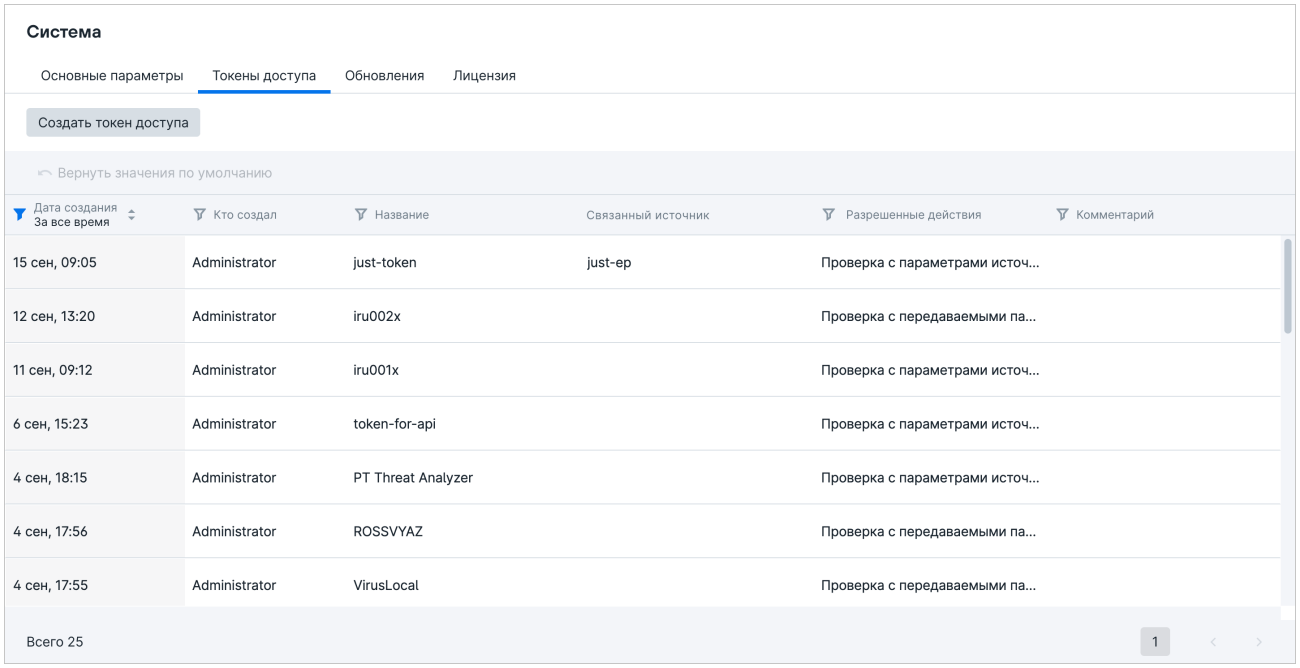

Рисунок 52. Страница **Токены доступа**

В рабочей области страницы расположены:

— кнопка **Создать токен доступа**, при нажатии которой открывается окно для создания нового токена доступа.

— таблица с информацией по всем созданным токенам доступа. При наведении курсора на строку таблицы отображаются значки:

  для изменения комментария к токену.

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

15.9.3. Страница «Обновления»

При выборе в главном меню в разделе **Система** пункта **Обновления** открывается страница **Обновления**. На этой странице вы можете просмотреть установленную версию PT Sandbox, проверить наличие новых версий, запустить ручное обновление или настроить автоматическое обновление системы.

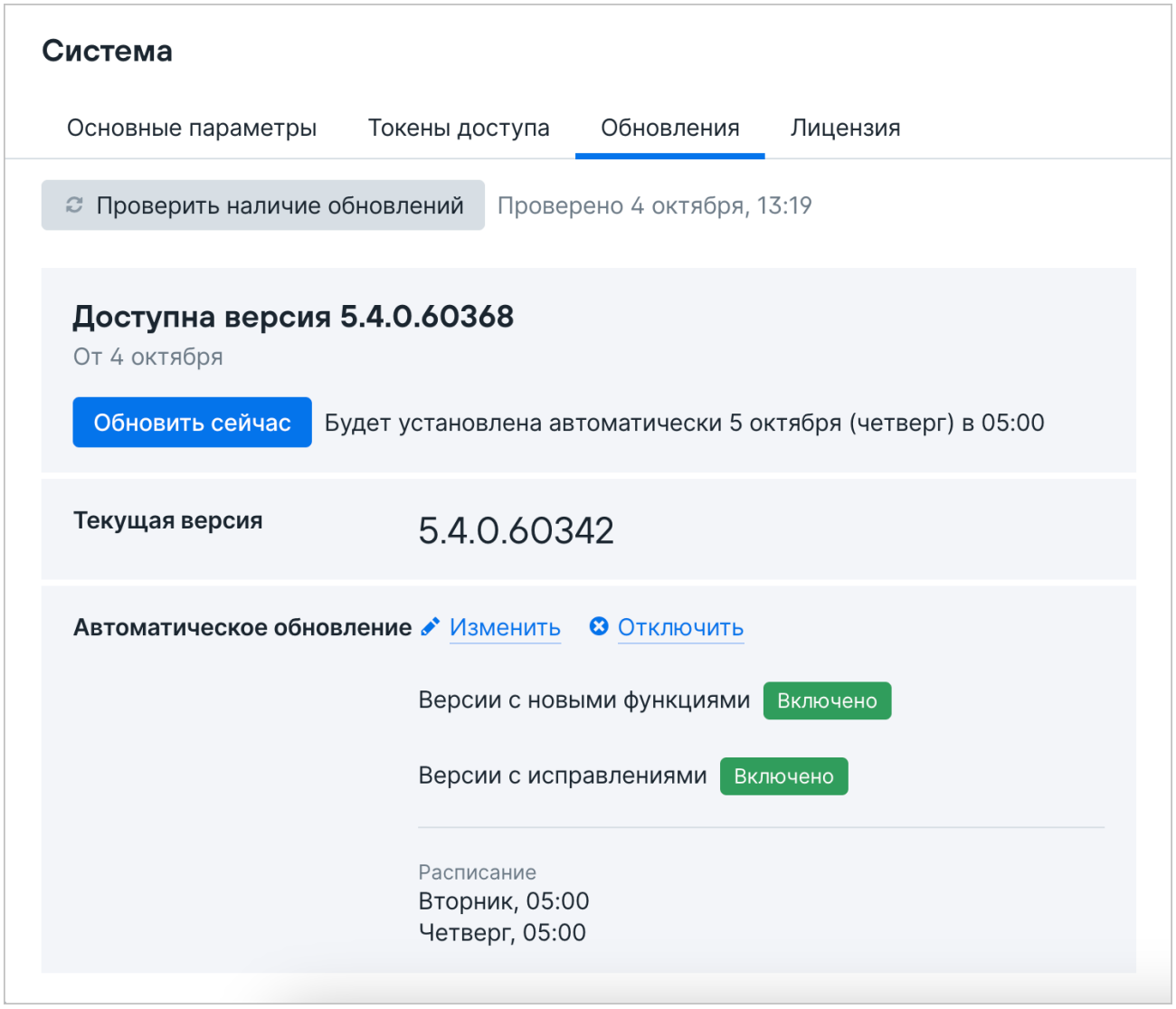

Рисунок 53. Страница **Обновления**

В рабочей области страницы расположены:

— кнопка **Проверить наличие обновлений** для проверки доступных для установки версий.

— блок с версией, которая доступна для установки. При наличии нескольких доступных версий каждая отображается в отдельном блоке. Также в блоке отображается кнопка **Обновить сейчас** для установки версии вручную (см. раздел 26.2).

— блок для настройки автоматического обновления системы (см. раздел 26.1). В блоке отображаются ссылки **Изменить** и **Отключить**, параметры установки версий с новыми функциями и версий с исправлениями, а также расписание автоматического обновления.

15.9.4. Страница «Лицензия»

При выборе в главном меню в разделе **Система** пункта **Лицензия** открывается страница **Лицензия**.

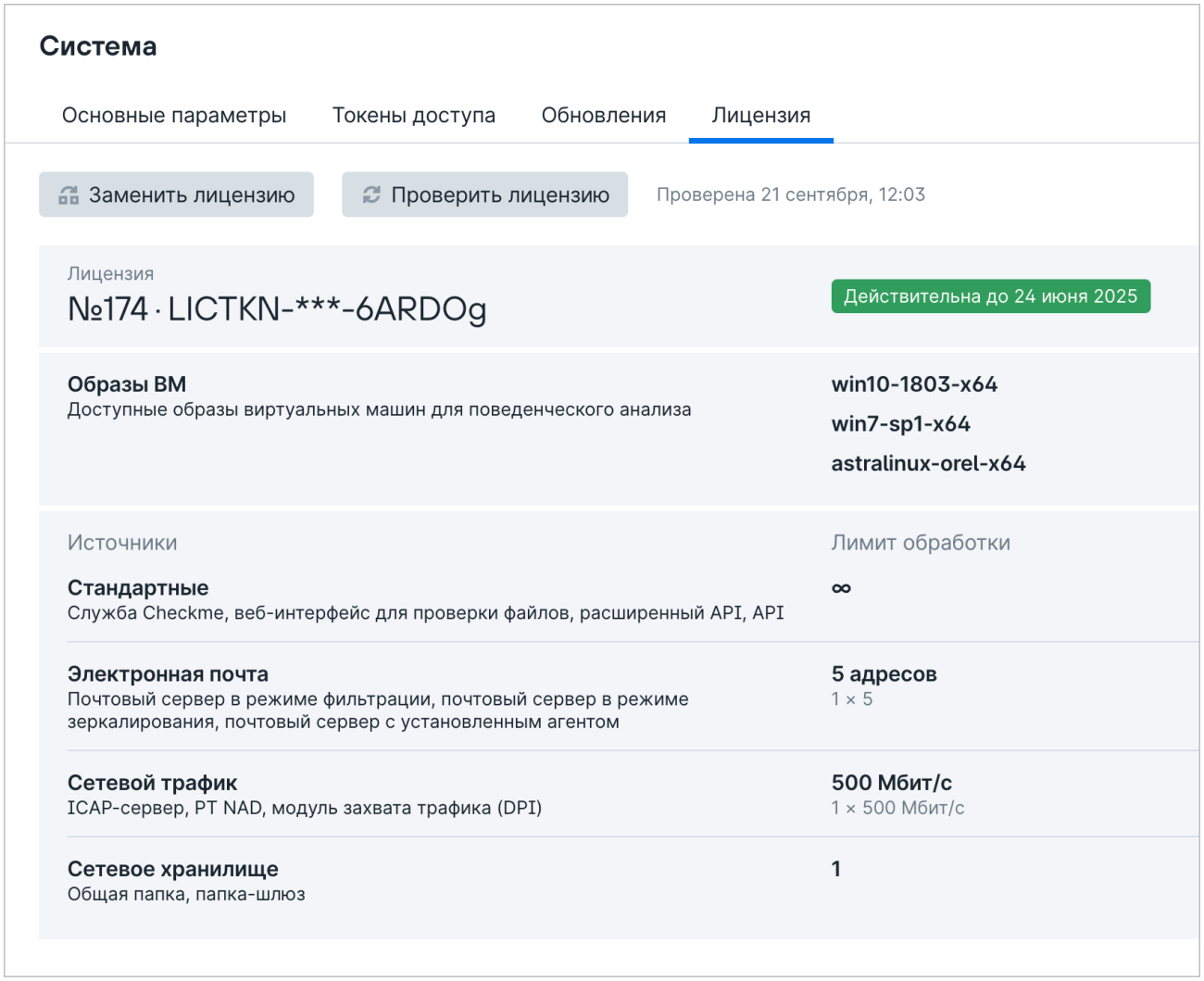

Рисунок 54. Страница **Лицензия**

В рабочей области страницы расположены:

— Кнопка **Заменить лицензию** для ввода серийного номера новой лицензии (см. раздел 25).

— Кнопка **Проверить лицензию** для обновления информации о параметрах текущей лицензии. Рядом с кнопкой также отображается дата последней проверки.

— Номер текущей лицензии и срок ее действия.

— Доступные образы виртуальных машин для поведенческого анализа.

— Источники для проверки и лимит их обработки в рамках текущей лицензии.

15.10. Смена языка и темы оформления интерфейса

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

► Чтобы сменить язык интерфейса,

в главном меню нажмите , в раскрывшемся меню выберите пункт **Язык** и название языка.

Язык интерфейса изменен.

► Чтобы сменить тему интерфейса,

в главном меню нажмите , в раскрывшемся меню выберите пункт **Тема** и название темы.

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

Тема интерфейса изменена.

16. Настройка антивирусов

Кроме средств проверки, разработанных специалистами Positive Technologies, для проверки объектов в PT Sandbox используются антивирусы сторонних разработчиков.

В комплект поставки PT Sandbox входят антивирус ClamAV компании Cisco Talos и антивирус NANO компании NANO Security. Базы и лицензии этих антивирусов обновляются автоматически. Вы не можете удалить основные антивирусы, но при необходимости можете их отключить.

Для повышения вероятности обнаружения угроз вы можете приобрести и установить дополнительные антивирусы:

— Avast Core Security 3.0;

— Dr.Web Server Security Suite 11.1;

— Kaspersky Web Traffic Security 6.1.0.4762;

— Symantec Protection Engine for Network Attached Storage 7.9.1.12.

Внимание! Поддерживаются только указанные версии дополнительных антивирусов. Для получения дистрибутивов вы можете обратиться в службу технической поддержки Positive Technologies. Для приобретения лицензий вам необходимо обратиться к разработчикам антивирусов.

Базы дополнительных антивирусов обновляются автоматически с серверов разработчиков или с указанных вами локальных серверов обновлений. Установку и обновление лицензий вам нужно выполнять самостоятельно. При необходимости вы можете отключить дополнительные антивирусы или удалить их.

В этом разделе

16.1. Просмотр сведений об антивирусах

► Чтобы просмотреть сведения об антивирусах,

в главном меню в разделе **Средства проверки** выберите пункт **Антивирусы**.

Откроется страница **Средства проверки** на вкладке **Антивирусы**.

16.2. Отключение и включение антивируса

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

► Чтобы отключить (включить) антивирус:

1. В главном меню в разделе **Средства проверки** выберите пункт **Антивирусы**.

   Откроется страница **Средства проверки** на вкладке **Антивирусы**.

2. В блоке с информацией об антивирусе отключите (включите) его.

   Блок с информацией об отключенном антивирусе выделен серым цветом.

Антивирус отключен (включен).

16.3. Установка дополнительного антивируса

Для установки дополнительного антивируса вам понадобятся его дистрибутив и файл лицензии.

Примечание. Установка дополнительного антивируса может быть ограничена лицензией.

► Чтобы установить дополнительный антивирус:

1. В главном меню в разделе **Средства проверки** выберите пункт **Антивирусы**.

   Откроется страница **Средства проверки** на вкладке **Антивирусы**.

2. В секции **Доступны к установке** в блоке с названием антивируса нажмите кнопку **Установить**.

   Откроется страница **Установка антивируса <Название антивируса>**.

3. По кнопке **Загрузить дистрибутив** загрузите файл дистрибутива антивируса.
4. По кнопке **Загрузить файл лицензии** загрузите файл с лицензией антивируса.
5. Если вам нужно, чтобы антивирус получал обновления своих баз из локального источника, укажите адрес этого источника в поле **Зеркало обновлений**.
6. 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**.
7. Нажмите кнопку **Установить**.

Начнется установка антивируса. По завершении установки на странице со списком антивирусов появится информация об установленном антивирусе.

Дополнительный антивирус установлен.

16.4. 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 **Средства проверки** выберите пункт **Антивирусы**.

   Откроется страница **Средства проверки** на вкладке **Антивирусы**.

2. В блоке с информацией об антивирусе нажмите ссылку **Параметры**.

   Откроется страница **Параметры антивируса <Название 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.

16.5. 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:

1. В главном меню в разделе **Средства проверки** выберите пункт **Антивирусы**.

   Откроется страница **Средства проверки** на вкладке **Антивирусы**.

2. В блоке с информацией об антивирусе нажмите ссылку **Параметры**.

   Откроется страница **Параметры антивируса <Название 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.

16.6. 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.

► Чтобы удалить дополнительный антивирус:

1. В главном меню в разделе **Средства проверки** выберите пункт **Антивирусы**.

   Откроется страница **Средства проверки** на вкладке **Антивирусы**.

2. В блоке с информацией об антивирусе нажмите ссылку **Параметры**.

   Откроется страница **Параметры антивируса <Название антивируса>**.

3. Нажмите кнопку **Удалить антивирус** и подтвердите удаление.

Дополнительный антивирус удален.

17. 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

17.1. 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 выберите раздел **Источники**.

   Откроется страница **Источники**.

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 специалистов по 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.

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. При автоматическом выборе типа аутентификации PT Sandbox выбирает наиболее безопасный тип из предложенных 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**.

Источник добавлен и настроен.

См. также

Отправка файлов на проверку по электронной почте (см. раздел 20.3)

17.2. 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

17.2.1. 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 выберите раздел **Источники**.

   Откроется страница **Источники**.

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 специалистов по 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.

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

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

6. Нажмите кнопку **Добавить источник**.

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 Positive Technologies в Руководстве администратора PT AF).

17.2.2. 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.

Примечание. Результат проверки, отправляемый ICAP-клиенту, формируется только на основании статического анализа.

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

В этом разделе

17.2.2.1. Настройка проверки по 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! В блокирующем режиме проверки файлов размер файла, передаваемого ICAP-серверу PT Sandbox, не должен превышать 1 ГБ. Иначе файл может не быть передан его получателю.

Внимание! В блокирующем режиме по истечении установленного тайм-аута сканирования контент будет передаваться как есть.

Примечание. Использование блокирующего режима может быть ограничено лицензией.

Вы можете настроить проверку по ICAP в конфигурационном файле стороннего ICAP-клиента, например прокси-сервера Squid (см. раздел 17.2.2.4). Перед настройкой ICAP-клиента вам нужно добавить в список источников ICAP-сервер (см. раздел 17.2.1).

Проверка по ICAP в блокирующем режиме настраивается с помощью URI следующего формата:

```
icap://<IP-адрес ICAP-сервера>:<Порт ICAP>/<Режим ICAP>?modify=y&block-
unwanted=<Блокировка потенциально опасных файлов>&timeout=<Тайм-аут сканирования>
```

► Чтобы настроить проверку по ICAP в блокирующем режиме:

1. Вместо `<Режим ICAP>` для режима REQMOD укажите `scanrequest` (`scan-request`) или для режима RESPMOD — `scanresponse` (`scan-response`).
2. Вместо `<Блокировка потенциально опасных файлов>` укажите `y` для включения блокировки потенциально опасных файлов или укажите `n` для отключения блокировки потенциально опасных файлов.

   Примечание. Если параметр отсутствует в запросе, блокировка потенциально опасных файлов отключена.
3. Вместо `<Тайм-аут сканирования>` укажите тайм-аут сканирования в секундах.

   Примечание. По умолчанию тайм-аут равен 30 секундам.
4. Если требуется, настройте отправку поля заголовка X-Client-IP с IP-адресом пользователя, скачавшего или отправившего файл, для записи этой информации в результаты проверки.

Проверка по ICAP в блокирующем режиме настроена.

17.2.2.2. Настройка проверки по 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 17.2.2.3).

Вы можете настроить проверку по ICAP в конфигурационном файле стороннего ICAP-клиента, например прокси-сервера Squid (см. раздел 17.2.2.4). Перед настройкой ICAP-клиента вам нужно добавить в список источников ICAP-сервер (см. раздел 17.2.1).

Проверка по ICAP в режиме ожидания настраивается с помощью URI следующего формата:

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

► Чтобы настроить проверку по ICAP в режиме ожидания:

1. Вместо `<IP-адрес ICAP-сервера>` и `<Порт ICAP>` укажите IP-адрес и порт из параметров ICAP-сервера (см. раздел 17.2.1).
2. Вместо `<Режим ICAP>` для режима REQMOD укажите `scanrequest` (`scan-request`) или для режима RESPMOD — `scanresponse` (`scan-response`).
3. Вместо `<Тайм-аут сканирования>` укажите тайм-аут сканирования в секундах.

   Примечание. По умолчанию тайм-аут равен 30 секундам.
4. Если требуется, настройте отправку поля заголовка X-Client-IP с IP-адресом пользователя, скачавшего или отправившего файл, для записи этой информации в результаты проверки.

Проверка по ICAP в режиме ожидания настроена.

17.2.2.3. Настройка проверки по 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.

Вы можете настроить проверку по ICAP в конфигурационном файле стороннего ICAP-клиента, например прокси-сервера Squid (см. раздел 17.2.2.4). Перед настройкой ICAP-клиента вам нужно добавить в список источников ICAP-сервер (см. раздел 17.2.1).

► 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 17.2.1).

   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. Если требуется, настройте отправку поля заголовка X-Client-IP с IP-адресом пользователя, скачавшего или отправившего файл, для записи этой информации в результаты проверки.

Проверка по ICAP в пассивном режиме настроена.

17.2.2.4. 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:

   - Если требуется, 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>/scanrequest`

- Если требуется, 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>/scanresponse
  ```

  Вместо `<IP-адрес ICAP-сервера>` и `<Порт ICAP>` в обеих строках укажите IP-адрес и порт из параметров ICAP-сервера (см. раздел 17.2.1).

  Например:

  ```
  icap_service ptsb_req reqmod_precache icap://198.51.100.32:1344/scanrequest
  icap_service ptsb_resp respmod_precache icap://198.51.100.32:1344/scanresponse
  ```

  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. Если требуется, 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. Если требуется, 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.

17.2.2.5. Настройка ICAP-клиента на примере UserGate 6

Ниже приводится инструкция по настройке ICAP-клиента для проверки файлов в блокирующем режиме на примере универсального интернет-шлюза безопасности UserGate 6. Более подробную информацию о настройке UserGate вы можете получить на сайте производителя.

► Чтобы настроить ICAP-клиент для UserGate 6:

1. Откройте браузер и в адресной строке введите IP-адрес веб-интерфейса UserGate.

   Откроется веб-консоль UserGate.

2. Авторизуйтесь под учетной записью администратора UserGate.
3. В главном меню перейдите по ссылке **Настройки**.
4. В левой части страницы выберите раздел **Политики безопасности** → **ICAP-серверы**.
5. В панели инструментов нажмите кнопку **Добавить**.

   Откроется окно **Свойства ICAP-сервера**.

6. На вкладке **Общие** настройте параметры:
   - В поле **Название** введите название ICAP-сервера.
   - В поле **Адрес сервера** введите адрес ICAP-сервера PT Sandbox.
   - Если используемый порт отличается от 1344, в поле **Порт** введите номер порта.
   - Если необходимо изменить максимальный размер отправляемых на проверку файлов, в поле **Максимальный размер сообщения** укажите этот размер (размер по умолчанию — 512 КБ).

     Внимание! Увеличение максимального размера отправляемых на проверку файлов приведет к увеличению объема используемой UserGate оперативной памяти. Объем используемой памяти вы можете отслеживать на дашборде **NOC** на виджете **Графики производительности**. Максимальный размер файлов, проверяемых PT Sandbox, составляет 1 ГБ.

7. Выберите вкладку **Данные** и настройте параметры:
   - В строке **Reqmod путь** установите флажок **Включено**, а в поле ниже введите `/scan-request?modify=y&timeout=5`.

     Примечание. Если вы увеличили максимальный размер отправляемых на проверку файлов, необходимо увеличить время проверки каждого файла в PT Sandbox, указанное в параметре `timeout`.

   - В строке **Respmod путь** установите флажок **Включено**, а в поле ниже введите `/scan-response?modify=y&timeout=5`.

Внимание! Если вы увеличили время проверки файлов в PT Sandbox, необходимо также увеличить тайм-аут ответа ICAP-сервера, оно должно быть на 5 секунд больше значения параметра `timeout`. Увеличение тайм-аута ответа ICAP-сервера приведет к увеличению объема используемой UserGate оперативной памяти.

Примечание. По умолчанию тайм-аут ответа ICAP-сервера составляет 10 секунд. Текущее значение тайм-аута вы можете узнать, выполнив на узле UserGate через интерфейс командной строки команду `proxy config -get icap_wait_timeout`. Изменить тайм-аут вы можете командой `proxy config -set icap_wait_timeout <Тайм-аут ответа ICAP-сервера>`.

- В строке **Посылать имя пользователя** установите флажки **Включено** и **Кодировать в base64**, а в поле ниже введите `X-Authenticated-User`.
- В строке **Посылать IP-адрес** установите флажок **Включено**, а в поле ниже введите `X-Client-Ip`.

8. Нажмите кнопку **Сохранить**.
9. В левой части страницы выберите раздел **Политики безопасности** → **ICAP-правила**.
10. В панели инструментов нажмите кнопку **Добавить**.

    Откроется окно **Свойства правила ICAP**.
11. На вкладке **Общие** настройте параметры:
    - В поле **Название** введите название правила.
    - В строке **Действие** по ссылке **Пропустить** откройте раскрывающийся список и выберите **Переслать**.
12. Выберите вкладку **ICAP-серверы**.
13. Нажмите кнопку **Добавить**.

    Откроется окно **Выбор ICAP-сервера**.
14. Выберите в списке добавленный ранее ICAP-сервер и нажмите кнопку **Добавить**.
15. Нажмите кнопку **Закрыть**.

ICAP-клиент настроен.

17.3. 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

17.3.1. Подключение к почтовому серверу при помощи агента

Если в вашей организации используется почтовый сервер Microsoft Exchange, 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 специалистам по безопасности настраивать блокировку писем, представляющих угрозу безопасности.

Почтовый агент PT Sandbox может работать со следующими версиями Microsoft Exchange:

— Microsoft Exchange 2010 версия 14;

— Microsoft Exchange 2013 версия 15.0 (кроме 15.0.847.32);

— Microsoft Exchange 2016 версия 15.1 (15.01);

— Microsoft Exchange 2019 версия 15.2 (15.02).

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

1. Установить почтовый агент PT Sandbox на сервере Microsoft Exchange с ролью Mailbox.

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

2. Добавить источник для проверки с параметрами установленного почтового агента в интерфейсе PT Sandbox.

Почтовый агент будет перехватывать все письма, проходящие через сервер Microsoft Exchange организации, и отправлять их на проверку в PT Sandbox. Специалист по безопасности может выбрать режим проверки писем:

— При пассивном режиме каждое письмо отправляется на проверку и не дожидаясь ее результата доставляется адресатам. Результат проверки не влияет на доставку письма.

— При блокирующем режиме письмо отправляются на проверку и до получения ее результата задерживается на сервере Microsoft Exchange. После окончания проверки безопасные письма доставляется адресатам, а опасные блокируются (удаляются или помещаются в карантин).

В случае потери связи между почтовым агентом и PT Sandbox письма доставляются адресатам без проверки.

В этом разделе

17.3.1.1. 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).

► 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 17.3.1.3) в интерфейсе PT Sandbox.

17.3.1.2. 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.

► 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 17.3.1.3) в интерфейсе PT Sandbox.

17.3.1.3. Подключение PT Sandbox к почтовому агенту

После установки почтового агента с параметрами по умолчанию (см. раздел 17.3.1.1) или переопределенными параметрами (см. раздел 17.3.1.2) вам нужно настроить его в интерфейсе PT Sandbox.

► Чтобы подключить почтовый агент к PT Sandbox:

1. В главном меню выберите раздел **Источники**.

   Откроется страница **Источники**.

2. Нажмите кнопку **Добавить источник**.

   Откроется страница **Новый источник для проверки**.

3. В поле **Название** введите название почтового агента.

   Название агента будет отображаться для специалистов по 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.

4. В раскрывающемся списке **Тип** выберите **Почтовый сервер с установленным агентом**.

   На странице отобразятся параметры подключения к почтовому агенту.

5. В поле **Адрес сервера** введите IP-адрес сервера Microsoft Exchange и укажите TCP-порт почтового агента (по умолчанию — 7536).

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

6. Нажмите кнопку **Добавить источник**.

Почтовый агент подключен к PT Sandbox.

17.3.1.4. 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.

17.3.2. 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

17.3.2.1. 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 выберите раздел **Источники**.

   Откроется страница **Источники**.

2. Нажмите кнопку **Добавить источник**.

   Откроется страница **Новый источник для проверки**.

3. В поле **Название** введите название bcc-сервера PT Sandbox.

   Название bcc-сервера будет отображаться для специалистов по 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 bcc-сервера.

5. Если вам нужно, чтобы почтовый сервер отправлял скрытые копии по TCP-порту, отличному от 25, в поле **Адрес сервера** измените номер порта.

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

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 bcc-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 источник**.

Bcc-сервер PT Sandbox создан.

Теперь вы можете приступить к настройке почтового сервера вашей организации для отправки скрытых копий всех писем на созданный bcc-сервер.

17.3.2.2. Настройка зеркалирования трафика с Postfix

Инструкция актуальна для агента пересылки почтовых сообщений Postfix версии 3.2.

Перед началом настройки вам нужно создать bcc-сервер (см. раздел 17.3.2.1).

► 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 bcc-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.

17.3.2.3. Настройка зеркалирования трафика с Exim

Инструкция актуальна для агента пересылки почтовых сообщений Exim версии 4 с раздельными 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 bcc-сервер (см. раздел 17.3.2.1).

► 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.

17.3.2.4. 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 17.3.2.1).

► 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 **OK**, 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 bcc-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.

17.3.3. Настройка фильтрации почтового трафика

Вы можете настроить фильтрацию почтового трафика с сервера Exchange, 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 Exchange, Postfix или Exim вам нужно:

1. В интерфейсе PT Sandbox добавить источник для фильтрации почтового трафика.
2. Настроить правила маршрутизации почтового трафика с сервера Exchange, Postfix или Exim в конфигурационных файлах сервера.

В этом разделе

17.3.3.1. Добавление источника для фильтрации почтового трафика

► Чтобы добавить источник для фильтрации почтового трафика:

1. В главном меню выберите раздел **Источники**.

Откроется страница **Источники**.

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 специалистов по 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.

5. При необходимости в поле **Адрес SMTP-сервера PT Sandbox** измените стандартный порт (25) для подключения к SMTP-серверу.

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

6. В блоке параметров **Почтовые серверы** укажите параметры доступа к почтовому серверу для проверенной почты:

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

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

   - Если соединение с сервером устанавливается по протоколу SSL, установите флажок **Подключаться по SSL**.
   - Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

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

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

7. Если в вашей организации используются несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.
8. Если в вашей организации используются несколько почтовых серверов и необходимо настроить маршрутизацию писем в зависимости от адреса домена, указанного в адресе электронной почты получателя, в блоке параметров **Правила маршрутизации почтового трафика** включите использование правил маршрутизации и настройте правила (см. раздел 17.3.3.2).
9. Нажмите кнопку **Добавить источник**.

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 17.3.3.3)

Настройка правил маршрутизации почтового трафика с сервера Exim (см. раздел 17.3.3.4)

17.3.3.2. Настройка правил маршрутизации проверенного почтового трафика

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

► Чтобы настроить правило маршрутизации:

1. В главном меню выберите раздел **Источники**.

   Откроется страница **Источники**.
2. В блоке с информацией об источнике перейдите по ссылке **Настроить источник**.

   Откроется страница с параметрами выбранного источника.
3. В блоке параметров **Правила маршрутизации почтового трафика** включите использование правила маршрутизации.
4. В поле **Домен электронной почты получателя** введите адрес домена электронной почты получателя, для которого необходимо настроить правило.

5. Если необходимо перенаправлять письма согласно MX-записям, выберите способ маршрутизации **По MX-записям**.

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

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

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

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

- Если соединение с сервером устанавливается по протоколу SSL, установите флажок **Подключаться по SSL**.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

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

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

  Примечание. Если требуется настроить правила маршрутизации для других доменов электронной почты получателей, по кнопке **Добавить правило** вы можете добавить для них блоки параметров и настроить правила аналогичным образом.

7. Нажмите кнопку **Сохранить**.

Правило маршрутизации настроено.

17.3.3.3. Настройка правил маршрутизации почтового трафика с сервера Postfix

Перед началом настройки вам нужно добавить источник для фильтрации почтового трафика (см. раздел 17.3.3.1).

► 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.

17.3.3.4. Настройка правил маршрутизации почтового трафика с сервера Exim

Инструкция актуальна для агента пересылки почтовых сообщений Exim версии 4 с раздельными 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 17.3.3.1).

► 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>M"
   ```
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 обслуживающихся 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.

17.4. 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 версии 3.

В подключенной к PT Sandbox общей папке будут проверяться все файлы, размер которых не превышает 5 ГБ.

► Чтобы добавить и настроить источник для проверки файлов из общей папки:

1. В главном меню выберите раздел **Источники**.

Откроется страница **Источники**.

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 специалистов по 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.

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.

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

   - 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**.

Источник добавлен и настроен.

17.5. 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 зацикливание сканирования.

Для общего доступа к папкам поддерживаются протоколы SMB версий 2 и 3 и 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.

► Чтобы добавить и настроить источник для проверки файлов в папке-шлюзе:

1. В главном меню выберите раздел **Источники**.

   Откроется страница **Источники**.

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 специалистов по 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.

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.

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

Источник для проверки файлов в папке-шлюзе добавлен и настроен.

17.6. 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.

После этого вам нужно в PT NAD установить и настроить модуль ptdpi-worker@icap. 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@icap приведена в Руководстве администратора PT NAD (для версий 7.1—10.0) и в Руководстве по внедрению PT NAD (для версий 10.1 и выше).

► Чтобы добавить источник для проверки файлов, извлеченных PT NAD:

1. В главном меню выберите раздел **Источники**.

   Откроется страница **Источники**.

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 специалистов по 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 PT NAD.

5. При необходимости в поле **Адрес сервера** измените стандартный TCP-порт (2344) для подключения модуля ptdpi-worker@icap к PT Sandbox.

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

6. Нажмите кнопку **Добавить источник**.

Источник для проверки файлов, извлеченных PT NAD, добавлен.

17.7. Подключение API в качестве источника файлов для проверки

PT Sandbox может получать файлы для проверки от сторонних приложений через публичный API.

Токен доступа к API можно получить двумя способами:

— Сгенерировать его с помощью консольной команды. Подробная инструкция по генерации токена доступа приведена в Руководстве разработчика.

— Создать токен доступа через интерфейс PT Sandbox. Подробные инструкции по управлению токенами доступа приведены в этом разделе (см. раздел 18).

Созданный токен доступа нужно использовать во всех запросах к API и при добавлении источника «API с выбранными параметрами проверки».

► Чтобы добавить API с выбранными параметрами проверки в качестве источника файлов:

1. В главном меню выберите раздел **Источники**.

   Откроется страница **Источники**.

2. Нажмите кнопку **Добавить источник**.

   Откроется страница **Новый источник для проверки**.

3. В поле **Название** введите название источника.

4. В раскрывающемся списке **Тип** выберите **API с выбранными параметрами проверки**.

5. В раскрывающемся списке **Токен доступа** выберите существующий токен доступа или создайте новый (см. раздел 18.1), нажав ссылку **Создать токен доступа**.

   Примечание. Вы можете привязать один токен доступа только к одному источнику.

6. Нажмите кнопку **Добавить источник**.

Источник добавлен.

17.8. 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 выберите раздел **Источники**.

   Откроется страница **Источники**.

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**.

Параметры источника для проверки изменены.

17.9. 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 выберите раздел **Источники**.

   Откроется страница **Источники**.

2. Отключите источник для проверки.

   Блок с информацией об источнике для проверки сменит цвет с зеленого на серый.

Источник для проверки отключен.

17.10. 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 17.9).

Примечание. Стандартный источник (веб-интерфейс) не может быть удален.

► Чтобы удалить источник для проверки:

1. В главном меню выберите раздел **Источники**.

Откроется страница **Источники**.

2. В блоке с информацией об источнике, который вам нужно удалить, перейдите по ссылке **Настроить источник**.

   Откроется страница с параметрами выбранного источника.

3. Нажмите кнопку **Удалить источник для проверки** и подтвердите удаление.

Источник для проверки удален.

18. Управление токенами доступа

Вы можете управлять токенами доступа с помощью консольных команд или через графический интерфейс PT Sandbox. Управление токенами доступа с помощью команд описано в Руководстве разработчика.

В этом разделе

18.1. Создание токена доступа

► Чтобы создать токен доступа:

1. В главном меню в разделе **Система** выберите пункт **Токены доступа**.

   Откроется страница **Система** на вкладке **Токены доступа**.

2. Нажмите кнопку **Создать токен доступа**.

   Откроется окно **Создание токена доступа**.

3. В поле **Название** введите название для токена доступа. Оно будет отображаться на странице **Токены доступа**.

4. В поле **Разрешенные действия** выберите действия, которые будут доступны при использовании токена.

5. Если требуется, в поле **Комментарий** введите любой текстовый комментарий.

6. Нажмите кнопку **Создать**.

Созданный токен доступа отобразится в окне **Токен доступа создан**. Нажмите кнопку **Скопировать в буфер обмена и закрыть**, чтобы скопировать токен. После закрытия этого окна он будет недоступен для просмотра и копирования.

18.2. Изменение комментария для токена доступа

► Чтобы изменить или добавить комментарий к уже созданному токену доступа:

1. В главном меню в разделе **Система** выберите пункт **Токены доступа**.

   Откроется страница **Система** на вкладке **Токены доступа**.

2. В строке с токеном доступа нажмите .

   Откроется окно **Изменение комментария**.

3. Измените комментарий или введите новый.
4. Нажмите кнопку **Сохранить**.

Комментарий изменен.

18.3. Отзыв токена доступа

► Чтобы отозвать токен доступа:

1. В главном меню в разделе **Система** выберите пункт **Токены доступа**.

   Откроется страница **Система** на вкладке **Токены доступа**.

2. В строке с токеном доступа нажмите ⊖.

   Если токен доступа используется источником, то он перестанет работать после отзыва токена.

   Если токен доступа используется сторонней системой, то ее работа также может быть нарушена.

3. Нажмите кнопку **Все равно отозвать**.

Токен доступа отозван.

19. Настройка основных параметров PT Sandbox

В этом разделе приводятся инструкции по настройке параметров PT Sandbox.

В этом разделе

19.1. 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 MC (доступен оператору PT MC).

19.2. 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.

Увеличение объема для файлов заданий может понадобиться, например, если на сервере с PT Sandbox был добавлен жесткий диск. 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.

19.3. Настройка карантина

Письмо, заблокированное в результате проверки, размер которого не превышает 1 ГБ, вместо удаления можно перемещать в карантин. Пока письмо находится в карантине, специалист по 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.

19.4. Изменение срока хранения заданий

На странице **Задания**, доступной в главном меню PT Sandbox, отображается информация о заданиях, поступивших на проверку. Вы можете изменить срок хранения этой информации. Срок хранения заданий по умолчанию — 3 года.

Примечание. Информация о заданиях в базе данных хранится и удаляется блоками, содержащими данные за один календарный месяц. Это означает, что если срок хранения задания истекает, например, в середине месяца, оно будет удалено из базы данных только по окончании этого месяца.

► Чтобы изменить срок хранения заданий:

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.

3. Нажмите кнопку **Сохранить**.

Срок хранения заданий изменен.

19.5. Настройка отправки сообщений в системный журнал по протоколу syslog

PT Sandbox может выступать в качестве источника сообщений для системного журнала. 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 **Сервер системного журнала** 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.

19.6. Настройка отправки данных для отчетов в PT Threat Analyzer

Вы можете настроить отправку результатов заданий, в которых обнаружены опасные или потенциально опасные файлы, из PT Sandbox в программную платформу для накопления знаний о существующих и потенциальных угрозах информационной безопасности Positive Technologies Threat Analyzer (далее — PT Threat Analyzer). Кроме отправки результатов вы также можете настроить отправку найденных в задании файлов с угрозами. Отправка этих данных выполняется через REST API. Для каждого задания в PT Threat Analyzer формируется отдельный отчет.

Перед выполнением инструкции вам необходимо получить ключ API для аутентификации и доступа PT Sandbox к REST API у администратора PT Threat Analyzer.

► Чтобы настроить отправку данных для отчетов в PT Threat Analyzer:

1. В главном меню в разделе **Система** выберите пункт **Основные параметры**.

   Откроется страница **Система** на вкладке **Основные параметры**.

2. В блоке параметров **Отправка данных в PT Threat Analyzer** включите отправку данных.

3. Укажите параметры PT Threat Analyzer:

- В поле **Адрес PT Threat Analyzer** введите адрес в формате `https://<Адрес PT Threat Analyzer>`.
- В поле **Ключ API** введите полученный у администратора PT Threat Analyzer ключ API.
- В раскрывающемся списке **Уровень доступа** выберите уровень доступа пользователя в PT Threat Analyzer, который необходим для доступа к отчету.

4. С помощью переключателя **Отправка файлов** настройте отправку файлов:
   - Если отправлять файлы не требуется, выберите **Не отправлять**.
   - Если требуется отправлять только опасные и потенциально опасные файлы, выберите **Только файлы с угрозами**.
   - Если требуется также отправлять файлы, в которых содержатся обнаруженные файлы с угрозами (например, архивы или письма), выберите **Файлы с угрозами и связанные с ними файлы**.
5. Нажмите кнопку **Сохранить**.

Отправка данных для отчетов настроена.

19.7. Настройка почтовых уведомлений об угрозах

Вы можете настроить отправку по электронной почте уведомлений об обнаруженных PT Sandbox файлах с угрозами. Для каждого задания уведомления отправляются только при обнаружении первого опасного и первого потенциально опасного файла.

В уведомлении указываются имя файла с угрозой, класс обнаруженного ВПО, название и тип источника, с которого поступил файл, информация о том, откуда и куда был направлен файл. В теме письма с уведомлением указывается идентификатор задания, в котором обнаружен файл с угрозой, а по кнопке в теле письма вы можете открыть карточку этого задания.

► Чтобы настроить отправку почтовых уведомлений об угрозах:

1. В главном меню в разделе **Система** выберите пункт **Основные параметры**.

   Откроется страница **Система** на вкладке **Основные параметры**.
2. В блоке параметров **Уведомления об угрозах** включите отправку почтовых уведомлений.
3. В блоке параметров **Отправка уведомлений** выберите, в каких случаях требуется отправлять уведомления:
   - Если только при обнаружении опасных файлов, выберите **Только об опасных файлах**.
   - Если при обнаружении опасных и потенциально опасных файлов, выберите **Об опасных и потенциально опасных**.
4. В поле **Адрес эл. почты отправителя** введите адрес, который будет указан в письме с уведомлением в качестве отправителя.

5. В поле **Адреса эл. почты получателей** введите адреса, на которые будут отправляться письма с уведомлениями.
6. Если требуется изменить язык уведомления, в раскрывающемся списке **Язык уведомлений** выберите нужный язык.
7. В блоке параметров **SMTP-серверы** настройте параметры доступа к SMTP-серверу для отправки писем с уведомлениями:
   - В поле **Адрес** введите IP-адрес или доменное имя сервера, в соседнем поле введите его порт.
   - Если в вашей организации используются несколько SMTP-серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

     Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.
   - Если соединение с сервером устанавливается по протоколу SSL, установите флажок **Подключаться по SSL**.
   - Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

     Примечание. При автоматическом выборе типа аутентификации PT Sandbox выбирает наиболее безопасный тип из предложенных почтовым сервером.
   - Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
8. Если в вашей организации используются несколько SMTP-серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.
9. Нажмите кнопку **Сохранить**.

Отправка почтовых уведомлений об угрозах настроена.

19.8. Включение анонимной проверки файлов

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

► Чтобы включить анонимную проверку файлов:

1. В главном меню в разделе **Система** выберите пункт **Основные параметры**.

Откроется страница **Система** на вкладке **Основные параметры**.

2. Включите анонимную проверку файлов.
3. Нажмите кнопку **Сохранить**.

Анонимная проверка файлов включена.

20. Проверка объектов

Через интерфейс PT Sandbox вы можете отправлять на проверку файлы и ссылки на файлы. Кроме того, если в PT Sandbox настроена служба Checkme, вы можете отправлять на проверку файлы и письма по электронной почте.

Внимание! Максимальный размер файла, который вы можете отправить на проверку через интерфейс PT Sandbox, — 1 ГБ.

В этом разделе

20.1. Проверка файлов через интерфейс

► Чтобы проверить файлы через интерфейс PT Sandbox:

1. В главном меню нажмите кнопку **Проверить объекты**.

   Откроется окно **Проверка объектов**.

2. На вкладке **Файлы** перетащите файлы для проверки в область загрузки или нажмите на ссылку **выберите**.

   В окне появится информация о загруженных файлах.

   Примечание. Вы можете отменить отправку файла на проверку по кнопке ⊗ и добавить другие файлы, перетащив их в область загрузки файлов или по ссылке **выберите**.

3. Настройте параметры проверки файлов.
4. Нажмите кнопку **Проверить**.

Файлы отправлены на проверку, для каждого файла создано отдельное задание на проверку. В Центре уведомлений появились уведомления о статусе выполнения этих заданий.

20.2. Проверка ссылок через интерфейс

► Чтобы проверить ссылку:

1. В главном меню нажмите кнопку **Проверить объекты**.

   Откроется окно **Проверка объектов**.

2. На вкладке **Ссылки** укажите в поле одну или несколько ссылок.

Примечание. Если по ссылке находится файл, размер которого превышает 1 ГБ, PT Sandbox скачивает первый гигабайт файла и проверяет его.

3. Если требуется, настройте параметры проверки.
4. Нажмите кнопку **Проверить**.

Ссылки отправлены на проверку, для каждой ссылки создано отдельное задание на проверку. В Центре уведомлений появились уведомления о статусе выполнения этих заданий.

20.3. 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 специалистом по 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.

6. В полученном письме нажмите кнопку **Отчет о сканировании**, чтобы просмотреть в интерфейсе PT Sandbox результаты проверки отправленного вами письма с вложениями.

21. Работа с результатами проверки

После завершения проверки файлов PT Sandbox генерирует отчет с результатами проверки. Если вы отправляли файлы на проверку через интерфейс или по ссылкам, уведомление об окончании проверки со ссылкой на отчет появится в Центре уведомлений. Если вы отправляли файлы на проверку по электронной почте, ссылка на отчет придет в ответном письме.

В этом разделе

21.1. 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.

   Для поиска нужного файла вы можете ввести в поле поиска название файла или использовать фильтры для отображения только опасных, потенциально опасных или непроверенных объектов.

   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.

В случае проверки электронных писем на странице с результатами проверки также отображаются свойства письма.

21.2. Создание отчета по объектам

Вы можете создавать отчеты по проверенным объектам. Отчет создается в формате CSV и содержит информацию об объектах, отображаемых на странице.

► Чтобы создать отчет:

1. В главном меню выберите раздел **Объекты**.

   Откроется страница **Объекты**.

2. Если требуется найти объекты, поступившие на проверку за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.

3. При необходимости найдите в таблице объекты, которые нужно отобразить в отчете.

4. Нажмите кнопку **Скачать отчет**.

   Файл отчета будет загружен на ваш компьютер.

21.3. Скачивание проверенных файлов

► Чтобы скачать из хранилища проверенный файл:

1. В главном меню выберите раздел **Объекты**.

   Откроется страница **Объекты**.

2. Щелчком мыши по строке в таблице откройте карточку объекта.

3. Если объект содержит несколько файлов, в боковой панели в иерархическом списке выберите нужный файл.

4. Нажмите кнопку **Скачать** и в раскрывшемся меню выберите **Выбранный файл**.

   Примечание. Вы также можете скачать файл, наведя курсор на название файла в боковой панели и нажав ↓.

Файл добавлен в ZIP-архив с паролем infected и скачан на ваш компьютер.

22. Изменение конфигурации PT Sandbox

Вы можете изменять конфигурацию PT Sandbox, добавляя и удаляя дополнительные узлы для поведенческого анализа файлов.

Например, если в базовой конфигурации PT Sandbox вам нужно уменьшить время проверки файлов, вы можете добавить в конфигурацию дополнительные узлы, отключить на основном узле функцию поведенческого анализа и получить тем самым высоконагруженную конфигурацию PT Sandbox.

Для добавления дополнительного узла в конфигурацию PT Sandbox вам необходимо:

1. Развернуть дополнительные узлы с помощью ISO-файла (см. раздел 10.3) или с помощью установщика (см. раздел 11.3).
2. Активировать на дополнительных узлах функцию поведенческого анализа (см. раздел 10.5.3).
3. Отключить на основном узле функцию поведенческого анализа.
4. Удалить с основного узла гипервизор Xen.

Если в высоконагруженной конфигурации PT Sandbox требуется переустановить дополнительный узел или перенести его на другой физический сервер, сперва необходимо удалить дополнительный узел из конфигурации PT Sandbox, а затем заново развернуть его на том же или другом сервере.

> **Примечание.** Если дополнительный узел вышел из строя, достаточно на основном узле исключить его из конфигурации PT Sandbox.

Для удаления дополнительного узла из конфигурации PT Sandbox вам необходимо:

1. На основном узле исключить дополнительный узел из конфигурации PT Sandbox.
2. Удалить с дополнительного узла компоненты PT Sandbox.
3. Удалить с дополнительного узла гипервизор Xen.

В этом разделе

22.1. Отключение функции поведенческого анализа

Инструкцию необходимо выполнять на основном узле.

► Чтобы на узле отключить функцию поведенческого анализа:

1. Получите список узлов, на которых установлены компоненты PT Sandbox:
   ```
   sudo ptmsctl sandbox nodes list
   ```
   Появится список узлов со статусом функции поведенческого анализа:
   - `Behavioral analysis is enabled` — узел уже используется для поведенческого анализа;
   - `Behavioral analysis is disabled` — узел не используется для поведенческого анализа;
   - `Not ready for behavioral analysis to be enabled` — узел не может быть использован для поведенческого анализа (не установлен гипервизор Xen).
2. Отключите функцию поведенческого анализа на узле:
   ```
   sudo ptmsctl sandbox nodes release <Имя узла>
   ```
   Например:
   ```
   sudo ptmsctl sandbox nodes release hostname4
   ```

Функция поведенческого анализа отключена на узле.

22.2. Исключение дополнительного узла из конфигурации PT Sandbox

Инструкцию необходимо выполнять на основном узле PT Sandbox.

► Чтобы исключить дополнительный узел из конфигурации PT Sandbox:

1. Получите список узлов PT Sandbox:
   ```
   sudo kubectl --kubeconfig /etc/kubernetes/admin.conf get node
   ```
2. Если дополнительный узел указан в списке, исключите его из конфигурации:
   ```
   sudo kubectl --kubeconfig /etc/kubernetes/admin.conf delete node <Имя дополнительного узла>
   ```
   Появится сообщение об удалении дополнительного узла.

Дополнительный узел исключен из конфигурации PT Sandbox.

22.3. Удаление с узла гипервизора Xen

► Чтобы удалить с узла гипервизор Xen:

1. Перейдите в каталог со скриптами установщика PT Sandbox:
   - Если при установке использовался ISO-файл:
     ```
     cd /home/administrator/installer
     ```

- Если использовался установщик (пример):
  `cd /home/user/ptsb-installer`

2. Запустите скрипт `purge.sh`:
   `sudo xen/purge.sh`
3. По завершении работы скрипта нажмите клавишу Enter.

   Узел будет перезагружен.

Гипервизор Xen удален с узла.

22.4. Удаление с узла компонентов PT Sandbox

► Чтобы удалить с узла компоненты PT Sandbox:

1. Перейдите в каталог со скриптами установщика PT Sandbox:
   - Если при установке использовался ISO-файл:
     `cd /home/administrator/installer`
   - Если использовался установщик (пример):
     `cd /home/user/ptsb-installer`
2. Запустите скрипт `purge-kubernetes.sh`:
   `sudo ./purge-kubernetes.sh`
3. По завершении работы скрипта нажмите клавишу Enter.

   Узел будет перезагружен.

Компоненты PT Sandbox удалены с узла.

23. Смена IP-адреса узла PT Sandbox

Смена IP-адресов узлов не поддерживается в конфигурации PT Sandbox с отказоустойчивым кластером.

Для смены IP-адреса основного узла в базовой конфигурации PT Sandbox вам необходимо:

1. Изменить IP-адрес в ОС на основном узле.

   Внимание! Сразу после смены IP-адреса в ОС необходимо на основном узле изменить IP-адрес в параметрах PT Sandbox.

2. На основном узле изменить IP-адрес в параметрах PT Sandbox.

Для смены IP-адреса основного узла в высоконагруженной конфигурации PT Sandbox вам необходимо:

1. Изменить IP-адрес в ОС на основном узле.

   Внимание! Сразу после смены IP-адреса в ОС необходимо на основном узле изменить IP-адрес в параметрах PT Sandbox.

2. На основном узле изменить IP-адрес в параметрах PT Sandbox.
3. На основном узле исключить каждый дополнительный узел из конфигурации PT Sandbox.
4. Установить компоненты PT Sandbox на каждый дополнительный узел (см. раздел 10.3.3).

   Примечание. Если на дополнительном узле уже установлены компоненты PT Sandbox, в процессе установки эти компоненты будут проверены и узел будет добавлен в конфигурацию PT Sandbox.

Для смены IP-адреса дополнительного узла в высоконагруженной конфигурации PT Sandbox вам необходимо:

1. Удалить компоненты PT Sandbox с дополнительного узла (с сохранением гипервизора Xen и конфигурационных файлов PT Sandbox).
2. Изменить IP-адрес в ОС на дополнительном узле.
3. Повторно установить компоненты PT Sandbox на дополнительный узел (см. раздел 10.3.3).

В этом разделе

23.1. Изменение IP-адреса узла в ОС

► Чтобы изменить IP-адрес узла в ОС:

1. Откройте файл `/etc/hosts`.
2. Укажите в файле новый IP-адрес и сохраните изменения.
3. Откройте файл `/etc/network/interfaces`.
4. Укажите в файле новый IP-адрес и сохраните изменения.
5. Перезапустите службу `networking`:

   ```
   sudo systemctl restart networking
   ```

   Примечание. После перезапуска службы SSH-соединение с узлом будет разорвано. Для продолжения настройки подключитесь к узлу, используя новый IP-адрес.

IP-адрес узла изменен в ОС.

23.2. Изменение IP-адреса основного узла в параметрах PT Sandbox

Инструкцию необходимо выполнять на основном узле PT Sandbox. Перед сменой IP-адреса основного узла в параметрах PT Sandbox необходимо изменить IP-адрес узла в ОС.

► Чтобы изменить IP-адрес основного узла в параметрах PT Sandbox:

1. Перейдите в каталог со скриптами установщика PT Sandbox:
   - Если при установке использовался ISO-файл:

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

   - Если использовался установщик (пример):

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

2. Запустите скрипт `change-master-node-ip.sh`:

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

3. По завершении работы скрипта нажмите клавишу Enter.

   Узел будет перезагружен.

IP-адрес основного узла изменен в параметрах PT Sandbox.

23.3. Исключение дополнительного узла из конфигурации PT Sandbox

Инструкцию необходимо выполнять на основном узле PT Sandbox.

► Чтобы исключить дополнительный узел из конфигурации PT Sandbox:

1. Получите список узлов PT Sandbox:
   ```
   sudo kubectl --kubeconfig /etc/kubernetes/admin.conf get node
   ```
2. Если дополнительный узел указан в списке, исключите его из конфигурации:
   ```
   sudo kubectl --kubeconfig /etc/kubernetes/admin.conf delete node <Имя дополнительного узла>
   ```
   Появится сообщение об удалении дополнительного узла.

Дополнительный узел исключен из конфигурации PT Sandbox.

23.4. Удаление компонентов PT Sandbox с дополнительного узла

► Чтобы удалить компоненты PT Sandbox с дополнительного узла:

1. Перейдите в каталог со скриптами установщика PT Sandbox:
   - Если при установке использовался ISO-файл:
     ```
     cd /home/administrator/installer
     ```
   - Если использовался установщик (пример):
     ```
     cd /home/user/ptsb-installer
     ```
2. Запустите скрипт `reset-kubernetes.sh`:
   ```
   sudo ./reset-kubernetes.sh
   ```
   Примечание. При таком удалении на узле сохраняются гипервизор Xen и конфигурационные файлы компонентов PT Sandbox.
3. По завершении работы скрипта нажмите клавишу Enter.

   Узел будет перезагружен.

Компоненты PT Sandbox удалены с дополнительного узла.

24. Смена DNS-сервера

В случае изменения адреса DNS-сервера, например при смене подсети, необходимо на основном узле PT Sandbox перезапустить службу CoreDNS.

Внимание! Не рекомендуется вносить изменения в файл `/etc/hosts`. Этот файл не используется компонентами PT Sandbox.

- Чтобы перезапустить службу CoreDNS,

  выполните команду:

  ```
  sudo kubectl --kubeconfig /etc/kubernetes/admin.conf -n kube-system rollout restart deploy/coredns
  ```

  Появится сообщение:

  ```
  deployment.apps/coredns restarted
  ```

  Служба CoreDNS перезапущена.

25. Замена лицензии PT Sandbox

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 Positive Technologies 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**.

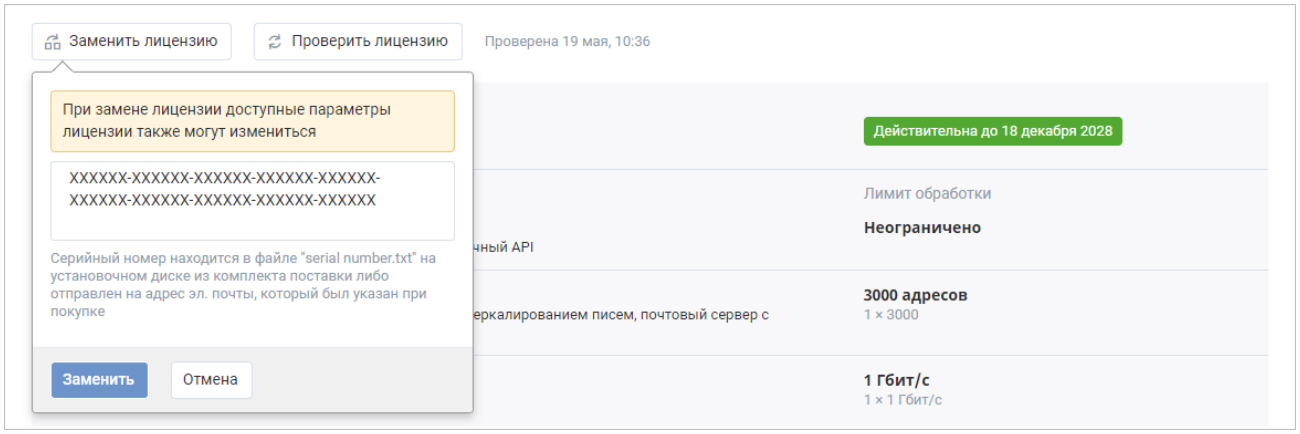

Рисунок 55. Замена лицензии

   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 Positive Technologies.

Если веб-интерфейс недоступен, вы можете заменить лицензию в консоли на узле с PT Sandbox (в многосерверной конфигурации — на основном узле).

► Чтобы заменить лицензию с помощью консоли,

выполните команду:

```
sudo ptmsctl license apply --serial-number '<Серийный номер лицензии>'
```

Например:

```
sudo ptmsctl license apply --serial-number 'xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-
xxxxxx-xxxxxx-xxxxxx-xxxxxx'
```

Появится сообщение `License was successfully replaced`.

Лицензия заменена.

Для проверки лицензии в консоли можно использовать команду `sudo ptmsctl license info`.

26. Обновление PT Sandbox

Вы можете устанавливать новые версии продукта в двух режимах: ручной и автоматический (включен по умолчанию).

В этом разделе

26.1. Автоматическое обновление

Автоматическое обновление системы включено по умолчанию. Вы можете настроить его или отключить, чтобы обновлять систему в ручном режиме (см. раздел 26.2).

► Чтобы настроить автоматическое обновление:

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

   Откроется страница **Система** на вкладке **Обновления**.

2. В блоке параметров **Автоматическое обновление** нажмите ссылку **Изменить**.

   Откроется страница настройки параметров автоматического обновления.

3. В блоке параметров **Тип обновления** выберите, какие версии нужно устанавливать автоматически.

   Если выбрана установка версий с новыми функциями, то по умолчанию включается и автоматическая установка версий с исправлениями.

   Если выбрана установка только версий с исправлениями, то критически важные обновления будут устанавливаться автоматически, а функциональные — в ручном режиме.

4. Если требуется, установите минимальный срок, который должен пройти с момента выхода новой версии. Для этого установите флажок **Не устанавливать версии, которым меньше <количество> дней** и укажите количество дней, по истечении которого нужно установить обновление.

5. В блоке параметров **Расписание** укажите дни недели и время, в которые будут устанавливаться обновления.

6. Нажмите кнопку **Сохранить**.

Автоматическое обновление настроено.

► Чтобы отключить автоматическое обновление:

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

Откроется страница **Система** на вкладке **Обновления**.

2. В блоке параметров **Автоматическое обновление** нажмите ссылку **Отключить**.

Автоматическое обновление отключено.

26.2. Ручное обновление

Вы можете запустить обновление PT Sandbox вручную при наличии доступной новой версии. Ручное обновление системы не зависит от параметров автоматического обновления.

► Чтобы обновить систему вручную:

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

   Откроется страница **Система** на вкладке **Обновления**.

2. Нажмите кнопку **Проверить наличие обновлений**, чтобы получить сведения о доступных новых версиях.

   Если новая версия доступна, отобразится оповещение с номером доступной версии. Если установлена последняя версия системы, отобразится статус **Обновлений нет**.

3. В оповещении о новой версии нажмите кнопку **Обновить сейчас**, чтобы запустить установку обновления. Функции системы будут доступны во время обновления.

   Запустится обновление системы. Вверху страницы отобразится индикатор выполнения обновления.

4. По окончании обновления в меню информации о продукте отобразится уведомление об успешном обновлении.

Обновление системы завершено.

27. 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

27.1. 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.

При создании файла резервной копии параметров PT Sandbox сохраняются:

- основные параметры и лицензия;
- параметры антивирусов и средств статического анализа;
- параметры источников проверки, кроме источников с типом «API с выбранными параметрами проверки»;
- параметры, заданные с помощью команды `ptmsctl`, кроме сгенерированных токенов API.

► Чтобы создать файл резервной копии параметров PT Sandbox,

перейдите в каталог с распакованным установщиком и выполните команду:

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

Например:

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

27.2. 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>`.

28. Удаление PT Sandbox

Вы можете удалить продукт полностью со всех узлов кластера, удалить продукт на определенном узле или функцию поведенческого анализа на определенном узле. Удаление производится с помощью скриптов, которые входят в комплект поставки системы.

► Чтобы удалить PT Sandbox:

1. Перейдите в каталог с установщиком:

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

2. Выполните подходящую команду:

   - Если требуется удалить продукт вместе с узлами кластера, выполните на каждом узле команду:
     `sudo ./purge-all.sh`

     Примечание. При выполнении команды `sudo ./purge-all.sh` не удаляются данные из БД. Для удаления данных из БД обратитесь в техническую поддержку Positive Technologies.

   - Если требуется удалить только продукт без удаления узлов, перейдите на любой основной узел и выполните команду:
     `sudo ./purge-product.sh`

   - Если требуется удалить продукт на определенном узле кластера, перейдите на этот узел и выполните команду:
     `sudo ./purge-kubernetes.sh`

     Внимание! После выполнения команды `sudo ./purge-kubernetes.sh` в односерверной конфигурации потребуется переустановка продукта, так как он перестанет работать.

   - Если требуется удалить функцию поведенческого анализа, перейдите на узел, на котором установлена эта функция, и выполните команду:
     `sudo ./xen/purge.sh`

     Примечание. Если функция поведенческого анализа установлена на нескольких узлах, то после выполнения команды она удалится только на том узле, на котором была выполнена команда. Вы также можете отключить функцию поведенческого анализа (см. раздел 22.1).

3. Подтвердите удаление.

PT Sandbox или функция поведенческого анализа удалены.

29. 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

29.1. Устранение проблем с действующей лицензией

Проблема

На странице с информацией о лицензии (см. раздел 15.9.4) 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 сайта Positive Technologies.

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 сайта Positive Technologies по HTTPS. Это можно сделать, проверив доступ к поддомену с обновлениями:

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

   Результат выполнения команды будет начинаться со строки `HTTP/1.1 200 OK`.

   Внимание! Если в вашей организации используется ПО, ограничивающее сетевой доступ, убедитесь, что доступ обеспечен не только к поддомену с обновлениями, но и к другим поддоменам сайта Positive Technologies.

4. Если результат выполнения команды отличается от указанного выше, обеспечьте доступ, после чего еще раз нажмите кнопку **Проверить лицензию**.

   Начнется проверка добавленной лицензии с использованием службы лицензирования.

5. Если сообщение о проблеме с лицензией не исчезло, соберите файлы журналов (см. раздел 29.4) и отправьте их в службу технической поддержки Positive Technologies для анализа.

29.2. Устранение проблем при замене лицензии

Проблема

Если при замене лицензии возникла проблема, информация о ней отображается на странице с информацией о лицензии (см. раздел 15.9.4).

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 25).
2. Если сообщение о проблеме с лицензией не исчезло, на сервере с установленным PT Sandbox проверьте доступ к поддоменам сайта Positive Technologies по HTTPS. Это можно сделать, проверив доступ к поддомену с обновлениями:

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

   Результат выполнения команды будет начинаться со строки `HTTP/1.1 200 OK`.

   Внимание! Если в вашей организации используется ПО, ограничивающее сетевой доступ, убедитесь, что доступ обеспечен не только к поддомену с обновлениями, но и к другим поддоменам сайта Positive Technologies.
3. Если результат выполнения команды отличается от указанного выше, обеспечьте доступ, после чего еще раз повторите попытку замены лицензии (см. раздел 25).
4. Если сообщение о проблеме с лицензией не исчезло, соберите файлы журналов (см. раздел 29.4) и отправьте их в службу технической поддержки Positive Technologies для анализа.

29.3. 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 выберите раздел **Источники**.

   Откроется страница **Источники**.
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 Positive Technologies.

См. также

Изменение параметров источника для проверки (см. раздел 17.8)

29.4. 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 Positive Technologies для анализа.

Собрать файлы журналов можно через:

— веб-интерфейс PT Sandbox;

— скрипт `collect-logs.sh`, который входит в комплект поставки системы. Для сбора файлов журналов через скрипт нужно запустить его без параметров на основном узле. Скрипт собирает файлы журналов PT Sandbox со всех узлов кластера, архивирует их и размещает в каталоге `/tmp` виртуальной машины или физического сервера, с которого был запущен скрипт.

► Чтобы собрать файлы журналов через веб-интерфейс:

1. В главном меню нажмите ⓘ.

   Откроется окно оповещений системы.

2. Нажмите кнопку **Скачать файлы журналов** и в раскрывшемся меню выберите период, за который нужно собрать файлы журналов.

   PT Sandbox начнет собирать файлы журналов продукта. Этот процесс может занять несколько минут в зависимости от общего размера файлов журналов и аппаратных ресурсов сервера или виртуальной машины с установленным PT Sandbox. По окончании сбора на вашем компьютере будет сохранен архив в формате `ptms-logs-ГГГГ-ММ-ДД_чч-мм-сс-T.zip`, где ГГГГ-ММ-ДД_чч-мм-сс — время скачивания архива в UTC, а T — период, за который скачаны журналы: 1H — за один час, 3H — за три часа, 1D — за один день, all — за все время.

Файлы журналов собраны.

30. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- предоставление рекомендаций по настройке продукта (оптимизации параметров) в процессе его эксплуатации;
- консультации по использованию функциональных возможностей продукта;
- диагностику сбоев, включая поиск причин и информирование клиента о выявленных проблемах;
- предоставление решений или возможностей обойти проблему с сохранением необходимой производительности;
- устранение ошибок в рамках выпуска обновлений;
- рассмотрение предложений по доработке продукта.

Вы можете получать техническую поддержку на специальном портале.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

30.1. Техническая поддержка на портале

Портал 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 содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, 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.

30.2. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний.

30.3. 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

30.3.1. Предоставление информации для технической поддержки

Для решения проблем с продуктом вам необходимо предоставить специалисту технической поддержки следующие данные:

- номер лицензии на использование продукта;
- файлы журналов и другие наборы диагностических данных, которые требуются для анализа;
- снимки экрана;
- результаты выполнения рекомендаций специалиста технической поддержки;
- оптимальный канал для удаленного доступа к продукту и его диагностики (выбирается по согласованию).

Если информация не будет предоставлена в течение двух недель с момента запроса, специалист технической поддержки имеет право закрыть заявку, предварительно уведомив вас об этом.

Positive Technologies не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

30.3.2. 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 Positive Technologies 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). Positive Technologies не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

Positive Technologies поставляет пакеты обновления в течение срока обновления, указанного в лицензии на продукт.

Positive Technologies не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, Positive Technologies обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

Доработка продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы также можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо доработок. Если Positive Technologies принимает решение о доработке продукта, то способы реализации доработки остаются на усмотрение Positive Technologies.

30.3.3. 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 15).

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 15. 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	До 24 часов	Не ограничено

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
	не оказывающие значительного влияния на бизнес		
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).

30.3.4. 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, Positive Technologies 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. Сценарии отказов

Если развернута конфигурация PT Sandbox с отказоустойчивым кластером, при выходе из строя любого аппаратного компонента (например, жесткого диска или модуля ОЗУ), физического сервера или при потере сетевого доступа к одному из узлов PT 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 16. Сценарии отказов компонентов PT Sandbox

Компонент	**Следствие отказа**		
	Потерянные данные	**Недоступность компонентов и функций**	**Ухудшение производительности**
Служба высокой доступности Keepalived	Результаты проверки файлов, которые проверялись на момент отказа	ICAP-сервер, почтовый сервер в режиме зеркалирования, почтовый сервер в режиме фильтрации —40 секунд	—
Веб-интерфейс	—	Веб-интерфейс — до 5 минут	—
База данных	Завершенные задания	Запись в базу данных — 20 секунд	—
API базы данных	Текущие задания в веб-интерфейсе	Запись в базу данных — 90 секунд	—
Ядро проверки	Часть файлов у трети текущих заданий	—	—
Хранилище файлов	Файлы	—	Модуль поведенческого анализа, скачивание файлов
Модуль поведенческого анализа	—	—	Модуль поведенческого анализа

Глоссарий

Checkme

Служба для проверки объектов по электронной почте. Пользователи могут отправить объект на специальный электронный адрес и получить результат проверки в ответном письме.

Keepalived

Служба, которая обеспечивает доступ к продукту по одному IP-адресу, независимо от того, какой из узлов отказоустойчивого кластера активен.

базовая конфигурация

Вариант развертывания, при котором все компоненты продукта устанавливаются на одном основном узле.

блокирующий режим

Режим проверки, при котором продукт влияет на распространение объектов в информационной системе организации. Поступившие на проверку объекты блокируются продуктом до окончания проверки. В зависимости от вынесенного вердикта объект пропускается в информационную систему или удаляется (или помещается в карантин).

вердикт

Решение продукта о наличии или отсутствии угрозы в объекте, уровне опасности этой угрозы и типе представляющего угрозу вредоносного ПО.

высоконагруженная конфигурация

Вариант развертывания продукта, при котором функции поведенческого анализа файлов перенесены на дополнительные узлы для повышения производительности.

динамический анализ

Совокупность методов проверки объекта, основанных на анализе его поведения. Имитируется взаимодействие пользователя с объектом и отслеживается появление связанных с этим угроз.

дополнительный узел

Узел продукта для поведенческого анализа файлов в высоконагруженной конфигурации.

дочерний объект

Объект, выделенный продуктом из другого объекта. Например, при распаковке архива, извлечении ссылок из письма или скачивании контента по ссылке.

единый вход

Технология, которая позволяет пользователям получать доступ к нескольким продуктам компании с помощью одного набора учетных данных и без повторной аутентификации.

задание на проверку

Совокупность информации, связанной с действиями продукта по выявлению угроз в поступивших на проверку объектах.

индикатор компрометации

Объект или свойство объекта, которые указывают на связь рассматриваемой активности в сети организации с известными угрозами ИБ. Индикаторами компрометации могут быть, например, хеш-суммы файлов, доменные имена или IP-адреса.

источник для проверки

Интерфейс в информационной системе организации, с которого в продукт поступают объекты на проверку.

карантин

Изолированная часть хранилища файлов, позволяющая сохранять заблокированные файлы с угрозами для последующего анализа.

карточка задания

Страница в интерфейсе продукта с информацией о задании на проверку. На странице отображается информация об обнаруженных в задании угрозах и вынесенном по заданию вердикте.

карточка объекта

Страница в интерфейсе продукта с информацией об объекте задания. На странице отображается информация об используемых методах проверки, обнаруженных угрозах и вынесенном по объекту вердикте.

карточка поведенческого анализа

Страница в интерфейсе продукта с информацией о проверке файла задания методом поведенческого анализа.

наследуемый вердикт

Вердикт, вынесенный на основании результатов проверки дочерних объектов.

объект

Выделенный продуктом или полученный извне объем данных, для которого выполняется проверка на наличие угрозы. Например, файл, архив, письмо или ссылка.

опасный объект

Объект, который является вредоносным ПО и представляет угрозу для информационной системы или данных организации.

основной узел

Первый узел, на который были установлены компоненты продукта при развертывании любой из конфигураций.

отказоустойчивый кластер

Вариант развертывания продукта, при котором для дублирования функций основного узла используются два резервных узла. Это позволяет обеспечить непрерывность работы продукта в случае отказа основного узла и избежать потери данных.

пассивный режим

Режим проверки, при котором продукт не влияет на распространение объектов в информационной системе организации. Поступившие на проверку объекты сразу пропускаются в информационную систему.

поведенческий анализ

Метод проверки объекта, основанный на анализе его поведения в изолированной виртуальной среде. Для выявления угроз в изолированной ОС имитируется взаимодействие пользователя с объектом и отслеживаются изменения, вносимые объектом в ОС и установленное ПО.

потенциально опасный объект

Объект, который при определенных обстоятельствах или действиях пользователя может представлять угрозу для информационной системы или данных организации.

прямой вердикт

Вердикт, вынесенный на основании результатов проверки самого объекта.

режим зеркалирования

Режим работы почтового сервера, при котором продукт не влияет на почтовый трафик сервера. На проверку в продукт отправляются копии писем.

режим ожидания

Режим проверки, при котором продукт не может влиять на распространение объектов в информационной системе организации. На проверку от источников приходят копии объектов и их распространене контролирует пользователь или сторонняя система.

режим фильтрации

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

резервный узел

Узел продукта для резервирования функций основного узла в конфигурациях с отказоустойчивым кластером.

ретроспективный анализ

Метод проверки, заключающийся в регулярной повторной проверке объектов в хранилище. Использование обновленных средств проверки и антивирусных баз позволяет выявлять ранее неизвестные угрозы в уже проверенных объектах.

статический анализ

Совокупность методов проверки объектов, основанных на анализе их свойств и содержимого.

угроза

Возможность того, что информационной системе или данным организации будет нанесен вред. Угроза исходит от опасных и потенциально опасных объектов.

positive technologies

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 200 тысяч акционеров.