Positive Technologies Incident Processing Center

Версия 2.7

Руководство администратора

POSITIVE TECHNOLOGIES

Дата редакции документа: 16.04.2020

Версия документа: 1

Содержание

1. Об этом документе

Руководство администратора Positive Technologies Incident Processing Center (далее также — PT Incident Processing Center) содержит:

- описание архитектуры PT Incident Processing Center, компонентов, программ и решений, с которыми взаимодействует PT Incident Processing Center;
- программные и аппаратные требования, другую информацию необходимую для развертывания PT Incident Processing Center;
- инструкции по развертыванию и первоначальной настройке PT Incident Processing Center.

Комплект документации PT Incident Processing Center включает в себя следующие документы:

- Этот документ.
- Руководство оператора (Личный кабинет оператора) — содержит описание сценариев работы и инструкции для оператора PT Incident Processing Center.
- Руководство участника (Личный кабинет участника) — содержит описание сценариев работы и инструкции для участника информационного обмена.

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

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

Пример текста с условным обозначением	Описание
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

2. О системе PT Incident Processing Center

Positive Technologies Incident Processing Center (далее также — PT Incident Processing Center) предназначен для поддержки бизнес-процессов национального или отраслевого центра реагирования на инциденты (далее также — центр) и организации непрерывного информационного взаимодействия между центром и участниками информационного обмена по вопросам нарушения режима информационной безопасности.

PT Incident Processing Center обеспечивает:

- взаимодействие между центром и участниками в части формирования и реагирования на угрозы и инциденты информационной безопасности;
- повышение уровня информированности участников об актуальных угрозах информационной безопасности;
- автоматизацию обработки инцидентов, поступающих от участников;
- проверку объектов и файлов, поступающих от участников, на присутствие вредоносного кода, опасной активности, а также на наличие угроз и уязвимостей информационной безопасности;
- взаимодействие с ГосСОПКА для эскалации вопросов информационной безопасности и получения инструкций.

По умолчанию система не подключена к ГосСОПКА (см. раздел 4.4). Данные из системы не передаются в ГосСОПКА. Для подключения к ГосСОПКА необходимо заключить соглашение с Национальным координационным центром по компьютерным инцидентам (НКЦКИ) Российской Федерации. После заключения соглашения с НКЦКИ Российской Федерации администратор системы настраивает подключение к ГосСОПКА.

См. также

ГосСОПКА (см. раздел 4.4)

3. Принципы работы PT Incident Processing Center

PT Incident Processing Center обеспечивает взаимодействие между национальным или отраслевым центром реагирования на инциденты (далее также — центр) и участником в части формирования и реагирования на угрозы и инциденты информационной безопасности.

Обмен информацией между центром и участником осуществляется по следующему алгоритму:

1. Участник направляет в центр сообщение об инциденте, угрозе, уязвимости или изменении данных в карточке участника, приложив к сообщению соответствующую электронную форму. При поступлении первого сообщения от участника через "Личный кабинет участника" PT Incident Processing Center формирует запрос. Все последующие сообщения, связанные с исходным, от участника и центра автоматически попадают в этот же запрос.
2. Центр получает сообщение от участника, проводит анализ запроса, проверку вложенных объектов и при необходимости формирует рекомендации для противодействия и направляет их участнику.
3. В сложных случаях, требующих дополнительной и более глубокой экспертизы, центр может перенаправить запрос в ГосСОПКА для дальнейшего расследования и получения рекомендаций.
4. Участник получает рекомендации по своему запросу, а также может получать бюллетени для своей отрасли, содержащие информацию о наличии или устранении уязвимостей в программном или аппаратном обеспечении.
5. Регулярная отраслевая аналитика по информационной безопасности и противодействию инцидентам публикуется Центром компетенции национального или отраслевого центра реагирования на инциденты для всех участников PT Incident Processing Center.

4. Архитектура и алгоритм работы PT Incident Processing Center

PT Incident Processing Center обеспечивает взаимодействие между центром и участником в части формирования и реагирования на угрозы и инциденты информационной безопасности.

Обмен информацией между центром и участником осуществляется по следующему алгоритму:

1. Участник направляет в центр сообщение об инциденте, угрозе, уязвимости или изменении данных в карточке участника, приложив к сообщению соответствующую электронную форму. При поступлении первого сообщения от участника через "Личный кабинет участника" PT Incident Processing Center формирует запрос. Все последующие сообщения, связанные с исходным, от участника и центра автоматически попадают в этот же запрос.
2. Центр получает сообщение от участника, проводит анализ запроса, проверку вложенных объектов и при необходимости формирует рекомендации для противодействия и направляет их участнику.
3. В сложных случаях, требующих дополнительной и более глубокой экспертизы, центр может перенаправить запрос в ГосСОПКА для дальнейшего расследования и получения рекомендаций.
4. Участник получает рекомендации по своему запросу, а также может получать бюллетени для своей отрасли, содержащие информацию о наличии или устранении уязвимостей в программном или аппаратном обеспечении.
5. Регулярная отраслевая аналитика по информационной безопасности и противодействию инцидентам публикуется центром для всех участников PT Incident Processing Center.

В этом разделе

4.1. "Личный кабинет участника"

"Личный кабинет участника" — это компонент продукта, который позволяет участнику взаимодействовать со специалистами центра по вопросам нарушения информационной безопасности организации и ее клиентов.

В "Личном кабинете участника" пользователю доступны следующие возможности:

- просмотр информации о своей организации;
- просмотр информации о пользователях;
- отправка сообщений специалистам центра о возникновении в организации или у ее клиентов инцидентов или угроз информационной безопасности;
- отправка сообщений специалистам центра об изменении данных организации или пользователей;
- двусторонний обмен данными со специалистами центра;
- просмотр бюллетеней безопасности о наличии или устранении уязвимостей в программном или аппаратном обеспечении.

4.2. "Личный кабинет оператора"

"Личный кабинет оператора" — это компонент продукта, который позволяет оператору взаимодействовать с участниками информационного обмена и ГосСОПКА в части реагирования на инциденты и угрозы информационной безопасности.

В "Личном кабинете оператора" оператору доступны следующие возможности:

- просмотр зарегистрированных в PT Incident Processing Center запросов, инцидентов, угроз и участников;
- регистрация запросов об инцидентах и угрозах, возникших в организациях участников;
- создание задач в рамках расследования инцидентов или обработки запросов;
- регистрация новых участников;
- изменение данных участников и их пользователей;
- двусторонний обмен данными с участниками информационного обмена и ГосСОПКА;
- рассылка бюллетеней безопасности участникам информационного обмена о наличии или устранении уязвимостей в программном или аппаратном обеспечении.

4.3. "Информационный портал"

"Информационный портал" — новостной сайт, на котором операторы PT Incident Processing Center публикуют информацию, аналитику и рекомендации в области обеспечения защиты информации при осуществлении переводов денежных средств.

"Информационный портал" является частью системы информационного обмена и доступен для всех участников системы PT Incident Processing Center.

4.4. ГосСОПКА

ГосСОПКА — главный центр Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Взаимодействие PT Incident Processing Center с ГосСОПКА обеспечивает:

- отправку запроса в ГосСОПКА на содействие по расследованию инцидентов;
- отправку запроса в ГосСОПКА на обновление информации по инцидентам;
- прием и обработку обновлений по инцидентам;
- прием и обработку информации по новым инцидентам;
- прием и обработку бюллетеней;
- прием и обработку сообщений от операторов ГосСОПКА;
- отправку сообщений операторам ГосСОПКА;
- отправку сообщений о закрытых инцидентах.

4.5. Почтовый сервер центра

Почтовый сервер центра отвечает за взаимодействие между участниками и операторами PT Incident Processing Center по электронной почте. Почтовый сервер центра обеспечивает:

- отправку сообщений о возникновении инцидентов или угроз информационной безопасности участниками по электронной почте в личные кабинеты операторов;
- отправку сообщений об изменении данных организации участниками по электронной почте в личные кабинеты операторов;
- отправку уведомлений о регистрации запроса из личного кабинета оператора на электронный адрес участника;
- рассылку бюллетеней из личного кабинета оператора на электронные адреса участников.

4.6. Пользовательский компонент

"Пользовательский компонент" обеспечивает автоматизированную отправку в PT Incident Processing Center инцидентов, зарегистрированных системами SIEM участника информационного обмена.

"Пользовательский компонент" разворачивается в инфраструктуре участника информационного обмена.

Как источник данных об инцидентах приложение использует информацию, передаваемую от SIEM (ArcSight, Qradar, PT MaxPatrol SIEM) по протоколу syslog RFC 5424. Полученные данные "Пользовательский компонент" конвертирует в формат JSON, совместимый с PT Incident Processing Center. После преобразования данных приложение отправляет их в PT Incident Processing Center.

"Пользовательский компонент" позволяет:

- отправлять данные инцидентов в PT Incident Processing Center в автоматическом и ручном режиме (по команде пользователя);
- при необходимости вручную изменять параметры инцидента перед отправкой;
- скачивать из приложения электронную форму инцидента в формате JSON для последующей пересылки в PT Incident Processing Center вручную.

"Пользовательский компонент" предоставляет пользователю интерфейс для просмотра инцидента и помогает выявлять и исправлять ошибки, которые могут мешать отправке инцидента в PT Incident Processing Center.

4.7. Интеграция PT Incident Processing Center с продуктами "Позитив Текнолоджиз"

В этом разделе приведено краткое описание продуктов "Позитив Текнолоджиз", которые могут быть подключены к PT Incident Processing Center.

В этом разделе

4.7.1. PT MaxPatrol SIEM

PT MaxPatrol SIEM обеспечивает комплексный мониторинг информационной безопасности как всей IT-инфраструктуры предприятия, так и отдельных подразделений, узлов и приложений. Система адаптируется к любой IT-инфраструктуре и работает для всех уровней управления.

4.7.2. PT KB

Knowledge Base — это единая база знаний продуктов компании , которая хранится в Microsoft SQL Server. База знаний включает в себя данные, необходимые для структурирования сведений, собранных от объектов инфраструктуры (например, для определения версий ОС, ПО, служб, типа аппаратного обеспечения).

Knowledge Base хранит сведения о следующих сущностях:

- программном обеспечении и операционных системах;
- уязвимостях, условиях их существования (наличие определенной ОС или ПО) и методах устранения (изменение настроек, применение пакетов обновлений и других);
- эксплойтах, условиях их применения;
- сигнатурах средств обнаружения атак (СОА);
- модулях САЗ и вредоносном ПО.

См. также

Настройка интеграции с PT KB (см. раздел 6.2.6)

4.7.3. PT MC

Сервис управления пользователями и доступом PT Management and Configuration (далее также — PT MC) обеспечивает механизм единого входа в продуктах "Позитив Технолоджиз".

Сервис предназначен:

- для создания и настройки учетных записей пользователей;
- назначения ролей, в соответствии с которыми в PT MC определен состав прав доступа к операциям по работе с сервисом;
- назначения ролей, в соответствии с которыми в PT Incident Processing Center определен состав прав доступа к операциям по работе с системой;
- блокировки и активации учетной записи пользователя.

В состав PT Incident Processing Center входит PT MC версии 19.0.

4.7.4. Honeypot

Honeypot — это система, которая проверяет файлы, ссылки и приложения на наличие угроз компьютеру пользователя или подозрительного поведения.

Преимущество проверки системой Honeypot перед обычной антивирусной проверкой заключается в комплексном анализе следующими методами:

- отслеживание поведения файлов и процессов, оценка последствий перехода по ссылкам в изолированной от пользователя среде;
- проверка файлов в соответствии с набором предустановленных правил;
- антивирусная проверка файла (если Honeypot поставляется с подсистемой статического анализа);
- получение информации от внешних репутационных сервисов об угрозах, исходящих от файлов и ссылок.

После проверки файла, ссылки или приложения Honeypot систематизирует результаты, присваивает проверенному объекту оценку опасности и формирует для пользователя отчет в краткой и подробной форме.

4.7.5. Cybsi

Positive Technologies Cybersecurity Intelligence (Cybsi) — это программная платформа для накопления знаний о существующих и потенциальных угрозах информационной безопасности, а также о способах их обнаружения. Cybsi собирает, анализирует и хранит информацию об угрозах информационной безопасности и индикаторах компрометации, которые могут быть выделены в рамках угрозы. Индикаторы компрометации — это артефакты, наблюдаемые в сети или в операционной системе и указывающие на вредоносную активность в инфраструктуре.

В системе PT Incident Processing Center Cybsi используется для получения информации об опасности файлов, IP-адресов, URL и доменов, получения названий операторов связи, обогащения дампов сетевого трафика, поиска похожих инцидентов.

См. также

Настройка интеграции с Cybsi (см. раздел 6.2.5)

4.8. Схема взаимодействия компонентов

Взаимодействие компонентов PT Incident Processing Center отражено на схеме.

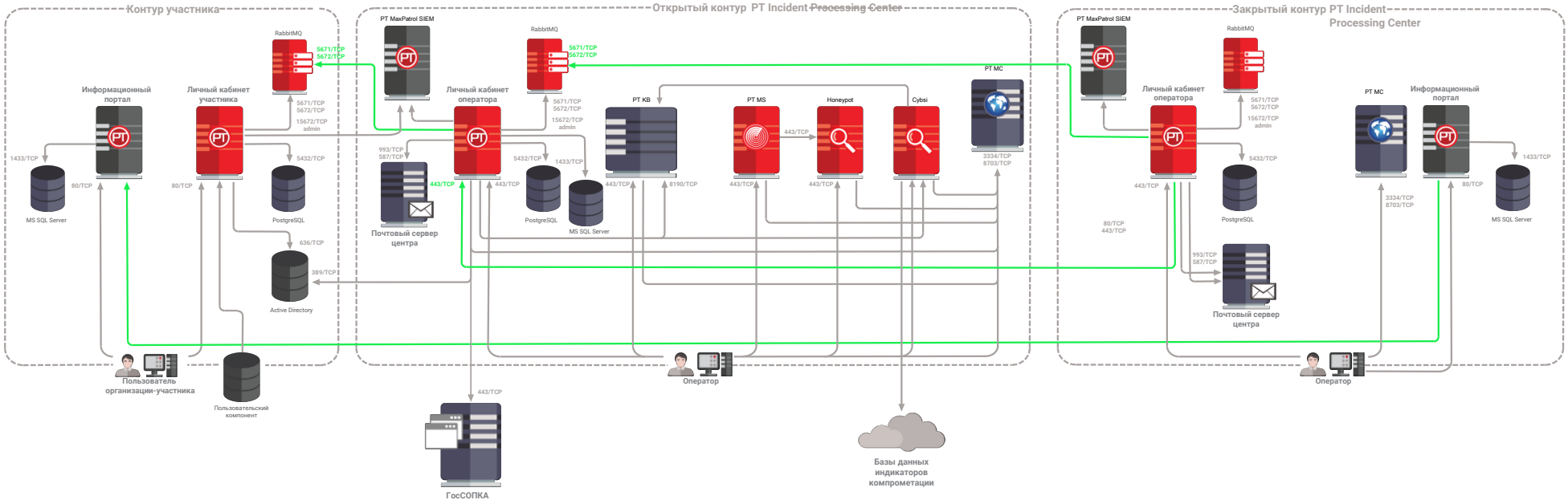

Рисунок 1. Схема взаимодействия компонентов

5. Аппаратные и программные требования

В этом разделе представлены системные требования, предъявляемые к аппаратному и программному обеспечению при развертывании компонентов PT Incident Processing Center.

В этом разделе

5.1. Требования к "Личному кабинету оператора"

"Личный кабинет оператора" включает следующие компоненты:

- сервер "Личного кабинета оператора";
- сервер RabbitMQ — для обмена данными с "Личным кабинетом участника";
- СУБД PostgreSQL — для хранения данных "Личного кабинета оператора".

Все компоненты рекомендуется размещать на разных виртуальных серверах, отвечающих следующим аппаратным и программным требованиям.

Таблица 2. Аппаратные и программные требования к серверу "Личного кабинета оператора"

Компонент	Минимальные требования
Виртуальный процессор	8 ядер
Память (ОЗУ)	64 ГБ
Свободное дисковое пространство	Для работы ОС – 600 ГБ Для обработки данных – 2000 ГБ
Операционная система	Microsoft Windows Server 2016

Таблица 3. Аппаратные и программные требования к серверу RabbitMQ

Компонент	Минимальные требования
Виртуальный процессор	2 ядра
Память (ОЗУ)	8 ГБ
Свободное дисковое пространство	Для работы ОС — 200 ГБ Для обработки данных — 200 ГБ
Операционная система	Microsoft Windows Server 2016

Таблица 4. Аппаратные и программные требования к серверу для PostgreSQL

Компонент	Минимальные требования
Виртуальный процессор	24 ядер
Память (ОЗУ)	128 ГБ
Свободное дисковое пространство	Для работы ОС – 200 ГБ Для обработки данных – 2000 ГБ
Операционная система	Microsoft Windows Server 2016

Подключение к "Личному кабинету оператора" выполняется с рабочего места оператора PT Incident Processing Center, которое должно соответствовать следующим аппаратным и программным требованиям.

Таблица 5. Аппаратные и программные требования к рабочему месту оператора

Компонент	Минимальные требования
Центральный процессор	Тактовая частота 2000 МГц
Память (ОЗУ)	3072 МБ
Сетевой адаптер	Ethernet 100 Base-T
Свободное дисковое пространство	80 ГБ
Операционная система	Microsoft Windows версии 7 Microsoft Windows версии 10
Браузер	Microsoft Edge версии 42.17134.1.0 Microsoft Internet Explorer версии 11 Google Chrome версии 60.0.31112.101
Программное обеспечение	Microsoft Office 2013 Adobe Acrobat Reader версии 11

5.2. Требования к "Личному кабинету участника"

Личный кабинет участника включает следующие компоненты:

- сервер "Личного кабинета участника";
- сервер RabbitMQ — для обмена данными с "Личным кабинетом оператора";
- СУБД PostgreSQL — для хранения данных "Личного кабинета участника".

Каждый компонент разворачивается на отдельном виртуальном сервере, соответствующем следующим аппаратным и программным требованиям.

Таблица 6. Аппаратные и программные требования к серверу "Личного кабинета участника"

Компонент	Минимальные требования
Виртуальный процессор	8 ядер
Память (ОЗУ)	64 ГБ
Свободное дисковое пространство	Для работы ОС — 600 ГБ Для обработки данных — 1000 ГБ
Операционная система	Microsoft Windows Server 2016

Таблица 7. Аппаратные и программные требования к серверу RabbitMQ

Компонент	Минимальные требования
Виртуальный процессор	2 ядра
Память (ОЗУ)	8 ГБ
Свободное дисковое пространство	Для работы ОС — 200 ГБ Для обработки данных — 200 ГБ
Операционная система	Microsoft Windows Server 2016

Таблица 8. Аппаратные и программные требования к серверу для PostgreSQL

Компонент	Минимальные требования
Виртуальный процессор	24 ядер
Память (ОЗУ)	128 ГБ
Свободное дисковое пространство	Для работы ОС – 200 ГБ Для обработки данных – 2000 ГБ
Операционная система	Microsoft Windows Server 2016

Рабочее место участника должно соответствовать следующим аппаратным и программным требованиям.

Таблица 9. Аппаратные и программные требования к рабочему месту участника

Компонент	Минимальные требования
Центральный процессор	Тактовая частота 2000 МГц
Память (ОЗУ)	3072 МБ
Сетевой адаптер	Ethernet 100 Base-T
Свободное дисковое пространство	80 ГБ
Операционная система	Microsoft Windows версии 7 Microsoft Windows версии 10

Компонент	Минимальные требования
Браузер	Microsoft Edge версии 42.17134.1.0 Microsoft Internet Explorer версии 11 Google Chrome версии 60.0.31112.101
Программное обеспечение	Microsoft Office 2013 Adobe Acrobat Reader версии 11

5.3. Требования к "Информационному порталу"

Сервер для развертывания "Информационного портала" PT Incident Processing Center должен соответствовать аппаратным и программным требованиям, представленным в таблице.

Таблица 10. Аппаратные и программные требования к серверу

Компонент	Минимальные требования
Виртуальный процессор	8 ядер
Память (ОЗУ)	32 ГБ
Свободное дисковое пространство	Для работы ОС – 200 ГБ Для обработки данных – 100 ГБ
Операционная система	Microsoft Windows Server 2016
Браузер	Microsoft Edge версии 42.17134.1.0 Microsoft Internet Explorer версии 11 Google Chrome версии 60.0.31112.101

На сервере Информационного портала должен быть установлен архиватор 7z и путь к нему (`C:\Program Files\7-Zip\7z.dll`) должен быть указан в качестве значения параметра `s7zLocation`.

6. Развертывание PT Incident Processing Center

PT Incident Processing Center развертывается в трех контурах, тесно взаимодействующих между собой:

- **Контур участника** — контур организации-участника, в рамках которого обеспечивается двусторонний информационный обмен участника и специалистов Центра компетенции PT Incident Processing Center в части реагирования на угрозы и инциденты информационной безопасности.
- **Открытый контур** — серверная площадка, предназначенная для сбора запросов от участников PT Incident Processing Center, анализа угроз и уязвимостей, расследования инцидентов, возникших на стороне участников, и выработки рекомендаций по предотвращению инцидентов и минимизации последствий для участников.
- **Закрытый контур** — контур PT Incident Processing Center, предназначенный для работы с информацией ограниченного доступа, а также для публикаций отраслевой аналитики по противодействию инцидентам нарушения режима информационной безопасности.

Для корректной работы PT Incident Processing Center после развертывания системы в трех контурах необходимо загрузить конфигурацию системы и справочники.

В этом разделе

6.1. Развертывание PT Incident Processing Center в контуре участника

Контур участника представляет собой серверную площадку, расположенную в IT-инфраструктуре центра. На этой площадке развертываются компоненты и их зависимости, необходимые для обмена информацией об инцидентах, угрозах, уязвимостях с операторами PT Incident Processing Center в открытом и закрытом контурах.

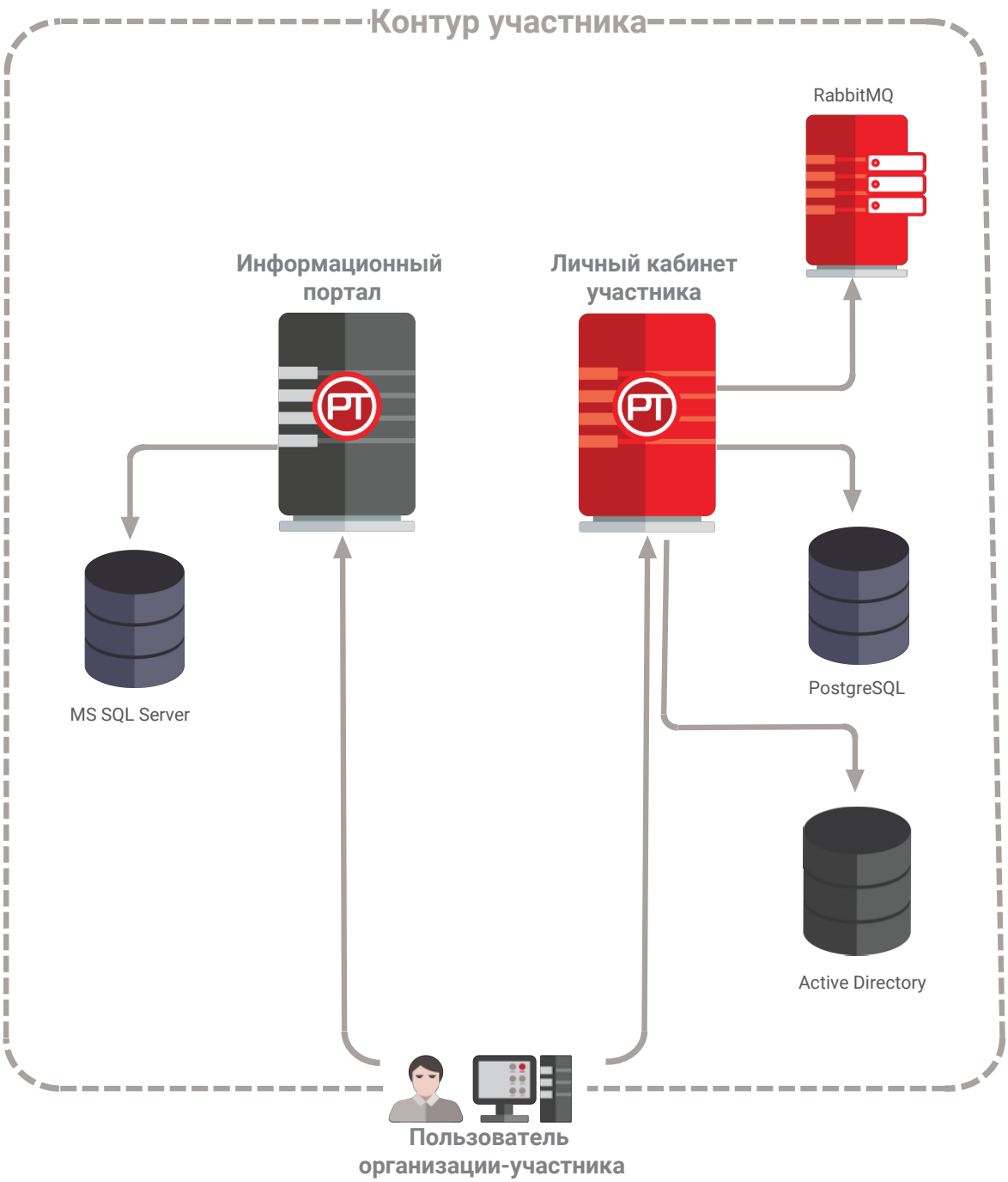

Рисунок 2. Схема развертывания компонентов в контуре участника

Перед началом установки убедитесь, что выполняются следующие условия:

- На сервере для установки "Информационного портала" отключена FIPS Compliant Policy (см. раздел 6.1.1).
- На отдельном сервере настроена Active Directory.

Вам потребуются следующие дистрибутивы:

- `PTIPCParticipantsPortal<Номер версии>.exe` — для установки "Личного кабинета участника", необходимых зависимостей, RabbitMQ и PostgreSQL.
- `InfoPortalDeployment.exe` — для установки "Информационного портала" и его зависимостей.

В этом разделе

6.1.1. Отключение FIPS Compliant Policy

► Чтобы отключить FIPS Compliant Policy:

1. В Панели управления выберите **Система и безопасность** → **Администрирование**.
2. В открывшемся окне выберите **Локальная политика безопасности**.

   Откроется окно **Локальная политика безопасности**.

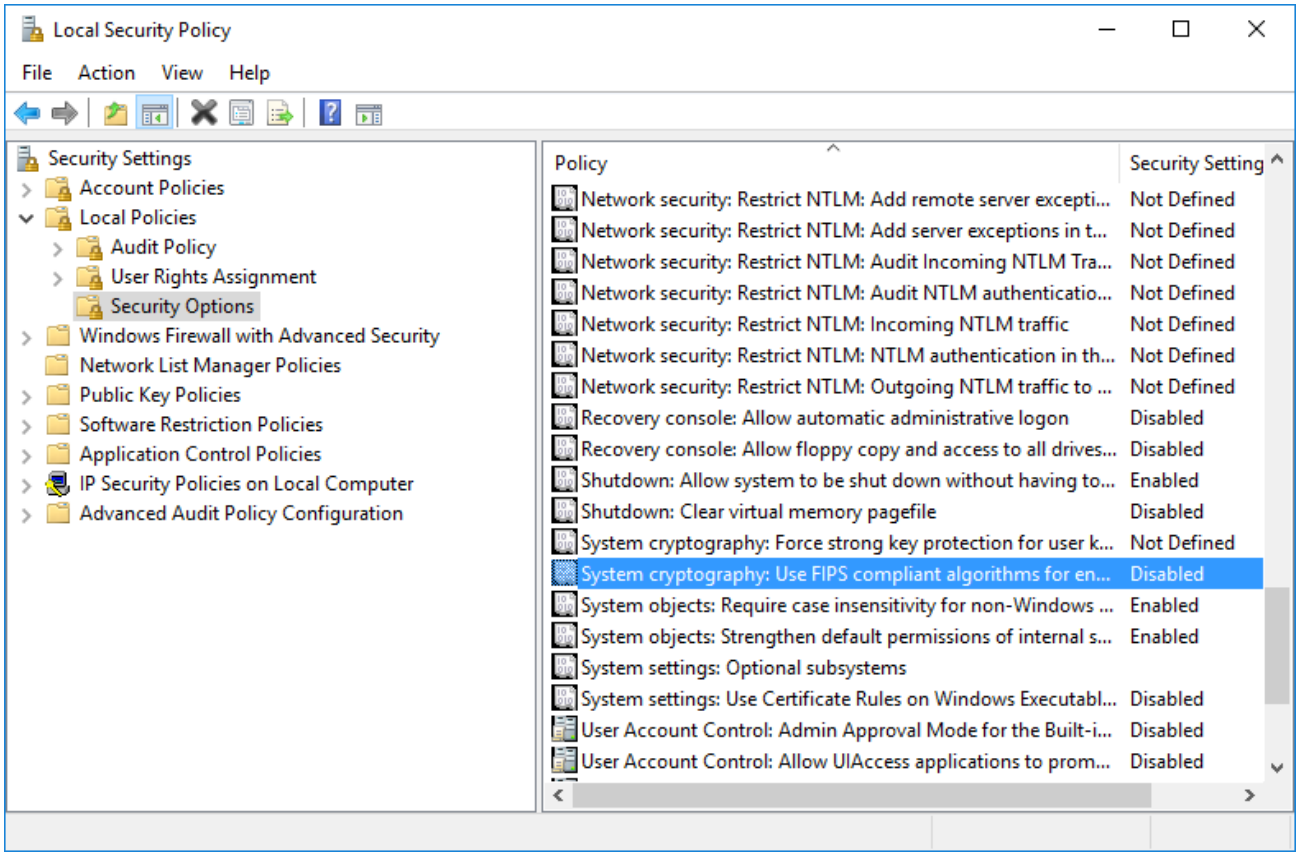

Рисунок 3. Параметры локальной политики безопасности

3. В дереве **Security Settings** раскройте узел **Local Policies** и выберите **Security Options**.
4. В столбце **Policy** дважды щелкните **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.
5. В открывшемся окне на вкладке **Local Security Settings** выберите **Disabled** и нажмите кнопку **OK**.

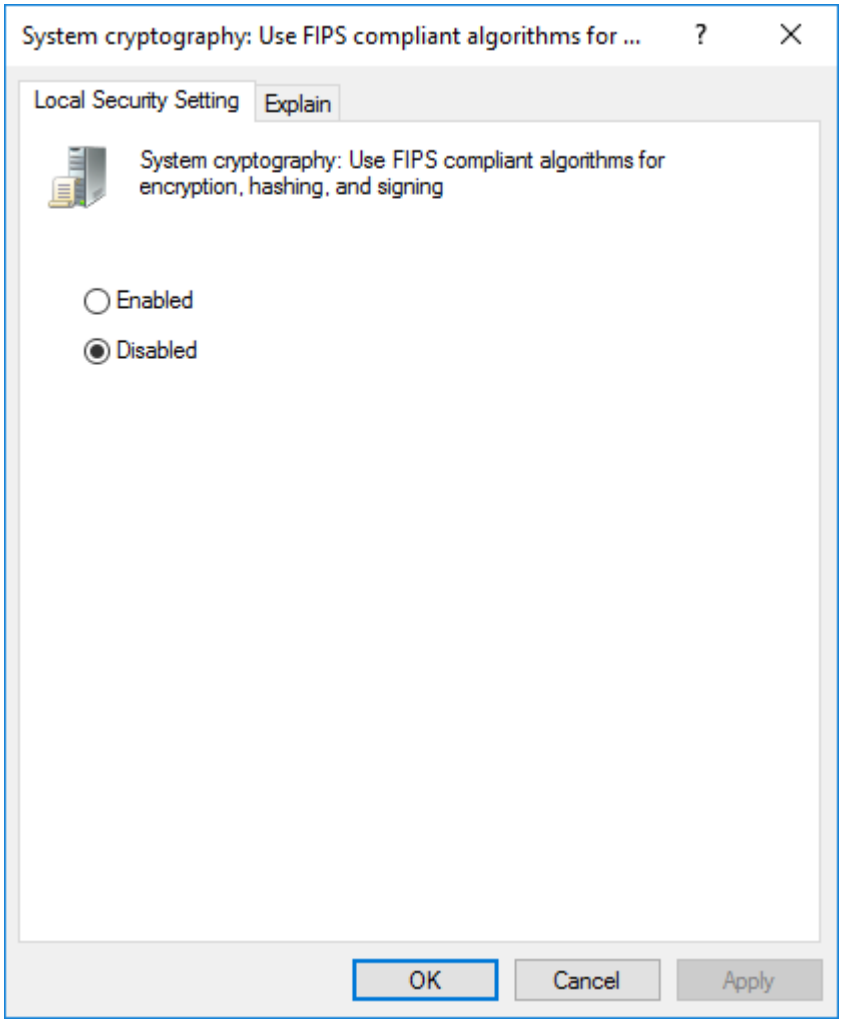

Рисунок 4. Отключение алгоритмов FIPS

FIPS Compliant Policy отключена.

Примечание. Вы можете отключить FIPS Compliant Policy в системном реестре, установив значение **0** для ключа HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\Enabled.

6.1.2. Развертывание Active Directory для "Личного кабинета участника"

Подготовка Active Directory для "Личного кабинета участника" включает в себя следующие этапы:

1. Установка роли Active Directory Domain Services.
2. Конфигурация доменных служб.
3. Установка роли Active Directory Certificate Services.

4. Установка сертификата и требований к паролю.
5. Создание контейнера Active Directory для хранения информации о пользователях участника.

В этом разделе

6.1.2.1. Конфигурация доменных служб

Внимание! После конфигурации доменных служб вам потребуется перезагрузить сервер с ролью Active Directory.

► Чтобы сконфигурировать доменные службы:

1. В панели задач в области уведомлений нажмите на значок центра уведомлений.

   Откроется окно **All Servers Task Details**.

2. По ссылке **Promote this server to a domain controller** назначьте сервер доменным контроллером.

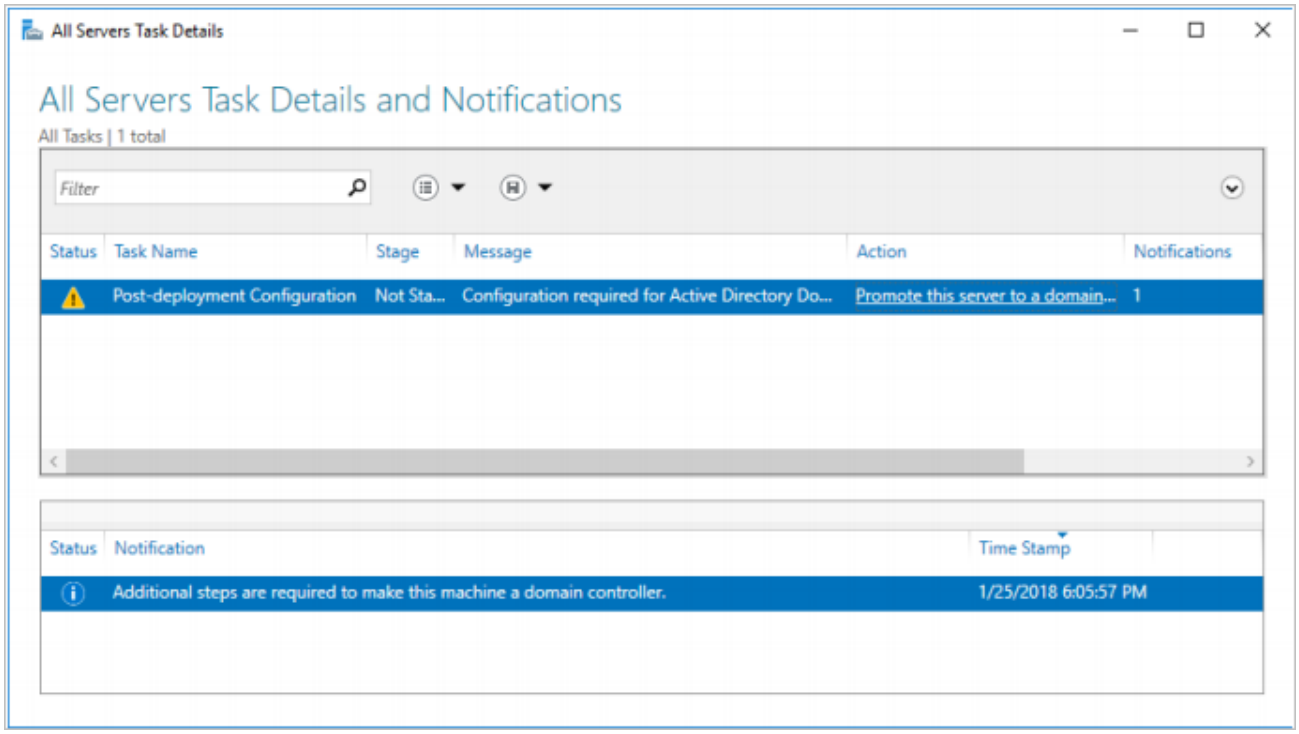

Рисунок 5. Назначение сервера доменным контроллером

3. С помощью мастера настройки доменных служб Active Directory добавьте новый лес доменов.
4. На вкладке **Domain Controller Options** установите флажки **Domain Name System (DNS) server** и **Global Catalog (GC)**.
5. Задайте пароль для восстановления (Directory Services Restore Mode (DSRM) password) в поле **Password** и повторите его в поле **Confirm password**.

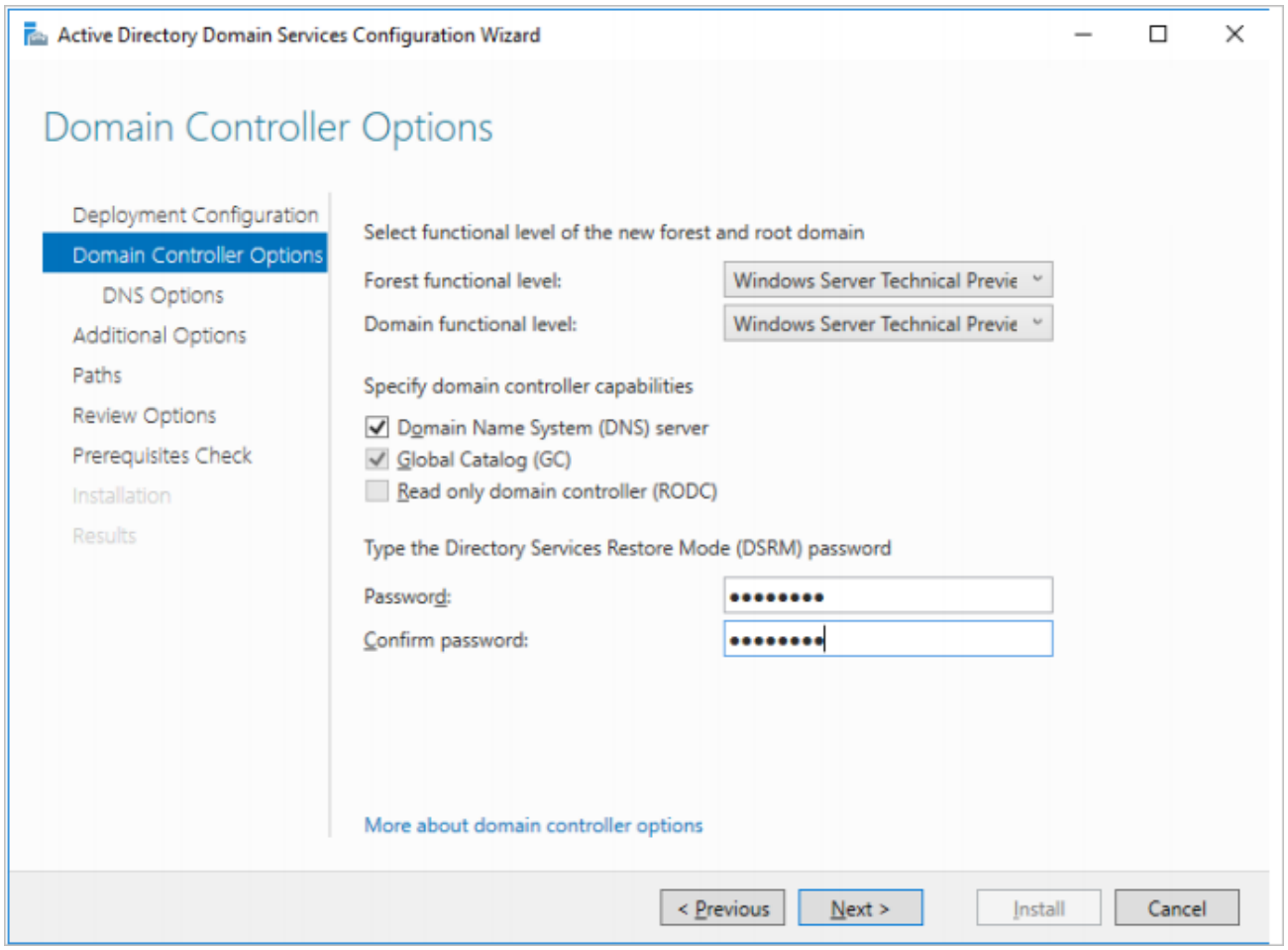

Рисунок 6. Настройка параметров доменного контроллера

6. На вкладке **Additional Options** укажите NetBIOS-имя домена.
7. На вкладке **Prerequisites Check** проверьте выполнение всех необходимых условий и нажмите кнопку **Install**.

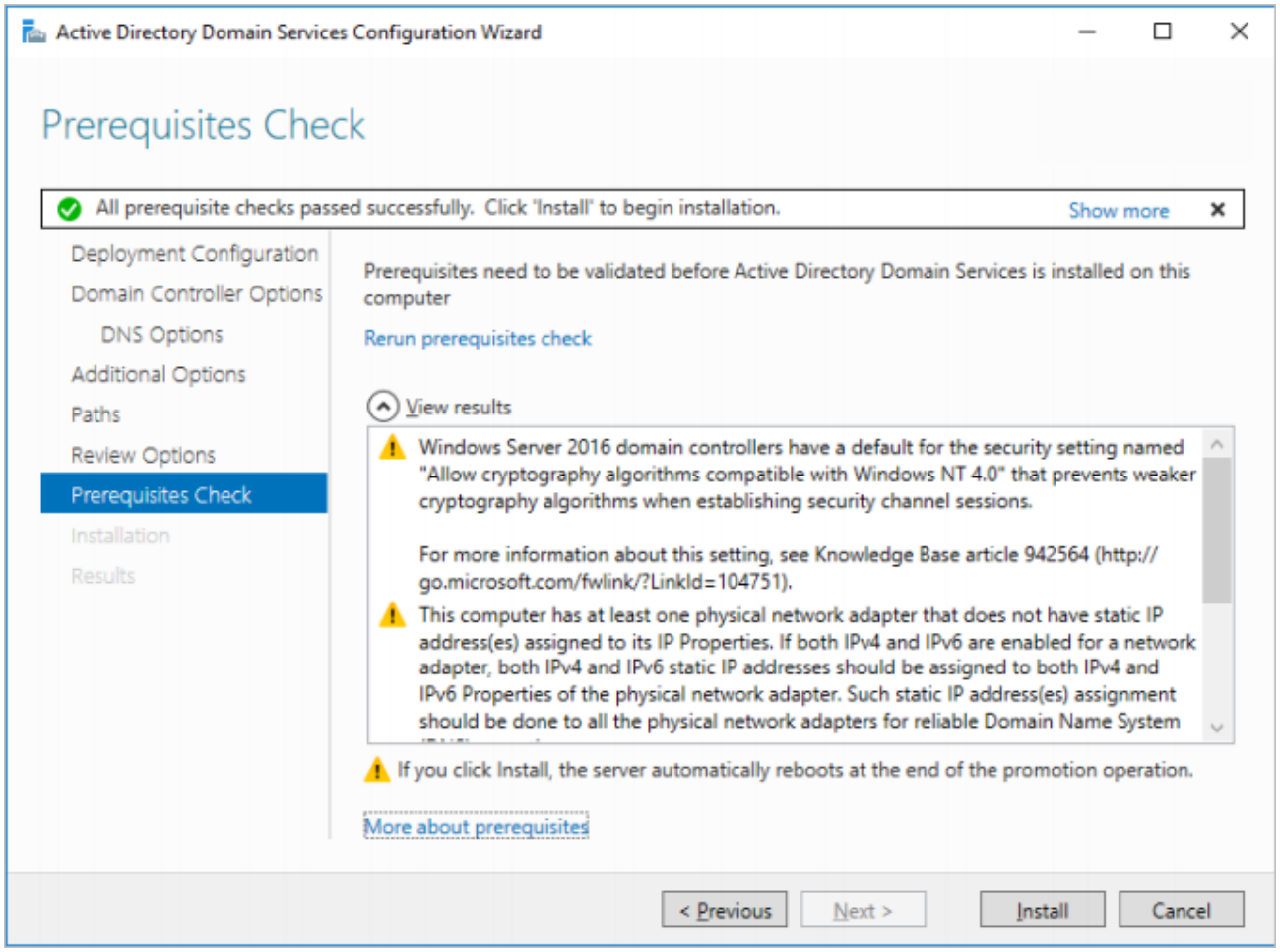

Рисунок 7. Завершение настройки доменных служб

8. Подключитесь к доменному контроллеру с помощью утилиты `ldp.exe`.
9. Выберите раздел каталога конфигураций `cn=Directory Service,CN=WindowsNT,CN=Services,CN=Configuration,dc=<имя домена>,dc=ru`.
10. Измените значение атрибута `dsHeuristics` на `000000001`.
11. Перезагрузите сервер с доменным контроллером.

Доменные службы сконфигурированы.

6.1.2.2. Установка роли Active Directory Certificate Services

► Чтобы установить роль Active Directory Certificate Services:

1. В мастере добавления ролей и компонентов Microsoft Windows на вкладке **Server Roles** установите флажок **Active Directory Certificate Services**.

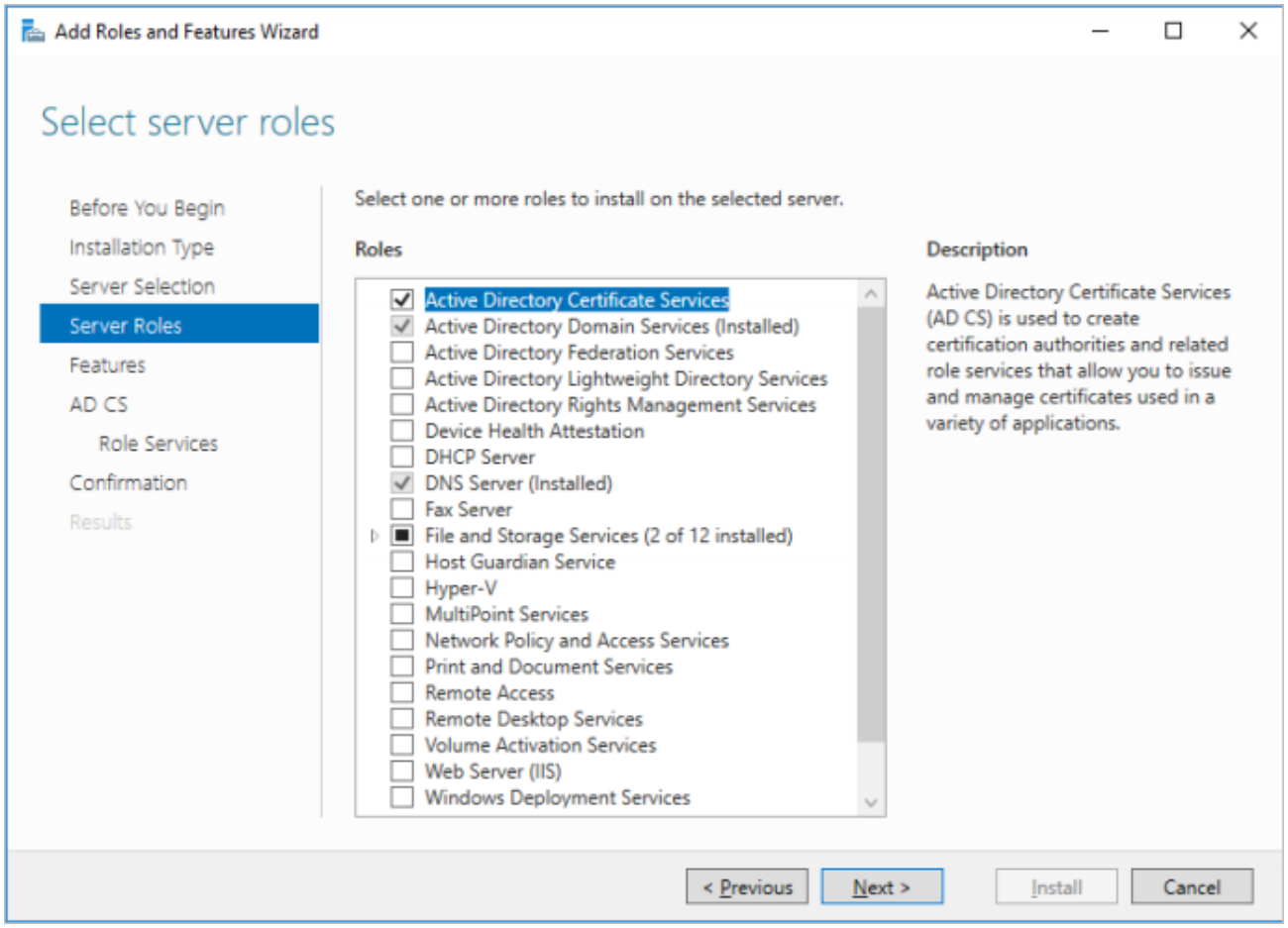

Рисунок 8. Добавление роли сервера

2. На вкладке **Role Services** установите флажок **Certification Authority**.

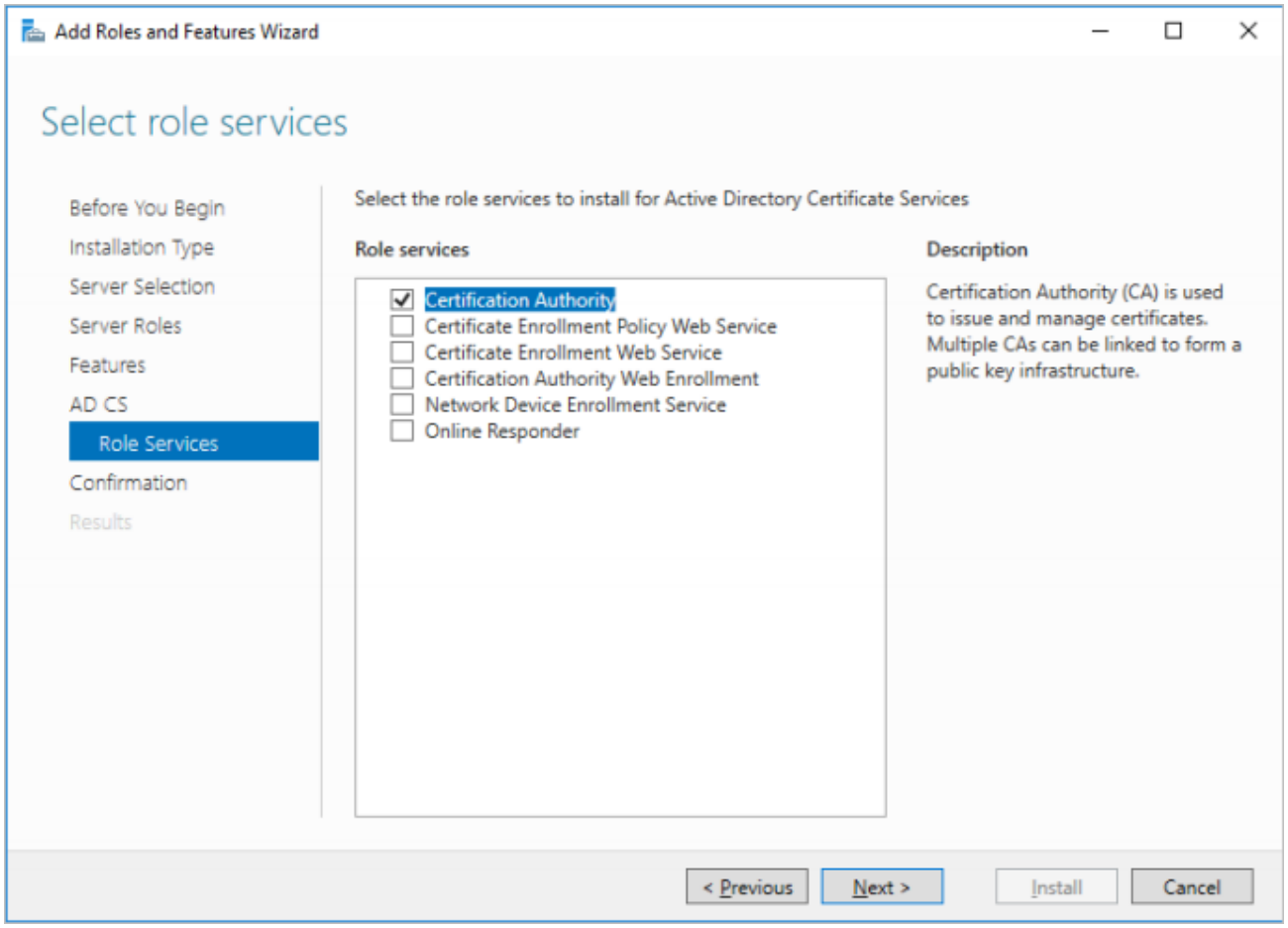

Рисунок 9. Настройка роли Certificate Services

3. Нажмите кнопку **Install** и дождитесь окончания установки роли.
4. В консоли Server Manager откройте окно **AD CS Configuration** по ссылке **Configure Active Directory Certificate Services**.
5. На вкладке **Credentials** укажите учетную запись доменного администратора.
6. На вкладке **Role Services** установите флажок **Certification Authority**.

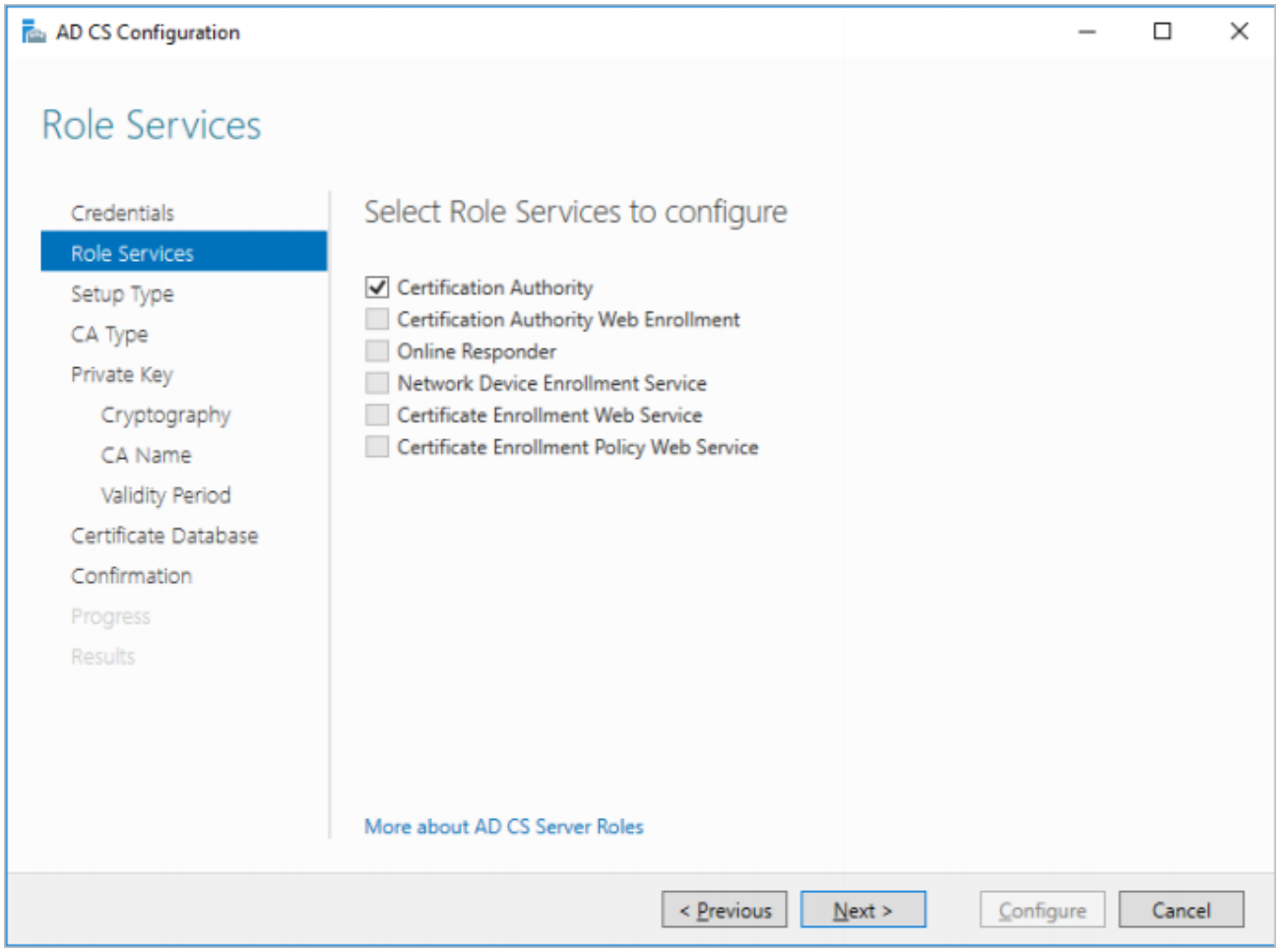

Рисунок 10. Настройка сервисов

7. На вкладке **Setup Type** выберите **Enterprise CA**.

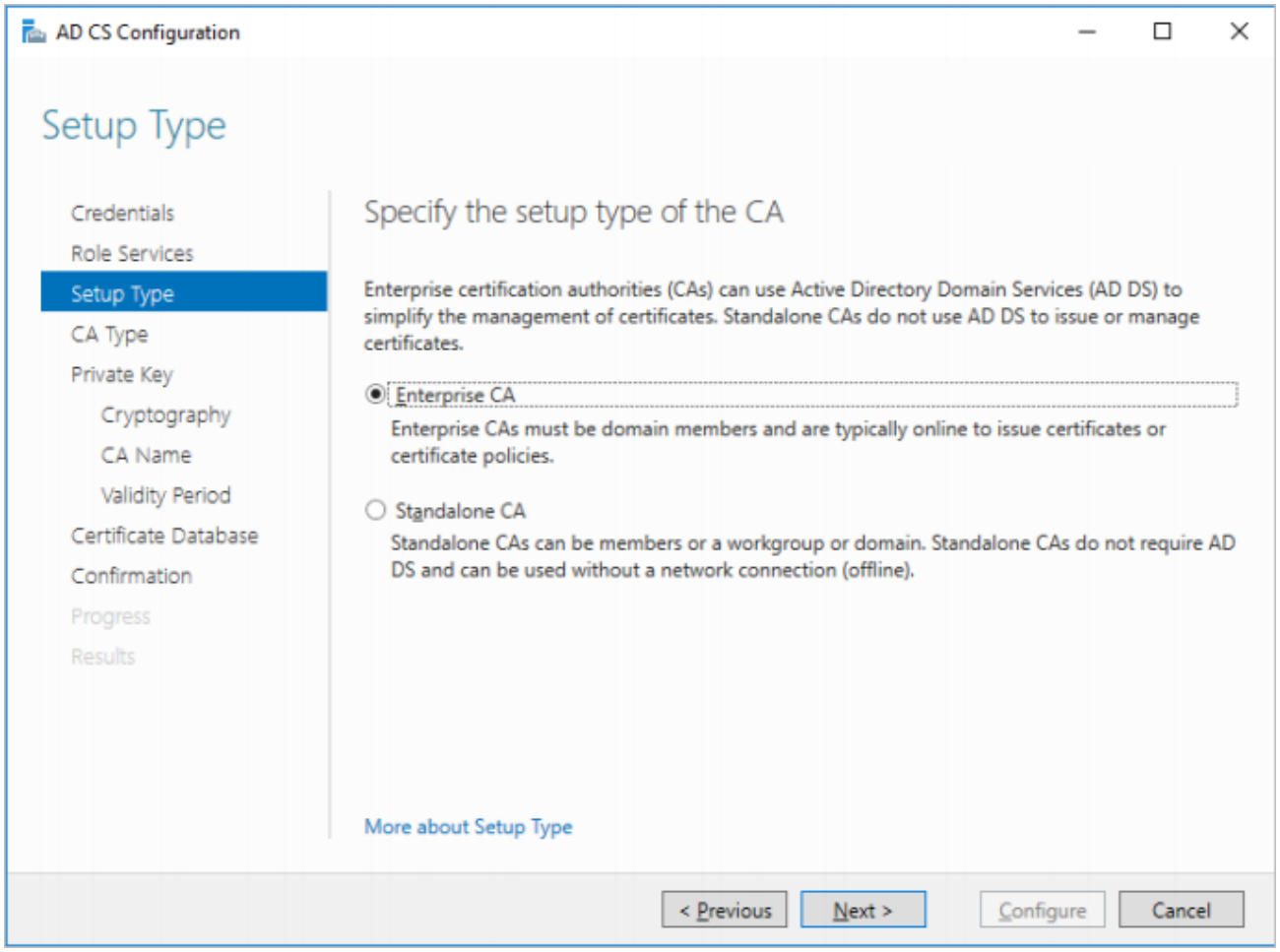

Рисунок 11. Выбор типа установки

8. На вкладке **CA Type** выберите **Root CA**.

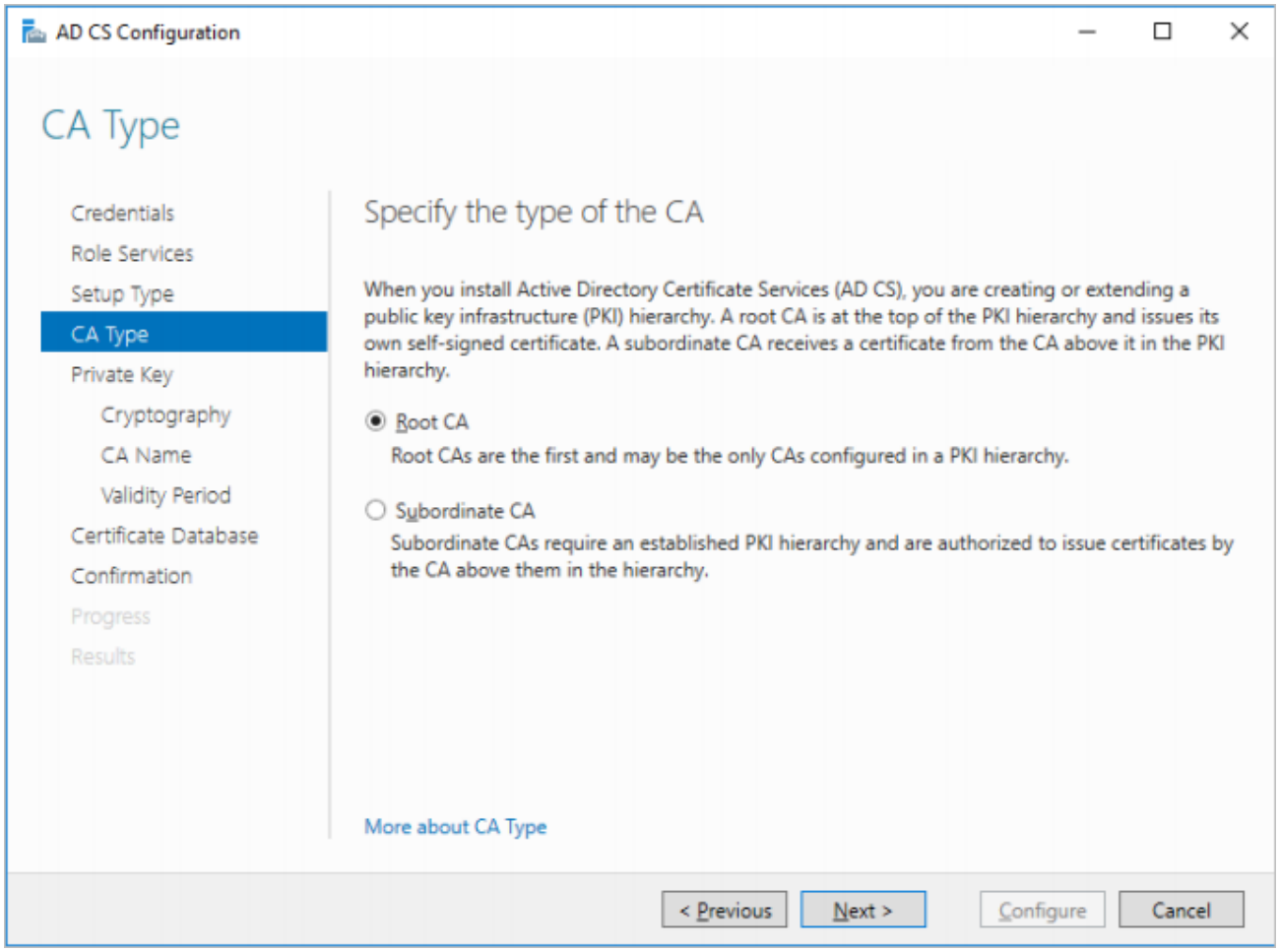

Рисунок 12. Выбор типа CA

9. На вкладке **Confirmation** проверьте указанные значения и нажмите кнопку **Configure**.

Роль Active Directory Certificate Services установлена.

6.1.2.3. Установка сертификата и требований к паролю

Внимание! После конфигурации доменных служб вам потребуется перезагрузить сервер с ролью Active Directory.

► Чтобы установить сертификат и требования к паролю:

1. В командной строке Windows выполните команду `C:\>certutil -ca.cert <имя домена>.crt`, чтобы выпустить сертификат.
2. В командной строке Windows выполните команду `gpupdate /force` для обновления групповых политик.
3. В консоли управления Microsoft нажмите Ctrl+M.

   Откроется окно **Add/Remove Snap-in**.

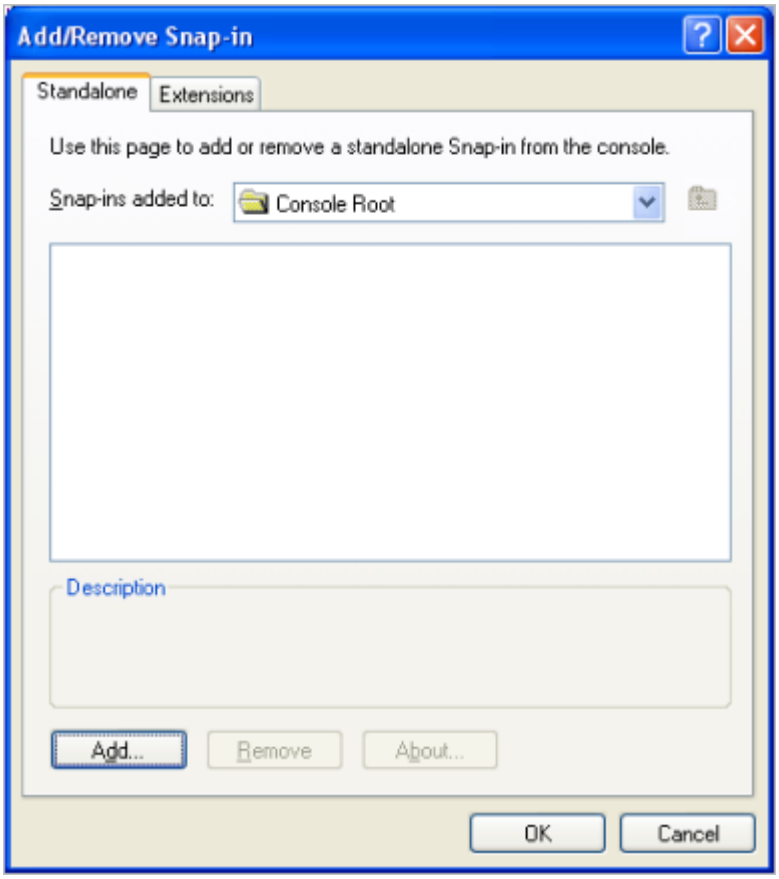

Рисунок 13. Добавление оснастки в консоли управления Microsoft

4. Нажмите кнопку **Add**.

   Откроется окно **Add Standalone Snap-in**.

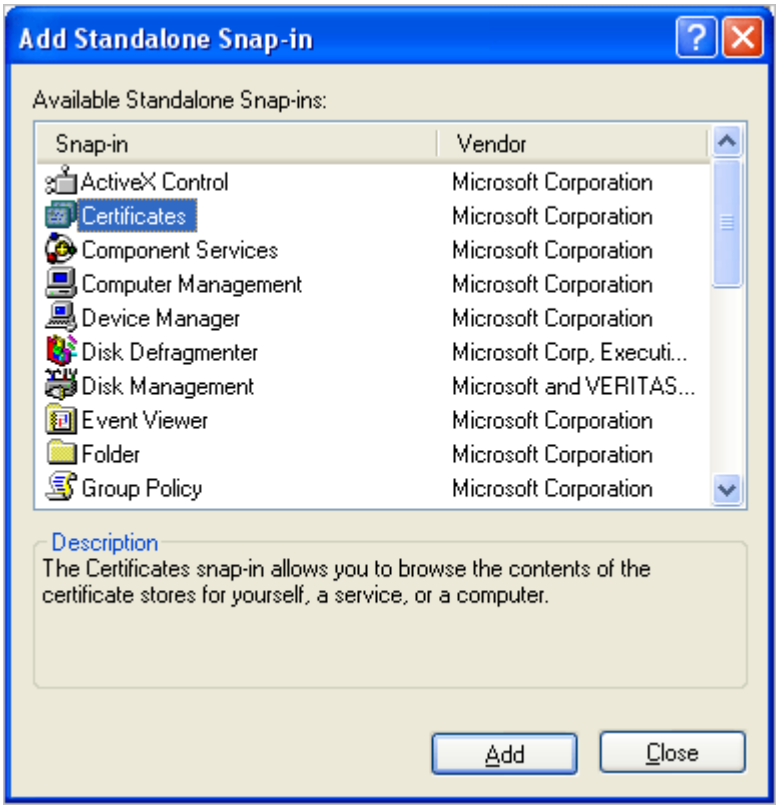

Рисунок 14. Добавление оснастки в консоли управления Microsoft

5. Выберите **Certificates** и нажмите кнопку **Add**.

   Откроется окно **Certificates snap-in**.

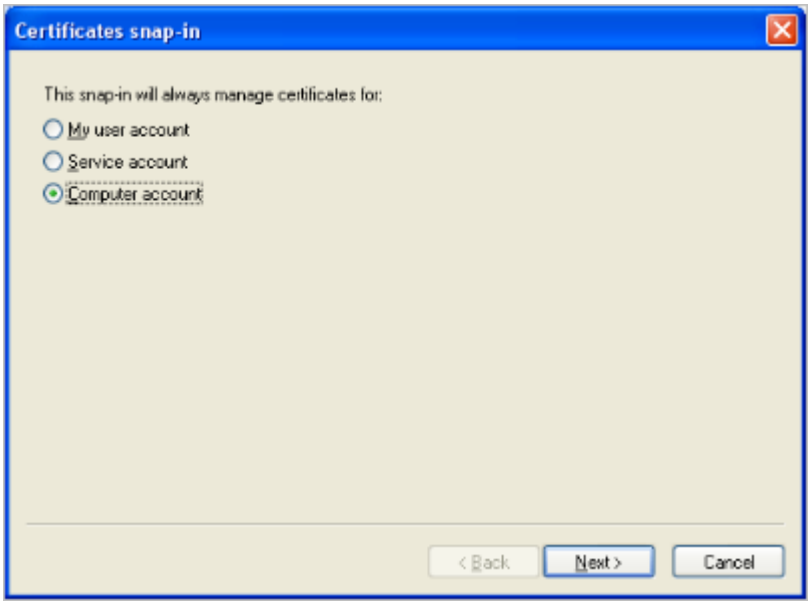

Рисунок 15. Добавление оснастки "Сертификаты"

6. Выберите **Computer account** и нажмите **Next**.

Откроется окно **Select Computer**.

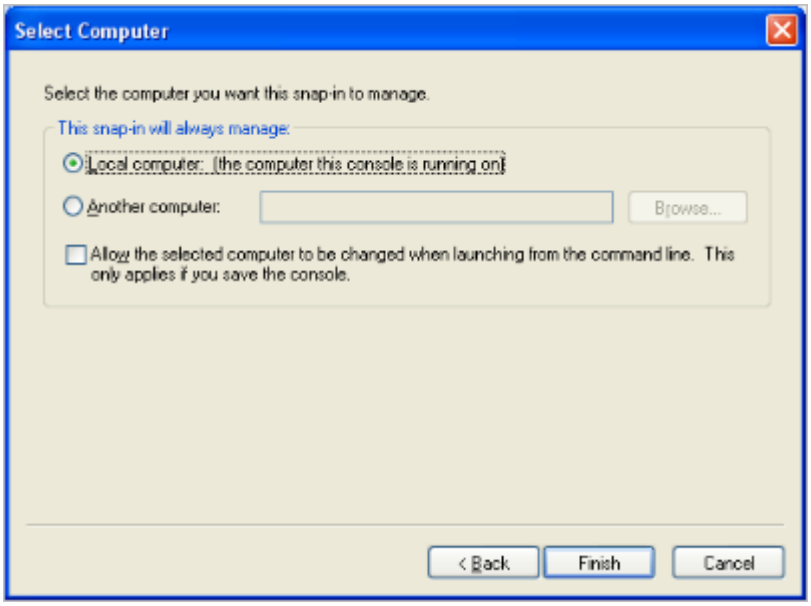

Рисунок 16. Выбор типа учетной записи

7. Выберите **Local computer** и нажмите **Finish**.
8. В окне **Add/Remove Snap-in** нажмите **OK**.

   В консоли управления Microsoft отобразится раздел **Certificates**.
9. Раскройте раздел **Certificates** и в контекстном меню раздела **Trusted Root Certification Authority** выберите **All Tasks** → **Import**.

   Запустится мастер импорта сертификатов.

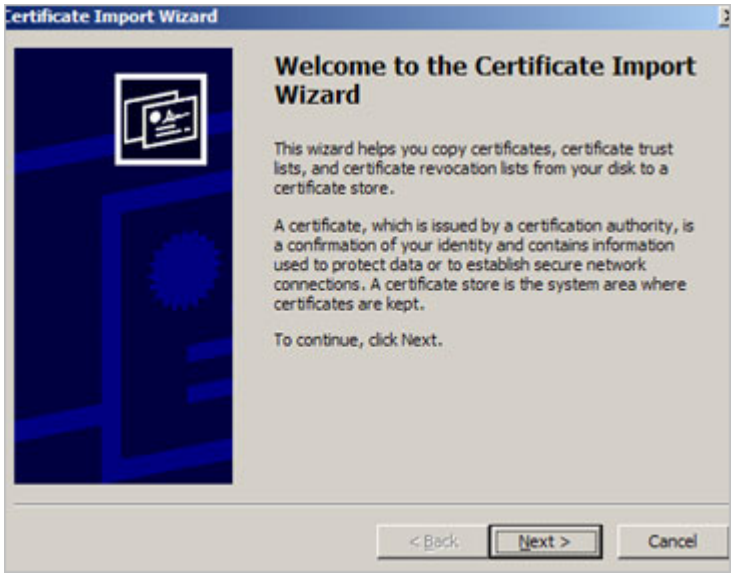

Рисунок 17. Приветственное окно мастера импорта сертификатов

10. Следуйте указаниям мастера.
11. Укажите IP-адрес доменного контроллера в файле `hosts` для установления SSL-соединения.
12. В редакторе групповых политик Windows в разделе **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Account Policies** → **Password Policy** установите требования к паролю.

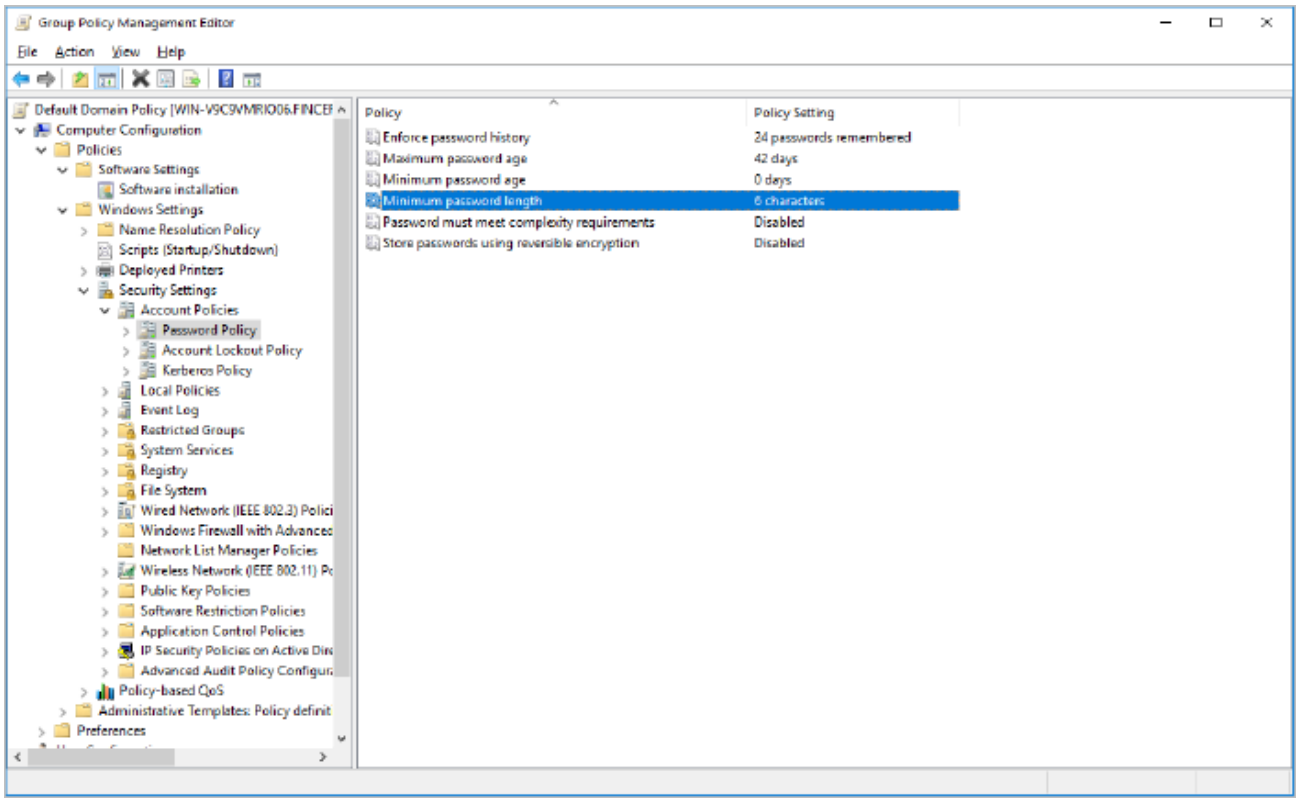

Рисунок 18. Установка требований к паролю с помощью групповой политики

13. Перезагрузите сервер с доменным контроллером.

Сертификат и требования к паролю установлены.

6.1.2.4. Создание контейнера Active Directory

► Чтобы создать контейнер Active Directory для хранения информации о пользователях участника:

1. На сервере с доменным контроллером запустите утилиту ADSI Edit.

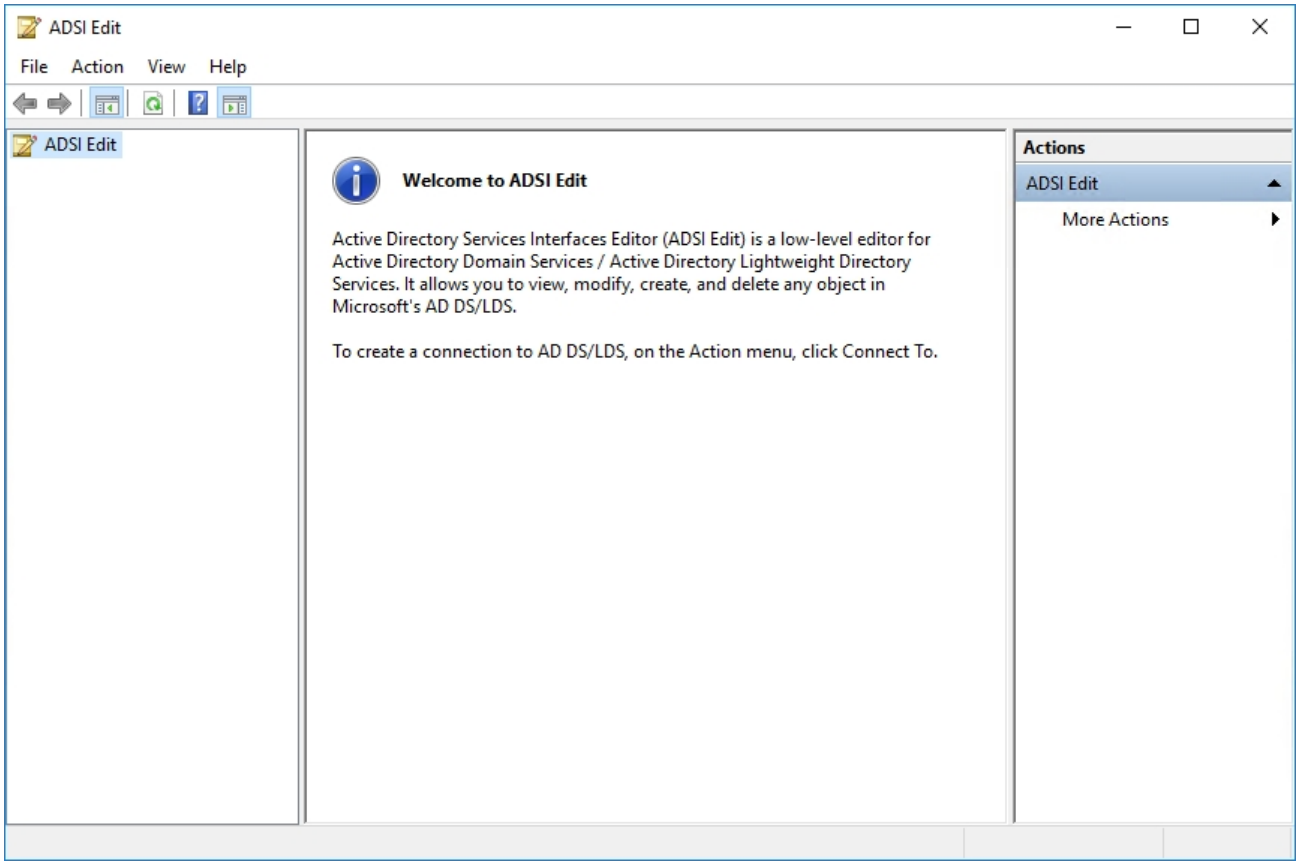

Рисунок 19. Консоль утилиты ADSI Edit

2. В панели управления в разделе **Action** выберите **Connect to**.

   Откроется окно **Connection Settings**.

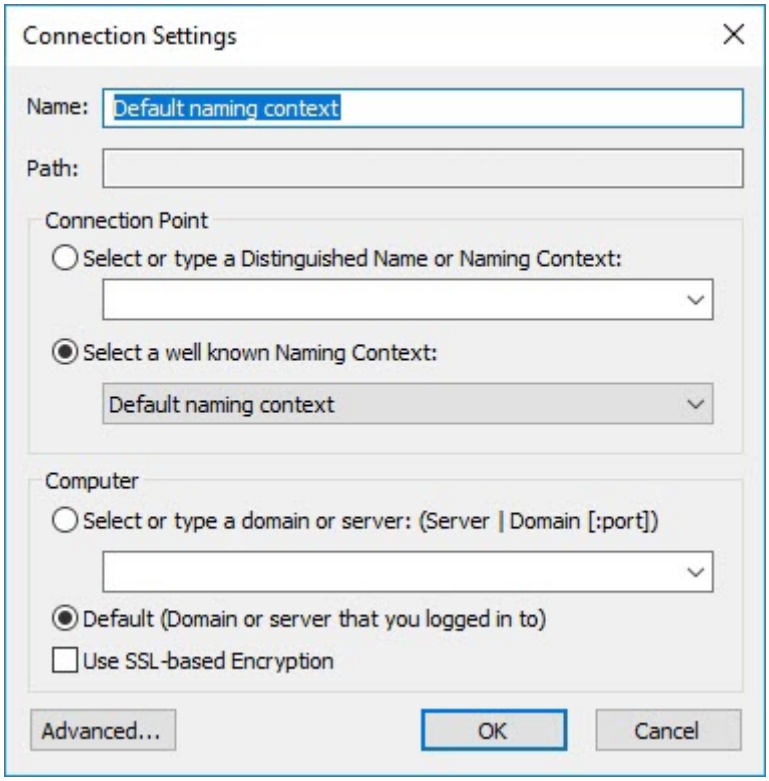

Рисунок 20. Подключение к Active Directory с помощью утилиты ADSI Edit

3. Нажмите кнопку **OK**.

   В консоли ADSI Edit отобразятся контейнеры Active Directory.

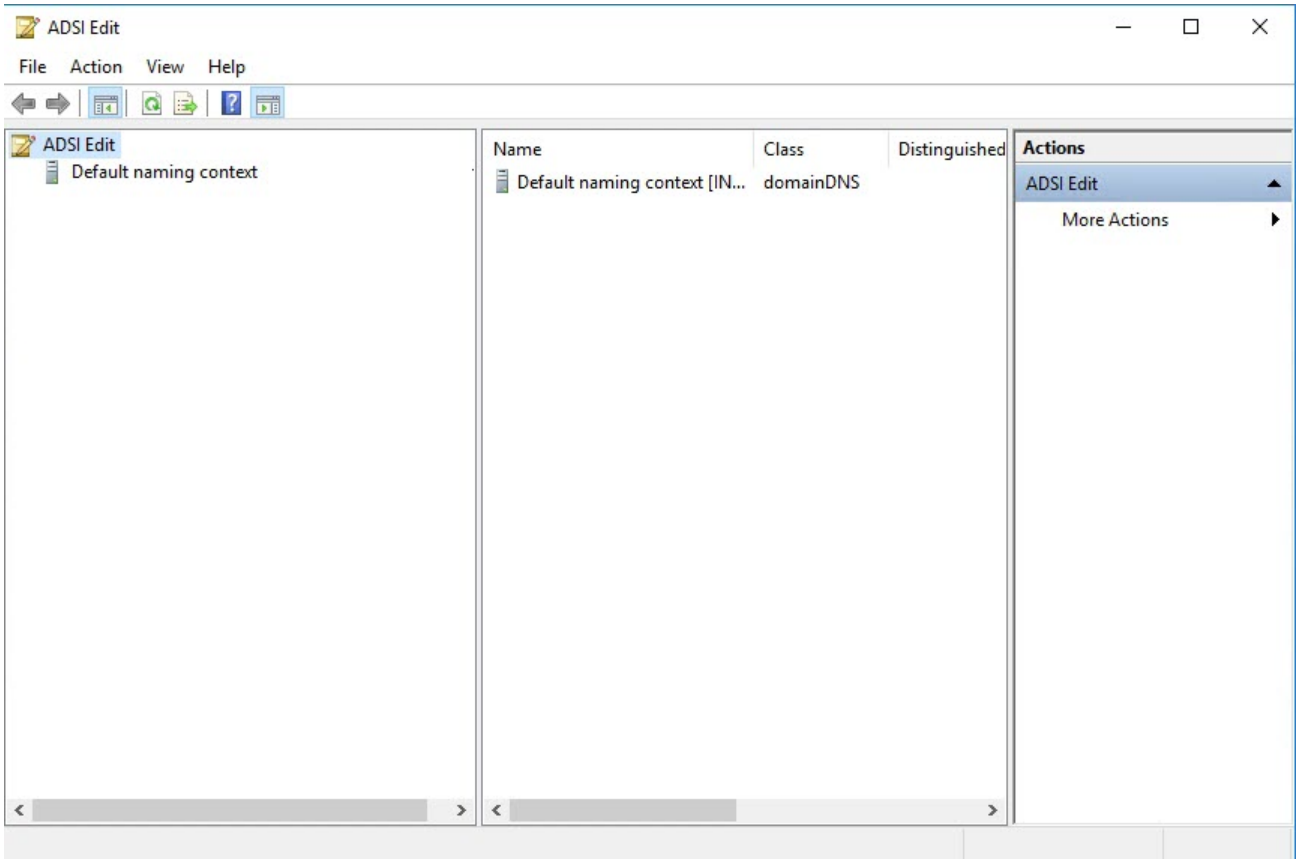

Рисунок 21. Консоль ADSI Edit после подключения к Active Directory

4. Раскройте узел **Default naming context** и в контекстном меню домена **DC=PTIPC,DC=local** выберите **New** → **Object**.

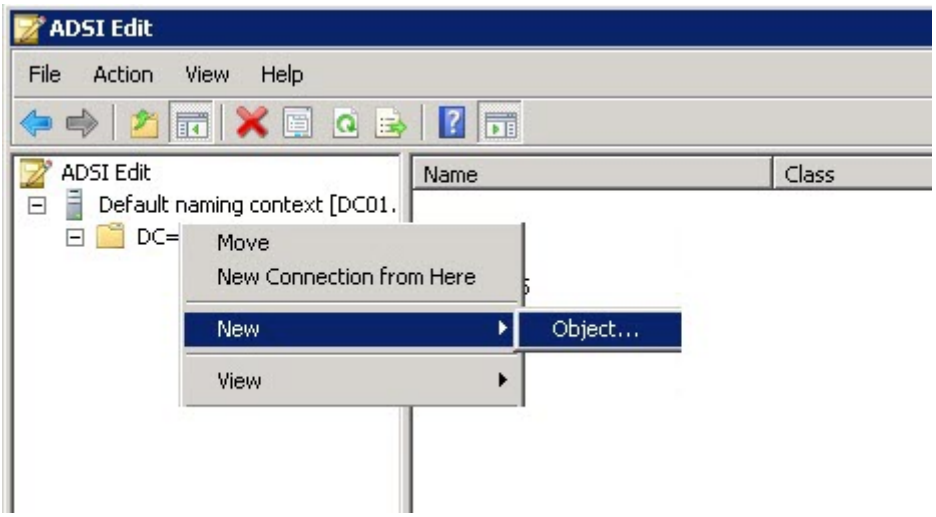

Рисунок 22. Создание нового объекта

Откроется окно **Create Object**.

5. В списке **Select a class** выберите **organizationalUnit** и нажмите кнопку **Next**.

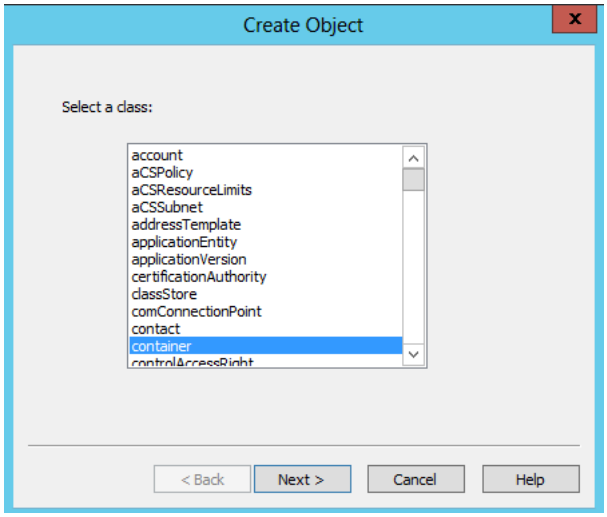

Рисунок 23. Выбор класса добавляемого объекта

6. В поле **Value** введите название контейнера `PTIPCMembers` и нажмите кнопку **Next**.

   Откроется окно подтверждения.

7. Нажмите кнопку **Finish**.

   Контейнер **PTIPCMembers** отобразится в консоли ADSI Edit.

8. В контекстном меню контейнера **PTIPCMembers** выберите **Properties**.

   Откроется окно **CN=PTIPCMembers Properties**.

9. Скопируйте значение параметра `distinguishedName` (например, `OU=PTIPCMembers,DC=PTIPC,DC=local`).

10. Установите это значение для параметра `ActiveDirectoryBaseDn`.

Контейнер Active Directory создан.

6.1.3. Установка "Личного кабинета участника"

► Чтобы установить "Личный кабинет участника":

1. Откройте папку `PTIPCParticipantsPortalDeployment.<номер_версии>` запустите файл `PTIPCParticipantsPortalSetup_<Номер версии>.exe`.

   Откроется окно мастера установки.

2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.

3. Установите флажок **Я прочитал(а) и согласен(согласна) с лицензионным соглашением** и нажмите кнопку **Продолжить**.

   Откроется окно с выбором компонентов для установки.

4. Снимите все флажки, чтобы установить только "Личный кабинет участника" и нажмите кнопку **Установить**.

Запустится процесс установки компонента.

5. Если требуется перезагрузить сервер, нажмите кнопку **Перезагрузить**.

   После перезагрузки сервера установка компонента продолжится автоматически. Мастер установки уведомит вас о завершении установки.

6. Нажмите кнопку **Закрыть**.

"Личный кабинет участника" установлен.

6.1.4. Установка PostgreSQL

► Чтобы установить СУБД PostgreSQL:

1. Откройте папку `PTIPCParticipantsPortalDeployment.<номер_версии>` и запустите файл `PTIPCParticipantsPortalSetup_<Номер версии>.exe`.

   Откроется окно мастера установки.

2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
3. Установите флажок **Я прочитал(а) и согласен(согласна) с лицензионным соглашением** и нажмите кнопку **Продолжить**.

   Откроется окно с выбором компонентов для установки.

4. Установите флажок **Установить PostgreSQL** и нажмите кнопку **Установить**.

   Запустится процесс установки компонента.

5. Если требуется перезагрузить сервер, нажмите кнопку **Перезагрузить**.

   После перезагрузки сервера установка компонента продолжится автоматически. Мастер установки уведомит вас о завершении установки.

6. Нажмите кнопку **Закрыть**.

СУБД PostgreSQL установлена.

6.1.5. Установка RabbitMQ

► Чтобы установить брокер сообщений RabbitMQ:

1. Откройте папку `PTIPCParticipantsPortalDeployment.<номер_версии>` и запустите файл `PTIPCParticipantsPortalSetup_<Номер версии>.exe`.

   Откроется окно мастера установки.

2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
3. Установите флажок **Я прочитал(а) и согласен(согласна) с лицензионным соглашением** и нажмите кнопку **Продолжить**.

   Откроется окно с выбором компонентов для установки.

4. Установите флажок **Установить RabbitMQ Server** и нажмите кнопку **Установить**.

Запустится процесс установки компонента.

5. Если требуется перезагрузить сервер, нажмите кнопку **Перезагрузить**.

   После перезагрузки сервера установка компонента продолжится автоматически. Мастер установки уведомит вас о завершении установки.

6. Нажмите кнопку **Закрыть**.

RabbitMQ установлен.

6.1.6. Установка "Информационного портала"

► Чтобы установить "Информационный портал":

1. Запустите файл `InfoPortalDeployment.exe`.

   Откроется окно мастера установки.

2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.

3. Установите флажок **Я прочитал(а) и согласен(согласна) с лицензионным соглашением** и нажмите кнопку **Продолжить**.

   Запустится процесс установки портала.

   Если для установки потребуется перезагрузка сервера, мастер установки уведомит об этом.

   После перезагрузки сервера установка портала продолжится автоматически. Мастер установки уведомит вас о завершении установки.

"Информационный портал" установлен и доступен по адресу http://<IP-адрес или FQDN сервера>.

Примечание. Одновременно с "Информационным порталом" на сервер устанавливается Microsoft SQL Server, необходимый для создания базы данных хранения информации "Информационного портала".

6.1.7. Первоначальная настройка в контуре участника

Команды, приведенные в этом разделе, нужно выполнять в интерфейсе командной строки Windows PowerShell от имени администратора.

Сразу после развертывания необходимо интегрировать независимые инсталляции компонентов в рамках контура, настроить интерфейсы и уточнить конфигурации.

► Чтобы настроить PT Incident Processing Center в контуре участника:

1. Настройте интеграцию "Личного кабинета участника" со службой Active Directory:
   ```
   ptipc set -p ActiveDirectoryHost '<ParticipantServer_FQDN>' ActiveDirectoryPort '389'
   ActiveDirectorySslPort '636' ActiveDirectoryTransportSecurity 'ssl' ActiveDirectoryUserDn
   'CN=root,CN=users,DC=ad1,DC=ru' ActiveDirectoryPassword 'P@ssw0rd' ActiveDirectoryBaseDn
   'DC=ad1,DC=ru'
   ```
2. Настройте интеграцию "Личного кабинета участника" с СУБД PostgreSQL:
   ```
   ptipc set –p PostgresHost '<PostgreSQL_IP-address>' PostgresPort '5432' PostgresLogin
   'pt_system' PostgresPassword 'P@ssw0rdP@ssw0rd'
   ```

   Примечание. Настроить перечисленную выше конфигурацию также можно непосредственно в файле `InstallationParameters.xml`. Получить параметры можно по команде `ptipc get -f InstallationParameters.xml`, а применить изменения – по команде `ptipc set -f InstallationParameters.xml`.
3. Скорректируйте параметры PostgreSQL в конфигурационном файле `postgresql.conf`:
   ```
   max_prepared_transactions = 600
   max_connections = 300
   shared_buffers = 6GB
   ```
4. Перезапустите сервис PostgreSQL:
   ```
   service postgresql restart
   ```
5. Установите для "Информационного портала" режим `Slave`. Для этого на сервере, где установлен "Информационный портал", выполните команду:
   ```
   infoportal set -p Mode Slave
   ```
6. Настройте параметры сбора данных по событиям PT Incident Processing Center для PT MaxPatrol SIEM:
   ```
   ptipc set -p SiemLoggingDik '<Путь к лог-файлам>' SiemStorageInterval '<Количество дней
   хранения файлов журналов>'
   ```

Взаимодействие компонентов системы настроено.

6.2. Развертывание PT Incident Processing Center в открытом контуре

Серверная площадка открытого контура базируется в IT-инфраструктуре центра и включает все компоненты PT Incident Processing Center, необходимые для информационного обмена с участниками системы, анализа запросов и расследования инцидентов информационной безопасности.

Каждый компонент развертывается на отдельном сервере.

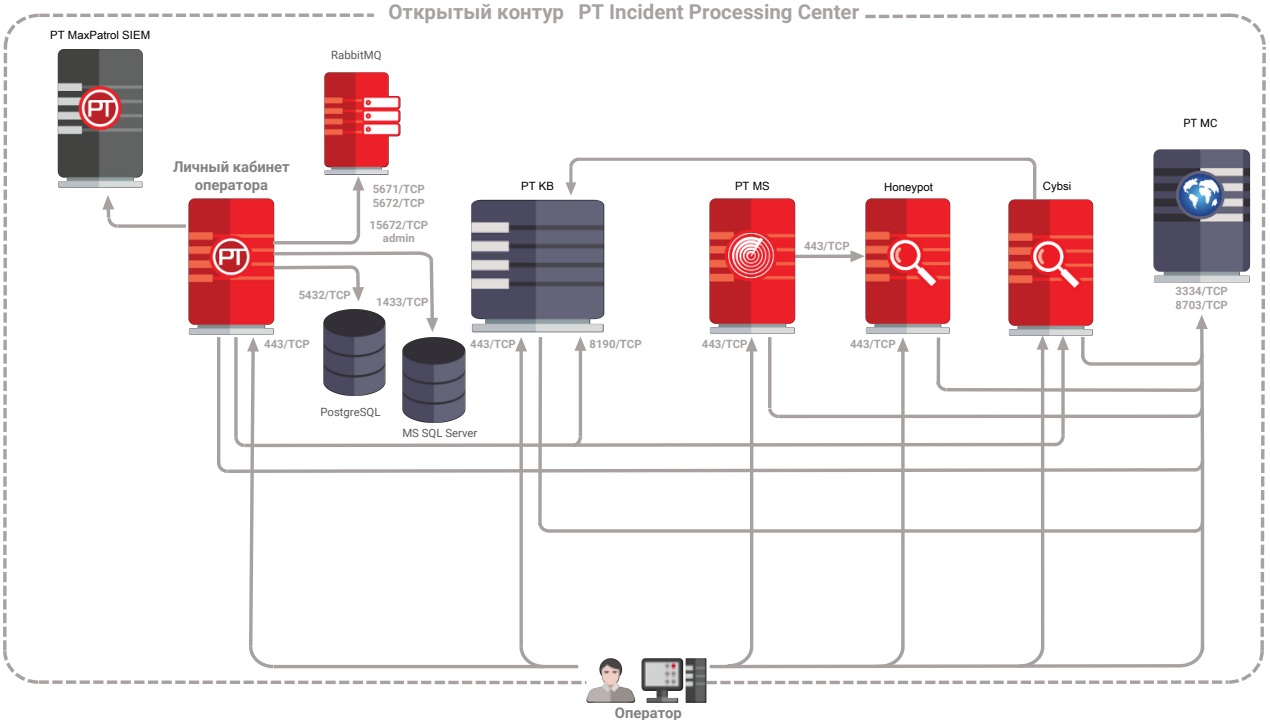

Рисунок 24. Схема развертывания в открытом контуре

В рамках данного руководства не описано развертывание PT MS, Honeypot, PT MC и PT KB. За дополнительной информацией обратитесь к документации этих продуктов.

Внимание! Перед развертыванием PT Incident Processing Center убедитесь, что сервис единого входа PT MC установлен на отдельном сервере. На этом сервере должны быть открыты порты 3334 и 8507. Серверы PT MC и PT Incident Processing Center должны быть синхронизированы по времени.

В этом разделе

6.2.1. Настройка контейнера Active Directory

► Чтобы настроить контейнер Active Directory:

1. На сервере с доменным контроллером запустите утилиту ADSI Edit.

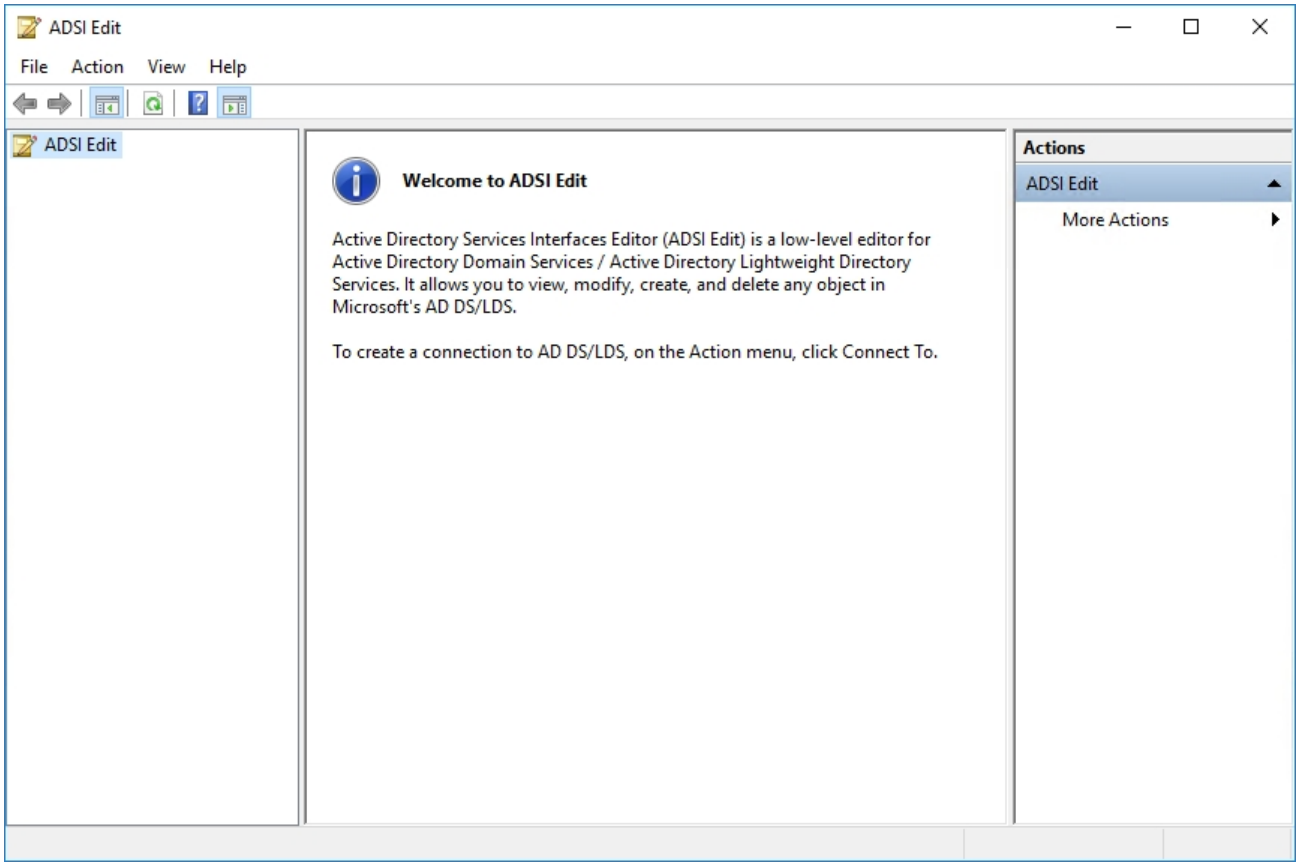

Рисунок 25. Консоль утилиты ADSI Edit

2. В панели управления в разделе **Action** выберите **Connect to**.

   Откроется окно **Connection Settings**.

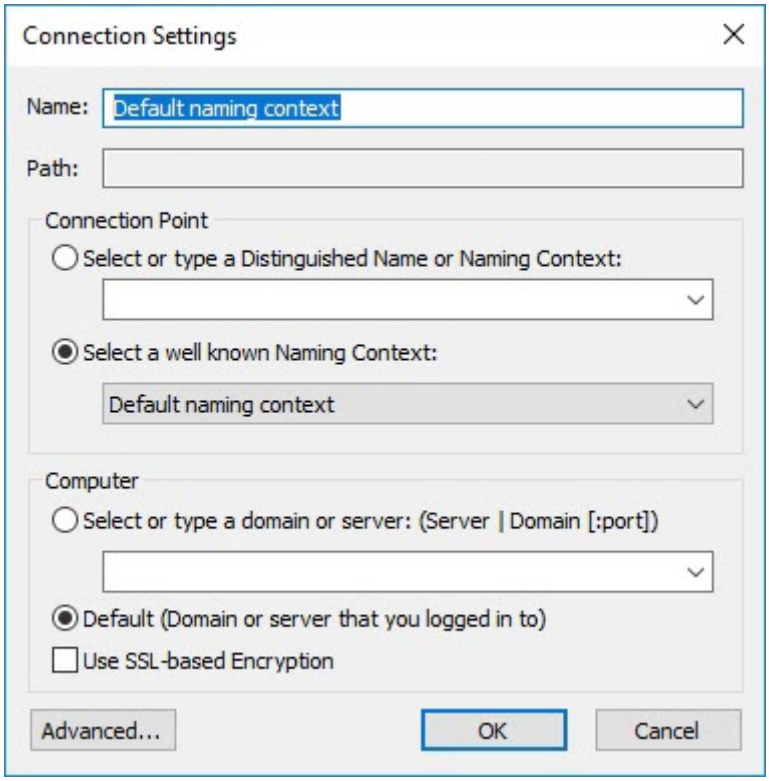

Рисунок 26. Подключение к Active Directory с помощью утилиты ADSI Edit

3. Нажмите кнопку **OK**.

   В консоли ADSI Edit отобразятся контейнеры Active Directory.

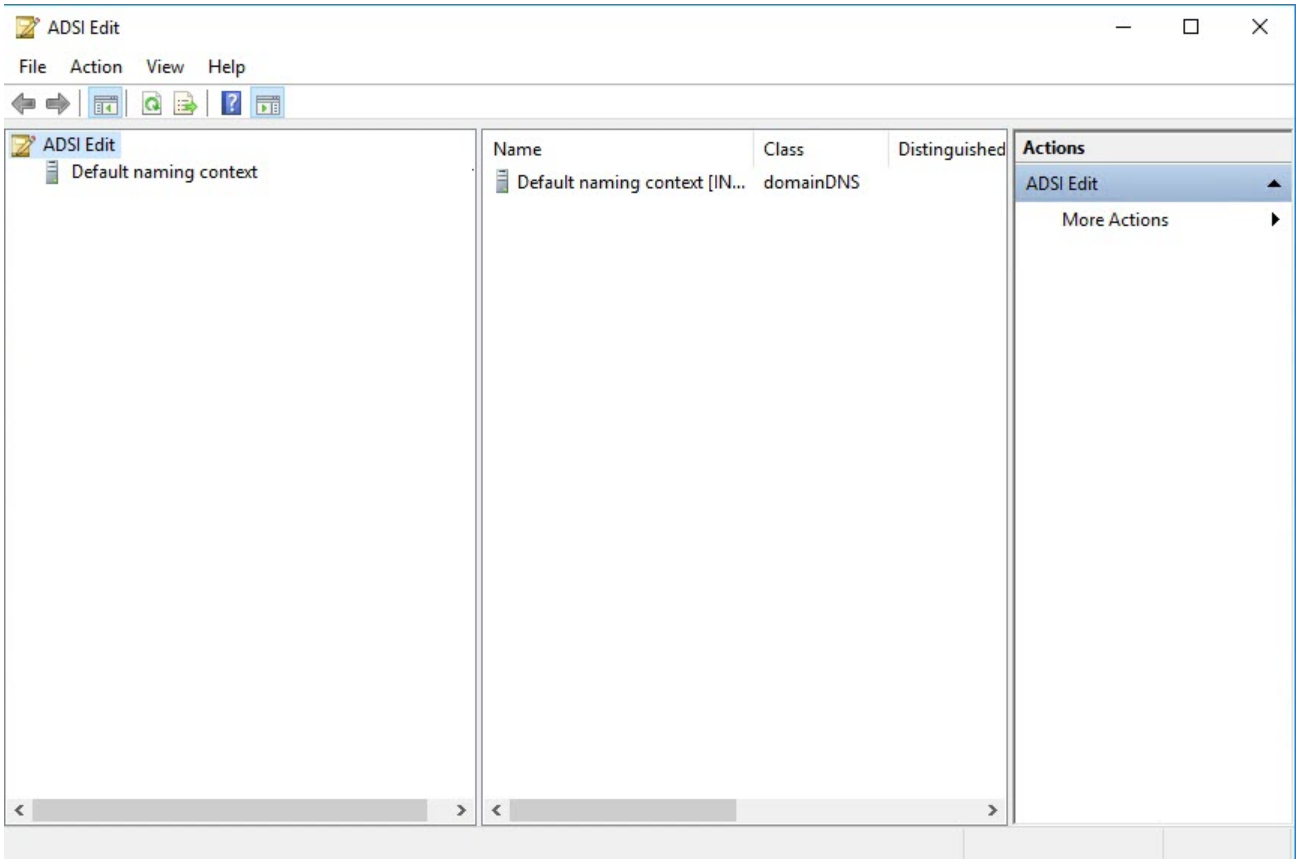

Рисунок 27. Консоль ADSI Edit после подключения к Active Directory

4. Раскройте узел **Default naming context** → **DC=ptipc,DC=local** и удалите все контейнеры из **OU=PTIPCMembers**.

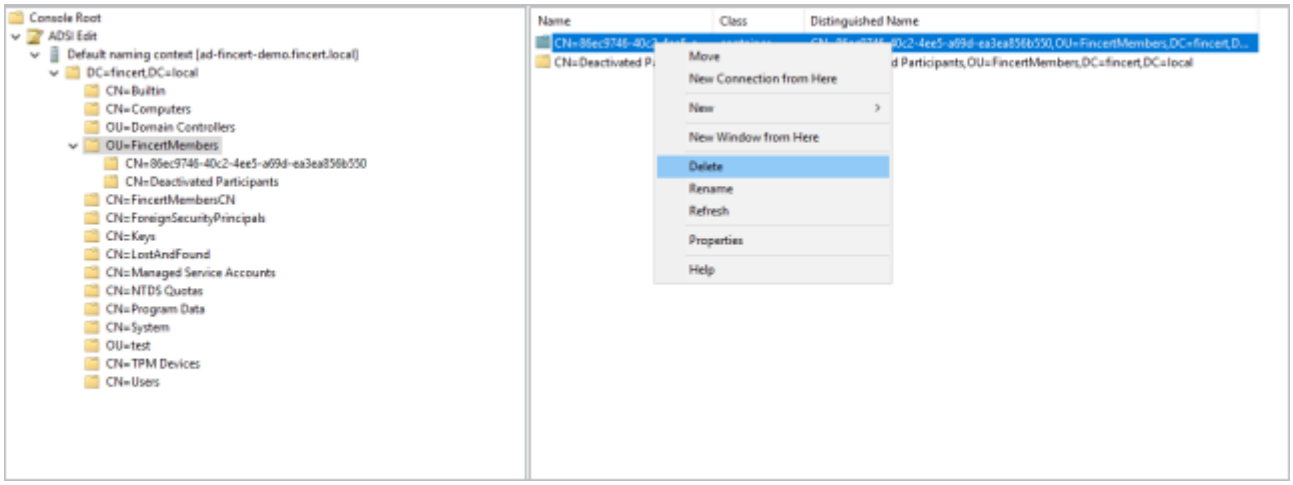

Рисунок 28. Удаление контейнеров Active Directory

Контейнер Active Directory настроен.

6.2.2. Установка "Личного кабинета оператора" в открытом контуре

► Чтобы установить "Личный кабинет оператора":

1. Откройте папку `PTIPCDeployment.<Номер версии>` и запустите файл `PTIPCSetup_<Номер версии>`.

   Откроется окно мастера установки.

2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.

   Откроется окно с выбором компонентов для установки.

   Запустится процесс установки компонента.

3. Если требуется перезагрузить сервер, нажмите кнопку **Перезагрузить**.

   После перезагрузки сервера установка компонента продолжится автоматически. Мастер установки уведомит вас о завершении установки.

4. Нажмите кнопку **Закрыть**.

"Личный кабинет оператора" установлен.

Примечание. Одновременно с "Личным кабинетом оператора" на сервер устанавливаются Python 3.5.4 и Microsoft .NET, необходимые для корректной работы микросервисов.

6.2.3. Установка PostgreSQL

► Чтобы установить СУБД PostgreSQL:

1. Откройте папку `PTIPCDeployment.<Номер версии>` и запустите файл `PTIPCSetup_<Номер версии>`.

   Откроется окно мастера установки.

2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.

3. Установите флажок **Я прочитал(а) и согласен(согласна) с лицензионным соглашением** и нажмите кнопку **Продолжить**.

   Откроется окно с выбором компонентов для установки.

4. Установите флажок **Установить PostgreSQL** и нажмите кнопку **Установить**.

   Запустится процесс установки компонента.

5. Если требуется перезагрузить сервер, нажмите кнопку **Перезагрузить**.

После перезагрузки сервера установка компонента продолжится автоматически. Мастер установки уведомит вас о завершении установки.

6. Нажмите кнопку **Закрыть**.

СУБД PostgreSQL установлена.

6.2.4. Установка RabbitMQ

► Чтобы установить брокер сообщений RabbitMQ:

1. Откройте папку `PTIPCDeployment.<Номер версии>` и запустите файл `PTIPCSetup_<Номер версии>`.

   Откроется окно мастера установки.

2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
3. Установите флажок **Я прочитал(а) и согласен(согласна) с лицензионным соглашением** и нажмите кнопку **Продолжить**.

   Откроется окно с выбором компонентов для установки.

4. Установите флажок **Установить RabbitMQ Server** и нажмите кнопку **Установить**.

   Запустится процесс установки компонента.

5. Если требуется перезагрузить сервер, нажмите кнопку **Перезагрузить**.

   После перезагрузки сервера установка компонента продолжится автоматически. Мастер установки уведомит вас о завершении установки.

6. Нажмите кнопку **Закрыть**.

RabbitMQ установлен.

6.2.5. Настройка интеграции с Cybsi

Перед настройкой интеграции вам нужно получить адрес Cybsi, ключ API Cybsi и идентификатор этого ключа у администратора Cybsi.

В этом разделе

См. также

Cybsi (см. раздел 4.7.5)

6.2.5.1. Настройка подключения к Cybsi

► Чтобы настроить подключение к Cybsi:

1. В открытом контуре PT Incident Processing Center на узле с установленным "Личным кабинетом оператора" перейдите в папку `C:\Program Files\Positive Technologies\PTIPC\ArtifactsService\pluggable_enrichers_zip`.
2. Извлеките из архива `cybsi.zip` файл `cybsi/config.ini` и откройте его.
3. В секции `ENVIRONMENT` в параметре `CYBSI_API_URL` измените URL Cybsi.
4. В секции `AUTH` в параметре `CYBSI_API_KEY` укажите ключ API Cybsi.
5. Сохраните файл `config.ini` и обновите его в архиве `cybsi.zip`.
6. Перезапустите микросервис PT.SP.Artifacts (см. приложение А), чтобы применить изменения.

Подключение к Cybsi настроено.

6.2.5.2. Настройка получения ссылок на результаты обогащения в Cybsi

Поиск ссылок с результатами обогащения артефактов PT Incident Processing Center в интерфейсе Cybsi можно настроить в файле `clinker.json`.

► Чтобы настроить получение ссылок на результаты обогащения в Cybsi:

1. Скопируйте архив `cybsilinker.zip` в папку `C:\Program Files\Positive Technologies\PTIPC\ArtifactsService\pluggable_enrichers_zip`.
2. Перезапустите микросервис PT.SP.Artifacts (см. приложение А).
3. Перейдите в папку `C:\Program Files\Positive Technologies\PTIPC\ArtifactsService\pluggable_enrichers\cybsilinker`.
4. Откройте файл `clinker.json`.
5. В параметре `CybsiPath` укажите URL запроса к API на получение информации об артефакте в формате URL API `https://<Корневой URL API Cybsi>/observable/entities`.
6. В параметре `CybsiUser` введите логин для авторизации в API Cybsi.
7. В параметре `CybsiPass` введите пароль для авторизации в Cybsi.
8. В параметре `CybsiObjUrl` укажите URL пользовательского интерфейса Cybsi.
9. Сохраните файл.

Получение ссылок на результаты обогащения в Cybsi настроено.

6.2.5.3. Настройка источников Cybsi для обогащения файлов

Вы можете настроить возможность обогащения информации о файлах в PT Incident Processing Center с помощью анализаторов кода и песочниц, являющихся источниками информации для Cybsi.

Таблица 11. Анализаторы кода и песочницы в Cybsi

Название	Тип в конфигурации
Positive Technologies MultiScanner (PT MS)	`ptms`
Trend Micro Deep Discovery Analyzer	`ddan`
RU-CERT Pyshok	`pyshok`
RU-CERT VirusLocal	`viruslocal`

► Чтобы настроить источники Cybsi:

1. Выполните запрос к API Cybsi, чтобы получить информацию о подключенных к нему анализаторах кода и песочницах:

   ```
   curl -u <Идентификатор ключа API>:<Ключ API> -H "Accept:application/vnd.ptsecurity.app-v2"
   -H "Content-type:application/json" http://<Адрес Cybsi>/enrichment/config/rules
   ```

   Например:

   ```
   curl -u ptipc:P@ssw0rd -H "Accept:application/vnd.ptsecurity.app-v2" -H "Content-
   type:application/json" http://cybsi.example.com/enrichment/config/rules
   ```

   Команда выведет JSON-массив с информацией об источниках Cybsi.

2. Из полученного на предыдущем шаге JSON-массива извлеките идентификаторы источников.

   Идентификаторы хранятся в ключах `dataSources` → `<JSON-объект с информацией об источнике>` → `uuid`.

3. В открытом контуре PT Incident Processing Center на узле с установленным "Личным кабинетом оператора" перейдите в папку `C:\Program Files\Positive Technologies \PTIPC\ArtifactsService\pluggable_enrichers_zip`.

4. Извлеките из архива `cybsi.zip` файл `cybsi/config.ini` и откройте его.

5. В секции `FILE_ANALYZERS` составьте список источников, от которых Cybsi должен получать данные о файлах.

   Каждый источник должен записываться в виде отдельной строки:

   ```
   <Название типа источника: ptms, viruslocal, ddan или pyshok>=<Идентификатор источника,
   полученный на шаге 2>
   ```

   Например:

   ```
   ptms=5f4d0290-98dc-4f51-bd48-ed34ac081a0e
   ```

6. В секции `FILE_ANALYZERS` в параметре `ON_SAVE_ANALYZERS` через запятую перечислите названия типов источников Cybsi, которые должны автоматически использоваться для получения информации о файлах.

Например:
`ON_SAVE_ANALYZERS=viruslocal,ptms`

Примечание. Для включения функции автоматического получения информации о файлах вам также нужно настроить конфигурацию в файле `artifactsRules.yaml`. Подробная информация приведена в разделе "Включение автоматического обогащения" в Справочном руководстве по конфигурированию системы.

7. Сохраните файл `config.ini` и обновите его в архиве `cybsi.zip`.
8. Перезапустите микросервис PT.SP.Artifacts (см. приложение А), чтобы применить изменения.

Источники Cybsi настроены.

6.2.6. Настройка интеграции с PT KB

► Чтобы настроить интеграцию с PT KB:

1. В открытом контуре PT Incident Processing Center на узле с установленным "Личным кабинетом оператора" перейдите в папку `C:\Program Files\Positive Technologies\PTIPC\ArtifactsService\pluggable_enrichers_zip`.
2. Извлеките из архива `ptkb.zip` файл `ptbk/config.ini` и откройте его.
3. Скорректируйте параметры:
```
PTKB_HOST=<IP-адрес PT KB>
PTKB_API_DB=<База данных PT KB>
```
4. Сохраните файл `config.ini` и обновите его в архиве `ptkb.zip`.
5. Перезапустите микросервис PT.SP.Artifacts (см. приложение А), чтобы применить изменения.

Интеграция с PT KB настроена.

См. также

PT KB (см. раздел 4.7.2)

6.2.7. Интеграция компонентов в открытом контуре

Команды, приведенные в этом разделе, нужно выполнять в интерфейсе командной строки Windows PowerShell от имени администратора.

Сразу после развертывания необходимо интегрировать независимые инсталляции компонентов в рамках контура, настроить интерфейсы и уточнить конфигурации.

► Чтобы интегрировать компоненты в открытом контуре:

1. Интегрируйте сервер "Личного кабинета оператора" с сервисом единого входа PT MC:
```
C:\Users\Administrator> ptipc set -p HostAddress <PTIPCServerId/FQDN> IAMHostAddress <IAM
Server IP/FQDN> IAMApplicationId <Application Id(string)>
```
2. Настройте интеграцию "Личного кабинета оператора" со службой Active Directory:
```
C:\Users\Administrator> ptipc set -p ActiveDirectoryHost '<PTIPCServer_FQDN>'
ActiveDirectoryPort '389' ActiveDirectorySslPort '636' ActiveDirectoryTransportSecurity
'ssl' ActiveDirectoryUserDn 'CN=root,CN=users,DC=ad1,DC=ru' ActiveDirectoryPassword
'P@ssw0rd' ActiveDirectoryBaseDn 'DC=ad1,DC=ru'
```
3. Настройте интеграцию "Личного кабинета оператора" с СУБД PostgreSQL:
```
C:\Users\Administrator> ptipc set –p PostgresHost '<PostgreSQL_IP-address>' PostgresPort
'5432' PostgresLogin 'pt_system' PostgresPassword 'P@ssw0rdP@ssw0rd'
```
4. Настройте взаимосвязь "Личного кабинета оператора" с компонентом PT MS:
```
C:\Users\Administrator> ptipc set –p MSBaseUrl '<MultiScanner_FQDN> 'MSLogin 'admin'
MSPasswrod 'admin' MSAutoScanMaxFileSize '10485760'
```
5. Настройте взаимосвязь "Личного кабинета оператора" с компонентом PT KB:
```
C:\Users\Administrator> ptipc set –p PtkbAddress '<Ptkb_IP-address:port>'
```

   Примечание. Настроить перечисленную выше конфигурацию также можно непосредственно в файле `InstallationParameters.xml`. Получить параметры можно по команде `ptipc get -f InstallationParameters.xml`, а применить изменения – по команде `ptipc set -f InstallationParameters.xml`.

6. Скорректируйте параметры PostgreSQL в конфигурационном файле `postgresql.conf`:
```
max_prepared_transactions = 600
max_connections = 300
shared_buffers = 6GB
```
7. Перезапустите сервис PostgreSQL:
```
service postgresql restart
```
8. Настройте параметры сбора данных по событиям PT Incident Processing Center для PT MaxPatrol SIEM:
```
ptipc set -p SiemLoggingDik '<Путь к лог-файлам>' SiemStorageInterval '<Количество дней
хранения файлов журналов>'
```

Компоненты интегрированы.

6.2.8. Настройка почты в открытом контуре

Команды, приведенные в этом разделе, нужно выполнять в интерфейсе командной строки Windows PowerShell от имени администратора.

► Чтобы настроить почту в открытом контуре:

1. Скопируйте текущую конфигурацию:
```
ptipc get -f c:\tmp\ptipc_conf.xml
```
2. Откройте файл `c:\tmp\ptipc_conf.xml`.

3. Добавьте или измените следующий параметр входящей почты:
```
param id="MailboxesConfiguration" value='mapi+ssl://<Логин почты>@<Адрес почтового
сервера>:<Порт почтового сервера>/<Адрес входящей почты 1>:<Папка, из которой читаются
письма>?remove_on_read=<no/trash/permanently>&amp;password=<Пароль>&amp;reply_id=<ID
SMTPConfiguration>&scan_interval=<Интервал чтения почты в секундах>&#xA; mapi+ssl://<Логин
почты>@<Адрес почтового сервера>:<Порт почтового сервера>/<Адрес входящей почты N>:<Папка,
из которой читаются письма>?remove_on_read=<no/trash/
permanently>&amp;password=<пароль>&amp;reply_id=<ID
SMTPConfiguration>&scan_interval=<Интервал чтения почты в секундах>'
```
4. Сохраните файл.
5. Примените конфигурацию входящей почты:
```
ptipc set -f c:\tmp\ptipc_conf.xml
```
6. Настройте исходящую почту:
```
C:\Users\Administrator> ptipc set -p EmailSenderEnabled 'false'
```

Почта настроена.

6.3. Развертывание PT Incident Processing Center в закрытом контуре

Серверная площадка закрытого контура располагается в IT-инфраструктуре центра и на ней устанавливаются три компонента для работы с информацией ограниченного доступа в рамках PT Incident Processing Center:

— "Личный кабинет оператора" с зависимостями, необходимыми для корректной работы;

— Сервис единого входа PT MC;

— "Информационный портал" с зависимостями.

Каждый компонент развертывается на отдельном сервере.

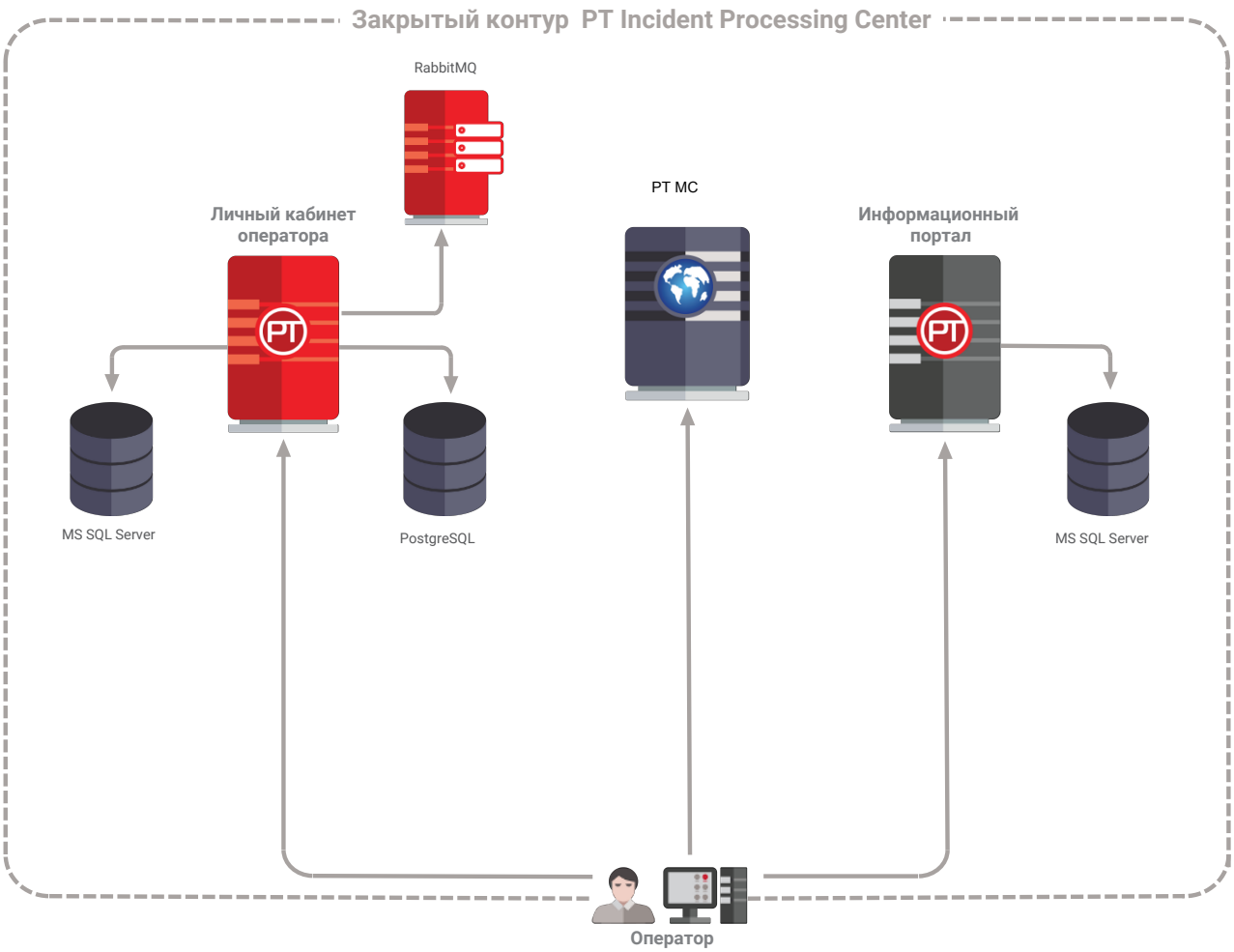

Рисунок 29. Схема развертывания в закрытом контуре

В этом разделе

6.3.1. Подготовка к установке PT Incident Processing Center в закрытом контуре

Перед установкой вам нужно убедиться в следующем:

— На отдельном сервере развернут сервис единого входа PT MC.

  Внимание! На сервере, где установлен PT MC, должны быть открыты порты 3334 и 8507 и серверы PT MC и PT Incident Processing Center должны быть синхронизированы по времени.

— На сервере для установки "Информационного портала" отключена FIPS Compliant Policy (см. раздел 6.3.2).

Вам потребуются следующие дистрибутивы:

— `PTIPCDeployment<Номер версии>.exe` — для установки Личного кабинета оператора, необходимых зависимостей, RabbitMQ и PostgreSQL.

— `InfoPortalDeployment.exe` — дистрибутив для установки Инфромационного портала и его зависимостей.

6.3.2. Отключение FIPS Compliant Policy

► Чтобы отключить FIPS Compliant Policy:

1. В Панели управления выберите **Система и безопасность** → **Администрирование**.
2. В открывшемся окне выберите **Локальная политика безопасности**.

   Откроется окно **Локальная политика безопасности**.

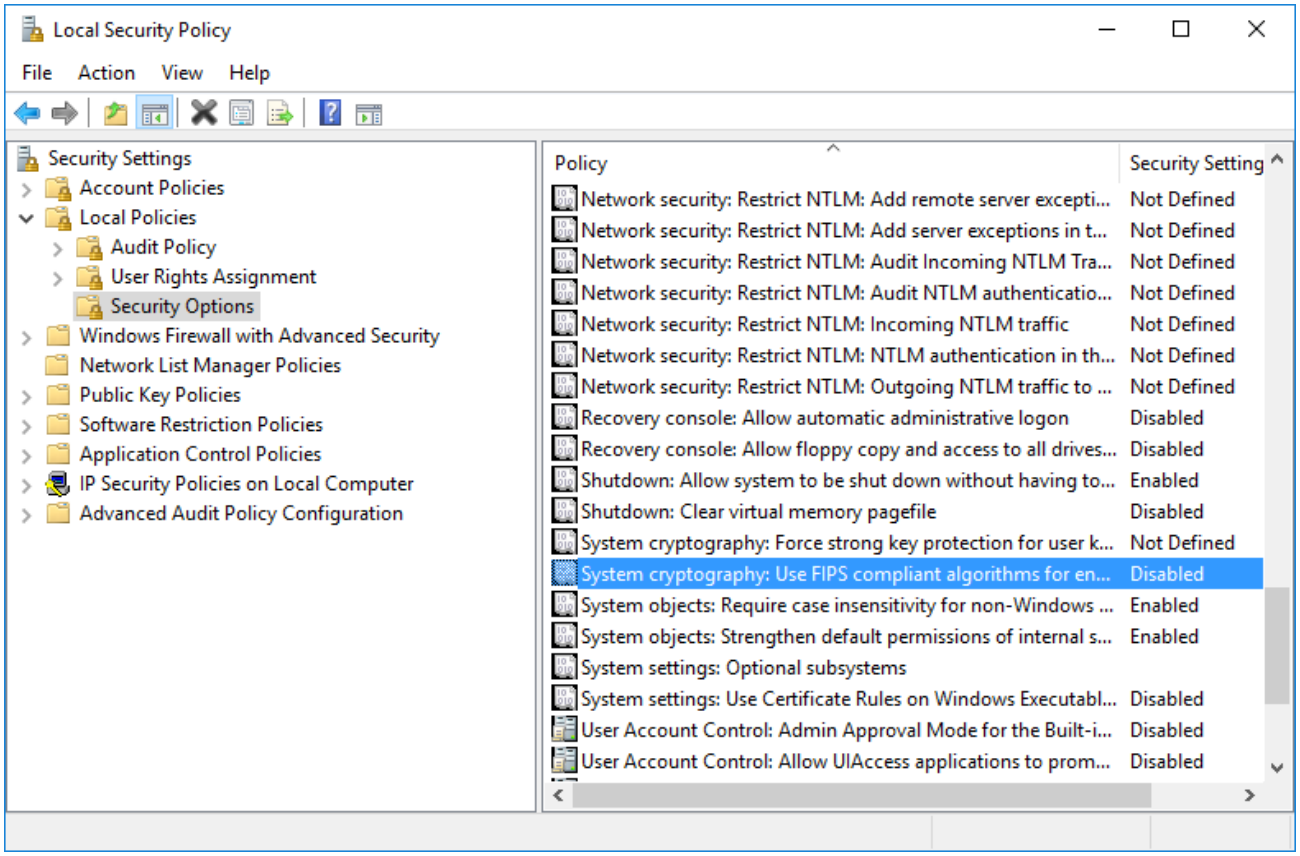

Рисунок 30. Параметры локальной политики безопасности

3. В дереве **Security Settings** раскройте узел **Local Policies** и выберите **Security Options**.
4. В столбце **Policy** дважды щелкните **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.
5. В открывшемся окне на вкладке **Local Security Settings** выберите **Disabled** и нажмите кнопку **OK**.

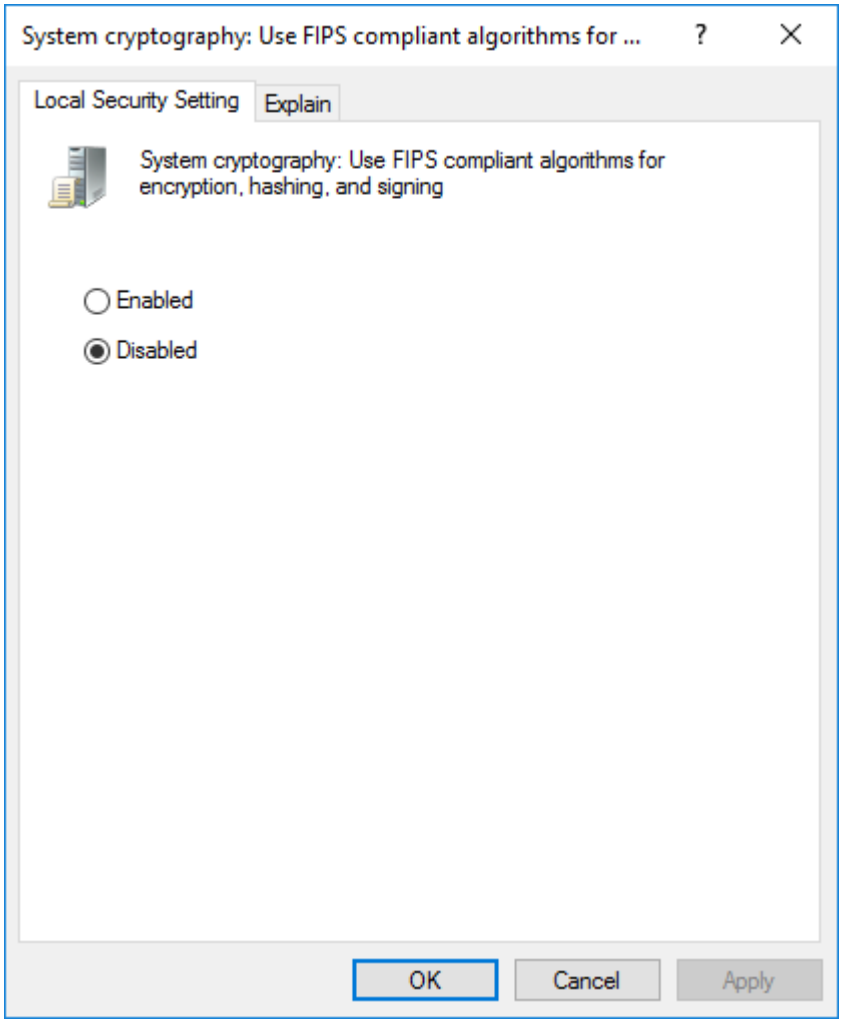

Рисунок 31. Отключение алгоритмов FIPS

FIPS Compliant Policy отключена.

Примечание. Вы можете отключить FIPS Compliant Policy в системном реестре, установив значение **0** для ключа HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\Enabled.

6.3.3. Установка "Личного кабинета оператора" в закрытом контуре

► Чтобы установить "Личный кабинет оператора" в закрытом контуре:

1. Откройте папку `PTIPCDeployment.<Номер версии>` и запустите файл `PTIPCSetup_<Номер версии>`.

   Откроется окно мастера установки.

2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.

Откроется окно с выбором компонентов для установки.

3. Снимите все флажки, чтобы установить только "Личный кабинет оператора" и необходимые зависимости (Python, Microsoft .Net и пр.) и нажмите кнопку **Установить**.

   Запустится процесс установки компонента.

4. Если требуется перезагрузить сервер, нажмите кнопку **Перезагрузить**.

   После перезагрузки сервера установка компонента продолжится автоматически. Мастер установки уведомит вас о завершении установки.

5. Нажмите кнопку **Закрыть**.

"Личный кабинет оператора" установлен в закрытом контуре.

Примечание. Одновременно с "Личным кабинетом оператора" на сервер устанавливаются Python 3.5.4 и Microsoft .NET, необходимые для корректной работы микросервисов.

6.3.4. Установка RabbitMQ

► Чтобы установить брокер сообщений RabbitMQ:

1. Откройте папку `PTIPCDeployment.<Номер версии>` и запустите файл `PTIPCSetup_<Номер версии>`.

   Откроется окно мастера установки.

2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.

3. Установите флажок **Я прочитал(а) и согласен(согласна) с лицензионным соглашением** и нажмите кнопку **Продолжить**.

   Откроется окно с выбором компонентов для установки.

4. Установите флажок **Установить RabbitMQ Server** и нажмите кнопку **Установить**.

   Запустится процесс установки компонента.

5. Если требуется перезагрузить сервер, нажмите кнопку **Перезагрузить**.

   После перезагрузки сервера установка компонента продолжится автоматически. Мастер установки уведомит вас о завершении установки.

6. Нажмите кнопку **Закрыть**.

RabbitMQ установлен.

6.3.5. Установка PostgreSQL

► Чтобы установить СУБД PostgreSQL:

1. Откройте папку `PTIPCDeployment.<Номер версии>` и запустите файл `PTIPCSetup_<Номер версии>`.

Откроется окно мастера установки.

2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
3. Установите флажок **Я прочитал(а) и согласен(согласна) с лицензионным соглашением** и нажмите кнопку **Продолжить**.

   Откроется окно с выбором компонентов для установки.
4. Установите флажок **Установить PostgreSQL** и нажмите кнопку **Установить**.

   Запустится процесс установки компонента.
5. Если требуется перезагрузить сервер, нажмите кнопку **Перезагрузить**.

   После перезагрузки сервера установка компонента продолжится автоматически. Мастер установки уведомит вас о завершении установки.
6. Нажмите кнопку **Закрыть**.

СУБД PostgreSQL установлена.

6.3.6. Установка "Информационного портала"

► Чтобы установить "Информационный портал":

1. Запустите файл `InfoPortalDeployment.exe`.

   Откроется окно мастера установки.
2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
3. Установите флажок **Я прочитал(а) и согласен(согласна) с лицензионным соглашением** и нажмите кнопку **Продолжить**.

   Запустится процесс установки портала.

   Если для установки потребуется перезагрузка сервера, мастер установки уведомит об этом.

   После перезагрузки сервера установка портала продолжится автоматически. Мастер установки уведомит вас о завершении установки.

"Информационный портал" установлен и доступен по адресу http://<IP-адрес или FQDN сервера>.

Примечание. Одновременно с "Информационным порталом" на сервер устанавливается Microsoft SQL Server, необходимый для создания базы данных хранения информации "Информационного портала".

6.3.7. Интеграция компонентов в закрытом контуре

Сразу после развертывания необходимо интегрировать независимые инсталляции компонентов в рамках контура, настроить интерфейсы и уточнить конфигурации.

► Чтобы интегрировать компоненты в закрытом контуре:

1. Интегрируйте сервер "Личного кабинета оператора" с сервисом единого входа PT MC:
```
ptipc set -p HostAddress <PTIPCServerId/FQDN> IAMHostAddress <IAM Server IP/FQDN>
IAMApplicationId <Application Id(string)>
```
2. Настройте интеграцию "Личного кабинета оператора" с СУБД PostgreSQL:
```
ptipc set –p PostgresHost '<PostgreSQL_IP-address>' PostgresPort '5432' PostgresLogin
'pt_system' PostgresPassword 'P@ssw0rdP@ssw0rd'
```
   Примечание. Настроить перечисленную выше конфигурацию также можно непосредственно в файле `InstallationParameters.xml`. Получить параметры можно по команде `ptipc get -f InstallationParameters.xml`, а применить изменения – по команде `ptipc set -f InstallationParameters.xml`.
3. Скорректируйте параметры PostgreSQL в конфигурационном файле `postgresql.conf`:
```
max_prepared_transactions = 600
max_connections = 300
shared_buffers = 6GB
```
4. Перезапустите сервис PostgreSQL:
```
service postgresql restart
```
5. Настройте режим Master для "Информационного портала":
```
infoportal set -p Mode Master
```
6. Настройте параметры сбора данных по событиям PT Incident Processing Center для PT MaxPatrol SIEM:
```
ptipc set -p SiemLoggingDik '<Путь к лог-файлам>' SiemStorageInterval '<Количество дней
хранения файлов журналов>'
```

Взаимодействие компонентов системы настроено.

6.3.8. Настройка почты в закрытом контуре

Команды, приведенные в этом разделе, нужно выполнять в интерфейсе командной строки Windows PowerShell от имени администратора.

► Чтобы настроить почту в закрытом контуре:

1. Скопируйте текущую конфигурацию:
```
ptipc get -f c:\tmp\ptipc_conf.xml
```
2. Откройте файл `c:\tmp\ptipc_conf.xml`.
3. Добавьте или измените следующий параметр исходящей почты:
```
param id="SMTPConfiguration" value='smtp+tls://<Логин почты>@<Адрес почтового
сервера>:<Порт почтового сервера>/<Адрес исходящей почты 1>?
password=<Пароль>&id=<reply_id>&useSigning=1&'smtp+tls://<Логин почты>@<Адрес почтового
сервера>:<Порт почтового сервера>/<Адрес исходящей почты N>?
password=<Пароль>&id=<reply_id>&useSigning=1'
```

4. Добавьте или измените следующий параметр входящей почты:
```
param id="MailboxesConfiguration" value='mapi+ssl://<логин почты>@<адрес почтового сервера>:<порт почтового сервера>/<адрес входящей почты 1>:<папка, из которой читаются письма>?remove_on_read=<no/trash/permanently>& password=<пароль>&reply_id=<ID SMTPConfiguration>read=0&'mapi+ssl://<логин почты>@<адрес почтового сервера>:<порт почтового сервера>/<адрес входящей почты N>:<папка, из которой читаются письма>?remove_on_read=<no/trash/permanently>&password=<пароль>&reply_id=<ID SMTPConfiguration>read=0'
```
5. Для параметра входящей почты `remove_on_read` задайте одно из значений:
   - `no` — письмо после прочтения не будет удалено;
   - `trash` — письмо после прочтения будет перенесено в корзину;
   - `permanently` — письмо после прочтения будет удалено.
6. Сохраните файл.
7. Включите функцию электронной подписи:
```
ptipc set -p EmailSigningEnabled 'true'
```
8. Настройте электронную подпись для внутренней и внешней исходящей почты:
```
ptipc set -p SMTPConfiguration 'smtp+tls://<Логин исходящей почты>@<Адрес почтового сервера>:<Порт>/<Электронный адрес исходящей почты>?password=<Пароль>&id=external>&useSigning=1
smtp+tls://<Логин исходящей почты>@<Адрес почтового сервера>:<Порт>/<Электронный адрес исходящей почты>?password=<Пароль>&id=internal&useSigning=0'
```
9. Настройте параметры электронной подписи:
```
ptipc set -p EmailSigningCertContainerPath'<Путь к файлу-сертификата>' EmailSigningCertContainerPassword '<Пароль к сертификату>' EmailCertValidation '1'
```

Почта в закрытом контуре настроена.

6.4. Интеграция контуров PT Incident Processing Center

Команды, приведенные в этом разделе, нужно выполнять в интерфейсе командной строки Windows PowerShell от имени администратора.

Сразу после развертывания необходимо интегрировать инсталляции компонентов трех контуров в единую систему PT Incident Processing Center, настроить интерфейсы и уточнить конфигурации.

Межконтурное взаимодействие отражено на схеме ниже зелеными линиями.

В этом разделе

6.4.1. Интеграция контура участника и открытого контура

Интеграция контуров выполняется на уровне Active Directory и RabbitMQ.

► Чтобы интегрировать контур участника и открытый контур PT Incident Processing Center:

1. Настройте интеграцию "Личного кабинета оператора" со службой Active Directory:

```
C:\Users\Administrator> ptipc set -p ActiveDirectoryHost '<PTIPCServer_FQDN>'
ActiveDirectoryPort '389' ActiveDirectorySslPort '636' ActiveDirectoryTransportSecurity
'ssl' ActiveDirectoryUserDn 'CN=root,CN=users,DC=ad1,DC=ru' ActiveDirectoryPassword
'P@ssw0rd' ActiveDirectoryBaseDn 'DC=ad1,DC=ru'
```

2. Настройте синхронизацию данных "Личного кабинета оператора" с "Личным кабинетом участника". Для этого настройте взаимосвязь с RabbitMQ сервера "Личного кабинета участника":

```
C:\Users\Administrator> ptipc set -p SyncExternalRabbitMQHost
'<Participant_IP_Address_and_Port>' SyncExternalRabbitMQUsername 'pt_system'
SyncExternalRabbitMQPassword 'P@ssw0rdP@ssw0rd'
```

Примечание. Настроить перечисленную выше конфигурацию также можно непосредственно в файле `InstallationParameters.xml`. Получить параметры можно по команде `ptipc get -f InstallationParameters.xml`, а применить изменения – по команде `ptipc set -f InstallationParameters.xml`.

Взаимодействие компонентов системы настроено.

6.4.2. Интеграция открытого и закрытого контуров

Интеграция выполняется на уровне "Личных кабинетов операторов".

► Чтобы настроить синхронизацию данных "Личного кабинета оператора" закрытого контура с "Личным кабинетом оператора" открытого контура,

настройте взаимосвязь "Личного кабинета оператора" закрытого контура с RabbitMQ "Личного кабинета оператора" открытого контура:

```
C:\Users\Administrator> ptipc set -p SyncExternalRabbitMQHost
'<PTIPC_IP_Address_and_Port>' SyncExternalRabbitMQUsername 'pt_system'
SyncExternalRabbitMQPassword 'P@ssw0rdP@ssw0rd'
```

6.4.3. Интеграция закрытого контура и контура участника

Интеграция выполняется на уровне "Информационных порталов".

► Чтобы настроить синхронизацию "Информационного портала" закрытого контура и контура участника:

1. На сервере "Личного кабинета оператора" в закрытом контуре создайте папку (например, `InfoportalSyncDir`) для синхронизации "Информационного портала" внутри хранилища, обозначенного параметром `AttachmentsStorageDir`..

В эту папку "Информационный портал" будет выгружать данные для синхронизации.

2. Сделайте эту папку папкой общего доступа для всех пользователей сети.
3. Укажите созданную папку в качестве сервиса вложений:
   ```
   ptipc set -p StorageSyncDirs InfoportalSyncDir
   ```
4. Активируйте сервис вложений:
   ```
   ptipc set -p StorageSyncEnabled on
   ```
5. На сервере "Информационного портала" в контуре участника создайте папку для синхронизации `D:\ProgramData\Positive Technologies\Info Portal\Sync\`.
6. Предоставьте пользователю Network Service полные права на созданную папку, а также на все папки, которые указаны в конфигурационном файле "Информационного портала" в контуре участника.
7. Задайте путь к созданной папке `Sync` в качестве значения параметра `SyncDir`:
   ```
   infoportal set -p SyncDir 'D:\ProgramData\Positive Technologies\Info Portal\Sync'
   ```
8. Настройте синхронизацию между общей папкой "Информационного портала" закрытого контура и папкой синхронизации контура участника:
   ```
   cd C:\Program Files\Positive Technologies\Info Portal\Utils\PTSP_fileMover
   .\ScheduledTaskInvoker.ps1 -source '\\<path_to\InfoportalSyncDir>' -destination '<path_to
   \Sync>'
   ```
9. Откройте планировщик задач TaskScheduler.
10. В контекстном меню задачи **FolderMonitoring** выберите пункт **Properties**.

    Откроется окно **Properties (Local Computer)**.

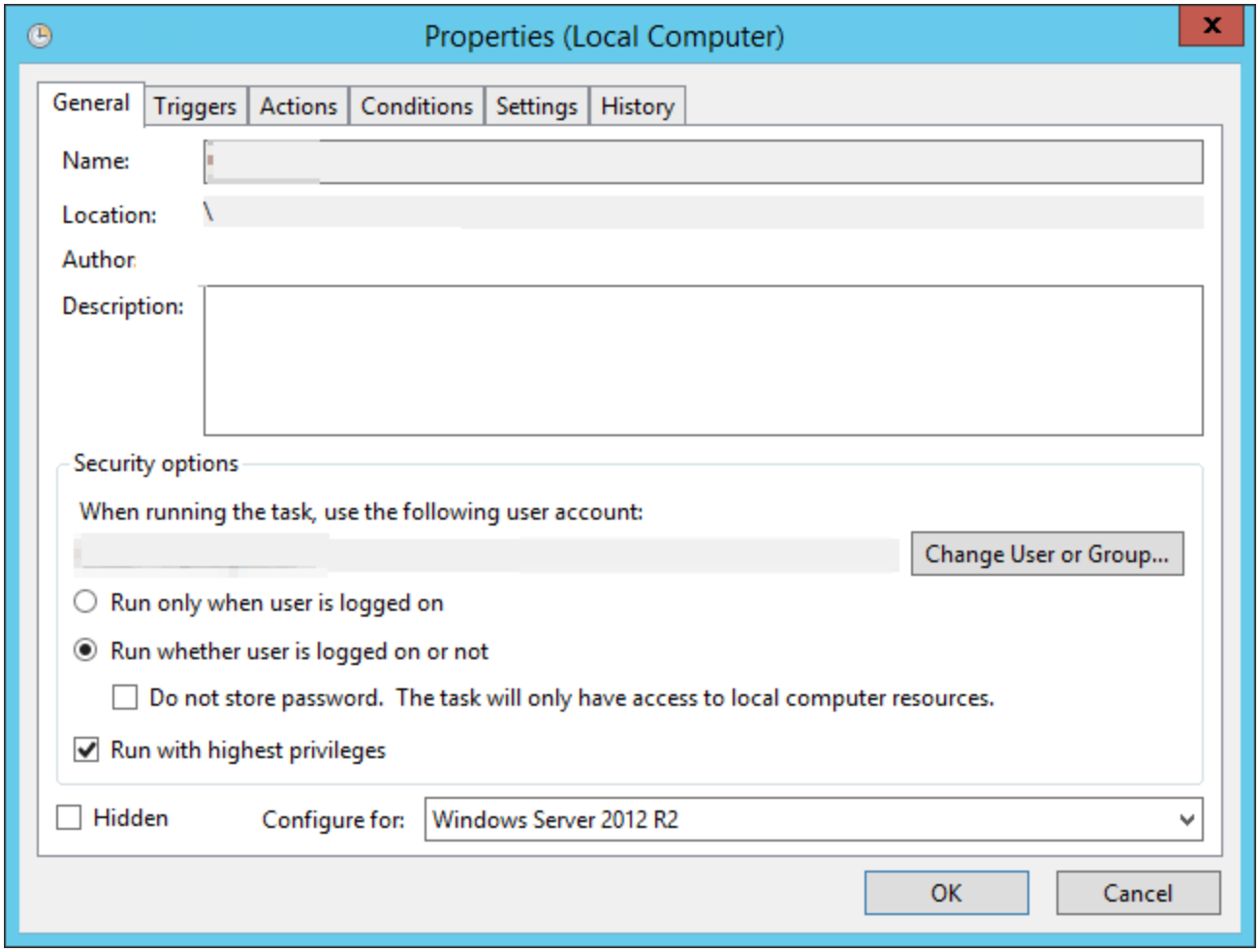

Рисунок 32. Свойства задачи планировщика задач

11. Выберите вариант **Run whether user is logged on or not**.
12. Установите флажок **Run with highest privileges**.
13. Нажмите кнопку **OK**.

Интеграция закрытого контура и контура участника завершена.

6.5. Проверка корректности развертывания и интеграции контуров

► Чтобы проверить корректность развертывания "Личного кабинета оператора" в закрытом контуре или в открытом контуре:

1. В адресной строке браузера введите ссылку для входа в интерфейс, содержащую FQDN сервера, на котором развернут "Личный кабинет оператора".

   Откроется окно авторизации PT MC.

2. В качестве логина укажите **Administrator**, а в качестве пароля — **P@ssw0rd**.

Эти учетные данные предусмотрены для первого входа и должны быть переопределены при последующем использовании.

Если в результате откроется стартовая страница "Личного кабинета оператора", установка и первоначальная настройка выполнены корректно.

► Чтобы проверить корректность развертывания "Личного кабинета участника":

1. В адресной строке браузера введите ссылку для входа в интерфейс, содержащую FQDN сервера, на котором развернут "Личный кабинет участника".

   Откроется окно авторизации PT MC.

2. В качестве логина укажите **ivanovTU1**, а в качестве пароля — **P@ssw0rd**.

   Эти учетные данные предусмотрены для первого входа и должны быть переопределены при последующем использовании.

Если в результате откроется стартовая страница "Личного кабинета участника", установка и первоначальная настройка выполнены корректно.

► Чтобы проверить корректность интеграции контура участника с открытым контуром:

1. Перейдите в "Личный кабинет участника".
2. Создайте тестовый запрос в "Личном кабинете участника" и отправьте его в PT Incident Processing Center.
3. Перейдите в "Личный кабинет оператора" в открытом контуре.
4. Убедитесь, что на странице **Запросы** присутствует тестовый запрос, отправленный из "Личного кабинета участника".

Интеграция выполнена корректно, если ни на одном шаге инструкции не обнаружено ошибок.

► Чтобы проверить синхронизацию контента между "Информационными порталами" закрытого контура и контура участника:

1. Войдите в "Информационный портал" закрытого периметра с правами учетной записи администратора.
2. Создайте тестовую новость и опубликуйте ее.

   Публикация новости занимает некоторое время. Пожалуйста, подождите.

3. Перейдите на "Информационный портал" в контуре участника.
4. Откройте страницу с новостями и убедитесь, что тестовая новость доступна для прочтения.

7. Вход в PT Incident Processing Center

Сервис управления пользователями и доступом PT MC обеспечивает механизм единого входа (технология single sign-on) в приложения "Позитив Текнолоджиз".

Перед входом в PT Incident Processing Center запросите у администратора PT MC :

— ссылку для входа в интерфейс продукта;

— тип учетной записи (локальная или доменная);

— логин и пароль вашей учетной записи пользователя.

Примечание. Убедитесь, что в браузере разрешены всплывающие окна, а также отключена функция Compatibility view для браузеров Microsoft Edge и Microsoft Internet Explorer.

► Чтобы войти в PT Incident Processing Center:

1. В адресной строке браузера введите ссылку для входа в интерфейс PT Incident Processing Center.

   Откроется страница входа в сервис PT MC.

2. Выполните одно из следующих действий:

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

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

   Примечание. Стандартная сессия пользователя в PT Incident Processing Center длится 12 часов. Вы можете продлить сессию, установив флажок **Запомнить меня**: тогда она завершится только через 7 дней бездействия.

4. Нажмите кнопку **Войти**.

8. Администрирование PT Incident Processing Center

В этом разделе приведена информация о разграничении прав доступа пользователей "Личного кабинета участника" и "Личного кабинета оператора".

В этом разделе

8.1. Настройка аутентификации пользователей через LDAP

В дополнение к локальной аутентификации пользователей вы можете настроить аутентификацию пользователей через LDAP. Для этого вам необходимо создать пул серверов LDAP и проверить соединение с пулом.

В этом разделе

8.1.1. Создание пула серверов LDAP

Для обеспечения защищенного соединения с серверами LDAP необходимо установить доверенный сертификат корневого центра сертификации на сервер в хранилище Local Computer\Trusted Root Certification Authorities.

► Чтобы создать пул серверов LDAP:

1. В главном меню нажмите ☰ и в раскрывшемся меню выберите пункт **Management and Configuration**.
2. В главном меню в разделе **Пользователи** выберите пункт **Настройка LDAP**.

   Откроется страница **Настройка LDAP**.
3. В панели инструментов нажмите кнопку **Создать пул серверов**.

4. В поле **Домены** введите DNS-имя домена, NetBIOS-имя домена или UPN-суффикс.
5. В поле **База пользователей** введите уникальное имя (DN) записи каталога, начиная с которой выполняется поиск учетных записей пользователей.
6. В блоке параметров **Серверы** в поле **Адрес** введите IP-адрес или FQDN сервера LDAP.

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

   Примечание. Вы можете добавлять в пул несколько серверов. При потере соединения с одним сервером запрос аутентификации может быть обработан другим сервером. После заполнения полей вы можете проверить соединение с пулом серверов LDAP (см. раздел 8.1.2).
9. Нажмите кнопку **Сохранить**.

Пул серверов LDAP создан.

8.1.2. Проверка соединения с пулом серверов LDAP

► Чтобы проверить соединение:

1. Нажмите кнопку **Проверить соединение**.

   Откроется окно **Проверка соединение**.
2. Введите логин и пароль пользователя с правами доступа на чтение базы пользователей, хранящихся в службе каталогов.
3. Нажмите кнопку **Проверить**.

   В окне **Проверка соединения** отобразятся результаты проверки.

8.1.3. Изменение параметров пула серверов LDAP

► Чтобы изменить параметры пула серверов LDAP:

1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Management and Configuration**.
2. В главном меню в разделе **Пользователи** выберите пункт **Настройка LDAP**.

   Откроется страница **Настройка LDAP**.
3. Выберите пул серверов LDAP.
4. В панели инструментов нажмите кнопку **Редактировать**.

5. Внесите необходимые изменения.

   Примечание. После внесения изменений вы можете проверить соединение с пулом серверов LDAP (см. раздел 8.1.2).

6. Нажмите кнопку **Сохранить**.

Параметры пула серверов LDAP изменены.

8.1.4. Удаление пула серверов LDAP

► Чтобы удалить пул серверов LDAP:

1. В главном меню нажмите ☰ и в раскрывшемся меню выберите пункт **Management and Configuration**.
2. В главном меню в разделе **Пользователи** выберите пункт **Настройка LDAP**.

   Откроется страница **Настройка LDAP**.

3. Выберите пул серверов LDAP.
4. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Пул серверов LDAP удален.

8.2. Разграничение прав доступа пользователей "Личного кабинета оператора"

В "Личном кабинете оператора" используется ролевая модель управления доступом пользователей. Роль — это набор привилегий, определяющих права доступа к функциям системы.

После развертывания "Личного кабинета оператора" необходимо:

1. Зарегистрировать учетные записи пользователей в PT MC.
2. Создать роли пользователей в "Личном кабинете оператора" и назначить им права.
3. Назначить пользователям роли.

В этом разделе

8.2.1. Права пользователей "Личного кабинета оператора"

В "Личном кабинете оператора" в качестве исходной ролевой модели существуют две системные роли:

- администратор — пользователь системы с доступом к настройке прав пользователей и справочников;
- дежурный оператор — пользователь системы с доступом ко всем операциям системы за исключением изменения закрытых инцидентов и настройки прав пользователей.

Вы не можете удалять или изменять системные роли.

Дежурный оператор может изменять закрытые задачи.

Ни одна из системных ролей не наделена привилегией изменять закрытые инциденты. Для предоставления пользователю права изменять закрытые инциденты необходимо создать роль (см. раздел 8.2.3) с соответствующей привилегией.

Таблица 12. Набор прав пользователей "Личного кабинета оператора"

Функциональная область	Права дежурного оператора	Права администратора
Инциденты		
Просмотр	+	–
Изменение	+	–
Создание	+	–
Изменение закрытых	–	–
Пользователи		
Просмотр	+	+
Изменение	–	+
Группы		
Управление группами	–	+
Добавление пользователя в группу	–	+
Роли и права доступа		
Просмотр	–	+
Управление ролями в группе	–	+
Управление общими ролями	–	+
Бюллетени		
Просмотр	+	–

Функциональная область	Права дежурного оператора	Права администратора
Создание	+	–
Изменение	+	–
Удаление черновика	+	–
Публикация	+	–
Задачи		
Просмотр	+	–
Создание	+	–
Изменение	+	–
Изменение закрытых	+	–
Угрозы		
Просмотр	+	–
Создание	+	–
Изменение	+	–
Запросы		
Просмотр	+	–
Создание	+	–
Изменение	+	–
Участники		
Просмотр	+	–
Изменение	+	–
Создание	+	–
Активация	+	–
Деактивация	+	–
Статистика		
Просмотр	+	–
Информационные карточки		
Просмотр	+	–
Изменение	+	–
Создание	+	–
Антифрод		
Просмотр	+	–
Изменение	+	–

Функциональная область	Права дежурного оператора	Права администратора
Уязвимости		
Просмотр	+	–
Изменение	+	–
Создание	+	–
Справочники		
Просмотр	+	+
Изменение	–	+
Удаление	–	+
Загрузка справочников		
Просмотр	Недоступно	Доступно
Редактирование	Недоступно	Доступно

8.2.2. Управление пользователями и доступом

Сервис управления пользователями и доступом PT Management and Configuration (далее также — PT MC) обеспечивает механизм единого входа в продуктах "Позитив Текнолоджиз".

Сервис предназначен:

— для создания и настройки учетных записей пользователей;

— назначения ролей, в соответствии с которыми в PT MC определен состав прав доступа к операциям по работе с сервисом;

— назначения ролей, в соответствии с которыми в PT Incident Processing Center определен состав прав доступа к операциям по работе с системой;

— блокировки и активации учетной записи пользователя.

В PT MC управление пользователями и доступом предусмотрено только для администратора PT MC. По умолчанию при первом входе в PT MC необходимо в поле **Логин** ввести `Administrator`, в поле **Пароль** ввести `P@ssw0rd`. После входа в PT MC пароль администратора рекомендуется изменить.

> **Примечание.** При изменении пароля администратора PT MC вам необходимо прописать новый пароль в конфигурационных файлах системы.

Администратор PT MC может назначать учетным записям пользователей следующие роли:

— администратора и пользователя — для работы с PT MC;

— администратора и оператора — для работы с PT Incident Processing Center.

Каждая учетная запись может иметь любое количество ролей. Если ролей несколько, то права суммируются.

Примечание. Учетная запись может не иметь ролей. Если учетная запись не имеет ролей в продукте, то от ее имени невозможно войти в этот продукт.

Для работы с PT MC существуют две роли — администратор и пользователь. Администратору PT MC предоставляются права доступа ко всем операциям в PT MC, включая создание и настройку учетных записей пользователей, назначение ролей, активацию и блокировку учетных записей пользователей. Пользователю PT MC предоставляются права доступа в личный кабинет для смены пароля, изменения данных профиля пользователя и организационной информации. Также пользователь PT MC может просматривать список ролей и прав в PT MC.

Для работы с PT Incident Processing Center существуют две роли — администратор и оператор. Администратору PT Incident Processing Center предоставляются права доступа ко всем операциям в системе. Оператору PT Incident Processing Center предоставляются права доступа для работы с системой в зависимости от его производственных задач.

Примечание. Роль администратора PT MC и роль администратора PT Incident Processing Center представляют собой разные роли. Если для учетной записи пользователя назначена роль администратора PT MC, то это не означает автоматическое назначение роли администратора PT Incident Processing Center.

Для учетной записи пользователя администратор и пользователь PT MC могут заполнять профиль пользователя. Эти сведения передаются в PT Incident Processing Center. Например, на указанный адрес электронной почты PT Incident Processing Center может автоматически отправлять уведомления и отчеты по расписанию.

Учетную запись пользователя администратор PT MC может заблокировать или активировать. Удалить учетную запись невозможно.

В этом разделе

8.2.2.1. Создание учетной записи пользователя в PT MC

► Чтобы создать учетную запись пользователя:

1. В главном меню нажмите ☰ и в раскрывшемся меню выберите PT MC.

   Откроется страница **Пользователи**.

2. В панели инструментов нажмите кнопку **Добавить пользователя**.

   Откроется страница **Новый пользователь**.

   Примечание. Вы не сможете изменить логин.

3. В поле **Пароль** введите пароль учетной записи или сгенерируйте его.
4. Нажмите кнопку **Создать**.

Учетная запись пользователя создана.

8.2.2.2. Изменение пароля учетной записи Administrator

При каждом изменении пароля учетной записи Administrator новый пароль необходимо указывать в конфигурационных файлах PT Incident Processing Center для корректной работы системы.

► Чтобы изменить пароль учетной записи Administrator:

1. В главном меню нажмите ☰ и в раскрывшемся меню выберите пункт **Management and Configuration**.

   Откроется страница **Пользователи**.
2. В списке выберите пользователя Administrator.
3. В панели инструментов нажмите кнопку **Редактировать информацию**.

   Откроется страница **Редактировать информацию о пользователе**.
4. Измените пароль пользователя.
5. Нажмите кнопку **Сохранить**.
6. На сервере, где установлена PT Incident Processing Center, откройте конфигурационный файл `C:\Program Files\Positive Technologies\MaxPatrol X Customer Portal\RequestManagementService.Host.exe.config`.
7. Укажите новый пароль:
   ```
   <add key="mpx:login" value="Administrator" />
   <add key="mpx:password" value="<Новый пароль>" />
   ```
8. Откройте конфигурационный файл `C:\Program Files\Positive Technologies\CSC\Web.config`.
9. Укажите новый пароль:
   ```
   <add key="mpx:login" value="Administrator" />
   <add key="mpx:password" value="<Новый пароль>" />
   ```

Пароль учетной записи Administrator изменен.

8.2.2.3. Назначение прав учетным записям

► Чтобы назначить права учетной записи:

1. В главном меню нажмите ☰ и в раскрывшемся меню выберите PT MC.

   Откроется страница **Пользователи**.
2. Выберите пользователя в списке.

3. В панели инструментов нажмите кнопку **Роли в приложениях**.

   Откроется окно **Роли пользователя <Логин пользователя>**.
4. Выберите продукт и в раскрывшемся меню выберите роль.
5. Нажмите кнопку **Сохранить**.

8.2.2.4. Блокирование учетной записи пользователя в PT MC

► Чтобы заблокировать учетную запись пользователя в PT MC:

1. В главном меню нажмите и в раскрывшемся меню выберите PT MC.

   Откроется страница **Пользователи**.
2. Выберите пользователя в списке.
3. В панели инструментов нажмите кнопку **Заблокировать**.

Учетная запись пользователя заблокирована. Напротив заблокированного пользователя отображается значок .

8.2.2.5. Разблокирование учетной записи пользователя

► Чтобы разблокировать учетную запись пользователя:

1. В главном меню нажмите и в раскрывшемся меню выберите PT MC.

   Откроется страница **Пользователи**.
2. Выберите пользователя в списке.
3. В панели инструментов нажмите кнопку **Разблокировать**.

8.2.3. Добавление роли пользователей в "Личном кабинете оператора"

► Чтобы добавить роль пользователей:

1. В главном меню в разделе **Система** выберите пункт **Роли и права доступа**.

   Откроется страница **Настройка групп, ролей и прав доступа**.
2. В панели **Группы** выберите группу.

   В таблице ролей отобразятся все существующие в группе роли пользователей с текущим объемом прав по каждой роли.
3. В панели инструментов нажмите кнопку **Добавить роль**.

   Откроется окно **Добавить роль**.

4. В поле **Наименование** введите название роли.
5. Нажмите кнопку **Добавить**.
6. Установите флажки напротив необходимых прав в столбце с наименованием роли.
7. Нажмите кнопку **Сохранить изменения** в панели инструментов.

Роль пользователей добавлена.

8.2.4. Предоставление прав пользователю

► Чтобы предоставить права пользователю системы:

1. В главном меню в разделе **Система** выберите пункт **Управление пользователями**.

   Откроется страница **Пользователи**.
2. В панели **Группы** выберите **Все пользователи**.
3. В списке пользователей выберите пользователя, права которому вы хотите предоставить.

   В панели информации о пользователе отобразится текущая принадлежность пользователя к группам и роли в этих группах.
4. В панели инструментов нажмите кнопку **Редактировать пользователя**.

   Откроется страница **Редактирование пользователя (<логин пользователя>)**.
5. В раскрывающемся списке воспользуйтесь поиском и выберите группу, доступ к которой вы хотите предоставить пользователю.
6. В раскрывающемся списке для выбранной группы выберите роли для пользователя.

   Примечание. Вы можете назначать пользователю роль дежурного оператора или другие несистемные роли. Роль администратора присваивается пользователю автоматически при назначении прав администратора в PT MC после первого входа пользователя.
7. Повторите шаги 5 и 6 для всех групп, доступ к которым вы хотите предоставить пользователю.
8. Нажмите кнопку **Сохранить**.

Права предоставлены.

8.3. Разграничение прав доступа ответственных лиц "Личного кабинета участника"

В "Личном кабинете участника" используется ролевая модель управления доступом ответственных лиц. Роль — это набор привилегий, определяющих права доступа к функциям системы.

По умолчанию в "Личном кабинете участника" существуют роли администратора и пользователя. Вы не можете удалять или изменять эти роли.

В этом разделе

Права пользователя и администратора "Личного кабинета участника" (см. раздел 8.3.1)

Предоставление пользователю участника полного набора прав доступа (см. раздел 8.3.2)

8.3.1. Права пользователя и администратора "Личного кабинета участника"

Администратор "Личного кабинета участника" обладает полным набором прав во всех функциональных областях продукта. Набор прав пользователя ограничен.

Таблица 13. Набор прав пользователя и администратора "Личного кабинета участника"

Функциональная область	Права пользователя	Права администратора
Раздел Ваша организация		
Просмотр информации об организации	+	+
Просмотр информации об используемом ПО	+	+
Просмотр списка пользователей	–	+
Сообщение об изменениях	–	+
Настройка уведомлений для пользователя	–	+
Раздел Бюллетени		
Просмотр бюллетеней	+	+
Скачивание бюллетеней	+	+
Раздел Запросы		
Запросы на расследование инцидентов. Просмотр и переписка	+	+
Запросы на изменение в карточке участника. Просмотр и переписка	–	+
Запросы на обработку угроз. Просмотр и переписка	+	+

Функциональная область	Права пользователя	Права администратора
Запросы на устранение уязвимостей. Просмотр и переписка	+	+
Запросы на добавление публикаций о мероприятиях. Просмотр и переписка	+	+
Другие запросы. Просмотр и переписка	+	+
Регистрация запросов		
Новый инцидент	+	+
Изменение в карточке участника	–	+
Угроза	+	+
Уязвимость	+	+
Публикация	+	+
Другое	+	+

8.3.2. Предоставление пользователю участника полного набора прав доступа

По умолчанию новые пользователи участника имеют ограниченный набор прав доступа к функциям продукта.

► Чтобы предоставить пользователю участника полный набор прав доступа:

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

   Откроется страница, которая содержит список всех зарегистрированных в PT Incident Processing Center участников.

2. По ссылке с названием участника перейдите в карточку участника.
3. В панели **Пользователи** выберите пользователя участника, которому необходимо предоставить полный набор прав доступа, и нажмите кнопку **Редактировать**.

   Откроется страница **<Имя пользователя участника>**.

4. В поле **Права доступа** выберите **Администратор**.

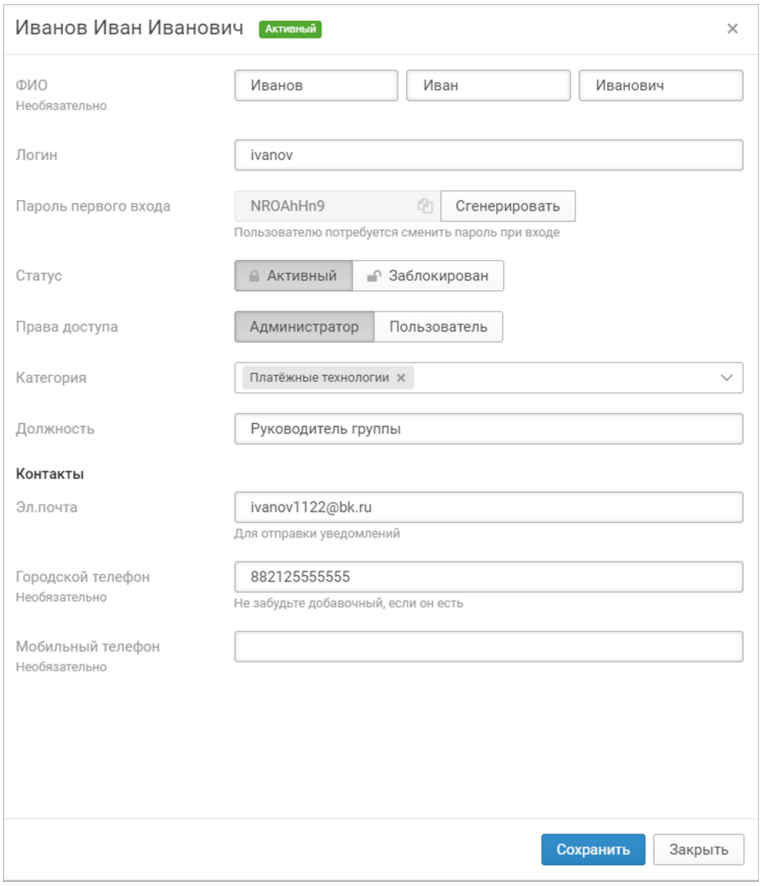

Рисунок 33. Предоставление ответственному лицу полного набора прав доступа

5. Нажмите кнопку **Сохранить**.

Ответственному лицу предоставлен полный набор прав доступа к функциям продукта.

8.4. Смена стандартного пароля архивов с вредоносным ПО

В целях безопасности PT Incident Processing Center зашифровывает архивы:

- с вредоносными URL и доменными именами (если ключ с паролем удален из конфигурационного файла);
- образцами вредоносного ПО в инцидентах с типом "Вредоносное ПО";
- файлами в запросах на анализ вредоносного ПО.

По умолчанию для шифрования используется пароль `infected`. Если политика информационной безопасности организации требует более сложных паролей для шифрования опасного или потенциально опасного контента, вы можете сменить этот пароль.

► Чтобы сменить стандартный пароль,

в интерфейсе командной строки Windows PowerShell от имени администратора выполните команду:

```
ptipc set -p MalwareArchivePassword "<Новый пароль>"
```

Например:

```
ptipc set -p MalwareArchivePassword "P@ssw0rd1033"
```

Стандартный пароль изменен.

8.5. Изменение конфигурации компонентов PT Incident Processing Center на Microsoft Windows

Вы можете изменять конфигурацию компонентов PT Incident Processing Center с помощью утилиты ptipc, которая устанавливается при установке компонентов. Путь к исполняемому файлу утилиты включается в переменную окружения PATH.

Также с помощью утилиты вы можете просматривать краткое описание параметров конфигурации и их значения.

Таблица 14. Команды утилит PT Incident Processing Center

Команда	Действие
`list`	Вывод описания параметров
`get`	Вывод значений параметров (значения выводятся в одинарных кавычках)
`set`	Ввод значений параметров (соответствующие службы перезапускаются автоматически)
`version`	Вывод версии компонента
`start`	Запуск всех сервисов
`stop`	Остановка всех сервисов
`restart`	Перезапуск всех сервисов
`help`	Вывод всех команд

Вы можете изменять значения параметров двумя способами: вручную вводя названия параметров и их новые значения или указывая путь к XML-файлу с новыми значениями. Утилиты необходимо запускать в интерфейсе командной строки Microsoft Windows от имени администратора.

8.6. Настройка шаблонов правил YARA и Snort

Оператор безопасности PT Incident Processing Center уведомляет участников информационного обмена об обнаружении опасного артефакта (URL, IP-адреса, доменного имени, файла и т. п.). При этом оператор может написать правило в формате YARA или

Snort с упоминанием этого артефакта в коде правила и разослать его участникам информационного обмена в виде бюллетеня. Участники могут использовать полученное правило для автоматической блокировки вредоносной активности. В PT Incident Processing Center существует возможность автоматической генерации подобных правил из шаблонов. После настройки шаблонов данные о том или ином артефакте будут автоматически добавляться в код правил. Операторы могут копировать правила из окна информации об артефакте.

Перед созданием шаблонов вам нужно скопировать архив `rules.zip` в папку `C:\Program Files\Positive Technologies\PTIPC\ArtifactsService\pluggable_enrichers_zip` и перезапустить микросервис PT.SP.Artifacts (см. приложение А).

► Чтобы создать шаблон для правил Snort:

1. Откройте файл `C:\Program Files\Positive Technologies\PTIPC\ArtifactsService\pluggable_enrichers\rules\rlist.cfg`.
2. Напишите правила в формате Snort.
3. В коде правил замените текст, который должен меняться в зависимости от данных артефакта, на `<OBJ>`.
4. Сохраните файл.

Шаблон для правил Snort создан.

► Чтобы создать шаблон для правил YARA:

1. Откройте файл `C:\Program Files\Positive Technologies\PTIPC\ArtifactsService\pluggable_enrichers\rules\Yaralist.cfg`.
2. Напишите правила в формате YARA.
3. В коде правил замените текст, который должен меняться в зависимости от данных артефакта, на `<OBJ>`.
4. Сохраните файл.

Шаблон для правил YARA создан.

См. также

Микросервисы PT Incident Processing Center (см. приложение А)

9. Интеграция PT Incident Processing Center с PT MaxPatrol SIEM

Вы можете просматривать статистику по объектам (инцидентам, операциям без согласия) и отслеживать динамику изменения количества объектов на дашбордах. Для создания дашбордов используется функциональность PT Incident Processing Center. Вы можете настраивать отображение нужной информации с помощью конструктора дашбордов. Кроме того, используя функциональность PT MaxPatrol SIEM, вы можете формировать аналитические отчеты с помощью конструктора отчетов или на основе уже существующего в системе отчета.

Для работы с дашбордами, виджетами и отчетами необходимо настроить PT Incident Processing Center, а затем PT MaxPatrol SIEM.

В этом разделе

9.1. Настройка PT Incident Processing Center для отправки данных в PT MaxPatrol SIEM

Для возможности просмотра дашбордов и выгрузки отчетов в PT MaxPatrol SIEM "Личный кабинет оператора" в закрытом контуре должен выступать в качестве источника событий для PT MaxPatrol SIEM. Для этого на стороне PT Incident Processing Center требуется:

- Предоставить пользователю СУБД PostgreSQL, который будет использоваться для подключения со стороны PT MaxPatrol SIEM, доступ к базам данных `eventstore` (события), `incidents` (инциденты), `references_service` (связи объектов), `participants` (участники), `requests` (запросы), `sp_antifraud` (операции без согласия), `bulletins` (бюллетени).
- В базе данных `participants` с помощью расширения dblink настроить представления (view) для сбора данных из базы `eventstore`.
- В базе данных `requests` с помощью расширения dblink настроить представления для сбора данных из баз `incidents` и `references_service`.

► Чтобы настроить PT Incident Processing Center для отправки данных в PT MaxPatrol SIEM:

1. Создайте учетную запись пользователя в PostgreSQL.

   Например:

   ```
   CREATE USER siemuser WITH PASSWORD 'test_password'
   ```

Примечание. Указанные имя пользователя и пароль потребуется указать на странице **Учетные записи** в веб-интерфейсе PT MaxPatrol SIEM.

2. Предоставьте этому пользователю права на подключение к базам и выбор данных из них:

```
GRANT CONNECT ON DATABASE eventstore incidents references_service  participants requests
sp_antifraud bulletins TO siemuser;
GRANT USAGE ON SCHEMA public TO siemuser;
GRANT SELECT ON TABLES TO siemuser;
```

3. В базе `participants` создайте расширение dblink и представление `remote_eventstore` для сбора данных из базы `eventstore`:

```
CREATE EXTENSION IF NOT EXISTS dblink;
DROP VIEW IF EXISTS remote_eventstore;
CREATE VIEW remote_eventstore AS
SELECT * FROM dblink('dbname=eventstore host=localhost user=siemuser
password=test_password', 'select  data ->> ''aggregateId'', created from public.mt_events
join public.mt_streams on
public.mt_events.stream_id = public.mt_streams.id
where mt_events.type = ''participant_created__v1'' or
mt_events.type = ''participant_created__v2'' or
mt_events.type = ''participant_created__v3'' or
mt_events.type = ''participant_created__v4'' or
mt_events.type = ''participant_created__v5'' or
mt_events.type = ''participant_created__v6'' or
mt_events.type = ''participant_created__v7'' or
mt_events.type = ''participant_created__v8''
')
AS t1(
participantId uuid, created timestamptz
);
```

4. В базе `requests` создайте расширение dblink и представление `remote_incidents` для сбора данных из базы `incidents` и представление `remote_references` для сбора данных из базы `references_service`:

```
CREATE EXTENSION IF NOT EXISTS dblink;
DROP VIEW IF EXISTS remote_incidents;
CREATE VIEW remote_incidents AS
SELECT * FROM dblink('dbname=incidents host=localhost user=siemuser
password=test_password',
'select "i"."Id",   "d"."Operating",   "d"."Relative" from public."Damages" as d join
public."Incidents" as i on "d"."IncidentId"="i"."Id"')
AS t1(incid uuid, operating text, relative integer);
DROP VIEW IF EXISTS remote_references;
CREATE VIEW remote_references AS
SELECT * FROM dblink('dbname=references_service host=localhost user=siemuser
password=test_password',
'select "target_id",  "source_id" from public."reference"')
AS t1(target_id uuid, source_id uuid);
```

PT Incident Processing Center настроен для отправки данных в PT MaxPatrol SIEM.

9.2. Настройка PT MaxPatrol SIEM для работы с дашбордами, отчетами, данными PT Incident Processing Center

Ниже представлена общая инструкция по настройке PT MaxPatrol SIEM. Подробную информацию по работе с функциональностью PT MaxPatrol SIEM (например, активами, задачами, профилями, дашбордами) см. в Руководстве оператора PT MaxPatrol SIEM.

► Чтобы настроить работу с дашбордами и отчетами в PT MaxPatrol SIEM:

1. Добавьте учетную запись **Логин-пароль**, созданную на этапе настройки (см. раздел 9.1) PT Incident Processing Center, в список учетных записей PT MaxPatrol SIEM.
2. В свойствах учетной записи выберите транспорты **PostgreSQL (ODBC)** и **Custom API**.
3. В качестве логина и пароля учетной записи укажите логин и пароль, созданные на этапе настройки PT Incident Processing Center.
4. Настройте профили сбора данных на основе существующих в системе профилей.

   Настраиваются путем импорта текста профиля в JSON.
5. Скопируйте файл `UserModel.xml` в папку `C:\ProgramData\Positive Technologies \MaxPatrol SIEM Core\Config\Layers`.

   Файл `UserModel.xml` поставляется вместе с дистрибутивом PT Incident Processing Center.
6. Перезапустите все сервисы ядра PT MaxPatrol SIEM.

   Для перезапуска вы можете использовать команду `restart-service –displayname “core*”`, запущенную в интерфейсе командной строки Windows PowerShell.
7. Импортируйте в PT KB при помощи утилиты `kb_importer` необходимые данные (формулы нормализации, правила обогащения, табличные списки, локализацию).
8. Добавьте импортированные данные в установочную группу Editable.
9. Провалидируйте все содержимое установочной группы.
10. Установите импортированные данные в PT MaxPatrol SIEM.
11. Создайте необходимые задачи.

    При создании задачи необходимо указать профиль PT Incident Processing Center, в качестве цели указать IP-адрес сервера SQL, в качестве учетной записи выбрать запись, созданную на этапе настройки PT Incident Processing Center.
12. Запустите задачи.
13. На странице **Активы** создайте статическую группу PT Incident Processing Center.
14. Создайте динамическую группу "Участники" с вышестоящей группой PT Incident Processing Center и фильтром "Participants".

Через 2—5 минут после этого этапа необходимо убедиться, что в системе есть события с типом "Инциденты", "Запросы", есть активы в группе "Участники".

15. Настройте фильтры на вкладке **События**.
16. Для каждого фильтра создайте графический виджет.

    В дальнейшем на основании виджетов вы сможете создавать отчеты и дашборды.

17. На вкладке **Отчеты** создайте необходимые отчеты.

Настройка PT MaxPatrol SIEM завершена.

9.3. Конвертация отчетов в разные форматы

Для создания отчетов о разных аспектах работы PT Incident Processing Center используется функциональность отчетов PT MaxPatrol SIEM.

Поскольку отчеты PT MaxPatrol SIEM формируются только в формате CSV, для быстрой конвертации отчетов в другие форматы нужно применять специальную утилиту CsvConverter. Утилита конвертирует отчеты в формате CSV в форматы XML, XLSX, JSON, DOCX.

CsvConverter предоставляется отдельно от системы. Утилита не требует установки и не интегрируется с системой. Можно помещать папку с файлами утилиты в любую папку компьютера, на котором хранятся отчеты в формате CSV.

► Чтобы конвертировать csv-файл отчета в другой формат с помощью утилиты CsvConverter:

1. Поместите csv-файл отчета в папку с файлами утилиты: `C:\<Путь к папке утилиты>\CsvConverter\bin\Release\netcoreapp3.0\win-x64\results`.
2. В консоли Windows запустите утилиту конвертации с ключом `all`:

   ```
   C:\<Путь к папке утилиты>\CsvConverter\bin\Release\netcoreapp3.0\win-x64>CsvConverter.exe
   results\<отчет>.csv all
   ```

   Примечание. Вы можете конвертировать отчет не во все доступные форматы сразу, а в какой-либо один формат. Для этого нужно запустить утилиту, подставив вместо ключа `all` нужный вам формат. Например, чтобы сконвертировать отчет только в формат JSON, нужно запустить утилиту с ключом `json`.

Утилита конвертирует исходный csv-файл отчета в одноименные файлы форматов XML, XLSX, JSON, DOCX. Исходный файл и файлы, полученные в результате конвертации, находятся в папке results.

10. Настройка уведомлений

Этот раздел содержит инструкции по настройке в системе уведомлений о различных событиях.

В этом разделе

10.1. Изменение шаблона почтового уведомления

В ответ на определенные события системы и действия пользователя "Личного кабинета оператора" или "Личного кабинета участника" PT Incident Processing Center отправляет уведомления на адрес электронной почты пользователя или в виде всплывающего окна в веб-интерфейсе. Шаблоны таких уведомлений настраиваются в папке `C:\Program Files\Positive Technologies\PTIPC\NotificationsService\extensions`, где каждому из типов событий соответствует своя папка с шаблонами, которая содержит следующие файлы:

- `email_content.html` — шаблон темы письма;
- `email_subject.html` — шаблон содержания письма;
- `notification.html` — шаблон уведомления в веб-интерфейсе.

► Чтобы изменить шаблон уведомления:

1. Откройте файл с шаблоном уведомления, например `C:\Program Files\Positive Technologies\PTIPC\NotificationsService\extensions\IncidentUpdated\templates\ email_content.html`.
2. Внесите изменения в текст уведомления.

   Например:

   ```
   Здравствуйте!<br/>
   Изменен инцидент {{ incident.hrid }}, созданный по запросу {{ request.hrid }}.<br/>
   {% include 'email_content_footer.html' %}
   ```

3. Сохраните файл.

10.2. Отключение отправки почтовых уведомлений на отдельные адреса

В ответ на определенные события в системе (например, добавление инцидента) на адреса электронной почты пользователей поступают уведомления. В PT Incident Processing Center существует возможность исключить один или несколько адресов электронной почты из рассылки.

Исключение адресов из рассылки может быть полезно, когда почтовый ящик получателя переполнен. Каждое автоматическое сообщение от почтового сервера о переполнении ящика будет воспринято системой как ответ на уведомление. Система в свою очередь будет отправлять новое уведомление, и такой обмен сообщениями увеличит нагрузку на систему.

Вы можете отключить отправку уведомлений, добавив адрес электронной почты в список исключений. Список исключений содержится в файле `blacklist.py`.

► Чтобы добавить адрес в список исключений:

1. Откройте файл `blacklist.py`, расположенный в папке `\Program Files\Positive Technologies\PTIPC\EmailsService\app\settings`.
2. Добавьте в список адрес, отправку уведомлений на который вы хотите отключить.

   Вы можете добавлять в список шаблоны адресов электронной почты. Шаблоны задаются с помощью регулярных выражений со стандартным синтаксисом.
3. Сохраните файл.

10.3. Настройка уведомлений о переназначении задач на операторов

Система позволяет настраивать уведомления о переназначении задачи на оператора для руководителя оператора. Переназначение — это изменение оператора, ответственного за задачу. Например, первоначально задача была назначена Оператору 1. Однако после этого она по какой-либо причине была назначена на Оператора 2. Если уведомления настроены, то руководитель Оператора 2 получит уведомление об этом на электронную почту и в Центре уведомлений. Система отправляет только уведомления о переназначении задачи. Если задача назначена на оператора впервые, руководитель оператора не получает уведомление.

Чтобы получать и просматривать уведомления, руководитель операторов должен иметь учетную запись в системе с правами оператора.

► Чтобы настроить уведомление о назначении задач на операторов:

1. На сервере с "Личным кабинетом оператора" откройте на редактирование файл `C:\Program Files\Positive Technologies\PTIPC\NotificationsService\extensions\TicketReassigned\listeners.json`.
2. В строке `listeners` → `id` укажите id в системе руководителя операторов, который должен получать уведомления о назначении задачи на операторов.
3. В строке `listeners` → `operators` укажите id в системе оператора, на которого назначаются задачи (см. ниже).

   ```
   "id": "<id руководителя операторов в системе>",
   "operators": ["<id подчиненного оператора>", "<id подчиненного оператора>"]
   ```

   Если у руководителя в подчинении несколько операторов, их id можно указать через запятую. В этом случае руководитель будет получать уведомления о назначении задач на каждого из этих операторов.
4. Если необходимо указать еще одного руководителя (например, руководителя другой группы операторов) добавьте еще одну пару строк id / operators и настройте в ней уведомления аналогично.
5. Сохраните изменения и закройте файл.

Руководители операторов, указанные в файле, будут получать уведомления о переназначении задач на операторов: по электронной почте и в Центре уведомлений.

10.4. Настройка уведомлений для пользователей в "Личном кабинете участника"

Администратор участника в интерфейсе "Личного кабинета участника" может настраивать уведомления об изменениях и подтверждения для ответственных лиц, групповых почтовых ящиков и ящиков входящей почты участника. Администратор участника настраивать параметры уведомлений по умолчанию, включать и выключать отдельные виды уведомлений, а также включать параметры уведомлений по умолчанию.

► Чтобы настроить уведомления:

1. В главном меню выберите раздел **Ваша организация**.
2. Выберите вкладку **Уведомления**.

   На вкладке содержатся почтовые ящики организации с указанием типа. Для каждого почтового ящика отображается статус уведомлений об изменениях и подтверждениях.
3. Выберите запись в списке и нажмите кнопку **Редактировать**.
4. В открывшемся окне настройте уведомления для почтового ящика:

   - **Уведомления об изменениях**: получать входящие уведомления о регистрации запросов в центре, новых сообщениях в запросах, о публикации бюллетеней.

- **Уведомления-подтверждения**: получать подтверждения из центра о запросах, принятых с этого почтового ящика.
- **Уведомления о публикации фидов**: получать уведомления о публикации фидов в центре.
- **Установить значения по умолчанию**: вернуть параметры уведомлений, настроенные при первоначальном конфигурировании системы.

5. Нажмите кнопку **Сохранить**.

Уведомления для адреса настроены.

11. Загрузка идентификационных данных из внешних источников

Примечание. В разделе приведены описания параметров для Российской Федерации.

Примечание. Сведения об операциях без согласия указывают участники, которым в рамках их деятельности необходимо фиксировать и обрабатывать такую информацию.

Для маршрутизации операций без согласия в кредитную организацию получателя в системе предусмотрена загрузка идентификационных данных (таких как БИК, БИН) из внешних источников.

Справочник "БИК и SWIFT BIC" расположен на сайте cbr.ru. Справочники "Таблицы БИН банков-эквайеров", "Таблицы БИН банков-эмитентов" предоставляются национальной системой платежных карт. Справочник "Соответствие идентификаторов участников в платежных системах и их регистрационных номеров" поставляется вместе с PT Incident Processing Center. В дальнейшем вы можете актуализировать справочник, используя информацию с сайта cbr.ru.

Работа со справочниками идентификационных данных осуществляется только через интерфейс "Личного кабинета оператора" в закрытом контуре. Справочники отображаются на странице **Система** → **Загрузка справочников**. Пользователь с правами администратора системы может загружать справочники в систему, а также скачивать их для изменения.

Примечание. Для изменения справочников необходимо использовать программу Notepad++ или другие текстовые редакторы, которые поддерживают CSV–формат.

► Чтобы загрузить справочник в систему:

1. В главном меню в разделе **Система** выберите **Загрузка справочников**.

   Откроется страница со списком справочников. На странице вы можете скачивать для изменения ранее загруженные справочники и загружать в систему обновленные версии справочника.

2. В списке выберите справочник, который вы хотите загрузить.
3. В панели инструментов нажмите кнопку **Загрузить справочник**.
4. В открывшемся окне добавьте CSV-файл справочника.

   Система провалидирует данные в файле. Если данные не прошли валидацию, система выведет сообщения об ошибке. Если данные прошли валидацию, в списке отобразится информация о новой версии справочника.

Справочник загружен.

12. Работа с белыми списками

Примечание. В разделе приведены описания параметров для Российской Федерации.

Белый список — это справочник с атрибутами получателей платежей, которые не выгружаются в файлы с фидами.

Работа с белыми списками осуществляется только через интерфейс "Личного кабинета оператора" в закрытом контуре. Белые списки отображаются на странице **Система** > **Загрузка справочников** с названиями в формате **Белый список - <тип фида>**, например, **Белый список – Телефон**.

Белые списки хранятся только в "Личном кабинете оператора" закрытого контура. Загружать в систему обновленные белые списки может пользователь с правами администратора системы.

Данные белых списков загружаются в систему в csv-файлах, в которых в качестве разделителя используется запятая (,).

Кодировка файла: UTF-8 или Windows-1251. Первая строка содержит названия столбцов и при загрузке в систему игнорируется. Порядок столбцов в файле должен соответствовать порядку столбцов в файлах с фидами.

Пример содержимого файла белого списка для типа фида Retail/ATM (файл `retail_atm.csv`):

```
Acquirer ID,Merchant name,MCC
123,merch,3453
```

В системе поддерживается набор файлов белых списков, соответствующих типам фидов.

Таблица 15. Названия CSV-файлов белого списка

Тип фида	Название CSV-файла
Хеш номера паспорта	`passport_hashes.csv`
Хеш номера СНИЛС	`snils_hashes.csv`
ИНН	`inn.csv`
Карта	`card_number.csv`
Лицевой счет	`account_number.csv`
SWIFT	`swift.csv`
Телефон	`phone_number.csv`
Электронный кошелек	`ewallet_number.csv`
Retail/ATM	`retail_atm.csv`
Иной идентификатор	`other.csv`

Данные в CSV-файлах белых списков должны соответствовать требованиям к атрибутам фидов для валидации.

Таблица 16. Требования к атрибутам фидов для валидации

Тип фида	Атрибут фида	Требования для валидации
Хеш номера паспорта	Хеш номера паспорта	Длина значения 64 символа. Допустимые символы: — цифры (1 2 3 4 5 6 7 8 9 0) — A a B b C c D d E e F f – здесь пробел используется для визуального разделения символов и не является допустимым символом
Хеш номера СНИЛС	Хеш номера СНИЛС	Длина значения 64 символа. Допустимые символы: — цифры (1 2 3 4 5 6 7 8 9 0) — A a B b C c D d E e F f - пробел используются для визуального разделения символов и не является допустимым символом
ИНН	ИНН	Длина значения 10 или 12 символов. Допустимые символы: цифры (1 2 3 4 5 6 7 8 9 0)
Карта	Номер карты	Длина значения не менее 16 и не более 18 символов Допустимые символы: цифры (1 2 3 4 5 6 7 8 9 0)
Лицевой счет	Номер счета	Длина значения 20 символов Допустимые символы: цифры (1 2 3 4 5 6 7 8 9 0) Маска: первый символ - 1, 2, 3, 4 или 5
	БИК	Длина значения 9 символов. Допустимые символы: цифры (1 2 3 4 5 6 7 8 9 0) Маска: первый символ - 0, 1 или 2
SWIFT	Номер счета SWIFT	Длина значения не более 50 символов
	SWIFT BIC	Строка с 8 или 11 символами формата 4!a2!a2!an[3!an]: — 4!a - 4 буквы латинского алфавита в верхнем регистре, — 2!a - 2 буквы латинского алфавита в верхнем регистре, — 2!an - 2 alphanumeric в верхнем регистре (буквы латинского алфавита в верхнем регистре или цифры), — [3!an] - alphanumeric в верхнем регистре (буквы латинского алфавита в верхнем регистре или цифры), могут отсутствовать Примеры:

Тип фида	Атрибут фида	Требования для валидации
		SKSBRUMMXXX SLABRU21 SGUBRU5S053 TEMBRUMMBLG
Телефон	Номер телефона	Длина значения: — если код страны 7, то 11 (включая код); — если код страны отличен от 7, то не менее 11 символов и не более 15 (включая код). Допустимые символы: цифры (1 2 3 4 5 6 7 8 9 0)
Электронный кошелек	Номер кошелька	Длина значения не более 15. Допустимые символы: — цифры (1 2 3 4 5 6 7 8 9 0) — буквы латинского алфавита в верхнем и нижнем регистре (aA - zZ) — знак +
	Название платежной системы	Требований нет, не валидируется
Retail/ATM	Acquirer ID	Длина строки не должна превышать 50 символов. Допустимые символы: — Цифры (0-9); — Буквы латинского алфавита в верхнем и нижнем регистре (aA-zZ)
	Merchant name	Длина строки не должна превышать 255 символов. Допустимые символы: — Цифры (0-9) — Буквы латинского алфавита в верхнем и нижнем регистре (aA-zZ) — Буквы кириллического алфавита в верхнем и нижем регистре (aA-яЯ) — Специальные символы - !"№;%:?*()_+=\-<>/|
	MCC	4 любые цифры
Иной идентификатор	Иной идентификатор	Не валидируется

В этом разделе

12.1. Обновление белого списка

Пользователь с правами администратора системы может обновлять белые списки, загружая в "Личном кабинете оператора" закрытого контура csv-файлы списков с обновленными атрибутами фидов.

► Чтобы обновить белый список в системе:

1. В главном меню в разделе **Система** выберите **Загрузка справочников**.

   Откроется страница со списком справочников. На странице можно скачивать для редактирования ранее загруженные справочники и загружать в систему обновленные версии справочника.

2. В списке выберите справочник **Белый список — <Название>**, обновленную версию которого вы хотите загрузить.

3. В панели инструментов нажмите кнопку **Загрузить справочник**.

4. В открывшемся окне загрузки добавьте csv-файл белого списка с обновленными данными (см. раздел 12).

   Система провалидирует данные в файле. Если данные не прошли валидацию, система отображает сообщения об ошибке. Если данные прошли валидацию, в списке отображается информация о новой версии справочника.

Белый список обновлен.

12.2. Удаление данных из белого списка

► Чтобы удалить данные из белого списка:

1. В главном меню в разделе **Система** выберите **Загрузка справочников**.

   Откроется страница со списком справочников.

2. В списке выберите справочник **Белый список — <Название>**, данные из которого вы хотите удалить.

3. Нажмите кнопку **Скачать файл**.

   Файл формата CSV с белым списком будет сохранен в папку для скачивания вашего браузера.

4. Удалите в файле все данные или оставьте только первую строку с заголовками столбцов.

5. Сохраните файл.

6. В панели инструментов нажмите кнопку **Загрузить справочник**.
7. В открывшемся окне загрузки добавьте CSV-файл белого списка с обновленными данными (см. раздел 12).

Данные белого списка удалены.

13. Автообновление списка запросов

Вы можете включить автообновление списка запросов и указать его частоту. Список запросов отображается в "Личном кабинете оператора" и "Личном кабинете участника" на странице **Запросы**. В "Личном кабинете оператора" автообновление будет выполняться, если список запросов отсортирован по дате создания (по убыванию) и включен переключатель **Обновлять автоматически**. В "Личном кабинете участника" автообновление будет выполняться сразу после включения.

Включить автообновление списка запросов и настроить частоту обновления вы можете с помощью утилиты finctl. В инструкции описана настройка автообновления списка запросов для "Личного кабинета оператора". Настройка автообновления списка в "Личном кабинете участника" производится аналогично.

► Чтобы включить автообновление:

1. На сервере с "Личным кабинетом оператора" запустите командную строку Microsoft Windows от имени администратора.
2. Перейдите в папку с утилитой finctl:
   ```
   cd C:\Program Files\Positive Technologies\PTIPC\Utils\ConfigurationTool
   ```
3. Включите автообновление:
   ```
   finctl.exe set --key isAutoRefreshEnabled --value true
   ```

Автообновление списка запросов включено.

После включения автообновления в интерфейсе "Личного кабинета оператора" на странице **Запросы** появится переключатель **Обновлять автоматически**.

По умолчанию автообновление будет запускаться каждые 60 секунд. Вы можете изменить частоту обновления списка запросов.

► Чтобы изменить частоту обновления:

1. На сервере с "Личным кабинетом оператора" запустите командную строку Microsoft Windows от имени администратора.
2. Перейдите в папку с утилитой finctl:
   ```
   cd C:\Program Files\Positive Technologies\PTIPC\Utils\ConfigurationTool
   ```
3. Укажите частоту обновления, установив параметру `value` нужное значение в миллисекундах:
   ```
   finctl.exe set --key refreshDelay --value 30000
   ```

Частота обновления изменена.

14. Изменение периода хранения записей в журнале аудита

Вы можете изменять время хранения в системе файлов, содержащих информацию о действиях пользователей в системе.

Команды необходимо выполнять в интерфейсе командной строки Microsoft Windows от имени администратора.

- Чтобы изменить время хранения файлов,

  укажите необходимое количество дней:

  ```
  ptipc set -p SiemStorageInterval <Количество дней>
  ```

  Примечание. Вы можете узнать время хранения файлов в системе, выполнив команду `ptipc get -p SiemStorageInterval`.

Приложение А. Микросервисы PT Incident Processing Center

PT Incident Processing Center имеет сервис-ориентированный тип архитектуры и состоит из связанных компонентов — микросервисов. Вы можете просматривать информацию о производительности запущенных микросервисов PT Incident Processing Center в "Диспетчере задач Windows". Перечень микросервисов PT Incident Processing Center представлен в таблице ниже.

Примечание. Сведения об операциях без согласия указывают участники, которым в рамках их деятельности необходимо фиксировать и обрабатывать такую информацию.

Таблица 17. Микросервисы PT Incident Processing Center

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
PT.SP.GatewayAPI	Прокси-сервер	.NET	7000	Все	Авторизация пользователей	Проксирование запросов из интерфейса в микросервисы. Авторизация пользователей. Получение информации о пользователе, его привилегиях (для ЛКУ). Смена пароля в Active Directory. Получение списка связей с метаинформацией о сущности. Поиск сущностей по тегам

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
PT.SP.ReportsService	Дашборды	Python	7002	^api/dashboards(.*)	Просмотр	Возвращает информацию для следующих виджетов (страница **Дашборды**). Для "ПТ ВЦ" : — количество объектов; — количество субъектов; — количество ИТС; — количество открытых инцидентов; — количество закрытых инцидентов; — топ из 10 субъектов, отсортированных по количеству инцидентов (в убывающем порядке); — количество созданных инцидентов, сгруппированных по времени (дни, недели) за

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						определенный промежуток времени (последние 30 дней, текущую неделю); — изменение статуса инцидентов за определенный промежуток времени. ДляPT Incident Processing Center: — количество объектов; — количество субъектов; — количество ИТС; — количество открытых инцидентов; — количество закрытых инцидентов; — количество созданных запросов, сгруппированных по времени (дни, недели) за определенный промежуток времени (например, последние 30 дней, текущую неделю);

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						— количество созданных инцидентов, сгруппированных по времени (дни, недели) за определенный промежуток времени (например, последние 30 дней, текущую неделю); — изменение статуса инцидентов за определенный промежуток времени. Создает отчеты следующих типов: — новые инциденты, сгруппированные по времени; — новые инциденты, сгруппированные по типу; — новые инциденты, сгруппированные по участникам;

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						— отчет об атаках на организации кредитно-финансовой сферы; — справка-отчет по инциденту
PT.SP.Incidents.DC	Инциденты ВЦ	.NET	7003	^api/incidents(.*)	Просмотр, Редактирование, Создание, Настройка расположения	Создание и изменение инцидентов. Получение списка инцидентов согласно установленному фильтру. Получение инцидента по id. Получение списка инцидентов по списку идентификаторов. Смена статуса инцидента. Получение возможных статусов для заданного инцидента. Запрос содействия ГЦ. Добавление принятых мер и рекомендаций.

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						Получение возможных фильтров для инцидентов и их значений. Получение короткого описания для инцидентов по groupId. Получение дерева СОС для инцидентов
PT.SP.Incidents.FC	Инциденты PT Incident Processing Center	.NET	7003	^api/incidents(.*)	Просмотр, Редактирование, Создание, Настройка расположения	Создание и изменение инцидентов. Получение списка инцидентов согласно установленному фильтру. Получение инцидента по id. Получение списка инцидентов по списку идентификаторов. Смена статуса инцидента. Получение возможных статусов для заданного инцидента. Запрос содействия ГЦ.

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						Добавление принятых мер и рекомендаций. Добавление комментариев, сообщений (сейчас не используется) Получение возможных фильтров для инцидентов и их значений. Получение короткого описания для инцидентов по groupId
PT.SP.Configuration	Конфигурация системы, настройки, доступные модули	.NET	7004	^api/settings(.*)	—	Получение конфигурации приложения, состоящей из имени приложения, списка модулей, списка внешних ссылок. Получение списка модулей
PT.SP.Participants	Участники PT Incident Processing Center	.NET	7005	^api/participants(.*)	Просмотр, изменение	Участники: — создание и изменение; — получение списка участников согласно установленному фильтру; — получение участника по id;

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						— добавление, изменение, удаление ПО; — активация и деактивация; — получение участника по электронной почте; — получение возможных фильтров для участников и их значений. Пользователи участников: — создание и изменение пользователей участников; — активация и деактивация; — создание временного пароля; — получение пользователей по id участника; — получение пользователя по id участника и id пользователя.

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						Общее: — создание и изменение участника вместе со списком пользователей; — получение статуса распределенных транзакций для участников
PT.SP.NotificationsService	Оповещение пользователей	Python	7006	^api/notifications(.*)	Просмотр	Получение списка связей указанной сущности (например, Участник, Пользователь, Инцидент) с другими сущностями системы с возможностью фильтрации по типу связи (например, parent, child). Создание новой связи указанных сущностей системы. Удаление указанной связи. Хранение тегов для сущностей
PT.SP.ReferencesService	Сервис связей между сущностями	Python	7007	^api/relations(.*)	Просмотр, создание, удаление	Получение списка связей указанной сущности (Участник, Пользователь, Инцидент) с

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						другими сущностями системы с возможностью фильтрации по типу связи (parent, child). Создание новой связи указанных сущностей системы. Удаление указанной связи. Хранение тегов для сущностей
PT.SP.MPX2CenterService	Прокси PT MaxPatrol SIEM -активов	Python	7008	^api/mpx16(.*)	Просмотр	Проксирование запросов к сервису PT MaxPatrol SIEM с целью получения и фильтрации списка активов (объектов, субъектов)
PT.SP.MPX2CenterService	Интеграция с PT MaxPatrol SIEM	Python	—	—	—	Синхронизация данных между "ПТ ВЦ" и PT MaxPatrol SIEM: из "ПТ ВЦ" в PT MaxPatrol SIEM синхронизируются: субъекты, объекты, ИТС; из PT MaxPatrol SIEM в "ПТ ВЦ": инциденты

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
PT.SP.ExternalIntegrationService	Интеграция с внешними системами (например, ArcSight)	Python	—	—	—	Создание инцидентов на основе файлов, сохраненных в формате ArcSight
PT.SP.IamUserSync	Синхронизация пользователей с PT MC	.NET	—	—	—	Синхронизация пользователей из PT MC
PT.SP.Bulletins	Бюллетени	.NET	7009	^api/bulletins(.*)	Просмотр, изменение, создание, удаление, публикация	Создание, изменение, удаление, публикация бюллетеней. Получение списка бюллетеней согласно установленному фильтру. Получение бюллетеня по id. Получение списка бюллетеней по списку идентификаторов. Получение возможных фильтров для бюллетеней и их значений
PT.SP.Tickets	Задачи	.NET	7010	^api/tickets(.*)	Просмотр, изменение, создание	Создание и изменение задач.

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						Получение списка задач согласно установленному фильтру. Получение задачи по id. Получение списка бюллетеней по списку идентификаторов. Получение возможных фильтров для задач и их значений. Назначение оператора на список задач. Смена статуса. Добавление итога для задачи. Получение обновления для списка задач, начиная с определенного момента времени
PT.SP.Requests	Запросы	.NET	7011	^api/requests(.*)	Просмотр, изменение, создание	Создание и изменение. Получение списка запросов согласно установленному фильтру. Получение запроса по id.

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						Получение списка запросов по списку идентификаторов. Получение возможных фильтров для запросов и их значений. Назначение оператора на список запросов. Смена статуса. Получение обновления для списка запросов, начиная с определенного момента времени. Получение возможных статусов запроса. Изменение статуса запроса. Изменение приоритета запроса. Добавление сообщения в запрос. Получение сообщения для запроса с заданным id.

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						CRUD для черновиков запросов. CRUD для черновиков сообщений
PT.SP.Fias	Адреса ФИАС	.NET	7012	^api/address(.*)	Просмотр	Получение адреса по почтовому индексу. Получение адреса по ОКТМО. Поиск адреса по строке и уровню в иерархии. Получение списка стран. Получение списка федеральных округов. Получение списка военных округов. Получение списка субъектов федерации. Поиск адреса по строке поиска, parentId и уровню. Импорт базы адресов ФИАС

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
PT.SP.InfoCardsService	Информационные карточки	Python	7013	^api/infoCards(.*)	Просмотр, изменение	Создание и изменение. Получение списка информационных карточек с возможностью фильтрации по типу. Получение информационной карточки по id. Получение списка информационных карточек по списку идентификаторов
PT.SP.AttachmentsService	Вложения	Python	7014	^api/attachments(.*)	—	Загрузка и скачивание файлов. Получение информации о файле. Отправка файла на сканирование в PT MS Получение информации о результатах сканирования в PT MS для указанного файла. Скачивание созданного в PT MS отчета сканирования указанного файла. Создание вложения.

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						Получение списка загруженных вложений по списку идентификаторов. Запуск синхронизации указанного вложения с другими контурами. Создании новой версии вложения. Получение истории версий вложения. Получение информации о вложении по идентификатору. Удаление вложения. Обновление информации о вложении. Создание файла-исходника бюллетеня на основе угрозы
PT.SP.Sync	Внутренняя синхронизация систем (например, ЛКУ и ЛКО)	.NET	7015	^api/sync(.*)	—	Синхронизация событий и команд между контурами системы

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
PT.SP.WorkflowEngineService	Сервис пользовательских сценариев	Python	7016	^api/we(.*)	—	Выполнение различных сценариев (выполнение запускается либо по запросу API (см. ниже), либо по событиям из RabbitMQ): — создание связи между сущностями системы; — создание запроса и сообщений в рамках запроса из электронной почты; — по API выполнять: • запуск указанного сценария; • получение статуса выполнения сценария
PT.SP.Dictionaries	Словари	.NET	7017	^api/dictionaries(.*)	—	Получение списка словарей по заданному типу словаря. Создание, изменение, активация, деактивация записи словаря. Список словарей:

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						форма юридического лица; отраслевая и другая принадлежность; типы объектов; виды услуг; типы обрабатываемой информации; категории объектов; страны; типы активов; типы компьютерных атак; операторы связи; категории ПО; категории пользователей; военные округа; федеральные округа; субъекты федерации; списки рассылок;

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						шаблоны рекомендаций для инцидентов; типовые сценарии реагирования
PT.SP.CommentsService	Комментарии	Python	7018	^api/comments(.*)	—	Получение всех комментариев для комментируемой сущности. Добавление комментария для указанной сущности. Получение количества непрочитанных комментариев. Выставление статуса "прочитано" для указанных комментариев
PT.SP.Threats	Угрозы	.NET	7019	^api/threats(.*)	Просмотр, изменение, добавление	Создание и изменение угроз. Получение списка угроз согласно установленному фильтру. Получение угрозы по id. Получение списка угроз по списку идентификаторов.

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						Назначение оператора на список угроз
PT.SP.GosSopka2CenterService	Интеграция с ГосСОПКА	Python	7020	^api/gossopka(.*)	—	Синхронизация следующих данных между ВЦ и ГосСОПКА: — инциденты и связанные с ними сущности (принятые меры, рекомендации, комментарии); — субъекты; — объекты; — ИТС; — ответственные лица
PT.SP.EmailsService	Работа с электронной почтой	Python	7034	—	—	Прием и отсылка почтовых сообщений
PT.SP.ArtifactsService	Артефакты	Python	7021	^api/artifacts(.*)	—	Получение списка артефактов (с результатами обогащения, если есть).

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						Получение статуса обогащения указанного артефакта (например, "в процессе", "завершено") Получение результата обогащения определенного типа (whois, nslookup) для указанного артефакта Обновление результата обогащения определенного типа (whois, nslookup) для указанного артефакта
PT.SP.LoggingNodeService	Журналирование действий пользователя	Python	7035	—	—	Журналирование событий ИБ по отношению к каким-либо сущностям системы (создание, чтение, обновление, удаление) и их статуса (success/fail)
PT.SP.AntifraudService	Антифрод	Python	7022	^api/antifraud(.*)	—	Обработка заявлений об операциях без согласия и их хранение в виде карточек. Запрос доп. информации по операции без согласия от КО получателя.

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						Получение списка антифрода карточек (с результатами обогащения и информацией от заявителя, если есть)
PT.SP.Vulnerabilities	Сервис уязвимостей	.NET	7023	^api/vulnerabilities(.*)	—	Создание, редактирование и получение угроз
PT.SP.Api	Фасад внешнего API	.NET	7024	^api/v1/(.*) (не проксируется через PT.SP.Gateway API)	—	Проксирование внешних запросов во внутренние сервисы ЛКУ и их обработка. Авторизация пользователей
PT.SP.HistoryService	Сервис истории	Python	7025	^api/history(.*)	—	Просмотр истории по объектам на основе событий из хранилища событий по сконфигурированным правилам
PT.SP.Campaigns	Сервис кампаний	.NET	7026	^api/campaigns(.*)	Просмотр, создание, изменение	Создание и изменение кампаний. Получение списка кампаний. Фильтрация списка кампаний и поиск по нему.

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
						Получение кампании по id
PT.SP.EventStore.Api	Сервис взаимодействие с Event store	.NET	7027	^api/eventstore(.*)	—	Взаимодействие с хранилищем событий для Python-сервисов: — запись и получение событий; — управление счетчиками
PT.SP.Entites	Сервис кастомизируемых доменных сущностей	.NET	7028	^api/entities(.*)	—	Доступ к работе с кастомными доменными сущностями
PT.SP.TransformationService	Сервис трансформации	Python	7029	^api/transformation(.*)	—	Преобразование данных из одного формата в другой по заданным правилам
PT.SP.Plugins.Host	Сервис хостинга плагинов	.NET	7030	^api/plugins(.*)	—	Хостинг плагинов в системе
PT.SP.Correlations	Сервис корреляций	Python	7031	^api/correlations(.*)	—	—
PT.SP.SlaService	Сервис правил SLA	Python	7036	^api/sla(.*)	—	—

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
PT.SP.AccessModel.Host	Сервис работы с access model	.NET	7037	^api/accessmodel(.*)	—	Управление ресурсами, действия, правилами, политиками, ролями пользователей
PT.SP.CustomDictionaries.Host	Сервис кастомизируемых справочников	.NET	7038	^api/dictionaries/v2(.*)	—	Доступ к работе с кастомными справочниками
PT.SP.EF	Сервис кастомизируемых электронных форм	.NET	7039	^api/efs/(.*)	Просмотр, создание, редактирование	Добавление и изменение ЭФ. Добавление и изменение схем ЭФ
PT.SP.DSS	Эмулятор криптографического сервиса	Python	7041	^api/dss(.*)	—	—
PT.SP.SubjectsObjectsSystems	Микросервис субъектов, объектов, систем (Информационный портал)	.NET	7001	Прочие	Субъекты: просмотр, изменение, деактивация, активация, создание.	—

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
					Объекты: просмотр, изменение, деактивация, активация, создание. Системы: просмотр, изменение, деактивация, активация, создание. Документы: просмотр, деактивация, активация. Справочники: просмотр, изменение, удаление. Пользователи: просмотр. Роли и права доступа: просмотр, управление ролями.	

Название микросервиса	Описание	Стек	Порт по умолчанию	Доступные API	Привилегии пользователей	Функция
					Импорт: просмотр, выполнение. XML импорт/экспорт: выполнение. Статистика об атаке: создание	

Приложение Б. Обмен сообщениями между компонентами системы

Для обмена сообщениями между компонентами системы в PT Incident Processing Center используется программная платформа RabbitMQ.

Сообщения бывают двух типов: сообщения о событиях в системе (например, добавление инцидента) и команды от одного компонента системы другому.

Сообщения отправляются о следующих событиях в системе:

- добавление или изменение запросов;
- добавление или изменение информации об инцидентах;
- добавление или изменение информации об участниках;
- добавление или изменение информации об угрозах;
- добавление, изменение или публикация бюллетеней;
- добавление или изменение информационной карточки;
- добавление или изменение задач;
- добавление вложения;
- добавление или изменение справочных данных;
- добавление комментариев;
- уведомления.

Команды пересылаются сообщениями при следующих действиях:

- сканировании файла в PT MS;
- отправка запроса на содействие в ГосСОПКА;

- создание связи с объектом;
- создание артефакта;
- запуск NSLOOKUP;
- запуск WHOIS;
- отправка письма;
- отправка ответного письма;
- создание записи в логе.

Таблица 18. Перечень событий и команд в очередях

Очередь	События и команды	Назначение очереди
PT.SP.Bulletins	PT.SP.Bulletins.Events:BulletinCreated PT.SP.Bulletins.Events:BulletinDeleted PT.SP.Bulletins.Events:BulletinPublished PT.SP.Bulletins.Events:BulletinUpdated PT.SP.Concurrency.Events:ConflictEncountered PT.SP.Dictionaries.Events:DictionaryActivated PT.SP.Dictionaries.Events:DictionaryDeactivated PT.SP.Dictionaries.Events:DistributionListCreated PT.SP.Dictionaries.Events:DistributionListUpdated PT.SP.Participants.Events:ParticipantActivated	Обработка событий по бюллетеням

Очередь	События и команды	Назначение очереди
	PT.SP.Participants.Events:ParticipantCreated PT.SP.Participants.Events:ParticipantDeactivated PT.SP.Participants.Events:ParticipantUpdated PT.SP.SubjectsObjectsSystems.Contracts.Users:UserCreated PT.SP.SubjectsObjectsSystems.Contracts.Users:UserUpdated	
PT.SP.Comments.Queue	PT.SP.Comments.Events:CommentCreated	Обработка событий по комментариям
PT.SP.Dictionaries	PT.SP.Concurrency.Events:ConflictEncountered PT.SP.Dictionaries.Events:CountryCreated PT.SP.Dictionaries.Events:DictionaryActivated PT.SP.Dictionaries.Events:DictionaryCreated PT.SP.Dictionaries.Events:DictionaryCreated_V2 PT.SP.Dictionaries.Events:DictionaryDeactivated PT.SP.Dictionaries.Events:DictionaryUpdated PT.SP.Dictionaries.Events:DistributionListCreated PT.SP.Dictionaries.Events:DistributionListCreated_V2 PT.SP.Dictionaries.Events:DistributionListUpdated PT.SP.Dictionaries.Events:FederalDistrictCreated PT.SP.Dictionaries.Events:IncidentRecommendationTemplateCreated PT.SP.Dictionaries.Events:IncidentRecommendationTemplateUpdated PT.SP.Dictionaries.Events:LegalEntityFormCreated PT.SP.Dictionaries.Events:LegalEntityFormCreated_V2 PT.SP.Dictionaries.Events:LegalEntityFormCreated_V3 PT.SP.Dictionaries.Events:LegalEntityFormUpdated PT.SP.Dictionaries.Events:SubjectOfFederationCreated	Обработка событий по словарям

Очередь	События и команды	Назначение очереди
PT.SP.Emails.Queue	PT.SP.Emails.Contracts.Email:ReplyToEmail PT.SP.Emails.Contracts.Email:SendEmail PT.SP.Emails.Contracts.Email:SendEmailBatch PT.SP.Emails:Processed	Обработка команд по отправке писем по электронной почте
PT.SP.Incidents.FC	PT.SP.Incidents.FC.Events:IncidentActionAdded PT.SP.Incidents.FC.Events:IncidentAssistanceRequested PT.SP.Incidents.FC.Events:IncidentCertInfoUpdated PT.SP.Incidents.FC.Events:IncidentCommentAdded PT.SP.Incidents.FC.Events:IncidentCreated_V2 PT.SP.Incidents.FC.Events:IncidentMessageAdded PT.SP.Incidents.FC.Events:IncidentRecommendationAdded PT.SP.Incidents.FC.Events:IncidentRegistered PT.SP.Incidents.FC.Events:IncidentStatusChanged_V2 PT.SP.Incidents.FC.Events:IncidentUpdated PT.SP.Participants.Events:ParticipantActivated PT.SP.Participants.Events:ParticipantCreated PT.SP.Participants.Events:ParticipantDeactivated PT.SP.Participants.Events:ParticipantUpdated PT.SP.SubjectsObjectsSystems.Contracts.Users:UserCreated PT.SP.SubjectsObjectsSystems.Contracts.Users:UserUpdated	Обработка событий по инцидентам
PT.SP.Participants	PT.SP.Dictionaries.Events:DictionaryCreated PT.SP.Dictionaries.Events:DictionaryUpdated PT.SP.Dictionaries.Events:LegalEntityFormCreated PT.SP.Dictionaries.Events:LegalEntityFormCreated_V2 PT.SP.Dictionaries.Events:LegalEntityFormUpdated PT.SP.Participants.Events:ParticipantActivated PT.SP.Participants.Events:ParticipantCreated	Обработка событий по участникам и пользователям участников

Очередь	События и команды	Назначение очереди
	PT.SP.Participants.Events:ParticipantDeactivated PT.SP.Participants.Events:ParticipantSoftwareAdded PT.SP.Participants.Events:ParticipantSoftwareDeleted PT.SP.Participants.Events:ParticipantSoftwareUpdated PT.SP.Participants.Events:ParticipantUpdated PT.SP.Participants.Events:ParticipantUserActivated PT.SP.Participants.Events:ParticipantUserCreated PT.SP.Participants.Events:ParticipantUserDeactivated PT.SP.Participants.Events:ParticipantUserUpdated PT.SP.Participants.Sagas.Contracts:ActivateParticipantInActiveDirectory PT.SP.Participants.Sagas.Contracts:ActivateParticipantUserInActiveDirectory PT.SP.Participants.Sagas.Contracts:CreateParticipantInActiveDirectory PT.SP.Participants.Sagas.Contracts:CreateParticipantUserInActiveDirectory PT.SP.Participants.Sagas.Contracts:DeactivateParticipantInActiveDirectory PT.SP.Participants.Sagas.Contracts:DeactivateParticipantUserInActiveDirectory PT.SP.Participants.Sagas.Contracts:UpdateParticipantInActiveDirectory PT.SP.Participants.Sagas.Contracts:UpdateParticipantUserInActiveDirectory PT.SP.SubjectsObjectsSystems.Contracts.References:LegalEntityFormCreated PT.SP.SubjectsObjectsSystems.Contracts.References:ObjectCategoryCreated PT.SP.SubjectsObjectsSystems.Contracts.References:ObjectTypeCreated PT.SP.SubjectsObjectsSystems.Contracts.References:ProcessedDataTypeCreated PT.SP.SubjectsObjectsSystems.Contracts.References:SectorTypeCreated PT.SP.SubjectsObjectsSystems.Contracts.References:SoftwareCategoryCreated PT.SP.SubjectsObjectsSystems.Contracts.References:TelecomOperatorCreated PT.SP.SubjectsObjectsSystems.Contracts.References:UserCategoryCreated PT.SP.SubjectsObjectsSystems.Contracts.Users:UserCreated PT.SP.SubjectsObjectsSystems.Contracts.Users:UserUpdated	

Очередь	События и команды	Назначение очереди
PT.SP.Participants.Sagas	PT.SP.Participants.Events:ParticipantActivated PT.SP.Participants.Events:ParticipantCreated PT.SP.Participants.Events:ParticipantDeactivated PT.SP.Participants.Events:ParticipantUpdated PT.SP.Participants.Events:ParticipantUserActivated PT.SP.Participants.Events:ParticipantUserCreated PT.SP.Participants.Events:ParticipantUserDeactivated PT.SP.Participants.Events:ParticipantUserUpdated PT.SP.Participants.Sagas.Contracts.FullParticipant.Creation:StartFullParticipantCreationSaga PT.SP.Participants.Sagas.Contracts.FullParticipant.Updating:StartFullParticipantUpdatingSaga PT.SP.Participants.Sagas.Contracts:ParticipantActivatedInActiveDirectory PT.SP.Participants.Sagas.Contracts:ParticipantActiveDirectoryActivationFailed PT.SP.Participants.Sagas.Contracts:ParticipantActiveDirectoryCreationFailed PT.SP.Participants.Sagas.Contracts:ParticipantActiveDirectoryDeactivationFailed PT.SP.Participants.Sagas.Contracts:ParticipantActiveDirectoryUpdatingFailed PT.SP.Participants.Sagas.Contracts:ParticipantCreatedInActiveDirectory PT.SP.Participants.Sagas.Contracts:ParticipantDeactivatedInActiveDirectory PT.SP.Participants.Sagas.Contracts:ParticipantUpdatedInActiveDirectory PT.SP.Participants.Sagas.Contracts:ParticipantUserActivatedInActiveDirectory PT.SP.Participants.Sagas.Contracts:ParticipantUserActiveDirectoryActivationFailed PT.SP.Participants.Sagas.Contracts:ParticipantUserActiveDirectoryCreationFailed PT.SP.Participants.Sagas.Contracts:ParticipantUserActiveDirectoryDeactivationFailed PT.SP.Participants.Sagas.Contracts:ParticipantUserActiveDirectoryUpdatingFailed PT.SP.Participants.Sagas.Contracts:ParticipantUserCreatedInActiveDirectory PT.SP.Participants.Sagas.Contracts:ParticipantUserDeactivatedInActiveDirectory PT.SP.Participants.Sagas.Contracts:ParticipantUserUpdatedInActiveDirectory	Реализация распределенных транзакций для участника

Очередь	События и команды	Назначение очереди
	PT.SP.Participants.Sagas.Contracts:StartActivateParticipantSaga PT.SP.Participants.Sagas.Contracts:StartActivateParticipantUserSaga PT.SP.Participants.Sagas.Contracts:StartCreateParticipantSaga PT.SP.Participants.Sagas.Contracts:StartCreateParticipantUserSaga PT.SP.Participants.Sagas.Contracts:StartDeactivateParticipantSaga PT.SP.Participants.Sagas.Contracts:StartDeactivateParticipantUserSaga PT.SP.Participants.Sagas.Contracts:StartUpdateParticipantSaga PT.SP.Participants.Sagas.Contracts:StartUpdateParticipantUserSaga	
PT.SP.References.Queue	PT.SP.References.Commands:CreateReference PT.SP.References.Contracts.References:CreateReference PT.SP.References.Events:ReferenceCreated PT.SP.References.Events:ReferenceDeleted	Обработка команд на создание связи. Обработка событий по созданию и удалению связей
PT.SP.Requests	PT.SP.Participants.Events:ParticipantActivated PT.SP.Participants.Events:ParticipantCreated PT.SP.Participants.Events:ParticipantDeactivated PT.SP.Participants.Events:ParticipantUpdated PT.SP.Participants.Events:ParticipantUserCreated PT.SP.Participants.Events:ParticipantUserUpdated PT.SP.Requests.Events:MessageCreated PT.SP.Requests.Events:RequestAssigned PT.SP.Requests.Events:RequestCreated PT.SP.Requests.Events:RequestPriorityChanged PT.SP.Requests.Events:RequestRegistered PT.SP.Requests.Events:RequestStatusChanged	Обработка событий по запросам

Очередь	События и команды	Назначение очереди
	PT.SP.Requests.Events:RequestUnassigned PT.SP.SubjectsObjectsSystems.Contracts.Users:UserCreated PT.SP.SubjectsObjectsSystems.Contracts.Users:UserUpdated	
PT.SP.SubjectsObjectsSystems	PT.SP.Dictionaries.Events:CountryCreated PT.SP.Dictionaries.Events:DictionaryCreated PT.SP.Dictionaries.Events:DictionaryUpdated PT.SP.Dictionaries.Events:FederalDistrictCreated PT.SP.Dictionaries.Events:LegalEntityFormCreated PT.SP.Dictionaries.Events:LegalEntityFormCreated_V2 PT.SP.Dictionaries.Events:LegalEntityFormUpdated PT.SP.Dictionaries.Events:SubjectOfFederationCreated PT.SP.SubjectsObjectsSystems.Contracts.Users:UserCreated PT.SP.SubjectsObjectsSystems.Contracts.Users:UserUpdated	Обработка событий по словарям, созданию и обновлению данных пользователей
PT.SP.Threats	PT.SP.Threats.Events:ThreatCreated PT.SP.Threats.Events:ThreatUpdated PT.SP.Threats.Events:ThreatRegistered PT.SP.Threats.Events:ThreatStatusChanged PT.SP.Threats.Events:ThreatAssigned	Обработка событий по угрозам
PT.SP.Tickets	PT.SP.SubjectsObjectsSystems.Contracts.Users:UserCreated PT.SP.SubjectsObjectsSystems.Contracts.Users:UserUpdated PT.SP.Tickets.Events:TicketAssigned PT.SP.Tickets.Events:TicketCreated_v2	Обработка событий по задачам

Очередь	События и команды	Назначение очереди
	PT.SP.Tickets.Events:TicketRegistered PT.SP.Tickets.Events:TicketStatusChanged PT.SP.Tickets.Events:TicketUpdated_v2	
PT.SP.Artifacts.Commands.Enrichers.Nslookup.Queue	PT.SP.Artifacts.Commands:RunEnricherNslookup	Обработка команды на запуск NSLOOKUP
PT.SP.Artifacts.Commands.Enrichers.Whois.Queue	PT.SP.Artifacts.Commands:RunEnricherWhois	Обработка команды на запуск WHOIS
PT.SP.Artifacts.Events.Queue	PT.SP.Artifacts.Events:ArtifactCreated PT.SP.Artifacts.Events:EnricherCompleted	Обработка событий по артефактам
PT.SP.Attachments.Commands.Queue	PT.SP.Attachments.Commands:AttachmentScan PT.SP.Attachments.Commands:AttachmentSync PT.SP.Attachments.Commands:AttachmentValidate	Обработка команд для вложений
PT.SP.Attachments.Events:AttachmentCreated.Queue	PT.SP.Attachments.Events:AttachmentCreated	Обработка события создания вложения
PT.SP.Attachments.Events:MSScanResultReceived.Queue	PT.SP.Attachments.Events:MSScanResultReceived	Обработка события получения результата сканирования
PT.SP.InfoCards.Events.Queue	PT.SP.InfoCards.Events:HridGenerated PT.SP.InfoCards.Events:HridRequested PT.SP.InfoCards.Events:InfoCardCreated_V2 PT.SP.InfoCards.Events:InfoCardUpdated	Обработка событий по информационным карточкам

Очередь	События и команды	Назначение очереди
PT.SP.Notifications.Participants.Queue	PT.SP.Participants.Events:ParticipantActivated PT.SP.Participants.Events:ParticipantCreated PT.SP.Participants.Events:ParticipantCreated_V2 PT.SP.Participants.Events:ParticipantDeactivated PT.SP.Participants.Events:ParticipantUpdated PT.SP.Participants.Events:ParticipantUserActivated PT.SP.Participants.Events:ParticipantUserCreated PT.SP.Participants.Events:ParticipantUserCreated_V2 PT.SP.Participants.Events:ParticipantUserDeactivated PT.SP.Participants.Events:ParticipantUserUpdated	Создание уведомлений по событиям участников и пользователей участников
PT.SP.Notifications.Queue	PT.SP.Notifications.Contracts.NotificationsEvent:UserNotificationCreate	—
PT.SP.Notifications.Requests.Queue	PT.SP.Requests.Events:MessageCreated PT.SP.Requests.Events:RequestAssigned PT.SP.Requests.Events:RequestCreated PT.SP.Requests.Events:RequestCreated_V2 PT.SP.Requests.Events:RequestRegistered PT.SP.Requests.Events:RequestStatusChanged PT.SP.Requests.Events:RequestUnassigned	Создание уведомлений по событиям запросов
PT.SP.Notifications.Users.Queue	PT.SP.SubjectsObjectsSystems.Contracts.Users:UserCreated PT.SP.SubjectsObjectsSystems.Contracts.Users:UserUpdated	Создание уведомлений по событиям добавления и изменения данных пользователей
PT.SP.WE.CreateReference.Queue	PT.SP.References.Commands:CreateReferenceCommand	Обработка команды на создание связей между объектами системы

Очередь	События и команды	Назначение очереди
PT.SP.WE.ParticipantUpdated .Queue	PT.SP.Participants.Events:ParticipantUpdated	Обновление субъектов, объектов, систем, групп при получении события о редактировании участ-ника
WE.CreateRequestFromEmail .Queue	PT.SP.WE:CreateRequestFromEmail	—
WE.CreateRequestMessageFr omEmail.Queue	PT.SP.WE:CreateRequestMessageFromEmail	—
WE.ParticipantCreated.Queue	PT.SP.Participants.Events:ParticipantCreated PT.SP.Participants.Events:ParticipantCreated_V2	Создание субъектов, объектов, систем, групп при получении события о создании участника
ReportsService.Events.Queue	PT.SP.Incidents.Events:IncidentActionAdded PT.SP.Incidents.Events:IncidentAssistanceRequested PT.SP.Incidents.Events:IncidentCreated PT.SP.Incidents.Events:IncidentStatusChanged PT.SP.Incidents.Events:IncidentUpdated PT.SP.Incidents.FC.Events:IncidentActionAdded PT.SP.Incidents.FC.Events:IncidentAssistanceRequested PT.SP.Incidents.FC.Events:IncidentCreated PT.SP.Incidents.FC.Events:IncidentCreated_V2 PT.SP.Incidents.FC.Events:IncidentRecommendationAdded PT.SP.Incidents.FC.Events:IncidentRegistered PT.SP.Incidents.FC.Events:IncidentStatusChanged PT.SP.Incidents.FC.Events:IncidentStatusChanged_V2	Формирование отчетов

Очередь	События и команды	Назначение очереди
	PT.SP.Incidents.FC.Events:IncidentUpdated PT.SP.Participants.Events:ParticipantActivated PT.SP.Participants.Events:ParticipantCreated PT.SP.Participants.Events:ParticipantCreated_V2 PT.SP.Participants.Events:ParticipantDeactivated PT.SP.Participants.Events:ParticipantUpdated PT.SP.Participants.ParticipantActivated PT.SP.Participants.ParticipantCreated PT.SP.Participants.ParticipantCreated_V2 PT.SP.Participants.ParticipantDeactivated PT.SP.Participants.ParticipantUpdated PT.SP.Requests.Events:RequestCreated PT.SP.Requests.Events:RequestCreated_V2 PT.SP.Requests.Events:RequestStatusChanged PT.SP.SubjectsObjectsSystems.Contracts.Objects:ObjectActivated PT.SP.SubjectsObjectsSystems.Contracts.Objects:ObjectCreated PT.SP.SubjectsObjectsSystems.Contracts.Objects:ObjectDeactivated PT.SP.SubjectsObjectsSystems.Contracts.Subjects:SubjectActivated PT.SP.SubjectsObjectsSystems.Contracts.Subjects:SubjectCreated PT.SP.SubjectsObjectsSystems.Contracts.Subjects:SubjectDeactivated PT.SP.SubjectsObjectsSystems.Contracts.Subjects:SubjectUpdated PT.SP.SubjectsObjectsSystems.Contracts.Systems:SystemActivated PT.SP.SubjectsObjectsSystems.Contracts.Systems:SystemCreated PT.SP.SubjectsObjectsSystems.Contracts.Systems:SystemDeactivated PT.SP.SubjectsObjectsSystems.Contracts.Users.UserCreated PT.SP.SubjectsObjectsSystems.Contracts.Users.UserUpdated PT.SP.SubjectsObjectsSystems.ContractsUsers.UserCreated PT.SP.SubjectsObjectsSystems.ContractsUsers.UserUpdated	

Очередь	События и команды	Назначение очереди
PT.SP.Sync.Internal	Эту очередь пересылаются все вышеперечисленные события, которые поступили в сервис синхронизации из другого контура	Синхронизация событий
PT.SP.Sync.Internal.Commands	В эту очередь пересылаются все вышеперечисленные команды, которые поступили в сервис синхронизации из другого контура	Синхронизация команд
PT.SP.Sync.External	В эту очередь попадают все вышеперечисленные события, обернутые в CrossSystemIntegrationEvent, которые поступили в сервис синхронизации из другого контура	Синхронизация событий
PT.SP.Sync.External.Commands	В эту очередь попадают все вышеперечисленные команды, обернутые в CrossSystemCommand, которые поступили в сервис синхронизации из другого контура	Синхронизация команд
PT.SP.Sync.Forward	В эту очередь попадают все вышеперечисленные события, обернутые в CrossSystemIntegrationEvent, которые необходимо переслать на другой кон~тур	Синхронизация событий
PT.SP.Sync.Forward.Commands	В эту очередь попадают все вышеперечисленные команды, обернутые в CrossSystemCommand, которые необходимо переслать на другой контур	Синхронизация команд

Очереди формата `<Очередь>_error` содержат сообщения о том, что события или команды были обработаны с ошибками.

Очереди формата `<Очередь>_skipped` содержат сообщения о том, что события или команды не были обработаны из-за отсутствия обработчиков или из-за неработающего сервиса.

Приложение B. Параметры конфигурации компонентов PT Incident Processing Center на Microsoft Windows

Раздел содержит описание параметров конфигурации компонентов PT Incident Processing Center на Microsoft Windows.

Таблица 19. Параметры конфигурации "Личного кабинета оператора"

Параметр	Значение по умолчанию	Описание
ProjectName	PT IPC	Наименование системы
FileStorageDir	{{params.ProgramDataDir}}\file_storage	Путь к папке для хранения файлов
TempFileStorageDir	{{params.ProgramDataDir}}\file_storage_temp	Путь к папке для хранения временных файлов
FiasStorageDir	C:\\ProgramData\\Positive Technologies\\PT IPC\\fias_storage	Путь к папке для хранения файлов ФИАС
FiasTempDir	C:\\ProgramData\\Positive Technologies\\PT IPC\\fias_temp_storage	Путь к папке для хранения временных файлов ФИАС
IISProxyDir	{{params.InstallDir}}\IISProxy	Каталог прокси-сервера IIS
HostAddress	localhost	IP-адрес или FQDN узла, на котором установлен компонент
HostPort	443	Порт хоста сервера, используемый для доступа к компоненту
IAMHostAddress	localhost	IP-адрес или FQDN, используемый пользователями для доступа к PT MC
IAMApplicationId	PT.IPC	Идентификатор системы в PT MC
IAMApplicationDisplayName	PT IPC	Наименование системы в PT MC
IAMApplicationSecret	secret	Код для получения токена в PT MC
SqlServerName	localhost\PTIPCCORE	Экземпляр SQL сервера для текущей инсталляции
SqlServerFiasNode1DBName	FiasNode1	Основная база данных ФИАС

Параметр	Значение по умолчанию	Описание
SqlServerFiasNode2DBName	FiasNode2	Резервная база данных ФИАС
SqlServerUserName	sa	Логин пользователя SQL Server
SqlServerPassword	P@ssw0rdP@ssw0rd	Пароль пользователя SQL Server
PostgresHost	localhost	IP-адрес или FQDN узла, на котором установлен PostgreSQL
PostgresPort	5432	Порт PostgreSQL
PostgresLogin	pt_system	Логин пользователя PostgreSQL
PostgresPassword	P@ssw0rdP@ssw0rd	Пароль пользователя PostgreSQL
EventStoreDbName	eventstore	Имя базы данных хранилища событий
RabbitMQHost	localhost	IP-адрес или FQDN узла, на котором установлена платформа RabbitMQ, реализующая обмен сообщениями между компонентами PT Incident Processing Center
RabbitMQUsername	guest	Логин служебной учетной записи компонента в платформе RabbitMQ, реализующей обмен сообщениями между компонентами
RabbitMQPassword	guest	Пароль служебной учетной записи компонента в платформе RabbitMQ, реализующей обмен сообщениями между компонентами
SyncExternalRabbitMQHost	—	IP-адрес или FQDN RabbitMQ контура, с которым происходит синхронизация данных
SyncExternalRabbitMQUsername	pt_system	Логин служебной учетной записи RabbitMQ, контура, с которым происходит синхронизация данных

Параметр	Значение по умолчанию	Описание
SyncExternalRabbitMQPassword	P@ssw0rdP@ssw0rd	Пароль служебной учетной записи RabbitMQ контура, с которым происходит синхронизация данных
SSLCertificateThumb	C668EE08D74CD083C7407DBAA42CE8E1371BFD2E	Сертификат для https для "Информационного портала"
s7zLocation	C:\Program Files\7-Zip\7z.dll	Путь к 7z.dll
PythonHome	$(Pt.Deployment\Get-PythonHome 3.5 x64)	Путь к корневой папке Python
DotnetLocation	C:\Program Files\dotnet	Путь к корневой папке ядра dotnet
PostgresBin	C:\\Program Files\\Positive Technologies\\Common\\PostgreSQL\\bin	Путь к папке bin PostgreSQL
EscapedLogsDir	C:\\ProgramData\\Positive Technologies\\PT IPC\\logs	Путь к каталогу лог-файлов
InternalAuthTmRegistrationId	6499bc91-05b9-4d06-822f-bac8469e1777	Идентификатор для регистрации приложения в PT MC
InternalAuthRedirectUri	/account/oauthcallback	Ссылка для редиректа после авторизации в PT MC
InternalAuthCookieExpireTimeInMinutes	1441	Время (в минутах) за которое истекают cookies PT MC
InternalJwtTokenSecret	the secret for HmacSha256 (32 b)	Секретный ключ для авторизационного токена
GatewayAPIPort	7000	Порт для сервиса маршрутизации
SubjectsObjectsSystemsServicePort	7001	Порт сервиса С-О-ИТС
ReportsServicePort	7002	Порт для сервиса отчетов
IncidentsServicePort	7003	Порт для сервиса инцидентов
ConfigurationServicePort	7004	Порт для сервиса настройки
ParticipantsServicePort	7005	Порт для сервиса участников

Параметр	Значение по умолчанию	Описание
NotificationsServicePort	7006	Порт для сервиса уведомлений
ReferencesServicePort	7007	Порт для сервиса связей
TicketsServicePort	7010	Порт для сервиса задач
BulletinsServicePort	7009	Порт для сервиса бюллетеней
RequestsServicePort	7011	Порт для сервиса запросов
FiasServicePort	7012	Порт для сервиса ФИАС
InfoCardsServicePort	7013	Порт для сервиса информационных карточек
AttachmentsServicePort	7014	Порт для сервиса вложений
SyncServicePort	7015	Порт для сервиса синхронизации
DictionariesServicePort	7017	Порт для сервиса словарей
WorkflowEngineServicePort	7016	Порт для сервиса сценариев
CommentsServicePort	7018	Порт для сервиса комментариев
AttachmentsStorageDir	C:\\ProgramData\\Positive Technologies\\PT IPC\\attachments_storage	Путь к файловому хранилищу dir для вложений
RarExecPath	C:\\Program Files\\WinRAR\\rar.exe	Путь к rar.exe
UnrarExecPath	C:\\Program Files\\WinRAR\\unrar.exe	Путь к unrar.exe
MasterAttachmentsApiHost	—	Хост сервиса вложений для синхронизации файлов между контурами
MasterAttachmentsApiToken	MAGIC_SYSTEM_ACCESS_TOKEN	Токен для авторизации в сервисе вложений для синхронизации файлов между контурами

Параметр	Значение по умолчанию	Описание
StorageSyncDirs	—	Разделенный запятыми список подпапок хранилища для синхронизации
StorageSyncEnabled	off	Включение (on) или выключение (off) просмотрщика папки синхронизации
EmailsAttachmentsStorageDir	C:\\ProgramData\\Positive Technologies\\PT IPC\\emails_attachments_storage	Путь к файловому хранилищу dir для вложений из писем
MailboxesConfiguration	—	Настройка почтовых ящиков для прослушивания (указываются через запятую)
SMTPConfiguration	—	Настройки для SMTP
DefaultFromEmail	—	Электронная почта, из которой будут отправляться письма
EmailSenderEnabled	on	Включение отправки электронных писем. SMTPConfiguration также должен быть установлен
EmailReceiverEnabled	on	Включение получения электронной почты. MailboxesConfiguration также должен быть установлен
EmailSigningEnabled	off	Включение (on) или отключение (off) электронной подписи. EmailSigningCertContainerPath, EmailSigningCertContainerPassword или EmailSigningCertFingerprint должны быть установлены
EmailSigningCertContainerPath	—	Путь к контейнеру сертификатов (pfx\p12) для подписи электронной почты
EmailSigningCertContainerPassword	—	Пароль для контейнера, указанный в EmailSigningCertContainerPath

Параметр	Значение по умолчанию	Описание
EmailCertValidation	on	Включение (on) выключение (off) проверки сертификата сервера для отправки электронной почты
EmailSigningCertFingerprint	—	Отпечаток сертификата для электронной подписи, если сертификат был импортирован в реестр
InternalMagicSystemAccessToken	MAGIC_SYSTEM_ACCESS_TOKEN	Внутренний токен авторизации
AppName	PT Incident Processing Center	Наименование системы
AppModules	References,Users,Management,Notifications,IncidentsFC,Participants,Requests,Tickets,Bulletins,Infocards,Dashboards,Comments	Модули приложения
NodeId	lk-operator-open	Идентификатор текущего узла
NodeType	main	Тип текущего узла
NodeRole	OperatorsPortal	Роль текущего узла
MSBaseUrl	https://localhost	URL для доступа к API PT MS
MSLogin	admin	Логин для API PT MS
MSPassword	admin	Пароль для API PT MS
MSEnabled	on	Переключатель для включения (on) или отключить (off) отправка вложений в PT MS
MSAutoScanMaxFileSize	10485760	Максимальный размер файла для автоматической загрузки в PT MS
ActiveDirectoryIsEnabled	true	Включение интеграции с Active Directory
ActiveDirectoryHost	localhost	IP-адрес или FQDN Active Directory
ActiveDirectoryPort	389	Порт для открытого соединения с Active Directory
ActiveDirectorySslPort	636	Порт для защищенного соединения с Active Directory
ActiveDirectoryTransportSecurity	ssl	Протокол для доступа к Active Directory

Параметр	Значение по умолчанию	Описание
ActiveDirectoryUserDn	CN=root,CN=users,DC=ptipc,DC=ru	Настройки пользователя для управления Active Directory
ActiveDirectoryPassword	P@ssw0rd	Пароль пользователя Active Directory
ActiveDirectoryBaseDn	DC=ptipc,DC=ru	Настройки пользователя для сохранения участников в Active Directory
ExternalDestinationNodeId	lku	Идентификатор внешней очереди
InternalPublishTo	true	Публиковать на внутренний RabbitMQ
InternalListenTo	true	Слушать внутренний RabbitMQ
InternalDestinationNodeId	lk-operator-closed	Идентификатор внутренней очереди
IsHridGenerator	true	Генерация человекочитаемого идентификатора сущности
InitializeSync	false	Инициализация синхронизации из других узлов
MSCountOfSendingDocuments	10	Количество отправок документов в PT MS
MSCountOfGettingResults	10	Количество попыток получить вердикт PT MS
CertCoreBaseUrl	http://localhost:3344	URL для доступа к Cert
CertCoreAuthToken	tokentoken	Токен авторизации в Cert
CertCoreCountOfFileRequests	5	Количество попыток получить файл от PT Incident Processing Center
CertCoreCountOfCertCoreResponses	10	Количество запросов, обрабатываемых одновременно
BaseUrl	http://+:3399/	Базовый URL для синхронизации
CertLogDebugInfo	false	Логировать сообщения PT Incident Processing Center

Таблица 20. Параметры конфигурации "Личного кабинета участника"

Параметр	Значение по умолчанию	Описание
InstallDir	C:\Program Files\Positive Technologies \PTIPCParticipantsPortal	Путь к папке для установки компонента
InstallationSubfolder	C:\Program Files\Positive Technologies \PTIPCParticipantsPortal \.install	Путь к дочерним папкам
ProgramDataDir	C:\ProgramData\Positive Technologies\PT IPC	Путь к папке с временными данными
ProjectName	PT IPC	Наименование системы
FiasStorageDir	C:\\ProgramData\\Positive Technologies\\PT IPC\ \fias_storage	Путь к хранилищу файлов ФИАС
FiasTempDir	C:\\ProgramData\\Positive Technologies\\PT IPC\ \fias_temp_storage	Путь к хранилищу временных файлов ФИАС
IISProxyDir	{{params.InstallDir}}\IISProxy	Каталог прокси-сервера IIS
HostAddress	localhost	IP-адрес или FQDN узла, на котором установлен компонент
HostPort	—	Порт хоста сервера, используемый для доступа к компоненту
PostgresHost	localhost	IP-адрес или FQDN узла, на котором установлен PostgreSQL
PostgresPort	5432	Порт Postgres
PostgresLogin	pt_system	Логин пользователя Postgres
PostgresPassword	P@ssw0rdP@ssw0rd	Пароль пользователя Postgres
EventStoreDbName	eventstore	Имя базы данных хранилища событий
RabbitMQHost	localhost	IP-адрес или FQDN узла, на котором установлена платформа RabbitMQ, реализующая обмен сообщениями между компонентами PT Incident Processing Center

Параметр	Значение по умолчанию	Описание
RabbitMQUsername	pt_system	Логин служебной учетной записи компонента в платформе RabbitMQ, реализующей обмен сообщениями между компонентами
RabbitMQPassword	P@ssw0rdP@ssw0rd	Пароль служебной учетной записи компонента в платформе RabbitMQ, реализующей обмен сообщениями между компонентами
SSLCertificateThumb	C668EE08D74CD083C7407DBAA42CE8E1371BFD2E	Сертификат для https для "Информационного портала"
AntifraudEnabled	False	Включение (true) или выключение (false) сервиса антифрода
DotnetLocation	C:\Program Files\dotnet	Путь к корневой папке ядра dotnet
PostgresBin	C:\\Program Files\\Positive Technologies\\Common\\PostgreSQL\\bin	Путь к папке bin PostgreSQL
EscapedLogsDir	C:\\ProgramData\\Positive Technologies\\PT IPC\\logs	Путь к каталогу лог-файлов
LogArchiveInterval	7	Интервал архивирования лог-файлов (в днях)
ArchiveLogs	true	Включение (true) или выключение (false) архивации логов
PythonHome	C:\Program Files\Python35	Путь к корневой папке Python
InternalAuthCookieExpireTimeInMinutes	1441	Время (в минутах), за которое истекают cookies PT MC
InternalJwtTokenSecret	the secret for HmacSha256 (32 b)	Секретный ключ для авторизационного токена
GatewayAPIPort	7000	Порт для сервиса маршрутизации
ConfigurationServicePort	7004	Порт сервиса настройки
ParticipantsServicePort	7005	Порт сервиса участников
DictionariesServicePort	7017	Порт сервиса словарей

Параметр	Значение по умолчанию	Описание
RequestsServicePort	7011	Порт сервиса запросов
FiasServicePort	7012	Порт сервиса ФИАС
AttachmentsServicePort	7014	Порт сервиса вложений
SyncServicePort	7015	Порт сервиса синхронизации
BulletinsServicePort	7009	Порт сервиса бюллетеней
ExternalApiServicePort	7024	Порт внешнего API
NotificationsServicePort	7006	Порт для сервиса уведомлений
SMTPConfiguration	—	Настройки для SMTP
DefaultFromEmail	—	Электронная почта, из которой будут отправляться письма
EmailSenderEnabled	false	Включение (true) или запрет (false) отправки электронных писем. SMTPConfiguration также должен быть установлен
EmailSenderInterval	1	Интервал отправки сообщений (в секундах)
EmailReceiverEnabled	false	Включение (true) или запрет (false) получения электронной почты. MailboxesConfiguration также должен быть установлен
EmailSigningEnabled	false	Включение (true) или отключение (false) электронной подписи
EmailSigningCertContainerPath	—	Путь к контейнеру сертификатов (pfx\p12) для подписи электронной почты
EmailSigningCertContainerPassword	—	Пароль для контейнера сертификатов для подписи электронной почты

Параметр	Значение по умолчанию	Описание
EmailCertValidation	true	Включение (true) выключение (false) проверки сертификата сервера для отправки электронной почты
EmailSigningCertFingerprint	—	Отпечаток сертификата для электронной подписи, если сертификат был импортирован в реестр
EmailSigningScriptPath	—	Полный путь к сценарию powershell для подписи электронной почты
EmailSigningDLLPath	—	Полный путь к DLL для скрипта подписи электронной почты
AttachmentsStorageDir	—	Путь к хранилищу вложений
RarExecPath	C:\\Program Files\\WinRAR\\rar.exe	Путь к rar.exe
UnrarExecPath	C:\\Program Files\\WinRAR\\unrar.exe	Путь к unrar.exe
InternalMagicSystemAccessToken	MAGIC_SYSTEM_ACCESS_TOKEN	Внутренний токен авторизации
AppName	PT Incident Processing Center ЛК Участника	Наименование компонента
AppModules	Notifications,Participants,Requests,Bulletins	Модули приложения
NodeId	lk-member	Идентификатор текущего узла
NodeRole	ParticipantsPortal	Роль текущего узла
NodeType	auxiliary	Тип текущего узла
AttachmentsStorageDir	—	Путь к файловому хранилищу dir для вложений
MSBaseUrl	https://localhost	URL для доступа к API PT MS
MSLogin	admin	Логин пользователя PT MS
MSPassword	admin	Пароль пользователя PT MS
MSEnabled	false	Переключатель для включения (true) или отключить (false) отправка вложений PT MS

Параметр	Значение по умолчанию	Описание
MSAutoScanMaxFileSize	10485760	Максимальный размер файла для автоматической загрузки в PT MS
ActiveDirectoryHost	mafin.ad2.ru	IP-адрес или FQDN Active Directory
ActiveDirectoryPort	389	Порт для Active Directory
ActiveDirectorySslPort	636	Порт Active Directory Ssl
ActiveDirectoryTransportSecurity	ssl	Протокол для доступа к Active Directory
ActiveDirectoryUserDn	CN=root,CN=users,DC=ad2,DC=ru	Настройки пользователя для управления Active Directory
ActiveDirectoryPassword	P@ssw0rd	Пароль пользователя Active Directory
ActiveDirectoryBaseDn	DC=ad2,DC=ru	Настройки пользователя для сохранения участников в Active Directory
InternalDestinationNodeId	lk-operator-open	Идентификатор внутренней очереди
InitializeSync	false	Синхронизация должна быть инициализирована из других узлов
WebsiteBaseUrl	—	URL для входа в систему
SiemLoggingDir	C:\ProgramData\Positive Technologies\PT IPC\SiemLogs	Путь к хранилищу лог-файлов SIEM
SiemStorageInterval	5	Продолжительность хранения файла журнала SIEM (в днях)
RequestMaxEFCount	10	Максимальное количество вложенных электронных форм в одном запросе
ClearBlackListJobIntervalInMinutes	360	Интервал (в минутах) очистки черного списка токенов авторизации
MaxRecipientsPerMessage	200	Максимальное количество получателей сообщения

Таблица 21. Параметры конфигурации "Информационного портала"

Параметр	Значение по умолчанию	Описание
`MediaDir`	`C:\ProgramData\Positive Technologies \Info Portal\PTIPCInfoPortal\Content \Media`	Путь к папке, в которую сохраняются медиа-файлы
`LogsDir`	`C:\ProgramData\Positive Technologies \Info Portal\PTIPCInfoPortal\Logs`	Путь к папке, в которую сохраняются лог-файлы
`SnapshotsDir`	`C:\ProgramData\Positive Technologies \Info Portal\PTIPCInfoPortal\Content \Snapshots`	Путь к папке, в которую сохраняются снимки файловой системы
`SyncDir`	`C:\ProgramData\Positive Technologies \Info Portal\PTIPCInfoPortal\Sync`	Путь к папке синхронизации. Система архивирует снимок файловой системы и помещает в папку синхронизации. Сервис вложений при появлении нового архива переносит его в соответствующую папку на ведомом контуре
`Mode`	`Master`	В режиме Master в "Информационном портале" доступна учетная запись администратора по адресу {{host_name}}/admin. В режиме Slave учетная запись администратора недоступна

Приложение Г. Журналирование действий пользователя в PT MaxPatrol SIEM

PT Incident Processing Center считывает информацию о действиях пользователей в системе в рамках каждого контура и сохраняет информацию в текстовых файлах в формате JSON. Для "Личного кабинета оператора" эти файлы хранятся в папке `C:\ProgramData\Positive Technologies\Department Center\siem logging\default`. Для "Личного кабинета участника" эти файлы хранятся в папке `C:\ProgramData\Positive Technologies \Department Center\siem logging`. По умолчанию файлы хранятся в системе 30 дней. Вы можете изменить время хранения файлов в системе.

Таблица 22. Журналируемые действия пользователей

Действие	"Личный кабинет оператора"	"Личный кабинет участника"
Вход пользователя в систему	+	+
Выход пользователя из системы	+	+
Время сессии истекло	+	+
Создание черновика запроса	+	+
Регистрация запроса	+	+
Отправка сообщения в карточке запроса	+	+
Смена статуса запроса	+	–
Смена приоритета запроса	+	–
Назначение ответственного за обработку запроса	+	–
Создание задачи	+	–
Присвоение идентификатора задаче	+	–
Изменение параметров задачи	+	–
Изменение итога задачи	+	–
Задача назначена на оператора	+	–
Задача снята с оператора	+	–
Смена статуса задачи	+	–
Просмотр задачи	+	–
Создание информационной карточки	+	–
Присвоение идентификатора информационной карточке	+	–
Изменение параметров информационной карточки	+	–

Действие	"Личный кабинет оператора"	"Личный кабинет участника"
Просмотр информационной карточки	+	–
Добавление связи	+	–
Удаление связи	+	–
Добавление комментария	+	–
Добавление вложения	+	–
Удаление вложения	+	–
Скачивание вложения	+	–
Добавление угрозы	+	–
Назначение угрозе идентификатора	+	–
Изменение статуса угрозы	+	–
Изменение параметров угрозы	+	–
Назначение ответственного за обработку угрозы	+	–
Создание бюллетеня	+	–
Изменение бюллетеня	+	–
Создание бюллетеня на основе существующего	+	–
Просмотр бюллетеня	+	–
Публикация бюллетеня	+	–
Добавление инцидента	+	–
Назначение инциденту идентификатора	+	–
Смена статуса инцидента	+	–
Изменение параметров инцидента	+	–
Назначение ответственного за расследование инцидента	+	–
Просмотр карточки инцидента	+	–
Формирование отчета по инциденту	+	–
Добавление уязвимости	+	–
Назначение ответственного за обработку уязвимости	+	–
Смена статуса уязвимости	+	–
Изменение параметров уязвимости	+	–
Назначение идентификатора уязвимости	+	–

Действие	"Личный кабинет оператора"	"Личный кабинет участника"
Просмотр карточки уязвимости	+	–
Добавление комментария	+	–

Вы можете просматривать информацию о действиях пользователей в PT MaxPatrol SIEM.

О компании

"Позитив Текнолоджиз" — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения "Позитив Текнолоджиз" для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты "Позитив Текнолоджиз" заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com