Позитив Текнолоджиз Ведомственный центр

Версия 0.9

Руководство оператора

POSITIVE TECHNOLOGIES

Дата редакции документа: 28.03.2018

Содержание

1. Об этом документе ... 5
   1.1. Условные обозначения ... 5
   1.2. Другие источники информации о ПТ ВЦ ... 6
2. О системе ПТ ВЦ ... 7
3. Вход в ПТ ВЦ через PT IAM ... 8
4. Интерфейс ПТ ВЦ ... 9
   4.1. Главное меню ... 10
   4.2. Панель инструментов ... 10
   4.3. Рабочая область ... 10
5. Представление статистических данных в ПТ ВЦ: дашборды и виджеты ... 12
   5.1. Работа со статистическими данными ... 12
   5.2. Просмотр статистических данных ... 13
   5.3. Настройка виджета ... 14
6. Работа с субъектами ... 15
   6.1. Создание субъекта ... 15
   6.2. Просмотр информации о субъекте ... 16
   6.3. Изменение параметров субъекта ... 16
   6.4. Деактивация субъекта ... 16
7. Работа с объектами ... 18
   7.1. Создание объекта ... 18
   7.2. Просмотр информации об объекте ... 19
   7.3. Изменение параметров объекта ... 19
   7.4. Деактивация объекта ... 20
8. Работа с активами ... 21
   8.1. Добавление актива ... 22
   8.2. Просмотр информации об активе ... 23
   8.3. Изменение данных паспорта актива ... 23
   8.4. Изменение ОС и ПО актива ... 24
   8.5. Выпуск отчета по активам ... 24
9. Работа с инцидентами ... 26
   9.1. Создание инцидента ... 26
   9.2. Просмотр карточки инцидента ... 27
   9.3. Изменение параметров инцидента ... 27
   9.4. Изменение статуса инцидента ... 28
   9.5. Создание задачи по инциденту ... 28
   9.6. Фильтрация инцидентов ... 29
      9.6.1. Фильтрация инцидентов по группе активов ... 29
      9.6.2. Фильтрация инцидентов с помощью системных или пользовательских фильтров ... 30
      9.6.3. Фильтрация инцидентов с помощью PDQL-запроса ... 30
      9.6.4. Фильтрация инцидентов по статусу ... 31
   9.7. Создание пользовательского фильтра по инцидентам ... 31
   9.8. Создание папки фильтров по инцидентам ... 32
   9.9. Ручное и автоматическое обновлений списка инцидентов ... 32
   9.10. Импорт инцидентов ... 32
   9.11. Экспорт инцидентов ... 33

9.12. Выпуск отчета по инцидентам ... 34
10. Работа со справочниками ... 35
10.1. Работа со справочником "Ответственные лица" ... 36
10.1.1. Добавление записи об ответственном лице ... 36
10.1.2. Изменение информации об ответственном лице ... 36
10.1.3. Удаление записи об ответственном лице ... 37
11. Обращение в службу технической поддержки ... 38
11.1. Техническая поддержка на портале ... 38
11.2. Техническая поддержка по телефону ... 39
11.3. Время работы технической поддержки ... 39
11.4. Как служба технической поддержки работает с заявками ... 39
11.4.1. Предоставление информации для технической поддержки ... 40
11.4.2. Типы инцидентов ... 40
11.4.3. Время реакции на обращение и приоритизация инцидентов ... 41
11.4.4. Выполнение работ по заявке ... 42

1. Об этом документе

Руководство оператора безопасности содержит пошаговые инструкции и справочную информацию об использовании Позитив Текнолоджиз Ведомственный центр (далее также — ПТ ВЦ) для защиты и управления информационными активами организации. В руководстве вы также найдете инструкции по настройке ключевых и дополнительных функций продукта для выполнения конкретных задач. Руководство не содержит инструкций по установке, первоначальной настройке и администрированию ПТ ВЦ.

Руководство адресовано руководителям и специалистам, ответственным за обеспечение информационной безопасности, контроль и расследование инцидентов.

Комплект документации ПТ ВЦ включает в себя следующие документы:

- Этот документ.
- Руководство администратора — содержит справочную информацию и инструкции по установке, настройке и администрированию продукта.
- Руководство по установке — содержит инструкции по установке, первоначальной настройке, обновлению и удалению продукта.

В этом разделе

- Условные обозначения (см. раздел 1.1)
- Другие источники информации о ПТ ВЦ (см. раздел 1.2)

1.1. Условные обозначения

В документе приняты условные обозначения (см. таблицу 1).

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, нажмите кнопку	Начало инструкции выделено специальным значком
Нажмите кнопку **OK**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом

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

1.2. Другие источники информации о ПТ ВЦ

Вы можете найти дополнительную информацию о ПТ ВЦ на www.ptsecurity.com и на портале технической поддержки support.ptsecurity.com.

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

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки (см. раздел 11).

Вы можете пройти обучение по ПТ ВЦ в одном из учебных центров, авторизованных "Позитив Текнолоджиз". Перечень учебных центров можно найти на www.ptsecurity.com.

2. О системе ПТ ВЦ

Позитив Текнолоджиз Ведомственный центр (далее также — ПТ ВЦ) предназначена для информационного взаимодействия с главным центром ГосСОПКА с целью обнаружения, предотвращения и ликвидации последствий компьютерных атак. С помощью ПТ ВЦ осуществляются:

- сбор данных об инцидентах;
- регистрация инцидентов путем создания заявок на их обработку;
- реагирование на инциденты (координация действий, определение причин, локализация инцидента, планирование мер по ликвидации последствий, контроль ликвидации последствий);
- обмен данными об инцидентах с главным центром ГосСОПКА;
- применение методических рекомендаций главного центра ГосСОПКА в процессе мониторинга информационной безопасности.

3. Вход в ПТ ВЦ через PT IAM

Сервис управления пользователями и доступом Positive Technologies Identity and Access Management (PT IAM) обеспечивает механизм единого входа (технология single sign-on) в приложения "Позитив Текнолоджиз".

Перед входом в ПТ ВЦ запросите у администратора PT IAM:

- ссылку для входа в интерфейс продукта;
- логин и пароль вашей учетной записи пользователя.

Примечание. Убедитесь, что в браузере разрешены всплывающие окна.

► Чтобы войти в ПТ ВЦ:

1. В адресной строке браузера введите ссылку для входа в интерфейс ПТ ВЦ.

   Откроется страница входа в сервис PT IAM (см. рисунок ниже).

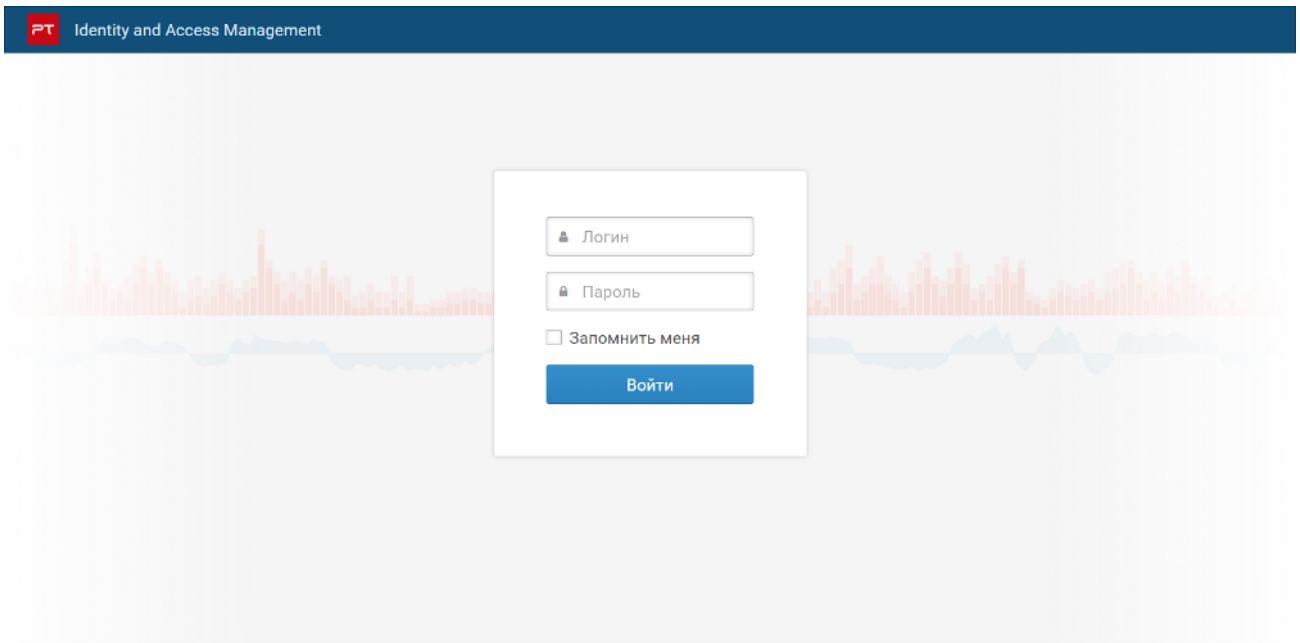

Рисунок 1. Ввод учетных данных

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

PT IAM проверяет введенные вами учетные данные. Если вы указали верные данные, откроется стартовая страница с системным дашбордом ПТ ВЦ. Если вы указали неверные данные, отобразится сообщение об ошибке.

4. Интерфейс ПТ ВЦ

При входе в ПТ ВЦ по умолчанию открывается домашняя страница.

Домашняя страница содержит главное меню, панель инструментов и рабочую область.

Главное меню обеспечивает доступ к основным функциям ПТ ВЦ и содержит следующие элементы:

- разделы для перехода к страницам ПТ ВЦ;
- кнопку ≡, по которой вы можете переходить из ПТ ВЦ в сервис управления пользователями и доступом PT Identity and Access Management;
- раздел с данными учетной записи.

Рабочая область главной страницы содержит системный дашборд **Домашняя страница**. Системный дашборд **Домашняя страница** содержит предустановленные виджеты, состав и расположение которых вы не можете изменять. Виджеты отображают следующую информацию:

- количество субъектов;
- количество объектов;
- количество активов;
- количество инцидентов;
- количество закрытых инцидентов;
- количество открытых инцидентов;
- диаграмму распределения количества инцидентов по статусу во времени;
- диаграмму распределения количества инцидентов по уровням опасности во времени;
- первые десять субъектов с наибольшей интегральной уязвимостью.

При работе с домашней страницей вы можете:

- просматривать данные на виджетах;
- настраивать период времени, за который вам требуется просматривать информацию, на виджетах **Созданные инциденты** и **Статус инцидентов**. По умолчанию каждый виджет содержит статистические данные за последние 30 дней.

При первом входе в ПТ ВЦ после установки виджеты системного дашборда **Домашняя страница** будут пустые, потому что в системе не заведены активы и нет информации об уязвимостях и созданных инцидентах.

В этом разделе

- Главное меню (см. раздел 4.1)
- Панель инструментов (см. раздел 4.2)
- Рабочая область (см. раздел 4.3)

4.1. Главное меню

Главное меню расположено в верхней части страницы.

Главное меню обеспечивает доступ к основным функциям ПТ ВЦ.

Главное меню содержит разделы для перехода к страницам системы. Если раздел объединяет несколько страниц системы, то у него есть меню.

Выбирая пункт, вы переходите на нужную страницу раздела.

Состав панели инструментов и содержимое рабочей области зависит от страницы.

Также главное меню содержит раздел **<Имя пользователя>**, кнопку ≡, по которой вы можете переходить из системы в сервис управления пользователями и доступом PT IAM и из этого сервиса в систему.

Раздел **<Имя пользователя>** расположен в правой части главного меню и позволяет выйти из ПТ ВЦ.

4.2. Панель инструментов

Панель инструментов расположена в верхней части страницы под главным меню.

Панель инструментов содержит кнопки. С их помощью вы можете выполнять действия с данными, представленными в рабочей области.

Кнопки могут иметь раскрывающееся меню, объединяющее группу пунктов.

4.3. Рабочая область

Рабочая область расположена на странице под панелью инструментов.

Рабочая область отображает различную информацию о работе системы одним из следующих способов:

- В виде списка. Например, информация о самых опасных уязвимостях отображается в виде списка. Списки бывают обычные и иерархические. Содержимое некоторых списков вы можете фильтровать.
- В виде таблицы. Например, информация о событиях отображается в виде таблицы. Рабочая область может содержать таблицы, в которых вы можете настраивать состав колонок, а также сортировать, группировать и фильтровать записи в таблице.
- В графическом виде. Например, история актива отображается в виде графика. Вы можете настраивать состав информации, представляемой на графике.

Для дополнительной группировки информации в рабочей области предусмотрены вкладки.

Также рабочая область может содержать инструменты, позволяющие настраивать представление информации в рабочей области: панель группировки, панель фильтрации.

В ПТ ВЦ предусмотрены системные группировки и фильтры. Вы можете создавать собственные группировки и фильтры.

5. Представление статистических данных в ПТ ВЦ: дашборды и виджеты

Домашняя страница обеспечивает доступ к основным статистическим данным ПТ ВЦ. Она содержит системный дашборд **Домашняя страница**.

Для работы со статистической информацией на домашней странице системы вам предоставляются следующие возможности:

1. Просмотр статистической информации на дашбордах.

   Вы можете просматривать статистические данные, представляемые на дашбордах. Виджеты отображают информацию об активах, уязвимостях, объектах, субъектах и инцидентах. При выборе элементов виджетов (например, диаграммы или ее части) открывается страница веб-интерфейса системы с подробной информацией. Информация на виджетах обновляется автоматически (по умолчанию каждые 15 минут).

2. Настройка виджетов. Вы можете настраивать виджеты. Вы можете настраивать период времени, за который вам требуется просматривать информацию. По умолчанию отображается информация за последние 30 дней.

   Примечание. Вы не можете менять состав и расположение виджетов системного дашборда **Домашняя страница**.

В этом разделе

- Работа со статистическими данными (см. раздел 5.1)
- Просмотр статистических данных (см. раздел 5.2)
- Настройка виджета (см. раздел 5.3)

5.1. Работа со статистическими данными

На дашборде расположены виджеты со статистическими данными, представляемыми:

- в виде количественного показателя;
- таблицы;
- диаграммы с распределением данных во времени.

Виджеты отображают информацию об активах, уязвимостях, субъектах, объектах и инцидентах. Например, системный дашборд **Домашняя страница** содержит предустановленные виджеты, приведенные в таблице ниже.

Таблица 2. Виджеты на системном дашборде Домашняя страница

Название виджета	Тип виджета	Описание информации
Количество субъектов	Индикатор	Количество заведенных в системе субъектов
Количество объектов	Индикатор	Количество заведенных в системе объектов
Количество активов	Индикатор	Количество заведенных в системе активов
Количество инцидентов	Индикатор	Количество созданных в системе инцидентов
Количество закрытых инцидентов	Индикатор	Количество инцидентов со статусом "Закрыт"
Количество открытых инцидентов	Индикатор	Количество инцидентов с любым статусом кроме "Закрыт"
Созданные инциденты	Временная диаграмма	Диаграмма распределения инцидентов по уровням опасности за период времени
Статус инцидентов	Временная диаграмма	Диаграмма распределения инцидентов по статусу за период времени
Топ-10 субъектов по количеству инцидентов	Список	Первые десять субъектов с наибольшим количеством инцидентов

Информация на виджетах обновляется автоматически каждые 15 минут.

5.2. Просмотр статистических данных

Для обеспечения информационной безопасности требуется всегда быть в курсе текущего состояния всей инфраструктуры организации. Вы можете просматривать статистические данные о состоянии инфраструктуры на дашборде.

► Чтобы просмотреть статистические данные:

1. В главном меню выберите раздел **Домашняя страница.**

   Откроется **Домашняя страница**.

2. Наведите курсор мыши на виджет **Созданные инциденты** или виджет **Статус инцидента**.

   Отобразится всплывающее сообщение, содержащее статистические данные.

Кроме того, на виджетах вы можете включать или отключать фильтры отображения данных. По умолчанию фильтры включены (отображаются все данные).

Существуют фильтры по уровню опасности инцидентов и статусу инцидентов. Этим фильтрам соответствуют кнопки: **Низкая**, **Средняя**, **Высокая критичность, Закрытые, Разрешенные, В работе, Уверждённые, Новые**. Подсвеченная кнопка означает, что фильтр включен.

► Чтобы отключить отображение информации определенного уровня важности,

нажмите кнопку фильтра.

Информация, соответствующая выбранному фильтру, не отображается на виджете.

5.3. Настройка виджета

По умолчанию виджет отображает статистические данные за последние 30 дней и обновляется каждые 15 минут. В процессе работы со статистическими данными, представленными на виджетах, вам может потребоваться настроить виджеты в соответствии с решаемыми задачами.

► Чтобы настроить виджет:

1. В главном меню выберите раздел **Домашняя страница.**

   Откроется **Домашняя страница**.

2. В панели инструментов виджета **Созданные инциденты** или виджета **Статус инцидентов** нажмите .

   Откроется панель настройки виджета.

3. В раскрывающемся списке **По группам** выберите группы активов, для которых требуется отображать статистические данные.

4. Выберите временной интервал, за который вы хотите просматривать статистические данные.

5. Выберите временной интервал диаграммы.

6. Нажмите , чтобы скрыть панель настройки виджета.

Виджет настроен.

6. Работа с субъектами

Субъект — юридическое лицо, самостоятельно создавшее информацию и (или) информационную систему либо получившее на основании договора право владения информацией и (или) информационной системой.

Всю информацию о субъектах вы можете просматривать на странице **Субъекты**. Страница **Субъекты** состоит из двух частей. В левой части представлен список субъектов. В правой части на вкладках **Реквизиты**, **Документы**, **Субъекты**, **Объекты**, **Комментарии**, **Оценка защищенности**, **Статистика атак** отображается подробная информация о выбранном субъекте.

На вкладке **Реквизиты** отображаются отрасль и тип субъекта, реквизиты (ИНН, КПП, ОГРН, ОКТМО) и адреса.

Вкладка **Документы** содержит данные о добавленных документах и перечень ответственных лиц с указанием их контактных данных.

Вкладка **Субъекты** содержит данные о родительском и дочернем субъекте.

Вкладка **Объекты** содержит данные о связанных с субъектом и эксплуатируемых объектах.

Вкладка **Комментарии** содержит поле для добавления комментариев.

На вкладке **Оценка защищенности** представлены таблицы с данными об уязвимостях информационных ресурсов.

На вкладке **Статистика атак** представлены таблицы с данными об атакуемых информационных ресурсах и источниках атак.

В этом разделе

- Создание субъекта (см. раздел 6.1)
- Просмотр информации о субъекте (см. раздел 6.2)
- Изменение параметров субъекта (см. раздел 6.3)
- Деактивация субъекта (см. раздел 6.4)

6.1. Создание субъекта

► Чтобы создать субъект:

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

   Откроется страница **Субъекты**.

2. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Новый субъект**.

3. В поле **Полное наименование организации** укажите полное наименование организации.

4. В поле **Отрасль** укажите отрасль субъекта.
5. В поле **Типы субъекта** укажите тип субъекта.
6. На вкладке **Реквизиты** в поле **ИНН** введите ИНН субъекта.
7. В поле **КПП** введите КПП субъекта.
8. В поле **ОКТМО** введите ОКТМО субъекта.
9. Нажмите кнопку **Сохранить**.

Субъект создан.

6.2. Просмотр информации о субъекте

► Чтобы просмотреть информацию о субъекте:

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

   Откроется страница **Субъекты**.
2. В левой панели выберите субъект.

Информация о субъекте отображается в правой панели.

6.3. Изменение параметров субъекта

► Чтобы изменить параметры субъекта:

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

   Откроется страница **Субъекты**.
2. В левой панели выберите субъект.
3. В панели инструментов нажмите кнопку **Редактировать**.

   Откроется окно **Редактирование субъекта**.
4. Измените необходимые параметры субъекта.

   Примечание. Вы не можете изменить полное наименование организации, ИНН и КПП.
5. Нажмите кнопку **Сохранить**.

Параметры субъекта изменены.

6.4. Деактивация субъекта

► Чтобы деактивировать субъект:

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

Откроется страница **Субъекты**.

2. В левой панели выберите субъект.
3. В панели инструментов нажмите кнопку **Деактивировать**.

Субъект деактивирован.

7. Работа с объектами

Объект — информационная система, находящаяся в зоне ответственности корпоративного сегмента ГосСОПКА, в отношении которой проводятся мероприятия по обнаружению, предупреждению и ликвидации последствий компьютерных атак.

Всю информацию об объектах вы можете просматривать на странице **Объекты**. Страница **Объекты** состоит из трех частей. В левой части представлены группы объектов. В центральной части отображаются объекты выбранной группы. В правой части на вкладках **Реквизиты**, **Ресурсы**, **Субъекты**, **Объекты**, **ГосСОПКА**, **Комментарии**, **Оценка защищенности**, **Статистика атак** отображается подробная информация о выбранном объекте.

На вкладке **Реквизиты** отображаются отрасль и тип объекта, реквизиты (ИНН, КПП, ОГРН, ОКТМО), адреса и вложенные документы.

Вкладка **Ресурсы** содержит данные об активах объекта, внутренних и внешних IP-адресах и доменах.

Вкладка **Субъекты** содержит данные о связанных с объектом субъектах.

Вкладка **Объекты** содержит данные о сопряжении с внешними информационными системами.

Вкладка **ГосСОПКА** содержит данные о компонентах и соглашениях.

Вкладка **Комментарии** содержит поле для добавления комментариев.

На вкладке **Оценка защищенности** представлены таблицы с данными об уязвимостях информационных ресурсов.

На вкладке **Статистика атак** представлены таблицы с данными об атакуемых информационных ресурсах и источниках атак.

В этом разделе

- Создание объекта (см. раздел 7.1)
- Просмотр информации об объекте (см. раздел 7.2)
- Изменение параметров объекта (см. раздел 7.3)
- Деактивация объекта (см. раздел 7.4)

7.1. Создание объекта

► Чтобы создать объект:

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

   Откроется страница **Объекты**.

2. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Новый объект**.

3. На вкладке **Реквизиты** в поле **Наименование объекта** укажите наименование объекта.
4. В поле **Категория** укажите категорию объекта.
5. В поле **Типы объекта** укажите тип объекта.
6. На вкладке **Обрабатываемая информация** укажите тип обрабатываемой информации.
7. На вкладке **Субъекты** в поле **Субъект-эксплуатант** укажите субъект.
8. Нажмите кнопку **Сохранить**.

Объект создан.

7.2. Просмотр информации об объекте

► Чтобы просмотреть информацию об объекте:

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

   Откроется страница **Объекты**.
2. В левой панели выберите группу объектов.
3. В центральной панели выберите объект.

В правой панели отображается информация об объекте.

7.3. Изменение параметров объекта

► Чтобы изменить параметры объекта:

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

   Откроется страница **Объекты**.
2. В левой панели выберите группу объектов.
3. В центральной панели выберите объект.
4. В панели инструментов нажмите кнопку **Редактировать**.

   Откроется окно **Редактирование объекта**.
5. Измените необходимые параметры объекта.

   Примечание. Вы не можете изменить наименование объекта.
6. Нажмите кнопку **Сохранить**.

Параметры объекта изменены.

7.4. Деактивация объекта

► Чтобы деактивировать объект:

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

   Откроется страница **Объекты**.
2. В левой панели выберите группу объектов.
3. В центральной панели выберите объект.
4. В панели инструментов нажмите кнопку **Деактивировать**.

Объект деактивирован.

8. Работа с активами

Работа с системой начинается со сбора сведений об активах. Это позволяет получить представление об информационной инфраструктуре компании.

Актив в ПТ ВЦ — базовая единица, которая представляет собой сканируемый сетевой узел. Сведения, собранные об активе, составляют модель актива.

При сборе и анализе событий, сетевом и системном сканировании система обнаруживает актив и создает о нем запись. Вы также можете добавлять и удалять активы вручную.

Страница **Активы** состоит из трех частей. В левой части представлены группы активов и фильтры. Фильтры позволяют выполнять поиск активов по определенным параметрам. Центральная часть окна представляет список активов, входящих в выбранную группу. Левую и центральную части можно скрыть или отобразить при необходимости. В правой части отображается подробная информация о выбранном активе.

Вы можете просматривать историю актива на графике. График показывает изменения на активе и может содержать до трех параметров. Набор параметров зависит от действий, которые производились над активом:

- Интегральная уязвимость — оценка уязвимости актива по системе CVSS. Этот параметр присутствует на графике всегда.
- Ручной ввод — изменения конфигурации актива, внесенные вручную.
- События — изменения конфигурации актива в результате событий на активе.

По умолчанию на графике отображается изменение состояния актива за последние 7 дней.

Подробная информация об активе отображается на вкладках под графиком.

На вкладке **Сводка** отображаются описание актива, краткая информация об аппаратном и программном обеспечении актива и сетевая конфигурация.

Вкладка **Уязвимости** содержит подробную информацию об уязвимостях актива с указанием оценки уязвимости по системе CVSS и идентификатора CVE.

Вкладка **Конфигурация** содержит подробную информацию об аппаратном и программном обеспечении актива.

На вкладке **Метрики CVSS** отображаются контекстные метрики CVSS и значимость актива. Установленные значения задаются пользователем при настройке паспорта актива. Эффективные значения определяются автоматически и являются максимальными для данной метрики из всех установленных значений (для актива и групп, в которые входит актив).

В верхней части панели состояния актива имеется указатель значимости актива. Эта метрика является функцией от эффективных значений метрик "Требования к доступности", "Требования к конфиденциальности", "Требования к целостности".

Метрика значимости может принимать следующие значения:

- не определена;
- низкая;

- средняя;
- высокая.

Числовая оценка для эффективных значений метрики (если они определены) следующая:

- низкая — 1;
- средняя — 3;
- высокая — 5.

Если определено хотя бы одно эффективное значение метрик актива "Требования к доступности", "Требования к конфиденциальности", "Требования к целостности", то суммируются числовые оценки эффективных значений. Значимость актива или группы активов вычисляется в соответствии с таблицей ниже в зависимости:

- от суммы эффективных значений метрик для актива или группы;
- количества определенных эффективных значений метрик "Требования к доступности", "Требования к конфиденциальности", "Требования к целостности" актива.

Таблица 3. Значения метрики значимости

Значимость актива	Количество определенных эффективных значений		
Низкая	3, 5	2	1
Средняя	7, 9, 11	4, 6	3
Высокая	13, 15	8, 10	5

Метрика значимости в правилах корреляции задается с помощью параметра AI. Вызов параметра может быть следующий data.Env.AI. Возможные значения параметра: «High», «Medium», «Low», «Not defined». Пример задания условия для метрики значимости:

```
data.Env.AI == "High"
```

В этом разделе

- Добавление актива (см. раздел 8.1)
- Просмотр информации об активе (см. раздел 8.2)
- Изменение данных паспорта актива (см. раздел 8.3)
- Изменение ОС и ПО актива (см. раздел 8.4)
- Выпуск отчета по активам (см. раздел 8.5)

8.1. Добавление актива

► Чтобы добавить актив:

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

Откроется страница **Активы**.

2. В панели инструментов нажмите кнопку **Актив** и в раскрывшемся меню выберите пункт **Добавить актив**.

   Откроется окно **Новый актив**.

3. В поле **Расположение** укажите расположение актива.
4. В поле **IP-адрес** введите IP-адрес актива.
5. Нажмите кнопку **Сохранить**.

   Откроется вкладка **Операционная система**.

6. В поле **ОС** укажите операционную систему.
7. В поле **OsName** укажите название операционной системы.
8. Нажмите кнопку **Сохранить**.

   Откроется вкладка **Программное обеспечение**.

9. Если требуется, в поле **Добавить ПО** укажите дополнительное программное обеспечение.
10. Нажмите кнопку **Сохранить**.

Актив добавлен в указанную группу активов.

8.2. Просмотр информации об активе

► Чтобы просмотреть информацию об активе:

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

   Откроется страница **Активы**.

2. В левой панели выберите группу, в которой расположен актив.

   Примечание. Вы можете фильтровать активы по группам по кнопке в случае масштабной инфраструктуры.

3. В центральной панели выберите актив.

   Примечание. Вы можете задать условие в строке поиска для быстрого поиска актива по названию, IP-адресу или FQDN.

4. Если требуется, измените временной интервал по кнопке .

8.3. Изменение данных паспорта актива

► Чтобы изменить данные паспорта актива:

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

Откроется страница **Активы**.

2. В левой панели выберите группу, в которой расположен актив.
3. В центральной панели выберите актив.
4. В панели инструментов нажмите кнопку **Актив** и в раскрывшемся меню выберите пункт **Редактировать паспорт**.

   Откроется окно **Редактирование актива <Название актива>**.
5. Измените необходимые данные.
6. Нажмите кнопку **Сохранить**.

Данные паспорта актива изменены.

8.4. Изменение ОС и ПО актива

► Чтобы изменить ОС и ПО актива:

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

   Откроется страница **Активы**.
2. В левой панели выберите группу, в которой расположен актив.
3. В центральной панели выберите актив.
4. В панели инструментов нажмите кнопку **Актив** и в раскрывшемся меню выберите пункт **Изменить ОС и ПО**.

   Откроется окно **Редактирование ОС и ПО актива <Название актива>**.
5. Наведите курсор на строку и нажмите появившуюся справа кнопку .
6. Измените необходимые данные.
7. Если требуется удалить ПО, нажмите кнопку .
8. Если требуется добавить ПО, в поле **Добавить ПО** укажите ПО.
9. Нажмите кнопку **Сохранить**.

ОС и ПО актива изменены.

8.5. Выпуск отчета по активам

► Чтобы выпустить отчет по активам:

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

   Откроется страница **Активы**.
2. Нажмите кнопку **Выпустить отчет**.

   Откроется окно **Выпуск отчета**.

3. В раскрывающемся списке **Отчет** выберите шаблон отчета.
4. Нажмите кнопку **Выпустить**.

Отчет сформирован и сохранен на вашем компьютере.

9. Работа с инцидентами

В контексте информационной безопасности управлением инцидентами называются мониторинг и обнаружение событий безопасности в системе, а также надлежащее реагирование на эти события. Целью управления инцидентами является формирование предсказуемого и адекватного ответа на события, которые могут приводить к ущербу.

Вы можете создавать задачи по инцидентам и составлять набор мер, которые следует принять по конкретному инциденту.

Страница **Инциденты** состоит из трех частей. В левой части представлены группы активов, к которым привязаны инциденты и фильтры. Фильтры позволяют выполнять поиск инцидентов по определенным параметрам. В правой части отображается подробная информация о выбранном инциденте. Левую и правую части можно скрыть или отобразить при необходимости. Центральная часть окна представляет список инцидентов, входящих в выбранную группу.

Для каждого инцидента указан набор параметров, включая уровень опасности, который в списке инцидентов определяет цвет строки (красный — высокий, желтый — средний и белый — низкий).

Существуют следующие статусы инцидентов: новый, утвержден, в работе, разрешен, закрыт.

В этом разделе

- Создание инцидента (см. раздел 9.1)
- Просмотр карточки инцидента (см. раздел 9.2)
- Изменение параметров инцидента (см. раздел 9.3)
- Изменение статуса инцидента (см. раздел 9.4)
- Создание задачи по инциденту (см. раздел 9.5)
- Фильтрация инцидентов (см. раздел 9.6)
- Создание пользовательского фильтра по инцидентам (см. раздел 9.7)
- Создание папки фильтров по инцидентам (см. раздел 9.8)
- Ручное и автоматическое обновлений списка инцидентов (см. раздел 9.9)
- Импорт инцидентов (см. раздел 9.10)
- Экспорт инцидентов (см. раздел 9.11)
- Выпуск отчета по инцидентам (см. раздел 9.12)

9.1. Создание инцидента

► Чтобы создать инцидент:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

Откроется страница **Инциденты**.

2. В левой панели выберите группу активов, в которой вы хотите создать инцидент.
3. В панели инструментов нажмите кнопку **Создать** и заполните форму в открывшемся окне:

   • **Название**: название инцидента (поле **Название** является обязательным);

   • **Описание**: подробное текстовое описание инцидента с необходимой для его обработки информацией;

   • **Расположение**: группа активов, в которой следует расположить инцидент;

   • **Обнаружен**: дата и время обнаружения инцидента;

   • **Категория и тип**: выберите категорию и тип инцидента из списка;

   • **Влияние**: значение, определяющее, какие последствия вызывает инцидент;

   • **Критичность**: степень опасности инцидента;

   • **Ответственный**: пользователь системы, который назначается ответственным за расследование инцидента;

   • **Активы и сети**: группа полей для активов, сетей и сетевых адресов, где зафиксирован инцидент;

   • **Атакующие активы**: группа полей для активов, сетей и сетевых адресов, с которых осуществляется атака.
4. Нажмите кнопку **Сохранить**.

Инцидент с указанными в форме данными создан. По окончании создания инцидента открывается карточка инцидента.

9.2. Просмотр карточки инцидента

► Чтобы просмотреть карточку инцидента:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница **Инциденты**.
2. Откройте карточку инцидента по ссылке с названием инцидента.

9.3. Изменение параметров инцидента

► Чтобы изменить параметры инцидента:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница **Инциденты**.
2. Выберите инцидент из списка.
3. В панели инструментов нажмите кнопку **Редактировать**.

Откроется окно, содержащее список параметров, указанных при создании инцидента.

4. Измените необходимые параметры инцидента.
5. Нажмите кнопку **Сохранить**.

Параметры инцидента изменены.

9.4. Изменение статуса инцидента

В системе существуют следующие статусы инцидентов:

- "Новый" — первичный статус при создании инцидента.
- "Утвержден" — инцидент, по которому должна проводиться работа.
- "В работе" — инцидент, по которому началась работа.
- "Разрешен" — инцидент, по которому завершена работа.
- "Закрыт" — инцидент, в отношении которого подтверждено завершение работы. Инцидент может быть закрыт успешно или по невозможности найти решение. Вы не можете изменить статус закрытого инцидента.

► Чтобы изменить статус инцидента:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница **Инциденты**.
2. По ссылке с названием инцидента перейдите в карточку инцидента.
3. В панели инструментов нажмите кнопку **Изменить статус**.

   Откроется окно **Сменить статус инцидента <Название инцидента>**.
4. В раскрывающемся списке **<Статус>** выберите статус.
5. Если требуется, в поле **Комментарий** укажите причину смены статуса.
6. Нажмите кнопку **Сменить статус**.

Статус инцидента изменен.

9.5. Создание задачи по инциденту

Задачи создаются для реагирования на инциденты (расследования, сбора доказательств, восстановления). Вы можете создавать несколько задач для каждого инцидента.

► Чтобы создать задачу по инциденту:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница **Инциденты**.
2. По ссылке с названием инцидента перейдите в карточку инцидента.

3. На вкладке **Задачи** нажмите кнопку **Поставить задачу**.
4. В поле **Название** укажите название задачи.
5. В раскрывающемся списке **Тип** выберите тип задачи.
6. Если требуется, в поле **Дедлайн** укажите срок выполнения задачи.
7. В раскрывающемся списке **Ответственный** выберите ответственного за выполнение задачи.
8. Если требуется, в поле **Описание** введите текстовое описание задачи.
9. Нажмите кнопку **Сохранить**.

Задача по инциденту создана.

Все задачи, относящиеся к инциденту, отображаются в карточке инцидента.

9.6. Фильтрация инцидентов

Вы можете фильтровать инциденты для удобства анализа системы.

Вы можете отобразить инциденты:

- связанные с выбранной группой активов;
- произошедшие в выбранный период;
- находящиеся в одном статусе (например, закрытые);
- отвечающие условиям системных и пользовательских фильтров;
- отвечающие условиям запроса на языке PDQL.

По умолчанию на странице **Инциденты** в рабочей области отображаются все незакрытые инциденты, созданные за последнюю неделю.

В этом разделе

- Фильтрация инцидентов по группе активов (см. раздел 9.6.1)
- Фильтрация инцидентов с помощью системных или пользовательских фильтров (см. раздел 9.6.2)
- Фильтрация инцидентов с помощью PDQL-запроса (см. раздел 9.6.3)
- Фильтрация инцидентов по статусу (см. раздел 9.6.4)

9.6.1. Фильтрация инцидентов по группе активов

В инцидентах участвуют активы, входящие в системные и пользовательские группы активов. Вы можете фильтровать инциденты по принадлежности к группам активов. Иерархический список групп активов отображается на странице **Инциденты** в панели **Инциденты**.

► Чтобы отфильтровать инциденты в таблице инцидентов по группе активов:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница **Инциденты**.

2. Если необходимо, настройте отображение групп активов требуемого типа в панели **Инциденты** по кнопке .

3. В панели **Инциденты** выберите группу активов.

   Название группы активов отобразится над таблицей инцидентов.

   В таблице отобразятся инциденты, произошедшие на активах из выбранной группы и вложенных в нее.

4. По умолчанию отображаются инциденты из вложенных групп. Если требуется скрыть инциденты из вложенных групп, в панели **Инциденты** по кнопке под раскрывающимся списком **Типы групп** снимите флажок **Показывать инциденты из вложенных групп**.

   В таблице не будут отображаться инциденты из вложенных групп.

9.6.2. Фильтрация инцидентов с помощью системных или пользовательских фильтров

Вы можете использовать системные или сохраненные пользовательские фильтры, чтобы фильтровать инциденты в таблице инцидентов. Иерархический список фильтров отображается на странице **Инциденты** в панели **Фильтры**.

► Чтобы отфильтровать инциденты в таблице инцидентов с помощью системного или пользовательского фильтра:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница **Инциденты**.

2. В панели **Фильтры** выберите фильтр.

   Название фильтра отобразится над списком инцидентов.

   Примечание. Вы можете отфильтровать список инцидентов только по одному фильтру из списка.

   В таблице отобразятся инциденты, удовлетворяющие условиям фильтрации.

9.6.3. Фильтрация инцидентов с помощью PDQL-запроса

Вы можете фильтровать инциденты с помощью PDQL-запросов. Запросы можно создавать из атрибутов инцидента или вручную.

► Чтобы отфильтровать инциденты по атрибутам инцидента:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница **Инциденты**.

2. В таблице инцидентов или в карточке инцидента по ссылке с подчеркиванием выберите атрибут инцидента (например, статус инцидента).

3. Во всплывающем окне выберите условие фильтрации.

Инциденты в таблице будут отфильтрованы в соответствии с выбранными условиями.

Вы также можете указать PDQL-запрос для фильтрации инцидентов вручную.

► Чтобы отфильтровать инциденты с помощью PDQL-запроса:

1. Над таблицей инцидентов нажмите **<Название фильтра инцидентов>**.

   Откроется всплывающее окно с PDQL-запросом.

2. В поле **WHERE** введите запрос на языке PDQL.

Инциденты в таблице будут отфильтрованы в соответствии с условиями PDQL-запроса.

9.6.4. Фильтрация инцидентов по статусу

► Чтобы отфильтровать инциденты по статусу:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница **Инциденты**.

2. Над таблицей инцидентов в раскрывающемся списке выберите статус инцидентов.

В таблице инцидентов отобразятся инциденты с выбранным статусом.

9.7. Создание пользовательского фильтра по инцидентам

Вы можете создавать пользовательские фильтры по инцидентам с указанием условий фильтрации.

► Чтобы создать пользовательский фильтр по инцидентам:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница **Инциденты**.

2. В панели **Инциденты** выберите группу активов.

3. В таблице инцидентов или в карточке инцидента по ссылке с подчеркиванием выберите атрибут инцидента (например, статус инцидента).

4. Во всплывающем окне выберите условие фильтрации.

   Примечание. Вы можете выбрать несколько условий фильтрации.

5. Нажмите ссылку с PDQL-запросом.

   Откроется всплывающее окно с PDQL-запросом.

   Примечание. Вы также можете указать запрос для фильтрации инцидентов вручную.

6. Нажмите кнопку **Сохранить**.

   Откроется окно **Новый фильтр**.

7. В поле **Название** укажите название фильтра.
8. В поле **Папка** укажите папку, в которой будет сохранен фильтр.
9. Нажмите кнопку **Сохранить**.

Пользовательский фильтр по инцидентам создан.

9.8. Создание папки фильтров по инцидентам

Вы можете создавать папки фильтров, чтобы группировать пользовательские фильтры по инцидентам.

► Чтобы создать папку фильтров по инцидентам:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница **Инциденты**.

2. В панели **Фильтры** нажмите + .

   Откроется окно **Новая папка фильтров**.

3. В поле **Название** укажите название папки.
4. В раскрывающемся списке **Внутри папки** выберите расположение папки.

5. Нажмите кнопку **Создать**.

Папка фильтров по инцидентам создана.

9.9. Ручное и автоматическое обновлений списка инцидентов

► Чтобы обновить список инцидентов:

1. Нажмите кнопку C для обновления списка вручную.
2. Установите флажок **Обновлять** на панели сверху и выберите желаемый период обновления для автоматического обновления.

9.10. Импорт инцидентов

Вы можете импортировать в ПТ ВЦ инциденты в унифицированном формате обмена.

► Чтобы импортировать инциденты:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница **Инциденты**.

2. В панели инструментов нажмите кнопку **Импорт**.

   Откроется окно **Импорт инцидентов**.

3. В поле **Расположение** выберите группы активов, где необходимо расположить инциденты.

4. Если требуется, снимите флажок **перезаписать существующие инциденты**.

   Примечание. Если флажок снят, инциденты с совпадающим идентификатором (параметром identification.source.id), экспортированные из разных систем, будут пропущены при импорте.

5. Загрузите файл с инцидентами, перетащив его на поле либо нажав **выбрать**.

   Примечание. Если формат импортируемого файла инцидентов отличается от JSON или содержимое файла некорректно, то ПТ ВЦотобразит в поле **Результат** и вверху окна импорта ошибку валидации. Кнопка **Импортировать** будет недоступна до удаления невалидных файлов. Максимальный объем одного импортируемого файла 512 МБ.

6. После успешной валидации загруженных файлов нажмите кнопку **Импортировать**.

Инциденты импортированы.

По окончании импорта открывается окно с результатами, содержащее записи о каждом импортированном файле, включая результат импорта и количество импортированных инцидентов. В случае возникновения ошибки при импорте инцидентов такие инциденты пропускаются. В поле **Импортировано инцидентов** отображается количество успешно импортированных инцидентов и общее количество инцидентов в файле. В нижней части окна отображается общий итог импорта: количество импортированных файлов, количество импортированных и пропущенных инцидентов.

После нажатия кнопки **Закрыть** вы перейдете в окно со списком импортированных инцидентов по фильтру **Импортированные из файла**. Общий фильтр для всех импортируемых инцидентов — **Инциденты по источнику импорта**.

Для импортированных инцидентов в поле **Источник** отображается значок .

9.11. Экспорт инцидентов

Вы можете экспортировать инциденты в унифицированном формате обмена для последующего их импорта в другие системы.

Примечание. В один файл можно экспортировать не более 10 000 инцидентов. Если вы выбрали более 10 000 инцидентов, то будут экспортированы первые 10 000 инцидентов.

► Чтобы экспортировать инциденты:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница **Инциденты**.

2. При необходимости выберите отдельные инциденты, удерживая нажатой клавишу Ctrl.

   Примечание. Вы также можете отфильтровать инциденты.

3. В панели инструментов нажмите кнопку **Экспорт**.

   Откроется окно экспорта инцидентов.

4. Выберите один из вариантов: все инциденты или только выбранные инциденты.
5. Нажмите кнопку **Экспортировать**.

Инциденты экспортированы. По окончании экспорта открывается окно загрузки созданного системой файла. Инциденты экспортируются в формате JSON.

9.12. Выпуск отчета по инцидентам

Отчеты по инцидентам используются для отображения статистики работы с инцидентами.

► Чтобы выпустить отчет по инцидентам:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница **Инциденты**.

2. Нажмите кнопку **Выпустить отчет**.

   Откроется окно **Выпуск отчета**.

3. В раскрывающемся списке **Отчет** выберите шаблон отчета.
4. В раскрывающемся списке **Период** выберите временной интервал.
5. Нажмите кнопку **Выпустить**.

Отчет сформирован и сохранен браузером на вашем компьютере.

10. Работа со справочниками

Справочники предназначены для хранения значений классифицируемых параметров описания субъектов, объектов и мероприятий, а также общих параметров. Справочники содержат значения для следующих параметров сущностей:

- субъекты:
  - форма юридического лица;
  - типы субъектов и их ответственности;
  - форма юридического лица;
- объекты:
  - виды услуг;
  - категории объектов;
  - типы объектов;
  - типы каналов;
  - типы компонентов;
  - типы обрабатываемой информации;
  - типы сопряжений с внешними ИС;
- общие:
  - адреса;
  - категории ответственных лиц;
  - ответственные лица;
  - страны;
  - типы документов.

Существуют системные и пользовательские справочники. Системные справочники поставляются вместе с ПТ ВЦ. Вы не можете редактировать системные справочники. К пользовательским справочникам относятся справочники "Ответственные лица" и "Адреса". Вы можете редактировать пользовательские справочники.

Страница **Справочники** состоит из трех частей. В левой части представлены группы сущностей, к которым привязаны справочники. Центральная часть окна представляет список значений параметров, входящих в выбранную группу. В правой части отображается подробная информация о выбранном значении параметра. Левую и правую части можно скрыть или отобразить при необходимости.

В этом разделе

- Работа со справочником "Ответственные лица" (см. раздел 10.1)

10.1. Работа со справочником "Ответственные лица"

Справочник "Ответственные лица" содержит персональную информацию о лицах, ответственных за расследование инцидентов.

В этом разделе

- Добавление записи об ответственном лице (см. раздел 10.1.1)
- Изменение информации об ответственном лице (см. раздел 10.1.2)
- Удаление записи об ответственном лице (см. раздел 10.1.3)

10.1.1. Добавление записи об ответственном лице

► Чтобы добавить запись об ответственном лице в справочник:

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

   Откроется страница **Справочники**.
2. В левой панели выберите справочник "Ответственные лица".
3. В панели инструментов нажмите кнопку **Добавить**.

   Откроется окно **Добавить запись**.
4. В поле **Фамилия** введите фамилию ответственного лица.
5. В поле **Имя** введите имя ответственного лица.
6. В поле **Отчество** введите отчество ответственного лица.
7. Если требуется, укажите дополнительную информацию об ответственном лице.
8. Нажмите кнопку **Сохранить**.
9. Запись об ответственном лице добавлена в справочник "Ответственные лица".

10.1.2. Изменение информации об ответственном лице

► Чтобы изменить информацию об ответственном лице:

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

   Откроется страница **Справочники**.
2. В левой панели выберите справочник **Ответственные лица**.
3. В центральной части окна выберите ответственное лицо.
4. Нажмите кнопку **Редактировать**.

   Откроется окно **Редактировать запись <Наименование записи>**.

5. Измените информацию об ответственном лице.
6. Нажмите кнопку **Сохранить**.

Информация об ответственном лице изменена.

10.1.3. Удаление записи об ответственном лице

► Чтобы удалить запись об ответственном лице из справочника:

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

   Откроется страница **Справочники**.
2. В левой панели выберите справочник "Ответственные лица".
3. В центральной части окна выберите ответственное лицо.
4. Нажмите кнопку **Удалить**.

   Примечание. Вы не можете удалить запись об ответственном лице, если оно назначено ответственным за расследование инцидента или выполнение задачи.

Запись об ответственном лице удалена из справочника.

11. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;
- диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;
- разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;
- устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале support.ptsecurity.com или по телефону. Заявки на портале — основной способ обращений за технической поддержкой.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

- Техническая поддержка на портале (см. раздел 11.1)
- Техническая поддержка по телефону (см. раздел 11.2)
- Время работы технической поддержки (см. раздел 11.3)
- Как служба технической поддержки работает с заявками (см. раздел 11.4)

11.1. Техническая поддержка на портале

Портал support.ptsecurity.com предоставляет вам возможность создавать заявки на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

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

Портал технической поддержки доступен на русском, английском, немецком и итальянском языках.

11.2. Техническая поддержка по телефону

Вы можете связаться со службой технической поддержки по следующим телефонам:

- Великобритания +44 20 3769 3606.
- США +1 857 208 7273.
- Италия +39 0 697631532.
- Швеция +46 8 121 111 86.
- Южная Корея +82 264 108 582.
- Россия +7 495 744 01 44.

Техническая поддержка по телефону предоставляется на русском и английском языке.

Сотрудники технической поддержки по телефону могут выполнить оперативную диагностику, ответить на простые вопросы или уточнить текущий статус работ по ранее созданной заявке.

Если решить вопрос по телефону в разумное время (15—20 минут) невозможно, создайте заявку на портале support.ptsecurity.com. Заявка на портале, созданная и обновляемая по рекомендациям специалиста технической поддержки, гарантирует дальнейшие работы по вашему обращению.

11.3. Время работы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять заявки, читать новости продуктов и пользоваться базой знаний. Сотрудники технической поддержки работают по имеющимся заявкам и принимают обращения по телефону с понедельника по пятницу с 9:00 до 19:00 UTC+3.

11.4. Как служба технической поддержки работает с заявками

При получении вашей заявки специалист службы технической поддержки классифицирует инцидент, указанный в заявке (присваивает инциденту тип и уровень значимости) и выполняет дальнейшие шаги по разрешению инцидента.

В этом разделе

- Предоставление информации для технической поддержки (см. раздел 11.4.1)
- Типы инцидентов (см. раздел 11.4.2)
- Время реакции на обращение и приоритизация инцидентов (см. раздел 11.4.3)
- Выполнение работ по заявке (см. раздел 11.4.4)

11.4.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста "Позитив Текнолоджиз" нужно предоставить:

- номер лицензии на использование продукта;
- файлы журналов и другие наборы диагностических данных, хранящихся в продукте;
- снимки экрана;
- результаты выполнения рекомендаций специалиста технической поддержки;
- каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

"Позитив Текнолоджиз" не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть заявку.

11.4.2. Типы инцидентов

Специалист технической поддержки относит инцидент в вашей заявке к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист "Позитив Текнолоджиз" оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате

продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). "Позитив Текнолоджиз" не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

"Позитив Текнолоджиз" поставляет пакеты обновления продукта в течение срока действия лицензии на продукт.

"Позитив Текнолоджиз" не несет ответственности за инциденты, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, "Позитив Текнолоджиз" обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

11.4.3. Время реакции на обращение и приоритизация инцидентов

Время реакции на ваше обращение рассчитывается как время с момента получения от вас информации по обращению до ответа специалиста технической поддержки с описанием дальнейших шагов по разрешению инцидента. Время реакции зависит от указанного вами уровня значимости инцидента (см. таблицу 4).

Время решения инцидента рассчитывается как время с момента регистрации обращения до ответа специалиста технической поддержки, ведущего к одному из вариантов решения инцидента (см. раздел 11.4.4).

Специалист технической поддержки может переопределять уровень значимости инцидента по приведенным ниже критериям. Значения сроков являются целевыми и подразумевают стремление и разумные усилия специалистов "Позитив Текнолоджиз" для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 4. Время реакции технической поддержки на обращение и решения инцидента

Уровень значимости инцидента	Критерии значимости инцидента	Время реакции на обращение по инциденту	Время решения инцидента
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку)	До 2 часов	До 2 рабочих дней

Уровень значимости инцидента	Критерии значимости инцидента	Время реакции на обращение по инциденту	Время решения инцидента
	либо оказывающие критическое влияние на бизнес		
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 4 часов	До 3 рабочих дней
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительное влияние на бизнес	До 8 часов	До 6 рабочих дней
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	До 10 рабочих дней

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки обращений).

11.4.4. Выполнение работ по заявке

По мере выполнения работ по вашей заявке специалист технической поддержки сообщает вам:

- о диагностике инцидента и ее результатах,
- поиске решения или возможности обойти причины возникновения инцидента,
- планировании и выпуске обновления продукта (если требуется для разрешения инцидента).

Если по итогам решения инцидента необходимо внести изменения в продукт, "Позитив Текнолоджиз" включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по заявке считаются выполненными, если:

- предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;
- инцидент диагностирован как дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- инцидент идентифицирован как вызванный программными продуктами или оборудованием сторонних производителей и не подпадающий под гарантийные обязательства по продукту;
- инцидент классифицирован как неподдерживаемый.

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