Positive Technologies Knowledge Base

Версия 19.0

Руководство пользователя

POSITIVE TECHNOLOGIES

Дата редакции документа: 09.11.2020

Содержание

1. О PT Knowledge Base

PT Knowledge Base (далее также — Knowledge Base) — это единая база знаний продуктов компании "Позитив Технолоджиз"). База знаний включает в себя данные, необходимые для структурирования сведений, собранных от объектов инфраструктуры (например, для определения версий ОС и ПО).

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).

В базе знаний реализована связь сущностей между собой. Например, на странице просмотра параметров ПО (карточке ПО) можно увидеть информацию о связанных с данным ПО уязвимостях и бюллетенях безопасности.

2. Архитектура Knowledge Base

Knowledge Base состоит из программных компонентов, которые вы можете размещать как на одном сервере, так и на нескольких. Такая структура обеспечивает масштабирование и позволяет внедрять систему в компаниях любого размера. Для высокопродуктивных систем рекомендуется распределенная установка.

В этом разделе

2.1. Компонент PT Management and Configuration

Компонент PT Management and Configuration (далее также — PT MC) обеспечивает:

- сервис единого входа в продукты "Позитив Текнолоджиз", развернутые в инфраструктуре организации;
- управление пользователями системы, включая создание учетных записей, назначение прав, блокирование и активацию учетных записей;
- доставку обновлений для компонентов Knowledge Base;
- журналирование действий пользователей.

В состав компонента входят следующие службы:

- Update and Configuration Service;
- MC Application Registration Management Service;
- MC Identity and Access Management Service;
- MC Notifications service;
- MC Tenant Manager Service;
- MC User Action Logging Service.

2.2. Компонент Knowledge Base

В состав компонента входят следующие службы:

- KB ApiGateway service;
- KB Candidates Service;
- KB Platform Registration Service;

— KB Portal service;

— KnowledgeBase service.

2.3. Компонент PT Update and Configuration Service

Компонент PT Update and Configuration Service (далее также — PT UCS) — это сервис онлайн-обновления компонентов Knowledge Base, установленных на серверах под управлением Microsoft Windows. PT UCS обеспечивает проверку наличия, загрузку и установку обновлений базы данных по уязвимостям.

Для доставки компонентам новых версий PT UCS использует ПО SaltStack: модуль Salt Master находится на сервере PT UCS, модуль Salt Minion — на серверах компонентов Knowledge Base. PT UCS получает новые версии компонентов с глобального сервера обновлений "Позитив Текнолоджиз" и с помощью модуля Salt Master отправляет их модулям Salt Minion для установки.

3. Аппаратные и программные требования

Программные требования

Поддерживаемые операционные системы для Knowledge Base и PT MC:

- Microsoft Windows Server 2012;
- Microsoft Windows Server 2012 R2;
- Microsoft Windows Server 2016;
- Microsoft Windows Server 2019.

Поддерживаемая операционная система для PT UCS — Debian 9.12, 9.13, 10.4 и 10.5.

Доступ к веб-интерфейсу Knowledge Base поддерживается в браузерах:

- Google Chrome 49 и выше с отключенным кэшированием и хранением cookies (можно использовать режим инкогнито);
- Mozilla Firefox 45 и выше.

Аппаратные требования

Таблица 1. Аппаратные требования к серверу Knowledge Base и PT MC

Центральный процессор	Сетевой адаптер	Память (ОЗУ)	Жесткие диски и свободное дисковое пространство
Тактовая частота 2,2 Гц, суммарно 4 логических ядра	1 порт со скоростью 1 Гбит/с	32 ГБ	SSD SATA, не менее 512 ГБ

Таблица 2. Аппаратные требования к серверу PT UCS

Центральный процессор	Сетевой адаптер	Память (ОЗУ)	Жесткие диски и свободное дисковое пространство
Тактовая частота 2,4 ГГц, суммарно 4 логических ядра	1 порт со скоростью 1 Гбит/с	4 ГБ	SSD SATA, не менее 400 ГБ

4. Установка Knowledge Base из инсталлятора

Установка продукт Knowledge Base включает в себя три шага:

- установку компонента PT MC;
- установку Knowledge Base;
- установку PT UCS (необязательно, требуется только для обновления контента серверов обновления "Позитив Текнолоджиз").

Установка компонента PT MC

► Чтобы установить компонент PT MC:

1. Запустите инсталлятор.
2. Следуйте шагам инсталлятора.

Компонент установлен.

Установка компонента Knowledge Base

Для установки компонента Knowledge Base требуются файлы:

- Ptkbsetup.<Номер версии продукта>.exe;
- packages\SnapshotData.VM.ptkb;
- packages\postgresql_<Номер версии PostgreSQL >.exe

► Чтобы установить компонент Knowledge Base:

1. Запустите инсталлятор с помощью команды:
```
ptkbsetup.<Номер версии продукта>.exe /variables
PARAMS="DeploymentType=vm;IdentityServerAddress=localhost;HostAddress=localhost"
```
2. Укажите значения параметров:

   для IdentityServerAddress укажите адрес узла, на котором установлен компонент PT MC;

   для HostAddress — адрес узла, на котором вы устанавливаете Knowledge Base.
3. Следуйте по шагам инсталлятора.

Компонент Knowledge Base установлен.

Установка и настройка компонента PT UCS

Компонент PT UCS может быть установлен только на отдельную машину с операционной системой Debian. Команды в интерфейсе терминала Debian необходимо выполнять от имени суперпользователя (root).

► Чтобы установить компонент PT UCS:

1. Распакуйте архив ucs-<Номер версии продукта>-debian<Номер версии Debian>.tar:
   ```
   tar -xf ucs-<Номер версии продукта>-debian<Номер версии Debian>.tar -C <Путь к каталогу для распаковки архива>
   ```
2. Запустите сценарий:
   ```
   <Путь к каталогу для распаковки архива>/<Продукт>-ucs-debian<Номер версии Debian>-<Номер версии продукта>/install.sh
   ```
   Откроется окно **UCS configuration**.
3. Выберите расширенный вариант параметров.

   Откроется страница со списком параметров.
4. Выберите продукты для обновления: KB VM DATA, KB BINARY.
5. Укажите значение параметра SaltMasterHost:
   ```
   SaltMasterHost: <IP-адрес или FQDN сервера компонента PT UCS>
   ```
6. Нажмите кнопку **Yes**.

   Запустится установка PT UCS. По завершении установки интерфейс терминала Debian отобразит сообщение:
   ```
   Done installing ucs-pt
   ```
7. Убедитесь, что порт 443/TCP открыт для исходящих соединений, порты 4505/TCP, 4506/TCP и 9035/TCP открыты для входящих соединений.
8. На серверах компонента Knowledge Base под управлением Microsoft Windows выполните команду:
   ```
   saltcfg set -p SaltMasterHost <IP-адрес или FQDN компонента PT UCS>
   ```
9. На сервере PT UCS выполните команду:
   ```
   salt-key -L
   ```
   Интерфейс терминала Debian в списке Unaccepted Keys отобразит FQDN серверов с неавторизованными модулями Salt Minion.
10. Авторизуйте модули Salt Minion:
    ```
    salt-key -a <FQDN сервера с модулем Salt Minion>
    ```

Компонент PT UCS установлен и настроен.

5. Вход в Knowledge Base через PT MC

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

Перед входом в Knowledge Base запросите у администратора PT MC:

— ссылку для входа в интерфейс продукта;

— тип учетной записи (локальная или доменная);

— логин и пароль вашей учетной записи пользователя.

Перед выполнением инструкции вам нужно убедиться, что в браузере разрешены всплывающие окна.

► Чтобы войти в Knowledge Base:

1. В адресной строке браузера введите ссылку для входа в интерфейс Knowledge Base.

   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 Knowledge Base длится 12 часов. Вы можете продлить сессию, установив флажок **Запомнить меня**: тогда она завершится только через 7 дней бездействия.

4. Нажмите кнопку **Войти**.

PT MC проверяет введенные вами учетные данные. Если вы указали верные данные, откроется стартовая страница со стандартным дашбордом Knowledge Base. Если вы указали неверные данные, отобразится сообщение об ошибке.

См. также

Пользователи и права доступа (см. раздел 6)

6. Пользователи и права доступа

В Knowledge Base реализована ролевая модель управления доступом. В общем случае пользователю могут быть назначены одна или несколько ролей. Каждая роль содержит набор привилегий, которые определяют доступные для пользователя разделы интерфейса и операции в системе.

При развертывании системы ее компоненты передают службе MC Identity and Access Management Service данные о доступных привилегиях и стандартных ролях. Роли и привилегии распределены по приложениям, которым соответствует определенный набор функций системы. Если пользователь имеет несколько ролей в приложении, права доступа суммируются. По умолчанию система содержит два приложения: Management and Configuration и Knowledge Base.

Приложение Management and Configuration предназначено для управления учетными записями и ролями пользователей во всех приложениях системы, а также для управления иерархией площадок и правилами репликации данных между ними. По умолчанию приложение содержит стандартные роли "Администратор" и "Пользователь".

Приложение Knowledge Base предназначено для работы с уязвимостями, эксплойтами, бюллетенями безопасности и сигнатурами. По умолчанию приложение содержит стандартную роль "Администратор".

Служба MC Identity and Access Management Service обеспечивает механизм единого входа (технология single sign-on), поэтому другие продукты "Позитив Текнолоджиз" в случае их интеграции с Knowledge Base также могут быть зарегистрованы службой, а их роли и привилегии будут доступны для назначения пользователям.

При развертывании Knowledge Base автоматически создается учетная запись (логин — `Administrator`, пароль — `P@ssw0rd`), имеющая все возможные стандартные роли. Эту учетную запись невозможно заблокировать, также невозможно изменить ее логин. После входа в систему рекомендуется сменить пароль этой учетной записи на более сложный.

Для обеспечения выполнения пользователем производственных задач необходимо:

1. Создать для пользователя учетную запись.
2. Если набор привилегий стандартных ролей не подходит для выполнения производственных задач — создать пользовательские роли с нужным набором привилегий.
3. Назначить пользователю необходимые роли.

В этом разделе

6.1. Управление учетными записями

Управление учетными записями различается в зависимости от типа аутентификации пользователей.

В случае локальной аутентификации необходимо вручную создавать учетные записи (см. раздел 6.1.3), аутентификация пользователей выполняется в РТ МС. Администратор указывает в приложении Management and Configuration логин, пароль, статус пользователя, персональную и организационную информацию, а также роли пользователя. Эти параметры доступны для изменения и хранятся только в РТ МС.

Для использования LDAP-аутентификации необходимо настроить LDAP-подключение (см. раздел 6.1.7) перед созданием учетных записей (см. раздел 6.1.3). Администратор указывает в приложении Management and Configuration логин, статус и роли пользователя. Пароль учетной записи хранится в Microsoft Active Directory и не может быть изменен в приложении Management and Configuration. Персональная и организационная информация по умолчанию загружается из Microsoft Active Directory, но может быть указана и изменена в приложении.

Учетная запись может автоматически создаваться в РТ МС при первом входе пользователя. Для этого необходимо настроить LDAP-подключение (см. раздел 6.1.7) и синхронизацию с Microsoft Active Directory (см. раздел 6.1.8). Логин, пароль, а также группы пользователя, соответствующие его ролям, хранятся в Microsoft Active Directory и не могут быть изменены в приложении Management and Configuration. Персональная и организационная информация также по умолчанию загружается из Microsoft Active Directory, но может быть указана и изменена в приложении.

Система может содержать учетные записи пользователей с разными типами аутентификации. Вы можете сменить пользователю тип аутентификации в системе.

В случае иерархической инсталляции в приложении Management and Configuration будут отображаться учетные записи пользователей других площадок. Вы можете сменить статус таких учетных записей на локальной площадке, а также, если эти учетные записи не синхронизируются с Microsoft Active Directory, назначить пользователям роли.

Список пользователей и назначенных им ролей приведен на странице **Пользователи**, список LDAP-подключений — на странице **Настройка LDAP-подключений**.

В этом разделе

6.1.1. Страница Пользователи

Страница **Пользователи** предназначена для работы с учетными записями пользователей. В панели инструментов страницы находятся следующие кнопки:

- **Добавить пользователя** — для создания учетной записи пользователя;
- **Изменить данные** — для изменения персональных данных пользователя и организационной информации;
- **Роли в приложениях** — для назначения пользователям ролей в приложениях;
- **Заблокировать** — для блокирования учетной записи пользователя;
- **Разблокировать** — для разблокирования учетной записи пользователя;
- **Экспорт** — для экспорта данных о пользователях в текстовый файл.

В рабочей области страницы расположены:

- Панель **Пользователи по приложениям**. Содержит список фильтров по приложениям и фильтр **Все пользователи**. При выборе приложения в панели **Пользователи <Название приложения>** отобразятся учетные записи пользователей, которым назначены роли в выбранном приложении, при выборе фильтра **Все пользователи** — все учетные записи, созданные в системе.
- Панель **Пользователи <Название приложения>**. Содержит таблицу с учетными записями и кнопки и . В таблице доступны выбор учетных записей, а также их сортировка по нажатию на название колонки. При нажатии в верхней части панели открывается поле для быстрого поиска учетной записи, при нажатии открывается панель для настройки фильтра учетных записей.
- Панель **<Логин пользователя>@<Домен> (Псевдоним площадки)**. Содержит данные о выбранной учетной записи пользователя, ссылки для просмотра его ролей и привилегий.

6.1.2. Страница Настройка LDAP-подключений

Страница **Настройка LDAP-подключений** предназначена для настройки подключения к LDAP-серверам. В панели инструментов страницы находятся следующие кнопки:

- **Добавить подключение** — для создания подключения;
- **Изменить параметры** — для изменения параметров подключения;

— **Удалить** — для удаления подключения;

— **Запустить синхронизацию** — для запуска вручную синхронизации с Microsoft Active Directory.

В рабочей области страницы расположены:

— Панель **Подключения**. Содержит таблицу с подключениями и кнопки и . В таблице доступны выбор подключения, а также сортировка подключений по нажатию на название колонки. При нажатии обновятся данные в таблице, при нажатии откроется блок параметров для настройки автоматического обновления данных. В таблице отображаются следующие статусы подключений:

— выполняется синхронизация с Microsoft Active Directory;

— синхронизация с Microsoft Active Directory завершилась с предупреждением;

— подключение к LDAP-серверам или синхронизация с Microsoft Active Directory завершились с ошибкой.

— Панель **<Название подключения>**. Содержит данные о выбранном подключении, а также сообщения о возникших ошибках и предупреждениях.

6.1.3. Создание учетной записи

Если аутентификация пользователя будет выполняться через LDAP, перед созданием учетной записи необходимо настроить этот тип аутентификации.

После создания учетная запись не может быть удалена. Если требуется запретить пользователю вход в систему, необходимо заблокировать его учетную запись (см. раздел 6.1.5).

► Чтобы создать учетную запись пользователя:

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

   Откроется страница **Пользователи**.

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

   Откроется страница **Новый пользователь**.

3. В блоке параметров **Учетные данные** выберите тип аутентификации.

4. Если вы выбрали локальную аутентификацию, введите логин и пароль пользователя.

   Примечание. Если требуется, чтобы пользователь сменил пароль при первом входе в систему, установите флажок.

5. Если вы выбрали LDAP-аутентификацию, введите доменное имя пользователя и по ссылке **Выбрать домен** выберите LDAP-подключение.
6. Нажмите кнопку **Создать**.

Учетная запись пользователя создана.

6.1.4. Изменение данных пользователя

► Чтобы изменить данные пользователя:

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

   Откроется страница **Пользователи**.
2. Выберите учетную запись пользователя, данные которого необходимо изменить.
3. В панели инструментов нажмите кнопку **Изменить данные**.

   Откроется страница **Изменение данных пользователя**.

   Откроется страница **Редактировать информацию о пользователе**.
4. Внесите необходимые изменения и нажмите кнопку **Сохранить**.

Данные пользователя изменены.

6.1.5. Блокирование и разблокирование учетной записи

► Чтобы заблокировать учетную запись:

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

   Откроется страница **Пользователи**.
2. В списке выберите пользователя, учетную запись которого необходимо заблокировать.

   Примечание. Вы можете выбирать несколько строк подряд, нажимая клавишу Shift, или несколько отдельных строк, нажимая клавишу Ctrl.
3. Нажмите кнопку **Заблокировать**.

Учетная запись пользователя заблокирована.

► Чтобы разблокировать учетную запись:

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

Откроется страница **Пользователи**.

2. В списке выберите пользователя, учетную запись которого необходимо разблокировать.

   Примечание. Вы можете выбирать несколько строк подряд, нажимая клавишу Shift, или несколько отдельных строк, нажимая клавишу Ctrl.

3. Нажмите кнопку **Разблокировать**.

Учетная запись пользователя разблокирована.

6.1.6. Экспорт данных пользователей в текстовый файл

► Чтобы экспортировать данные пользователей:

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

   Откроется страница **Пользователи**.

2. Выберите учетные записи пользователей для экспорта.

   Примечание. Вы можете выбирать несколько учетных записей подряд, нажимая клавишу Shift, или несколько отдельных учетных записей, нажимая клавишу Ctrl.

3. Нажмите кнопку **Экспорт**.
4. В открывшемся окне выберите вариант экспорта выбранных учетных записей и подтвердите экспорт.

   Браузер загрузит текстовый файл с данными пользователей.

Данные пользователей экспортированы.

6.1.7. Создание LDAP-подключения

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

► Чтобы создать LDAP-подключение:

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

   Откроется страница **Пользователи**.

2. В главном меню в разделе **Пользователи** выберите пункт **Настройка LDAP-подключений**.

   Откроется страница **Настройка LDAP-подключений**.

3. В панели инструментов нажмите кнопку **Добавить подключение**.

Откроется страница **Новое LDAP-подключение**.

4. Введите название LDAP-подключения.
5. В блоке параметров **Серверы** в поле **Адрес** введите IP-адрес или FQDN LDAP-сервера.

   Примечание. Если требуется устанавливать защищенное соединение с LDAP-сервером, адрес необходимо вводить в зависимости от типа доверенного сертификата (он выпускается или для IP-адреса, или для FQDN).

6. В поле **Порт** введите номер порта.
7. Если требуется устанавливать защищенное соединение с LDAP-сервером, установите флажок **SSL**.

   Примечание. Вы можете добавлять дополнительные серверы, нажимая **+**. При потере соединения с одним сервером запрос аутентификации может быть обработан другим сервером. После заполнения полей вы можете проверить соединение (см. раздел 6.1.11) с LDAP-серверами.

8. В поле **Домены** введите DNS-имя домена, NetBIOS-имя домена или UPN-суффикс.
9. В поле **База поиска** введите имя записи каталога, начиная с которой выполняется поиск учетных записей пользователей.

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

10. Если требуется, настройте синхронизацию с Microsoft Active Directory (см. раздел 6.1.8).
11. Нажмите кнопку **Сохранить**.

LDAP-подключение создано.

6.1.8. Настройка синхронизации с Microsoft Active Directory

Вы можете настраивать синхронизацию при создании LDAP-подключения на странице **Новое LDAP-подключение** или при его изменении на странице **Изменение параметров LDAP-подключения**. Перед настройкой синхронизации необходимо создать в Microsoft Active Directory учетную запись с правами на чтение данных о пользователях и группах пользователей.

► Чтобы настроить синхронизацию с Microsoft Active Directory:

1. Включите синхронизацию с Microsoft Active Directory.
2. В блоке параметров **Учетная запись** введите логин и пароль служебной учетной записи с правами на чтение данных о пользователях и группах пользователей Active Directory.
3. Если необходимо, включите синхронизацию по расписанию и по ссылке настройте расписание.

Примечание. Синхронизация также может быть запущена вручную на странице **Настройка LDAP-подключений**.

4. В блоке **Соответствие ролей и групп** в раскрывающихся списках выберите группы Microsoft Active Directory, соответствующие ролям пользователей.
5. Нажмите кнопку **Сохранить**.

   Синхронизация с Microsoft Active Directory настроена.

6.1.9. Запуск вручную синхронизации с Microsoft Active Directory

► Чтобы вручную запустить синхронизацию с Microsoft Active Directory:

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-подключений**.

   Откроется страница **Настройка LDAP-подключений**.
3. Выберите LDAP-подключение.
4. Нажмите кнопку **Запустить синхронизацию**.

   В таблице отобразится значок ◯.

Синхронизация с Microsoft Active Directory запущена вручную.

По завершении синхронизации:

— если синхронизация была выполнена успешно — значок статуса ◯ пропадет, в панели **<Название подключения>** время последней синхронизации изменится на актуальное;

— если синхронизация была выполнена с предупреждениями — значок статуса ◯ сменится на ⚠, в панели **<Название подключения>** отобразится текст предупреждения;

— если синхронизация была выполнена с ошибками — значок статуса ◯ сменится на ⚠, в панели **<Название подключения>** отобразится текст ошибки.

6.1.10. Изменение параметров LDAP-подключения

► Чтобы изменить параметры LDAP-подключения:

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-подключений**.

Откроется страница **Настройка LDAP-подключений**.

3. Выберите LDAP-подключение.
4. В панели инструментов нажмите кнопку **Изменить подключение**.

   Откроется страница **Изменение параметров LDAP-подключения**.

5. Внесите изменения.

   Примечание. После внесения изменений рекомендуется проверить подключение (см. раздел 6.1.11).

6. Нажмите кнопку **Сохранить**.

Параметры LDAP-подключения изменены.

6.1.11. Проверка LDAP-подключения

При проверке LDAP-подключения устанавливается пробное соединение с LDAP-серверами. Вы можете проверять подключение при его создании на странице **Новое LDAP-подключение** или изменении его параметров на странице **Изменение параметров LDAP-подключения**.

► Чтобы проверить LDAP-подключение:

1. Нажмите кнопку **Проверить соединение**.

   Откроется окно **Проверка соединения**.

2. Введите логин и пароль пользователя с правами доступа на чтение данных о пользователях.
3. Нажмите кнопку **Проверить**.

   Результаты проверки отобразятся в окне **Проверка соединения**.

4. Нажмите кнопку **Закрыть**.

LDAP-подключение проверено.

6.1.12. Удаление LDAP-подключения

► Чтобы удалить LDAP-подключение:

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-подключений**.

   Откроется страница **Настройка LDAP-подключений**.

3. Выберите LDAP-подключение.
4. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

LDAP-подключение удалено.

6.2. Управление ролями

В разделе приведены описание страницы **Роли**, инструкции по созданию, изменению и удалению ролей.

В этом разделе

6.2.1. Страница Роли

Страница **Роли** предназначена для работы с ролями и привилегиями. В панели инструментов страницы находятся следующие кнопки:

— **Создать** — для создания роли (см. раздел 6.2.2);

— **Редактировать** — для изменения доступных для роли привилегий (см. раздел 6.2.4);

— **Создать копию** — для создания роли на основе существующей роли (см. раздел 6.2.3);

— **Удалить** — для удаления роли (см. раздел 6.2.5);

— **Назначить** — для назначения роли пользователям (см. раздел 6.3.1).

В рабочей области страницы расположены:

— Панель **Роли**. Содержит список ролей по приложениям. При выборе роли в панели **Привилегии** отобразятся доступные для роли привилегии.

— Панель **Привилегии**. Содержит список привилегий, доступных для выбранной роли.

— Панель **<Название роли>**. Содержит описание выбранной роли, ссылку для просмотра учетных записей всех пользователей, которым назначена выбранная роль.

6.2.2. Создание роли

► Чтобы создать роль:

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

Откроется страница **Пользователи**.

2. В главном меню выберите раздел **Роли**.

   Откроется страница **Роли и права доступа**.

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

   Откроется окно **Создание роли**.

4. В раскрывающемся списке выберите приложение, для которого необходимо создать роль.
5. Введите название роли.
6. В блоке параметров **Права доступа** укажите флажки для тех привилегий, которые будет иметь создаваемая роль.
7. Нажмите кнопку **Создать**.

Роль создана.

6.2.3. Создание роли на основе существующей роли

► Чтобы создать роль на основе существующей:

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

   Откроется страница **Пользователи**.

2. В главном меню выберите раздел **Роли**.

   Откроется страница **Роли и права доступа**.

3. Выберите роль, на основе которой будет создана новая роль.
4. В панели инструментов нажмите кнопку **Создать копию**.

   Откроется окно **Создание роли**.

5. Введите название роли.
6. В блоке параметров **Права доступа** укажите флажки для тех привилегий, которые будет иметь создаваемая роль.
7. Нажмите кнопку **Создать**.

Роль создана.

6.2.4. Изменение роли

Вы можете изменять только созданные пользователями роли, системные роли недоступны для изменения.

► Чтобы изменить роль:

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

   Откроется страница **Пользователи**.

2. В главном меню выберите раздел **Роли**.

   Откроется страница **Роли и права доступа**.

3. В панели **Роли** выберите роль пользователя.

   Примечание. Вы можете выбирать несколько ролей подряд, нажимая клавишу Shift, или несколько отдельных ролей, нажимая клавишу Ctrl.

4. В панели инструментов нажмите кнопку **Редактировать**.

   Откроется страница **Редактирование роли <Название роли>**.

5. Внесите необходимые изменения и нажмите кнопку **Сохранить**.

Роль изменена.

6.2.5. Удаление роли

Вы можете удалять только созданные пользователями роли, системные роли недоступны для удаления.

► Чтобы удалить роль:

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

   Откроется страница **Пользователи**.

2. В главном меню выберите раздел **Роли**.

   Откроется страница **Роли и права доступа**.

3. В панели **Роли** выберите роль пользователя.

   Примечание. Вы можете выбирать несколько ролей подряд, нажимая клавишу Shift, или несколько отдельных ролей, нажимая клавишу Ctrl.

4. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Роль удалена.

6.3. Управление правами доступа

Вы можете управлять правами доступа к разделам веб-интерфейса и операциям во всех зарегистрированных в системе приложениях.

Права доступа к разделам веб-интерфейса и операциям в системе назначаются в приложении Management and Configuration и определяются набором доступных привилегий для роли, назначенной пользователю.

Если аутентификация пользователей выполняется локально или через LDAP без синхронизации с Microsoft Active Directory, вы можете назначать:

— роли в нескольких приложениях одному пользователю — при создании его учетной записи на странице **Новый пользователь** или изменении его данных на странице **Изменение данных пользователя**;

— роли в нескольких приложениях одному пользователю — при создании его учетной записи на странице **Новый пользователь** или изменении его данных на странице **Изменение данных пользователя**;

— роли в одном приложении нескольким пользователям — на странице **Роли и права доступа**;

— роли в нескольких приложениях нескольким пользователям — на странице **Пользователи**.

Если учетные записи пользователей синхронизируются с Microsoft Active Directory, назначение им ролей в приложении Management and Configuration недоступно. Назначать роли таким пользователям необходимо в Microsoft Active Directory, добавляя их в группы, соответствующие требуемых ролям.

В этом разделе

6.3.1. Назначение пользователям ролей одного приложения

► Чтобы назначить пользователям роли:

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

   Откроется страница **Пользователи**.

2. В главном меню выберите раздел **Роли**.

   Откроется страница **Роли и права доступа**.

3. В панели **Роли** выберите роли, которые необходимо назначить пользователям.

   Примечание. В панели **Роли** вы можете выбрать роли только одного приложения.

4. В панели инструментов нажмите кнопку **Назначить**.

5. Во всплывающем окне установите флажки для тех пользователей, которым необходимо назначить выбранные роли.
6. Нажмите кнопку **Назначить выбранные роли пользователям**.

Пользователям назначены роли.

6.3.2. Назначение пользователям ролей нескольких приложений

► Чтобы назначить пользователям роли:

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

   Откроется страница **Пользователи**.
2. Выберите учетные записи пользователей, которым необходимо назначить роли.

   Примечание. Вы можете выбирать несколько учетных записей подряд, нажимая клавишу Shift, или несколько отдельных учетных записей, нажимая клавишу Ctrl.
3. В панели инструментов нажмите кнопку **Роли в приложениях**.

   Откроется окно **Роли пользователей**.
4. В раскрывающемся списке **<Название приложения>** установите флажки для назначаемых пользователям ролей.
5. Нажмите кнопку **Сохранить**.

Пользователям назначены роли.

6.4. Страница Журнал действий пользователей

Страница **Журнал действий пользователей** предназначена для просмотра записей о действиях пользователей.

В рабочей области страницы расположены:

— Панель **Действия**. Содержит список возможных действий пользователей. При выборе действия в панели **Действия пользователей** отобразятся записи о выбранном действии.

— Панель **Пользователи**. Содержит список учетных записей пользователей и кнопку 🔍 для их быстрого поиска. При выборе учетной записи в панели **Действия пользователей** отобразятся записи о действиях пользователя с выбранной учетной записью.

— Панель **Действия пользователей**. Содержит таблицу с записями, ссылку со значком 📅 и кнопки 🔍 , 🔄 и ⋮ . В таблице доступны выбор записи, а также сортировка записей по времени регистрации действий. При нажатии ссылки со значком 📅 открывается всплывающее окно для выбора периода просмотра записей. При нажатии 🔍 в верхней

части панели открывается поле для быстрого поиска записей, при нажатии обновятся данные в таблице, при нажатии откроется блок параметров для настройки автоматического обновления данных.

— Панель **<Дата и время действия>**. Содержит данные о выбранной записи.

6.5. Просмотр записей о действиях пользователей

► Чтобы просмотреть записи о действиях пользователя:

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

   Откроется страница **Пользователи**.

2. В главном меню выберите раздел **Журнал действий**.

   Откроется страница **Журнал действий пользователя**.

3. В панели **Пользователи** выберите пользователя, записи о действиях которого необходимо просмотреть.

4. В панели **Действия** выберите группу действий, записи о которых необходимо просмотреть.

5. Если требуется, выберите период для просмотра записей, нажав .

   В панели **Действия пользователей** отобразится список записей о действиях пользователя.

7. Интерфейс Knowledge Base

Страница веб-интерфейса Knowledge Base состоит из главного меню и рабочей области.

С помощью разделов главного меню, расположенного в верхней части веб-интерфейса, вы можете выбирать базу данных и переключаться между разными типами объектов в базе (компоненты, эксплойты, сигнатуры и прочее). В рабочей области отображается список объектов, относящихся к выбранной базе и типу: например, уязвимости, которые содержатся в базе VM Content.

В списке отображается информация об объектах: название, дата добавления в базу данных и другие сведения. Вы можете настраивать отображение информации в списке, а также фильтровать объекты и искать их с помощью строки поиска.

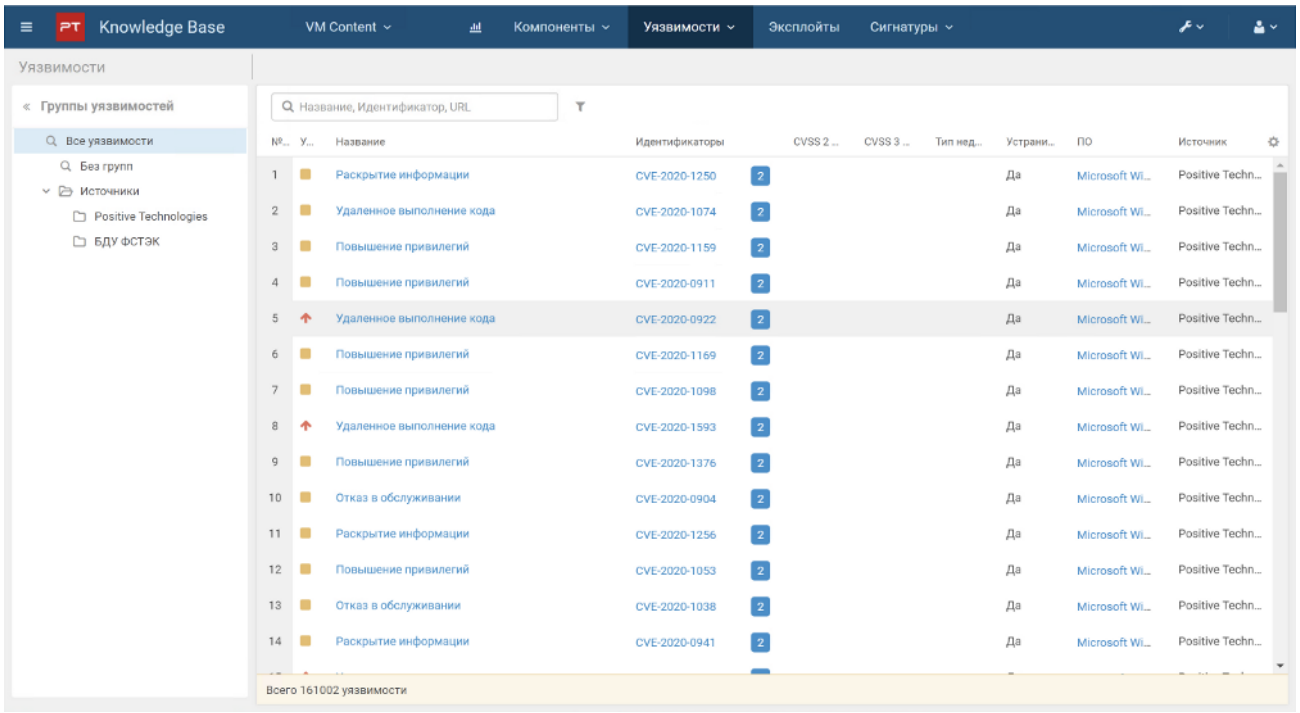

Рисунок 1. Интерфейс Knowledge Base

8. Базы данных

В Knowledge Base для хранения данных используется иерархическая модель БД. Все базы данных связаны как "предок — потомок" по принципу "один ко многим".

По типам доступа базы данных делятся на системные (недоступные для изменения пользователями) и пользовательские. Требуется задать модификаторы доступа к пользовательской базе данных при ее создании и изменении.

В комплект поставки продукта входит корневая системная база данных VM Content. VM Content содержит данные, формируемые в "Позитив Текнолоджиз" и регулярно обновляемые с серверов "Позитив Текнолоджиз". На основе базы данных VM Content вы можете создать собственную иерархическую структуру пользовательских баз данных.

В комплект поставки продукта входит корневая системная база данных VM Content. Основное назначение VM Content — получать актуальные данные с серверов обновления "Позитив Текнолоджиз". На основе базы данных VM Content вы можете создать собственную иерархическую структуру пользовательских баз данных.

При создании новой БД происходит копирование всего содержимого из родительской базы. Работа с данными в Knowledge Base осуществляется в рамках единственной выбранной БД.

Произведенные изменения (ревизии) выбранной БД можно просмотреть в истории изменений и внести в родительскую или дочернюю БД посредством механизмов слияния и импорта ревизий соответственно.

В интерфейсе Knowledge Base база VM Content отмечена значком  .

В этом разделе

8.1. Создание пользовательской БД

► Чтобы создать пользовательскую БД:

1. В главном меню в разделе **<Название БД>** выберите пункт **Базы данных**.

   Откроется страница **Базы данных / <Название БД>**.
2. В панели **Базы данных** выберите родительскую БД.
3. В панели инструментов нажмите кнопку **Создать ветку**.

4. В открывшемся окне в поле **Имя** введите название БД.
5. В поле **Идентификатор** введите идентификатор БД.
6. В блоке параметров **Модификаторы доступа** настройте параметры БД.
7. Нажмите кнопку **Сохранить**.

Начнется процесс создания пользовательской БД. По завершении БД будет доступна для выбора.

8.2. Изменение и удаление БД

► Чтобы изменить параметры БД:

1. В главном меню в разделе **<Название БД>** выберите пункт **Базы данных**.

   Откроется страница **Базы данных / <Название БД>**.

2. В панели инструментов нажмите кнопку **Управление** и в раскрывшемся меню выберите пункт **Редактировать**.

   Откроется окно **Редактирование базы данных**.

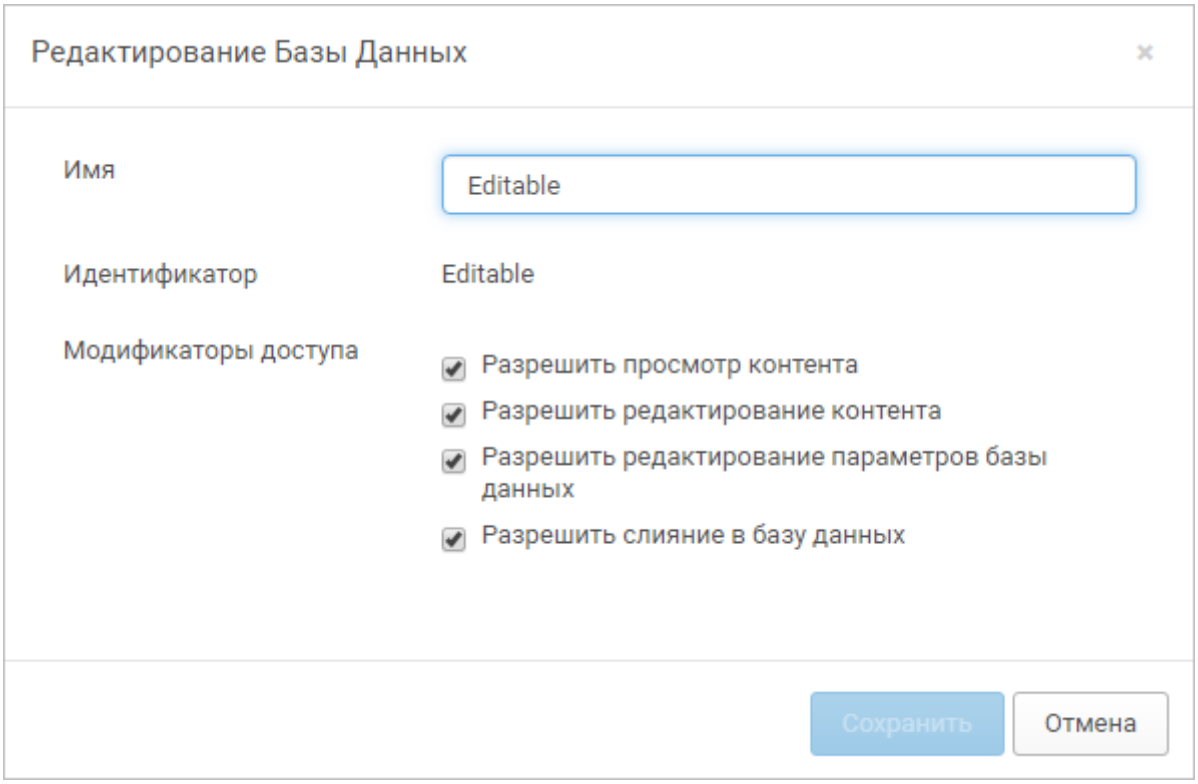

Рисунок 2. Изменение параметров БД

3. Измените параметры БД.
4. Нажмите кнопку **Сохранить**.

БД изменена.

► Чтобы удалить пользовательскую БД:

1. В главном меню в разделе **<Название БД>** выберите пункт **Базы данных**.

   Откроется страница **Базы данных / <Название БД>**.
2. В панели инструментов нажмите кнопку **Управление** и в раскрывшемся меню выберите пункт **Удалить**.
3. В открывшемся окне подтвердите удаление по кнопке **Продолжить**.

БД удалена.

8.3. О ревизиях БД и просмотре разницы между ревизиями

Изменение любого объекта в БД, приводит к изменению ревизии БД. Произведенные изменения БД можно просмотреть в истории изменений. Внести изменения в родительскую или дочернюю БД можно посредством механизмов слияния и импорта ревизий соответственно. Чтобы облегчить пользователям работу с ревизиями, реализована функция сравнения ревизий и просмотра разницы между ревизиями в пользовательских БД. История ревизий БД и функция просмотра разницы ревизий доступны на странице **Базы данных**.

С помощью просмотра разницы ревизий:

— Администратор может отслеживать изменения в БД и контролировать действия операторов с объектами в созданных для них дочерних БД.

— Оператор может просматривать изменения БД и отдельных объектов, с которыми он работает.

Администратор с помощью просмотра разницы ревизий может отслеживать изменения содержимого БД (например, в БД For Robots) и контролировать действия операторов с объектами Knowledge Base в созданных для них дочерних БД.

Оператор с помощью просмотра разницы ревизий может просматривать изменения в БД и отдельных объектов, с которыми он работает. Нарпример, оператор может быстро найти карточку объекта, в которую были внесены некорректные изменения.

8.4. Сравнение ревизий БД

► Чтобы сравнить ревизии БД и просмотреть изменения объектов в БД:

1. В главном меню в разделе **<Название БД>** выберите пункт **Базы данных**.

   Откроется страница **Базы данных / <Название БД>**.
2. В панели **Базы данных** выберите БД.

На странице отобразится список ревизий выбранной БД. В списке для каждой ревизии отображаются имя пользователя, который изменил БД, дата и время изменения.

3. Наведите курсор на ревизию, которую вы хотите добавить в сравнение.

   В правой части строки выбранной ревизии отобразится кнопка **Сравнение по объектам**.

4. Нажмите кнопку **Сравнение по объектам** и в раскрывшемся меню выберите вариант сравнения ревизии:

   - **С начальной ревизией** — чтобы просмотреть все изменения в БД с момента ее создания до выбранной ревизии.
   - **С предыдущей ревизией**.
   - **Выбрать ревизию для сравнения** — чтобы сравнить ревизию с любой другой ревизией в списке. Если вы выбрали этот вариант, наведите курсор на ревизию, с которой вы хотите сравнить выбранную, и нажмите кнопку **Сравнить по объектам выбранные версии**.
   - **Сравнение со слитой ревизией** — чтобы просмотреть изменения в БД после последнего импорта в родительскую БД.

     Примечание. Вариант **Сравнение со слитой ревизией** не отображается в раскрывающемся меню, если импорт в родительскую БД не производился или родительской БД является системная БД VM Content.

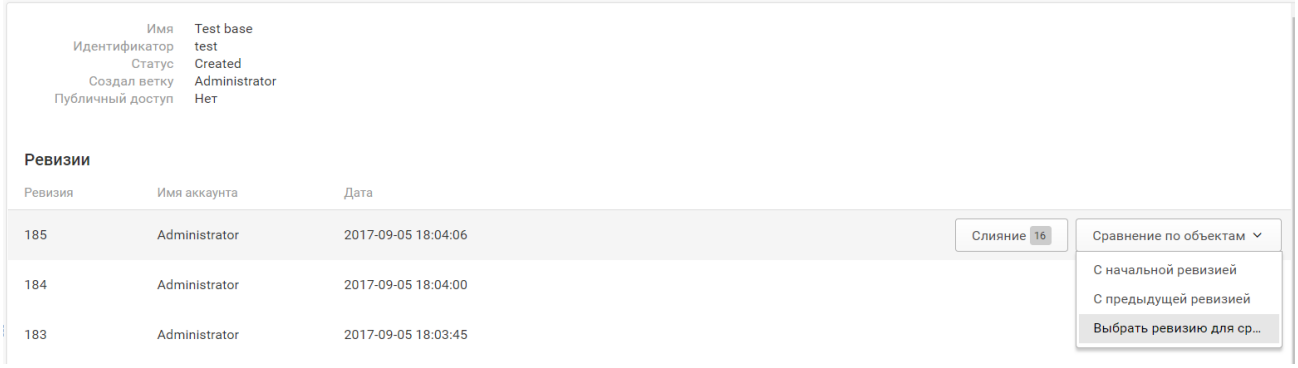

Рисунок 3. Выбор варианта сравнения ревизии

   Отобразится страница **Сравнение ревизий**.

5. В левой панели на странице **Сравнение ревизий** выберите группу объектов, например уязвимости.
6. В левой панели на странице **Сравнение ревизий** выберите тип объектов, например уязвимости.
7. В центральной панели выберите объект, изменения в котором вы хотите просмотреть.

Вы можете фильтровать объекты по кнопке **Статус**: **Новые** (добавленные в БД), **Удаленные** и **Измененные**. По умолчанию все флажки в меню кнопки **Статус** сняты, отображаются объекты во всех статусах.

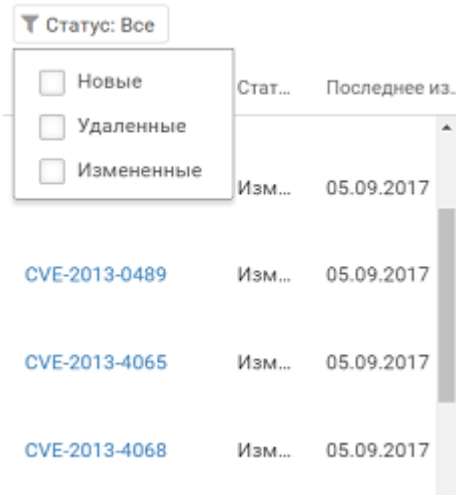

Рисунок 4. Выборка объектов по статусу

В правой панели отобразятся свойства объекта в соответствии с его карточкой в БД. По умолчанию отображаются все свойства объекта.

Карточку объекта можно просмотреть, перейдя по ссылке с названием объекта. Карточка объекта открывается в новой вкладке браузера.

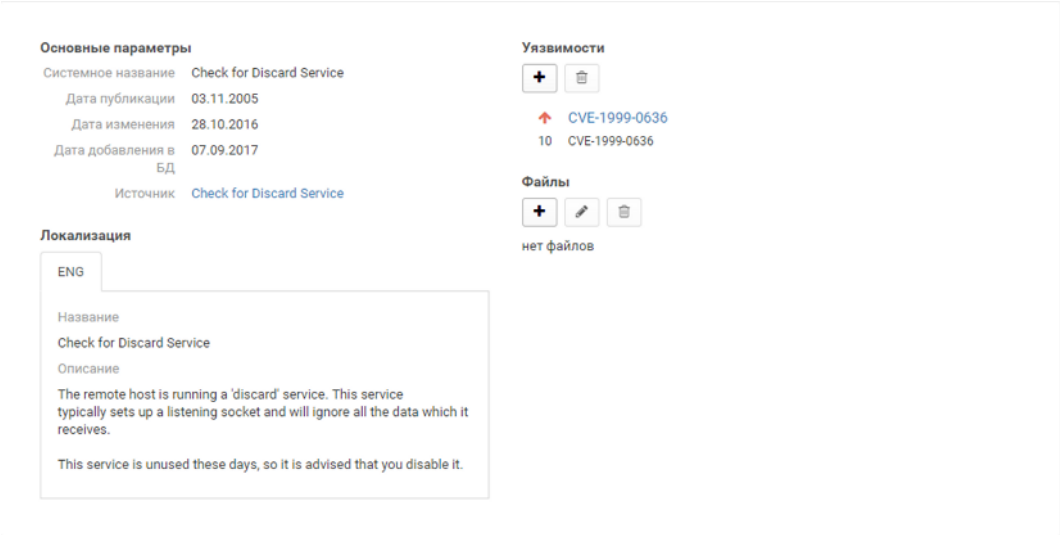

Рисунок 5. Просмотр карточки объекта

8. Если требуется отображать только измененные свойства объекта, включите показ изменений в верхнем правом углу панели.

Изменения каждого свойства объекта между ревизиями отображаются в столбцах **Было** и **Стало**. Чтобы облегчить поиск и просмотр изменений, применяется цветовая индикация: добавленные свойства объекта отмечены зеленым цветом, измененные — оранжевым, удаленные — красным.

Свойство объекта может содержать несколько подразделов (например, несколько условий существования и закрытия уязвимости). Вы можете раскрывать и скрывать эти подразделы кнопками **Развернуть все** и **Свернуть все**.

Свойство объекта может содержать несколько вложенных свойств. Вы можете раскрывать и скрывать эти подразделы кнопками **Развернуть все** и **Свернуть все**.

► Чтобы отменить изменения свойств объекта:

1. Наведите курсор мыши на изменение и нажмите .

   Цвет кнопки изменится на красный. В левой панели отобразится блок **Отмена изменений**.

2. Выберите блок **Отмена изменений**.

   В центральной панели отобразится список объектов для отмены изменений.

3. Если требуется восстановить отмененные изменения, нажмите .
4. В центральной панели нажмите кнопку **Отменить <n> объекта** и подтвердите отмену изменений.
5. Нажмите кнопку **Завершить**.

8.5. Импорт ревизий из родительской БД

► Чтобы выполнить импорт изменений из родительской БД:

1. В главном меню в разделе **<Название БД>** выберите пункт **Базы данных**.

   Откроется страница **Базы данных / <Название БД>**.

2. В панели **Базы данных** выберите БД.
3. В панели инструментов нажмите кнопку **Импорт ревизий**.

   Начнется импорт ревизий, появится индикатор выполнения. По завершении импорта появится сообщение "Импорт выполнен".

   Примечание. Вы можете остановить импорт, нажав кнопку **Отменить**.

4. В строке сообщения нажмите кнопку **Завершить**.

Выполнен импорт изменений из родительской БД.

8.6. Слияние ревизий в родительской базе данных

► Чтобы экспортировать данные в родительскую БД (выполнить слияние баз):

1. В веб-интерфейсе Knowledge Base на странице **Базы данных** выберите дочернюю БД.

   Примечание. Экспорт данных в базу VM Content невозможен.

2. Наведите курсор на строку с ревизией, которую нужно экспортировать, и нажмите кнопку **Слияние**.

   Начнется экспорт данных. На странице отобразится сообщение **Слияние выполняется**.

3. Если требуется прервать процесс экспорта, нажмите кнопку **Отменить**.

4. По завершении экспорта нажмите кнопку **Завершить**.

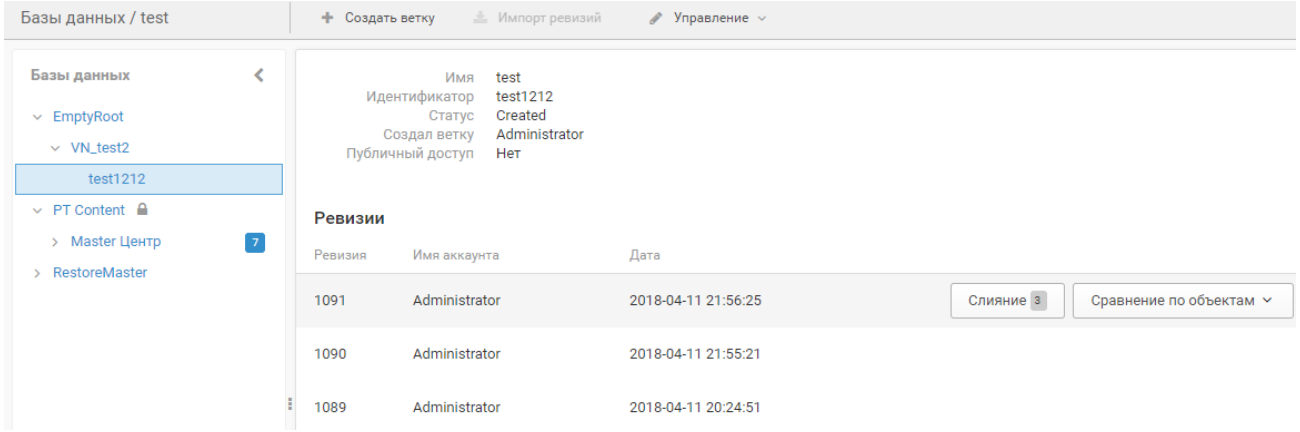

Рисунок 6. Слияние баз данных

5. Если нужно просмотреть изменения в базе данных между ревизиями, нажмите кнопку **Сравнение**.

   Откроется страница **Сравнение ревизий**. Изменения будут выделены зеленым цветом.

Данные экспортированы в родительскую базу данных. Экспортированный элемент в списке **Ревизии** выделен желтым цветом.

9. Источники обновлений контента

Обновления контента Knowledge Base формируются из трех источников:

— Уязвимости, бюллетени безопасности и программное обеспечение — приходят с серверов обновлений "Позитив Текнолоджиз". Обновление выполняется в рамках процедуры Live Update. Обновления поступают в системную базу VM Content.

— Пользовательский контент Knowledge Base, созданный операторами в рамках процесса синхронизации контента — поступает в автоматически создаваемые дочерние ветки базы Master.

10. Программное обеспечение

Knowledge Base содержит информацию о программном обеспечении (ПО) с указанием производителей, количества уязвимостей и эксплойтов. Вы можете добавлять в базы данных записи о новом ПО, изменять существующие записи (карточки ПО) и добавлять ПО в группы.

Knowledge Base также позволяет добавлять дистрибутивы ПО в хранилище для использования в экспериментах.

Информация о программном обеспечении (ПО) в выбранной базе данных отображается на странице **Программное обеспечение** (раздел главного меню **Компоненты** → **Программное обеспечение**).

Объекты представлены в виде списка. По умолчанию отображаются все объекты в выбранной базе. Над списком находится строка быстрого поиска. Для поиска и отображения по набору признаков вы можете использовать настраиваемый фильтр. Фильтр доступен по кнопке над списком.

Вы можете настраивать отображение столбцов по кнопке в правой части списка.

Этот раздел содержит инструкции по работе с записями и дистрибутивами ПО в интерфейсе системы.

В этом разделе

10.1. Добавление ПО в базу знаний

Вы можете добавлять в базу знаний ПО различных типов: операционные системы, патчи, обновления и другие. ПО для телекоммуникационного оборудования (ПО для CPE, customer premises equipment) добавляется при помощи отдельной формы.

► Чтобы добавить новое ПО в базу знаний:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.

   Примечание. Вы не можете вносить изменения в базу данных VM Content.

2. В веб-интерфейсе системы на странице **Программное обеспечение** нажмите кнопку **Создать ПО**.

   Откроется форма добавления ПО.

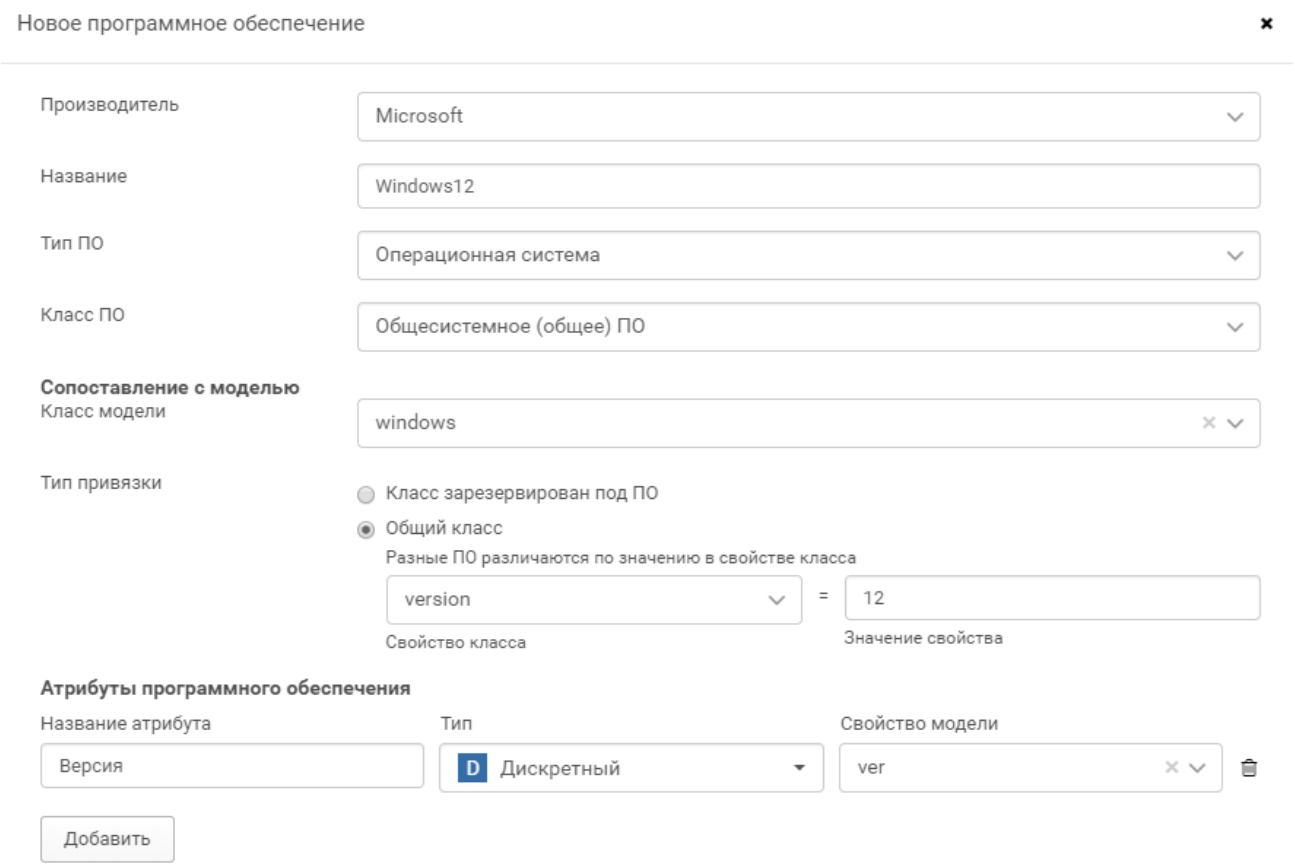

Рисунок 7. Добавление ПО

3. В раскрывающемся списке выберите название производителя ПО.

   Если наименование производителя отсутствует в списке, введите наименование в поле **Производитель**, затем в раскрывающемся списке выберите пункт **Создать производителя**.

4. Введите название ПО.
5. В раскрывающемся списке выберите тип ПО.
6. В раскрывающемся списке выберите группы ПО, в которые будет включено добавляемое ПО.
7. Выберите класс модели ПО в раскрывающемся списке или введите новое наименование класса модели ПО, затем в раскрывающемся списке выберите пункт **Создать класс модели**.
8. Выберите тип связи класса с ПО в блоке параметров **Тип привязки**:

   • **Класс зарезервирован под ПО** — класс модели привязывается к ПО и будет недоступен для выбора при добавлении или изменении параметров другого ПО.

   • **Общий класс** — класс модели будет доступен для выбора при добавлении или изменении параметров другого ПО. При выборе данного типа привязки заполните поля **Свойство класса** и **Значения свойства**.

9. При необходимости создайте атрибуты для ПО. Нажмите кнопку **Добавить**, чтобы добавить новый атрибут, и заполните поля:

   • **Название атрибута**. Укажите название атрибута в свободной форме.

   • **Тип**. Выберите тип атрибута в раскрывающемся списке.

   • **Свойство модели**. Выберите свойство модели в раскрывающемся списке или создайте новое.

10. Нажмите кнопку **Сохранить**.

В результате новое ПО будет добавлено в список.

10.2. Изменение параметров ПО

► Чтобы изменить параметры ПО:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.

   Примечание. Вы не можете вносить изменения в базу данных VM Content.

2. В главном меню выберите раздел **Программное обеспечение**.

3. Нажмите на название ПО в списке.

   Откроется карточка ПО.

4. При помощи кнопок +, , создайте, измените или удалите атрибуты ПО и их значения.

5. Нажмите кнопку **Редактировать параметры**.

   Откроется форма изменения параметров ПО.

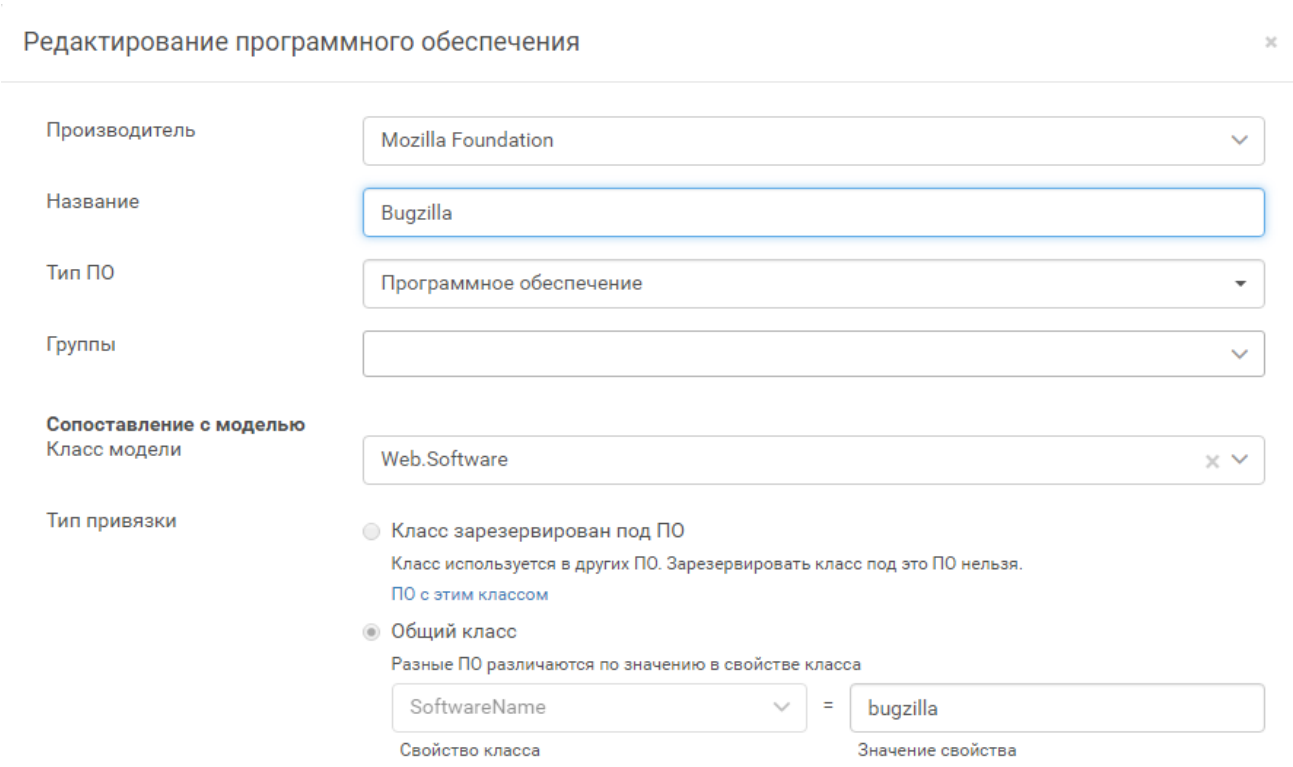

Рисунок 8. Изменение параметров ПО

6. Внесите необходимые изменения и нажмите кнопку **Сохранить**.
7. Нажмите кнопку **Редактировать зависимости при установке**, расположенную в верхней части карточки ПО.

   Откроется форма ввода зависимостей при установке.

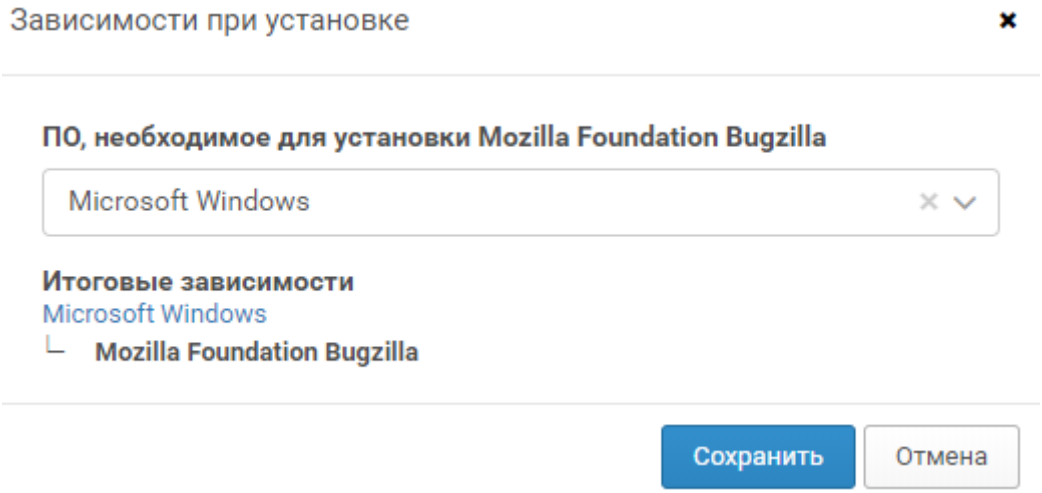

Рисунок 9. Добавление зависимости при установке ПО

8. В раскрывающемся списке выберите ПО, которое необходимо для установки программы.
9. Нажмите кнопку **Сохранить**.

10.3. Работа с группами ПО

ПО в системе можно группировать. Группы выполняют функцию фильтров для быстрого поиска и отображения нужного ПО. Вы можете создавать дополнительные (пользовательские) фильтры в виде иерархического списка групп.

По умолчанию в системе добавлены два преднастроенных фильтра для ПО:

— **Все ПО** (отображает все ПО, добавленное в систему)

— **Без групп** (отображает ПО, не распределенное по группам).

В интерфейсе системы фильтры находятся в левой части страницы **Программное обеспечение**.

В этом разделе

10.3.1. Создание группы ПО

► Чтобы создать группу ПО:

1. В веб-интерфейсе системы на странице **Программное обеспечение** в меню **Группа** выберите пункт **Создать группу**.

   Откроется форма создания группы.
2. Введите идентификатор группы.
3. В раскрывающемся списке выберите родительскую группу.
4. Введите название группы в одно из полей (**ENG** или **RUS**), или в оба поля.
5. Нажмите кнопку **Сохранить**.

В результате новая группа появится в иерархическом списке групп в левой части страницы.

10.3.2. Добавление ПО в группу

В веб-интерфейсе системы вы можете добавлять ПО в группу двумя способами:

— на странице **Программное обеспечение** из списка ПО;

— из окна изменения параметров ПО.

► Чтобы добавить ПО в группу из списка ПО:

1. В веб-интерфейсе системы на странице **Программное обеспечение** выберите ПО в списке.

   Примечание. При необходимости введите часть названия ПО в поле быстрого поиска.

2. В раскрывающемся списке **Расположение в группах** установите флажки напротив групп, в которые следует включить выбранное ПО.

В результате ПО будет включено в выбранные группы.

► Чтобы добавить ПО в группу из окна изменения параметров ПО:

1. В веб-интерфейсе системы на странице **Программное обеспечение** выберите ПО в списке.
2. Нажмите кнопку **Редактировать**.

   Откроется карточка ПО.

3. В раскрывающемся списке **Группы** установите флажки напротив групп, в которые следует включить выбранное ПО.
4. Нажмите кнопку **Сохранить**.

В результате ПО будет включено в выбранные группы.

ПО будет отображаться в списке при выборе группы, а также при выборе фильтра **Все ПО**, но не будет отображаться при выборе фильтра **Без групп**.

10.4. Добавление дистрибутивов ПО

Вы можете добавлять в систему дистрибутивы ПО. Добавление дистрибутивов выполняется в карточке ПО. Для одного ПО в системе можно создать несколько дистрибутивов с разными параметрами. В каждый дистрибутив можно добавить несколько файлов.

► Чтобы добавить дистрибутив ПО:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.

   Примечание. Вы не можете вносить изменения в базу данных VM Content.

2. В главном меню выберите раздел **Программное обеспечение**.

   Откроется страница со списком ПО, добавленного в систему.

3. В списке нажмите название ПО, дистрибутив которого нужно загрузить.

   Откроется карточка ПО.

4. В левой верхней части карточки ПО нажмите ссылку **Дистрибутивы**.

Вы перейдете в панель **Дистрибутивы**.

5. В панели **Дистрибутивы** нажмите кнопку [+].

   Откроется окно добавления дистрибутива.

6. В окне укажите параметры добавляемого дистрибутива.

   - В поле **Описание** введите описание дистрибутива в свободной форме.
   - Выберите значения атрибутов дистрибутива.

     Примечание. Для разных типов ПО в окне отображаются разные атрибуты. Чтобы новый дистрибутив был создан, выберите значение хотя бы одного атрибута.

   - В поле **Выпущен** укажите дату выпуска дистрибутива.

     Примечание. Чтобы учесть возможную разницу в часовых поясах, в поле **Выпущен** при необходимости можно указать дату на сутки вперед.

7. Нажмите кнопку **Добавить**.

   Окно добавления дистрибутива закроется. Указанные параметры отобразятся в панели **Дистрибутивы**.

8. В панели **Дистрибутивы** нажмите кнопку **Добавить файл**.

   Откроется окно **Новый файл дистрибутива**.

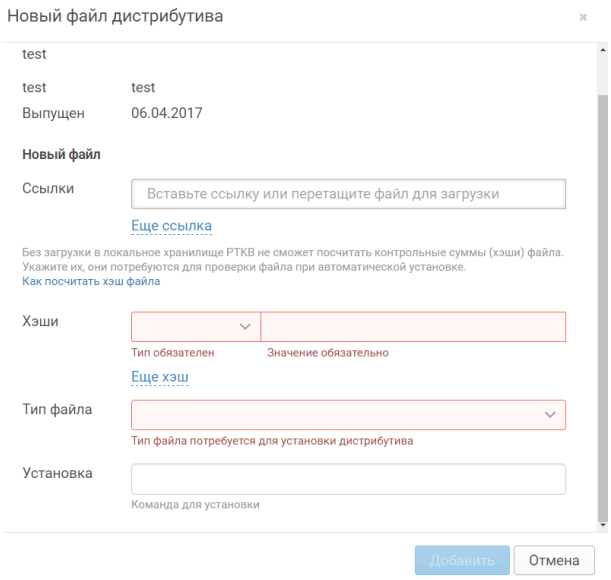

Рисунок 10. Добавление файла дистрибутива

9. В поле **Ссылки** укажите ссылку на файл дистрибутива или перетащите файл в это поле.

   Если вы перетащили файл в поле **Ссылки**, начнется загрузка файла во временное хранилище. Во временном хранилище файл находится до добавления в постоянное хранилище по кнопке **Добавить**. Если в течение 24 часов после загрузки работа в

окне **Новый файл дистрибутива** не завершена и файл не добавлен в постоянное хранилище, система удалит файл из временного хранилища. В этом случае загрузку файла придется повторить.

10. В поле **Хэши** укажите тип и значение контрольной суммы файла дистрибутива.

    Поле является обязательным для заполнения. Нужно указать хотя бы одну контрольную сумму. При перетаскивании файла в поле **Ссылки** система рассчитывает все четыре типа хэшей (MD5, SHA1, SHA256, SHA215).

11. Укажите расширение добавленного файла в раскрывающемся списке **Тип файла** и команду для установки файла в поле **Установка**.

    Параметры **Тип файла** и **Установка** не являются обязательными.

12. Нажмите кнопку **Добавить**.

Система добавит файл дистрибутива в постоянное хранилище. Ссылка на скачивание файла из хранилища, контрольные суммы, тип файла и команда для установки отобразятся на карточке ПО.

10.5. Удаление дистрибутивов ПО

Вы можете удалять из системы дистрибутивы ПО. Доступны два варианта удаления:

— Удаление только ссылки на файл дистрибутива. В этом случае удаляется только ссылка на файл на карточке ПО, а файл дистрибутива остается в хранилище. Пользователи, которые сохранили ссылку на файл, по-прежнему смогут загружать файл из хранилища.

— Удаление и ссылки на файл, и самого файла из хранилища. Пользователи, которые сохранили ссылку на файл, не смогут загрузить его из хранилища.

► Чтобы удалить файл дистрибутива:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню выберите раздел **Программное обеспечение**.

   Откроется страница со списком ПО, добавленного в систему.

3. В списке нажмите название ПО, дистрибутив которого нужно загрузить.

   Откроется карточка ПО.

4. В левой верхней части карточки ПО нажмите ссылку **Дистрибутивы**.

   Вы перейдете в панель **Дистрибутивы**.

5. В панели **Дистрибутивы** нажмите значок 🗑 напротив записи о файле дистрибутива.
6. В открывшемся окне подтвердите удаление по кнопке **Удалить**.
7. Выберите вариант удаления:

- Нажмите **Удалить ссылку на файл**, чтобы удалить только ссылку, а сам файл оставить в хранилище.
- Нажмите **Удалить файл**, чтобы удалить и ссылку, и сам файл из хранилища.

Система удалит файл и (или) ссылку на него согласно выбранному вами варианту удаления. Запись об удаленном файле дистрибутива перестанет отображаться в карточке ПО.

При удалении не одного файла дистрибутива, а всего дистрибутива или всего ПО целиком, система предложит удалить все файлы и (или) ссылки, которые относятся к удаляемому дистрибутиву или ПО.

11. Уязвимости

Knowledge Base содержит информацию об уязвимостях из разных источников. Для каждой уязвимости отображается идентификатор CVE, значения CVSS, количество связанных эксплойтов и бюллетеней. Доступен поиск уязвимостей по идентификаторам (CVE, CWE, FSTEC, MS, MP8ID), по идентификатору связанного бюллетеня, по названию уязвимого ПО и его производителя.

Вы можете добавлять в систему новые уязвимости, изменять параметры уязвимостей, указывать условия существования и закрытия и распределять уязвимости по группам. Также доступна фильтрация уязвимостей по интервалу базовых оценок CVSS.

Информация об уязвимостях в выбранной базе данных отображается на странице **Уязвимости** (раздел главного меню **Уязвимости** → **Уязвимости**).

Объекты представлены в виде списка. По умолчанию отображаются все объекты в выбранной базе. Над списком находится строка быстрого поиска. Для поиска и отображения по набору признаков вы можете использовать настраиваемый фильтр. Фильтр доступен по кнопке над списком.

Вы можете настраивать отображение столбцов по кнопке в правой части списка.

Этот раздел содержит инструкции по работе с уязвимостями в интерфейсе системы.

В этом разделе

11.1. Добавление уязвимости

Вы можете добавлять в систему уязвимости, указывая идентификатор уязвимости и его значение, а также базовый и временный векторы CVSS.

► Чтобы создать новую уязвимость:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.

   Примечание. Вы не можете вносить изменения в базу данных VM Content.

2. В главном меню в разделе **Уязвимости** выберите пункт **Уязвимости**.

   Откроется страница **Уязвимости**.

3. Нажмите кнопку **Создать**.

   Откроется форма создания новой уязвимости.

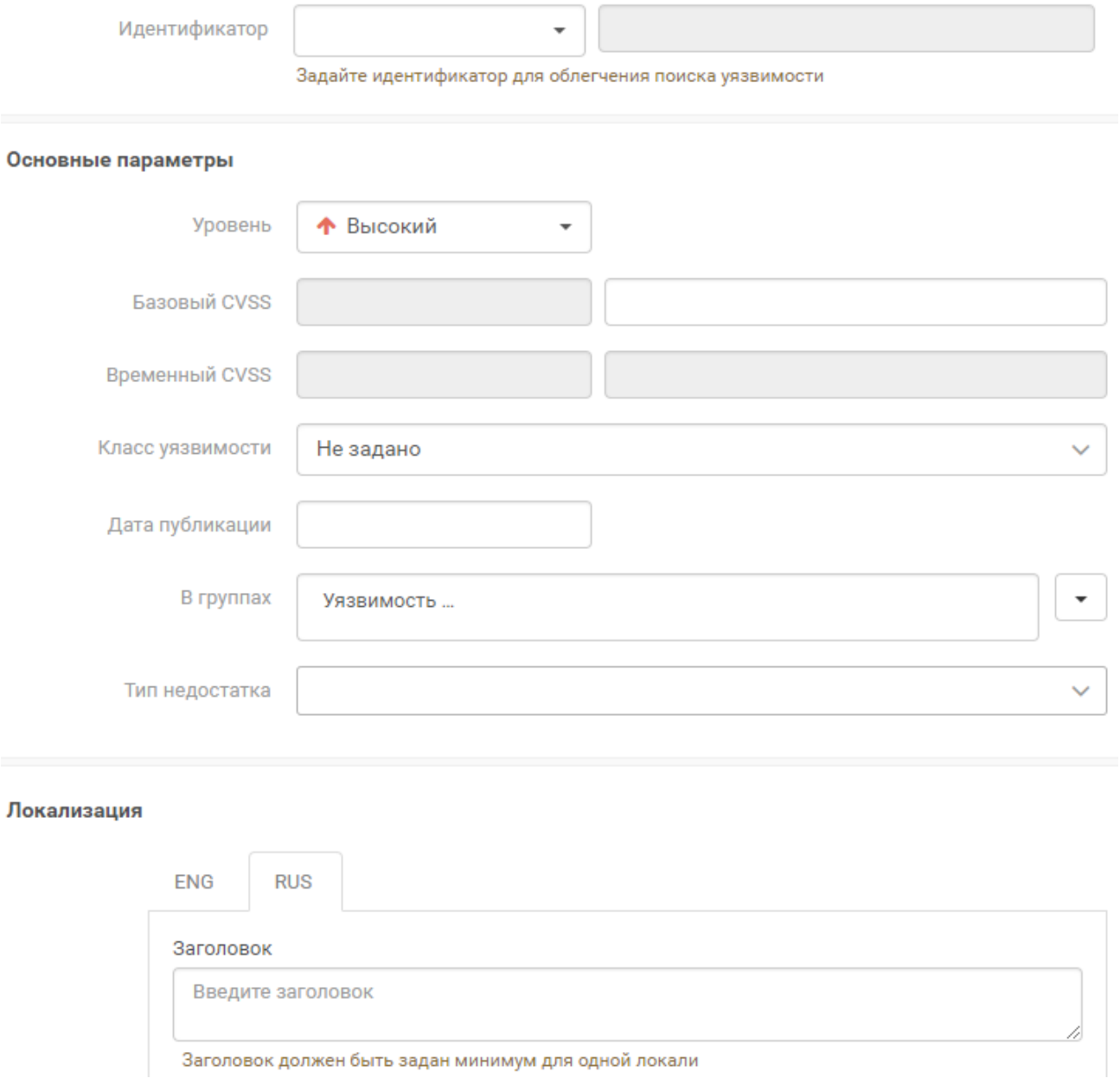

Рисунок 11. Добавление уязвимости

4. В раскрывающемся списке **Идентификатор** выберите тип идентификатора.
5. Введите значение идентификатора, соответствующее его типу.
6. В раскрывающемся списке **Уровень** выберите уровень опасности уязвимости.
7. Введите значение базового CVSS.

   Оценка будет рассчитана автоматически. Активируется поле **Временный CVSS**.

8. Введите значение временного CVSS.

   Оценка будет рассчитана автоматически.

9. В раскрывающемся календаре выберите дату публикации уязвимости.

10. Выберите класс модели в раскрывающемся списке.

    Если наименование класса модели отсутствует в списке, введите новое наименование класса модели, затем в раскрывающемся списке выберите пункт **Создать класс модели**.

11. В раскрывающемся списке выберите группы уязвимостей, в которые будет включена создаваемая уязвимость.

12. Заполните поля в блоке параметров **Локализация**.

    Поле **Заголовок** является обязательным для заполнения.

13. Нажмите кнопку **Сохранить**.

В результате будет создана уязвимость с указанными параметрами и откроется карточка уязвимости.

11.2. Поиск уязвимостей по идентификаторам

Вы можете искать уязвимости в базе данных по идентификатору CVE и по идентификаторам других типов. Зная только значение идентификатора, вы можете определить, какому типу идентификатора оно соответствует.

Доступен поиск по идентификаторам уязвимостей BID, Cisco, CVE, CWE, FSTEC, MS, MP8ID, OSVDB, Secunia, OVAL.

► Чтобы найти в базе данных уязвимость по значению идентификатора:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.

2. В главном меню в разделе **Уязвимости** выберите пункт **Уязвимости**.

   Отобразится страница со списком уязвимостей.

3. В поле поиска в верхней части страницы введите значение идентификатора (идентификатора CVE или другого).

   В списке отобразятся только те уязвимости, которые содержат введенный идентификатор. Если уязвимость имеет больше одного идентификатора, в столбце **Идентификаторы** рядом со значением идентификатора CVE отобразится кнопка с числом идентификаторов этой уязвимости. Например, кнопка с числом 3 означает что у найденной уязвимости есть три идентификатора.

4. Нажмите кнопку с числом идентификаторов.

Отобразится всплывающее сообщение с идентификаторами уязвимости, распределенными по типам.

11.3. Поиск уязвимости по идентификатору бюллетеня

Вы можете искать уязвимости в базе данных Knowledge Base по идентификаторам бюллетеней, связанных с этими уязвимостями.

► Чтобы найти уязвимость по идентификатору связанного с ней бюллетеня:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Уязвимости** выберите пункт **Уязвимости**.
3. Нажмите кнопку над списком уязвимостей.

   Отобразится список фильтров.
4. Выберите фильтр **Идентификатор бюллетеня** и в отобразившемся поле введите идентификатор.
5. Нажмите кнопку **Применить**.

   В списке отобразятся только уязвимости, с которыми связан бюллетень с указанным идентификатором.

Ссылка на бюллетень с указанным идентификатором содержится в карточке уязвимости в поле **Бюллетени**.

11.4. Поиск уязвимостей по названию или производителю ПО

Вы можете искать в базе данных уязвимости по названию или производителю ПО. Эта функция упрощает поиск в случаях, когда нужно быстро найти все уязвимости, относящиеся к одной программе или производителю, не указывая детальную информацию (например, конкретный патч или версию ПО).

► Чтобы найти в базе данных уязвимости по названию или производителю ПО:

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

   Отобразится страница со списком уязвимостей.
2. Нажмите кнопку над списком уязвимостей.

   Отобразится список фильтров.
3. Выберите фильтр **Производитель или наименование ПО** и в поле фильтра укажите значение, по которому нужно фильтровать уязвимости (например, название производителя ПО).
4. Нажмите кнопку **Применить**.
5. Если необходимо, укажите дополнительные фильтры для поиска уязвимостей.
6. Нажмите кнопку **Применить**.

В списке отобразятся найденные уязвимости, удовлетворяющие условиям фильтрации.

11.5. Фильтрация уязвимостей по базовой оценке CVSS

Вы можете фильтровать уязвимости в базе данных Knowledge Base по базовым оценкам CVSS 2 и (или) CVSS 3. Фильтрация позволяет быстро обнаруживать новые уязвимости, представляющие наибольшую опасность.

► Чтобы найти уязвимость по базовой оценке CVSS:

1. В главном меню выберите базу данных, в которой нужно искать уязвимость.
2. В главном меню в разделе **Уязвимости** выберите пункт **Уязвимости**.
3. Нажмите кнопку над списком уязвимостей.

   Отобразится список фильтров.
4. Выберите фильтр **CVSS** и в раскрывающемся списке фильтров выберите версию CVSS — **CVSS** 2 или **CVSS 3**.
5. В полях **От** и **До** задайте диапазон базовых оценок для отображения (от 0.0 до 10.0).
6. Нажмите кнопку **Применить**.

В списке отобразятся найденные уязвимости, удовлетворяющие условиям фильтрации.

11.6. Изменение параметров уязвимости

Вы можете добавлять, изменять и удалять из системы параметры уязвимости:

— идентификаторы уязвимости;

— ссылки на дополнительные источники информации об уязвимости;

— сведения об условиях существования и закрытия уязвимости.

В веб-интерфейсе системы параметры уязвимости отображаются в карточке уязвимости.

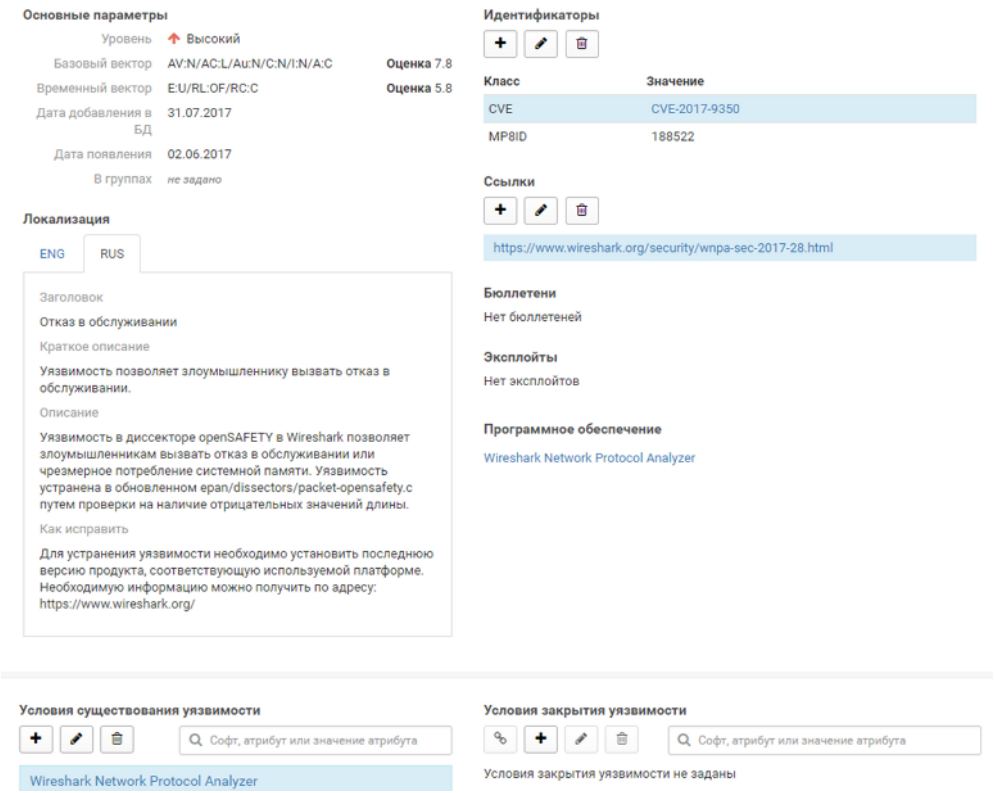

Рисунок 12. Карточка уязвимости

В этом разделе

11.6.1. Добавление идентификатора уязвимости

► Чтобы добавить идентификатор уязвимости:

1. В карточке уязвимости в блоке параметров **Идентификаторы** нажмите кнопку +.

   Откроется окно создания идентификатора уязвимости.

2. В раскрывающемся списке **Класс** выберите класс идентификатора и заполните поле **Значение**.

3. Нажмите кнопку **Сохранить**, чтобы добавить идентификатор и закрыть окно, или нажмите кнопку **Сохранить и добавить еще**, чтобы добавить новый идентификатор.

В результате в карточке уязвимости отобразится информация об идентификаторе с указанием класса и значения.

11.6.2. Добавление источников информации об уязвимостях

► Чтобы добавить ссылку на источник информации об уязвимости:

1. В карточке уязвимости в блоке параметров **Ссылки** нажмите кнопку [+].
2. Откроется окно создания ссылки.
3. Введите ссылку и при необходимости добавьте комментарий.
4. Нажмите кнопку **Сохранить**, чтобы добавить ссылку и закрыть окно, или нажмите кнопку **Сохранить и добавить еще**, чтобы добавить новую ссылку.

В результате в карточку уязвимости будет добавлена ссылка на источник информации об уязвимости.

11.6.3. Добавление условия существования уязвимости

Условие существования уязвимости содержит набор критериев, выполнение которых указывает на наличие уязвимости в системе. Условие существования включает атрибуты:

— Уязвимый компонент — ПО, содержащее уязвимость. При добавлении условия существования уязвимости нужно обязательно указать уязвимый компонент.

— Контекст существования уязвимости — ПО, не содержащее уязвимость, но необходимое для ее существования. Частным случаем контекста существования уязвимости является операционная система, на которой установлен уязвимый компонент. При добавлении условия существования уязвимости указывать контекст не обязательно.

Например, если уязвимость обнаружена в браузере Microsoft Internet Explorer 11 и эксплуатируется на компьютерах с установленной операционной системой Microsoft Windows 7 и выше, то уязвимым компонентом будет Microsoft Internet Explorer 11, а контекстом существования уязвимости — Microsoft Windows версии 7 и выше.

► Чтобы добавить условие существования уязвимости:

1. В карточке уязвимости в блоке параметров **Условие существования уязвимости** нажмите кнопку [+].

   Откроется окно создания условия.
2. В раскрывающемся списке **Уязвимые компоненты** выберите ПО, содержащее уязвимость.
3. Выберите свойство ПО (например, версию) в раскрывающемся списке.
4. Установите границы значений атрибута или создайте новые значения.

Примечание. Условием существования уязвимости может являться наличие нескольких уязвимых компонентов ПО. Чтобы указать несколько компонентов в рамках одного условия, нажмите кнопку **Добавить компонент**.

5. Нажмите кнопку **Добавить контекст**.
6. В раскрывающемся списке **Контекст существования уязвимости** выберите ПО.
7. В раскрывающемся списке **Свойства** выберите атрибут ПО (например, версию ПО).
8. Установите границы значений атрибута или создайте новые значения.
9. Если требуется, задайте несколько контекстов существования уязвимости по кнопке **Добавить контекст**.
10. Нажмите кнопку **Сохранить**.

Новое условие отобразится в списке.

11.6.4. Добавление условия закрытия уязвимости

Условие закрытия уязвимости содержит набор критериев, выполнение которых необходимо для устранения уязвимости. Условие закрытия включает следующие атрибуты:

— Компонент закрытия — ПО, которое необходимо установить для устранения уязвимости. При добавлении условия закрытия уязвимости нужно обязательно указать компонент закрытия.

— Контекст закрытия — ПО, необходимое для корректной работы компонента закрытия (например, операционная система). При установке такого ПО (например, новой версии операционной системы) свойства уязвимого актива могут существенно измениться. Поэтому ПО, указанное в контексте закрытия, не рекомендуется к обязательной установке. При добавлении условия закрытия уязвимости указывать контекст не обязательно.

Например, если уязвимый компонент — Microsoft Internet Explorer 11, контекст существования уязвимости — Microsoft Windows 7 и выше, то компонентом закрытия будет являться обновление операционной системы Microsoft Updates KB4056894, а контекстом закрытия (условием, при котором можно применять данное обновление) — операционная система Microsoft Windows 7 с пакетом обновлений Service Pack 1 (SP1).

► Чтобы создать условие закрытия уязвимости:

1. В карточке уязвимости в блоке параметров **Условия закрытия уязвимости** нажмите кнопку [+].

   Откроется окно создания условия.

2. Выберите ПО в раскрывающемся списке.
3. Выберите свойство ПО (например, версию) в раскрывающемся списке.

4. Установите границы значений атрибута ПО или создайте новые значения.

   Примечание. Условием закрытия уязвимости может являться наличие нескольких компонентов закрытия. Чтобы указать несколько компонентов в рамках одного условия, нажмите кнопку **Добавить компонент**.

5. Нажмите кнопку **Добавить контекст**.
6. Выберите ПО в раскрывающемся списке.
7. В раскрывающемся списке **Свойства** выберите атрибут ПО (например, версию ПО).
8. Установите границы значений атрибута или создайте новые значения.
9. Если требуется, задайте несколько контекстов закрытия уязвимости по кнопке **Добавить контекст**.
10. Нажмите кнопку **Сохранить**.

Новое условие отобразится в списке.

11.6.5. Установка связи между условиями существования и закрытия уязвимости

► Чтобы установить связь между условием существования уязвимости и условием закрытия уязвимости:

1. В карточке уязвимости нажмите на условие существования уязвимости в списке.

   Условие будет выделено синим цветом.

2. Нажмите на условие закрытия уязвимости в списке.

   Условие будет выделено синим цветом.

3. Нажмите кнопку .

   Цвет условия закрытия изменится на зеленый.

В результате выбранные условия существования и закрытия будут связаны.

При выборе условия существования все связанные условия закрытия выделяются зеленым цветом, и наоборот.

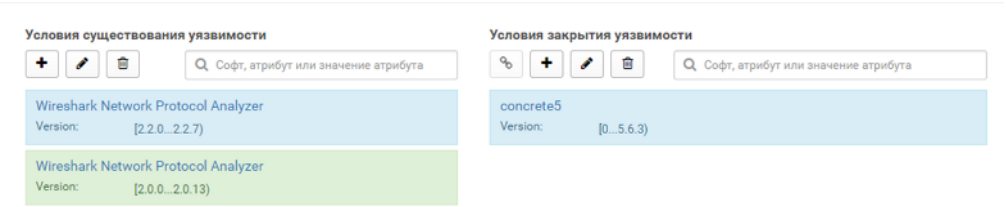

Рисунок 13. Условия существования и закрытия уязвимости

12. Бюллетени безопасности

Бюллетенем безопасности называют сообщение о наличии и исправлении уязвимостей в программном или аппаратном обеспечении, публикуемое производителем.

Knowledge Base содержит информацию о бюллетенях безопасности с указанием производителя, связанных уязвимостей и ПО, а также значений CVSS.

Система позволяет добавлять и удалять бюллетени, изменять параметры бюллетеня, указывать условия его существования и закрытия.

Информация о сигнатурах в выбранной базе данных отображается на странице **Бюллетени** (раздел главного меню **Уязвимости** → **Бюллетени**).

Объекты представлены в виде списка. По умолчанию отображаются все объекты в выбранной базе. Над списком находится строка быстрого поиска. Для поиска и отображения по набору признаков вы можете использовать настраиваемый фильтр. Фильтр доступен по кнопке над списком.

Вы можете настраивать отображение столбцов по кнопке в правой части списка.

Бюллетень может относиться к нескольким уязвимостям или программам. В этом случае рядом с названием бюллетеня отображается кнопка с количеством уязвимостей или программ. При нажатии на кнопку эти уязвимости или программы отображаются во всплывающем сообщении.

Для сортировки и поиска бюллетеней вы можете присваивать бюллетеням метки. Метка отображается в списке бюллетеней и на карточке бюллетеня.

Этот раздел содержит инструкции по работе с бюллетенями безопасности в интерфейсе системы.

В этом разделе

12.1. Добавление бюллетеня

Вы можете добавлять в систему бюллетени, указывая идентификатор, метку, дату публикации и дату обновления бюллетеня производителем.

► Чтобы добавить новый бюллетень:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.

   Примечание. Вы не можете вносить изменения в базу данных VM Content.

2. В главном меню выберите раздел **Бюллетени**.

   Откроется страница **Бюллетени**.

3. Нажмите кнопку **Создать**.

   Откроется форма создания бюллетеня.

4. Выберите производителя в раскрывающемся списке.
5. Введите значение идентификатора.
6. Выберите дату публикации бюллетеня в раскрывающемся календаре.

   Активируется поле **Обновлен производителем**.

7. Выберите дату обновления бюллетеня производителем.
8. При необходимости укажите метку бюллетеня.
9. Заполните поля в блоке параметров **Локализация**.

   Поле **Заголовок** является обязательным для заполнения.

10. Нажмите кнопку **Сохранить**.

В результате будет создан бюллетень безопасности с указанными параметрами и откроется карточка бюллетеня.

12.2. Карточка бюллетеня

В карточке бюллетеня вы можете добавлять, изменять и удалять следующую информацию:

— идентификаторы бюллетеня;

— ссылки на дополнительные источники информации;

— данные о связанных уязвимостях;

— условия существования и закрытия бюллетеня.

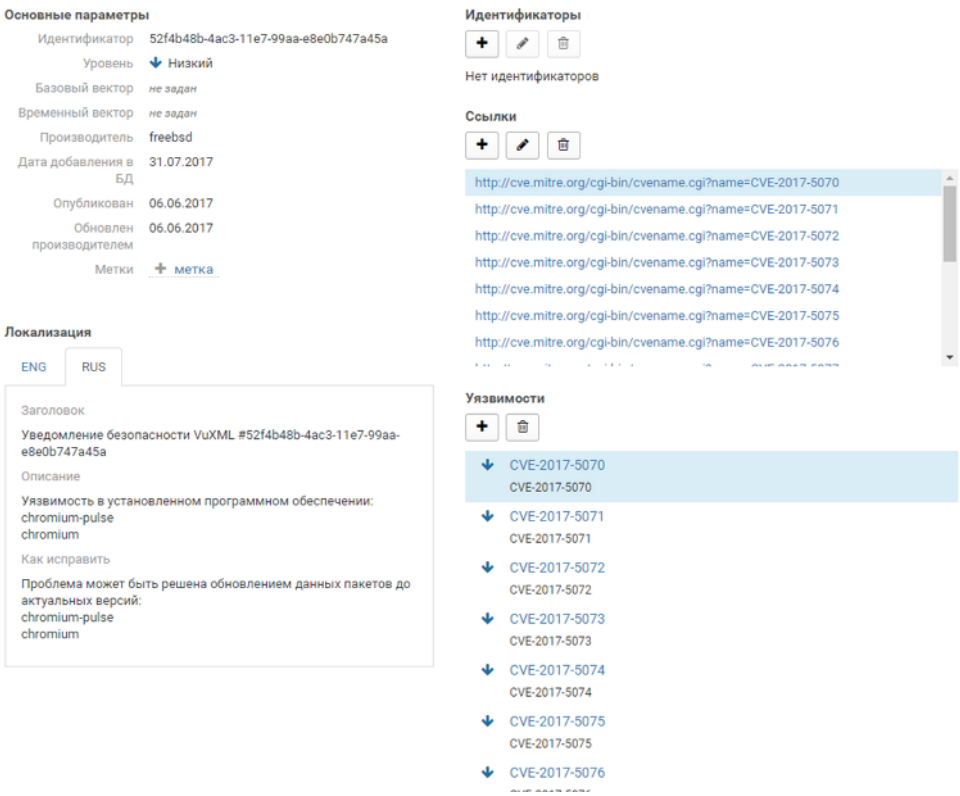

Рисунок 14. Карточка бюллетеня

В этом разделе

12.2.1. Добавление идентификатора бюллетеня

► Чтобы добавить идентификатор:

1. В карточке бюллетеня в блоке параметров **Идентификаторы** нажмите кнопку +.

Откроется окно создания идентификатора.

2. Выберите класс идентификатора в раскрывающемся списке и заполните поле **Значение**.
3. Нажмите кнопку **Сохранить**, чтобы добавить идентификатор и закрыть окно, или нажмите **Сохранить и добавить еще**, чтобы добавить новый идентификатор.

Идентификатор будет добавлен в карточку бюллетеня.

12.2.2. Добавление ссылок на дополнительные источники информации о бюллетене

► Чтобы добавить в карточку ссылку на дополнительный источник информации о бюллетене:

1. В карточке бюллетеня в блоке параметров **Ссылки** нажмите кнопку +.
2. Откроется окно создания ссылки.
3. В поле **URL** введите веб-адрес источника информации о бюллетене.
4. Нажмите **Сохранить**, чтобы добавить ссылку и закрыть окно, или нажмите **Сохранить и добавить еще**, чтобы добавить новую ссылку.

Ссылка на дополнительные источники информации будет добавлена в карточку бюллетеня.

12.2.3. Добавление информации о связанных с бюллетенем уязвимостях

► Чтобы добавить информацию о связанных уязвимостях:

1. В карточке бюллетеня в блоке параметров **Уязвимости** нажмите кнопку +.

   Откроется окно добавления связанных уязвимостей.
2. Выберите уязвимость в раскрывающемся списке.
3. Нажмите кнопку **Сохранить**.

Информация о связанной уязвимости будет добавлена в карточку бюллетеня.

12.2.4. Добавление условия существования бюллетеня

► Чтобы создать условие существования бюллетеня:

1. В карточке бюллетеня в блоке параметров **Условие существования бюллетеня** нажмите кнопку +.

Откроется окно создания условия.

2. В раскрывающемся списке **Уязвимые компоненты** выберите ПО.
3. Выберите свойство ПО (например, версию) в раскрывающемся списке.
4. Установите границы значений атрибута или создайте новые значения.

   Примечание. Условием существования бюллетеня может быть наличие нескольких установленных программ. Чтобы указать несколько программ в рамках одного условия, нажмите кнопку **Добавить компонент**.

5. Нажмите кнопку **Добавить контекст**.
6. Выберите ПО в раскрывающемся списке.
7. Выберите свойство ПО (например, версию) в раскрывающемся списке.
8. Установите границы значений атрибута или создайте новые значения.
9. Если требуется, задайте несколько контекстов существования бюллетеня по кнопке **Добавить компонент**.
10. Нажмите кнопку **Сохранить**.

Новое условие отобразится в списке.

12.2.5. Добавление условия закрытия бюллетеня

► Чтобы создать условие закрытия бюллетеня:

1. В карточке бюллетеня в блоке параметров **Условие закрытия бюллетеня** нажмите кнопку [+].

   Откроется окно создания условия.

2. Выберите ПО в раскрывающемся списке.
3. Выберите свойство ПО (например, версию) в раскрывающемся списке.
4. Установите границы значений атрибута или создайте новые значения.

   Примечание. Условием существования уязвимости может являться наличие нескольких уязвимых компонентов ПО. Чтобы указать несколько компонентов в рамках одного условия, нажмите кнопку **Добавить компонент**.

5. Нажмите кнопку **Добавить контекст**.
6. Выберите ПО в раскрывающемся списке.
7. В раскрывающемся списке **Свойства** выберите атрибут ПО (например, версию ПО).
8. Установите границы значений атрибута или создайте новые значения.

9. Если требуется, задайте несколько контекстов существования уязвимости по кнопке **Добавить контекст**.
10. Нажмите кнопку **Сохранить**.

Новое условие отобразится в списке.

12.2.6. Установка связи между условиями существования и закрытия бюллетеня

► Чтобы установить связь между условием существования бюллетеня и условием закрытия бюллетеня:

1. В карточке бюллетеня в списке условий существования бюллетеня нажмите условие.

   Условие будет выделено синим цветом.

2. В списке условий закрытия бюллетеня нажмите условие закрытия.

   Условие будет выделено синим цветом.

3. Нажмите кнопку .

   Цвет условия закрытия изменится на зеленый.

В результате выбранные условия существования и закрытия будут связаны.

При выборе условия существования все связанные условия закрытия выделяются зеленым цветом, и наоборот.

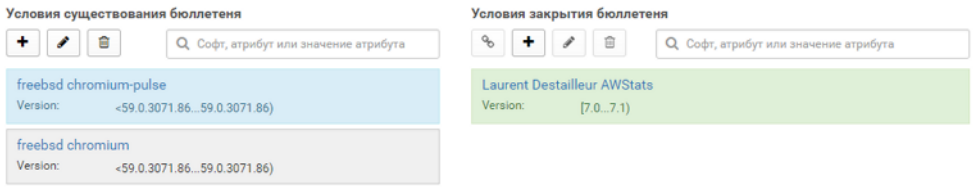

Рисунок 15. Просмотр условий существования и закрытия бюллетеня

13. Эксплойты

Эксплойт — фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на узлы сетевой инфраструктуры.

Knowledge Base может выступать хранилищем сведений об эксплойтах из разных источников. Информация о них заносится пользователем вручную либо через API.

Вы можете добавлять в систему новые эксплойты и изменять параметры эксплойтов.

Информация об эксплойтах в выбранной базе данных отображается на странице **Эксплойты** (раздел главного меню **Эксплойты**).

Объекты представлены в виде списка. По умолчанию отображаются все объекты в выбранной базе. Над списком находится строка быстрого поиска. Для поиска и отображения по набору признаков вы можете использовать настраиваемый фильтр. Фильтр доступен по кнопке над списком.

Вы можете настраивать отображение столбцов по кнопке в правой части списка.

Эксплойт может быть связан с уязвимостями, ПО и экспериментами. Количество связанных с эксплойтом объектов отображается рядом с названием эксплойта в виде кнопки с числом (например, 2). При нажатии на кнопку связанные с эксплойтом объекты отображаются во всплывающем сообщении.

В этом разделе

13.1. Добавление эксплойта

Вы можете добавлять в систему эксплойты. Для каждого эксплойта нужно указать идентификатор и его значение, а также базовый и временный векторы CVSS.

► Чтобы создать новый эксплойт:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.

   Примечание. Вы не можете вносить изменения в базу данных VM Content.

2. В главном меню выберите раздел **Эксплойты**.

   Откроется страница **Эксплойты**.

3. Нажмите кнопку **Создать**.

   Откроется форма создания нового эксплойта.

Уязвимость

Основные параметры

Идентификатор Canvas Введите идентификатор

Ранг Нет ранга

Дата публикации

Хранилище исходного кода

Внутреннее

Внешнее

Url внешнего либо внутреннего хранилища должен быть задан

Локализация

ENG RUS

Заголовок

Введите заголовок

Заголовок обязателен для хотя бы одной локали

Рисунок 16. Создание эксплойта

4. В раскрывающемся списке **Уязвимость** выберите уязвимость.
5. В раскрывающемся списке **Идентификатор** выберите идентификатор уязвимости.
6. Введите значение идентификатора, соответствующее его типу.
7. В раскрывающемся списке **Ранг** выберите ранг эксплойта.
8. В раскрывающемся календаре выберите дату публикации эксплойта.
9. Укажите ссылку внутреннего и (или) внешнего хранилища исходного кода.
10. Заполните поля в блоке параметров **Локализация**.

Поле **Заголовок** является обязательным для заполнения.

11. Нажмите кнопку **Сохранить**.

В результате будет создан эксплойт с указанными параметрами и откроется карточка эксплойта.

13.2. Карточка эксплойта

На карточке эксплойта вы можете добавлять, изменять и удалять информацию о связанных с эксплойтом уязвимостях, а также ссылки на дополнительные источники информации об эксплойтах.

Карточка эксплойта открывается по нажатию на название эксплойта в списке на странице **Эксплойты**.

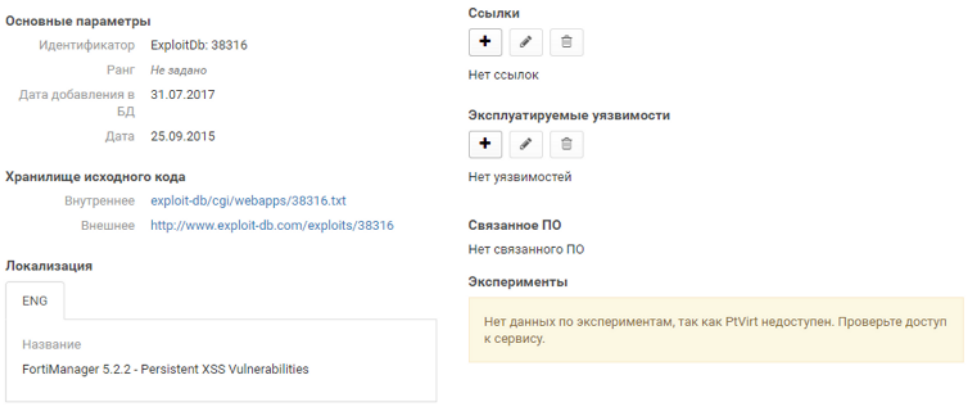

Рисунок 17. Карточка эксплойта

В этом разделе

13.2.1. Добавление дополнительных источников информации об эксплойтах

► Чтобы добавить ссылку на источник информации об эксплойте:

1. В карточке эксплойта в блоке параметров **Ссылки** нажмите кнопку +.
2. Откроется окно создания ссылки.

3. Введите веб-адрес источника информации и при необходимости добавьте комментарий.
4. Нажмите кнопку **Сохранить**, чтобы добавить ссылку и закрыть окно, или нажмите кнопку **Сохранить и добавить еще**, чтобы добавить новую ссылку.

Добавленные ссылки отобразятся в карточке эксплойта в блоке параметров **Ссылки**.

13.2.2. Добавление связанной с эксплойтом уязвимости

► Чтобы добавить уязвимость, связанную с эксплойтом:

1. В карточке эксплойта в блоке параметров **Эксплуатируемые уязвимости** нажмите кнопку [+].

   Откроется окно создания уязвимости.

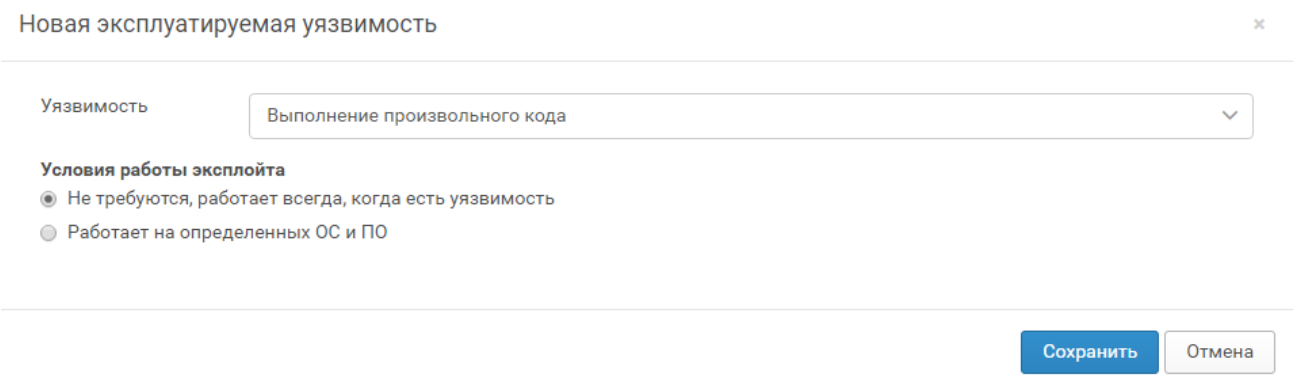

Рисунок 18. Добавление связанной уязвимости

2. Выберите уязвимость в раскрывающемся списке.

   Отобразится блок параметров **Условия работы эксплойта**.

3. Выберите условие работы эксплойта:

   • **Не требуются, работает всегда, когда есть уязвимость** — дополнительные условия не требуются. При выборе этого варианта переходите к последнему шагу данной инструкции.

   • **Работает на определенных ОС и ПО** — при выборе данного варианта отображаются инструменты для добавления условий работы эксплойта. Условие работы эксплойта можно выбрать из условий существования уязвимости или добавить новое.

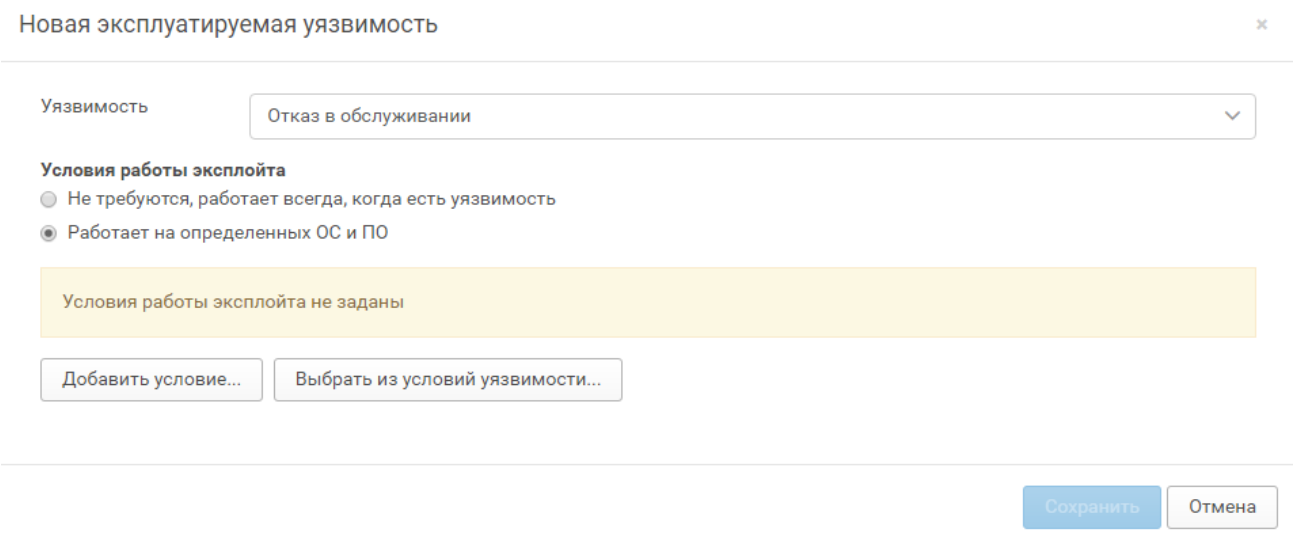

Рисунок 19. Выбор условий работы эксплойта

4. Для создания условия нажмите кнопку **Добавить условие**.

   Отобразится блок параметров **Новое условие работы**.

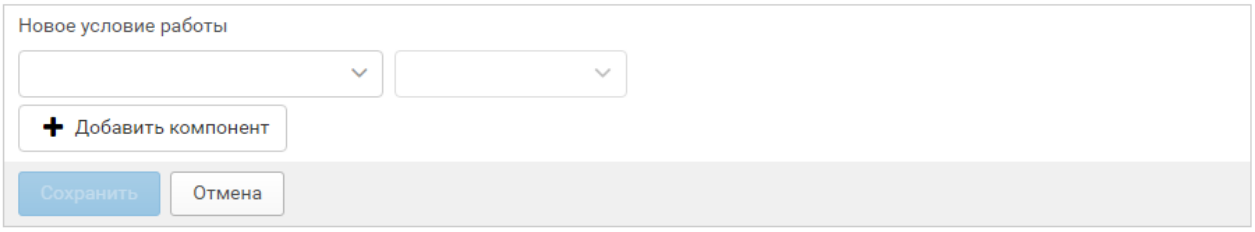

Рисунок 20. Добавление условий работы эксплойта

5. Выберите ПО в раскрывающемся списке.
6. Выберите свойство ПО (например, версию) в раскрывающемся списке.
7. Установите границы значений атрибута или создайте новые значения.
8. Если нужно добавить больше одного условия, нажмите кнопку **Добавить компонент**.
9. В блоке параметров **Новое условие работы** нажwмите кнопку **Сохранить**.
10. Чтобы выбрать условие работы эксплойта из условий существования уязвимости, нажмите кнопку **Выбрать из условий уязвимости**.

    Откроется окно **Выбрать условия из уязвимости**.

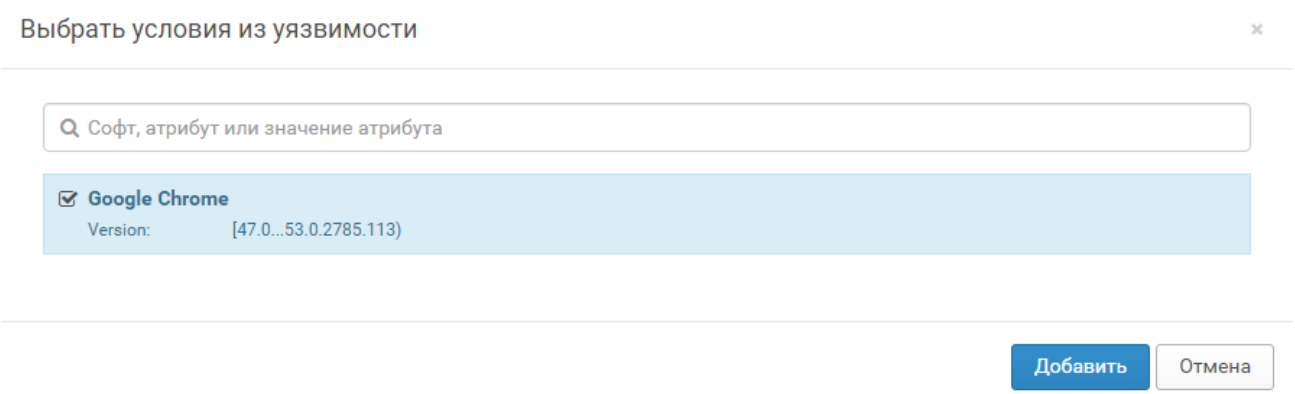

Рисунок 21. Выбор условия из уязвимости

11. Установите флажок напротив названия ПО, которое будет являться условием существования эксплойта, и нажмите кнопку **Добавить**.
12. Нажмите кнопку **Сохранить**.

Условия существования эксплойта отобразятся в карточке эксплойта.

14. Сигнатуры

Сигнатура — это формализованное описание признаков, по которым можно определить атаку посредством анализа сетевых пакетов.

Вы можете добавлять в Knowledge Base сигнатуры вручную и импортировать их в формате Snort, объединять сигнатуры в группы, выполнять поиск и фильтрацию сигнатур по разным критериям.

Система поддерживает версионирование сигнатур. На странице сигнатуры в системе (карточке сигнатуры) можно добавлять новые ревизии сигнатур из разных источников, а также указывать, какую ревизию сигнатуру и из какого источника использовать.

Информация о сигнатурах в выбранной базе данных отображается на странице **Сигнатуры** (раздел главного меню **Сигнатуры** → **Сигнатуры**).

Объекты представлены в виде списка. По умолчанию отображаются все объекты в выбранной базе. Над списком находится строка быстрого поиска. Для поиска и отображения по набору признаков вы можете использовать настраиваемый фильтр. Фильтр доступен по кнопке над списком.

Вы можете настраивать отображение столбцов по кнопке в правой части списка.

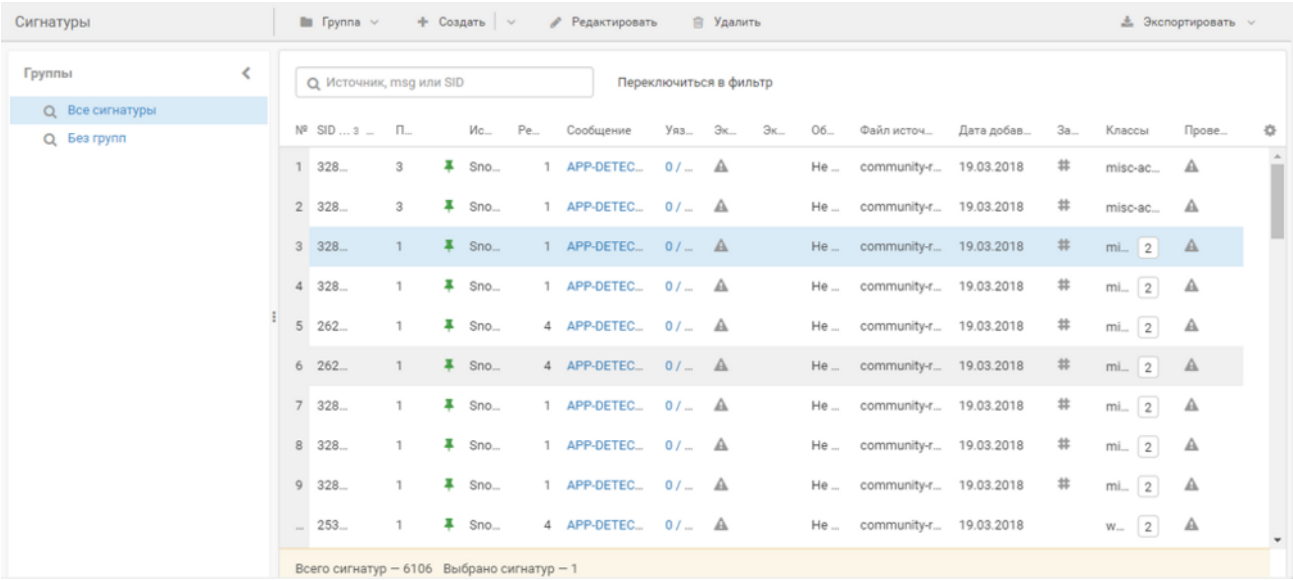

Рисунок 22. Просмотр списка сигнатур

В левой части страницы отображается панель **Группы** с группами сигнатур (см. раздел 14.5).

Панель инструментов над списком сигнатур содержит кнопки действий с группами сигнатур (**Группа**) и с отдельными сигнатурами (**Создать**, **Редактировать**, **Удалить**). По кнопке **Экспортировать** можно выполнить экспорт выбранных сигнатур в формате Snort или сенсоров.

Все ревизии сигнатуры сгруппированы в списке по ее SID / GIT. Используемые ревизии и источники сигнатур отмечены в списке сигнатур значком . Если используется не последняя ревизия сигнатуры (есть новые ревизии), рядом с сигнатурой в списке отображается значок .

Примечание. Сигнатуры в Центре автоматически поступают в базу данных For Robots от программ-роботов, установленных на отдельной виртуальной машине. Полученные сигнатуры путем слияния ревизий включаются в состав базы Master Центр и затем распространяются в Регионы в рамках процедуры обновления.

В этом разделе

См. также

14.1. Просмотр карточки сигнатуры

► Чтобы просмотреть карточку сигнатуры:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.
3. Выберите в списке сигнатуру, карточку которой нужно просмотреть.
4. По ссылке с названием сигнатуры откройте карточку сигнатуры.

APP-DETECT Absolute Software Computrace outbound connection - bh.namequery.com

Редактировать Удалить

SID/GID: 32847/

Группы

Стратегия использования

Использовать последнюю ревизию из фиксированного списка источников

Ревизии

Источник	Количество
Snort.Rules	1
1	

Сигнатура

```
# alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS
(msg:"APP-DETECT Absolute Software Computrace outbound
connection - bh.namequery.com";
flow:to_server,established; content:"Host|3A|
bh.namequery.com|0D 0A|"; fast_pattern:only;
http_header; content:"TagId: "; http_header;
metadata:policy security-ips drop, ruleset community,
service http;
reference:url,absolute.com/support/consumer/technology
_computrace; reference:url,www.blackhat.com/docs/us-
14/materials/us-14-Kamlyuk-Kamluk-Computrace-Backdoor-
Revisited.pdf;
reference:url,www.blackhat.com/presentations/bh-usa-
09/ORTEGA/BHUSA09-Ortega-DeactivateRootkit-PAPER.pdf;
classtype:misc-activity; sid:32847; rev:1;)
```

Основные параметры

Сообщение	APP-DETECT Absolute Software Computrace outbound connection - bh.namequery.com
Статус	закомментирована разработчиком
Объект атаки	Не определен
Приоритет	1
Дата добавления в БД	15.11.2017

Классы

misc-activity, test

Проверено Snort

Закомментировано

Уязвимости

Нет уязвимостей

Эксплойты

Нет эксплойтов

Ссылки

http://www.blackhat.com/docs/us-14/materials/us-14-Kamlyuk-Kamlu...
http://absolute.com/support/consumer/technology_computrace
http://www.blackhat.com/presentations/bh-usa-09/ORTEGA/BHUSA09...

Эксперименты

Нет экспериментов

Локализация

Нет локализаций

Рисунок 23. Просмотр карточки сигнатуры

Карточка сигнатуры состоит из трех панелей. В левой панели вы можете перемещать сигнатуру в другие группы, просматривать ревизии и выбирать, какую ревизию и из какого источника использовать. В центральной панели отображается тело сигнатуры выбранной ревизии. Вы можете копировать тело сигнатуры по кнопке и загружать его по кнопке в локальную папку для загрузки, указанную в свойствах браузера. В правой панели вы можете просматривать основные параметры сигнатуры, а также добавлять или удалять уязвимости и эксплойты, связанные с сигнатурой.

В панели инструментов отображаются кнопки **Редактировать** и **Удалить**. По кнопке **Редактировать** вы можете редактировать выбранную ревизию сигнатуры или создать новую ревизию. По кнопке **Удалить** вы можете удалить выбранную ревизию сигнатуры.

В этом разделе

14.1.1. Просмотр ревизии сигнатуры и установка ревизии как используемой

► Чтобы просмотреть ревизии сигнатуры и установить ревизию сигнатуры как используемую:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.
3. По ссылке с названием сигнатуры откройте карточку сигнатуры.
4. В панели **Ревизии** выберите ревизию сигнатуры, которую вы хотите просмотреть.

   В панели **Сигнатура** отобразится ревизия сигнатуры.
5. По ссылке **<Стратегия использования>** выберите стратегию использования ревизий сигнатуры. При появлении новых ревизий сигнатуры к ним применяется выбранная стратегия:

- **Использовать последнюю ревизию из любого источника** — используется последняя ревизия сигнатуры из всех источников. При появлении новой ревизии сигнатуры из любого источника новая ревизия становится используемой.
- **Использовать последнюю ревизию из фиксированного источника** — используется последняя ревизия сигнатуры из выбранных источников сигнатур. Вы можете выбрать несколько источников. Если появилась новая ревизия сигнатуры из выбранного источника, эта ревизия становится используемой. Если появилась новая ревизия сигнатуры из другого источника, продолжает использоваться последняя ревизия из выбранного источника. Стратегия выбрана по умолчанию.
- **Использовать зафиксированную ревизию** — используется выбранная ревизия сигнатуры из выбранного источника. Ревизия продолжает использоваться при появлении новых ревизий сигнатуры из любых источников — пока оператор не выберет другую ревизию или не изменит стратегию использования.

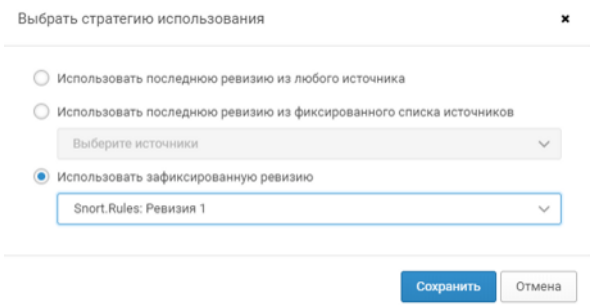

Рисунок 24. Выбор стратегии использования ревизии

6. Нажмите кнопку **Сохранить**.

Ревизия сигнатуры установлена как используемая.

14.1.2. Добавление связанного с сигнатурой эксплойта

► Чтобы добавить связанный с сигнатурой эксплойт:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.
3. По ссылке с названием сигнатуры откройте карточку сигнатуры.
4. В блоке параметров **Эксплойты** нажмите кнопку [+].

   Откроется окно **Новый связанный эксплойт**.
5. В раскрывающемся списке выберите эксплойт.
6. Нажмите кнопку **Сохранить**.

Эксплойт добавлен в карточку сигнатуры.

14.1.3. Добавление связанной с сигнатурой уязвимости

► Чтобы добавить связанную с сигнатурой уязвимость:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.
3. По ссылке с названием сигнатуры откройте карточку сигнатуры.
4. В блоке параметров **Уязвимости** нажмите кнопку [+].

   Откроется окно **Новая связанная уязвимость**.
5. В раскрывающемся списке **Уязвимость** выберите уязвимость, которую нужно связать с сигнатурой.

   Примечание. Раскрывающийся список снабжен строкой поиска. Вы можете искать уязвимость по ее CVE (запись в базе Common Vulnerabilities and Exposures), либо по заголовку (если заголовок отличается от CVE).
6. Нажмите кнопку **Сохранить**.

Уязвимость добавлена в карточку сигнатуры.

14.1.4. Изменение параметров сигнатуры

Вы можете изменять источник и тело сигнатуры, а также другие основные параметры и описание сигнатуры на русском и английском языках.

► Чтобы изменить параметры сигнатуры:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.
3. По ссылке с названием сигнатуры откройте карточку сигнатуры.
4. В панели **Ревизии** выберите ревизию сигнатуры, которую вы хотите изменить.

   В панели **Сигнатура** отобразится ревизия сигнатуры.
5. В панели инструментов нажмите кнопку **Редактировать**.

   Откроется окно **Редактирование сигнатуры**.

Основные параметры

Источник: Snort.Rules

Файл источника: community-rules/community.rules

Объект атаки: Не определен

Классы

Значение:

```
# alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"APP-DETECT
Absolute Software Computrace outbound connection - 209.53.113.223";
flow:to_server,established; content:"Host|3A| 209.53.113.223|0D 0A|";
fast_pattern:only; http_header; content:"TagId: "; http_header;
metadata:policy security-ips drop, ruleset community, service http;
reference:url,absolute.com/support/consumer/technology_computrace;
reference:url,www.blackhat.com/docs/us-14/materials/us-14-Kamlyuk-Kamluk-
Computrace-Backdoor-Revisited.pdf;
reference:url,www.blackhat.com/presentations/bh-usa-09/ORTEGA/BHUSA09-
Ortega-DeactivateRootkit-PAPER.pdf; classtype:misc-activity; sid:32845;
rev:1;)
```

Рассчитанная информация

Сообщение: APP-DETECT Absolute Software Computrace outbound connection - 209.53.113.223

SID: 32845

Ревизия: 1

Ссылки:
http://www.blackhat.com/docs/us-14/materials/us-14-Kamlyuk-Kamluk-Computrace-Backdoor-Revisited.pdf
http://www.blackhat.com/presentations/bh-usa-09/ORTEGA/BHUSA09-Ortega-DeactivateRootkit-PAPER.pdf
http://absolute.com/support/consumer/technology_computrace

Закомментирована разработчиком

Рисунок 25. Изменение параметров сигнатуры

6. Измените необходимые параметры.

   Примечание. При изменении источника или номера ревизии сигнатуры, система предлагает сохранить изменения как новую ревизию сигнатуры (отображается кнопка **Сохранить как новую ревизию**).

7. Включите или отключите видимость сигнатуры для других систем переключателем **Закомментирована разработчиком**.

   Примечание. Вы можете экспортировать сигнатуры из Knowledge Base и импортировать их в другие системы. Признаки закомментированных разработчиком сигнатур не будут определяться другими системами. Закомментированные сигнатуры также исключаются из проверки на соответствие формату Snort.

8. Нажмите кнопку **Сохранить**.

Будут сохранены изменения в текущей ревизии сигнатуры.

Параметры сигнатуры изменены.

14.1.5. Создание ревизии сигнатуры

Все ревизии сигнатуры сгруппированы в списке сигнатур по ее SID / GIT. Вы можете создавать новые ревизии сигнатуры, изменяя источник сигнатуры или номер ревизии в теле сигнатуры.

► Чтобы создать ревизию сигнатуры:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.
3. По ссылке с названием сигнатуры откройте карточку сигнатуры.
4. В панели инструментов нажмите кнопку **Редактировать**.
5. Если требуется, в поле **Значение** внесите необходимые изменения.
6. Измените источник сигнатуры в поле **Источник** или номер ревизии сигнатуры в теле сигнатуры.
7. Нажмите кнопку **Сохранить как новую ревизию**.

Новая ревизия сигнатуры создана.

14.2. Импорт сигнатур

Вы можете импортировать в систему сигнатуры в формате Snort. Система поддерживает импорт сигнатур в архивах форматов ZIP, TAR или TGZ.

► Чтобы импортировать сигнатуры:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.
3. В панели **Группы** выберите группу, в которую вы хотите импортировать сигнатуры.
4. В меню кнопки **Создать** выберите **Импортировать сигнатуры из файла**.

   Откроется окно **Импорт сигнатур**.

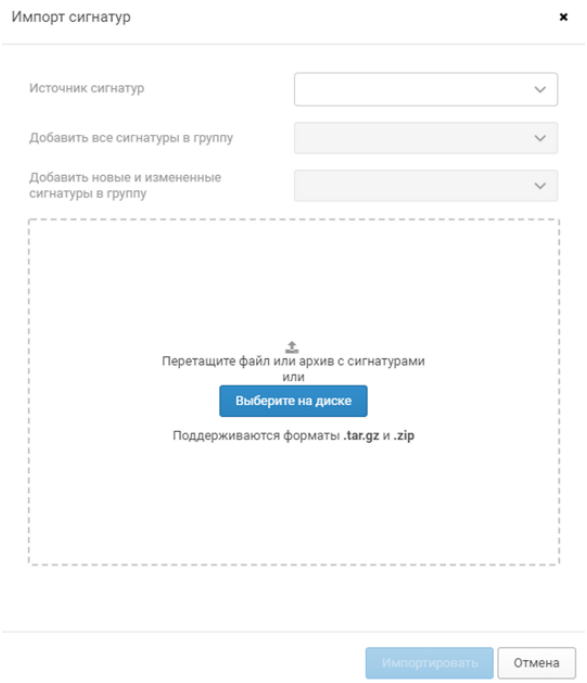

Рисунок 26. Импорт сигнатур

5. Заполните поле **Источник сигнатур**:
   - выберите источник в раскрывающемся списке.
   - если источник отсутствует в списке, введите новое название источника и нажмите кнопку **Создать источник сигнатур**.
6. В раскрывающемся списке **Добавить все сигнатуры в группу** выберите группу, в которую будут отнесены все импортируемые сигнатуры.
7. В раскрывающемся списке **Добавить новые сигнатуры в группу** выберите группу, в которую будут добавлены только новые сигнатуры (среди всех импортируемых).

   К новым относятся сигнатуры, которые имеют новый SID / GID, либо являются новыми ревизиями сигнатур с существующими в базе SID / GID. При импорте Knowledge Base сравнивает импортируемые сигнатуры с имеющимися в базе данных и распределяет новые в соответствующую группу. Группы являются фильтрами для сигнатур. Поэтому новые сигнатуры оказываются и в группе, выбранной для импорта всех сигнатур, и в группе только для новых сигнатур.

   Примечание. Функция добавления новых сигнатур в отдельную группу особенно полезна при одномоментном импорте большого количества сигнатур, среди которых есть и уже имеющиеся в базе данных, и новые сигнатуры. После импорта вы можете сразу перейти к просмотру новых сигнатур, не тратя время на их поиск и распределение по группам вручную.
8. Нажмите кнопку **Выберите на диске** и укажите путь к файлу для импорта.

В нижней части окна **Импорт сигнатур** отобразится список файлов, содержащихся в архиве. Флажки будут автоматически установлены напротив файлов с сигнатурами.

9. Нажмите кнопку **Импортировать**.

   Откроется страница **Журнал импорта**. В списке **Операции** появится новая строка с указанием даты, инициатора и значка статуса импорта (— импорт без ошибок; — импорт с ошибками).

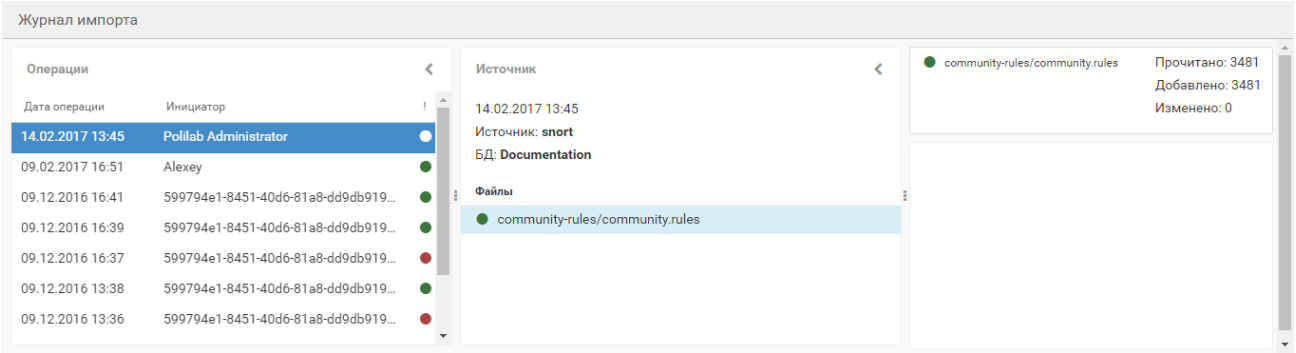

Рисунок 27. Просмотр журнала импорта

Сигнатуры импортированы в систему.

14.3. Экспорт сигнатур

► Чтобы экспортировать сигнатуры:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.
3. Выберите в списке одну или несколько сигнатур.
4. В панели инструментов нажмите кнопку **Экспортировать** и в раскрывающемся меню выберите один из предложенных вариантов экспорта.

Выбранные сигнатуры сохранены локально в виде архива (расположение сохраненных файлов зависит от параметров вашего браузера).

14.4. Создание сигнатуры

Вы можете добавлять в систему сигнатуры, указывая источник, объект атаки, классы сигнатур и их значение.

► Чтобы создать новую сигнатуру:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.

Примечание. Вы не можете вносить изменения в базу данных VM Content.

2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.

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

   Откроется окно **Создание сигнатуры**.

4. В раскрывающемся списке **Источник** выберите или введите название источника сигнатуры.

   Примечание. Если вы ввели название источника сигнатуры, источник будет добавлен в список источников выбранной базы данных.

5. В раскрывающемся списке **Файл источника** выберите или введите название файла источника сигнатуры.

   Примечание. Если вы ввели название файла источника сигнатуры, файл будет добавлен в список файлов источников выбранной базы данных.

6. В раскрывающемся списке **Объект атаки** выберите объект атаки.
7. В раскрывающемся списке выберите классы сигнатур.
8. Укажите группы, в которые вы хотите добавить сигнатуру.
9. В поле **Значение** введите значение сигнатуры.

   На основании введенных данных будет заполнен блок параметров **Рассчитанная информация**.

10. При необходимости введите описание сигнатуры в блоке параметров **Локализация**.
11. Нажмите кнопку **Сохранить**.

Сигнатура создана.

14.5. Работа с группами сигнатур

В веб-интерфейсе системы для удобства работы с сигнатурами предусмотрена фильтрация сигнатур по группам. Вы можете создавать группы и помещать в них сигнатуры. Одна сигнатура может входить в несколько групп. По умолчанию система содержит две группы сигнатур: **Новые** и **Рекомендованные к использованию**.

В группу **Новые** в Центре автоматически включаются новые сигнатуры, полученные от программ-роботов. При импорте сигнатур (см. раздел 14.2) также можно настроить включение новых сигнатур в группу **Новые**. К новым относятся сигнатуры, которые имеют новый SID / GID, либо являются новыми ревизиями сигнатур с существующими в базе SID / GID.

В этом разделе

Изменение параметров группы сигнатур (см. раздел 14.5.3)

Удаление группы сигнатур (см. раздел 14.5.4)

14.5.1. Создание группы сигнатур

► Чтобы создать группу сигнатур:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.
3. В панели инструментов в меню кнопки **Группа** выберите **Создать группу**.

   Откроется окно **Новая группа**.
4. В поле **Идентификатор** введите идентификатор группы сигнатур.
5. Если вы хотите сделать создаваемую группу дочерней, в поле **Родительская группа** выберите родительскую группу.
6. Если требуется, в блоке параметров **Локализация** введите название группы.
7. Нажмите кнопку **Создать**.

Группа сигнатур создана.

14.5.2. Добавление сигнатур в группу

Вы можете добавить в группу одну сигнатуру или несколько сигнатур одновременно.

► Чтобы добавить сигнатуру в группу:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.
3. По ссылке с названием сигнатуры откройте карточку сигнатуры.
4. В левой панели по ссылке **Группы** выберите группу, в которую вы хотите добавить сигнатуру.
5. Нажмите кнопку **Сохранить**.

Сигнатура добавлена в группу.

► Чтобы добавить несколько сигнатур в группу:

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

Откроется страница **Сигнатуры**.

2. Удерживая нажатой клавишу Ctrl, в списке сигнатур выберите несколько сигнатур, которые необходимо добавить в группу.
3. Нажмите кнопку **Редактировать**.

   Откроется окно **Массовые операции**.
4. В раскрывающемся списке **Выберите операцию** выберите **Группы сигнатур**.
5. В раскрывающемся списке **Группы сигнатур** выберите группы, в которые необходимо добавить сигнатуры.

   Примечание. Флажки ☑ установлены напротив групп, которые содержат все выбранные сигнатуры. Флажки ▬ установлены напротив групп, которые содержат только часть выбранных сигнатур. Чтобы переместить выбранные сигнатуры в группу, установите флажок ☑ напротив нее. Чтобы удалить выбранные сигнатуры из группы, снимите флажок напротив нее.
6. Нажмите кнопку **Сохранить**.

Сигнатуры добавлены в группу.

14.5.3. Изменение параметров группы сигнатур

► Чтобы изменить параметры группы сигнатур:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.
3. В панели **Группы** выберите группу, параметры которой вы хотите изменить.
4. В панели инструментов нажмите кнопку **Группа** и в раскрывшемся меню выберите **Редактировать группу**.

   Откроется окно **Редактирование группы**.

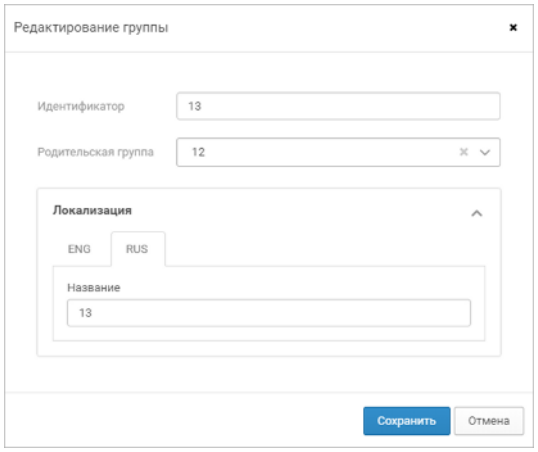

Рисунок 28. Изменение параметров группы сигнатур

5. Если требуется, в поле **Идентификатор** измените идентификатор группы.
6. Если требуется, в раскрывающемся списке **Родительская группа** измените расположение группы в структуре групп.
7. Если требуется, в блоке параметров **Локализация** измените название группы.
8. Нажмите кнопку **Сохранить**.

Параметры группы сигнатур изменены.

14.5.4. Удаление группы сигнатур

► Чтобы удалить группу сигнатур:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.
3. В панели **Группы** выберите группу, которую вы хотите удалить.
4. В панели инструментов нажмите кнопку **Группа**, в раскрывшемся меню выберите **Удалить группу** и подтвердите удаление группы.

   Примечание. При удалении группы входящие в нее сигнатуры удалены не будут.

Группа сигнатур удалена.

14.6. Фильтрация сигнатур

С помощью фильтрации вы можете настраивать отображение только тех сигнатур в списке, которые соответствуют определенному критерию, например, имеют один и тот же приоритет или класс.

► Чтобы выполнить фильтрацию сигнатур:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.
3. Нажмите кнопку над списком сигнатур.

   Отобразится список фильтров.
4. Выберите фильтр и в отобразившемся поле введите значение параметра.
5. Нажмите кнопку **Применить**.

В списке отобразятся объекты.

14.7. Поиск сигнатур по регулярным выражениям

► Чтобы искать сигнатуры по регулярным выражениям:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.
3. Нажмите кнопку над списком сигнатур.

   Отобразится список фильтров.
4. Выберите фильтр **Регулярное выражение** и в поле поиска введите регулярное выражение.

   Например, для поиска сигнатур, номера ревизий которых начинаются с цифр 3 и 4, введите в поле выражение `rev:[43]`.

   Примечание. Поиск по регулярному выражению производится в теле сигнатуры. При создании регулярных выражений для поиска учитывайте особенности содержания сигнатур и синтаксиса регулярных выражений. Например, поиск по регулярному выражению `^rev:[43]` не даст результатов, так как символ «^» указывает на то, что совпадение выражения с текстом сигнатуры должно быть в начале строки, а искомое значение (ревизия) находится в конце тела сигнатуры. Вы можете ознакомиться с синтаксисом и примерами регулярных выражений на сайте документации компании Microsoft.
5. Нажмите кнопку **Применить**.

   В списке отобразятся только сигнатуры, соответствующие регулярному выражению. Если регулярное выражение содержит ошибку, в верхней части страницы отобразится уведомление о ней.

Кнопка с активным фильтром по регулярному выражению выделяется цветом. Вы можете сбросить результаты поиска и вернуться к общему списку сигнатур по кнопке **Сбросить** в правой части страницы.

14.8. Работа с конфигурациями IDS

Пткб может выступать редактором и хранилищем конфигураций IDS. Конфигурации IDS с набором сигнатур можно выгрузить в IDS через экспорт.

В этом разделе

14.8.1. Добавление файла конфигурации IDS

► Чтобы добавить файл конфигурации IDS:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Файлы конфигурации IDS**.
3. На открывшейся странице в панели инструментов нажмите кнопку **Создать**.

   Откроется страница создания файла конфигурации IDS.
4. В поле **Название** укажите название файла конфигурации, отражающее его назначение, например, «Конфигурация по умолчанию».

   В системе можно создавать файлы конфигурации с одинаковыми именами. В имени допустимо использовать любые символы.
5. В поле **Путь при выгрузке** укажите путь, по которому файл будет выгружаться при выгрузке набора сигнатур.

   По умолчанию задан как `snort.conf` для IDS Snort и `suricata.yaml` для IDS Suricata.

   Допустимо существование в системе нескольких файлов с одинаковыми путями выгрузки для использования в разных группах.
6. В поле **Описание** укажите особенности файла, существенные отличия его от других или оставьте комментарий.
7. В поле **Файл конфигурации** перетащите файл, выберите его по ссылке **Выбрать** или вставьте его текст.

Система определит тип IDS для файла. По умолчанию файлам формата YAML соответствует Suricata, прочим файлам соответствует Snort. Если тип IDS для файла был определен неправильно, выберите его вручную по кнопке **Snort** или **Suricata**.

8. Нажмите кнопку **Сохранить**.

Файл конфигурации IDS добавлен.

14.8.2. Создание конфигурации IDS для группы сигнатур

► Чтобы создать конфигурацию IDS для группы сигнатур:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.
3. В панели **Группы** выберите группу сигнатур, которую нужно валидировать.
4. В рабочей области выберите вкладку **Конфигурация IDS**.
5. Нажмите кнопку **Создать конфигурацию**.

   Откроется страница создания конфигурации IDS.
6. В поле **Название** укажите название конфигурации, которое будет отображаться в интерфейсе.
7. В поле **Конфигурационные файлы** добавьте файлы конфигурации IDS, которые должны входить в состав конфигурации.

   Вы можете выбрать файлы конфигурации, добавленные в Knowledge Base ранее, либо создать новый файл.
8. Из добавленных файлов конфигурации выберите стартовый файл.

   Если конфигурация состоит из одного файла, он назначается стартовым автоматически. В одной конфигурации могут присутствовать файлы конфигурации Snort и Suricata.
9. Если необходимо, в поле **Путь к IDS** укажите путь к исполняемому файлу IDS на выбранной машине.
10. Если необходимо, в поле **Параметры запуска** введите укажите дополнительные параметры, с которыми IDS должна запускаться при старте валидации.
11. Нажмите кнопку **Создать**.

Конфигурация IDS для группы сигнатур создана.

Новая конфигурация отображается на странице **Сигнатуры** на вкладке **Конфигурация IDS**.

14.8.3. Экспорт набора сигнатур в формате IDS

Вы можете экспортировать набор сигнатур в формате IDS (Snort или Suricata) как вместе с файлами конфигурации, так и без них.

► Чтобы экспортировать набор сигнатур с файлами конфигурации IDS:

1. В главном меню Knowledge Base в раскрывающемся списке баз данных выберите нужную вам базу.
2. В главном меню в разделе **Сигнатуры** выберите пункт **Сигнатуры**.

   Откроется страница **Сигнатуры**.
3. Выберите группу с сигнатурами, которые нужно экспортировать.
4. На вкладке **Конфигурация IDS** выберите конфигурацию, которую нужно экспортировать вместе с набором сигнатур.
5. Нажмите кнопку **Экспортировать**.

   В папку для загрузки будет экспортирован архив вида `<число>_<месяц>_<год>_Signatures.zip`. Архив содержит папку с сигнатурами в формате соответствующей IDS и файлы конфигурации.

Экспорт сигнатур в формате IDS с файлами конфигурации завершен.

► Чтобы экспортировать набор сигнатур в формате IDS без файлов конфигурации:

1. Выберите группу с сигнатурами, которые нужно экспортировать.
2. Выберите вкладку **Сигнатуры**.
3. Нажмите кнопку **Экспортировать**.
4. В открывшемся меню выберите **Все <количество сигнатур> в формате IDS**.

   В папку для загрузки будет экспортирован архив вида `<число>_<месяц>_<год>_Signatures.zip`. Архив содержит папку с сигнатурами в формате соответствующей IDS.

Экспорт сигнатур в формате IDS без файлов конфигурации завершен.

О компании

"Позитив Текнолоджиз" уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявить, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга "Эксперт-400".

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com