SOLAR

Солар Программный Комплекс Обнаружения и Реагирования

Руководство системного администратора

МОСКВА, 2024

Содержание

Список иллюстраций

Список таблиц

1. Перечень терминов и сокращений

АРМ	Автоматизированное рабочее место
БД	База данных
БРП	База решающих правил
ИБ	Информационная безопасность – безопасность, связанная с угрозами в информационной сфере
Инцидент ИБ	Непредвиденное или нежелательное событие (группа событий) ИБ, которое привело (могут привести) к нарушению функционирования информационного ресурса или возникновению угроз безопасности информации или нарушению требований по защите информации
Модуль	Программный компонент, выполняющий некоторое количество связанных между собой функций
ОС	Операционная система – специальный набор программ, благодаря которому все системы устройства взаимодействуют между собой и с пользователем
ПО	Программное обеспечение
Политика безопасности	Совокупность правил, регулирующих управление, защиту и распределение информационных ресурсов, контролируемых ПО
СЗИ	Средства защиты информации
Событие ИБ	Событие информационной безопасности – зафиксированное состояние информационной (автоматизированной) системы, сетевого, телекоммуникационного, коммуникационного, иного прикладного сервиса или информационно-телекоммуникационной сети, указывающее на возможное нарушение безопасности информации, сбой СЗИ, или ситуацию, которая может быть значимой для безопасности информации
СОВ	Система обнаружения вторжений – программное или программно-техническое средство, реализующее функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней
Сокет	socket – название программного интерфейса для обеспечения обмена данными между процессами. Процессы при таком обмене могут исполняться как на одной ЭВМ, так и на различных ЭВМ, связанных между собой только сетью. Сокет — абстрактный объект, представляющий конечную точку соединения
СУБД	Система управления базами данных
СХД	Система хранения данных
ФС	Файловая система
Хост	Добавленный в систему объект защиты (узел сети, компьютер или сетевое устройство)
ADAM	Authentication, Deployment and Monitoring – компонент, предназначенный для подтверждения легитимности агента, начального раз-

	вертывания и обновления, а также независимого мониторинга состояния других компонентов
EDR	Endpoint Detection & Response – класс решений для обнаружения целевых атак и сложных угроз на конечных точках (серверах, устройствах, подключенных к сети рабочих станциях и т. д.), способный оперативно реагировать на найденные инциденты
LUA	Процедурный динамически типизированный модульный язык с автоматическим управлением памятью. Включает базовые элементы для поддержки функционального и объектного стилей программирования. Таким образом, LUA можно называть мультипарадигменным языком. Встроенные средства параллельного программирования позволяют писать многопоточные программы только средствами языка, не обращаясь к API операционной системы или внешним библиотекам
NTA	Network Traffic Analyzer – класс решений для комплексного анализа всего сетевого трафика, передаваемого/циркулирующего во внутренней сети предприятия в режиме реального времени
SIEM	Security information and event management – класс решений для сбора и анализа информации о событиях информационной безопасности
SOC	Security Operations Center – центр мониторинга и реагирования на инциденты информационной безопасности
Solar EDR	Solar Endpoint Detection and Response – компонент, предназначенный для обнаружения и реагирования на киберугрозы на конечных точках. Конечной точкой может быть рабочая станция и/или сервер
Solar NTA	Solar Network Traffic Analysis – компонент, предназначенный для обнаружения как известных, так и неизвестных угроз безопасности в сетевом трафике во всей сети, либо в отдельных сегментах сети организации путём его захвата и анализа с помощью различных механизмов/технологий в режиме, приближенном к реальному времени

2. Введение

В настоящем руководстве описаны задачи, возникающие при эксплуатации и сопровождении Программного Комплекса Обнаружения и Реагирования (далее – Солар ПКОиР), а также способы и примеры их решения.

Документ предназначен для администраторов СЗИ, обеспечивающих устойчивое функционирование Солар ПКОиР.

2.1. Область применения

Солар ПКОиР – это комплекс программных средств, объединяющий средства защиты информации и технологии анализа данных в единый продукт, обеспечивающий консолидацию и обогащение собираемой информации для эффективного обнаружения, обработки, расследования и реагирования на киберугрозы.

Базовыми компонентами системы, которые предоставляют информацию о событиях на уровне конечных точек и сети, являются Solar EDR и Solar NTA соответственно.

2.2. Краткое описание возможностей

К основным целевым функциональным возможностям Солар ПКОиР относятся:

- предоставление информации об атаках и помощь в принятии решений;
- обнаружение атак, сбор и связывание событий с конечных устройств, систем ИБ для формирования общего контекста;
- выявление вредоносных программ, зараженных устройств, действий злоумышленников в защищаемой сети;
- объединение функций анализа событий из разных систем в едином интерфейсе;
- упорядочивание и координация процесса реагирования на основании консолидированных событий из разных источников;
- автоматизация реагирования на инциденты информационной безопасности.

В работе Солар ПКОиР можно выделить следующие основные этапы:

1. Сбор сетевого трафика и данных с конечных узлов.
2. Контекстный и контентный анализ собранных данных, обогащение событий, определение инцидентов, построение цепочки атаки.
3. Принятие мер по предотвращению атак / реагированию на атаки.
4. Формирование отчетов.

2.3. Перечень эксплуатационной документации для ознакомления

Пользователю Солар ПКОиР рекомендуется ознакомиться со следующими эксплуатационными документами:

- *Руководство администратора безопасности*,

- *Руководство системного администратора* (настоящий документ)[1] – содержит описание процедур установки и эксплуатации Солар ПКОиР.

2.4. Требования к АРМ администратора

Требования к аппаратному обеспечению

АРМ системного администратора Солар ПКОиР должно быть оборудовано персональным компьютером с подключением к сети Интернет, с одним или несколькими мониторами с разрешением экрана при работе с веб-интерфейсом Солар ПКОиР от 1920x1080.

Требования к программного обеспечению

Для настройки и работы с системой через веб-интерфейс на АРМ должен быть установлен один из следующих браузеров актуальной версии:

- Google Chrome;
- Mozilla Firefox;
- Microsoft Edge.

2.5. Исполнения Солар ПКОиР

Программный комплекс обнаружения и реагирования представлен в трех исполнениях:

- Исполнение 1: Система обнаружения вторжений уровня сети и узла (реализуется компонентами Solar NTA и Solar EDR).
- Исполнение 2: Система обнаружения вторжений уровня сети (реализуется компонентом Solar NTA).
- Исполнение 3: Система обнаружения вторжений уровня узла (реализуется компонентом Solar EDR).

2.5.1. Исполнение 1: Система обнаружения вторжений уровня сети и узла

Программный комплекс в Исполнении 1 – это система обнаружения вторжений уровня сети и узла, являющаяся объединением СОВ уровня сети (см. раздел 2.5.2) и СОВ уровня узла (см. раздел 2.5.3).

Солар ПКОиР в Исполнении 1 реализуется компонентами Solar NTA и Solar EDR.

2.5.2. Исполнение 2: Система обнаружения вторжений уровня сети

Солар ПКОиР в Исполнении 2 – это система обнаружения вторжений уровня сети, представляющая собой элемент системы защиты информации информационных систем, функционирующих на базе вычислительных сетей. Система обнаружения вторжений уровня сети применяется совместно с другими средствами защиты информации от несанкционированного доступа к информации в информационных системах.

Солар ПКОиР в Исполнении 2 реализуется компонентом Solar NTA.

[1] Для сотрудников служб безопасности, которые выполняют функции системного администратора

Программный комплекс обеспечивает обнаружение и/или блокирование следующих основных угроз безопасности информации, относящихся к вторжениям (атакам):

- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена;
- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

Основными компонентами СОВ являются датчики (сенсоры) и анализаторы.

Датчики (сенсоры) собирают информацию о пакетах данных, передаваемых в пределах ИС (или сегмента ИС), в которой (котором) установлены эти датчики. Датчики СОВ уровня сети могут быть реализованы в виде программного обеспечения, устанавливаемого на стандартные программно-технические платформы, а также в виде программно-технических устройств, подключаемых к ИС (или сегменту ИС). Анализаторы выполняют анализ собранной датчиками информации, генерируют отчеты по результатам анализа и управляют процессами реагирования на выявленные вторжения.

Решение об обнаружении вторжения СОВ принимают в соответствии с результатами анализа информации, собираемой датчиками СОВ, с применением базы решающих правил СОВ.

2.5.3. Исполнение 3: Система обнаружения вторжений уровня узла

Программный комплекс в Исполнении 3 является системой обнаружения вторжений уровня узла, которая представляет собой элемент системы защиты информации информационных систем, функционирующих на базе вычислительных сетей. Система обнаружения вторжений уровня узла применяется совместно с другими средствами защиты информации от несанкционированного доступа к информации в информационных системах.

Солар ПКОиР в Исполнении 3 реализуется компонентом Solar EDR.

Программный комплекс обеспечивает обнаружение и/или блокирование следующих основных угроз безопасности информации, относящихся к вторжениям (атакам):

- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена;
- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

Основными компонентами СОВ являются датчики (сенсоры) и анализаторы.

Датчики СОВ уровня узла представляют собой программные модули, устанавливаемые на защищаемые узлы информационной системы и предназначенные для сбора информации о событиях, возникающих на этих узлах. Анализаторы выполняют анализ собранной

датчиками информации, генерируют отчеты по результатам анализа и управляют процессами реагирования на выявленные вторжения.

Решение об обнаружении вторжения СОВ принимают в соответствии с результатами анализа информации, собираемой датчиками СОВ, с применением базы решающих правил СОВ.

2.6. Описание среды функционирования

2.6.1. Исполнение 1: Система обнаружения вторжений уровня сети и узла

Описание среды функционирования Солар ПКОиР в Исполнении 1 является объединением соответствующих описаний Исполнения 2 (см. 2.6.2) и Исполнения 3 (см. 2.6.3).

2.6.2. Исполнение 2: Система обнаружения вторжений уровня сети

Рекомендуемые характеристики **Сервера** Солар ПКОиР приведены в таблице ниже.

Табл. 2.1. Рекомендуемые характеристики

Тип аппаратного обеспечения	Параметр	Значение
CPU	Частота	2,2 ГГц
	Количество ядер	72
RAM	Объём	256 ГБ
NIC	Портов для внутреннего взаимодействия и управления (Management Interface)	2 × 10 Гбит/с
Disk	Для ОС и компонентов ПО, SSD, объём	200 ГБ
	Для хранения данных, SSD, объём	17 ТБ

Рекомендуемые характеристики оборудования для **Сенсора NTA** приведены в таблице ниже.

Табл. 2.2. Рекомендуемые характеристики оборудования для Сенсора NTA

Тип аппаратного обеспечения	Параметр	Значение
CPU	Частота	2,2 ГГц
	Количество ядер	72
RAM	Объём	256 ГБ
NIC	Количество портов для приёма трафика (SPAN Interface)	2 × 10 Гбит/с
	Количество портов для внутреннего взаимодействия и управления (Management Interface)	1 × 10 Гбит/с
Disk	Для ОС и компонентов ПО, SSD, объём	200 ГБ
	Для хранения захваченного трафика, HDD, объём	17 ТБ
	Для хранения захваченного трафика, HDD, скорость записи	1,25 ГБ/с

Рекомендуемые характеристики оборудования для **Сервера NTA** приведены ниже.

Табл. 2.3. Рекомендуемые характеристики оборудования для Сервера NTA

Тип аппаратного обеспечения	Параметр	Значение
CPU	Частота	2,2 ГГц
	Количество ядер	72
RAM	Объём	256 ГБ
NIC	Количество портов для внутреннего взаимодействия и управления (Management Interface)	2 × 10 Гбит/с
Disk	Для ОС и компонентов ПО, SSD, объём	200 ГБ
	Для хранения данных, SSD, объём	17 ТБ

Минимальные требования к оборудованию для хранилища NTA:

СХД 2 контроллера, 2 порта 10 ГБ, 2 блока питания, пропускная способность не менее 400 kIOPS, 18 SSD U.2 NVMe 7600 ГБ Samsung PM1733.

ПО всех компонентов Solar NTA должно функционировать в среде Linux на базе ядра Linux 5.10.0-22-amd64 x86_64.

2.6.3. Исполнение 3: Система обнаружения вторжений уровня узла

Характеристики серверной части

Рекомендуемые характеристики **Сервера** Солар ПКОиР приведены в таблице ниже.

Табл. 2.4. Рекомендуемые характеристики

Тип аппаратного обеспечения	Параметр	Значение
CPU	Частота	2,2 ГГц
	Количество ядер	72
RAM	Объём	256 ГБ
NIC	Портов для внутреннего взаимодействия и управления (Management Interface)	2 × 10 Гбит/с
Disk	Для ОС и компонентов ПО, SSD, объём	200 ГБ
	Для хранения данных, SSD, объём	17 ТБ

Характеристики конечного устройства

Рекомендуемые аппаратные характеристики конечного устройства для установки Solar EDR приведены в таблице ниже.

Табл. 2.5. Рекомендуемые характеристики конечного устройства для установки Solar EDR

Тип аппаратного обеспечения	Параметр	Значение
CPU	Частота	2,2 ГГц
	Количество ядер	2
RAM	Объём	16 ГБ
Disk	SSD, объём	50 ГБ

Solar EDR должен быть установлен на конечное устройство под управлением следующих ОС:

- Windows 10 x64 версии не менее 1803;
- Windows Server 2016, 2019, 2022.

Перечень ПО, совместимого с Solar EDR, приведен в приложении **Приложение G, *Тестирование стабильной работы агента Solar EDR Windows с прикладным ПО***.

3. Развертывание, обновление и удаление ПО

Описание процессов установки ПО компонентов Solar NTA и EDR Windows, а также серверной части Солар ПКОиР приведено в документе «Инструкция по установке для экспертов».

4. Основные принципы работы с Солар ПКОиР

4.1. Общий процесс работы с Солар ПКОиР

Солар ПКОиР ориентирован на работу по двум основным направлениям:

- оперативный мониторинг текущей обстановки;
- принятие мер по обезвреживанию атаки.

4.2. Принципы работы в интерфейсе Солар ПКОиР

4.2.1. Начало работы. Вход в систему

Для начала работы с веб-интерфейсом Солар ПКОиР необходимо:

1. В адресной строке веб-браузера ввести адрес сервера Солар ПКОиР: **https://<адрес сервера Солар ПКОиР>**
2. На отобразившейся странице в соответствующих полях указать **Логин** (адрес электронной почты) и **Пароль** для входа в систему и нажать кнопку **Войти** (см. Рис.4.1).

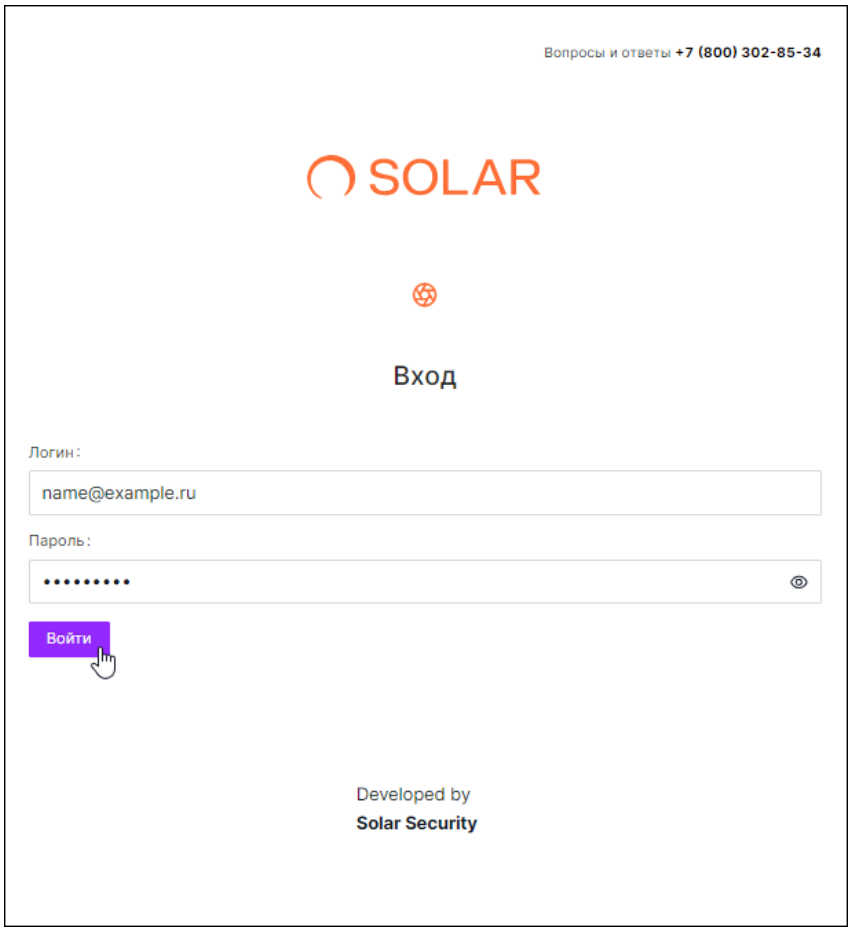


Рис. 4.1. Вход в систему

После успешного входа в систему по умолчанию на экране отобразится раздел **События** со сведениями о поступивших событиях или последняя страница, которая была открыта перед завершением сессии.

Внимание!

Приведенные в документе изображения элементов веб-интерфейса носят исключительно ознакомительный характер и могут отличаться от реальных.

При вводе неверных данных (логина и/или пароля) вход в систему выполнен не будет, а на экране отобразится соответствующее сообщение (см. Рис.4.2).

Рис. 4.2. Неверный ввод данных для входа в систему

По всем вопросам, связанным с доступом в Солар ПКОиР, следует обращаться к системному администратору Солар ПКОиР.

4.2.2. Описание основных элементов интерфейса и общих операций

Каждая страница веб-интерфейса Солар ПКОиР содержит набор стандартных элементов управления и отображения, необходимый для выполнения конкретных задач. К таким элементам относятся меню, панель навигации, кнопка, флажок, поле ввода данных, переключатель, список объектов, таблица и т. д.

В левой части экрана отображается **Главное меню** системы в свернутом виде. Чтобы развернуть панель главного меню, необходимо навести на нее курсор мыши. При перемещении курсора за пределы области меню панель будет сворачиваться. Чтобы закрепить панель в свернутом виде, следует нажать на значок с надписью **Свернуть меню**, который расположен внизу панели (Рис.4.3). Пункты главного меню соответствуют основным разделам веб-интерфейса системы:

- **События** – раздел предназначен для мониторинга нарушений политики ИБ и используется для отображения информации о поступающих в систему событиях (см. раздел 5).
- **Сессии** – раздел предназначен для мониторинга распознаваемого трафика с целью выявления инцидентов (см. раздел 6). Раздел веб-интерфейса недоступен в Исполнении 3 (см. раздел 2.5.3).
- **Сеть** – используется для отображения информации о добавленных в систему объектах защиты (хостах) (см. раздел 7). Раздел веб-интерфейса недоступен в Исполнении 2 (см. раздел 2.5.2).
- **Политики** – раздел предназначен для настройки механизма взаимодействия сервера Солар ПКОиР с подключенными агентами Solar EDR и Solar NTA (см. раздел 8).
- **Расследования** – раздел предназначен для мониторинга информации об инцидентах, предоставления детальной информации о событиях и артефактах, входящих в инцидент, выполнения действий по работе с инцидентом (см. раздел 9).
- **Правила** – раздел используется для отображения и настройки правил обнаружения инцидентов (см. раздел 10).
- **Настройки** – раздел предназначен для управления учетными записями пользователей (см. раздел 11).

Примечание

Доступ к разделам веб-интерфейса и отдельным функциональным возможностям может различаться в зависимости от роли пользователя (подробнее о ролевой модели см. в разделе 11.1.6).

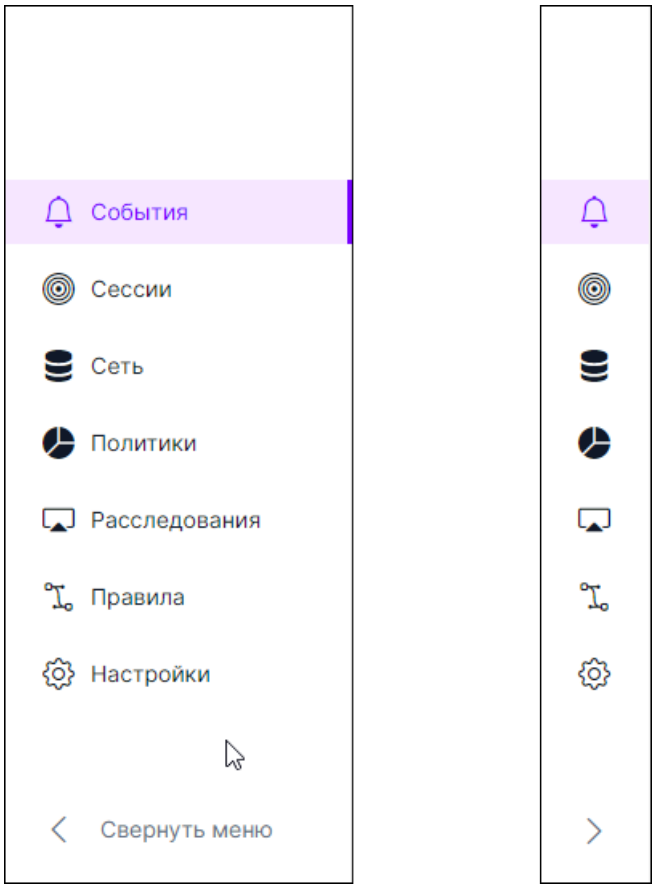


Рис. 4.3. Главное меню веб-интерфейса Солар ПКОиР

На верхней панели (в верхней части) веб-интерфейса Солар ПКОиР расположены следующие элементы:

- фотография, имя и адрес электронной почты пользователя;
- значок – для выхода из системы.

5. Раздел «События»

Раздел **События** предназначен для мониторинга нарушений политики ИБ. Под нарушениями политики ИБ понимаются:

- событие ИБ – зафиксированное состояние информационной (автоматизированной) системы, сетевого, телекоммуникационного, коммуникационного, иного прикладного сервиса или информационно-телекоммуникационной сети, указывающее на возможное нарушение безопасности информации, сбой СЗИ, или ситуацию, которая может быть значимой для безопасности информации. События создаются системой автоматически в зависимости от настроенных в ней правил политики безопасности;
- инцидент ИБ – непредвиденное или нежелательное событие (группа событий) ИБ, которое привело (может привести) к нарушению функционирования информационного ресурса или возникновению угроз безопасности информации или нарушению требований по защите информации. Инциденты создаются вручную специалистом по информационной безопасности по результатам анализа событий или системой автоматически.

Солар ПКОиР фиксирует события ИБ, обрабатывает их по заданным правилам политики безопасности и отмечает признак инцидента при его обнаружении. Основная задача пользователя в процессе мониторинга нарушений политики ИБ – просмотреть зафиксированные в системе события и определить, являются ли они инцидентами ИБ.

Мониторинг нарушений политики ИБ выполняется в специальном разделе интерфейса – **События** (Рис.5.1).

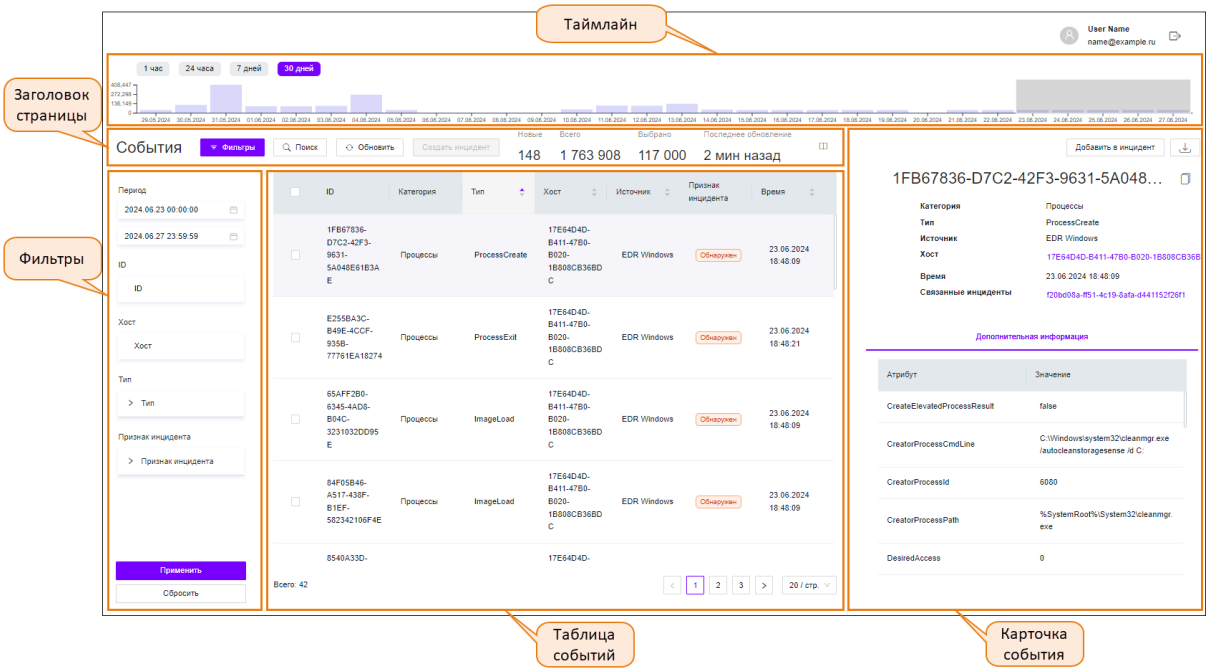


Рис. 5.1. Раздел «События»

В результате выбора раздела в главном меню отобразится страница для работы с событиями, которая состоит из следующих областей (см. Рис.5.1):

- таймлайн;

- заголовок страницы;
- фильтры;
- таблица событий;
- карточка события.

5.1. Таймлайн: количество событий за период времени

Таймлайн представляет собой гистограмму, на которой в виде столбцов выводятся события, полученные в определенный диапазон времени. На горизонтальной шкале отображается заданный период времени, а на вертикальной – количество событий (см. Рис.5.2). Высота столбцов на гистограмме пропорциональна соответствующим им значениям, однако высота минимального столбца будет равна 10% от максимального (при наличии событий за период).

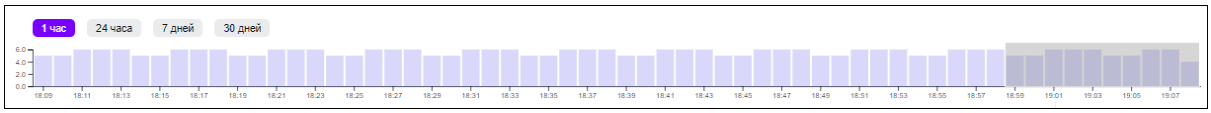


Рис. 5.2. Таймлайн событий

Примечание

Если ранее в разделе применялся поиск событий с помощью запросов, в области таймлайна может отображаться поле для ввода поискового запроса (см. Рис.5.8). Чтобы закрыть это поле и перейти к таймлайну, необходимо нажать одну из кнопок: Поиск *или* Фильтры.

По умолчанию на **Таймлайне** выводятся события за последний час. Выделенная область таймлайна позволяет определить, за какой период времени отображать данные в таблице событий.

Изменить период отображения событий позволяют **Пресеты**, расположенные в левом верхнем углу таймлайна:

- **1 час** – гистограмма таймлайна строится за 1 час. Цена деления горизонтальной шкалы – 2 минуты. На такой гистограмме показывается количество событий поминутно, т. е. количество столбцов на таймлайне будет соответствовать количеству минут. Выделенная область таймлайна – последние 10 минут.
- **24 часа** – гистограмма строится за сутки (24 часа). Цена деления горизонтальной шкалы – 1 час. На таймлайне отображается количество событий за каждый час, т. е. каждому часу будет соответствовать один столбец. Выделенная область таймлайна – последний час.
- **7 дней** – гистограмма строится за неделю (7 дней). Цена деления горизонтальной шкалы – 1 день. Гистограмма показывает количество событий за каждый день, т. е. каждому дню будет соответствовать один столбец таймлайна. Выделенная область таймлайна – последний день.

- **30 дней** – гистограмма строится за месяц (30 дней). Цена деления горизонтальной шкалы – 1 день. На таймлайне показывается количество событий за каждый день, т. е. каждому дню будет соответствовать один столбец. Выделенная область таймлайна – последний день.

Помимо пресетов, можно вручную изменять выделенную область таймлайна для более гибкого управления периодом, за который будут отображаться события в таблице. Для этого с помощью мыши можно расширять или сужать выделенную область, а также перемещать ее по горизонтальной шкале.

Следует отметить, что при изменении выделенной области таймлайна значения параметра **Период** в фильтрах (см. раздел 5.4) также изменятся.

5.2. Таблица событий

Информация о поступающих в систему событиях отображается в виде таблицы. Каждая строка соответствует определенному событию. Период, за который отображаются события в таблице, определяется выбранным временным диапазоном **Таймлайна** или фильтрацией по периоду. По умолчанию при открытии раздела **События** будут показаны события за последние 10 минут.

Столбцы таблицы содержат следующие данные о событиях:

- **ID** – идентификатор события.
- **Категория**, к которой относится полученное событие. Например, **Сетевая активность**, **Файловая система** и т. д. Полный список категорий событий представлен в разделе ***Приложение В, Сведения о типах событий***.
- **Тип** события (подробнее о типах событий см. в разделе ***Приложение В, Сведения о типах событий***).
- **Хост**, на котором произошло событие. Столбец недоступен в Исполнении 2 (см. раздел 2.5.2).
- **Источник** полученных данных о событии: **Solar EDR Windows** или **Solar NTA**.
- **Признак инцидента**:
  - **Обнаружен** – отображается в случае, если у события есть хотя бы один связанный инцидент.
  - **Не обнаружен** – отображается, если событие не содержит ни одного связанного инцидента.
- **Время** – дата и время возникновения события.

Дополнительные столбцы для отображения сведений о событиях, полученных из источника Solar NTA (недоступны в Исполнении 3 – см. раздел 2.5.3):

- **IP-адрес источника** – IP-адрес отправителя трафика.
- **Порт источника трафика** – порт отправителя трафика.
- **IP-адрес получателя** – IP-адрес получателя трафика.

- **Порт получателя трафика**.
- **Транспортный протокол** – наименование транспортного протокола L3/L4: TCP, UDP, ICMP или IP.
- **Хеш-сумма** – фиксированная строка символов, созданная при помощи хеш-функции, анализирующей содержимое передаваемых в рамках события данных.
- **Критичность** – уровень критичности события:
  - **Informational**;
  - **Minor**;
  - **Major**;
  - **High**;
  - **Critical**.
- **Идентификатор сигнатуры (SID)** – уникальный идентификатор сигнатуры правила Suricata.
- **Название правила**.
- **Признак IOC** – наблюдаемый в сети или на конкретном устройстве объект (или активность), который с большой вероятностью указывает на несанкционированный доступ к системе, то есть ее компометацию. Возможные значения: **Обнаружен**/**Не обнаружен**.
- **Класс события**. Может относиться к типу сетевого трафика или виду атаки, который Suricata пытается обнаружить.
- **Размер файла** – размер передаваемых в рамках события данных, в байтах.
- **Тип файла** – тип файла, передаваемого в рамках события.
- **URL** ресурса файла.
- **Ревизия** – версия сигнатуры.
- **Протокол L5/L7**.

Слева от каждого события расположен флажок, который используется при создании нового инцидента, связанного с событиями. Подробнее об этом см. в разделе 5.7.

При необходимости можно изменить набор столбцов в таблице. Подробнее об этом см. в разделе 5.3.1.

Кроме того, для удобства можно изменить ширину таблицы. Для этого следует захватить мышью вертикальный разделитель между таблицей и карточкой события и перетащить его вправо (для расширения столбцов) или влево (для сужения).

Слева под таблицей отображается количество записей в таблице с учетом фильтрации (см. раздел 5.4) и выделенной области таймлайна (см. раздел 5.1).

Под таблицей справа расположены кнопки для перехода между страницами. По умолчанию на одной странице таблицы отображаются 20 записей. Для удобства можно изменить количество отображаемых событий на странице, нажав на соответствующее поле и выбрав в раскрывающемся списке требуемое число (см. Рис.5.3).

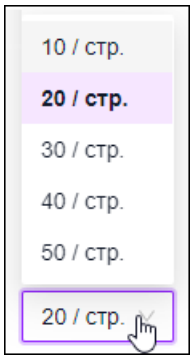


Рис. 5.3. Настройка количества записей на странице таблицы

5.2.1. Сортировка событий в таблице

По умолчанию события в таблице отсортированы по времени их создания в обратном хронологическом порядке (вверху таблицы находятся самые свежие события).

При необходимости можно изменить порядок отображения событий, нажав на значок в названии требуемого столбца:

- изменение значка на означает, что в столбце применена сортировка по возрастанию (для чисел – от наименьшего к наибольшему, для текста – в алфавитном порядке, т. е. от А до Я / от A до Z);
- изменение значка на означает, что в столбце применена сортировка по убыванию (для чисел – от наибольшего к наименьшему, для текста – в обратном алфавитном порядке, т. е. от Я до А / от Z до A);
- значок означает, что в столбце сортировка не применена.

Также для удобства заголовок столбца, по которому отсортированы данные в таблице, выделяется светло-серым цветом. Например, на Рис.5.4 выделен заголовок столбца **Источник**.

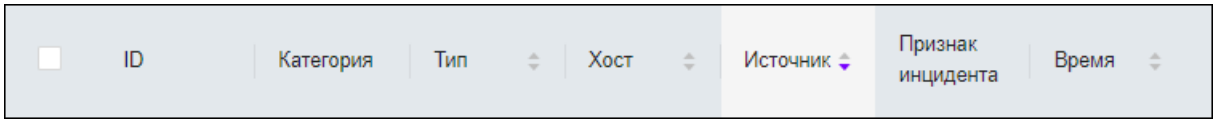


Рис. 5.4. Заголовки столбцов таблицы: сортировка данных по столбцу «Источник»

5.3. Заголовок страницы «События»

В заголовке страницы **События** содержатся:

- название текущего раздела;

- кнопка Фильтры / Фильтры – **Фильтры**, позволяющая развернуть/свернуть панель с полями для фильтрации событий (см. раздел 5.4);
- кнопка Поиск / Поиск – **Поиск**, позволяющая развернуть/свернуть поле для ввода поискового запроса (см. раздел 5.5);
- кнопка **Обновить**, с помощью которой можно оперативно получить актуальную на текущий момент информацию о событиях ИБ без обновления страницы;
- кнопка **Создать инцидент**, с помощью которой можно вручную создать новый инцидент, связанный с событиями (см. раздел 5.7). Кнопка доступна только при условии, что в таблице отмечено флажком хотя бы одно событие.
- сводная информация по событиям:
  - **Новые** – количество новых событий, которые появились в таблице после нажатия кнопки **Обновить**;
  - **Всего** – общее количество событий, которые отображаются на таймлайне в текущий момент времени;
  - **Выбрано** – количество событий, которые представлены в выбранном временном диапазоне таймлайна;
  - **Последнее обновление** – информация о последнем обновлении данных. При наведении курсора мыши на значение отобразится всплывающее окно с датой и временем последнего обновления.
- значок ◫ для настройки отображения таблицы (см. раздел 5.3.1).

5.3.1. Настройки отображения таблицы «События»

Чтобы изменить набор столбцов в таблице, необходимо нажать на значок ◫, расположенный в заголовке страницы (см. Рис.5.5).

Примечание

В зависимости от Исполнения программного комплекса Солар ПКОиР (см. раздел 2.5) перечень доступных для отображения столбцов будет различаться.

Для отображения/скрытия определенного столбца в таблице следует установить/снять соответствующий флажок, расположенный рядом с его названием.

Примечание

При изменении настроек отображения таблицы набор полей для фильтрации (см. раздел 5.4) также изменится.

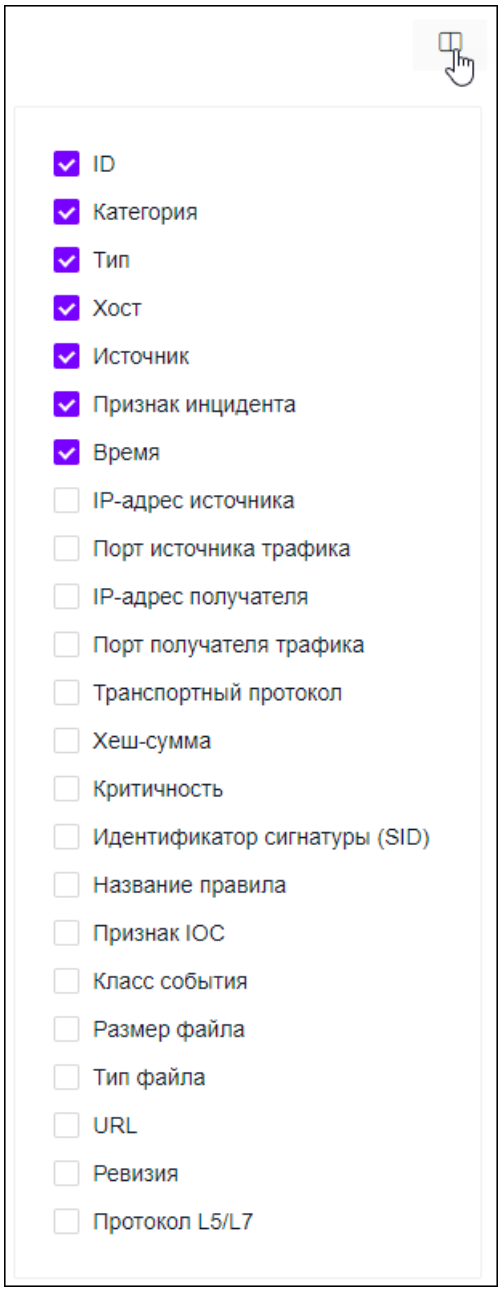


Рис. 5.5. Настройки отображения таблицы событий

5.4. Фильтры событий

Для быстрого поиска требуемых событий по выбранным критериям предусмотрены **Фильтры**. Они расположены на боковой панели слева от **Таблицы событий**. Чтобы открыть панель с полями для фильтрации, необходимо нажать кнопку Фильтры.

Примечание

Набор полей для фильтрации может различаться в зависимости от Исполнения программного комплекса (см. раздел 2.5), а также от настроек отображения таблицы (см. раздел 5.3.1).

События можно фильтровать по следующим параметрам:

- **Период** – позволяет найти все события, которые были созданы в заданном диапазоне времени. Для этого необходимо нажать на значок , расположенный в соответствующих полях. Откроется окно в виде календаря (см. Рис.5.6), в котором требуется выбрать дату и время начала/окончания периода. При нажатии на ссылку **Сейчас**, расположенную в левом нижнем углу, в поле установятся текущие дата и время.

  Здесь есть ряд особенностей:

  - Дату и время в этом фильтре можно выбрать только в пределах границ **Пресета** (см. 5.1 [стр.22]), установленного на таймлайне, например, в рамках одного дня.
  - Значения параметра **Период** изменяются при изменении выделенной области таймлайна (см. раздел 5.1).
  - После применения этого фильтра выделенная область на таймлайне также изменится.

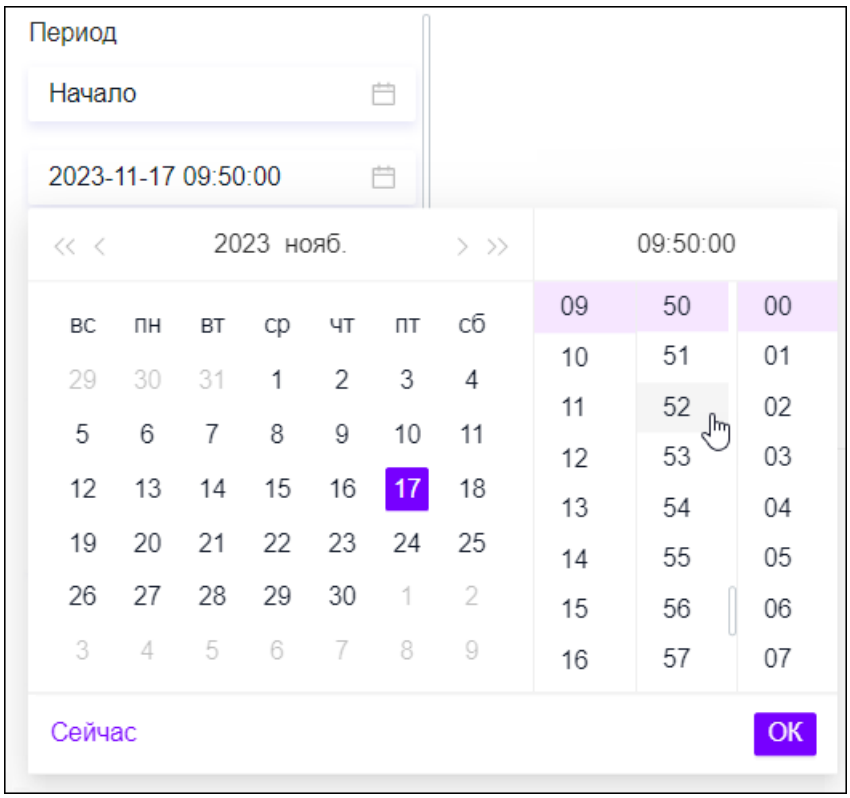


Рис. 5.6. Раздел «События». Фильтр «Период»: выбор даты и времени

- **ID** события. Параметр используется, если требуется найти определенное событие по его идентификатору. Поиск по этому полю является регистрозависимым и осуществляется по полному совпадению значения.
- **Хост**. Позволяет найти события, полученные из источника Solar EDR Windows, которые произошли на определенном хосте. Код устройства хоста вводится с клавиатуры. Поиск по этому полю является регистрозависимым и осуществляется по полному совпадению значения. Фильтр недоступен в Исполнении 2 (см. раздел 2.5.2).

- **Тип** – это древовидный фильтр, который состоит из трех уровней (см. Рис.5.7):
  - Первый уровень позволяет найти события, которые поступили из определенного источника. Для этого необходимо отметить флажком требуемый источник. При этом в дочерних фильтрах по категории и типу событий будут автоматически выбраны все значения.
  - Второй уровень позволяет найти события, относящиеся к определенной категории. Для этого следует развернуть соответствующий источник отметить флажком одну или несколько требуемых категорий. При этом в дочернем фильтре по типу событий автоматически будут выбраны все значения, а источник, к которому эта категория относится, будет отмечен значком ■.
  - Третий уровень позволяет осуществить более гибкую фильтрацию по типам событий. Для этого необходимо развернуть соответствующую категорию и отметить флажком один или несколько требуемых типов. При этом родительская категория будет отмечена значком ■.

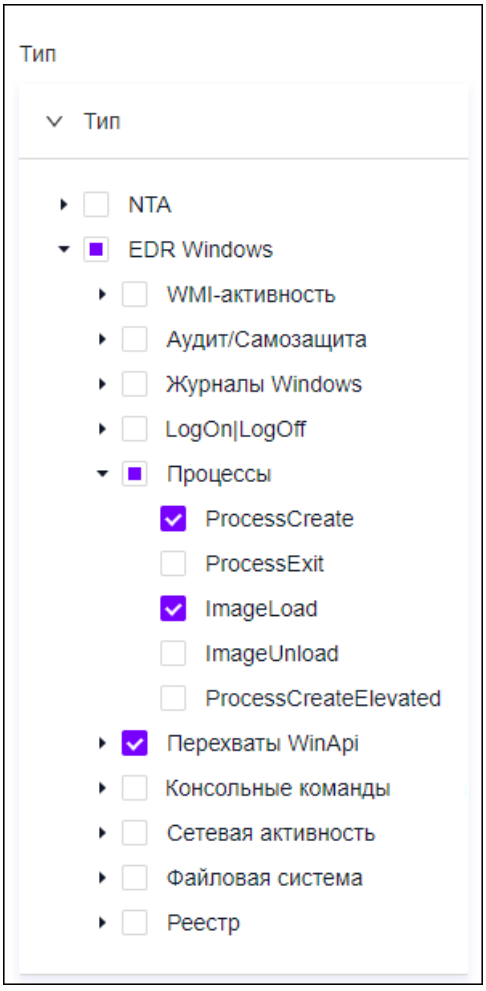


Рис. 5.7. Раздел «События». Фильтр «Тип»

- Фильтр **Признак инцидента** позволяет определить, какие события попадут в выборку:
  - с признаком инцидента **Обнаружен**, то есть события, у которых есть связанные инциденты;

- с признаком инцидента **Не обнаружен**, то есть события, у которых нет ни одного связанного инцидента;
- с любым признаком инцидента.

Кроме того, события, полученные из источника Solar NTA, можно фильтровать по следующим дополнительным параметрам (фильтры недоступны в Исполнении 3 – см. раздел 2.5.3):

- **IP-адрес источника**. Позволяет найти события по IP-адресу источника трафика. IP-адрес вводится с клавиатуры. Поиск по этому полю осуществляется по полному совпадению значения.
- **Порт источника трафика**. Позволяет найти события по порту источника трафика. Порт вводится с клавиатуры. Поиск по этому полю осуществляется по полному совпадению значения.
- **IP-адрес получателя**. Позволяет найти события по IP-адресу получателя трафика. IP-адрес вводится с клавиатуры. Поиск по этому полю осуществляется по полному совпадению значения.
- **Порт получателя трафика**. Позволяет найти события по порту получателя трафика. Порт вводится с клавиатуры. Поиск по этому полю осуществляется по полному совпадению значения.
- **Транспортный протокол**. Позволяет найти события по наименованию транспортного протокола L3/L4. Для этого следует отметить флажком одно или несколько значений.
- **Критичность**. Позволяет найти события по уровню критичности. Для этого необходимо отметить флажком одно или несколько значений:
  - **Informational**;
  - **Minor**;
  - **Major**;
  - **High**;
  - **Critical**.
- **Идентификатор сигнатуры (SID)**. Позволяет найти события по уникальному идентификатору сигнатуры. Значение вводится с клавиатуры. Поиск по этому полю осуществляется по полному совпадению значения.
- **Название правила**. Позволяет найти события по названию сработавшего правила Suricata. Значение вводится с клавиатуры. Поиск по этому полю является регистрозависимым и осуществляется по полному совпадению значения.
- **Признак IOC**. Позволяет найти события по наличию признака IOC. Для этого необходимо отметить флажком требуемое значение: **Обнаружен** или **Не обнаружен**.
- **Класс события**. Позволяет найти события по их классу. Значение вводится с клавиатуры. Поиск по этому полю является регистрозависимым и осуществляется по полному совпадению значения.

- **Тип файла**. Позволяет найти события по типу файла, передаваемого в рамках события. Значение вводится с клавиатуры. Поиск по этому полю является регистрозависимым и осуществляется по полному совпадению значения.
- **Ревизия**. Позволяет найти события по версии сигнатуры. Значение вводится с клавиатуры. Поиск по этому полю осуществляется по полному совпадению значения.
- **Протокол L5/L7**. Значение вводится с клавиатуры. Поиск по этому полю является регистрозависимым и осуществляется по полному совпадению значения.

Чтобы отфильтровать таблицу событий по заданным параметрам, необходимо нажать кнопку **Применить** или клавишу **Enter** на клавиатуре. После этого значение в поле **Всего**, которое расположено под таблицей событий слева, также изменится. Очистить параметры фильтров и привести таблицу к исходному виду позволяет кнопка **Сбросить**.

Чтобы скрыть область работы с фильтрами, необходимо нажать кнопку Фильтры.

5.5. Поиск событий с помощью запросов

Зачастую, чтобы найти нужные события для расследования атаки, пользователю недостаточно фиксированных параметров, предусмотренных фильтрами. В этом случае можно задать более гибкие условия поиска и найти требуемые события по специфичному запросу. Чтобы найти события с помощью запроса, необходимо выполнить следующие действия:

1. Нажать кнопку Поиск. Поле для ввода поискового запроса (см. Рис.5.8) отобразится в верхней части страницы вместо таймлайна.
2. Ввести текст поискового запроса в формате, близком к SQL (Clickhouse). Подробнее о синтаксисе запросов см. на сайте https://clickhouse.com/docs/ru/sql-reference/statements/select.

Примечание

*Следует обратить внимание, что параметр **limit** не применим для поискового запроса.*

3. Нажать на значок, расположенный справа от поля для ввода.

После этого на странице отобразятся все события, удовлетворяющие условиям запроса.

Рис. 5.8. Раздел «События». Поле для ввода поискового запроса

Чтобы сбросить введенный запрос и очистить поле для ввода, следует нажать на значок .

Примечание

В текущей версии одновременное использование поисковых запросов и стандартных фильтров, а также поисковых запросов и таймлайна невозможно. Однако поиск событий будет осуществляться в рамках заданного ранее ***Пресета*** *(см. 5.1 [стр.22]).*

Чтобы скрыть поле для ввода поискового запроса, необходимо нажать кнопку Поиск.

5.6. Карточка события

Справа от таблицы расположена карточка события. По умолчанию при переходе в раздел **События** открывается карточка первого события из таблицы. Чтобы открыть карточку требуемого события, необходимо найти его в таблице и нажать на строку, в которой это событие записано.

Карточка содержит общие сведения о событии, а также дополнительную информацию. Внешний вид и набор полей на карточке события различается в зависимости от источника, из которого это событие получено (см. разделы 5.6.1 и 5.6.2).

В правом верхнем углу карточки события расположены следующие кнопки:

- Кнопка **Добавить в инцидент** позволяет добавить событие в инцидент (то есть связать это событие с инцидентом). Подробнее об этом см. в разделе 5.8.
- Кнопка позволяет выгрузить исходное событие в файл формата JSON. Файл выгруженного исходного события будет содержать:
  - обязательные атрибуты для всех событий (полный список обязательных атрибутов представлен в разделе *Приложение C, Обязательные атрибуты событий Solar EDR Windows и Solar NTA*);
  - атрибуты, характерные для событий, полученных из источника Solar EDR Windows / Solar NTA. Список атрибутов Solar EDR Windows представлен в разделе *Приложение D, Атрибуты событий Solar EDR Windows*.

Значок, расположенный на карточке события, позволяет скопировать идентификатор данного события, чтобы в дальнейшем поделиться с коллегами или использовать в процессе расследования инцидента.

5.6.1. Карточка события Solar EDR Windows

Примечание

В Исполнении 2 программного комплекса события из источника Solar EDR Windows не поступают, поэтому информация, содержащаяся в данном разделе, неактуальна для Исполнения 2 (см. раздел 2.5.2).

Общие сведения, которые отображаются на карточке события, полученного из источника **Solar EDR Windows** (см. Рис.5.9):

- **ID** – идентификатор события (расположен в заголовке карточки).
- **Категория** – категория, к которой относится событие.
- **Тип** – тип события.
- **Источник** – источник, из которого событие было получено.
- **Хост** – код устройства хоста, на котором произошло событие. При нажатии на ссылку будет осуществлен переход в раздел **Сеть**, в котором будет открыта карточка данного хоста (см. раздел 7.5).
- **Время** – дата и время создания события.
- **Связанные инциденты** – список инцидентов, в которые входит данное событие. При нажатии на ссылку с идентификатором определенного инцидента будет открыта страница этого инцидента (см. раздел 9.4). По умолчанию здесь отображаются три инцидента. Чтобы открыть полный список инцидентов, связанных с данным событием, необходимо нажать на ссылку **Показать все**.

Ниже на карточке события располагается панель **Дополнительная информация**. Здесь в виде таблицы отображаются атрибуты события и их значения (см. раздел Приложение D, *Атрибуты событий Solar EDR Windows*).

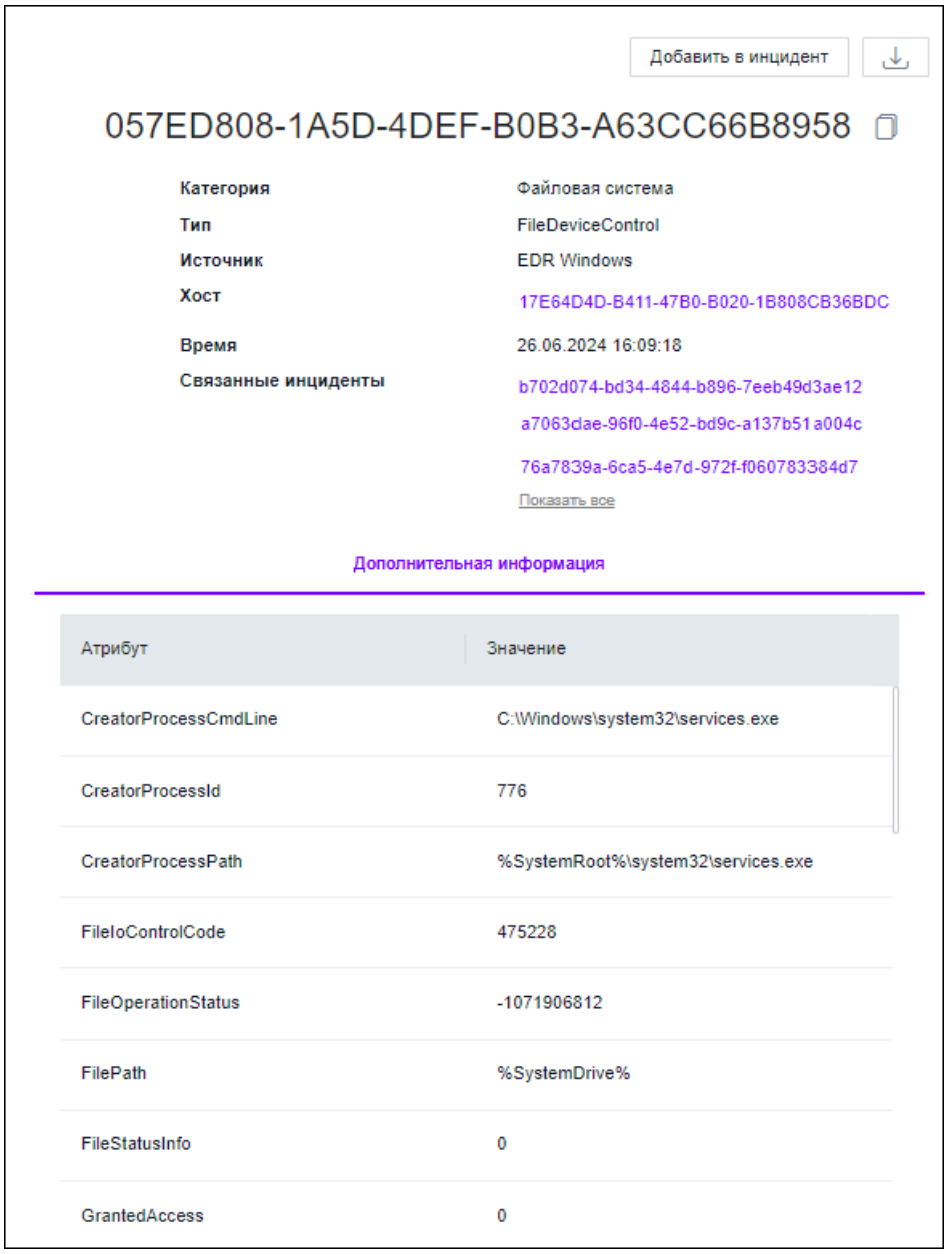


Рис. 5.9. Карточка события Solar EDR Windows

5.6.2. Карточка события Solar NTA

Примечание

В Исполнении 3 программного комплекса события из источника Solar NTA не поступают, поэтому информация, содержащаяся в данном разделе, неактуальна для Исполнения 3 (см. раздел 2.5.3).

Общие сведения, которые содержатся на карточке события, полученного из источника Solar NTA (см. Рис.5.10):

- **ID** – идентификатор события (расположен в заголовке карточки).

- **Категория** – категория, к которой относится событие.
- **Тип** – тип события.
- **Источник** – источник, из которого событие было получено.
- **Время** – дата и время создания.
- **Связанные инциденты** – список инцидентов, в которые входит данное событие. При нажатии на ссылку с названием определенного инцидента будет открыта страница этого инцидента (см. раздел 9.4). По умолчанию здесь отображаются три инцидента. Чтобы открыть полный список инцидентов, связанных с данным событием, необходимо нажать на ссылку **Показать все**.
- **ID сессии** – идентификатор сессии, в рамках которой было получено это событие. При нажатии на ссылку с идентификатором сессии будет открыта его карточка (см. раздел 6.3.2).
- **Источник трафика** – IP-адрес и порт источника трафика.
- **Получатель трафика** – IP-адрес и порт получателя трафика.
- **Транспортный протокол** – наименование транспортного протокола L3/L4: **TCP**, **UDP**, **ICMP** или **IP**.

Ниже на карточке события располагается панель **Дополнительная информация**. Здесь в виде таблицы отображаются атрибуты события и их значения.

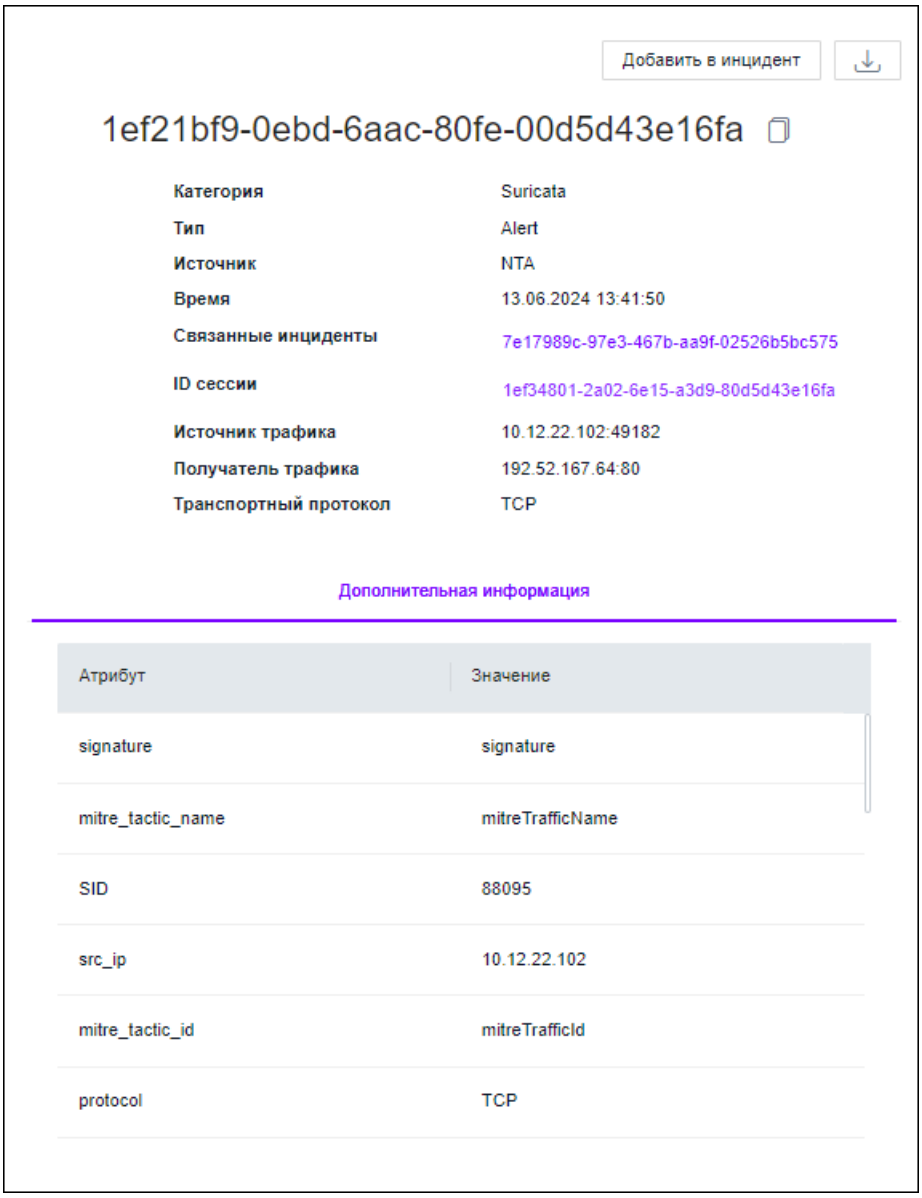


Рис. 5.10. Карточка события Solar NTA

5.7. Создание нового инцидента из событий

При работе с событиями пользователь может принять решение о необходимости создания нового инцидента, связанного с событием (или событиями), чтобы зафиксировать факт возникновения подозрительной активности, если это не было ранее выполнено системой. Для этого необходимо выполнить следующие действия:

1. В разделе **События** в таблице отметить флажком одно или несколько требуемых событий. Если таких событий много, можно воспользоваться таймлайном, фильтрами или поисковым запросом, чтобы отфильтровать записи в таблице. Затем нажать на флажок, расположенный в заголовке таблицы, чтобы выбрать все события.

2. В заголовке страницы нажать кнопку **Создать инцидент** (см. Рис.5.11).

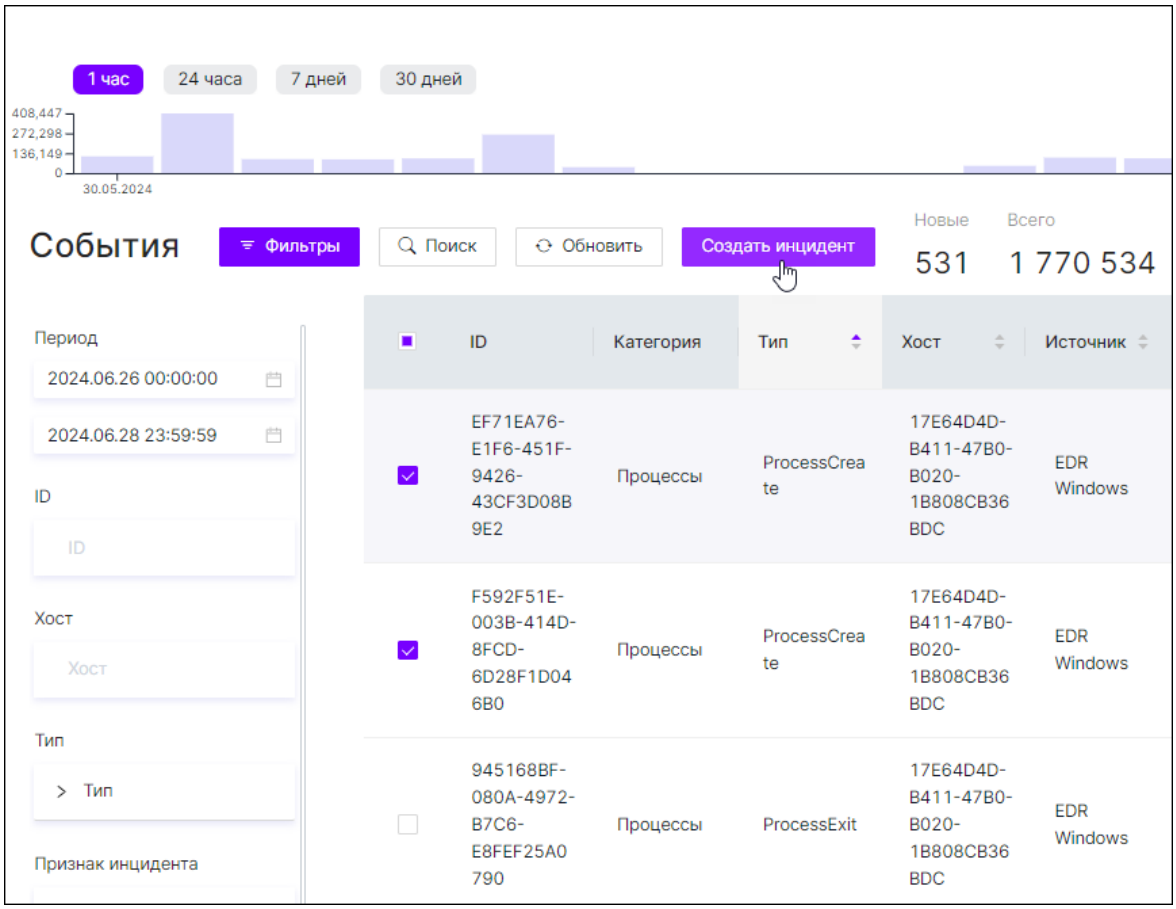


Рис. 5.11. Раздел «События». Таблица событий: создание нового инцидента из событий

3. В диалоговом окне (см. Рис.5.12) заполнить информацию о создаваемом инциденте:

   - **Тип** – название создаваемого инцидента.
   - **Редактировал** – текущий пользователь, создающий инцидент. Поле заполняется автоматически и недоступно для изменения.
   - **Критичность** – уровень значимости инцидента. По умолчанию установлена низкая критичность.
   - **Время первого события** – дата и время возникновения первого события в создаваемом инциденте. Поле заполняется автоматически и недоступно для изменения.

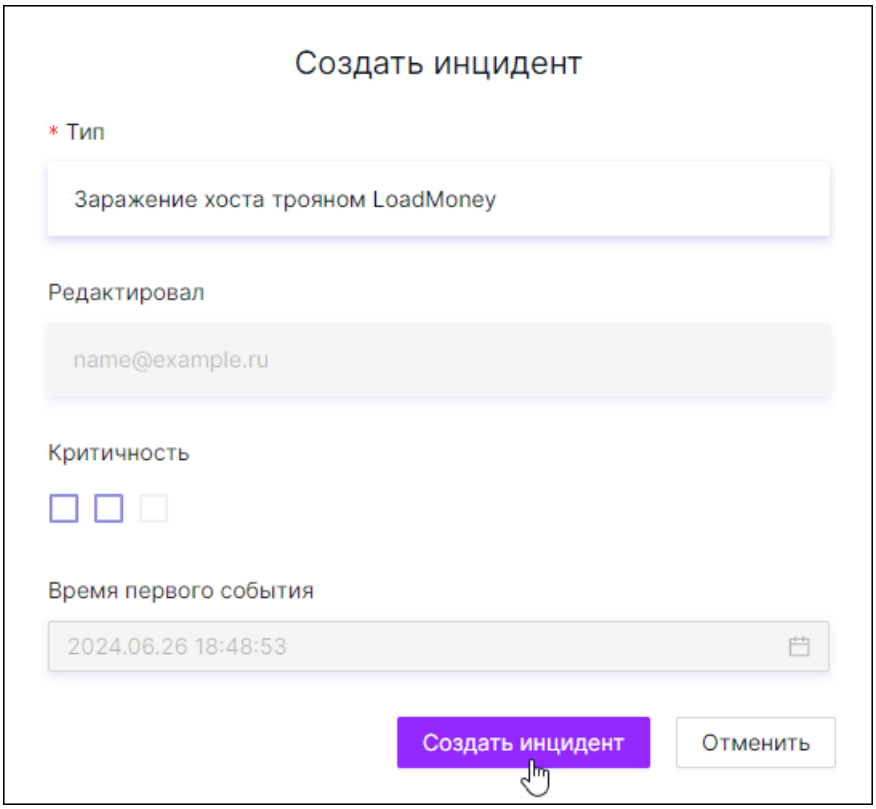


Рис. 5.12. Раздел «События». Окно создания нового инцидента из событий

4. Нажать кнопку **Создать инцидент**.

После этого в правом верхнем углу появится уведомление об успешном создании нового инцидента (Рис.5.13).

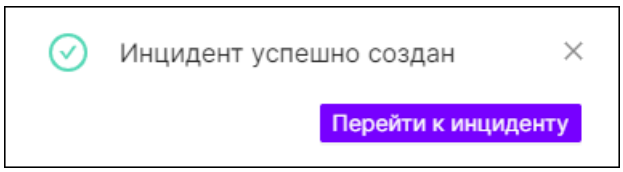


Рис. 5.13. Уведомление об успешном создании инцидента

При нажатии кнопки **Перейти к инциденту** откроется страница созданного инцидента. Здесь в поле **Способ создания** будет отображен значок ручного создания, а в списке связанных событий будут показаны события, из которых этот инцидент был создан (Рис.5.14).

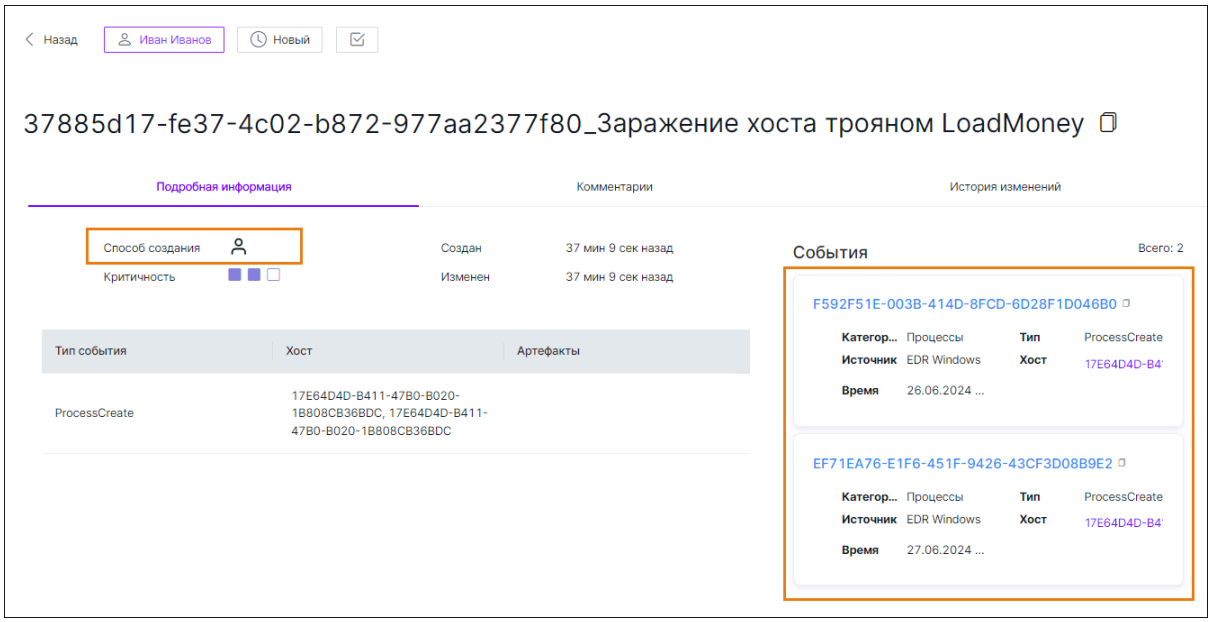


Рис. 5.14. Страница инцидента, созданного из событий

В карточках событий, связанных с новым инцидентом, появится ссылка на этот инцидент. Если ранее события имели **Признак инцидента Не обнаружен**, то сейчас он изменится на **Обнаружен** (см. Рис.5.15). Следует отметить, что изменение признака инцидента может занять до 5 минут.

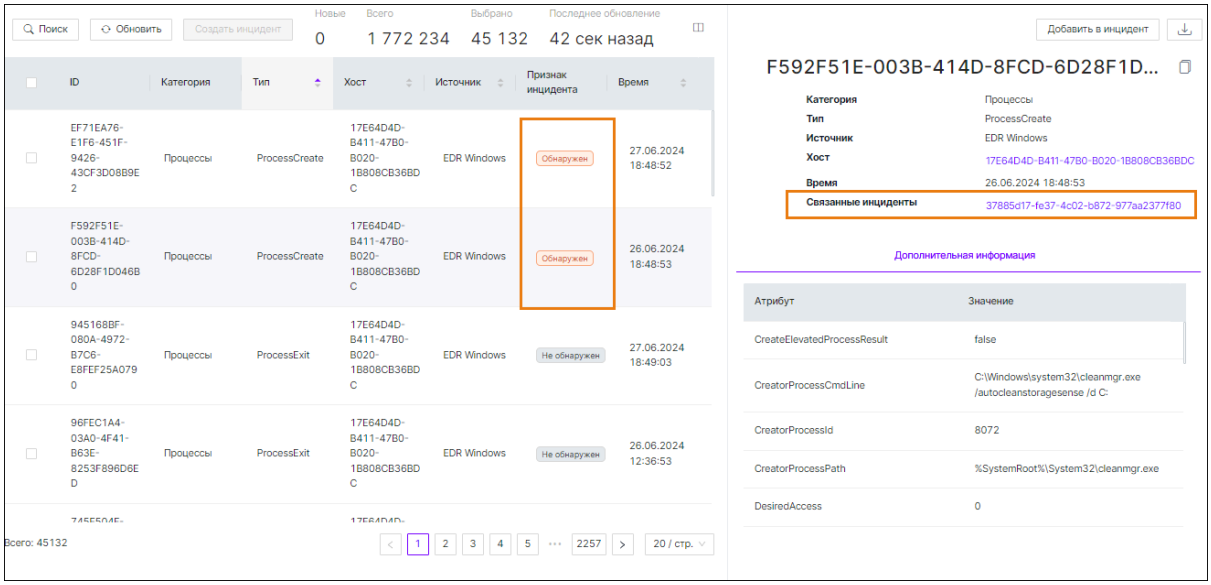


Рис. 5.15. Раздел «События»: изменения в событиях после создания нового связанного инцидента

5.8. Добавление события в инцидент

В ходе расследования инцидента может возникнуть необходимость вручную добавить определенное событие в этот инцидент, если это не было выполнено автоматически. Для этого следует:

1. В разделе **События** найти требуемое событие и открыть его карточку.

2. В правом верхнем углу карточки события нажать кнопку **Добавить в инцидент**.

3. В появившемся диалоговом окне в таблице найти инцидент, с которым требуется связать событие, и отметить его флажком (см. Рис.5.16). При необходимости можно воспользоваться строкой поиска по идентификатору или типу искомого инцидента. Следует отметить, что поиск является регистрозависимым и осуществляется по полному совпадению значений. Также для удобства поиска можно воспользоваться сортировкой по столбцам.

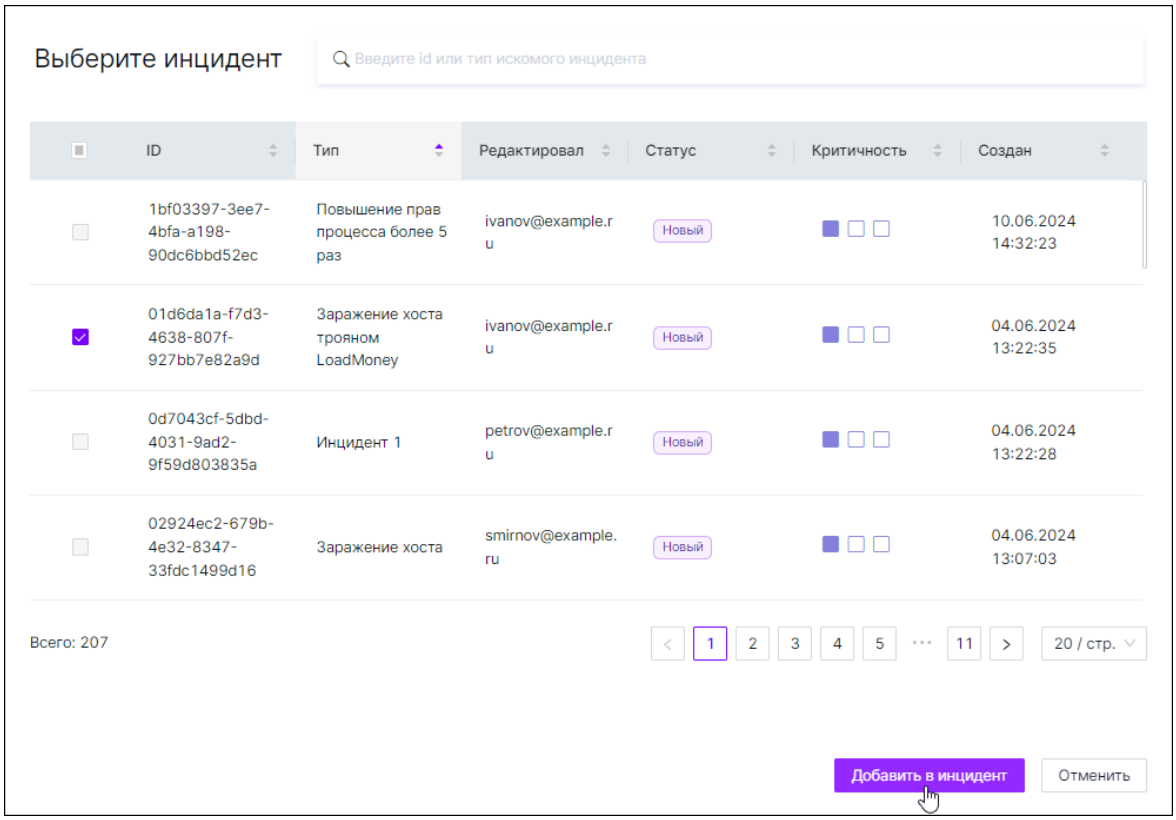


Рис. 5.16. Раздел «События». Окно добавления события в инцидент

4. Нажать кнопку **Добавить в инцидент**.

После этого в правом верхнем углу появится уведомление об успешном добавлении события в инцидент (Рис.5.17).

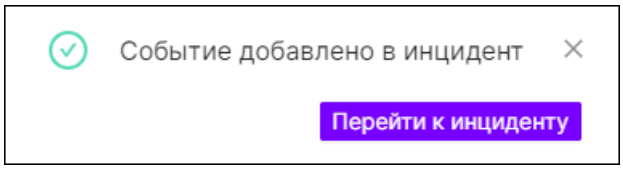


Рис. 5.17. Уведомление об успешном добавлении события в инцидент

При нажатии кнопки **Перейти к инциденту** откроется страница инцидента, в который было добавлено событие. Добавленное в инцидент событие отобразится на странице этого инцидента в списке связанных событий (см. раздел 9.4.2.2). А в карточке события, добавленного в инцидент, появится ссылка на этот инцидент. Если ранее событие имело

Признак инцидента Не обнаружен, то сейчас он изменится на **Обнаружен**. Следует отметить, что изменение признака инцидента может занять до 5 минут.

6. Раздел «Сессии»

Примечание

Раздел веб-интерфейса недоступен в Исполнении 3 (см. раздел 2.5.3).

Раздел **Сессии** (см. Рис.6.1) состоит из следующих областей:

- Наименование раздела.
- Пресеты и временной диапазон для настройки периода отображения информации (см. раздел 6.1).
- Поле для ввода поискового запроса (см. раздел 6.2).
- Вкладки раздела:
  - **Данные** (см. раздел 6.3);
  - **Графики** (см. раздел 6.4). В текущей версии вкладка находится в разработке.

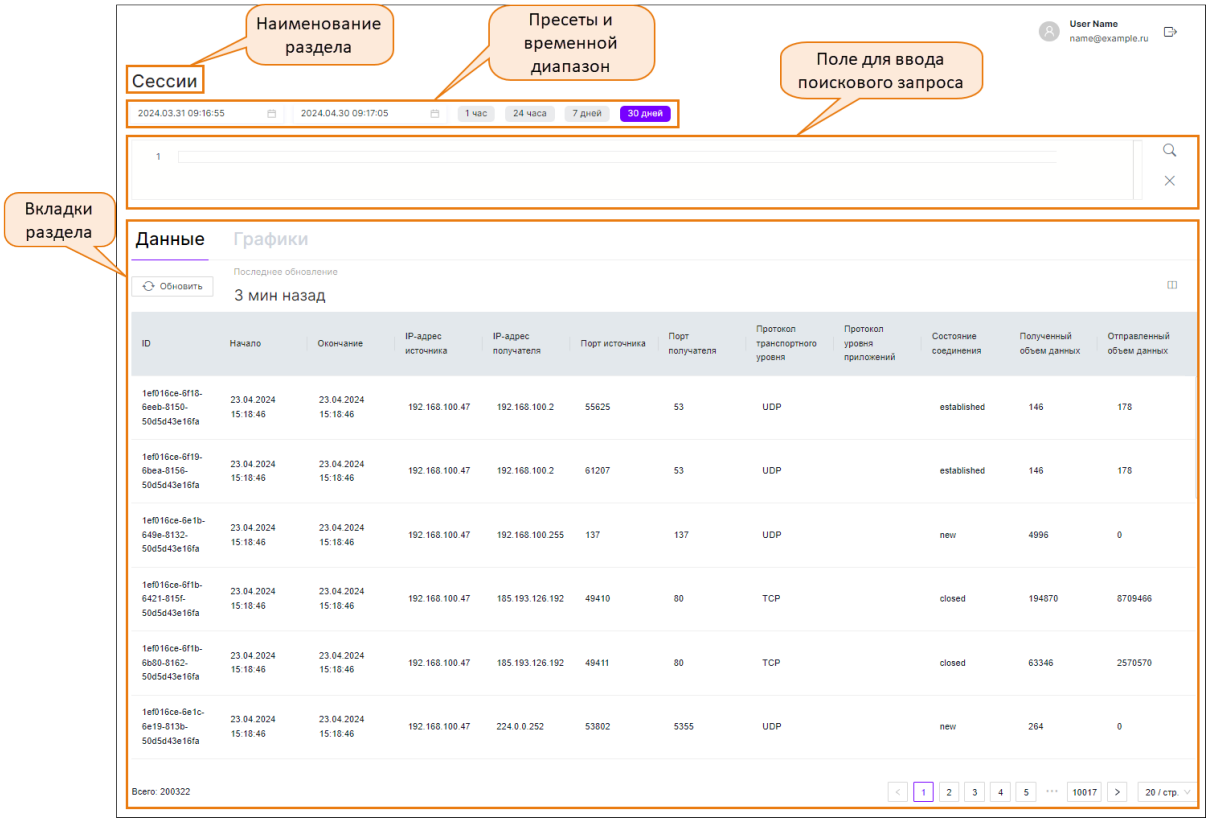


Рис. 6.1. Раздел «Сессии»

6.1. Пресеты и временной диапазон

Информация, размещенная на вкладках **Данные** и **График**, отображается за определенный период времени.

Чтобы изменить период, за который будет отображаться информация, следует воспользоваться преднастроенными пресетами или вручную задать временной диапазон.

Здесь доступны следующие пресеты:

- **1 час** – при выборе данного пресета в таблице и на графиках отобразится информация за последний час.
- **24 часа** – при выборе этого пресета в таблице и на графиках отобразится информация за последние сутки.
- **7 дней** – при выборе данного пресета в таблице и на графиках отобразится информация за последнюю неделю.
- **30 дней** – при выборе этого пресета в таблице и на графиках отобразится информация за последний месяц (30 дней).

Сделает отметить, что после установки определенного пресета значения в полях временного диапазона также изменятся. При необходимости их можно изменить. Для этого следует нажать на значок, расположенный в соответствующих полях слева от пресетов. Откроется окно в виде календаря, в котором требуется выбрать дату и время начала/окончания периода (см. Рис.6.2). При нажатии на ссылку **Сейчас**, расположенную в левом нижнем углу, в поле установятся текущие дата и время.

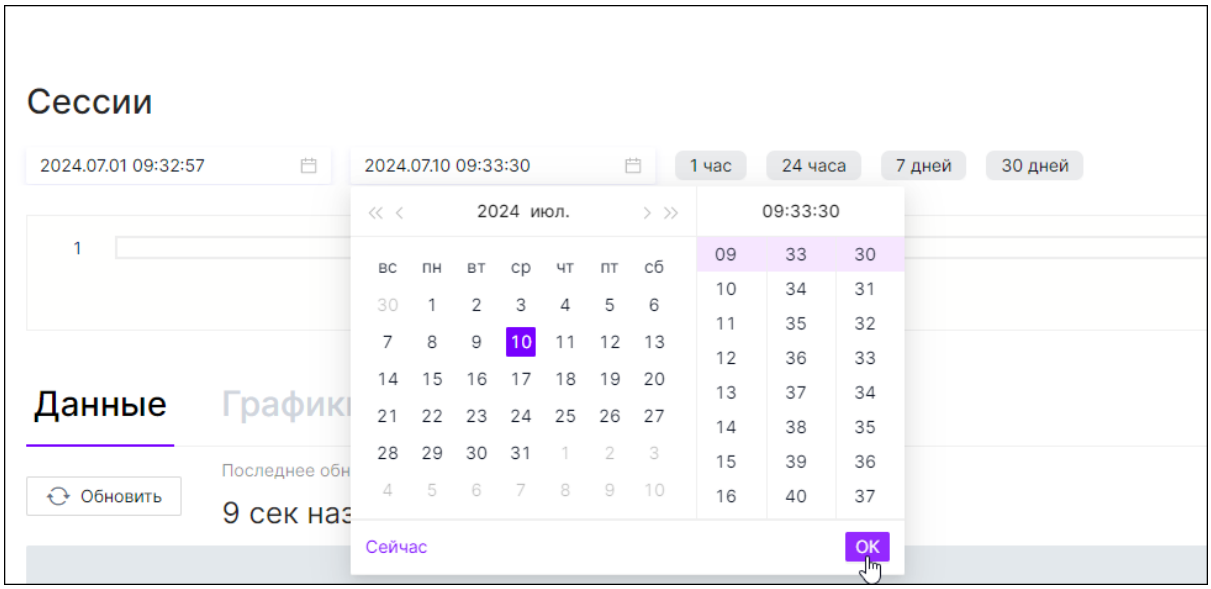


Рис. 6.2. Раздел «Сессии». Настройка временного диапазона

6.2. Поиск сессий с помощью запросов

В разделе **Сессии** присутствует возможность использования поисковых запросов. Эта возможность позволяет задавать гибкие условия поиска и находить требуемые сессии по специфичному запросу, например, по полям используемых протоколов. Чтобы найти сессии с помощью запроса, необходимо выполнить следующие действия:

1. Выбрать требуемый период для поиска сессий с помощью пресетов или временного диапазона (см. раздел 6.1).

2. Ввести текст поискового запроса в специальном поле, расположенном вверху страницы. Описание языка запросов, который используется при поиске сессий, представлено в разделе **Приложение Е, *Описание языка запросов, используемого при поиске сессий***.

3. Нажать на значок 🔍, размещенный справа от поля для ввода.

После этого на странице отобразится информация, удовлетворяющая условиям запроса.

Чтобы сбросить введенный запрос и очистить поле для ввода, следует нажать на значок ✕.

6.3. Вкладка «Данные»

Вкладка **Данные** (Рис.6.1) представляет собой таблицу с информацией о сетевых подключениях – сессиях. Каждая строка таблицы соответствует определенной сессии. Период, за который отображаются сессии в таблице, определяется выбранным пресетом или заданным временным диапазоном (см. раздел 6.1).

Столбцы таблицы содержат следующую информацию:

- **ID** – идентификатор сессии;
- **Начало** – дата и время начала сессии;
- **Окончание** – дата и время окончания сессии;
- **IP-адрес источника** – IP-адрес отправителя трафика;
- **IP-адрес получателя** – IP-адрес получателя трафика;
- **Порт источника** – порт отправителя трафика;
- **Порт получателя** – порт получателя трафика;
- **Протокол транспортного уровня**: **TCP**, **UDP**;
- **Протокол уровня приложений**: **http**, **dhcp**, **ftp**, **dns**, **smtp**, **ssh**, **dce_rpc**, **tls**, **ntlm**, **kerberos**, **rdp**, **smb**, **LDAP**;
- **Состояние соединения** потока данных:
  - **new** – новое;
  - **established** – установлено;
  - **closed** – закрыто;
  - **bypassed** – соединение установлено в обход потока;
- **Полученный объем данных**, в байтах;
- **Отправленный объем данных**, в байтах.

При необходимости можно изменить набор столбцов в таблице. Подробнее об этом см. в разделе 6.3.1).

Слева под таблицей отображается количество записей в таблице с учетом заданного пресета или временного диапазона.

Так же как и в разделе **События**, под таблицей справа расположены кнопки для перехода между страницами. По умолчанию на одной странице таблицы отображаются 20 записей. Для удобства можно изменить количество отображаемых записей на одной странице, нажав на соответствующее поле и выбрав в раскрывающемся списке требуемое число.

При нажатии на кнопку **Обновить**, которая расположена над таблицей, можно оперативно получить актуальную на текущий момент информацию о сессиях без обновления страницы.

Числовой виджет **Последнее обновление**, расположенный справа от кнопки **Обновить**, отображает информацию о последнем обновлении данных в таблице. При наведении курсора мыши на значение появится всплывающее окно с датой и временем последнего обновления.

Примечание

В текущей версии сессии в таблице отсортированы по времени их создания в прямом хронологическом порядке (в конце таблицы находятся самые свежие сессии). Поэтому чтобы просмотреть более новые сессии, необходимо перейти на последние страницы таблицы.

6.3.1. Настройки отображения таблицы с данными о сессиях

Чтобы изменить набор столбцов в таблице, необходимо нажать на значок ◫, расположенный в правом верхнем углу вкладки **Данные**. Помимо основных столбцов, которые отображаются в таблице по умолчанию, здесь присутствуют следующие дополнительные столбцы:

- **Количество переданных пакетов**;
- **Продолжительность потока**, в секундах;
- **Причина прерывания**:
  - **timeout** – ожидание;
  - **forced** – принудительное прерывание;
  - **shutdown** – неисправность;
- **Сработка правила**:
  - **true** – для данной сессии сработало правило политики безопасности;
  - **fasle** – для данной сессии не сработало ни одно из правил политики безопасности;
- **Резервный маршрут**, который может быть использован для перенаправления трафика в случае отказа основного пути:
  - **local** – соединение потока данных установлено в обход;
  - **capture** – трафик захвачен.

Для отображения/скрытия определенного столбца в таблице следует установить/снять соответствующий флажок, расположенный рядом с его названием.

6.3.2. Карточка сессии

Чтобы открыть карточку требуемой сессии, необходимо найти сессию в таблице и нажать на строку, в которой она записана.

Карточка сессии содержит:

- **ID** – идентификатор сессии (отображается в заголовке карточки);
- общие сведения:
  - **Время сессии** – дата и время начала и окончания сессии;
  - **Адресаты** – IP-адреса источника и получателя трафика;
  - **Порты** – порты источника и получателя трафика;
  - **Объем данных**: полученные и отправленные данные, в байтах;
  - **Протоколы** – наименования протоколов уровня приложений и транспортного уровня;
  - **Состояние** соединения потока данных;
- вкладки:
  - **Детализация**;
  - **Протоколы**;
  - **Файлы**.

Нажав на значок , расположенный на карточке сессии, можно скопировать идентификатор данной сессии, чтобы в дальнейшем поделиться с коллегами или использовать в процессе расследования.

В правом верхнем углу карточки сессии расположена кнопка вызова меню действий – ⋮. Она позволяет скачать информацию о сессии в файл формата PCAP.

6.3.2.1. Карточка сессии. Вкладка «Детализация»

На вкладке **Детализация** (см. Рис.6.3) отображается следующая информация:

- **Количество переданных пакетов**;
- **Продолжительность потока**, в секундах;
- **Сработка правила**;
- **Причина прерывания**.

Некоторые поля могут не отображаться на карточке сессии, если они пустые.

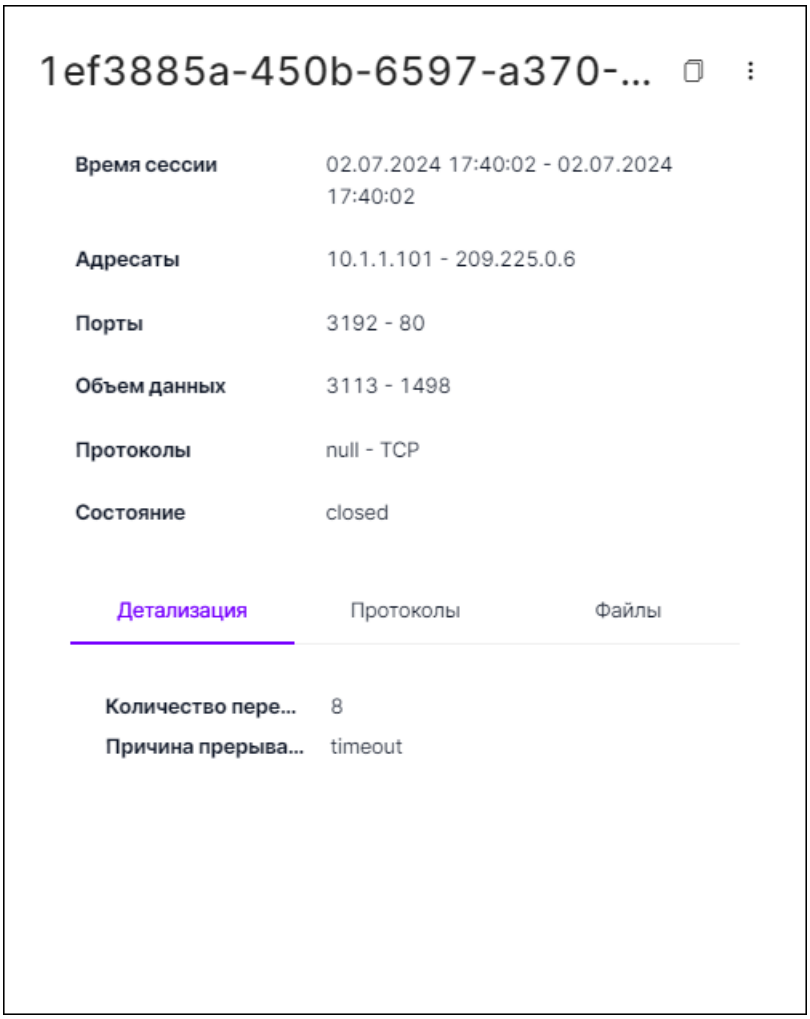


Рис. 6.3. Карточка сессии. Вкладка «Детализация»

6.3.2.2. Карточка сессии. Вкладка «Протоколы»

На вкладке **Протоколы** (см. Рис.6.4) размещены блоки с детальной информацией об используемых протоколах транспортного уровня и уровня приложений.

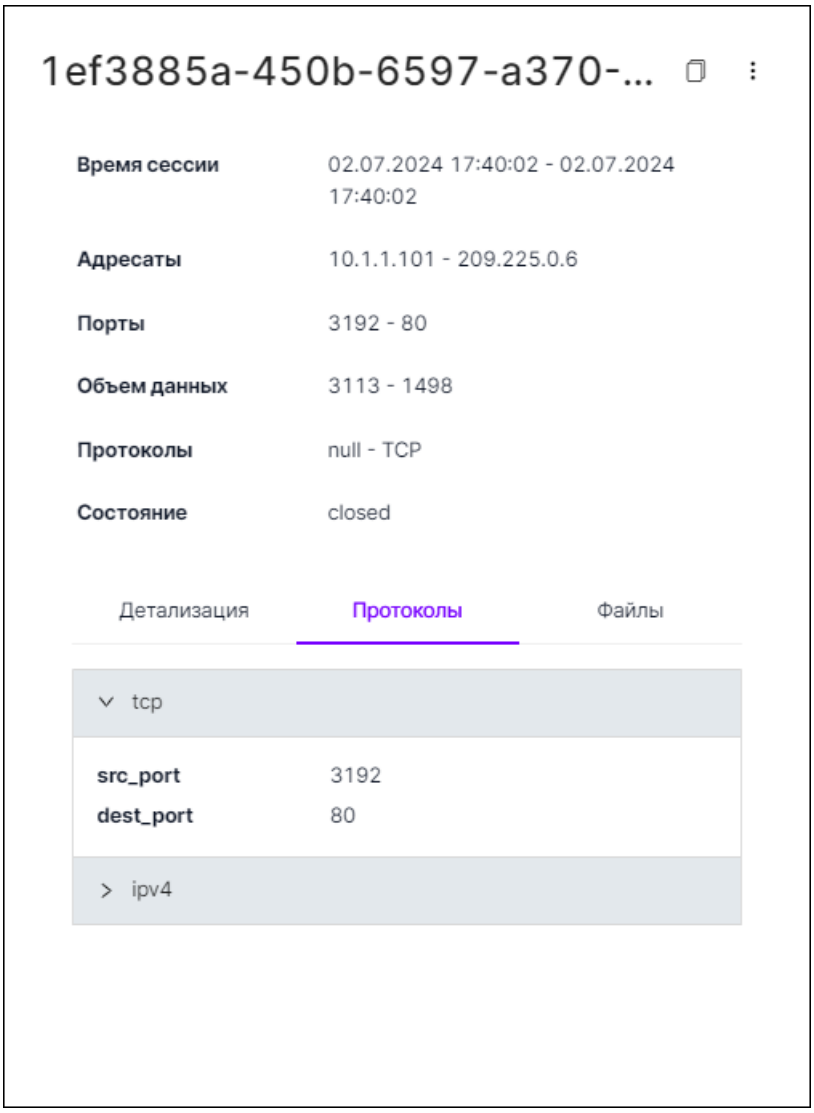


Рис. 6.4. Карточка сессии. Вкладка «Протоколы»

6.3.2.3. Карточка сессии. Вкладка «Файлы»

Вкладка **Файлы** (см. Рис.6.5) содержит файлы, которые передаются в рамках сессии. В дальнейшем это позволит произвести их анализ и определить, являются ли они вредоносными. Информация на вкладке разбита на блоки. Каждый блок соответствует определенному файлу. Внутри блока размещаются следующие данные:

- **Идентификатор файла**;
- **Тип файла**;
- **Имя файла**;
- **Размер файла**.

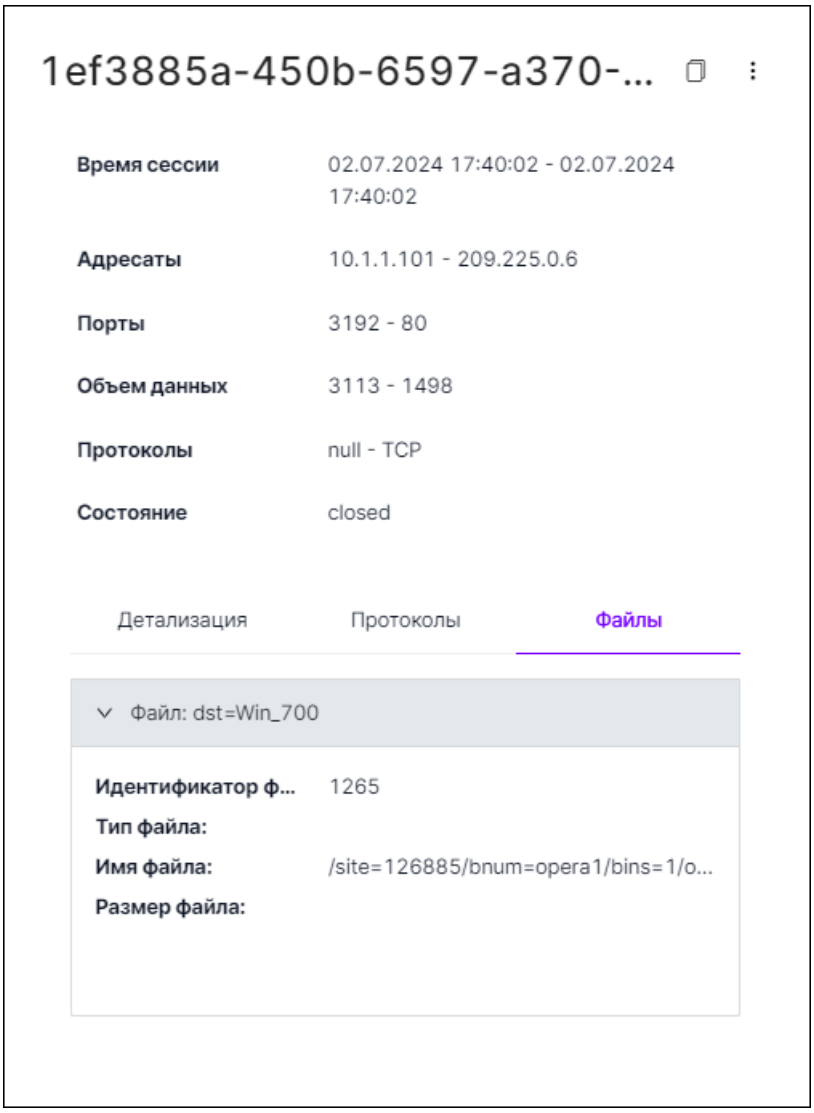


Рис. 6.5. Карточка сессии. Вкладка «Файлы» (иллюстрация будет обновлена после завершения разработки)

6.4. Вкладка «Графики»

Вкладка находится в разработке.

7. Раздел «Сеть»

Примечание

Раздел веб-интерфейса недоступен в Исполнении 2 (см. раздел 2.5.2).

Раздел **Сеть** содержит информацию о добавленных в систему объектах защиты (хостах). Для удобства работы с большим количеством хостов, а также для распространения на них правил политики, хосты объединяются в группы. Группы хостов имеют иерархическую структуру.

После перехода в раздел **Сеть** отобразится страница, которая состоит из следующих областей (см. Рис.7.1):

- заголовок страницы;
- панель навигации по группам хостов;
- фильтры;
- таблица с данными о хостах;
- карточка хоста.

Рис. 7.1. Раздел «Сеть»

7.1. Таблица с данными о хостах

Данные обо всех объектах защиты, добавленных в систему, представлены в виде таблицы. Состав и количество хостов, отображаемых в таблице, зависит от выбранной группы хостов на панели навигации (см. раздел 7.3).

Каждая строка таблицы соответствует определенному хосту. Столбцы таблицы содержат следующую информацию о хостах:

- **Полное имя хоста**;
- **Код устройства** – уникальный генерируемый системой код устройства;
- **ОС** – операционная система;
- **Критичность** – уровень критичности хоста в виде шкалы из трех значений, где: ■ □ □ – низкий уровень критичности, ■ ■ ■ – высокий уровень критичности;
- **Статус агента**: **Активен**, **Деактивирован**, **Неактивен**, **Не установлен**. Подробное описание статусов агента см. в разделе 7.5.

Слева от каждого хоста расположен флажок, который используется при перемещении хостов из одной группы в другую – действия при этом аналогичны действиям при перемещении правил из одной группы в другую (подробнее см. в разделе 10.1.3.4).

При необходимости можно изменить набор столбцов в таблице – действия при этом аналогичны действиям при настройке таблицы со списком событий (подробнее см. в разделе 5.3.1).

Кроме того, для удобства можно изменить ширину таблицы. Для этого следует захватить мышью вертикальный разделитель между таблицей и карточкой хоста и перетащить его вправо (для расширения столбцов) или влево (для сужения).

Слева под таблицей отображается количество записей в таблице с учетом фильтрации (см. раздел 7.4), а также выбранной группы хостов на панели навигации (см. раздел 7.3).

Так же, как и в разделе **События**, под таблицей справа расположены кнопки для перехода между страницами. По умолчанию на одной странице таблицы отображаются 20 записей. Для удобства можно изменить количество отображаемых записей на одной странице, нажав на соответствующее поле и выбрав в раскрывающемся списке требуемое число.

7.1.1. Сортировка хостов в таблице

По умолчанию хосты в таблице отсортированы в порядке их добавления. Для удобства работы можно изменить порядок отображения хостов в таблице, нажав на значок ⇕ в названии требуемого столбца. Настройки сортировки таблицы в разделе **Сеть** аналогичны настройкам в разделе **События** (см. раздел 5.2.1).

7.2. Заголовок страницы «Сеть»

В заголовке страницы **Сеть** содержатся:

- название текущего раздела;
- кнопка Фильтры / Фильтры – **Фильтры**, позволяющая развернуть/свернуть панель с полями для фильтрации;
- кнопка **Обновить**, с помощью которой можно оперативно получить актуальную на текущий момент информацию о хостах без обновления страницы;

- кнопка **Переместить**, которая предназначена для перемещения хостов из одной группы в другую – действия при этом аналогичны действиям при перемещении правил из одной группы в другую (подробнее см. в разделе 10.1.3.4).
- сводная информация по хостам:
  - **Всего** – общее количество хостов в таблице.
  - **Онлайн** – количество агентов со статусами **Активен** или **Деактивирован**.
  - **С проблемами** – количество хостов с открытыми инцидентами.
  - **Последнее обновление** – информация о последнем обновлении данных в таблице. При наведении курсора мыши на значение отобразится информация о дате и времени последнего обновления.
- значок ◫ для настройки отображения таблицы – действия аналогичны действиям при настройке отображения таблицы событий (см. раздел 5.3.1).

7.3. Панель навигации по группам хостов

В левой части страницы расположена панель навигации по группам хостов (см. Рис.7.2).

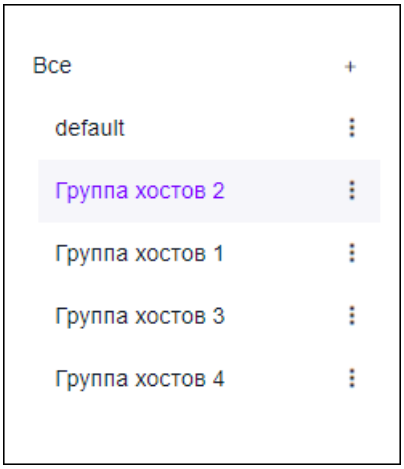


Рис. 7.2. Раздел «Сеть». Панель навигации по группам хостов

Панель навигации имеет древовидную структуру. По умолчанию на самом верхнем уровне расположен элемент **Все**. При нажатии на этот элемент в таблице отображаются все хосты из всех групп. На втором уровне размещены группы, добавленные пользователем, а также системная группа **default**, которую нельзя удалить. При выборе определенной группы в таблице отображаются только хосты, входящие в эту и дочерние группы.

Примечание

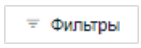
Следует отметить, что в текущей версии панель навигации имеет только два уровня вложенности. Это значит, что все создаваемые группы хостов будут находиться на втором уровне. Внутри групп второго уровня нельзя создавать новые группы.

Таким образом, если требуется отобразить в таблице все хосты, необходимо нажать на элемент **Все**. Если нужно показать только хосты из определенной группы, следует найти требуемую группу и нажать на ее название. При этом количество хостов, входящих в эту группу, можно увидеть под таблицей слева в поле **Всего**.

Здесь доступны следующие возможности:

- добавление новой группы хостов – действия аналогичны действиям при добавлении новой группы правил (подробнее см. в разделе 10.1.3.1);
- удаление группы хостов – действия аналогичны действиям при удалении группы правил (подробнее см. в разделе 10.1.3.2);
- изменение названия группы хостов – действия аналогичны действиям при изменении названия группы правил (подробнее см. в разделе 10.1.3.3).

7.4. Фильтры хостов

Чтобы открыть панель с полями для фильтрации, необходимо нажать кнопку 

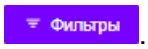
, расположенную в заголовке страницы.

Примечание

Набор полей для фильтрации может различаться в зависимости от настроек отображения таблицы.

Фильтрация возможна по следующим полям:

- **Полное имя хоста** – значение вводится с клавиатуры.
- **Код устройства** – значение вводится с клавиатуры. Поиск по этому полю является регистрозависимым.
- **ОС** – название операционной системы вводится с клавиатуры. Поиск по этому полю является регистрозависимым.
- **Критичность** – уровень критичности хоста. С помощью флажков выбирается одно или несколько значений.
- **Статус агента**. С помощью флажков выбирается одно или несколько значений.

Чтобы отфильтровать таблицу хостов по заданным параметрам, следует нажать кнопку **Применить** или клавишу **Enter** на клавиатуре. После этого значение в поле **Всего**, которое расположено под таблицей хостов слева, также изменится. Очистить поля для фильтрации и вернуть таблицу в исходный вид позволяет кнопка **Сбросить**. Для скрытия области работы с фильтрами необходимо нажать кнопку 

.

7.5. Карточка хоста

Справа от таблицы расположена карточка хоста. По умолчанию при переходе в раздел **Сеть** открывается карточка первого хоста из таблицы. Чтобы открыть карточку требуе-

мого хоста, необходимо найти его в таблице и нажать на строку, в которой этот хост записан.

Карточка хоста (см. Рис.7.3) содержит следующую информацию:

- Имя хоста (отображается в заголовке карточки).
- Числовой виджет **События**, который показывает количество событий, обнаруженных агентом на хосте:
  - за неделю;
  - за сутки;
  - за последний час.
- Блок **Основные параметры**:
  - **Статус агента**:
    - **Активен** – штатный режим работы агента: сервисы агента включены, осуществляется сбор и отправка событий на сервер.

      Примечание

      *Следует обратить внимание, что в текущей версии статус **Активен** также может присваиваться агенту в случае успешной установки ADAM и неуспешной установки агента. Однако в этом случае в поле **Версия агента** будет отображено значение **0.0.0.0** или **unknown**, а в поле **Концентратор** и **Анализатор** будет прочерк. Чтобы выяснить причину неуспешной установки агента, следует ознакомиться с лог-файлами, расположенными в папках C:\Program Files (x86)\SolarUpdaterEDR\logs и C:\Program Files (x86)\SolarUpdaterEDR\update.*
    - **Деактивирован** – аварийная остановка сервисов агента: прекращен сбор событий с агента и отправка их на сервер.
    - **Неактивен** – хост, на котором установлен агент, выключен.
    - **Не установлен** – агент отсутствует на хосте (удален).
  - **Версия агента** – номер текущей версии агента, установленного на хосте.
  - **Концентратор** – текущая версия конфигурации концентратора на агенте.
  - **Анализатор** – текущая версия конфигурации анализатора на агенте.
  - **Код устройства** – уникальный генерируемый системой код устройства.
  - **IP-адрес** – последний IP-адрес, с которого хост был активен. В текущей версии IP-адрес не отображается.
  - **Группа хоста** – группа, к которой относится хост.
  - **Тип устройства** – тип устройства хоста: **Сервер**, **Рабочая станция**, **VM**, **Ноутбук**. В текущей версии тип устройства не отображается.

- **Критичность** – уровень значимости хоста.
- **Политики безопасности** – политики, применяемые на хосте.
- **Версия политик** – версия политик, применяемых на хосте.

- Блок **Характеристики**:
  - **Процессор** – наименование процессора.
  - **Количество ядер**.
  - **Оперативная память**.
  - **ОС** – операционная система.
  - **Жесткие диски** – информация о жестких дисках на устройстве.

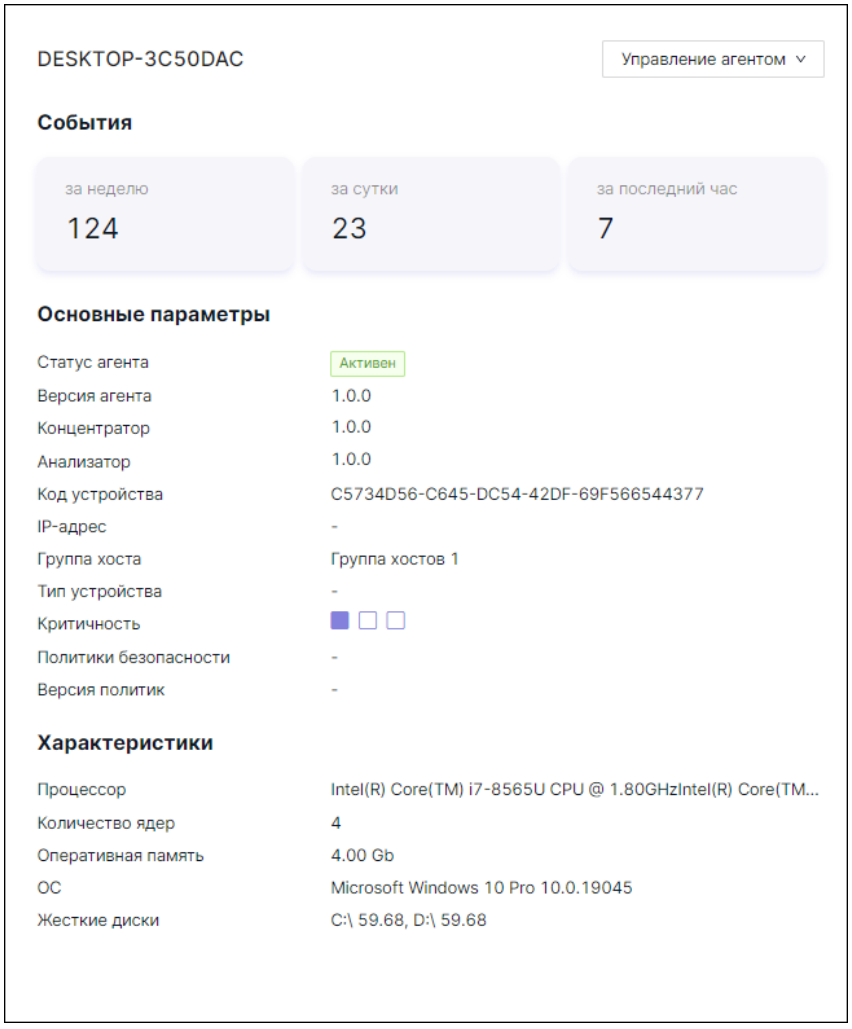


Рис. 7.3. Карточка хоста

В правом верхнем углу карточки хоста размещена кнопка меню **Управление агентом**, которая позволяет активировать/деактивировать агент (см. раздел 7.6) или удалить его (см. раздел 7.7). Кнопка **Управление агентом** недоступна, если статус агента **Неактивен** или **Не установлен**.

7.6. Управление агентом: деактивация/активация

7.6.1. Деактивация агента

Деактивация агента – это аварийная остановка служб агента: прекращение сбора событий и отправки их на сервер.

Чтобы временно деактивировать агент, например, с целью проведения расследования в случае его компрометации, необходимо выполнить следующие действия:

1. В разделе **Сеть** открыть карточку хоста, на котором установлен требуемый агент.
2. В правом верхнем углу карточки нажать кнопку меню **Управление агентом** и выбрать пункт **Деактивация**. Следует отметить, что деактивировать можно только агент со статусом **Активен**.
3. В появившемся диалоговом окне (см. Рис.7.4) подтвердить деактивацию агента, нажав на соответствующую кнопку.

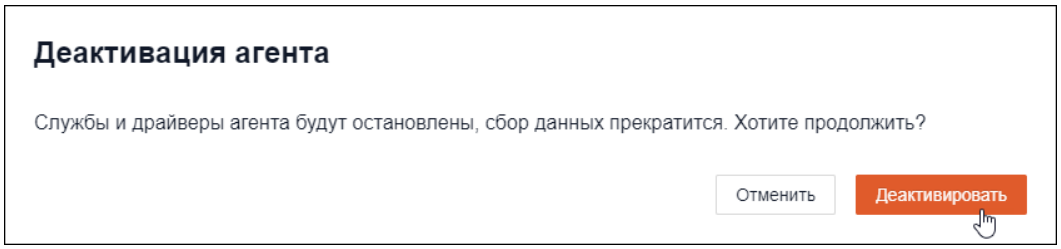


Рис. 7.4. Диалоговое окно подтверждения деактивации агента

4. После подтверждения в правом верхнем углу страницы отобразится сообщение об отправке запроса на деактивацию агента (см. Рис.7.5).

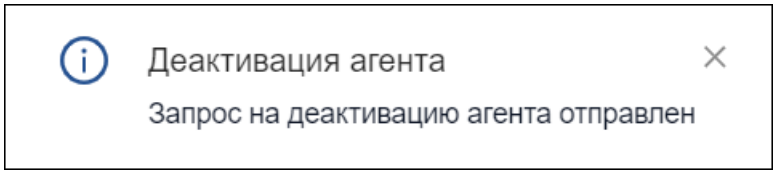


Рис. 7.5. Окно с сообщением об отправке запроса на деактивацию агента

После успешной деактивации статус агента изменится на **Деактивирован**, а в разделе **События** появится новое событие **DeactivationOn**. В карточке такого события в атрибуте **OperationResult** будет записано значение **success**.

В случае неуспешной деактивации статус агента останется прежним, а в разделе **События** появится новое событие **DeactivationOn**. В карточке такого события в атрибуте **OperationResult** будет записано значение **failure**.

7.6.2. Активация агента

Активация агента – это отключение деактивации агента, то есть возобновление работы агента в штатном режиме: включаются сервисы агента, возобновляется сбор и отправка событий на сервер.

Чтобы активировать агент, необходимо выполнить следующие действия:

1. В разделе **Сеть** открыть карточку хоста, на котором установлен требуемый агент.
2. В правом верхнем углу карточки нажать кнопку меню **Управление агентом** и выбрать пункт **Активация**. Следует отметить, что активировать можно только агент со статусом **Деактивирован**.
3. В появившемся диалоговом окне (см. Рис.7.6) подтвердить активацию агента, нажав на соответствующую кнопку.

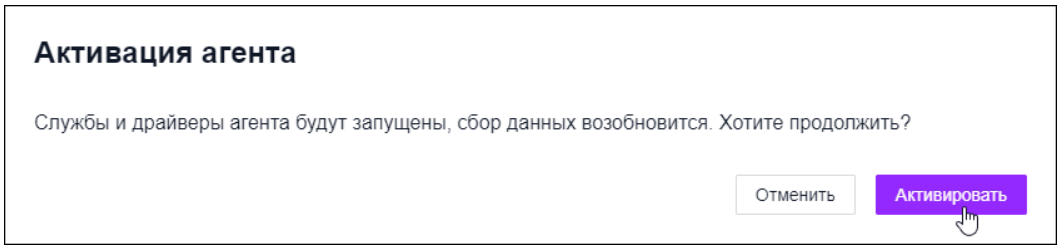


Рис. 7.6. Диалоговое окно подтверждения активации агента

4. После подтверждения в правом верхнем углу страницы отобразится сообщение об отправке запроса на активацию агента (см. Рис.7.7).

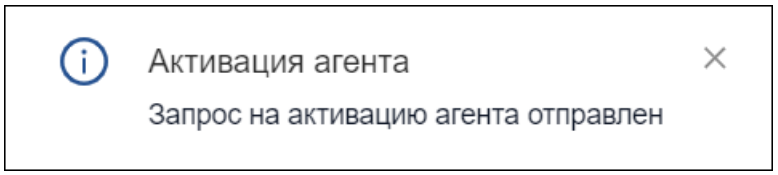


Рис. 7.7. Окно с сообщением об отправке запроса на активацию агента

После успешной активации статус агента изменится на **Активен**, а в разделе **События** появится новое событие **DeactivationOff**. В карточке такого события в атрибуте **OperationResult** будет записано значение **success**.

При неуспешной активации статус агента остается прежним, а в разделе **События** появится новое событие **DeactivationOff**. В карточке такого события в атрибуте **OperationResult** будет записано значение **failure**.

Примечание

*В случае неуспешной активации агента успешно запущенные службы остаются запущенными, однако статус агента остается **Деактивирован**, так как полноценная активация не была выполнена.*

7.7. Управление агентом: удаление

Чтобы удалить агент с хоста, необходимо выполнить следующие действия:

1. В разделе **Сеть** открыть карточку хоста, на котором установлен требуемый агент.

2. В правом верхнем углу карточки нажать кнопку меню **Управление агентом** и выбрать пункт **Удаление**.

3. В появившемся диалоговом окне (см. Рис.7.8) подтвердить удаление агента с хоста, нажав на соответствующую кнопку.

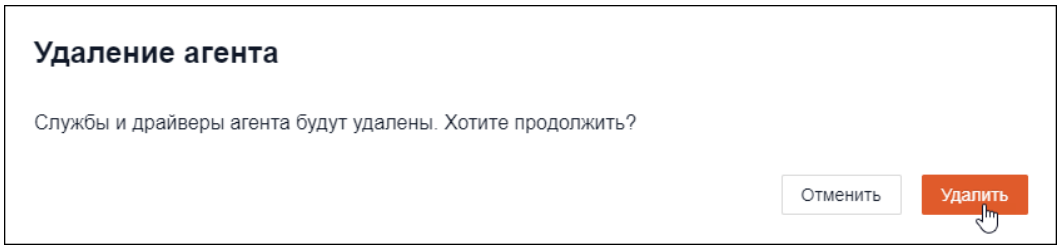


Рис. 7.8. Диалоговое окно подтверждения удаления агента

4. После подтверждения в правом верхнем углу страницы отобразится сообщение об отправке запроса на удаление агента (см. Рис.7.9).

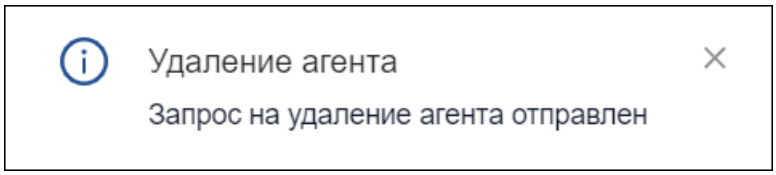


Рис. 7.9. Окно с сообщением об отправке запроса на удаление агента

После успешного удаления статус агента в карточке хоста изменится на **Не установлен**. В зависимости от результата удаления агента в разделе **События** появятся соответствующие события:

- **AgentRemoveStarted** – старт удаления агента.
- **AgentRemoveComplete** – результат удаления агента: **success** – при успешном удалении агента с хоста, **failure** – при неуспешном удалении.
- **AdamRemoveFailed** – неуспешный старт удаления ADAM.

8. Раздел «Политики»

Политика – это совокупность правил, регулирующих управление, защиту и распределение информационных ресурсов.

Раздел **Политики** предназначен для настройки механизма взаимодействия компонентов Solar EDR и Solar NTA. Политика включает в себя перечень наборов правил, которые действуют на определенные группы хостов.

После перехода в данный раздел отобразится страница, которая состоит из следующих областей (см. Рис.8.1):

- заголовок страницы;
- фильтры;
- таблица со списком политик.

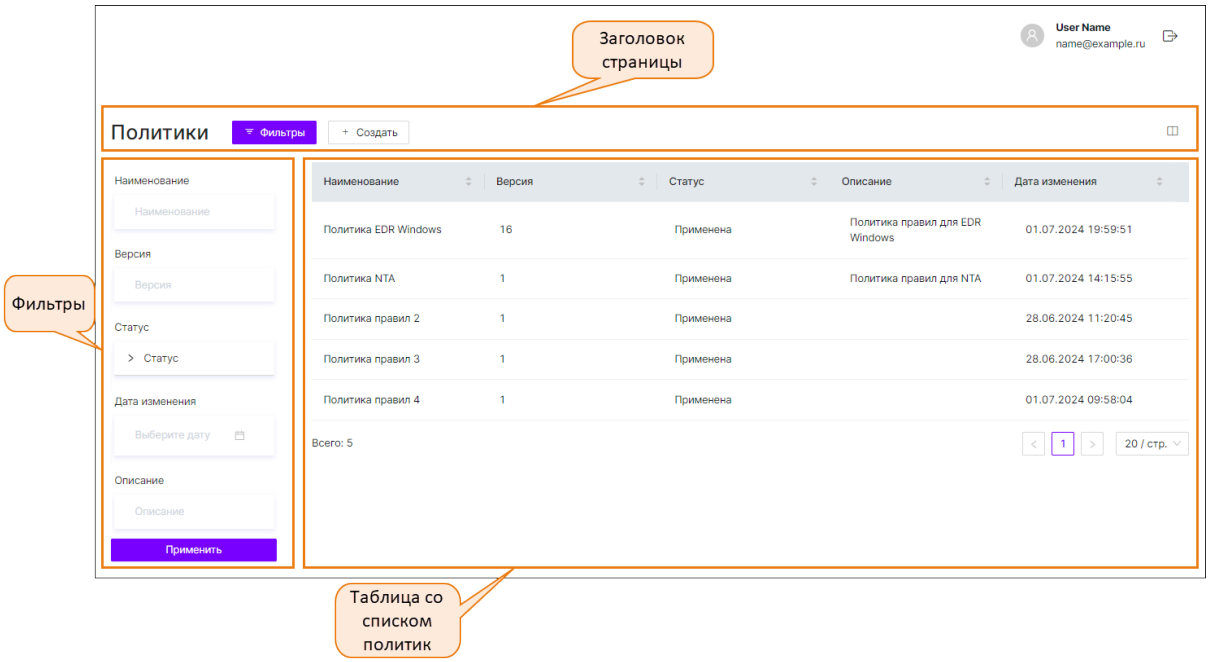


Рис. 8.1. Раздел «Политики»

8.1. Таблица со списком политик

Информация о политиках представлена в виде таблицы. Каждая строка таблицы соответствует определенной политике. Столбцы таблицы содержат следующую информацию:

- **Наименование** политики.
- **Версия**.
- **Статус** политики: **Применена**/**Изменена** (подробнее о статусах политик см. в разделе 8.4.1).
- **Описание** – краткая информация о политике.

- **Дата изменения** – дата и время внесения последних изменений в политику. Если политика еще не изменялась, здесь будет отображаться дата ее создания.

При необходимости можно изменить набор столбцов в таблице – действия при этом аналогичны действиям при настройке таблицы со списком событий (подробнее см. в разделе 5.3.1).

Слева под таблицей отображается количество записей в таблице с учетом фильтрации (см. раздел 8.3).

Так же как и в разделе **События**, под таблицей справа расположены кнопки для перехода между страницами. По умолчанию на одной странице таблицы отображаются 20 записей. Для удобства можно изменить количество отображаемых записей на одной странице, нажав на соответствующее поле и выбрав в раскрывающемся списке требуемое число.

8.1.1. Сортировка политик в таблице

По умолчанию политики в таблице отсортированы в алфавитном порядке. Для удобства работы можно изменить порядок отображения политик в таблице, нажав на значок в названии требуемого столбца. Настройки сортировки таблицы в разделе **Политики** аналогичны настройкам в разделе **События** (см. раздел 5.2.1).

8.2. Заголовок страницы «Политики»

В заголовке страницы **Политики** содержатся:

- название текущего раздела;
- кнопка Фильтры / Фильтры – **Фильтры**, позволяющая развернуть/свернуть панель с полями для фильтрации;
- кнопка **Создать**, позволяющая добавить новую политику (подробнее о создании новой политики см. в разделе 8.5);
- значок для настройки отображения таблицы – действия аналогичны действиям при настройке отображения таблицы событий (см. раздел 5.3.1).

8.3. Фильтры политик

Чтобы открыть панель с полями для фильтрации, необходимо нажать кнопку Фильтры, расположенную в заголовке страницы.

Примечание

Набор полей для фильтрации может различаться в зависимости от настроек отображения таблицы.

Фильтрация возможна по следующим полям:

- **Наименование** – позволяет найти политику по ее названию. Значение вводится с клавиатуры. Поиск по этому полю является регистрозависимым.

- **Версия** – параметр используется для поиска политик по номеру версии. Значение вводится с клавиатуры. Поиск осуществляется по полному совпадению значения.
- **Статус** – параметр используется для поиска политик по статусу. Значение выбирается из раскрывающегося списка.
- **Дата изменения** – фильтр позволяет найти политики, которые были последний раз отредактированы в заданном диапазоне времени. Для этого следует нажать на значок , расположенный в соответствующем поле. Откроется окно в виде календаря, в котором требуется выбрать дату и время и нажать кнопку **ОК**
- **Описание** – позволяет найти политику по ее описанию. Значение вводится с клавиатуры. Поиск по этому полю является регистрозависимым.

Чтобы отфильтровать таблицу политик по заданным параметрам, следует нажать кнопку **Применить** или клавишу **Enter** на клавиатуре. После этого значение в поле **Всего**, которое расположено под таблицей политик слева, также изменится. Очистить поля для фильтрации и вернуть таблицу в исходный вид позволяет кнопка **Сбросить**. Для скрытия области работы с фильтрами необходимо нажать кнопку Фильтры.

8.4. Страница политики

Чтобы открыть страницу требуемой политики, необходимо найти эту политику в таблице и нажать на строку, в которой она записана.

Страница политики (см. Рис.8.2) состоит из следующих областей:

- Заголовок страницы:
  - указатель текущей страницы (при нажатии на ссылку **Список политик** будет осуществлен переход на предыдущую страницу со списком политик);
  - наименование политики.
- Блок с основной информацией о политике (см. раздел 8.4.1).
- Вкладки:
  - **Область применения** (см. раздел 8.4.2);
  - **Наборы правил** (см. раздел 8.4.3).
- Область действий с политикой:
  - кнопка **Применить версию**, позволяющая распространить внесенные в политику изменения (при изменении области применения или перечня наборов правил);
  - значок , позволяющий внести изменения в политику (подробнее об этом см. в разделе 8.6);
  - значок , позволяющий удалить политику (подробнее см. в разделе 8.7).

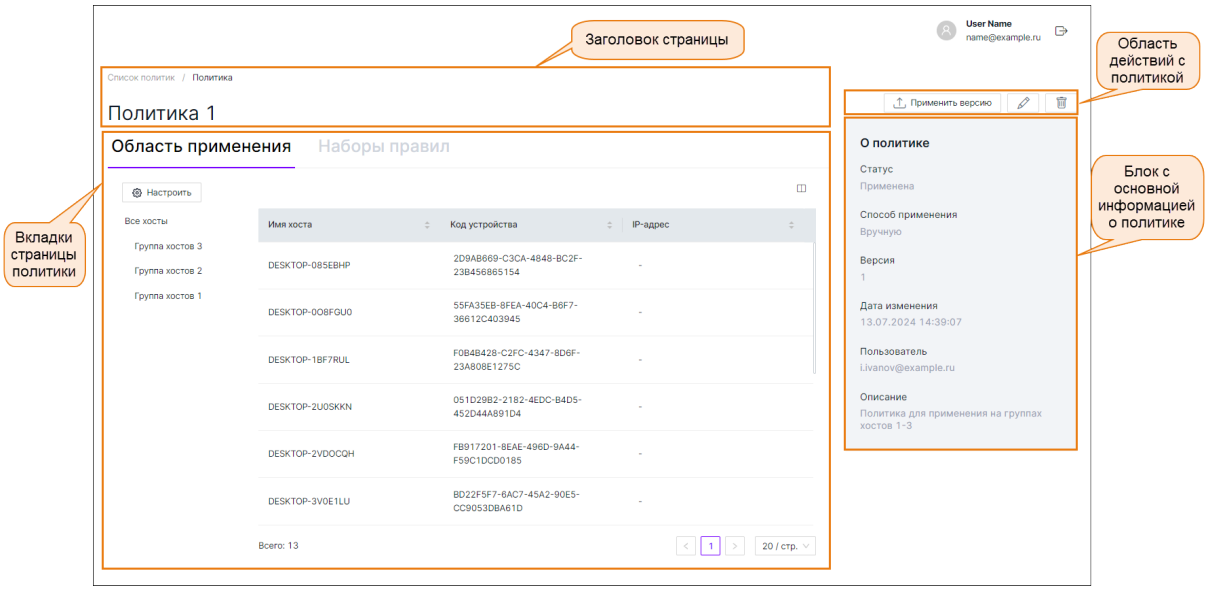


Рис. 8.2. Страница политики

8.4.1. Основная информация о политике

В блоке с основой информацией о политике содержатся следующие сведения:

- **Статус** политики:
  - **Применена** – текущая версия политики сконвертирована корректно;
  - **Изменена** – в текущую версию политики внесены изменения, которые еще не были применены к области применения. Статус присваивается политике в следующих случаях:
    - при изменении перечня наборов правил, включенных в политику;
    - при изменении перечня правил в составе наборов, включенных в политику.
- **Способ применения**:
  - **Автоматизировано** – изменения, внесенные в политику, распространяются на область применения автоматически;
  - **Вручную** – изменения, внесенные в политику, распространяются на область применения вручную с помощью кнопки **Применить версию**.

Примечание

*В текущей версии доступен только один **Способ применения** – **Вручную**.*

- **Версия** – номер версии политики. Версия политики изменяется в следующих случаях:
  - при изменении перечня наборов правил, включенных в политику;
  - при изменении версий правил в составе наборов, включенных в политику.

Примечание

Следует обратить внимание, что в текущей версии номер версии политики изменится только после нажатия кнопки ***Применить версию****.*

- **Дата изменения** – дата и время внесения последних изменений в политику. Если в политику еще не вносились изменения, здесь будут отображаться дата и время ее создания.
- **Пользователь** – пользователь, который последним внес изменения в политику. Если в политику еще не вносились изменения, здесь будет отображаться ее автор.
- **Описание** – краткое описание политики. Если описание не задано, то поле не отображается на странице политики.

8.4.2. Вкладка «Область применения»

Вкладка **Область применения** содержит информацию о хостах, на которые распространяются правила политики.

Вкладка состоит из следующих элементов (см. Рис.8.3):

- кнопка для настройки области применения политики;
- панель навигации по группам хостов в области применения политики;
- таблица со списком хостов в области применения политики.

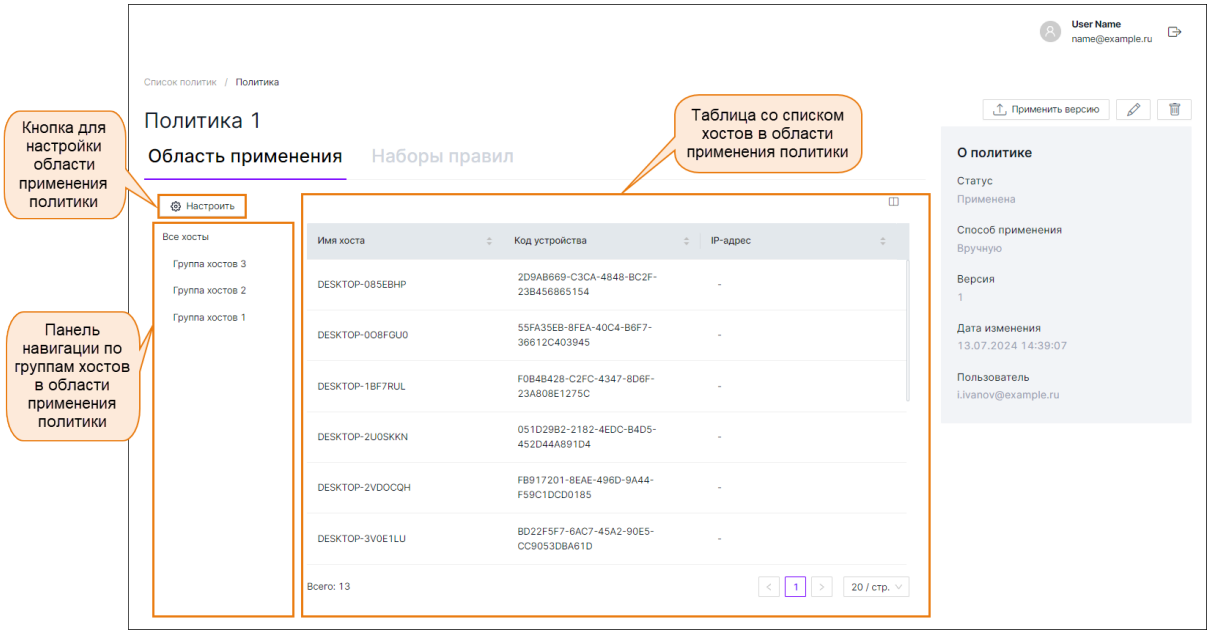


Рис. 8.3. Страница политики. Вкладка «Область применения»

8.4.2.1. Таблица со списком хостов в области применения политики

На центральной части страницы расположена таблица со списком хостов, включенных в область применения политики. Состав и количество хостов, отображаемых в таблице, зависит от выбранной группы хостов на панели навигации (см. раздел 8.4.2.2).

Каждая строка таблицы соответствует определенному хосту. Столбцы таблицы содержат следующую информацию:

- **Имя хоста** – полное имя хоста.
- **Код устройства** – уникальный генерируемый системой код устройства.
- **IP-адрес** – последний IP-адрес, с которого хост был активен. В текущей версии IP-адрес не отображается.

При необходимости можно изменить набор столбцов в таблице – действия при этом аналогичны действиям при настройке таблицы со списком событий (подробнее см. в разделе 5.3.1).

Слева под таблицей отображается количество записей в таблице с учетом выбранной группы хостов на панели навигации (см. раздел 8.4.2.2).

Так же как и в разделе **События**, под таблицей справа расположены кнопки для перехода между страницами. По умолчанию на одной странице таблицы отображаются 20 записей. Для удобства можно изменить количество отображаемых записей на одной странице, нажав на соответствующее поле и выбрав в раскрывающемся списке требуемое число.

8.4.2.2. Панель навигации по группам хостов в области применения политики

Слева от таблицы расположена панель навигации по группам хостов, которые входят в область применения политики.

Если требуется отобразить в таблице все хосты, на которые распространяется политика, необходимо нажать на элемент **Все**. Если нужно показать только хосты из определенной группы, следует найти требуемую группу и нажать на ее название. При этом количество хостов, включенных в эту группу, будет показано под таблицей слева в поле **Всего**.

Управлять набором групп хостов, на которые распространяется политика, можно с помощью кнопки **Настроить**. Подробнее об этом см. в разделе 8.4.2.3.

8.4.2.3. Настройка области применения политики

Чтобы изменить область применения политики, необходимо выполнить следующие действия:

1. В разделе **Политики** открыть карточку требуемой политики на вкладке **Область применения**.
2. Нажать кнопку **Настроить**.
3. В появившемся диалоговом окне (см. Рис.8.4) слева будет отображен список доступных для выбора групп хостов, а справа – список групп, включенных в область применения политики.

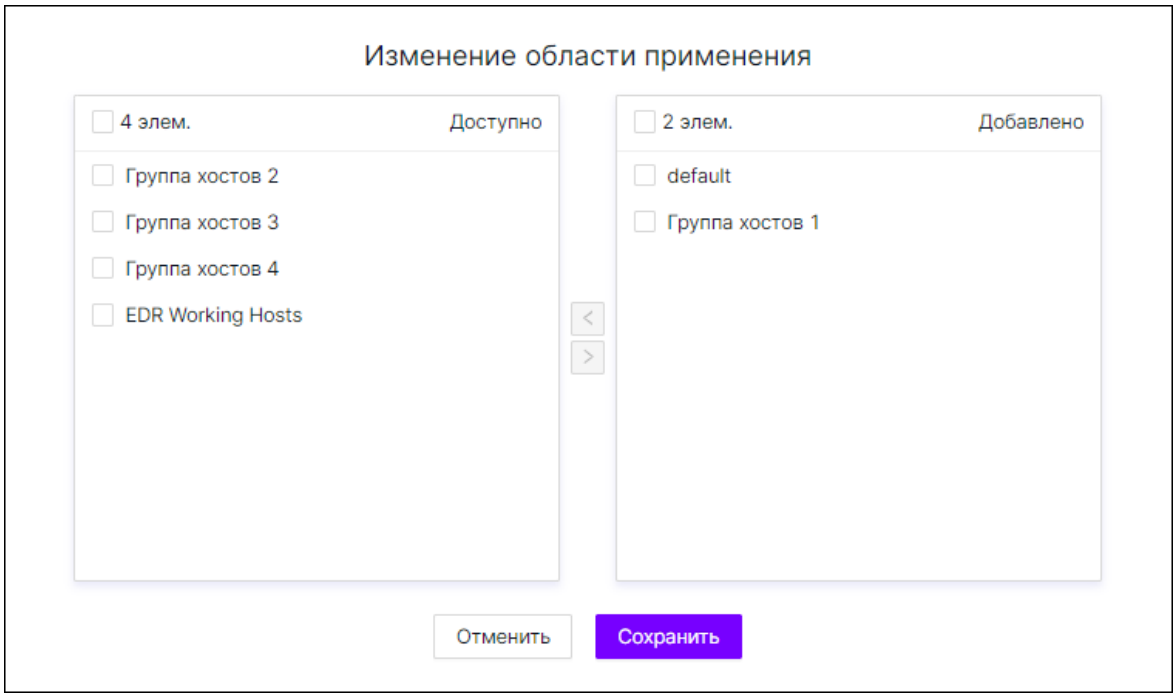


Рис. 8.4. Страница политики. Вкладка «Область применения». Настройка области применения

Здесь пользователь может выполнить следующие действия:

- Добавить группы хостов в область применения политики. Для этого следует в списке **Доступно** отметить флажками требуемые группы и нажать кнопку . После этого отмеченные группы хостов переместятся в список добавленных.
- Исключить группы хостов из области применения политики. Для этого следует в списке **Добавлено** отметить флажками требуемые группы и нажать кнопку . После этого отмеченные группы хостов переместятся в список доступных. При этом группы хостов, исключенные из области применения какой-либо политики, переносятся в область применения политики **Default**.

4. По завершении изменений необходимо нажать кнопку **Сохранить**, чтобы сохранить внесенные изменения, или **Отменить**, чтобы сбросить внесенные изменения и вернуться к странице политики.

Примечание

*Чтобы применить внесенные в политику изменения, по завершении настроек необходимо нажать кнопку **Применить версию**.*

8.4.2.4. Карточка хоста, включенного в область применения политики

Чтобы посмотреть подробную информацию о хосте, который входит в область применения политики, необходимо открыть его карточку. Для этого следует найти этот хост в таблице и нажать на строку, в которой он записан. Подробнее о карточке хоста см. в разделе 7.5.

8.4.3. Вкладка «Наборы правил»

Вкладка **Наборы правил** содержит информацию о наборах правил, которые входят в политику и распространяются на область применения.

Вкладка состоит из следующих элементов (см. Рис.8.5):

- кнопка для настройки перечня наборов правил, включенных в политику;
- таблица со списком наборов правил, включенных в политику.

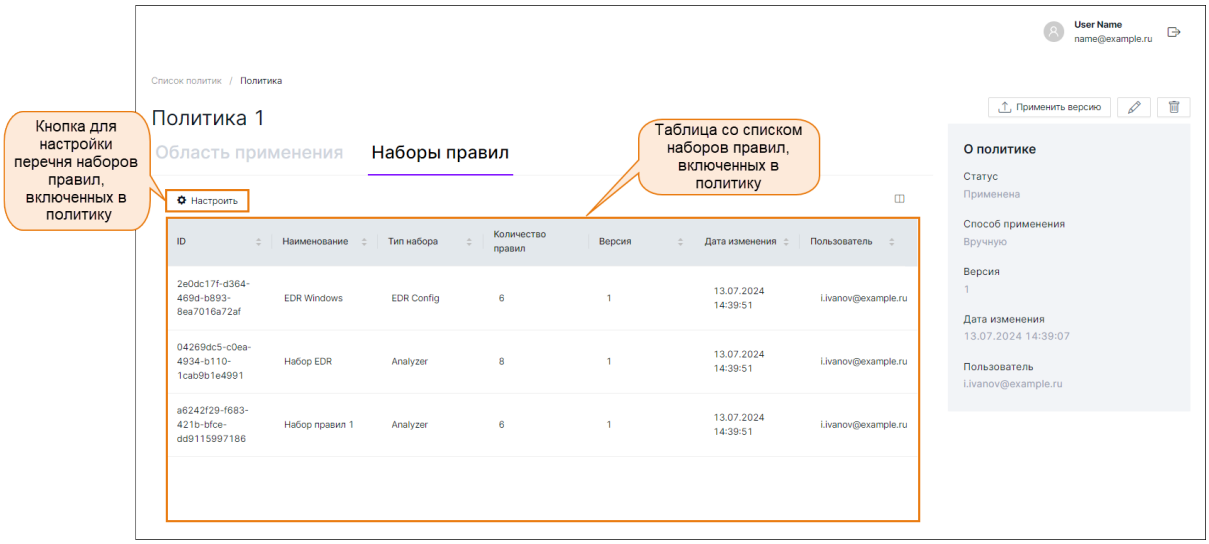


Рис. 8.5. Страница политики. Вкладка «Наборы правил»

8.4.3.1. Таблица со списком наборов правил, включенных в политику

На центральной части страницы расположена таблица с информацией о наборах правил, включенных в политику. Каждая строка таблицы соответствует определенному набору правил. Столбцы таблицы содержат следующую информацию:

- **ID** – идентификатор набора правил.
- **Наименование** набора правил.
- **Тип набора**:
  - **EDR Config**;
  - **NTA Config**;
  - **Analyzer**.
- **Количество правил** – количество правил, входящих в набор.
- **Версия** – номер версии набора.
- **Дата изменения** – дата и время внесения последних изменений в набор правил, например, при добавлении правила в набор. Если в набор правил еще не вносились изменения, здесь будут отображаться дата и время его создания.

- **Пользователь** – ФИО пользователя, который последним внес изменения в набор. Если в набор правил еще не вносились изменения, здесь будет отображаться автор набора.

При необходимости можно изменить набор столбцов в таблице – действия при этом аналогичны действиям при настройке таблицы со списком событий (подробнее см. в разделе 5.3.1).

Так же как и в разделе **События**, под таблицей справа расположены кнопки для перехода между страницами. По умолчанию на одной странице таблицы отображаются 20 записей. Для удобства можно изменить количество отображаемых записей на одной странице, нажав на соответствующее поле и выбрав в раскрывающемся списке требуемое число.

8.4.3.2. Настройка перечня наборов правил в политике

Чтобы изменить область применения политики, необходимо выполнить следующие действия:

1. В разделе **Политики** открыть карточку требуемой политики на вкладке **Наборы правил**.
2. Нажать кнопку **Настроить**.
3. В появившемся диалоговом окне (см. Рис.8.6) слева будет отображен список доступных для выбора наборов правил, а справа – список наборов, включенных в состав политики.

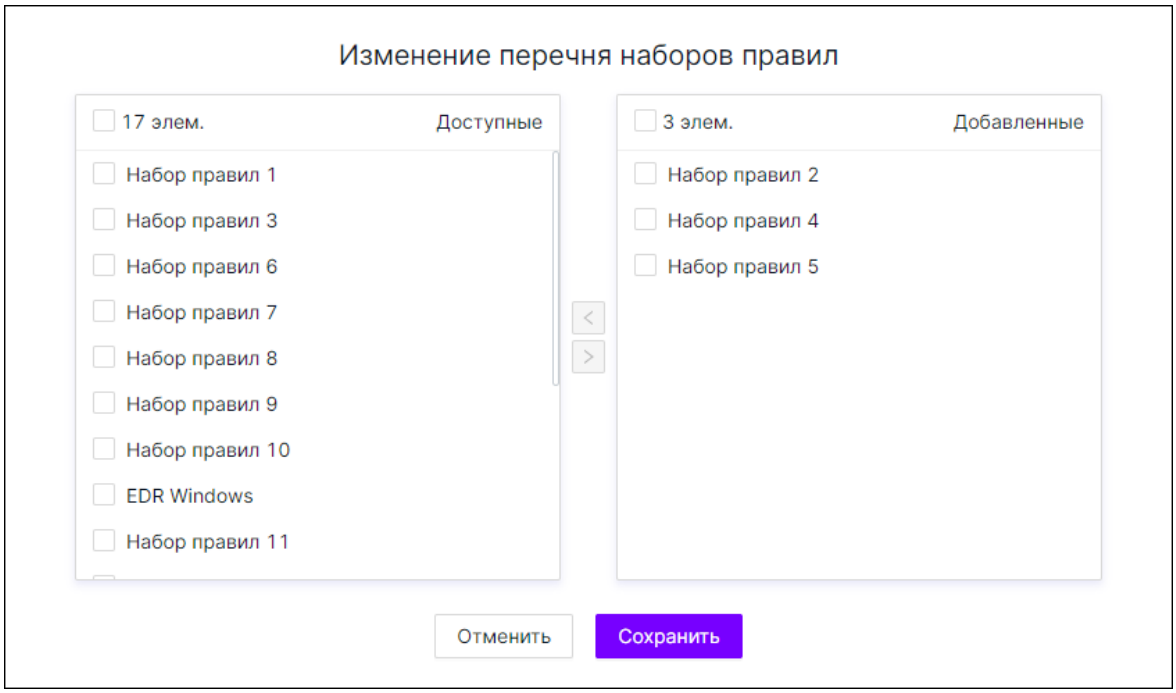


Рис. 8.6. Страница политики. Вкладка «Наборы правил». Настройка перечня наборов правил

Здесь пользователь может выполнить следующие действия:

- Добавить наборы правил в состав политики. Для этого следует в списке **Доступно** отметить флажками требуемые наборы и нажать кнопку >. После этого отмеченные наборы правил переместятся в список добавленных.

- Исключить наборы правил из состава политики. Для этого следует в списке **Добавлено** отметить флажками требуемые наборы и нажать кнопку <. После этого отмеченные наборы правил переместятся в список доступных.

Примечание

*В текущей версии для корректного применения политики на хостах с агентом Solar EDR необходимо, чтобы в политике был хотя бы один набор, содержащий правило типа **Analyzer**.*

4. По завершении изменений необходимо нажать кнопку **Сохранить**, чтобы сохранить внесенные изменения, или **Отменить**, чтобы сбросить внесенные изменения и вернуться к странице политики.

Примечание

*Чтобы применить внесенные в политику изменения, по завершении настроек необходимо нажать кнопку **Применить версию**.*

8.5. Создание новой политики

Чтобы добавить новую политику, необходимо выполнить следующие действия:

1. Открыть раздел **Политики** и нажать кнопку **Создать** в заголовке страницы.
2. В появившемся диалоговом окне (см. Рис.8.7) заполнить следующие поля:
   - **Наименование** политики. Поле является обязательным для заполнения.
   - **Описание** – краткое описание политики.

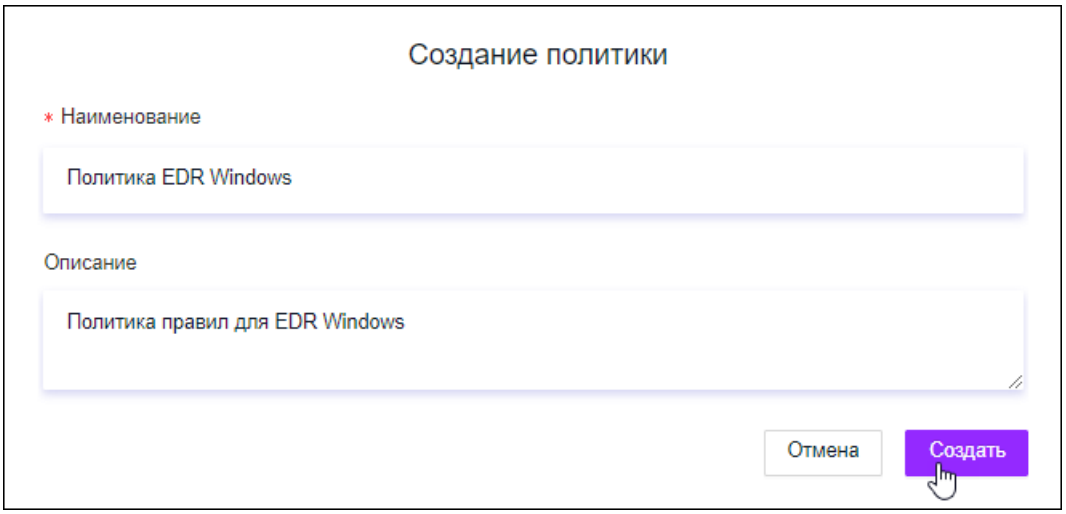


Рис. 8.7. Раздел «Политики». Создание новой политики

3. Нажать кнопку **Создать**.

4. Найти созданную политику в таблице и открыть её карточку.

5. Настроить область применения политики с помощью кнопки **Настроить** на вкладке **Область применения** (подробнее об этом см. в разделе 8.4.2.3).

6. Настроить перечень наборов правил с помощью кнопки **Настроить** на вкладке **Наборы правил** (подробнее об этом см. в разделе 8.4.3.2).

7. Чтобы распространить правила политики на область применения, следует нажать кнопку **Применить версию**.

8.6. Редактирование политики

Примечание

*Политики **Политика NTA** и **Политика EDR Windows** являются системными и их нельзя изменить.*

Чтобы внести изменения в политику, необходимо выполнить следующие действия:

1. Перейти в раздел **Политики** и открыть страницу требуемой политики.

2. Нажать на значок ✎, расположенный в правом верхнем углу страницы.

3. В появившемся окне (см. Рис.8.8) внести требуемые изменения в поля:

   - **Наименование** политики;
   - **Описание**.

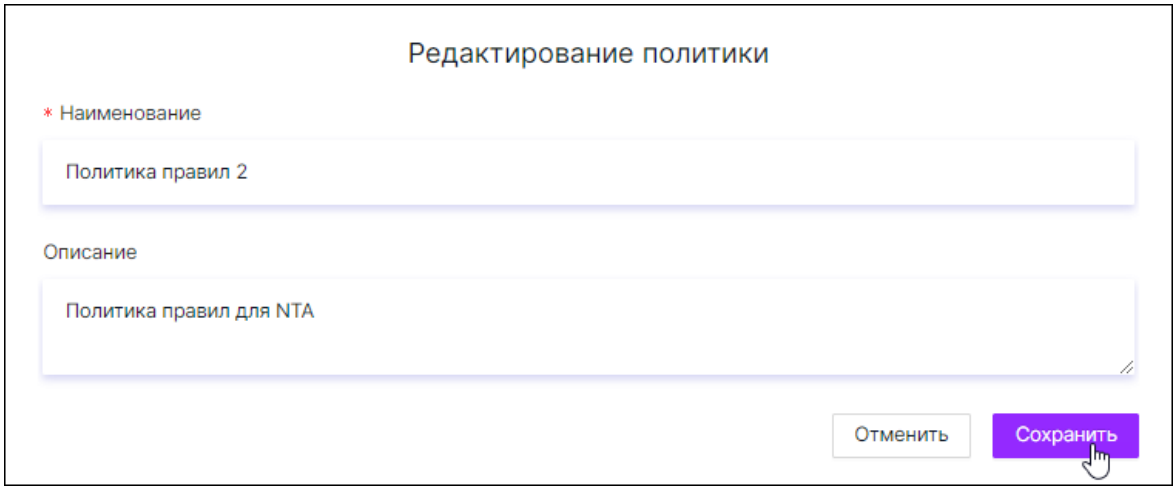


Рис. 8.8. Страница политики. Редактирование данных

4. Нажать кнопку **Сохранить**.

Политика будет изменена.

8.7. Удаление политики

Примечание

*Политики **Политика NTA** и **Политика EDR Windows** являются системными и их нельзя удалить.*

Если в области применения политики есть хотя бы одна группа хостов, удалить такую политику нельзя.

Чтобы удалить политику, необходимо выполнить следующие действия:

1. Если в политике, которую нужно удалить, содержатся группы хостов, следует исключить их из области применения (подробнее об этом см. в разделе 8.4.2.3).
2. Перейти в раздел **Политики** и открыть страницу требуемой политики.
3. Нажать на значок 🗑, расположенный в правом верхнем углу страницы.
4. В появившемся диалоговом окне (см. Рис.8.9) подтвердить удаление политики, нажав на соответствующую кнопку.

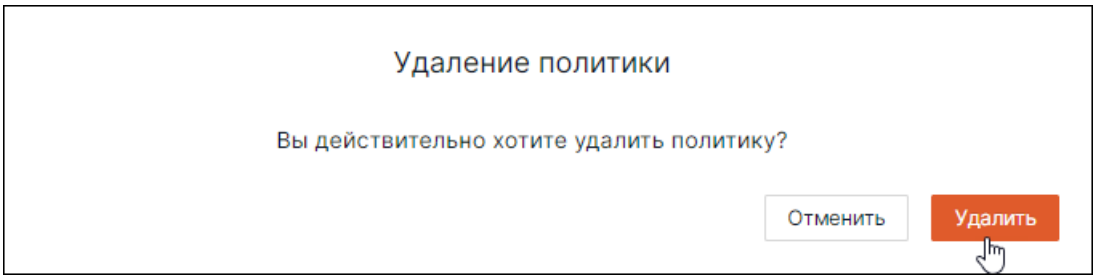


Рис. 8.9. Диалоговое окно подтверждения удаления политики

Политика будет удалена. При этом наборы правил, входящие в эту политику, удалены не будут, на страницах таких наборов изменится значение поля **Применение**.

9. Раздел «Расследования»

Раздел **Расследования** предназначен для мониторинга информации об инцидентах, предоставления детальных сведений о событиях и артефактах, входящих в инцидент, выполнения действий по работе с инцидентом.

Инцидент может быть создан двумя способами:

- автоматически;
- вручную пользователем в ходе анализа полученных событий при обнаружении подозрительной активности, которую пропустили автоматические средства (подробнее об этом см. в разделе 5.7).

После перехода в раздел **Расследования** отобразится страница, которая состоит из следующих областей (см. Рис.9.1):

- заголовок страницы;
- фильтры;
- таблица со списком инцидентов.

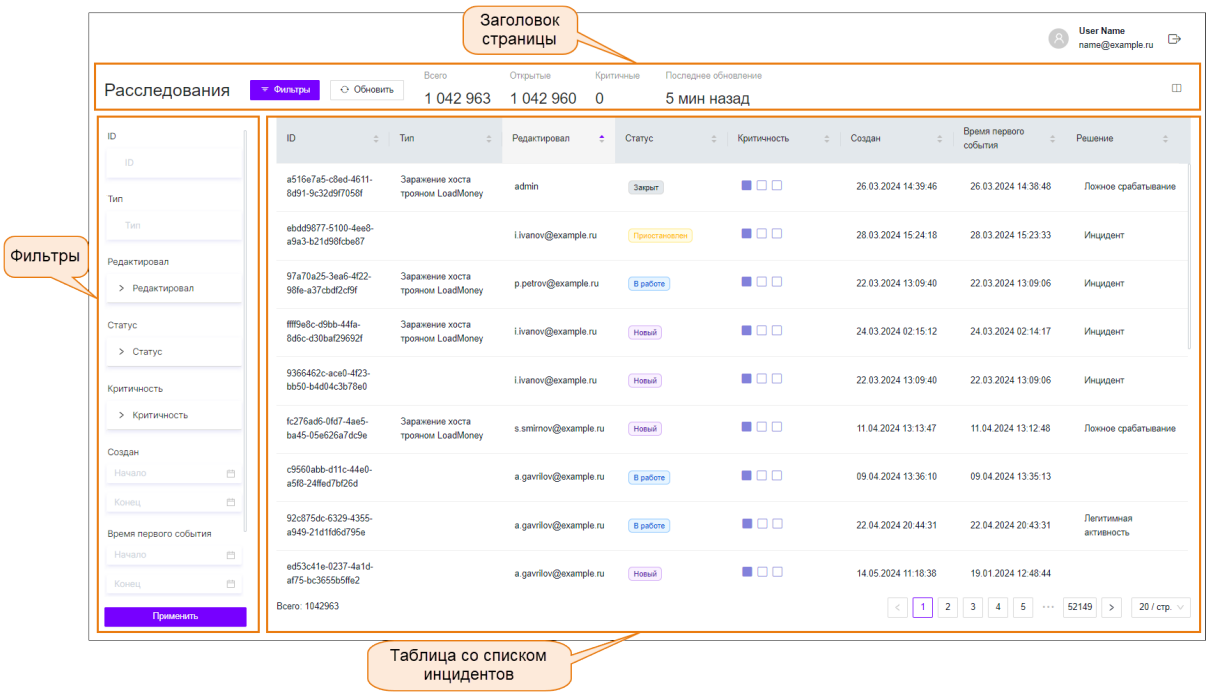


Рис. 9.1. Раздел «Расследования»

9.1. Таблица со списком инцидентов

Информация об инцидентах ИБ, обнаруженных Солар ПКОиР, представлена в виде таблицы. Каждая строка таблицы соответствует определенному инциденту. Столбцы таблицы содержат следующую информацию об инцидентах:

- **ID** – идентификатор инцидента.

- **Тип** – сработавшее правило политики ИБ, по которому был обнаружен инцидент.
- **Редактировал** – пользователь, который последним вносил изменения в инцидент: изменил статус или решение по инциденту.
- **Статус** – текущее состояние инцидента в его жизненном цикле: **Новый**, **В работе**, **Приостановлен**, **Закрыт**. Подробнее о каждом статусе см. в разделе 9.4.1.
- **Критичность** – уровень значимости инцидента в виде шкалы из трех значений, где: ■ □ □ – низкий уровень критичности, ■ ■ ■ – высокий уровень критичности:
  - Если инцидент был создан вручную (см. раздел 5.7), уровень критичности проставляется вручную на этапе создания инцидента.
  - Если инцидент был создан автоматически, уровень критичности рассчитывается автоматически исходя из параметров:
    - критичность хоста, на котором произошел инцидент;
    - критичность учетной записи, используемой на данном защищаемом хосте;
    - критичность сработавшего правила политики ИБ.
- **Создан** – дата и время создания инцидента.
- **Время первого события** – дата и время возникновения первого события в инциденте.
- **Решение** – принятое в рамках расследования решение по инциденту. Подробнее описание каждого решения см. в разделе 9.4.1.

При необходимости можно изменить набор столбцов в таблице – действия при этом аналогичны действиям при настройке таблицы со списком событий (подробнее см. в разделе 5.3.1).

Слева под таблицей отображается количество записей в таблице с учетом фильтрации (см. раздел 9.3).

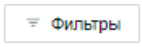
Так же, как и в разделе **События**, под таблицей справа расположены кнопки для перехода между страницами. По умолчанию на одной странице таблицы отображаются 20 записей. Для удобства можно изменить количество отображаемых записей на одной странице, нажав на соответствующее поле и выбрав в раскрывающемся списке требуемое число.

9.1.1. Сортировка инцидентов в таблице

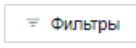
По умолчанию инциденты в таблице отсортированы по дате их создания в обратном хронологическом порядке (вверху таблицы находятся самые свежие инциденты). Для удобства работы можно изменить порядок отображения инцидентов в таблице, нажав на значок в названии требуемого столбца. Настройки сортировки таблицы в разделе **Расследования** аналогичны настройкам в разделе **События** (см. раздел 5.2.1).

9.2. Заголовок страницы «Расследования»

В заголовке страницы **Расследования** содержатся:

- название текущего раздела;
- кнопка  /  – **Фильтры**, позволяющая развернуть/свернуть панель с полями для фильтрации;
- кнопка **Обновить**, с помощью которой можно оперативно получить актуальную на текущий момент информацию об инцидентах без обновления страницы;
- сводная информация по инцидентам:
  - **Всего** – общее количество инцидентов в таблице.
  - **Открытые** – количество незакрытых инцидентов (со статусами **Новый**, **В работе**, **Приостановлен**).
  - **Критичные** – количество инцидентов высокой критичности.
  - **Последнее обновление** – информация о последнем обновлении данных в таблице. При наведении курсора мыши на значение отобразится всплывающее окно с датой и временем последнего обновления.
- значок ◫ для настройки отображения таблицы – действия аналогичны действиям при настройке отображения таблицы событий (см. раздел 5.3.1).

9.3. Фильтры инцидентов

Чтобы открыть панель с полями для фильтрации, необходимо нажать кнопку  , расположенную в заголовке страницы.

Примечание

Набор полей для фильтрации может различаться в зависимости от настроек отображения таблицы.

Фильтрация возможна по следующим полям:

- **ID** – идентификатор инцидента вводится с клавиатуры. Поиск по этому полю осуществляется по полному совпадению значения.
- **Тип** – фильтр позволяет найти все инциденты определенного типа. Значение вводится с клавиатуры.
- **Редактировал** – с помощью флажков указывается один или несколько пользователей, которые вносили изменения в инцидент.
- **Статус** – с помощью данного фильтра можно найти все инциденты, которые находятся на определенном этапе работы. Для этого в списке необходимо выбрать один или несколько статусов.
- **Критичность** – фильтр позволяет найти все инциденты определенного уровня значимости. Для этого следует отметить флажком одно или несколько значений.

- **Создан** – фильтр предназначен для поиска инцидентов по дате и времени их создания. При нажатии на значок , расположенный в соответствующих полях, откроется окно в виде календаря, в котором можно выбрать дату и время, тем самым указав интервал для поиска.

- **Время первого события** – данный фильтр позволяет осуществить поиск инцидентов по дате и времени возникновения в них первого события. Работа с этим фильтром аналогична работе с фильтром **Создан**.

- **Решение** – позволяет найти все инциденты, по которым вынесено определенное решение. Для этого необходимо отметить флажком один или несколько вариантов решений.

Чтобы отфильтровать таблицу со списком инцидентов по заданным параметрам, следует нажать кнопку **Применить** или клавишу **Enter** на клавиатуре. После этого значение в поле **Всего**, которое расположено под таблицей инцидентов слева, также изменится. Очистить поля для фильтрации и вернуть таблицу в исходный вид позволяет кнопка **Сбросить**. Для скрытия области работы с фильтрами необходимо нажать кнопку Фильтры.

9.4. Страница инцидента

Чтобы открыть страницу требуемого инцидента, необходимо найти инцидент в таблице и нажать на строку, в которой он записан.

На странице инцидента отображаются:

- подробная информация об инциденте;
- сведения о событиях, входящих в инцидент;
- информация об артефактах;
- данные о сработавших правилах политики ИБ;
- информация о затронутых активах.

Страница инцидента состоит из следующих областей (см. Рис.9.2):

- **Заголовок страницы инцидента** (см. раздел 9.4.1);
- Вкладки:
  - **Подробная информация** (см. раздел 9.4.2);
  - **Комментарии** (см. раздел 9.4.3);
  - **История изменений** (см. раздел 9.4.4).

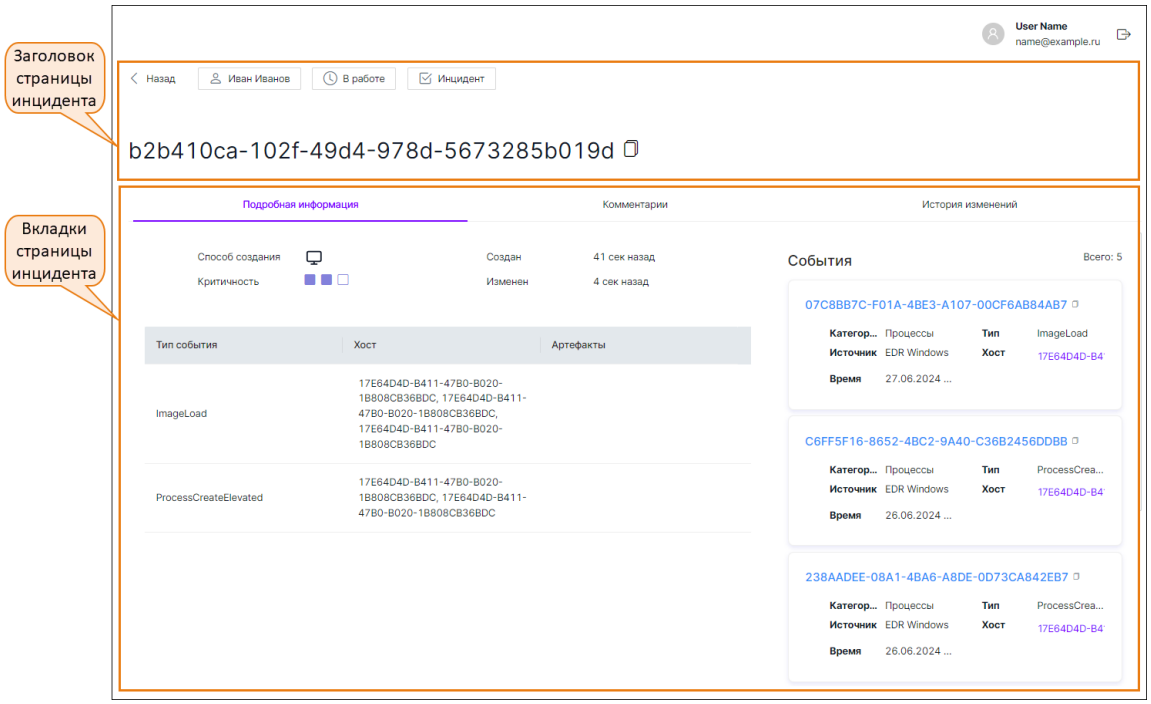


Рис. 9.2. Страница инцидента

9.4.1. Заголовок страницы инцидента

В заголовке страницы инцидента содержатся:

- Ссылка **Назад**, позволяющая закрыть страницу и вернуться к списку инцидентов.
- Пользователь, который последним редактировал инцидент – сменил статус или решение по инциденту:
  - если инцидент был создан автоматически и расследование еще не начато (статус инцидента **Новый**), поле будет пустым.
  - если инцидент был создан вручную и изменения в него еще не вносились, здесь будет отображаться пользователь, который создал инцидент.
- Текущий статус инцидента. Чтобы изменить статус инцидента, следует нажать на кнопку с названием текущего статуса и выбрать из раскрывающегося списка требуемый (см. Рис.9.3):
  - **Новый** – расследование не начато. Статус присваивается автоматически после появления инцидента в системе.
  - **В работе** – расследование инцидента начато. Статус присваивается вручную пользователем или автоматически при изменении данных в инциденте.
  - **Приостановлен** – работа с инцидентом временно приостановлена, ожидается действие от заказчика. Статус выставляется вручную пользователем.
  - **Закрыт** – расследование инцидента завершено. Выставляется пользователем вручную.

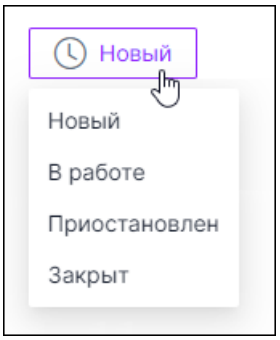


Рис. 9.3. Страница инцидента. Смена статуса инцидента

- Принятое в рамках расследования решение по инциденту. Чтобы вынести решение по инциденту или изменить его, следует нажать на кнопку с названием текущего решения и выбрать из списка требуемое (см. Рис.9.4):
  - **<Отсутствует>** – расследование по инциденту не начато или не завершено. Выставляется автоматически.
  - **Ложное срабатывание** – в результате расследования выявлена некорректная отработка настроенных правил политики ИБ. Выставляется пользователем вручную.
  - **Инцидент** – расследование подтвердило нелегитимную активность. Выставляется пользователем вручную.
  - **Легитимная активность** – корректная отработка заданных правил политики ИБ, легитимная активность подтверждена пользователем.

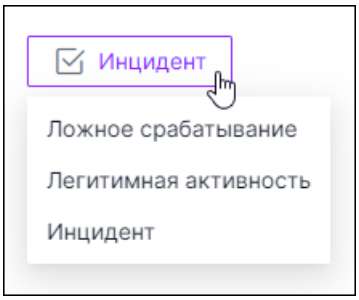


Рис. 9.4. Страница инцидента. Вынесение/изменение решения по инциденту

- Идентификатор инцидента. Справа от него расположен значок, позволяющий его скопировать, чтобы в дальнейшем оперативно поделиться с коллегами или использовать в процессе расследования.

9.4.2. Вкладка «Подробная информация»

Вкладка **Подробная информация** состоит из следующих областей (см. Рис.9.5):

- общие сведения об инциденте;
- таблица с детализацией событий;
- список событий, относящихся к инциденту.

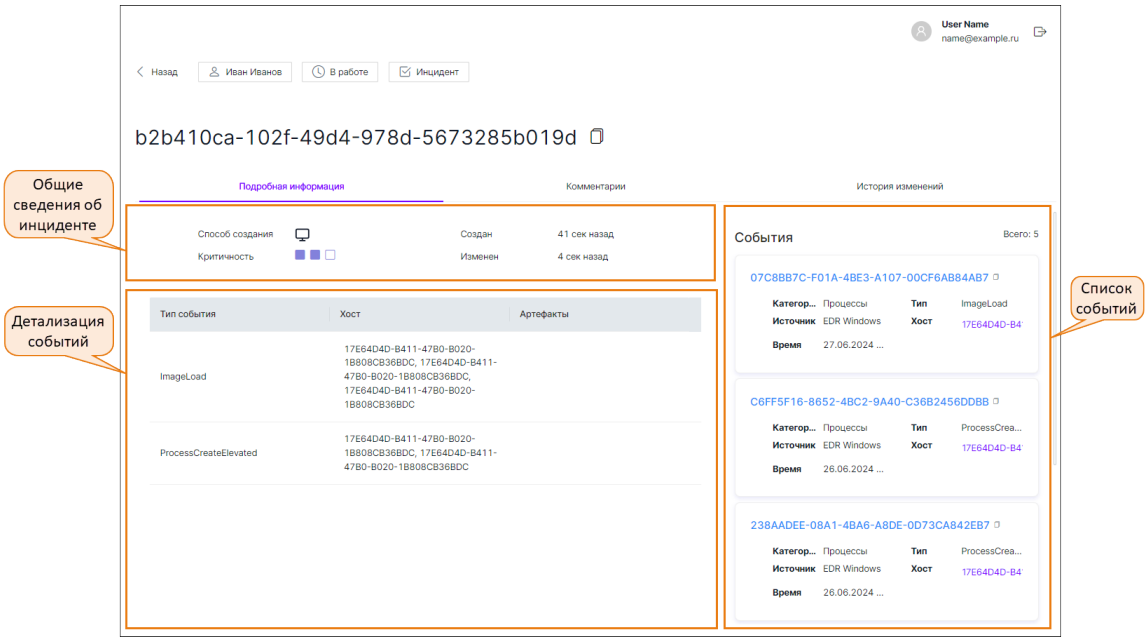


Рис. 9.5. Страница инцидента. Вкладка «Подробная информация»

9.4.2.1. Общие сведения об инциденте

Вверху вкладки в области общих сведений отображаются:

- способ создания инцидента:

  – автоматически;

  – вручную пользователем (подробнее об этом см. в разделе 5.7);

- уровень критичности инцидента;
- поле **Создан**, в котором показывается, сколько времени назад был создан инцидент;
- поле **Изменен**, которое показывает, сколько времени назад были внесены последние изменения в инцидент.

9.4.2.2. Список событий

Справа на странице инцидента отображается перечень входящих в данный инцидент событий. В правом верхнем углу списка отображается общее количество событий, связанных с данным инцидентом. По каждому событию здесь можно просмотреть следующую информацию:

- Идентификатор события. Нажав на значок , расположенный справа от идентификатора события, можно его скопировать в буфер обмена, чтобы в дальнейшем поделиться с коллегами или использовать в процессе расследования инцидента. При нажатии на идентификатор события будет открыта его карточка (см. Рис.9.6). Чтобы открыть карточку данного события в разделе **События** (см. раздел 5.6), необходимо нажать кнопку **Перейти к событию**, расположенную в правом верхнем углу.
- **Категория**, к которой относится событие.

- **Тип** события.
- **Источник**, из которого событие было получено.
- **Хост** – код устройства хоста, на котором произошло событие.
- **Время** – дата и время возникновения события.
- Блок с атрибутами события и их значениями.

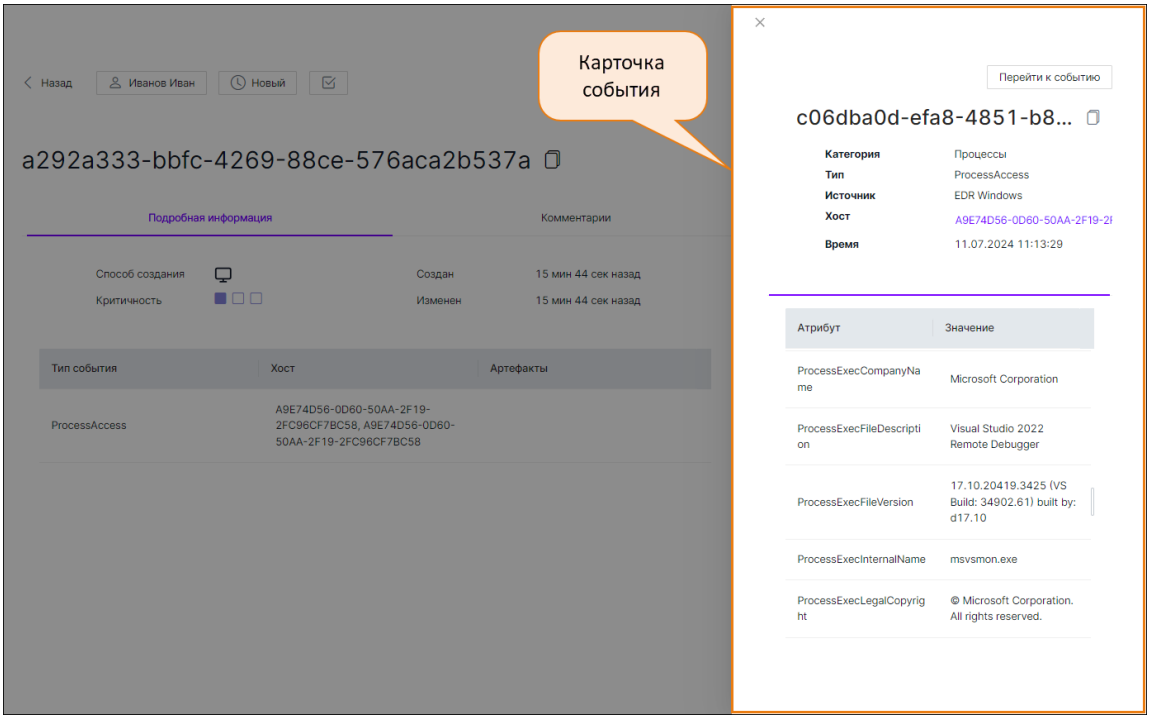


Рис. 9.6. Вкладка «Подробная информация». Карточка события

9.4.2.3. Детализация событий

В блоке **Детализация событий** отображается таблица с артефактами входящих в инцидент событий. Таблица состоит из следующих столбцов:

- **Тип события**;
- **Хост**;
- **Артефакты**.

9.4.3. Вкладка «Комментарии»

Вкладка **Комментарии** (см. Рис.9.7) предназначена для фиксации промежуточных результатов расследования инцидента. Здесь можно добавлять новые комментарии, а также просматривать комментарии других сотрудников, чтобы понимать, как продвигается работа по инциденту.

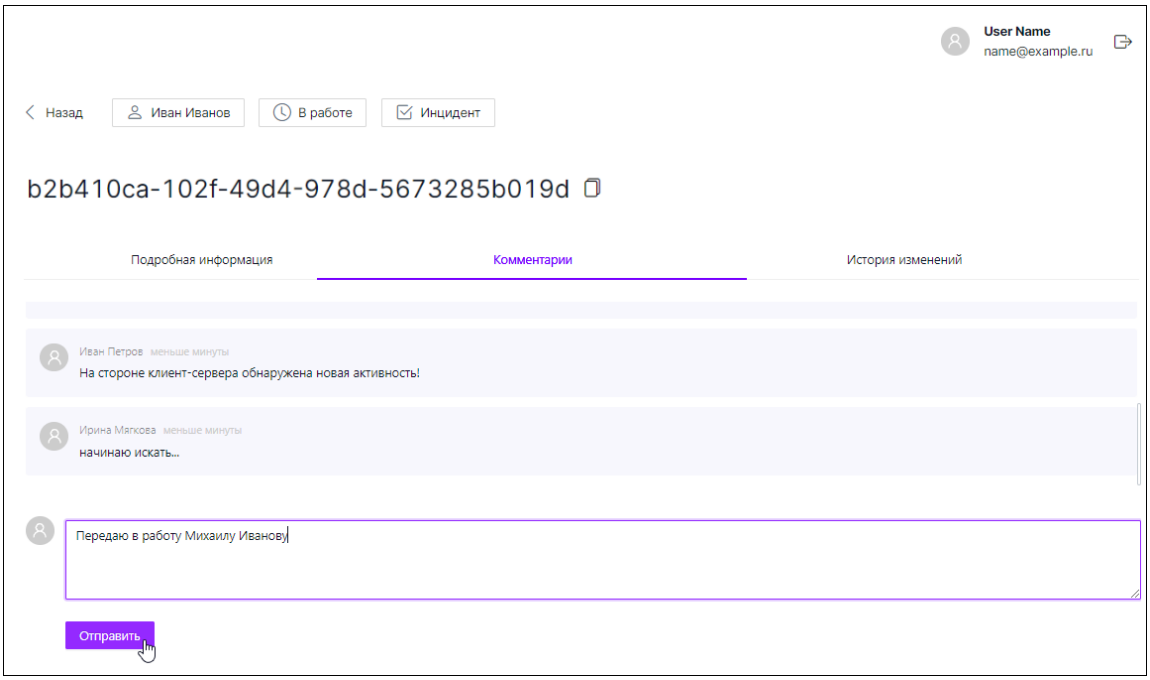


Рис. 9.7. Страница инцидента. Вкладка «Комментарии»

Чтобы добавить новый комментарий, следует ввести его в текстовое поле внизу страницы и нажать кнопку **Отправить**. Автор, текст и время создания комментария отобразятся на вкладке.

При необходимости автор комментария может изменить или удалить его. Для этого достаточно навести курсор мыши на требуемый комментарий и вызвать меню действий, нажав на значок ⋮, расположенный справа от текста, и в появившемся списке выбрать один из пунктов:

- **Редактировать** – при нажатии кнопки текст комментария станет доступным для редактирования. Чтобы сохранить внесенные изменения, следует нажать кнопку **Сохранить**, отменить изменения – кнопку **Отменить**.
- **Удалить** – при нажатии кнопки появится диалоговое окно, в котором требуется подтвердить или отменить удаление комментария со страницы инцидента. После удаления восстановить комментарий будет невозможно.

9.4.4. Вкладка «История изменений»

На вкладке **История изменений** фиксируются изменения, произошедшие с инцидентом. Информация об изменениях представлена в виде таблицы (см. Рис.9.8). Столбцы таблицы содержат следующую информацию:

- **Время** – дата и время зафиксированного действия.
- **Действие** – зафиксированное изменение данных на странице инцидента.
- **Пользователь** – пользователь, который внес изменения в инцидент.
- **IP** – IP-адрес, с которого были внесены изменения в инцидент.

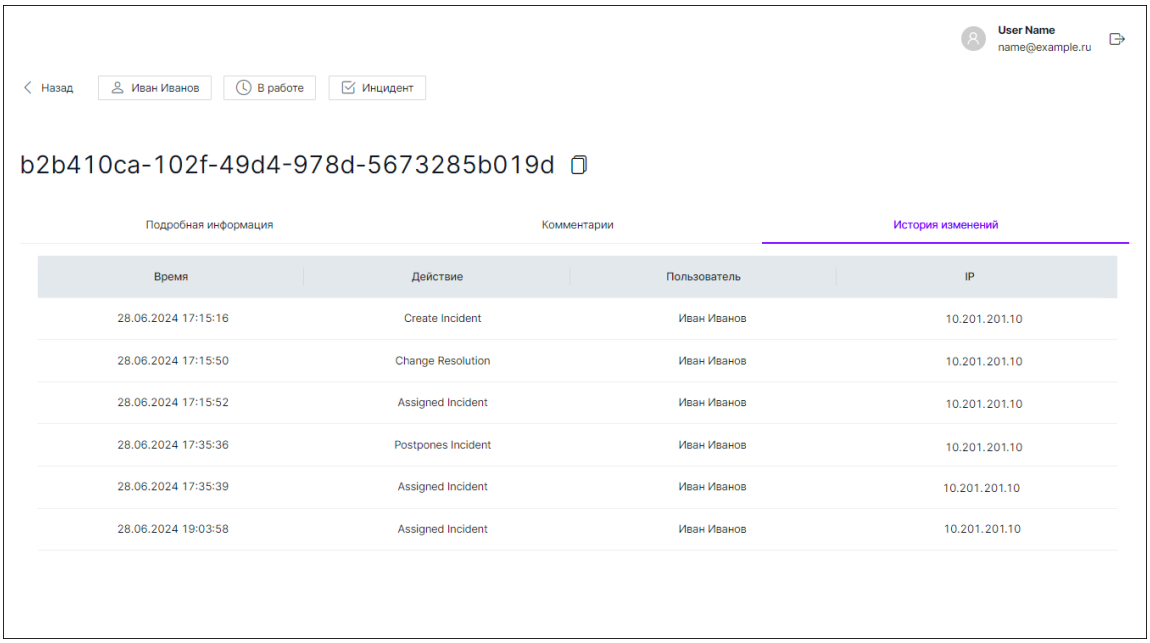


Рис. 9.8. Страница инцидента. Вкладка «История изменений»

10. Раздел «Правила»

Раздел **Правила** предназначен для настройки и отображения базы решающих правил (БРП) с целью обнаружения атак. Правила делятся на две категории:

- **Вендорские** – правила, импортированные в БРП из внешних по отношению к системе центров экспертизы.
- **Пользовательские** – правила, созданные пользователем системы.

Для удобства работы с большим количеством правил пользователь может объединять их в группы. **Группа правил** – это перечень правил, которые хранятся в базе данных. Группы правил имеют иерархическую структуру.

При необходимости указания множества значений в условиях правил могут быть использованы **Справочники**. Так же, как и правила, справочники можно объединять в **Группы**.

Для применения на конечных защищаемых точках правила объединяются в наборы. **Набор правил** – это перечень правил, объединенных пользователем для распространения на определенных группах хостов. Следует отметить, что наборы правил не содержат в себе правила, как сущности, а только ссылаются на них.

Раздел **Правила** состоит из следующих вкладок:

- **Правила** (см. раздел 10.1);
- **Справочники** (см. раздел 10.2);
- **Наборы** (см. раздел 10.3).

10.1. Вкладка «Правила»

После перехода в раздел **Правила** по умолчанию будет открыта одноименная вкладка, которая содержит список всех имеющихся в системе правил. Вкладка **Правила** (см. Рис.10.1) состоит из следующих областей:

- заголовок страницы;
- панель навигации по группам правил;
- фильтры;
- таблица со списком правил.

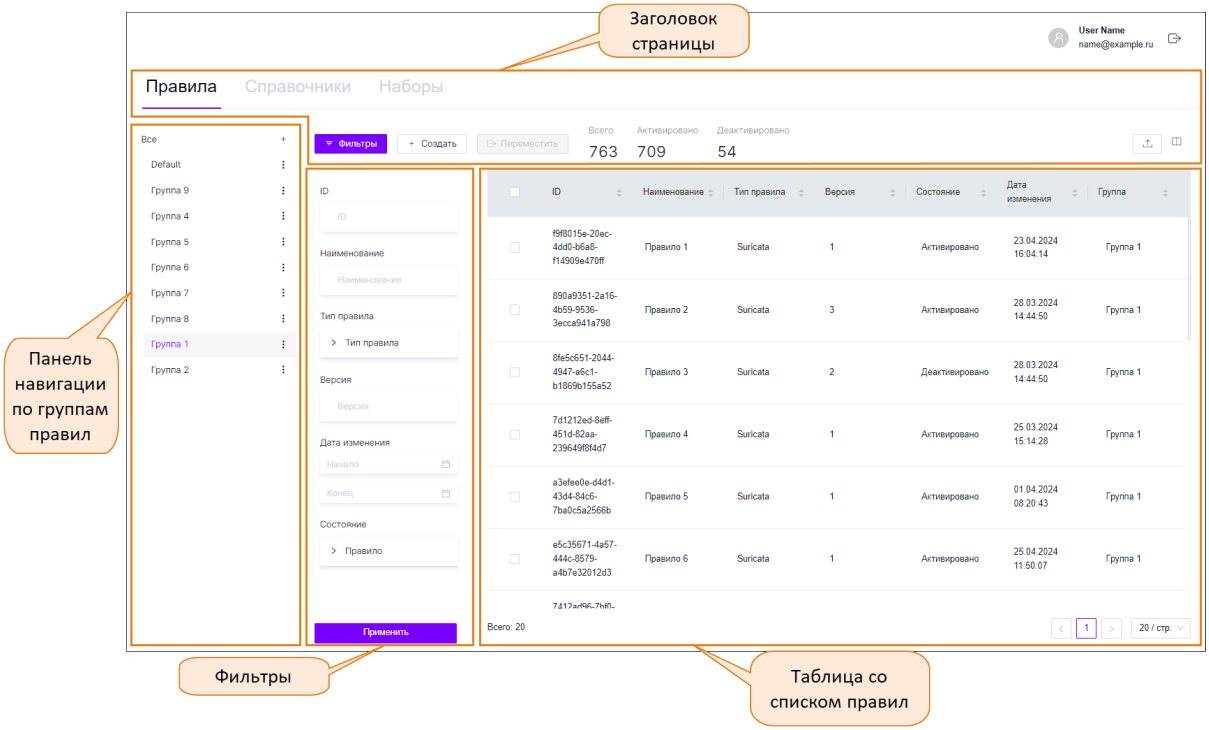


Рис. 10.1. Раздел «Правила». Вкладка «Правила»

10.1.1. Таблица со списком правил

Информация о правилах представлена в виде таблицы. Состав и количество правил, отображаемых в таблице, зависит от выбранной группы правил на панели навигации (см. раздел 10.1.3).

Каждая строка таблицы соответствует определенному правилу. Столбцы таблицы содержат следующую информацию:

- **ID** – идентификатор правила.
- **Наименование** правила.
- **Тип правила**. Подробнее о типах правил см. в разделе 10.1.7.
- **Версия** правила.
- **Состояние** правила:
  - **Активировано** (включено);
  - **Деактивировано** (выключено).
- **Дата изменения** – дата и время внесения последних изменений в правило. Если правило еще не изменялось, здесь будет отображаться дата его создания.
- **Группа** – группа, в которую входит правило.

Слева от каждого правила расположен флажок, который используется при перемещении правил из одной группы в другую. Подробнее об этом см. в разделе 10.1.3.4.

При необходимости можно изменить набор столбцов в таблице – действия при этом аналогичны действиям при настройке таблицы со списком событий (подробнее см. в разделе 5.3.1).

Слева под таблицей отображается количество записей в таблице с учетом фильтрации (см. раздел 10.1.4), а также выбранной группы правил на панели навигации (см. раздел 10.1.3).

Так же, как и в других разделах, например, **События**, под таблицей справа расположены кнопки для перехода между страницами. По умолчанию на одной странице таблицы отображаются 20 записей. Для удобства можно изменить количество отображаемых записей на одной странице, нажав на соответствующее поле и выбрав в раскрывающемся списке требуемое число.

10.1.1.1. Сортировка правил в таблице

По умолчанию правила в таблице отсортированы в порядке их добавления. Для удобства работы можно изменить порядок отображения, нажав на значок в названии требуемого столбца. Настройки сортировки этой таблицы аналогичны настройкам в разделе **События** (см. раздел 5.2.1).

10.1.2. Заголовок страницы

В заголовке страницы содержатся:

- название текущей вкладки;
- кнопка Фильтры / Фильтры – **Фильтры**, позволяющая развернуть/свернуть панель с полями для фильтрации;
- кнопка **Создать**, позволяющая добавить новое правило (подробнее о создании нового правила см. в разделе 10.1.7);
- кнопка **Переместить**, которая предназначена для перемещения правил из одной группы в другую (подробнее об этом см. в разделе 10.1.3.4).
- сводная информация по правилам:
  - **Всего** – общее количество правил в системе.
  - **Активировано** – количество правил в состоянии **Активировано**.
  - **Деактивировано** – количество правил в состоянии **Деактивировано**.
- кнопка , предназначенная для импорта готовых правил в систему (см. раздел 10.1.9).
- значок для настройки отображения таблицы – действия аналогичны действиям при настройке отображения таблицы событий (см. раздел 5.3.1).

10.1.3. Панель навигации по группам правил

В левой части страницы расположена панель навигации по группам правил (см. Рис.10.2).

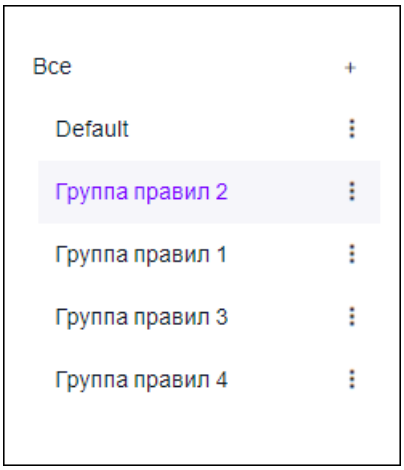


Рис. 10.2. Раздел «Правила». Вкладка «Правила». Панель навигации по группам правил

Панель навигации имеет древовидную структуру. По умолчанию на самом верхнем уровне расположен элемент **Все**. При нажатии на этот элемент в таблице отображаются все правила из всех групп. На втором уровне размещены группы, добавленные пользователем, а также системная группа **Default**, которую нельзя удалить. При выборе определенной группы в таблице отображаются только правила, входящие в эту и дочерние группы.

Примечание

Следует отметить, что в текущей версии панель навигации имеет только два уровня вложенности. Это значит, что все создаваемые группы правил будут находиться на втором уровне. Внутри групп второго уровня нельзя создавать новые группы.

Таким образом, если требуется отобразить в таблице все правила, необходимо нажать на элемент **Все**. Если нужно показать только правила из определенной группы, следует найти требуемую группу и нажать на ее название. При этом количество правил, входящих в эту группу, можно увидеть под таблицей слева в поле **Всего**.

10.1.3.1. Добавление новой группы правил

Чтобы добавить новую группу правил, необходимо:

1. На панели навигации напротив элемента **Все** нажать на значок **+** (см. Рис.10.3).

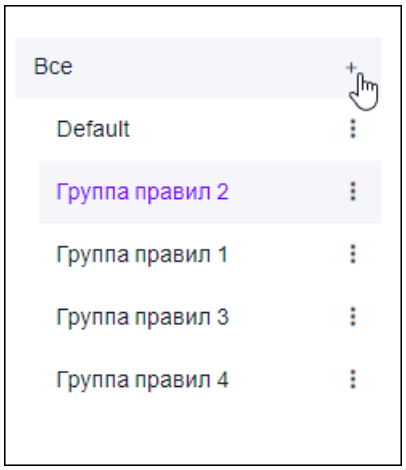


Рис. 10.3. Раздел «Правила». Вкладка «Правила». Панель навигации: создание новой группы правил

2. В открывшемся диалоговом окне задать наименование новой группы правил и нажать кнопку **Сохранить**.

Новая группа появится на панели навигации.

10.1.3.2. Удаление группы правил

Примечание

*Удалить можно только группы, созданные пользователем. Удалить системную группу **Default** нельзя.*

Если в группе есть хотя бы одно правило, удалить такую группу нельзя.

Чтобы удалить группу правил, необходимо выполнить следующие действия:

1. Если в группе, которую нужно удалить, содержатся правила, следует переместить их в другую группу (см. раздел 10.1.3.4).

2. На панели навигации найти требуемую группу и напротив ее названия нажать кнопку вызова меню – ⋮.

3. В списке выбрать пункт **Удалить** (см. Рис.10.4).

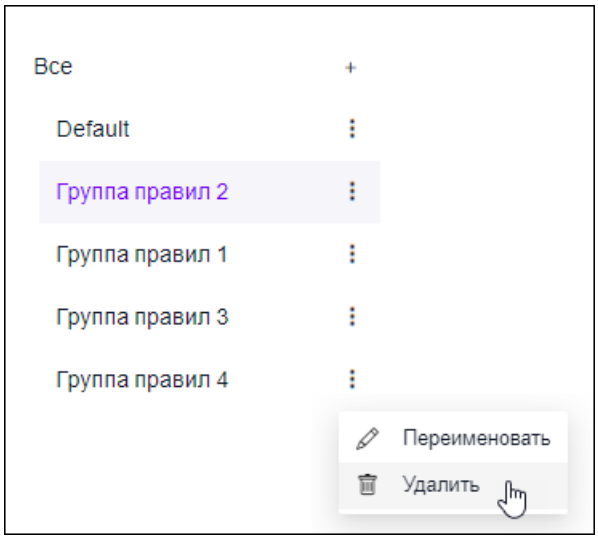


Рис. 10.4. Раздел «Правила». Вкладка «Правила». Панель навигации: удаление группы правил

4. В появившемся диалоговом окне подтвердить удаление группы нажатием кнопки **ОК**.

Удаленная группа правил пропадет из панели навигации.

10.1.3.3. Изменение названия группы правил

Чтобы изменить название группы правил, необходимо:

1. На панели навигации найти требуемую группу и напротив ее названия нажать кнопку вызова меню – ⋮.

Примечание

*Изменить название системной группы правил **Default** невозможно.*

2. Выбрать пункт **Переименовать** (см. Рис.10.5).

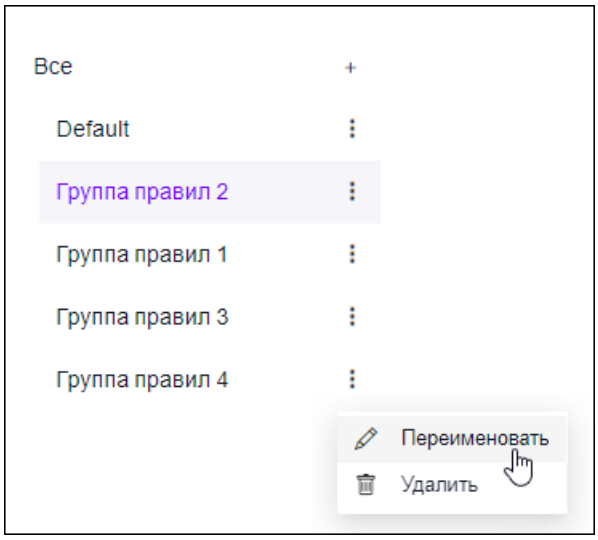


Рис. 10.5. Раздел «Правила». Вкладка «Правила». Панель навигации: изменение названия группы правил

3. В открывшемся диалоговом окне ввести новое название группы правил и нажать кнопку **Сохранить**.

10.1.3.4. Перемещение правил из одной группы в другую

В Солар ПКОиР существует два способа перемещения правил из одной группы в другую:

- Редактирование карточки правила – этот способ подойдет в том случае, если нужно переместить в другую группу небольшое количество правил (подробнее об этом см. в разделе **10.1.5**).
- Массовый перенос правил с помощью кнопки **Переместить** в заголовке страницы – данный способ удобен тем, что позволяет быстро переместить большое количество правил в другую группу.

Чтобы массово переместить правила из одной группы в другую, необходимо выполнить следующие действия:

1. В таблице отметить флажком одно или несколько правил, которые требуется переместить. Чтобы выбрать все правила, размещенные на текущей странице таблицы, следует нажать на флажок, расположенный в заголовке таблицы.
2. В заголовке страницы нажать кнопку **Переместить** (см. **Рис.10.6**).

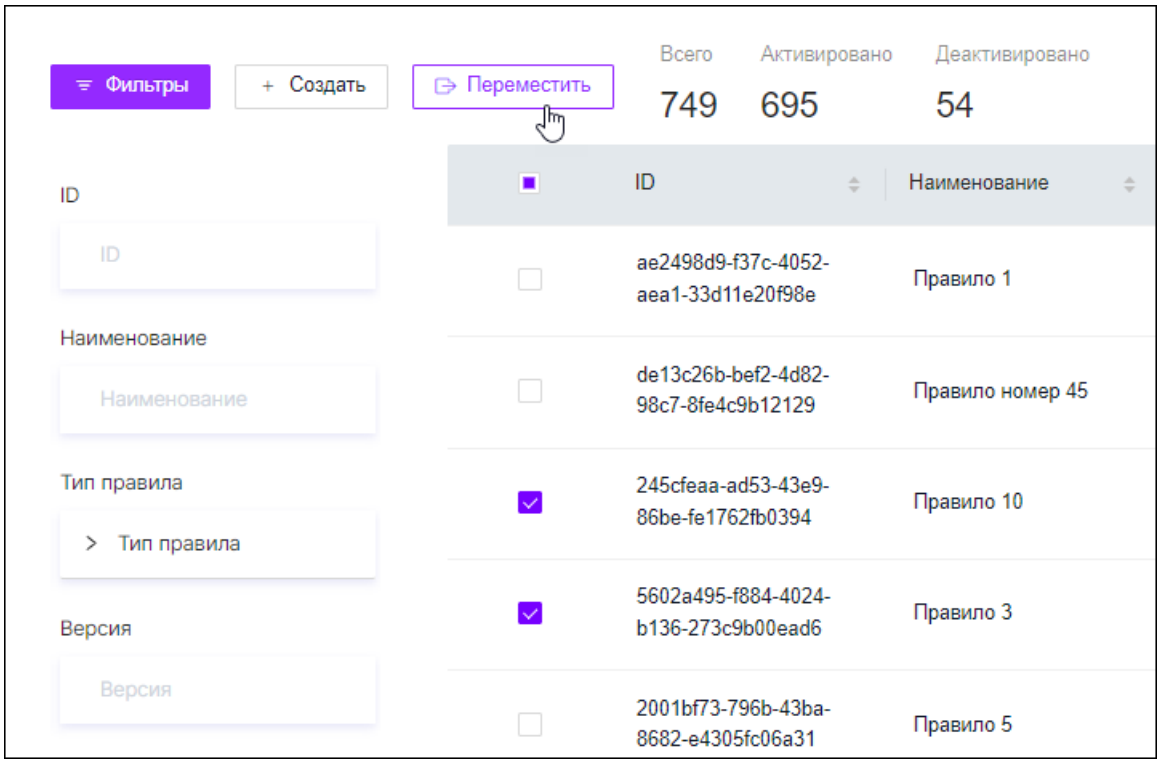
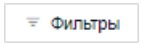


Рис. 10.6. Раздел «Правила». Вкладка «Правила». Панель навигации: перемещение правил в другую группу

3. В появившемся диалоговом окне выбрать группу, в которую необходимо переместить правила, и нажать кнопку **Переместить**.

Отмеченные флажками правила будут перенесены в выбранную группу.

10.1.4. Фильтры правил

Чтобы открыть панель с полями для фильтрации, необходимо нажать кнопку 

, расположенную в заголовке страницы.

Примечание

Набор полей для фильтрации может различаться в зависимости от настроек отображения таблицы.

Примечание

*Фильтры и панель навигации по группам правил (см. раздел 10.1.3) работают в связке. Например, если требуется найти все деактивированные правила, входящие в группу **Группа правил 1**, необходимо на панели навигации нажать на группу **Группа правил 1**, затем в фильтре в поле **Состояние** установить флажок **Деактивировано** и нажать кнопку **Применить**. Фильтрация в этом случае будет производиться в рамках выбранной группы.*

Фильтрация правил возможна по следующим полям:

- **ID** – параметр используется, если требуется найти определенное правило по его идентификатору. Значение вводится с клавиатуры. Поиск осуществляется по полному совпадению значения.
- **Наименование** – позволяет найти правило по его названию. Значение вводится с клавиатуры. Поиск по этому полю является регистрозависимым.
- **Тип правила** – фильтр позволяет найти все правила определенного типа. Требуемое значение отмечается флажком в раскрывающемся списке.
- **Версия** – параметр используется для поиска правил по номеру версии. Значение вводится с клавиатуры. Поиск осуществляется по полному совпадению значения.
- **Дата изменения** – фильтр позволяет найти правила, которые были последний раз отредактированы в заданном диапазоне времени. Для этого следует нажать на значок , расположенный в соответствующих полях. Откроется окно в виде календаря, в котором требуется выбрать дату и время начала/окончания периода и нажать кнопку **ОК**.
- **Состояние** – параметр используется для поиска правил по их состоянию. Значение выбирается из раскрывающегося списка.

Чтобы отфильтровать таблицу со списком правил по заданным параметрам, следует нажать кнопку **Применить** или клавишу **Enter** на клавиатуре. После этого значение в поле **Всего**, которое расположено под таблицей слева, также изменится. Очистить поля для фильтрации и вернуть таблицу в исходный вид позволяет кнопка **Сбросить**. Для скрытия области работы с фильтрами необходимо нажать кнопку Фильтры.

10.1.5. Карточка правила: просмотр и редактирование данных

Чтобы открыть карточку требуемого правила, необходимо найти это правило в таблице и нажать на строку, в которой оно записано.

Карточка правила (см. Рис.10.7) содержит следующую информацию:

- Идентификатор правила (расположен в заголовке карточки).
- **Пользователь** – ФИО пользователя, который последним вносил изменения в правило. Если в правило еще не вносились изменения, здесь будет отображаться его автор.
- **Версия** – номер версии правила.
- **Тип правила**: **Analyzer** или **Suricata**. Подробнее о типах правил см. в разделе 10.1.7.
- **Наименование** правила. Поле доступно для редактирования.
- **Состояние**: **Активировано** (включено) или **Деактивировано** (выключено). Поле доступно для редактирования.
- **Группа** – группа, в которую входит правило. Поле доступно для редактирования.
- **Набор** – набор, к которому относится правило. Правило может относиться к нескольким наборам, поэтому здесь может быть выбрано несколько значений. Поле доступно для редактирования.

- **Описание** – краткое описание правила. Поле доступно для редактирования.
- **Код** – содержимое правила (скрипт). Поле доступно для редактирования.

Примечание

*При внесении изменений в поле **Код** создается новая версия текущего правила – подробнее об этом см. в разделе 10.1.6.*

После внесения изменений в карточку правила необходимо нажать кнопку **Сохранить**, чтобы сохранить настройки. Чтобы отменить внесенные изменения, следует закрыть карточку правила, нажав на соответствующий значок в правом верхнем углу.

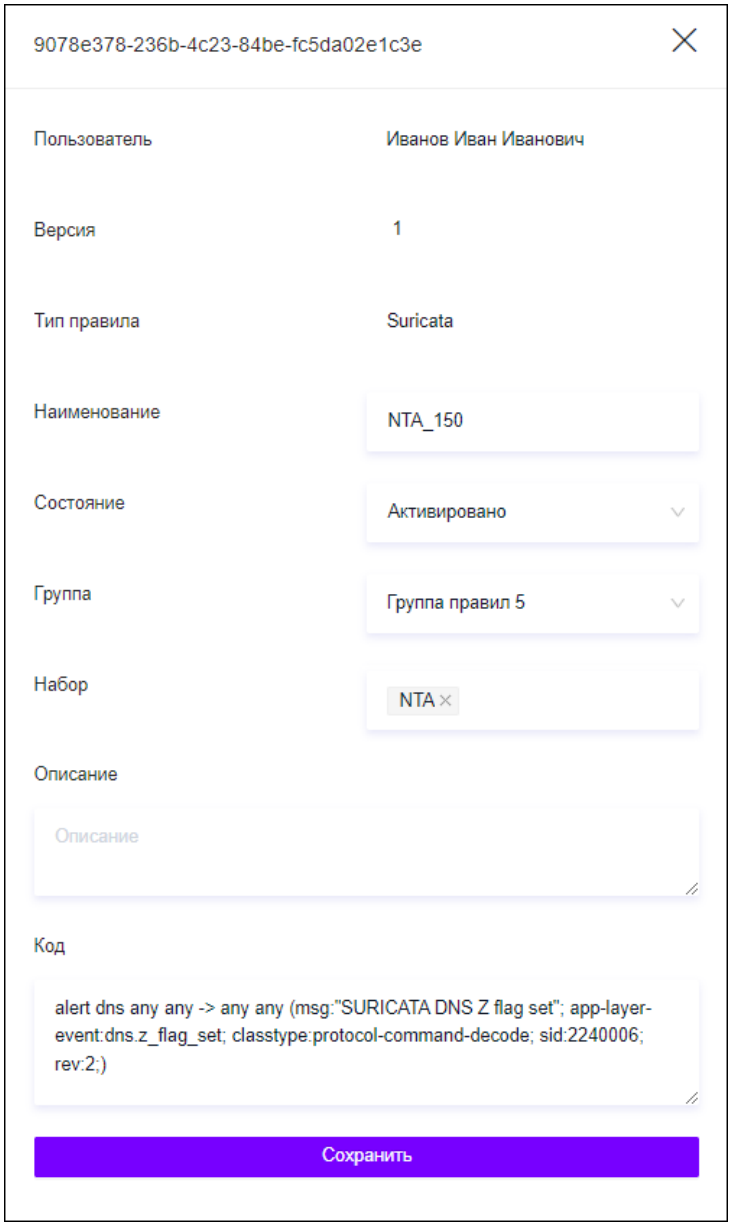


Рис. 10.7. Карточка правила

10.1.6. Создание новой версии правила

Каждая версия правила – это новое правило, которое также отображается в таблице. Новая версия автоматически создается после внесения изменений в код текущего правила. Здесь есть ряд особенностей:

- Номер текущей версии в карточке правила остается без изменений, а номер новой версии присваивается по принципу: **<номер текущей версии>+1**. Например, если внести изменения в код правила с номером версии 5, то новая версия создастся с номером 6, а номер старой версии останется без изменений.
- Все внесенные в текущее правило изменения сохраняются в новой версии. Например, если в карточке текущего правила изменить поля **Наименование**, **Код** и **Группа**, то новая версия создастся с новым названием и кодом, также она будет расположена в другой группе. В предыдущей версии правила эти поля останутся без изменений.

Примечание

*Следует помнить, что если поле **Код** не редактировалось, то новая версия не создастся, а изменения, внесенные в другие поля, сохранятся в текущей версии.*

- Если изменяется код активированного правила, то после сохранения изменений новая версия правила автоматически принимает состояние **Активировано**, а предыдущая – **Деактивировано**. При условии, что пользователь вручную не изменит состояние правила перед сохранением.
- При создании новой версии правила (при редактировании поля **Код**) **Дата изменения** старой версии также изменится.

10.1.7. Создание нового правила

Создать новое правило можно двумя способами:

- на вкладке **Правила**;
- на странице требуемого набора правил.

Чтобы создать новое правило, необходимо выполнить следующие действия:

1. Открыть раздел **Правила** и воспользоваться одним из вариантов:
   - на вкладке **Правила** нажать кнопку **Создать** в заголовке страницы.
   - на вкладке **Наборы**, открыть страницу требуемого набора правил и нажать кнопку **Создать** в списке правил.
2. В появившемся диалоговом окне (см. Рис.10.8) заполнить следующие поля:
   - **Наименование** правила. Поле является обязательным для заполнения.
   - **Тип правила**:
     - **Analyzer** – используется для обработки событий, поступающих из источника Solar EDR Windows (подробнее см. в разделе 10.1.8);

- **Suricata** – используется для обработки событий, поступающих из источника Solar NTA.

Значение выбирается из раскрывающегося списка. Поле является обязательным для заполнения.

- **Состояние**: **Активировано** или **Деактивировано**. Значение выбирается из раскрывающегося списка. Поле является обязательным для заполнения.
- **Группа**, в которую входит правило. Значение выбирается из раскрывающегося списка. Поле является обязательным для заполнения.
- **Набор**, к которому относится правило. Значение выбирается из раскрывающегося списка. Правило может относиться к нескольким наборам, поэтому здесь может быть выбрано несколько значений. Подробнее о наборах правил см. в разделе 10.3. Если правило создается со страницы набора, данное поле будет предзаполнено.
- **Описание** – текстовое описание создаваемого правила, например: «Подозрительная последовательность запуска процессов».
- **Код** – содержимое правила (скрипт). Поле является обязательным для заполнения. Подробнее о формате решающих правил типа **Analyzer** см. в разделе 10.1.8.

3. Нажать кнопку **Создать**.

После этого новое правило появится в таблице.

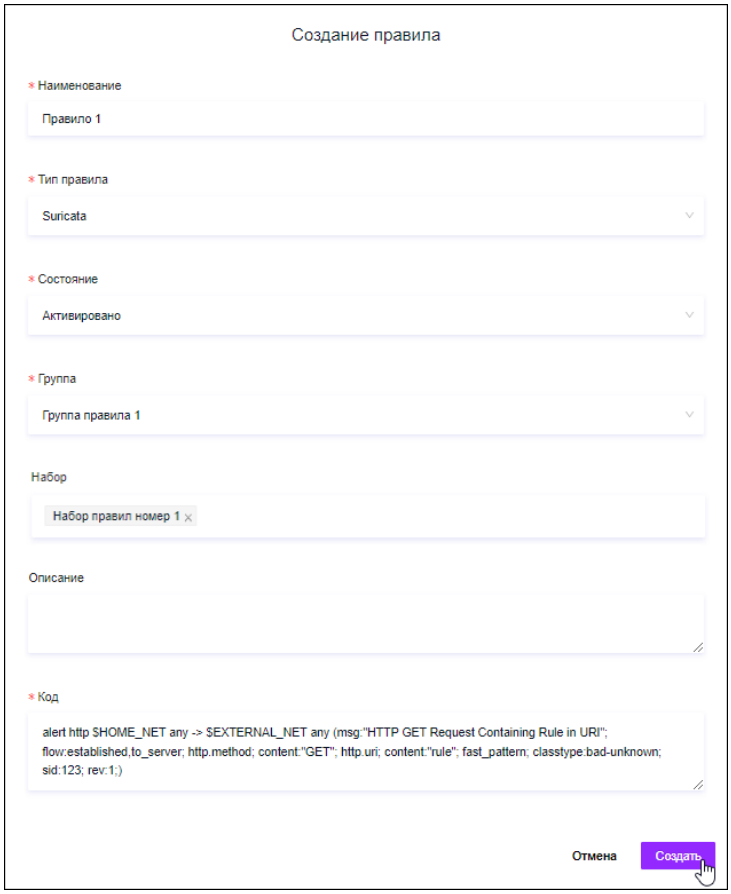


Рис. 10.8. Диалоговое окно создания нового правила

10.1.8. Формат решающих правил типа «Analyzer»

Правила типа **Analyzer** используются для обработки событий, поступающих из источника Solar EDR Windows. Правило типа **Analyzer** имеет следующую структуру:

- Тип события (см. раздел **Приложение B, *Сведения о типах событий***).
- Условие:
  - Атрибут события (см. разделы **Приложение C, *Обязательные атрибуты событий Solar EDR Windows и Solar NTA*** и **Приложение D, *Атрибуты событий Solar EDR Windows***);
  - Оператор (см. раздел **Приложение F, *Операторы в условиях правил***);
  - Значение: строка или справочник (см. раздел **10.2**).
- Логический оператор (используется для связи условий между собой):
  - **&&** – логическое «И»;
  - **||** – логическое «ИЛИ»;
  - **&& !(...)** – логическое «НЕ И»;
  - **|| !(...)** – логическое «НЕ ИЛИ».
- Реакция:
  - **filter** – прекращение обработки события;
  - **incident** – формирование инцидента.

Пример правила:

```
eventType = ImageLoad && (ImageName == "test" && ImageHash == 123) REACTION filter
```

Пример правила с использованием справочника в качестве значения представлен в разделе **10.2.8**.

10.1.9. Импорт правил

Солар ПКОиР позволяет не только вручную создавать правила, но и загружать готовые. Для этого предусмотрена процедура импорта. Чтобы загрузить готовое правило в систему, необходимо выполнить следующие действия:

1. Открыть раздел **Правила** и перейти на вкладку **Правила**.
2. Нажать кнопку  , расположенную над таблицей справа.
3. В открывшемся окне выбрать тип импортируемого правила, а также группу, в которую будет производиться импорт (см. **Рис.10.9**).

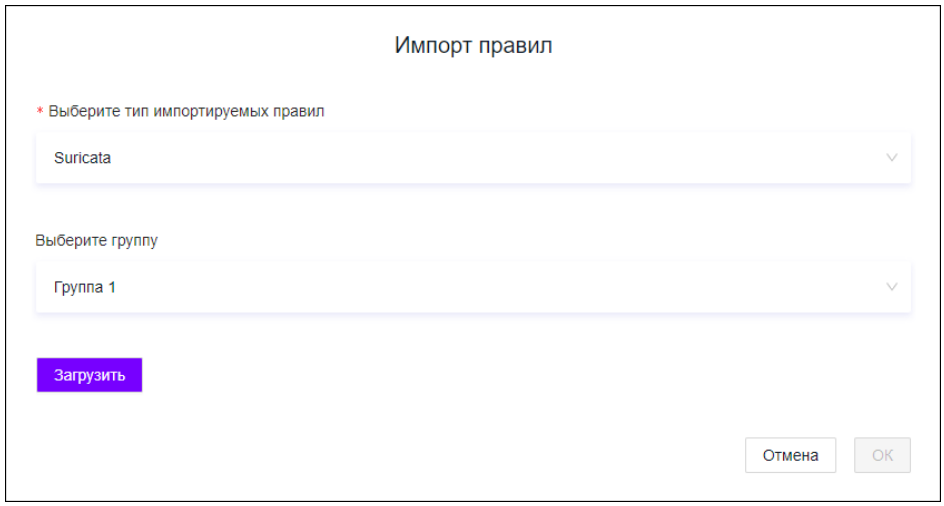


Рис. 10.9. Раздел «Правила». Вкладка «Правила». Импорт правил

4. Нажать кнопку **Загрузить** и в стандартном диалоговом окне выбрать файл с расширением ***.rules**. После этого в окне импорта правил отобразится имя импортируемого файла. Затем произойдет автоматическая проверка выбранного файла на соответствие формату:

   - если файл корректен и прошел проверку, пользователь увидит следующее сообщение: «Формат правил соответствует выбранному типу правил».
   - если файл не прошел проверку, отобразится сообщение: «Формат правил не соответствует выбранному типу». Загрузка такого файла будет невозможна. В этом случае пользователь может удалить некорректный файл (см. рис **Рис.10.10**) и загрузить новый.

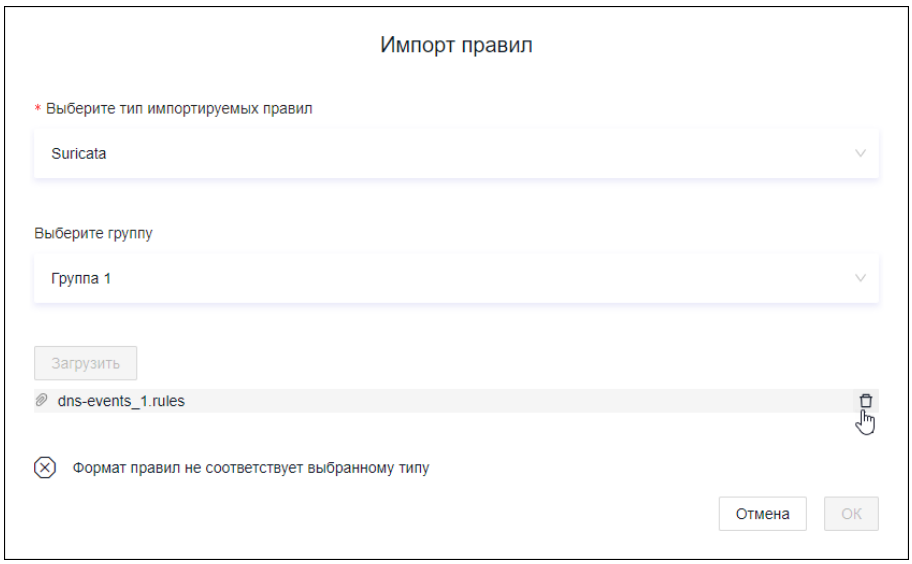


Рис. 10.10. Раздел «Правила». Вкладка «Правила». Импорт правил: удаление некорректного файла

5. Нажать кнопку **OK**, чтобы начать импорт.

Правило будет импортировано в группу, выбранную на шаге 4. **Состояние** импортированного правила будет **Активировано**.

10.2. Вкладка «Справочники»

Справочники содержат перечень значений, которые могут быть использованы в условиях правил.

Вкладка (см. Рис.10.11) состоит из следующих областей:

- заголовок страницы;
- панель навигации по группам справочников;
- фильтры;
- таблица со списком справочников.

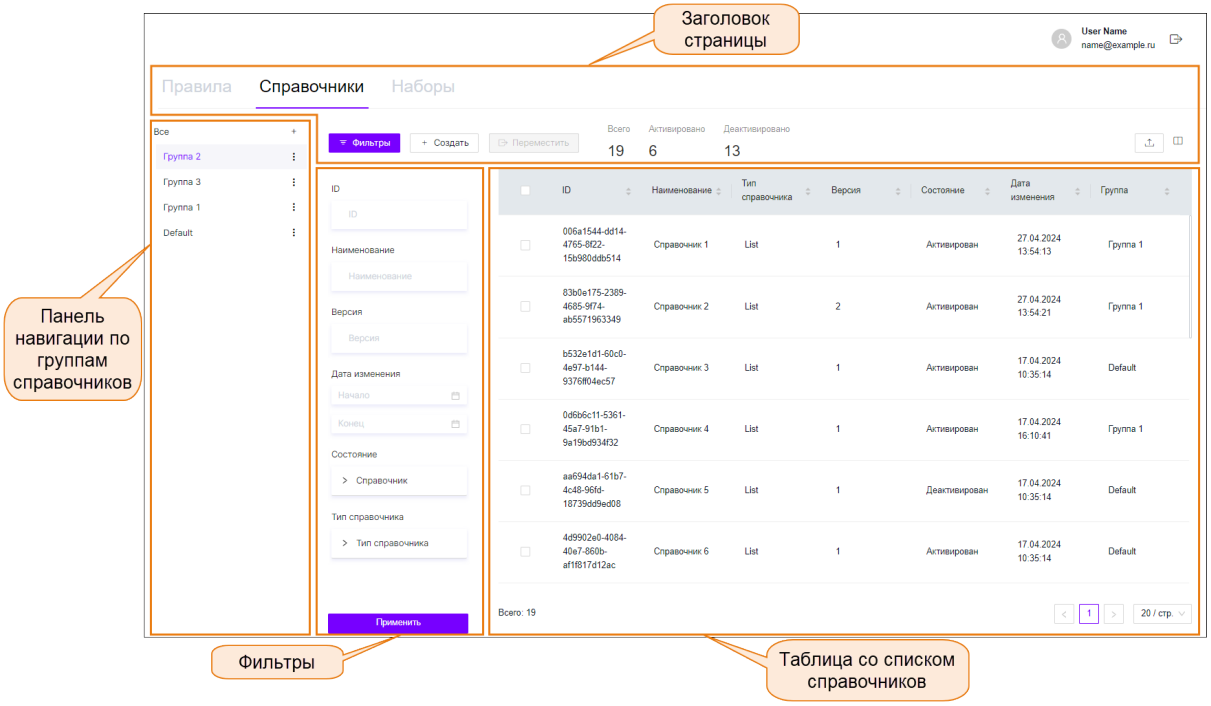


Рис. 10.11. Раздел «Правила». Вкладка «Справочники»

10.2.1. Таблица со списком справочников

Информация о справочниках представлена в виде таблицы. Состав и количество справочников, отображаемых в таблице, зависит от выбранной группы справочников на панели навигации (см. раздел 10.2.3).

Каждая строка таблицы соответствует определенному справочнику. Столбцы таблицы содержат следующую информацию:

- **ID** – идентификатор справочника.
- **Наименование** справочника.

- **Тип справочника**:
  - **List** (подробнее см. в разделе 10.2.8);
  - **IoC** (подробнее см. в разделе 10.2.9).
- **Версия** справочника.
- **Состояние** справочника:
  - **Активирован** (включен);
  - **Деактивирован** (выключен).
- **Дата изменения** – дата и время внесения последних изменений в справочник. Если справочник еще не изменялся, здесь будет отображаться дата его создания.
- **Группа** – группа, в которую входит справочник.

Кроме того, слева от каждого справочника расположен флажок, который используется при перемещении справочников из одной группы в другую – действия при этом аналогичны действиям при перемещении правил из одной группы в другую (подробнее см. в разделе 10.1.3.4).

При необходимости можно изменить набор столбцов в таблице – действия при этом аналогичны действиям при настройке таблицы со списком событий (подробнее см. в разделе 5.3.1).

Слева под таблицей отображается количество записей в таблице с учетом фильтрации (см. раздел 10.2.4), а также выбранной группы справочников на панели навигации (см. раздел 10.2.3).

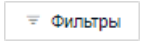
Так же, как и в других разделах, например, **События**, под таблицей справа расположены кнопки для перехода между страницами. По умолчанию на одной странице таблицы отображаются 20 записей. Для удобства можно изменить количество отображаемых записей на одной странице, нажав на соответствующее поле и выбрав в раскрывающемся списке требуемое число.

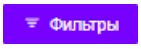
10.2.1.1. Сортировка справочников в таблице

По умолчанию справочники в таблице отсортированы в порядке их добавления. Для удобства работы можно изменить порядок отображения, нажав на значок в названии требуемого столбца. Настройки сортировки этой таблицы аналогичны настройкам в разделе **События** (см. раздел 5.2.1).

10.2.2. Заголовок страницы

В заголовке страницы содержатся:

- название текущей вкладки;
- кнопка 

/ 

– **Фильтры**, позволяющая развернуть/свернуть панель с полями для фильтрации;

- кнопка **Создать**, позволяющая добавить новый справочник (подробнее о создании нового справочника см. в разделе 10.2.7);
- кнопка **Переместить**, которая предназначена для перемещения справочников из одной группы в другую – действия при этом аналогичны действиям при перемещении правил из одной группы в другую (подробнее см. в разделе 10.1.3.4).
- сводная информация по справочникам:
  - **Всего** – общее количество справочников в системе.
  - **Активировано** – количество справочников в состоянии **Активирован**.
  - **Деактивировано** – количество справочников в состоянии **Деактивирован**.
- кнопка  , предназначенная для импорта готовых справочников в систему (см. раздел 10.2.10).
- значок ◫ для настройки отображения таблицы – действия аналогичны действиям при настройке отображения таблицы событий (подробнее см. в разделе 5.3.1).

10.2.3. Панель навигации по группам справочников

В левой части страницы расположена панель навигации по группам справочников. Панель навигации имеет древовидную структуру. По умолчанию на самом верхнем уровне расположен элемент **Все**. При нажатии на этот элемент в таблице отображаются все справочники из всех групп. На втором уровне размещены группы, добавленные пользователем, а также системная группа **Default**, которую нельзя удалить. При выборе определенной группы в таблице отображаются только справочники, входящие в эту и дочерние группы.

Примечание

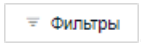
Следует отметить, что в текущей версии панель навигации имеет только два уровня вложенности. Это значит, что все создаваемые группы справочников будут находиться на втором уровне. Внутри групп второго уровня нельзя создавать новые группы.

Таким образом, если требуется отобразить в таблице все справочники, необходимо нажать на элемент **Все**. Если нужно показать только справочники из определенной группы, следует найти требуемую группу и нажать на ее название. При этом количество справочников, входящих в эту группу, можно увидеть под таблицей слева в поле **Всего**.

Здесь доступны следующие возможности:

- добавление новой группы справочников – действия аналогичны действиям при добавлении новой группы правил (подробнее см. в разделе 10.1.3.1);
- удаление группы справочников – действия аналогичны действиям при удалении группы правил (подробнее см. в разделе 10.1.3.2);
- изменение названия группы справочников – действия аналогичны действиям при изменении названия группы правил (подробнее см. в разделе 10.1.3.3).

10.2.4. Фильтры справочников

Чтобы открыть панель с полями для фильтрации, необходимо нажать кнопку 

, расположенную в заголовке страницы.

Примечание

Набор полей для фильтрации может различаться в зависимости от настроек отображения таблицы.

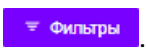
Примечание

*Фильтры и панель навигации по группам справочников (см. раздел 10.2.3) работают в связке. Например, если требуется найти все деактивированные справочники, входящие в группу **Группа справочников 1**, необходимо на панели навигации нажать на группу **Группа справочников 1**, затем в фильтре в поле **Состояние** установить флажок **Деактивирован** и нажать кнопку **Применить**. Фильтрация в этом случае будет производиться в рамках выбранной группы.*

Фильтрация справочников возможна по следующим полям:

- **ID** – параметр используется, если требуется найти определенный справочник по его идентификатору. Значение вводится с клавиатуры. Поиск осуществляется по полному совпадению значения.
- **Наименование** – позволяет найти справочник по его названию. Значение вводится с клавиатуры. Поиск по этому полю является регистрозависимым.
- **Версия** – параметр используется для поиска справочников по номеру версии. Значение вводится с клавиатуры. Поиск осуществляется по полному совпадению значения.
- **Дата изменения** – фильтр позволяет найти справочники, которые были последний раз отредактированы в заданном диапазоне времени. Для этого следует нажать на значок, расположенный в соответствующих полях. Откроется окно в виде календаря, в котором требуется выбрать дату и время начала/окончания периода и нажать кнопку **ОК**.
- **Состояние** – параметр используется для поиска справочников по их состоянию. Значение выбирается из раскрывающегося списка.
- **Тип справочника** – параметр используется для поиска справочников по их типу. Значение выбирается из раскрывающегося списка.

Чтобы отфильтровать таблицу со списком справочников по заданным параметрам, следует нажать кнопку **Применить** или клавишу **Enter** на клавиатуре. После этого значение в поле **Всего**, которое расположено под таблицей слева, также изменится. Очистить поля для фильтрации и вернуть таблицу в исходный вид позволяет кнопка **Сбросить**.

Для скрытия области работы с фильтрами необходимо нажать кнопку 

.

10.2.5. Карточка справочника: просмотр и редактирование данных

Чтобы открыть карточку требуемого справочника, необходимо найти этот справочник в таблице и нажать на строку, в которой он записан. Внешний вид и набор полей на карточке справочника различается в зависимости от его типа (см. Рис.10.12 и Рис.10.13).

Карточка справочника содержит следующую информацию:

- Идентификатор справочника (расположен в заголовке карточки).
- **Наименование** справочника.
- **Тип справочника**.
- **Версия** – номер версии справочника.
- **Пользователь** – ФИО пользователя, который последним вносил изменения в справочник. Если в справочник еще не вносились изменения, здесь будет отображаться его автор.
- **Дата изменения** – дата и время внесения последних изменений в справочник. Если справочник еще не изменялся, здесь будет отображаться дата его создания.
- **Тип данных**: **Строка** или **Число**. Отображается только в карточках справочников типа **List**.
- **Состояние**: **Активирован** (включен) или **Деактивирован** (выключен). Поле доступно для редактирования.
- **Группа** – группа, в которую входит справочник. Поле доступно для редактирования.
- **Наименования полей**. Отображается только в карточках справочников типа **IoC**.
- **Значения** справочника. Поле доступно для редактирования. Отображается только в карточках справочников типа **List**.

  Примечание

  *При внесении изменений в поле **Значения** создается новая версия текущего справочника – подробнее об этом см. в разделе 10.2.6.*

- **Описание** – краткое описание справочника. Поле доступно для редактирования.

После внесения изменений в карточку справочника необходимо нажать кнопку **Сохранить**, чтобы сохранить настройки. Чтобы отменить внесенные изменения, следует закрыть карточку справочника, нажав на соответствующий значок в правом верхнем углу.

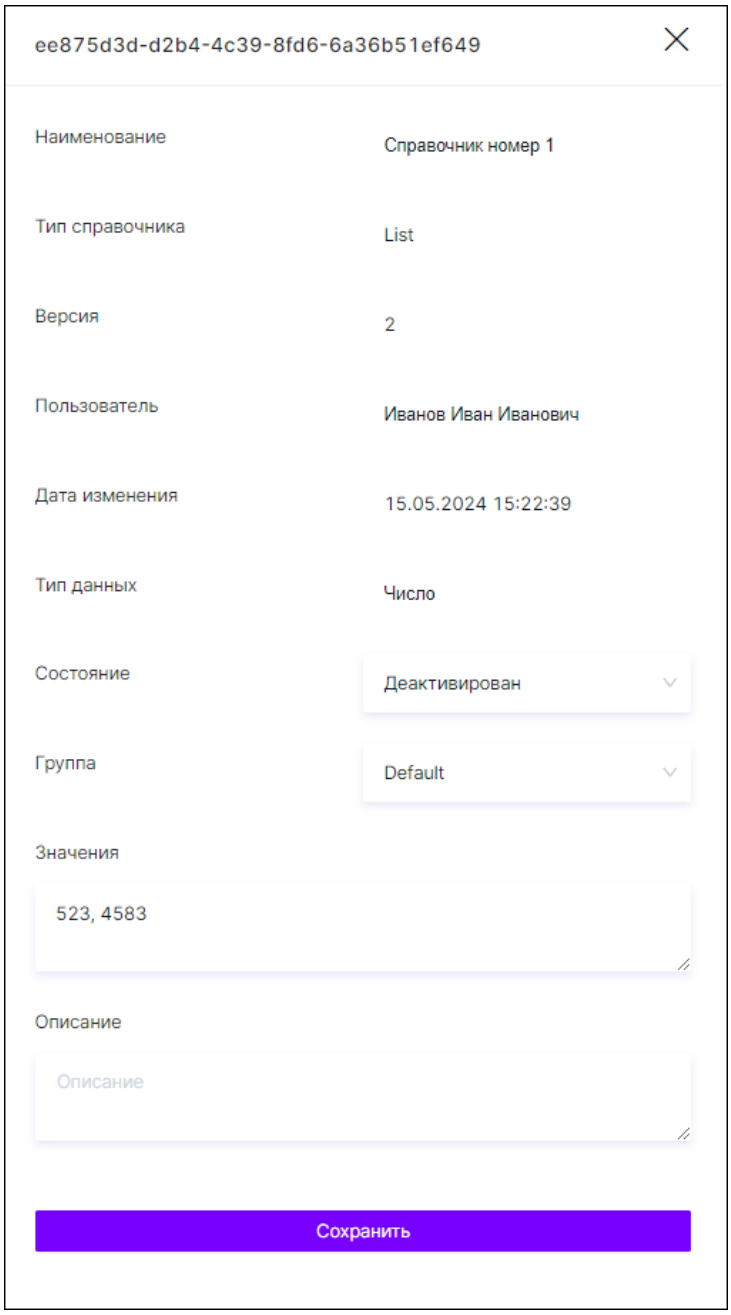


Рис. 10.12. Раздел «Правила». Вкладка «Справочники». Карточка справочника типа «List»

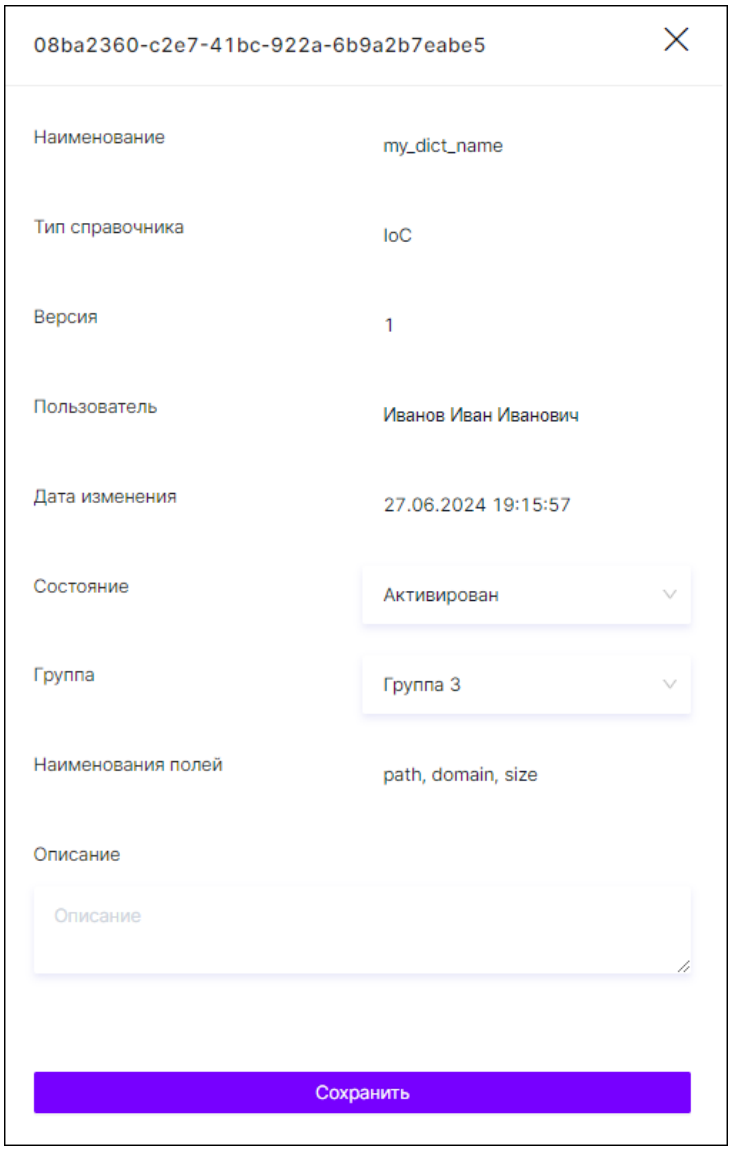


Рис. 10.13. Раздел «Правила». Вкладка «Справочники». Карточка справочника типа «IoC»

10.2.6. Создание новой версии справочника типа «List»

Каждая версия справочника – это новый справочник, который также отображается в таблице. Новая версия справочника типа **List** автоматически создается после внесения изменений в поле **Значения** текущего справочника. Здесь есть ряд особенностей:

- Номер текущей версии в карточке справочника остается без изменений, а номер новой версии присваивается по принципу: **<номер текущей версии>+1**. Например, если внести изменения в поле **Значения** справочника с номером версии 5, то новая версия создастся с номером 6, а номер старой версии останется без изменений.

- Все внесенные в текущий справочник изменения сохраняются в новой версии. Например, если в карточке текущего справочника изменить поля **Описание**, **Значения** и **Группа**, то новая версия создастся с новыми описанием и значениями, также она будет расположена в другой группе. В предыдущей версии справочника эти поля останутся без изменений.

Примечание

*Следует помнить, что если поле **Значения** не редактировалось, то новая версия не создастся, а изменения, внесенные в другие поля, сохранятся в текущей версии.*

- Если изменяется поле **Значения** в активированном справочнике, то после сохранения изменений новая версия справочника автоматически принимает состояние **Активирован**, а предыдущая – **Деактивирован**. При условии, что пользователь вручную не изменит состояние справочника перед сохранением.
- При создании новой версии справочника (при редактировании поля **Значения**) **Дата изменения** старой версии также изменится.

10.2.7. Создание нового справочника

Примечание

*В текущей версии создавать можно только справочники типа **List**. Справочники типа **IoC** создаются посредством импорта (см. раздел).*

Чтобы добавить новый справочник в систему, необходимо выполнить следующие действия:

1. Открыть раздел **Правила** на вкладке **Справочники**.
2. Нажать кнопку **Создать** в заголовке страницы.
3. В появившемся диалоговом окне (см. Рис.10.14) заполнить следующие поля:
   - **Наименование** справочника. Поле является обязательным для заполнения.
   - **Тип справочника**:
     - **List**.
     - **IoC**. В текущей версии данный тип справочника недоступен.
   - **Тип данных**: **Строка** или **Число**. Значение выбирается из раскрывающегося списка. Поле является обязательным для заполнения.
   - **Группа**, в которую входит справочник. Значение выбирается из раскрывающегося списка. Поле является обязательным для заполнения.
   - **Значения** – значения справочника. Поле является обязательным для заполнения.
   - **Описание** – текстовое описание создаваемого справочника.
4. Нажать кнопку **Создать**.

После этого новый справочник появится в таблице. **Состояние** нового справочника будет **Активирован**.

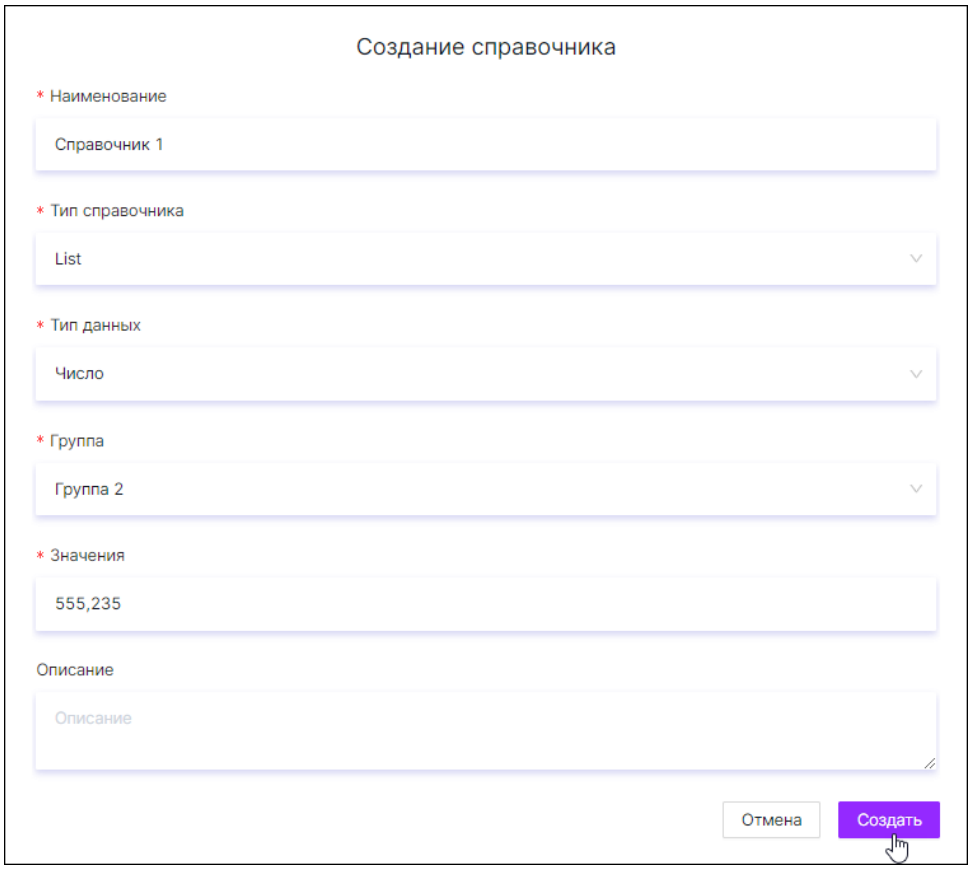


Рис. 10.14. Раздел «Правила». Вкладка «Справочники». Создание нового справочника

10.2.8. Справочники типа «List»

Справочник типа **List** используется при необходимости указания множества значений в условиях правил.

Пример справочника типа **List**:

```
name: my_dict_name
type: List
fields:
  - name: size
    type: int
    values:
      - 123654
      - 25897
      - 522222
```

где:

name – наименование справочника;

type – тип справочника;

fields – поля:

- **name** – наименование поля;

- **type** – тип данных: **string** или **int**;
- **values** – значения.

При использовании справочника в условиях правил в качестве оператора используется **includes**.

Пример правила с использованием справочника типа **List**:

```
eventType = WmiExecMethod && (User == tester && OperationId includes List_123 || Namespace includes List_Namespace) REACTION filter
```

10.2.9. Справочники типа «IoC»

Индикатор компрометации (Indicator of Compromise, IoC) – наблюдаемый в сети или на конкретном устройстве объект (или активность), который с большой долей вероятности указывает на несанкционированный доступ к системе (т. е. ее компрометацию).

Справочник типа **IoC**, так же как и **List**, используется в условиях правил.

Репутационный список IoC представляет собой многострочную таблицу, состоящую из четырех столбцов (см. Табл.10.1). В текущей версии в репутационных списках применяется три типа индикаторов.

Табл. 10.1. Репутационный список IoC

fields indicator	indicator_type	meta.source	meta.do_notice
43.229.13.208	Intel::ADDR	feed_solar	T
panel228.site	Intel::DOMAIN	feed_solar	T
2f8c6775ac4c32f2f9754168a2396c13	Intel::FILE_HASH	feed_solar	T

где:

fields indicator – значение индикатора;

indicator_type – тип индикатора;

meta.source – источник индикатора;

meta.do_notice – примечание.

Пример справочника типа **IoC**:

```
name: my_dict_name
type: IoC
fields:
  - name: path
    type: string
    values:
      - c:\\windows\\(system32|syswow64)\\image1.png
      - c:\\windows\\system32\\*
      - c:\\windows\\(system32|syswow64)\\test\\image2.jpg
  - name: domains
    type: string
    values:
      - domain1
```

```
    - domain2
- name: size
  type: int
  values:
    - 123654
    - 25897
    - 522222
```

где:

name – наименование справочника;

type – тип справочника;

fields – поля:

- **name** – наименование поля;
- **type** – тип данных: **string** или **int**;
- **values** – значения.

При использовании справочника в условиях правил в качестве оператора используется **includes**.

Пример правила с использованием справочника типа **IoC**:

```
eventType = WmiExecMethod && (User == "tester" && OperationId includes "my_dict_name.domains")
 REACTION incident
```

где:

my_dict_name – наименование справочника IoC;

domains – наименование массива атрибута в справочнике, по которым выполняется проверка.

10.2.10. Импорт справочников

Солар ПКОиР позволяет не только вручную создавать справочники, но и загружать готовые. Для этого предусмотрена процедура импорта. Чтобы загрузить готовый справочник в систему, необходимо выполнить следующие действия:

1. Открыть раздел **Правила** и перейти на вкладку **Справочники**.
2. Нажать кнопку  , расположенную над таблицей справа.
3. В открывшемся окне выбрать тип импортируемого справочника и группу, в которую будет производиться импорт (см. **Рис.10.15**).

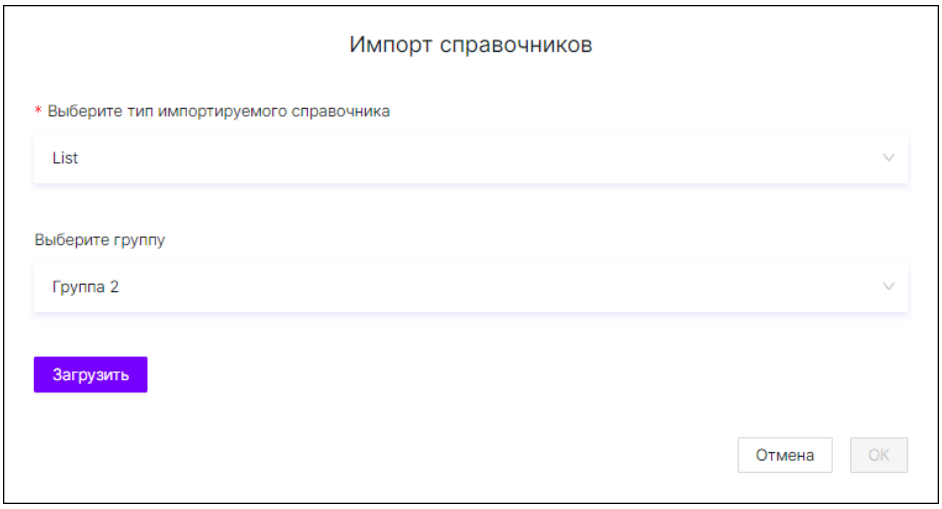


Рис. 10.15. Раздел «Правила». Вкладка «Справочники». Импорт справочников

4. Нажать кнопку **Загрузить** и в стандартном диалоговом окне выбрать файл с расширением ***.tl**. После этого в окне импорта справочников отобразится имя импортируемого файла. Затем произойдет автоматическая проверка выбранного файла на соответствие формату:

   - если файл корректен и прошел проверку, пользователь увидит следующее сообщение: «Справочник соответствует формату».
   - если файл не прошел проверку, отобразится сообщение: «Справочник не соответствует формату». Загрузка такого файла будет невозможна. В этом случае пользователь может удалить некорректный файл (см. Рис.10.16) и загрузить новый.

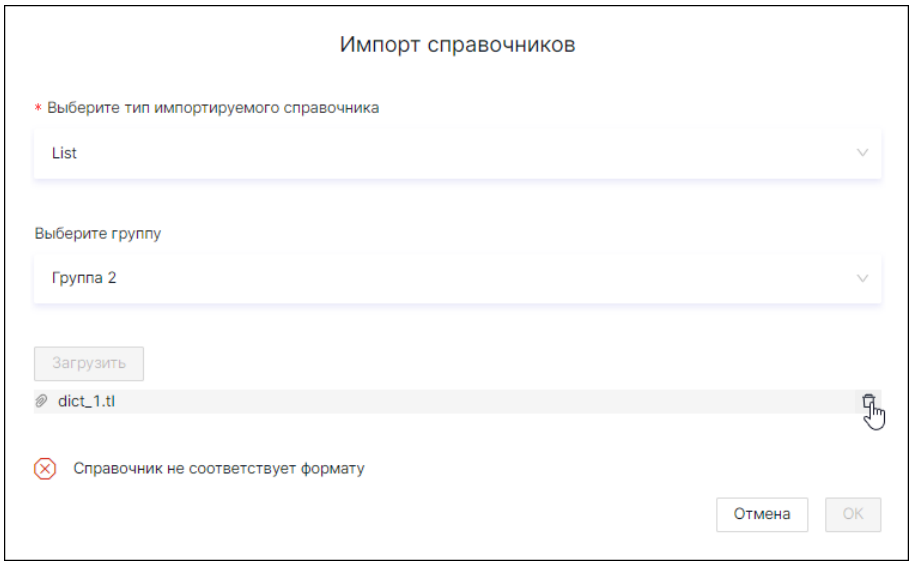


Рис. 10.16. Раздел «Правила». Вкладка «Справочники». Импорт справочников: удаление некорректного файла

5. Нажать кнопку **OK**, чтобы начать импорт.

Справочник будет импортирован в группу, выбранную на шаге 4. **Состояние** импортированного справочника будет **Активирован**.

10.3. Вкладка «Наборы»

Набор правил представляет собой сгруппированный пользователем список правил для более удобного управления большим количеством правил и создания стандартных конфигураций. Вкладка **Наборы** (см. Рис.10.17) состоит из следующих областей:

- заголовок страницы;
- фильтры;
- таблица со списком наборов правил.

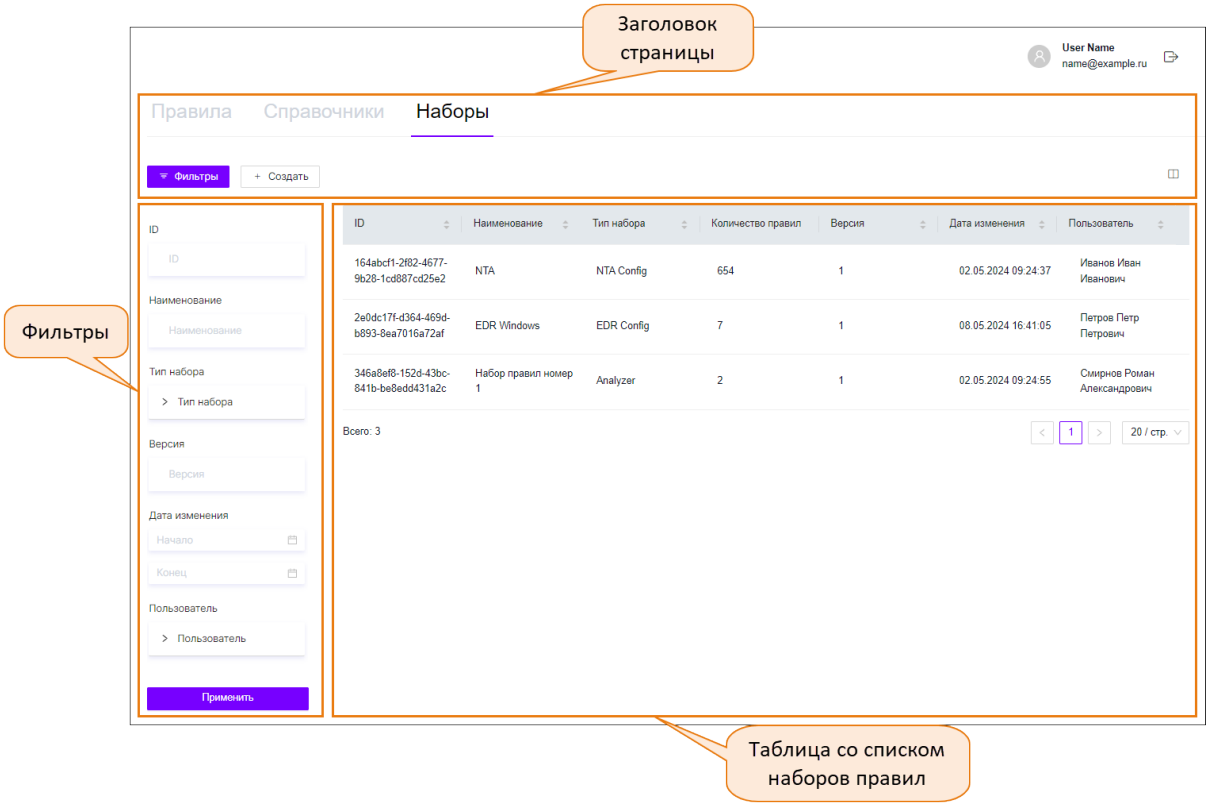


Рис. 10.17. Раздел «Правила». Вкладка «Наборы»

10.3.1. Таблица со списком наборов правил

Информация о наборах правил представлена в виде таблицы. Каждая строка таблицы соответствует определенному набору правил. Столбцы таблицы содержат следующую информацию:

- **ID** – идентификатор набора правил.
- **Наименование** набора.
- **Тип набора**:
  - **EDR Config**;

- **NTA Config**;
- **Analyzer**.

- **Количество правил** – количество правил, входящих в набор.
- **Версия** – версия набора правил.
- **Дата изменения** – дата и время внесения последних изменений в набор правил, например, при добавлении правила в набор. Если в набор правил еще не вносились изменения, здесь будут отображаться дата и время его создания.
- **Пользователь** – ФИО пользователя, который последним внес изменения в набор. Если в набор правил еще не вносились изменения, здесь будет отображаться автор набора.

При необходимости можно изменить набор столбцов в таблице – действия при этом аналогичны действиям при настройке таблицы со списком событий (подробнее см. в разделе 5.3.1).

Слева под таблицей отображается количество записей в таблице с учетом фильтрации (см. раздел 10.3.3).

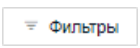
Так же, как и в других разделах, например, **События**, под таблицей справа расположены кнопки для перехода между страницами. По умолчанию на одной странице таблицы отображаются 20 записей. Для удобства можно изменить количество отображаемых записей на одной странице, нажав на соответствующее поле и выбрав в раскрывающемся списке требуемое число.

10.3.1.1. Сортировка правил в таблице

По умолчанию наборы правил в таблице отсортированы в порядке их добавления. Для удобства работы можно изменить порядок отображения, нажав на значок ⇕ в названии требуемого столбца. Настройки сортировки этой таблицы аналогичны настройкам в разделе **События** (см. раздел 5.2.1).

10.3.2. Заголовок страницы

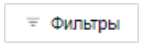
В заголовке страницы содержатся:

- название текущей вкладки;
- кнопка 

/ 

– **Фильтры**, позволяющая развернуть/свернуть панель с полями для фильтрации;
- кнопка **Создать**, позволяющая добавить новый набор правил (подробнее об этом см. в разделе 10.3.5);
- значок ◫ для настройки отображения таблицы – действия аналогичны действиям при настройке отображения таблицы событий (см. раздел 5.3.1).

10.3.3. Фильтры наборов правил

Чтобы открыть панель с полями для фильтрации, необходимо нажать кнопку 

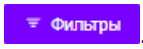
, расположенную в заголовке страницы.

Примечание

Набор полей для фильтрации может различаться в зависимости от настроек отображения таблицы.

Фильтрация наборов правил возможна по следующим полям:

- **ID** – параметр используется, если требуется найти определенный набор правил по его идентификатору. Значение вводится с клавиатуры. Поиск осуществляется по полному совпадению значения.
- **Наименование** – позволяет найти набор правил по его названию. Значение вводится с клавиатуры. Поиск по этому полю является регистрозависимым.
- **Тип набора** – фильтр позволяет найти все наборы правил определенного типа. Требуемое значение отмечается флажком в раскрывающемся списке.
- **Версия** – параметр используется для поиска наборов правил по номеру версии. Значение вводится с клавиатуры. Поиск осуществляется по полному совпадению значения.
- **Дата изменения** – фильтр позволяет найти наборы, которые были последний раз отредактированы в заданном диапазоне времени. Для этого следует нажать на значок  , расположенный в соответствующих полях. Откроется окно в виде календаря, в котором требуется выбрать дату и время начала/окончания периода и нажать кнопку **ОК**.
- **Пользователь** – параметр используется для поиска набора правил по пользователю, который последним вносил в него изменения. Значение вводится с клавиатуры. Поиск по этому полю является регистрозависимым и осуществляется по полному совпадению значения.

Чтобы отфильтровать таблицу с наборами правил по заданным параметрам, следует нажать кнопку **Применить** или клавишу **Enter** на клавиатуре. После этого значение в поле **Всего**, которое расположено под таблицей слева, также изменится. Очистить поля для фильтрации и вернуть таблицу в исходный вид позволяет кнопка **Сбросить**. Для скрытия области работы с фильтрами необходимо нажать кнопку 

.

10.3.4. Страница набора правил

Чтобы открыть страницу требуемого набора правил, необходимо найти этот набор в таблице и нажать на строку, в которой он записан.

Страница набора правил (см. Рис.10.18) состоит из следующих областей:

- Заголовок страницы:

- путь к набору, содержащий название раздела и наименование набора правил;
- кнопка **Назад**, которая позволяет вернуться к списку наборов правил;
- кнопка **Редактировать**, позволяющая внести изменения в набор правил (подробнее об этом см. в разделе 10.3.7);
- кнопка **Удалить**, позволяющая удалить набор правил (подробнее см. в разделе 10.3.8).

- Основная информация о наборе правил:
  - **ID** – идентификатор набора правил.
  - **Описание** – краткое описание набора правил.
  - **Применение** – политики, в состав которых входит данный набор правил.
  - **Тип набора**.
  - **Версия набора** – номер версии набора правил. Следует обратить внимание, что версия набора изменяется при изменении состава входящих в него правил.
  - **Дата изменения** – дата и время внесения последних изменений в набор правил. Если в набор правил еще не вносились изменения, здесь будет отображаться дата его создания.
  - **Пользователь** – пользователь, который последним внес изменения в набор. Если в набор правил еще не вносились изменения, здесь будет отображаться автор набора.
- Список входящих в набор правил (см. раздел 10.3.4.1).

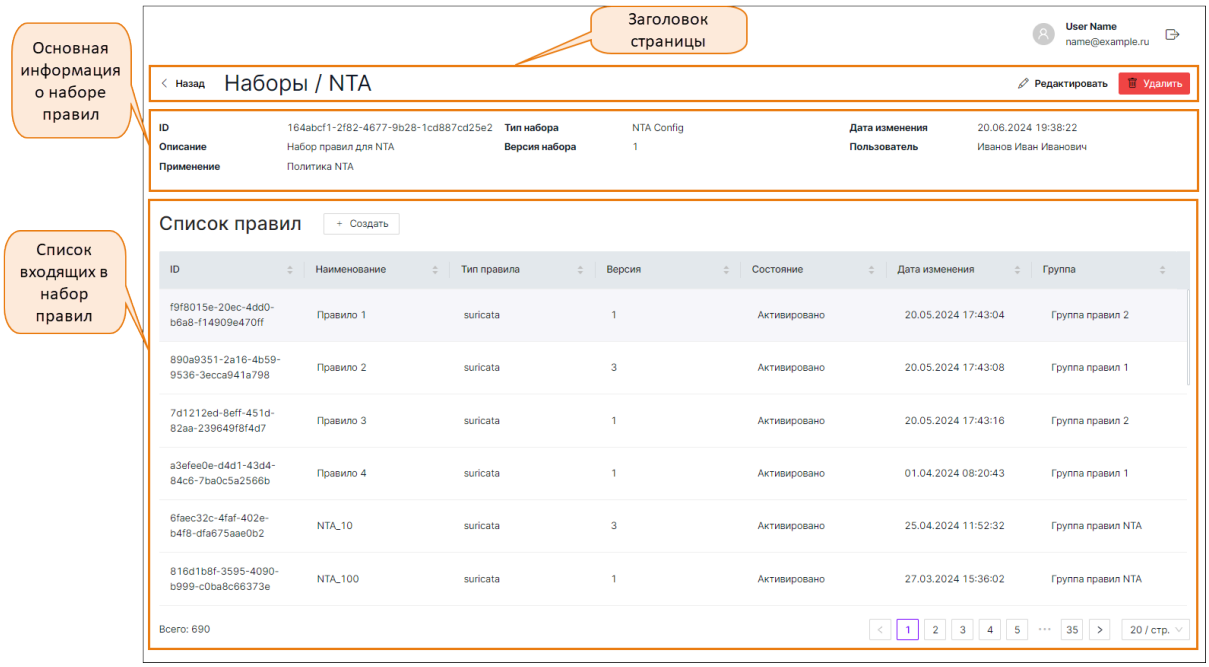


Рис. 10.18. Раздел «Правила». Вкладка «Наборы». Страница набора правил

10.3.4.1. Список входящих в набор правил

Под основной информацией о наборе правил расположена таблица со списком правил, входящих в этот набор. Каждая строка таблицы соответствует определенному правилу. Столбцы таблицы содержат следующую информацию:

- **ID** – идентификатор правила.
- **Наименование** правила.
- **Тип правила**.
- **Версия** правила.
- **Состояние** правила:
  - **Активировано**;
  - **Деактивировано**.
- **Дата изменения** – дата и время внесения последних изменений в правило. Если правило еще не изменялось, здесь будет отображаться дата его создания.
- **Группа** – группа, в которую входит правило.

Слева под таблицей в поле **Всего** отображается количество правил, входящих в набор.

При нажатии на строку с правилом, будет открыта карточка этого правила (подробнее о карточке правила см. в разделе 10.1.5).

Вверху таблицы расположена кнопка **Создать**, позволяющая создать новое правило в наборе (подробнее об этом см. в разделе 10.1.7).

Так же, как и в других разделах, например, **События**, под таблицей справа расположены кнопки для перехода между страницами. По умолчанию на одной странице таблицы отображаются 20 записей. Для удобства можно изменить количество отображаемых записей на одной странице, нажав на соответствующее поле и выбрав в раскрывающемся списке требуемое число.

По умолчанию правила в таблице отсортированы в порядке их добавления. Для удобства работы можно изменить порядок отображения, нажав на значок в названии требуемого столбца.

10.3.5. Создание набора правил

Чтобы создать новый набор правил, необходимо выполнить следующие действия:

1. Открыть раздел **Правила** на вкладке **Наборы**.
2. Нажать кнопку **Создать**, расположенную в области заголовка страницы (см. Рис.10.17).
3. В появившемся диалоговом окне (см. Рис.10.19) заполнить поля:
   - **Наименование** набора правил. Поле является обязательным для заполнения.

- **Тип набора**. Значение выбирается из раскрывающегося списка. Поле является обязательным для заполнения.
- **Описание** – краткое описание создаваемого набора.
- **Применение** – список политик, в состав которых будет входить создаваемый набор правил. Таких политик может быть несколько. Значения выбираются из раскрывающегося списка.

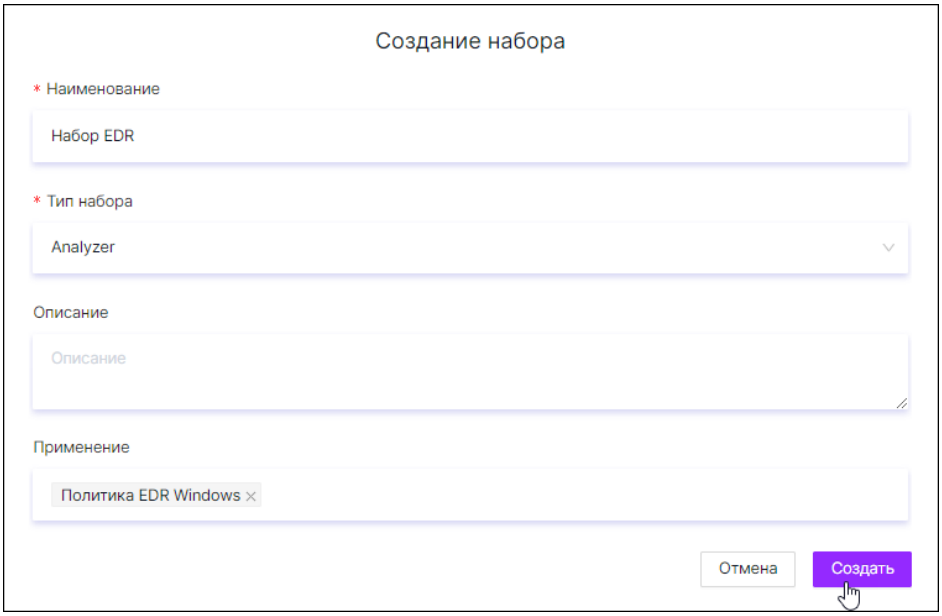


Рис. 10.19. Раздел «Правила». Вкладка «Наборы». Окно создания набора правил

4. Нажать кнопку **Создать**. После этого будет открыта карточка созданного набора.
5. Добавить в набор правила. Подробнее об этом см. в разделе 10.3.6

10.3.6. Добавление правил в набор

Добавить правило в набор можно несколькими способами:

- со страницы набора (см. Рис.10.18) с помощью кнопки **Создать** – в этом случае создастся новое правило;
- из вкладки **Правила** с помощью кнопки **Созадать** – в этом случае так же создастся новое правило (подробнее см. в разделе 10.1.7);
- из карточки существующего правила, путем добавления требуемого набора в поле **Набор** (см. в разделе 10.1.5).

Примечание

*В текущей версии для корректного применения политики на хостах с агентом Solar EDR необходимо, чтобы в политике был хотя бы один набор, содержащий правило типа **Analyzer**.*

10.3.7. Редактирование набора правил

Примечание

*Наборы правил **NTA** и **EDR Windows** являются системными и их нельзя изменить.*

Чтобы внести изменения в набор правил, необходимо выполнить следующие действия:

1. Открыть раздел **Правила** на вкладке **Наборы**.
2. В таблице найти требуемый набор правил и открыть его страницу.
3. Нажать кнопку **Редактировать**, которая расположена в правом верхнем углу (см. Рис.10.18).
4. В появившемся окне (см. Рис.10.20) внести требуемые изменения в поля:
   - **Наименование** правила;
   - **Описание**;
   - **Применение** – список политик, в состав которых входит данный набор правил.

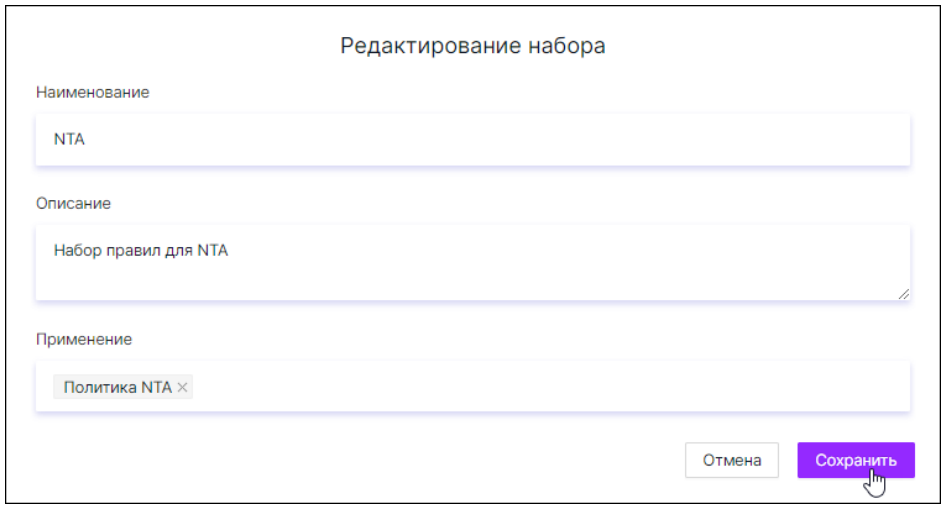


Рис. 10.20. Страница набора правил. Редактирование данных

5. Нажать кнопку **Сохранить**.

Набор правил будет изменен.

10.3.8. Удаление набора правил

Примечание

*Наборы правил **NTA** и **EDR Windows** являются системными и их нельзя удалить.*

Чтобы удалить набор правил, необходимо выполнить следующие действия:

1. Открыть раздел **Правила** на вкладке **Наборы**.
2. В таблице найти требуемый набор правил и открыть его страницу.
3. Нажать кнопку **Удалить**, которая расположена в правом верхнем углу (см. Рис.10.18).
4. В появившемся диалоговом окне (см. Рис.10.21) подтвердить удаление набора правил, нажав на соответствующую кнопку.

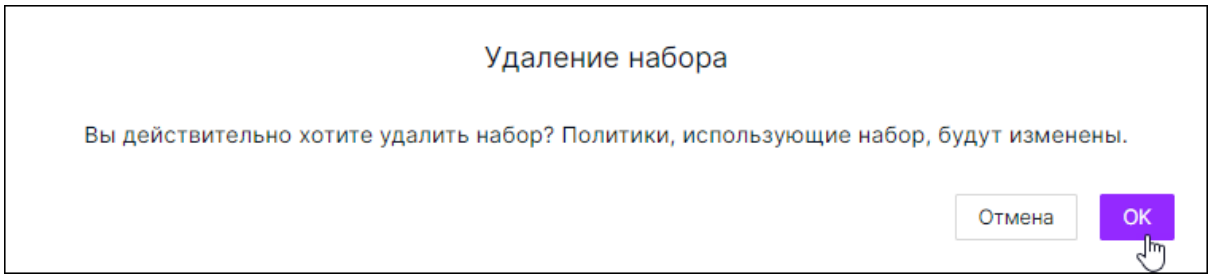


Рис. 10.21. Диалоговое окно подтверждения удаления набора правил

Набор будет удален. При этом правила, входящие в этот набор, удалены не будут, в карточках таких правил изменится значение поля **Набор**. Кроме того, после удаления набора изменятся и политики, в которых был использован данный набор правил.

11. Раздел «Настройки»

Раздел **Настройки** предназначен для просмотра, создания и редактирования учетных записей пользователей, а также для управления ролевым доступом.

Примечание

Доступ к отдельным компонентам и функциональным возможностям раздела может различаться в зависимости от роли пользователя (подробнее о ролевой модели см. в разделе 11.1.6).

В рамках текущей версии раздел состоит из вкладки **Пользователи** (см. раздел 11.1).

11.1. Вкладка «Пользователи»

После перехода в раздел **Настройки** по умолчанию будет открыта вкладка **Пользователи**, которая содержит таблицу с информацией об учетных записях пользователей Солар ПКОиР. Вкладка **Пользователи** (см. Рис.11.1) состоит из следующих областей:

- заголовок страницы;
- фильтры;
- таблица со списком пользователей.

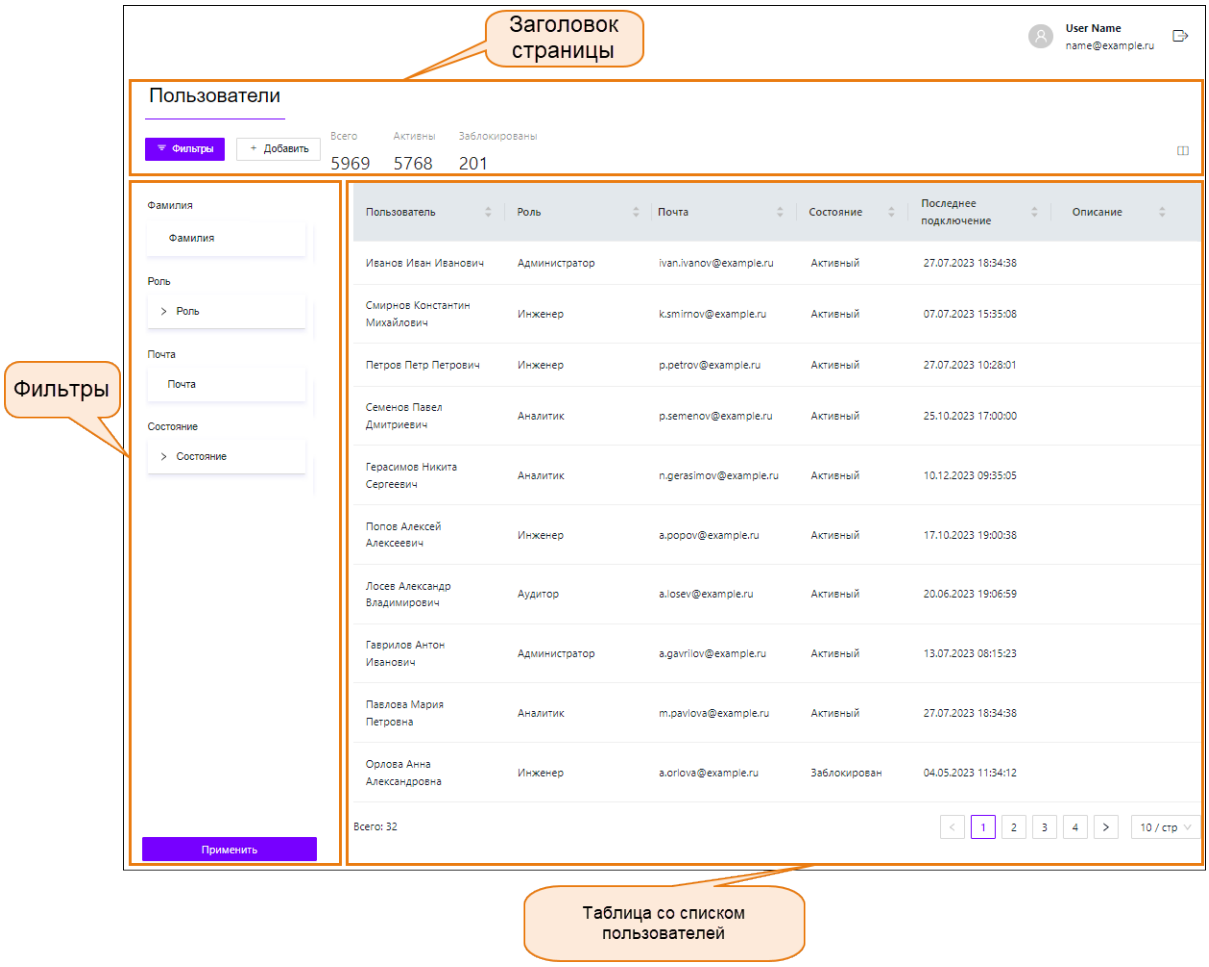


Рис. 11.1. Раздел «Настройки». Вкладка «Пользователи»

11.1.1. Таблица со списком пользователей

Информация о пользователях системы представлена в виде таблицы. Каждая строка таблицы соответствует определенному пользователю. Столбцы таблицы содержат следующую информацию:

- **Пользователь** – фамилия, имя и отчество пользователя системы.
- **Роль** – совокупность прав доступа, назначаемых пользователю для выполнения конкретных задач. Подробнее о ролевой модели см. в разделе 11.1.6.
- **Почта** – адрес электронной почты, используемый при входе в систему.
- **Состояние** учетной записи пользователя:
  - **Активный** – доступ к системе разрешен.
  - **Заблокирован** – доступ к системе заблокирован.
- **Последнее подключение** – дата и время последнего подключения к системе.
- **Описание** – комментарий по пользователю.

При необходимости можно изменить набор столбцов в таблице – действия при этом аналогичны действиям при настройке таблицы со списком событий (подробнее см. в разделе 5.3.1).

Слева под таблицей отображается количество записей в таблице с учетом фильтрации (см. раздел 11.1.4).

Так же, как и в других разделах, например, **События**, под таблицей справа расположены кнопки для перехода между страницами. По умолчанию на одной странице таблицы отображаются 20 записей. Для удобства можно изменить количество отображаемых записей на одной странице, нажав на соответствующее поле и выбрав в раскрывающемся списке требуемое число.

11.1.1.1. Сортировка пользователей в таблице

По умолчанию учетные записи пользователей в таблице отсортированы в порядке их добавления. Для удобства работы можно изменить порядок отображения, нажав на значок в названии требуемого столбца. Настройки сортировки этой таблицы аналогичны настройкам в разделе **События** (см. раздел 5.2.1).

11.1.2. Заголовок страницы

В заголовке страницы содержатся:

- название текущей вкладки;
- кнопка Фильтры / Фильтры – **Фильтры**, позволяющая развернуть/свернуть панель с полями для фильтрации;
- кнопка **Добавить**, позволяющая создать нового пользователя системы (подробнее о добавлении нового пользователя см. в разделе 11.1.3);
- сводная информация по пользователям:
  - **Всего** – общее количество пользователей системы.
  - **Активны** – количество активных пользователей (имеющих доступ к системе).
  - **Заблокированы** – количество заблокированных пользователей (не имеющих доступа к системе).
- значок для настройки отображения таблицы – действия аналогичны действиям при настройке отображения таблицы событий (см. раздел 5.3.1).

11.1.3. Добавление нового пользователя

Примечание

*Возможность добавления новых пользователей системы доступна только пользователям с ролью **Суперадминистратор** и **Администратор**. Подробнее о ролевой модели см. в разделе 11.1.6.*

Чтобы добавить нового пользователя системы, например, при приеме сотрудника на работу, необходимо выполнить следующие действия:

1. Открыть раздел **Настройки** и перейти на вкладку **Пользователи**.

2. Нажать кнопку **Добавить** в заголовке страницы.

3. В появившемся диалоговом окне (см. **Рис.11.2**) заполнить следующие поля:

   - **Фамилия** пользователя. Поле является обязательным для заполнения.
   - **Имя** пользователя. Поле является обязательным для заполнения.
   - **Отчество** пользователя.
   - **Роль** – совокупность прав доступа, назначаемых пользователю для выполнения конкретных задач (подробнее о ролевой модели см. в разделе **11.1.6**). Значение выбирается из раскрывающегося списка. Набор значений в раскрывающемся списке будет различаться в зависимости от роли пользователя, который создает нового пользователя. Поле является обязательным для заполнения.
   - **Почта** – уникальный адрес электронной почты пользователя, который будет использоваться в качестве логина при входе в систему. Поле является обязательным для заполнения. В дальнейшем на этот адрес будет отправлено письмо со ссылкой для активации учетной записи.
   - **Телефон** – номер телефона пользователя в формате +7(XXX)-XXX-XX-XX.

4. Нажать кнопку **Сохранить**.

После этого новый пользователь появится в таблице, а на указанный адрес электронной почты придет письмо со ссылкой для активации учетной записи и установки пароля.

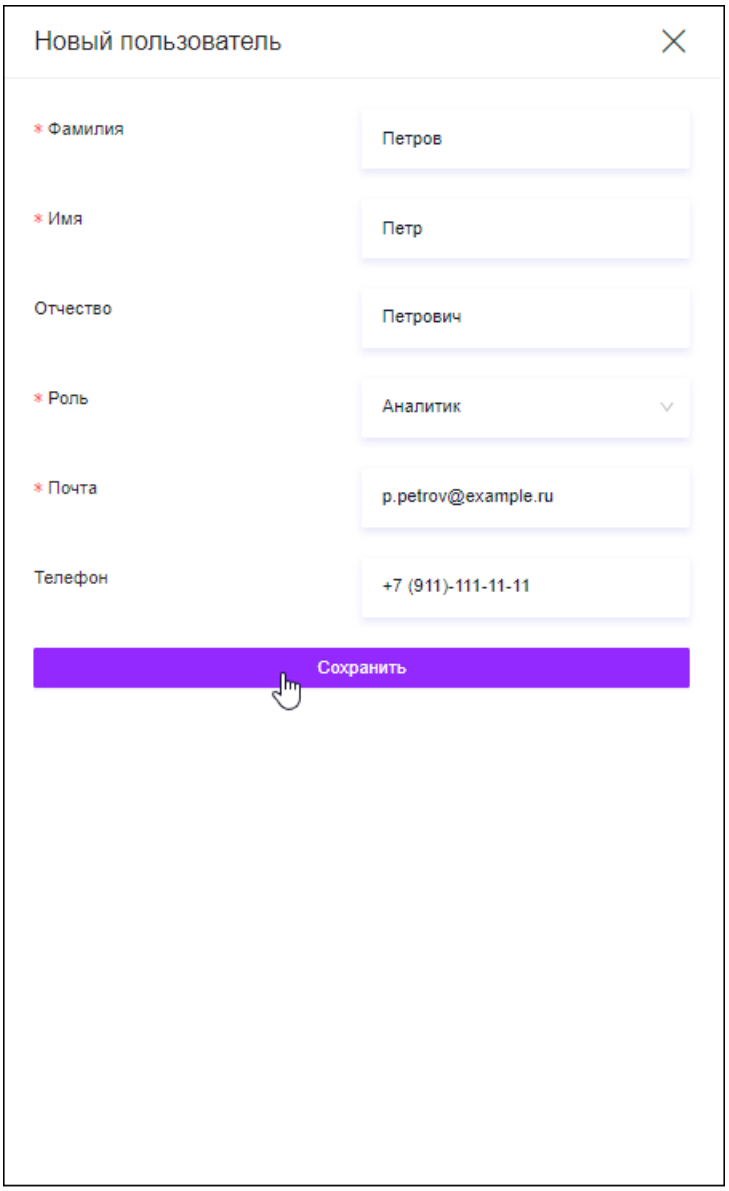


Рис. 11.2. Раздел «Настройки». Вкладка «Пользователи». Добавление нового пользователя

11.1.4. Фильтры учетных записей пользователей

Чтобы открыть панель с полями для фильтрации, необходимо нажать кнопку Фильтры, расположенную в заголовке страницы.

Примечание

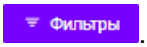
Набор полей для фильтрации может различаться в зависимости от настроек отображения таблицы.

Фильтрация возможна по следующим полям:

- **Фамилия** – позволяет найти пользователя по его фамилии. Значение вводится с клавиатуры. Поиск по этому полю является регистрозависимым.

- **Роль** – фильтр позволяет найти всех пользователей системы с определенной ролью. Для этого следует отметить флажками одно или несколько значений.
- **Почта** – с помощью этого фильтра можно найти пользователя системы по электронной почте. Значение вводится с клавиатуры. Поиск по этому полю является регистрозависимым.
- **Состояние** – этот фильтр позволяет найти все активные или заблокированные учетные записи пользователей. Для этого в списке необходимо выбрать требуемое значение.

Чтобы отфильтровать таблицу со списком пользователей по заданным параметрам, следует нажать кнопку **Применить** или клавишу **Enter** на клавиатуре. После этого значение в поле **Всего**, которое расположено под таблицей слева, также изменится. Очистить поля для фильтрации и вернуть таблицу в исходный вид позволяет кнопка **Сбросить**.

Для скрытия области работы с фильтрами необходимо нажать кнопку 

.

11.1.5. Карточка пользователя: просмотр и редактирование данных

Чтобы открыть карточку требуемого пользователя, необходимо найти его в таблице и нажать на строку, в которой он записан.

Примечание

*Внешний вид карточки может различаться в зависимости от роли пользователя, который ее открыл. Например, пользователь с ролью **Администратор** при открытии карточки пользователя с ролью **Администратор** сможет только просмотреть данные, а при открытии карточки пользователя с ролью **Инженер** сможет внести изменения. Подробнее о ролевой модели см. в разделе 11.1.6.*

Карточка пользователя (см. Рис.11.3) содержит следующую информацию:

- **Состояние** – состояние учетной записи пользователя. В режиме редактирования этот переключатель позволяет управлять доступом пользователя к системе (подробнее об этом см. в разделе 11.1.7):
  - **Активный** – доступ к системе разрешен.
  - **Заблокирован** – доступ к системе заблокирован.
- **Фамилия** – фамилия пользователя. В режиме редактирования поле является обязательным для заполнения.
- **Имя** – имя пользователя. В режиме редактирования поле является обязательным для заполнения.
- **Отчество** – отчество пользователя.
- **Роль** – совокупность прав доступа, назначаемых пользователю для выполнения конкретных задач (подробнее о ролевой модели см. в разделе 11.1.6). В режиме редактирования значение выбирается из раскрывающегося списка. Набор значений в раскрывающемся списке будет различаться в зависимости от роли пользователя, который редактирует карточку.

- **Почта** – уникальный адрес электронной почты пользователя, используемый при входе в систему. Следует обратить внимание, что в текущей версии Солар ПКОиР возможность изменить значение этого поля отсутствует.
- **Телефон** – номер телефона пользователя в формате +7(XXX)-XXX-XX-XX.
- **Последнее подключение** – дата и время последнего подключения текущего пользователя к системе. Поле доступно только для просмотра.
- **Описание** – в этом поле **Суперадминистратор**/**Администратор** может оставить комментарий по пользователю. Например, «Проверить действия пользователя с инцидентом ID-123».

После внесения изменений в карточку пользователя необходимо нажать кнопку **Сохранить**, чтобы сохранить настройки. Чтобы отменить внесенные изменения, следует закрыть карточку пользователя, нажав на соответствующий значок в правом верхнем углу.

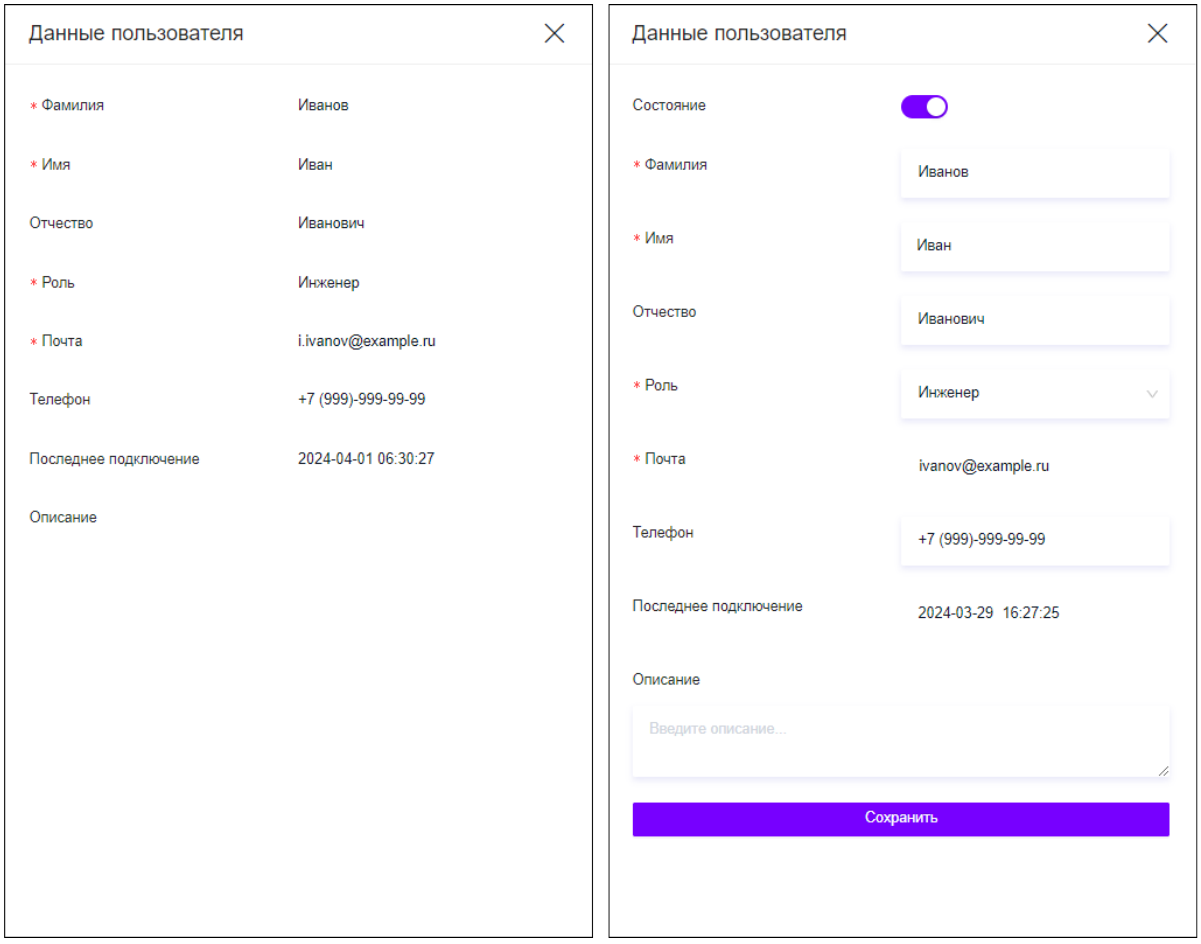


Рис. 11.3. Раздел «Настройки». Вкладка «Пользователи». Карточка пользователя: просмотр и редактирование данных

11.1.6. Управление правами доступа пользователей

Управление доступом на основе ролей – это политика избирательного управления доступом, при которой права доступа группируются с учетом специфики их применения, образуя роли. Роль представляет собой набор прав доступа, который назначается пользователю, в результате чего тот получает полномочия на выполнение конкретных действий, задан-

ных в параметрах роли. Ролевая модель позволяет реализовать гибкие правила разграничения доступа.

При установке текущей версии Солар ПКОиР создаются следующие системные роли: **Суперадминистратор**, **Администратор**, **Инженер**, **Аналитик**, **Аудитор**.

В Табл.11.1 показан набор прав доступа, предоставляемый для каждой роли по умолчанию.

Пользователь может назначаться на роль в процессе создания его учетной записи (см. раздел 11.1.3) или при редактировании его карточки (см. раздел 11.1.5).

Табл. 11.1. Ролевая модель разграничения прав доступа

	Суперадминистратор	Администратор	Инженер	Аналитик	Аудитор
Доступ к разделу **События**	+	+	+	+	+
Раздел **События**. Просмотр списка событий	+	+	+	+	+
Раздел **События**. Просмотр карточки события	+	+	+	+	+
Раздел **События**. Добавление события в инцидент	+	+	+	+	+
Раздел **События**. Создание инцидента из событий	+	+	+	+	+
Доступ к разделу **Сессии**	+	+	+	+	+
Раздел **Сессии**. Просмотр списка сессий	+	+	+	+	+
Раздел **Сессии**. Просмотр карточки сессии	+	+	+	+	+
Раздел **Сессии**. Просмотр и настройка виджетов с данными по сессиям	+	+	+	+	+
Доступ к разделу **Сеть**	+	+	+	+	+
Раздел **Сеть**. Просмотр списка хостов	+	+	+	+	+
Раздел **Сеть**. Просмотр карточки хоста	+	+	+	+	+
Раздел **Сеть**. Создание, изменение и удаление группы хостов	+	+	+	+	+
Раздел **Сеть**. Управление агентом	+	+	+	+	+
Доступ к разделу **Политики**	+	+	+	+	+

	Суперадминистратор	Администратор	Инженер	Аналитик	Аудитор
Раздел **Политики**. Просмотр списка политик	+	+	+	+	+
Раздел **Политики**. Просмотр страницы политики	+	+	+	+	+
Раздел **Политики**. Создание, изменение и удаление политики	+	+	+	+	+
Раздел **Политики**. Просмотр и настройка области применения политики	+	+	+	+	+
Раздел **Политики**. Просмотр и настройка наборов правил, включенных в политику	+	+	+	+	+
Доступ к разделу **Расследования**	+	+	+	+	+
Раздел **Расследования**. Просмотр списка инцидентов	+	+	+	+	+
Раздел **Расследования**. Просмотр карточки инцидента	+	+	+	+	+
Доступ к разделу **Правила**	+	+	+	+	+
Правила > Правила. Просмотр списка правил	+	+	+	+	+
Правила > Правила. Создание правила	+	+	+	+	+
Правила > Правила. Просмотр и изменение карточки правила	+	+	+	+	+
Правила > Правила. Создание, изменение и удаление группы правил	+	+	+	+	+
Правила > Правила. Импорт правил	+	+	+	+	+
Правила > Справочники. Просмотр списка справочников	+	+	+	+	+
Правила > Справочники. Создание справочника	+	+	+	+	+
Правила > Справочники. Просмотр и изменение карточки справочника	+	+	+	+	+
Правила > Справочники. Создание, изме-	+	+	+	+	+

	Суперадминистратор	Администратор	Инженер	Аналитик	Аудитор
нение и удаление группы справочников					
Правила > Справочники. Импорт справочников	+	+	+	+	+
Правила > Наборы. Просмотр списка наборов правил	+	+	+	+	+
Правила > Наборы. Создание набора правил	+	+	+	+	+
Правила > Наборы. Просмотр страницы набора правил	+	+	+	+	+
Правила > Наборы. Добавление нового правила в набор	+	+	+	+	+
Правила > Наборы. Изменение и удаление набора правил	+	+	+	+	+
Доступ к разделу **Настройки**	+	+	+	+	+
Настройки > Пользователи. Просмотр списка пользователей	+	+	+	+	+
Настройки > Пользователи. Просмотр карточки пользователя	+	+	+	+	+
Настройки > Пользователи. Внесение изменений в карточку пользователя	доступно редактирование карточек пользователей с ролью **Администратор**, **Инженер**, **Аналитик**, **Аудитор**	доступно редактирование карточек пользователей с ролью **Инженер**, **Аналитик**, **Аудитор**	—	—	—
Настройки > Пользователи. Добавление нового пользователя	доступно добавление пользователей с ролью **Администратор**, **Инженер**, **Аналитик**, **Аудитор**	доступно добавление пользователей с ролью **Инженер**, **Аналитик**, **Аудитор**	—	—	—
Настройки > Пользователи. Блокировка/активация пользователей	доступна блокировка/активация пользователей с ролью **Администратор**, **Инженер**, **Аналитик**, **Аудитор**	доступна блокировка/активация пользователей с ролью **Инженер**, **Аналитик**, **Аудитор**	—	—	—

11.1.7. Управление доступом к системе: блокировка/активация пользователей

Примечание

*Блокировка и активация пользователей доступна только пользователям с ролью **Суперадминистратор** и **Администратор**. Подробнее о ролевой модели см. в разделе 11.1.6.*

11.1.7.1. Блокировка пользователей

Чтобы заблокировать доступ пользователя к системе, например, при прекращении с ним трудовых отношений, необходимо выполнить следующие действия:

1. Открыть раздел **Настройки** и перейти на вкладку **Пользователи**.
2. В таблице найти требуемого пользователя и открыть его карточку.
3. Переключатель **Состояние** установить в положение **Заблокирован**.
4. В появившемся диалоговом окне подтвердить блокировку пользователя, нажав на соответствующую кнопку.

После этого состояние учетной записи пользователя изменится на **Заблокирован** и пользователь больше не сможет войти в систему.

11.1.7.2. Активация пользователей

Чтобы восстановить доступ пользователя к системе, необходимо выполнить следующие действия:

1. Открыть раздел **Настройки** и перейти на вкладку **Пользователи**.
2. В таблице найти требуемого пользователя и открыть его карточку.
3. Переключатель **Состояние** установить в положение **Активный**.
4. В появившемся диалоговом окне подтвердить активацию пользователя, нажав на соответствующую кнопку.

После этого состояние учетной записи пользователя изменится на **Активный** и пользователь сможет войти в систему под своими учетными данными.

12. Администрирование Солар ПКОиР

12.1. Solar EDR Windows

Настройка Solar EDR Windows

Настройка компонентов Solar EDR Windows выполняется в соответствии с инструкцией, приведенной в приложении **Приложение А. *Настройка конфигурации концентраторов и анализатора EDR-агента***.

Взаимодействие с антивирусным ПО

Solar EDR Windows может использоваться на хосте с установленным ПО **Kaspersky Endpoint Security for Windows** (протестировано для версии KES 12.1.0.506). Состав модулей:

- Essential protection:
  - File Threat Protection;
  - Web Threat Protection;
  - Mail Threat Protection;
  - Network Threat Protection;
  - Firewall;
  - AMSI Protection;
- Advanced protection:
  - Kaspersky Security Network;
  - Behavior Detection;
  - Exploit Prevention;
  - Host Intrusion Prevention;
  - Remediation Engine;
- Security Control:
  - Device Control;
  - Web Control;
  - Adaptive Anomaly Control.

Взаимодействие с диспетчером задач и остасткой «Сервисы»

Агент Solar EDR Windows, начиная с версии 0.3.1, не отображается в диспетчере задач и оснастке **Сервисы** ОС.

Взаимодействие с Dozor Endpoint Agent

Агент Solar EDR Windows совместим с агентом Dozor Endpoint Agent.

Агент Solar EDR Windows поддерживает:

- исключение процессов агента Dozor Endpoint Agent и его updater из инжектов Solar EDR Windows;
- исключение директорий агента Dozor Endpoint Agent и его updater из контроля файловым драйвером Solar EDR Windows;
- автоматическое добавление директорий агента Dozor Endpoint Agent и его updater в **whiteList** сенсора процессов (для событий старта/остановки процессов и событий imageLoad|Unload);
- автоматическое добавление серверов Dozor Endpoint Agent и его updater в **whiteList** сенсора сети (читаются из реестра). Будет работать **только для случая**, когда серверы заданы через IP. **При задании сервера через доменное имя исключения работать не будут**, так как на данный момент механизм resolve URL в IP отсутствует.

Не удалось исключить для Dozor Endpoint Agent: агент Dozor Endpoint Agent имеет возможность отправлять перехваченный сетевой трафик по протоколу ICAP на отдельный от основного сервера Solar Dozor ICAP-сервер. Данный параметр хранится в «защищенной» конфигурации агента Dozor Endpoint Agent и отсутствует в реестре, следовательно агент Solar EDR Windows не может его найти и использовать для **whiteList** своего сенсора сети.

Взаимодействие с агентом addVisor

Агент Solar EDR Windows совместим с агентом addVisor.

Агент Solar EDR Windows поддерживает:

- исключение процессов addVisor и его updater из инжектов Solar EDR Windows;
- исключение директорий addVisor и его updater из контроля файловым драйвером Solar EDR Windows;
- автоматическое добавление директорий addVisor и его updater в **whiteList** сенсора процессов (для событий старта/остановки процессов и событий imageLoad|Unload);
- автоматическое добавление серверов addVisor и его updater в **whiteList** сенсора сети (читаются из реестра). Будет работать **только для случая**, когда серверы заданы через IP. **При задании сервера через доменное имя исключения работать не будут**, так как сейчас нет механизма resolve URL в IP.

Настройка мониторинга командной строки PowerShell

Для мониторинга Powershell агенту Solar EDR Windows требуется активировать режим **PowerShell script block logging** ОС.

Агент активирует данный режим созданием флага в реестре самостоятельно.

```
"HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" ->
"EnableScriptBlockLogging"=1
```

В логах агента можно увидеть запись вида:

```
[2024-04-23 22:46:49.218] [Agent] [Info] [ EdrEtwSensor.exe, PID 2240, TID 8868 ] [EtwSensor.cpp:235]
 EnableScriptBlockLogging currValue = 0
[2024-04-23 22:46:49.218] [Agent] [Info] [ EdrEtwSensor.exe, PID 2240, TID 8868 ] [EtwSensor.cpp:239]
 set EnableScriptBlockLogging=1 success
```

Если в системе до запуска инстанса Powershell режим EnableScriptBlockLogging был отключен, то в уже запущенном Powershell не будет перехвата исполняемых команд.

В процессах Powershell, запущенных после установки флага "EnableScriptBlockLogging"=1, перехват команд будет. Перезапуск ОС при это не требуется.

Алгоритм выбора уникального идентификатора (key) системы

ADAM при первом соединении с сервером Солар ПКОиР (после своей установки) проходит процедуру регистрации нового Endpoint на сервере Солар ПКОиР.

С целью уникальной идентификации конкретного АРМ среди других при регистрации ADAM использует уникальный сгенерированный ComputerGUID.

ComputerGUID хранится в ключе реестра ОС.

HKLM\SOFTWARE\OrioleID\ComputerGUIDComputerGUID сохраняется в реестре ОС при удалении ADAM с АРМ, чтобы при последующих установках АРМ сохраняло уникальный ID на сервере Солар ПКОиР. Переустановка ОС Windows приведет к потере значения ComputerGUID в реестре. В этом случае потребуется провести процедуру повторной регистрации хоста на сервере Солар ПКОиР с новым ComputerGUID после установки ADAM.

12.2. Solar NTA

12.2.1. Конфигурирование Solar NTA

12.2.1.1. Конфигурирование СУБД

1. Клонировать репозиторий NTA **<path>/service builder** (<path> – заменить на путь к репозиторию) в директорию **/opt/solar/nta**.

2. Отредактировать конфигурацию сокета для подключения к СУБД PostgreSQL:

   - выполнить команду:

     nano /etc/scylla/scylla.yaml
     раскомментировать строку «listen_address: "0.0.0.0"» и указать значение IP-адреса;

   - в строке «broadcast_address:» указать адрес широковещательного канала (broadcast) той сети, к которой принадлежит интерфейс, связанный с остальными сервисами NTA;

   - в строке «rpc_address:» указать IP-адрес своего интерфейса;

   - завершить редактирование файла конфигурации, перезапустить ScyllaDb командой:

     systemctl restart scylla-server

3. Отредактировать конфигурацию сокета для подключения к СУБД ScyllaDb:

- развернуть СУБД PostgreSQL в соответствии с инструкциями производителя СУБД, опубликованными на ресурсе https://www.postgresql.org/download/linux/debian/;
- указать доступ до узла NTA-сервера путем добавления в конце файла **/etc/postgresql/13/main/pg_hba.conf** строки по шаблону:

```
host all all <IP_NTA_SERVER/mask> password
```

- в файле **/etc/postgresql/13/main/postgresql.conf** раскомментировать строку:

```
listen_addresses = '*'
```

и добавить строки:

```
statement_timeout = 180000            # in milliseconds, 0 is disabled
idle_in_transaction_session_timeout = 60000     # in milliseconds, 0 is disabled
```

- перезапустить сервер.

4. Выполнить скрипт wipeandcreate.sh в директории **/opt/solar/nta/service-builder/tools**.

12.2.1.2. Конфигурирование сервисов

В директории **/opt/solar/nta/etc** присутствуют следующие конфигурационные файлы: **scylla.json, postgresql-metadata-types.json, postgresql-metadata.json, nta-storage.json, nta-server.json, nta-broker-suricata.json**.

Конфигурирование сервисов NTA осуществляется в изолированном или аварийном режиме – через CLI с помощью команд, выдаваемых пользователем **СуперАдминистратор**:

- импорт настроек из файла на внешнем носителе;
- изменение конкретной настройки, указанной в параметрах команды (конфигурационной утилиты).

Конфигурирование сервиса nta-storage

Табл. 12.1. Описание параметров файла «nta-storage.json»

Наименование параметра	Тип данных	Описание параметра	Значение
log	object	Описывает логирование	Табл. 12.2. Описание логирования

Табл. 12.2. Описание логирования

Наименование параметра	Тип данных	Описание параметра	Значения
sink	enum	Направление вывода	Console - вывод в stdout (default) Text - запись в текстовые файлы Syslog - запись в syslog

<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значение</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значения</th></tr>
<tr><td>verbosity</td><td>enum</td><td>Уровень логирования</td><td>Trace (default), Debug, Info, Warning, Error, Critical</td></tr>
<tr><td>directory</td><td>string</td><td>Каталог с файлами логов</td><td>/var/log/solar/

nta/[service_name]

(default)</td></tr>
</table>
</td></tr>
<tr><td>capture</td><td>object</td><td>Описывает захват</td><td>
Табл. 12.3. Захват
<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значения</th></tr>
<tr><td>type</td><td>string</td><td>Вид захвата</td><td></td></tr>
<tr><td>afpacket</td><td>object</td><td>Описание параметров захвата в режиме AFPacket</td><td></td></tr>
<tr><td>deviceName</td><td>string</td><td>Имя интерфейса захвата</td><td></td></tr>
<tr><td>promiscuousMode</td><td>boolean</td><td>Включение неразборчивого режима на интерфейсе</td><td></td></tr>
<tr><td>maximumPacketSize</td><td>number</td><td>Максимальный размер пакета для захвата</td><td></td></tr>
<tr><td>blockTimeout</td><td>number</td><td>Таймаут актуальности блока</td><td></td></tr>
<tr><td>bufferSize</td><td>number</td><td>Размер буфера захвата</td><td></td></tr>
<tr><td>blockSize</td><td>number</td><td>Максимальный размер блока для захвата</td><td></td></tr>
<tr><td>useRingBuffer</td><td>boolean</td><td>Использование кольцевого буфера</td><td></td></tr>
</table>
</td></tr>
<tr><td>generator</td><td>object</td><td>Локальный генератор трафика (для тестов)</td><td>
Табл. 12.4. Локальный генератор трафика
<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значения</th></tr>
<tr><td>packetSizes</td><td>array</td><td>Массив значений размеров пакетов</td><td></td></tr>
<tr><td>packetsPerSecond</td><td>number</td><td>Количество пакетов в секунду</td><td></td></tr>
</table>
</td></tr>
</table>

Наименование параметра	Тип данных	Описание параметра	Значение
id	string	Идентификатор узла захвата (UUID)	
cpuAffinity	array	Привязка к ядрам ЦП	

Конфигурирование сервиса nta-server (опционально)

Если в разделе **pcapDirectory** файла **nta-broker-suricata.json** значение было изменено, то в конфигурации сервиса **nta-server** в строке «pcapDirectory» следует указать идентичное значение.

Для вывода лога работы **nta-server** в файл необходимо в секции **log** изменить значение параметра «sink» с «console» на «text». В таком случае лог-файлы будут расположены в **/var/log/solar**.

Конфигурация ScyllaDb не требует изменений в файле **scylla.json**. Опционально можно в поле «port» указать порт подключения к БД. По умолчанию установлен стандартный порт 9042.

Конфигурация PostgreSQL не требует изменений в файле **postgresql-metadata-types.json**. Опционально можно указать порт подключения к БД в поле «port». По умолчанию установлен стандартный порт 5432.

Конфигурация PostgreSQL не требует изменений в файле **postgresql-metadata.json**. Опционально можно в поле «port» указать порт подключения к БД. По умолчанию установлен стандартный порт 5432.

Табл. 12.5. Описание параметров файла «nta-server.json»

Наименование параметра	Тип данных	Описание параметра	Значение
broker	object	Контейнер брокера	Табл. 12.6. Контейнер брокера Наименование параметра / Тип данных / Описание параметра / Значения heartBeatInterval / number / heartBeat интервал брокера / pollingInterval / number / Интервал опроса / defaultParentId / string / Идентификатор узла захвата (UUID) /
pcapDirectory	string	Директория хранения pcap-файлов для обра-	

<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значение</th></tr>
<tr><td></td><td></td><td>ботки Suricata</td><td></td></tr>
<tr><td>log</td><td>object</td><td>Описывает логирование</td><td>Табл. 12.7. Описание логирования
<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значения</th></tr>
<tr><td>sink</td><td>enum</td><td>Направление вывода</td><td>Console - вывод в stdout (default)

Text - запись в текстовые файлы

Syslog - запись в syslog</td></tr>
<tr><td>verbosity</td><td>enum</td><td>Уровень логирования</td><td>Trace (default), Debug, Info, Warning, Error, Critical</td></tr>
<tr><td>directory</td><td>string</td><td>Каталог с файлами логов</td><td>/var/log/solar/nta/

[service_name] (default)</td></tr>
</table></td></tr>
<tr><td>storage</td><td>object</td><td>Контейнер описания хранилища</td><td>Табл. 12.8. Контейнер описания хранилища
<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значения</th></tr>
<tr><td>type</td><td>string</td><td>Тип БД</td><td></td></tr>
<tr><td>maximumParallelRequests</td><td>number</td><td>Максимальное количество параллельных запросов</td><td></td></tr>
<tr><td>maximumRecordsInResult</td><td>number</td><td>Максимальное количество записей в файле</td><td></td></tr>
<tr><td>bucketCount</td><td>number</td><td>Количество баккетов</td><td></td></tr>
<tr><td>scylla</td><td>object</td><td>Описание БД Scylla</td><td></td></tr>
<tr><td>$ref</td><td>string</td><td>Ссылка на конфигурацию БД</td><td></td></tr>
</table></td></tr>
<tr><td>metadataDatabase</td><td>object</td><td>Описание БД metadata

Database</td><td>Табл. 12.9. Описание БД metadataDatabase
<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значения</th></tr>
<tr><td>type</td><td>string</td><td>Тип БД</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значение</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значения</th></tr>
<tr><td>postgresql</td><td>object</td><td>Описание в соответствии с типом СУБД</td><td></td></tr>
<tr><td>$ref</td><td>string</td><td>Ссылка на конфигурационный файл</td><td></td></tr>
</table>
</td></tr>
<tr><td>metadataTypesDatabase</td><td>object</td><td>Описание конфигурации для хранения типов метаданных</td><td>
Табл. 12.10. Описание конфигурации для хранения типов метаданных
<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значения</th></tr>
<tr><td>type</td><td>string</td><td>Тип БД</td><td></td></tr>
<tr><td>postgresql</td><td>object</td><td>Описание в соответствии с типом СУБД</td><td></td></tr>
<tr><td>$ref</td><td>string</td><td>Ссылка на конфигурационный файл</td><td></td></tr>
</table>
</td></tr>
<tr><td>websocket</td><td>object</td><td>Описание подключения по websocket</td><td>
Табл. 12.11. Описание подключения по websocket
<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значения</th></tr>
<tr><td>address</td><td>string</td><td>Адрес слушающего интерфейса</td><td></td></tr>
<tr><td>port</td><td>number</td><td>Номер слушающего порта</td><td></td></tr>
<tr><td>backlog</td><td>number</td><td>-</td><td></td></tr>
<tr><td>connection</td><td>object</td><td>Параметры подключения к websocket</td><td></td></tr>
<tr><td>socket</td><td>object</td><td>Контейнер сокета</td><td></td></tr>
<tr><td>noDelay</td><td>boolean</td><td>-</td><td></td></tr>
<tr><td>noPush</td><td>boolean</td><td>-</td><td></td></tr>
<tr><td>receiveBufferSize</td><td>number</td><td>Буфер приема</td><td></td></tr>
<tr><td>sendBufferSize</td><td>number</td><td>Буфер отправки</td><td></td></tr>
<tr><td>userAgent</td><td>string</td><td>Строка userAgent</td><td></td></tr>
<tr><td>origin</td><td>string</td><td>-</td><td></td></tr>
<tr><td>subProtocol</td><td>string</td><td>Используемый протокол</td><td></td></tr>
</table>
</td></tr>
</table>

Наименование параметра	Тип данных	Описание параметра	Значение
			Наименование параметра / Тип данных / Описание параметра / Значения masking / boolean / - maximumHttpHeaderSize / number / Максимальная длина заголовка HTTP maximumFrameSize / number / Максимальная длина фрейма pingInterval / number / Интервал проверочного пинга

Табл. 12.12. Описание параметров файла «scylla.json»

Наименование параметра	Тип данных	Описание параметра
broker	object	Контейнер брокера
hosts	string	Имя узла с БД Scylla или IP адрес
database	string	Имя базы данных
port	number	Номер порта подключения к БД
protocolVersion	number	Версия протокола подключения
readConsistency	string	Уровень консистентности (параметр БД0)
writeConsistency	string	Уровень консистентности (параметр БД0)

Табл. 12.13. Описание параметров файла «nta-broker-suricata.json»

Наименование параметра	Тип данных	Описание параметра	Значение
pcapDirectory	string	Директория, из которой будут получены файлы для анализа	
log	object	Описывает логирования	Табл. 12.14. Описание логирования Наименование параметра / Тип данных / Описание параметра / Значения sink / enum / Направление вывода / Console - вывод в stdout (default) Text - запись в текстовые файлы Syslog - запись в syslog

<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значение</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значения</th></tr>
<tr><td>verbosity</td><td>enum</td><td>Уровень логирования</td><td>Trace (default), Debug, Info, Warning, Error, Critical</td></tr>
<tr><td>directory</td><td>string</td><td>Каталог с файлами логов</td><td>/var/log/solar/nta/

[service_name] (default)</td></tr>
</table>
</td></tr>
<tr><td>connection</td><td>object</td><td>Параметры подключения к websocket</td><td>
Табл. 12.15. Параметры подключения к websocket
<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значения</th></tr>
<tr><td>url</td><td>string</td><td>Адрес подключения</td><td></td></tr>
<tr><td>reconnectInterval</td><td>number</td><td>Интервал времени, через которой производится переподключение</td><td></td></tr>
<tr><td>connectTimeout</td><td>number</td><td>Интервал времени, через который производится закрытие соединения по таймауту</td><td></td></tr>
<tr><td>closeTimeout</td><td>number</td><td>Закрытие соединения после таймаута</td><td></td></tr>
<tr><td>socket</td><td>object</td><td>Контейнер описания параметров подключения к серверу по websocket</td><td></td></tr>
<tr><td>noDelay</td><td>boolean</td><td>-</td><td></td></tr>
<tr><td>noPush</td><td>boolean</td><td>-</td><td></td></tr>
<tr><td>receiveBufferSize</td><td>number</td><td>Буфер приема</td><td></td></tr>
<tr><td>sendBufferSize</td><td>number</td><td>Буфер отправки</td><td></td></tr>
<tr><td>userAgent</td><td>string</td><td>Параметр протокола соединения</td><td></td></tr>
<tr><td>origin</td><td>string</td><td>-</td><td></td></tr>
<tr><td>subProtocol</td><td>string</td><td>Используемый sub протокол</td><td></td></tr>
<tr><td>masking</td><td>boolean</td><td>-</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значение</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значения</th></tr>
<tr><td>maximumHttpHeaderSize</td><td>number</td><td>Максимальный размер HTTP заголовка</td><td></td></tr>
<tr><td>maximumFrameSize</td><td>number</td><td>Максимальный размер фрейма</td><td></td></tr>
<tr><td>pingInterval</td><td>number</td><td>Интервал keepalive</td><td></td></tr>
</table>
</td></tr>
<tr><td>suricata</td><td>object</td><td>Контейнер описания параметров работы Suricata</td><td>
Табл. 12.16. Контейнер описания параметров работы Suricata
<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значения</th></tr>
<tr><td>bin-path</td><td>string</td><td>Путь к бинарному файлу сурикаты</td><td></td></tr>
<tr><td>socket-path</td><td>string</td><td>Путь к сокету сурикаты</td><td></td></tr>
<tr><td>output-dir</td><td>string</td><td>Путь к директории где сурикаата выкладывает результат работы</td><td></td></tr>
<tr><td>connection-timeout</td><td>number</td><td>Таймаут соединения после которого соединение считается утерянным</td><td></td></tr>
<tr><td>connection-try-period</td><td>number</td><td>Период попытки повторного восстановления соединения</td><td></td></tr>
<tr><td>check-version</td><td>string</td><td>Указатель версии сурикаты</td><td></td></tr>
<tr><td>packet-batch-size</td><td>number</td><td>Количество пакетов в ожидаемом файле для сурикаты</td><td></td></tr>
<tr><td>do-not-remove-processed</td><td>boolean</td><td>Отладочная опция: не удалять файлы после обработки сурикатой</td><td></td></tr>
<tr><td>backup-eve</td><td>boolean</td><td>Резервировать suricata eve.json, копировать с расширением .bak</td><td></td></tr>
</table>
</td></tr>
</table>

Табл. 12.17. Описание параметров файла «postgresql-metadata.json»

Наименование параметра	Тип данных	Описание параметра
hosts	array	Хост подключения
port	number	Порт подключения
databaseName	string	Имя базы данных
authenticationMethod	string	Тип аутентификации
userName	string	Пользователь БД
password	string	Пароль пользователя для подключения к БД
connectionsPerHost	number	Количество соединений на 1 узел
maximumDelayedRequests	number	Максимальная задержка запросов
autoReconnect	boolean	Включение опции переподключения
checkQueryParameters	boolean	-
sharding	object	-
type	string	Вид шардинга

Табл. 12.18. Описание параметров файла «solar-nta-outer-api.json»

Наименование параметра	Тип данных	Описание параметра	Значение
listener	object	Директория, из которой будут получены файлы для анализа	
log	object	Описывает логирования	Табл. 12.19. Описание логирования Наименование параметра / Тип данных / Описание параметра / Значения protocolVersion websocket address port backlog connection socket noDelay noPush receiveBufferSize sendBufferSize
server	object		Табл. 12.20. Описание server Наименование параметра / Тип данных / Описание параметра / Значения peerId

<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значение</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значения</th></tr>
<tr><td>websocket</td><td></td><td></td><td></td></tr>
<tr><td>url</td><td></td><td></td><td></td></tr>
<tr><td>reconnectInterval</td><td></td><td></td><td></td></tr>
<tr><td>connectTimeout</td><td></td><td></td><td></td></tr>
<tr><td>closeTimeout</td><td></td><td></td><td></td></tr>
<tr><td>socket</td><td></td><td></td><td></td></tr>
<tr><td>noDelay</td><td></td><td></td><td></td></tr>
<tr><td>noPush</td><td></td><td></td><td></td></tr>
<tr><td>receiveBufferSize</td><td></td><td></td><td></td></tr>
<tr><td>sendBufferSize</td><td></td><td></td><td></td></tr>
<tr><td>userAgent</td><td></td><td></td><td></td></tr>
<tr><td>origin</td><td></td><td></td><td></td></tr>
<tr><td>subProtocol</td><td></td><td></td><td></td></tr>
<tr><td>masking</td><td></td><td></td><td></td></tr>
<tr><td>maximumHttpHeaderSize</td><td></td><td></td><td></td></tr>
<tr><td>maximumFrameSize</td><td></td><td></td><td></td></tr>
<tr><td>pingInterval</td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>httpAccess</td><td>object</td><td></td><td>Табл. 12.21. Описание httpAccess
<table>
<tr><th>Наименование параметра</th><th>Тип данных</th><th>Описание параметра</th><th>Значения</th></tr>
<tr><td>address</td><td></td><td></td><td></td></tr>
<tr><td>port</td><td></td><td></td><td></td></tr>
<tr><td>fileStoragePath</td><td></td><td></td><td></td></tr>
</table>
</td></tr>
</table>

12.2.1.3. Межсетевое взаимодействие

Обязательным пунктом настройки внешнего API является ограничение доступа к порту списком разрешенных IP адресов. Данную настройку можно выполнить как с помощью встроенных в систему утилит (iptables/nftables), так и с помощью firewall на границе сети.

Табл. 12.22. Список защищаемых портов

Сервис	Порт	Описание	Рекомендации
Outer API	tcp/1443	Доступен, взаимодействие между общим ПО Солар ПКОиР и NTA	Закрыть, доступ только с доверенных IP адресов
Outer API	tcp/21977	Доступен, взаимодействие между общим ПО Солар ПКОиР и NTA	Закрыть, доступ только с доверенных IP адресов
Outer API (websocket)	tcp/24138	Доступен только на localhost, взаимодействие между сервисами	
Broker (websocket)	tcp/24138	Доступен только на localhost, взаимодействие между сервисами	

12.2.1.4. Конфигурирование ОС

В файл **/etc/hosts** необходимо добавить записи для наименований «postgres1» и «scylla1» с указанием IP адреса:

- <IP адрес_сервера_ScyllaDB> scylla1;
- <IP адрес_сервера_postgresql> postgres1.

13. Мониторинг системы

13.1. Мониторинг Solar NTA

13.1.1. Интеграция с Zabbix

Объем трафика на интерфейсах съёма трафика

Реализация с помощью шаблона **Linux_NTA_Prometheus.yaml**.

Список системных метрик:

- net.if.in["{#IFNAME}"] – количество полученных бит;
- net.if.out["{#IFNAME}"] – количество отправленных бит;
- net.if.in["{#IFNAME}",dropped] – количество отброшенных пакетов на входе;
- net.if.in["{#IFNAME}",errors] – количество ошибок на входе;
- vfs.file.contents["/sys/class/net/{#IFNAME}/operstate"] – состояние интерфейса (up/down/etc);
- net.if.out["{#IFNAME}",dropped] – количество отброшенных пакетов на выходе;
- net.if.out["{#IFNAME}",errors] – количество ошибок на выходе.

Список метрик микросервисов NTA:

```
NTA.Broker.metrics.keyGetPacketPPS
NTA.Broker.metrics.keyGetPacketTotalPPS
NTA.Broker.metrics.keySentPacketsToSuricataTotalPPS
NTA.Broker.metrics.keySentToServerPPS
NTA.Broker.metrics.keySentToServerTotalPPS
NTA.Broker.metrics.NumberLostPacketsToSuricata
NTA.Broker.metrics.NumberPackagesSentToSuricataTotal
NTA.Broker.metrics.NumberPacketsReceivedFromServerTotal
NTA.Broker.metrics.NumberPacketsReceivedFromSuricata
NTA.Broker.metrics.NumberPacketsSentToServerTotal
NTA.Server.metrics.GetRawPacketsTotal
NTA.Server.metrics.SaveMetadataTotal
NTA.Storage.metrics.current_received_count
NTA.Storage.metrics.current_received_size
NTA.Storage.metrics.current_writed_count
NTA.Storage.metrics.current_writed_size
NTA.Storage.metrics.keyCurrentDroppedCount
NTA.Storage.metrics.keyCurrentReadBPS
NTA.Storage.metrics.keyCurrentWriteBPS
NTA.Storage.metrics.keyCurrentWritePPS
NTA.Storage.metrics.keyGetPacketPPS
NTA.Storage.metrics.keyTotalDroppedCount
NTA.Storage.metrics.keyTotalDroppedSize
NTA.Storage.metrics.keyTotalReadPPS
NTA.Storage.metrics.keyTotalWriteBPS
NTA.Storage.metrics.keyTotalWritePPS
NTA.Storage.metrics.total_received_count
NTA.Storage.metrics.total_received_size
```

```
NTA.Storage.metrics.total_writed_count
NTA.Storage.metrics.total_writed_size
```

Состояние модулей NTA

Минимальная реализация выполнена с помощью внедрения метрик Zabbix Agent (UserParameter).

Пример реализации:

1. Создать файл **template_nta_services.conf** в директории Zabbix Agent **/etc/zabbix/zabbix_agentd.d**.
2. Создать в файле метрики:

```
UserParameter=nta.services.server[*], ps -ef | grep solar_nta_server | grep -iv "grep" | wc -l

UserParameter=nta.services.broker[*], ps -ef | grep solar_nta_broker | grep -iv "grep" | wc -l

UserParameter=nta.services.storage[*], ps -ef | grep solar_nta_storage | grep -iv "grep" | wc -l

UserParameter=nta.services.aggregator[*], ps -ef | grep solar_nta_aggregator | grep -iv "grep" | wc
-l

UserParameter=nta.services.outerapi[*], ps -ef | grep solar_nta_outer_api_interface | grep -iv "grep"
 | wc -l

UserParameter=nta.services.suricata[*], ps -ef | grep suricata| grep -iv "grep" | wc -l
```

3. Перезагрузить zabbix agent командой:
   systemctl restart zabbix-agent.service
4. Применить шаблон Zabbix **Linux_NTA_Prometheus.yaml**. В шаблоне присутствуют метрики и триггеры с алертами:

Name ▲	Triggers	Key
HTTP agent NTA Broker metrics		nta.services.broker.metrics
HTTP agent NTA Server metrics		nta.services.server.metrics
HTTP agent NTA Storage metrics		nta.services.storage.metrics
HTTP agent NTA Broker metrics: NTA.Broker.metrics.keyGetPacketPPS		nta.services.broker.metrics.keyGetPacketPPS
HTTP agent NTA Broker metrics: NTA.Broker.metrics.keyGetPacketTotalPPS		nta.services.broker.metrics.keyGetPacketTotalPPS
HTTP agent NTA Broker metrics: NTA.Broker.metrics.keySentPacketsToSuricataTotalPPS		nta.services.broker.metrics.keySentPacketsToSuricataTotalPPS
HTTP agent NTA Broker metrics: NTA.Broker.metrics.keySentToServerPPS		nta.services.broker.metrics.keySentToServerPPS
HTTP agent NTA Broker metrics: NTA.Broker.metrics.keySentToServerTotalPPS		nta.services.broker.metrics.keySentToServerTotalPPS
HTTP agent NTA Broker metrics: NTA.Broker.metrics.NumberLostPacketsToSuricata		nta.services.broker.metrics.NumberLostPacketsToSuricata
HTTP agent NTA Broker metrics: NTA.Broker.metrics.NumberPackagesSentToSuricataTotal		nta.services.broker.metrics.NumberPackagesSentToSuricataTotal
HTTP agent NTA Broker metrics: NTA.Broker.metrics.NumberPacketsReceivedFromServerTotal		nta.services.broker.metrics.NumberPacketsReceivedFromServerTotal
HTTP agent NTA Broker metrics: NTA.Broker.metrics.NumberPacketsReceivedFromSuricata		nta.services.broker.metrics.NumberPacketsReceivedFromSuricata
HTTP agent NTA Broker metrics: NTA.Broker.metrics.NumberPacketsSentToServerTotal		nta.services.broker.metrics.NumberPacketsSentToServerTotal
HTTP agent NTA Server metrics: NTA.Server.metrics.GetRawPacketsTotal		nta.services.server.metrics.GetRawPacketsTotal
HTTP agent NTA Server metrics: NTA.Server.metrics.SaveMetadataTotal		nta.services.server.metrics.SaveMetadataTotal
HTTP agent NTA Storage metrics: NTA.Storage.metrics.current_received_count		nta.services.storage.metrics.current_received_count
HTTP agent NTA Storage metrics: NTA.Storage.metrics.current_received_size		nta.services.storage.metrics.current_received_size
HTTP agent NTA Storage metrics: NTA.Storage.metrics.current_writed_count		nta.services.storage.metrics.current_writed_count
HTTP agent NTA Storage metrics: NTA.Storage.metrics.current_writed_size		nta.services.storage.metrics.current_writed_size
HTTP agent NTA Storage metrics: NTA.Storage.metrics.keyCurrentDroppedCount		nta.services.storage.metrics.keyCurrentDroppedCount
HTTP agent NTA Storage metrics: NTA.Storage.metrics.keyCurrentReadBPS		nta.services.storage.metrics.keyCurrentReadBPS
HTTP agent NTA Storage metrics: NTA.Storage.metrics.keyCurrentWriteBPS		nta.services.storage.metrics.keyCurrentWriteBPS
HTTP agent NTA Storage metrics: NTA.Storage.metrics.keyCurrentWritePPS		nta.services.storage.metrics.keyCurrentWritePPS
HTTP agent NTA Storage metrics: NTA.Storage.metrics.keyGetPacketPPS		nta.services.storage.metrics.keyCurrentReadPPS
HTTP agent NTA Storage metrics: NTA.Storage.metrics.keyTotalDroppedCount		nta.services.storage.metrics.keyTotalDroppedCount
HTTP agent NTA Storage metrics: NTA.Storage.metrics.keyTotalDroppedSize		nta.services.storage.metrics.keyTotalDroppedSize
HTTP agent NTA Storage metrics: NTA.Storage.metrics.keyTotalReadPPS		nta.services.storage.metrics.keyTotalReadPPS
HTTP agent NTA Storage metrics: NTA.Storage.metrics.keyTotalWriteBPS		nta.services.storage.metrics.keyTotalWriteBPS
HTTP agent NTA Storage metrics: NTA.Storage.metrics.keyTotalWritePPS		nta.services.storage.metrics.keyTotalWritePPS
HTTP agent NTA Storage metrics: NTA.Storage.metrics.total_received_count		nta.services.storage.metrics.total_received_count
HTTP agent NTA Storage metrics: NTA.Storage.metrics.total_received_size		nta.services.storage.metrics.total_received_size
HTTP agent NTA Storage metrics: NTA.Storage.metrics.total_writed_count		nta.services.storage.metrics.total_writed_count
HTTP agent NTA Storage metrics: NTA.Storage.metrics.total_writed_size		nta.services.storage.metrics.total_writed_size
NTA services - API status	Triggers 1	nta.services.outerapi
NTA services - broker status	Triggers 1	nta.services.broker
NTA services - server status	Triggers 1	nta.services.server
NTA services - storage status	Triggers 1	nta.services.storage

Рис. 13.1. Шаблон Zabbix Linux_NTA.yaml

5. При отсутствии какого-либо сервиса срабатывает триггер и в столбце **Problem • Severity**. На иллюстрации ниже показан вывод предупреждений при отсутствии всех сервисов.

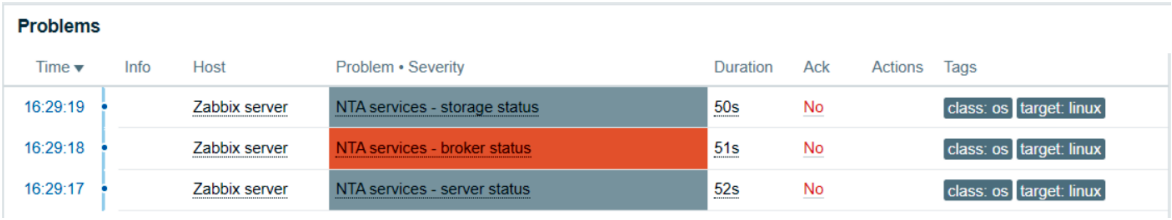


Рис. 13.2. Срабатывание предупреждений

Очередь записи на диск, IOPS, свободное место

1. Склонировать репозиторий.
2. Выполнить команду:
   cd /tmp
3. Выполнить команду (<path> – заменить на путь к репозиторию):
   git clone <path>/metrics.git
4. Для создания рабочей директории выполнить команду:
   mkdir -p /opt/solar/nta/etc/zabbix
5. Переместить скрипты из **/tmp/iostat/scripts** в **/opt/solar/nta/etc/zabbix**.
6. Создать crontab задание:
   crontab -e
   # Zabbix monitoring iostat
   59 23 * * * root /opt/solar/nta/etc/zabbix/scripts/iostat-collect.sh > /dev/null 2>&1
7. Создать файл **template_iostat.conf** в директории Zabbix Agent **/etc/zabbix/zabbix_agentd.d**
8. Создать в файле метрики:

```
# Disk statistics iostat
UserParameter=iostat.discovery, iostat -d | awk 'BEGIN {check=0;count=1;array[0]="total";}
{if(check==1 && $1 != ""){array[count]=$1;count=count+1;}if($1=="Device:"){check=1;}} END
{printf("{\n\t\"data\":[\n");for(i=0;i<count;++i){printf("\t\t{\n\t\t\t\"{#HARDDISK}\":\"%s\"}", array[i]);
  if(i+1<count){printf(",\n");}} printf("]}\n");}'
UserParameter=iostat.metric[*],/opt/solar/nta/etc/zabbix/scripts/iostat-parse.sh /tmp/iostat-collect.tmp
 $1 $2
```

9. Перезагрузить zabbix agent:
   systemctl restart zabbix-agent.service
10. Загрузить в Zabbix Server шаблон **Template_OS_Linux_IOSTAT.xml** и назначить его на хост, который требуется контролировать.

Host	Name ▲	Last check	Last value
Zabbix server	Disk total average queue size	44s	48.2 req
Zabbix server	Disk total average requests size	43s	5.65 sector/request
Zabbix server	Disk total await	42s	2.6 ms
Zabbix server	Disk total read await	38s	4.96 ms
Zabbix server	Disk total read from device per second	40s	0
Zabbix server	Disk total read operations per second	41s	0 ops
Zabbix server	Disk total read requests merge per second	39s	0 rps
Zabbix server	Disk total utilization	37s	0 %
Zabbix server	Disk total write await	33s	0.24 ms
Zabbix server	Disk total write operations per second	36s	0 ops
Zabbix server	Disk total write requests merge per second	34s	0 rps
Zabbix server	Disk total written to the device per second	35s	0 kB/s

Рис. 13.3. Результат работы Zabbix

Утилизация памяти/RAM и CPU

Утилизация памяти/RAM и CPU выполняется с помощью шаблона Zabbix **Linux_NTA_Prometheus.yaml**.

13.2. Мониторинг состояния Солар ПКОиР

13.2.1. Логирование Солар ПКОиР

Солар ПКОиР выполняет логирование событий безопасности, регистрируемых в системе. События безопасности представляют собой зафиксированное в обрабатываемом виде состояние информационной (автоматизированной) системы, сетевого, телекоммуникационного, коммуникационного, иного прикладного сервиса или информационно-телекоммуникационной сети, указывающее на возможное нарушение целостности, доступности и (или) конфиденциальности информации, а также на сбой в работе средства защиты/обработки информации или иную ситуацию, которая может быть значимой для безопасности информации.

Список событий

Системные события:

1. Запуск, остановка сервиса.
2. Установка, обновление сервиса.

События безопасности:

1. Создание, редактирование, блокировка/разблокировка пользователей.
2. Вход, выход пользователя.
3. Создание, редактирование правил.
4. Создание, редактирование политик.

Типы событий

Наименование	Группа	EventType(16)	EventType(10)	Критичность	Источник	Комментарий
Создание пользователя	Аудит	0x3A00E	237582	низкий	Сервер Солар ПКОиР	
Редактирование пользователя	Аудит	0x3A00B	237579	низкий	Сервер Солар ПКОиР	Включая изменение роли, но не включая изменение прав на уровне ролей
Блокировка пользователя	Аудит	0x3A00A	237578	средний	Сервер Солар ПКОиР	
Разблокировка пользователя	Аудит	0x3A00E	237582	низкий	Сервер Солар ПКОиР	
Вход пользователя	Аудит	0x3A00B	237579	низкий	Сервер Солар ПКОиР	Привязка сервису авторизации
Выход пользователя	Аудит	0x3A011	237585	низкий	Сервер Солар ПКОиР	
Запуск сервиса	Аудит	0x3A00A	237578	низкий	Сервер Солар ПКОиР	
Остановка сервиса	Аудит	0x3A00E	237582	низкий	Сервер Солар ПКОиР	
Установка сервиса	Аудит	0x3A00B	237579	низкий	Сервер Солар ПКОиР	
Обновление сервиса	Аудит	0x3A013	237587	низкий	Сервер Солар ПКОиР	
Создание правила	Аудит	0x3A00A	237578	низкий	Сервер Солар ПКОиР	
Редактирование правила	Аудит	0x3A00E	237582	низкий	Сервер Солар ПКОиР	
Деактивация правила	Аудит	0x3A00B	237579	низкий	Сервер Солар ПКОиР	
Создание политики	Аудит	0x3A013	237587	низкий	Сервер Солар ПКОиР	

Наименование	Группа	EventType(16)	EventType(10)	Критичность	Источник	Комментарий
Редактирование политики	Аудит	0x3A00A	237578	средний	Сервер Солар ПКОиР	
Применение политики	Аудит	0x3A00E	237582	средний	Сервер Солар ПКОиР	

Состав атрибутов события

Атрибут сервера Солар ПКОиР	Атрибут NTA	Атрибут EDR	Получение	Пример	Описание
ClientID	ClientID	ClientID	Агент	f16166e1-efed-4ff2-8956-04f05e7a3019	Идентификатор хоста - источника события. Генерируется в соответствии с контрактом передачи данных back-end продукта.
ComponentID	EventSource	ComponetID	Агент	EDRL 0.3	ID компонента в системе + версия
Subject	SubjectID	ComponentUserName	Агент	User	Имя внутреннего пользователя, выполнивший действие (если возможно определить. Иначе: system)
EventTime	EventTime	EventTime	Агент	2023-08-25T14:08:57.265Z	Дата-время возникновения события
EventID	EventID	EventID	Агент	016b1f5b-3640-63ec-93ee-2313a06abf22	Уникальный ID события
EventType	EventTypeID	EventType	Агент	131072	Код типа события
EventResult	EventResultDesc	Result	Агент	Успешно	Результат операции, вызвавшей гене-

Атрибут сервера Солар ПКОиР	Атрибут NTA	Атрибут EDR	Получение	Пример	Описание
					рацию события
EventDescription	EventTypeDesc	Description	Агент	Конфигурация v 0.9 загружена	Описание события
EventSeverity	EventSeverityDesc	-	Агент	Критический	Описание серьёзности события

Пример записи:

{"clientId":"http://10.101.31.7:36939/","componentId":"xdr-business-rules-service 0.0.5-SNAPSHOT",
"createdAt":[2024,6,25,16,39,16,497484032],"severity":"MEDIUM","type":"POLICY_EDITED","success":true,
"userIdentity":"test@rt-solar.ru","attributeMap":{}}

13.2.2. Просмотр журнальных файлов

14. Сопровождение Солар ПКОиР

14.1. Сопровождение Базы решающих правил

14.1.1. Экспорт политик решающих правил

Для экспорта политик решающих правил необходимо выполнить следующее:

1. Получить идентификатор политики EDR Windows. Его можно получить командой в Swagger или запросом из БД.

   В Swagger выполнить команду:
   POST /api/v1/policies

   Или в БД сервиса БРП (по умолчанию **xdr_business_rules**) выполнить запрос:

   select id from rule_policies where name = 'Политика EDR Windows'

2. В Swagger (по умолчанию порт 36939) выполнить команду, используя полученное значение id вместо параметра {id}:
   GET /api/v1/policies/{id}/export

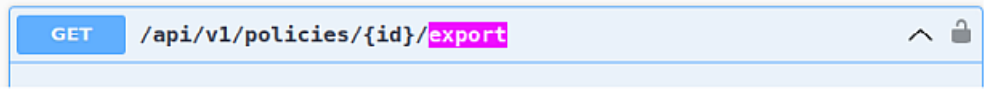


Рис. 14.1. Выполнение команды в Swagger

3. Выполнить проверочный запрос в БД xdr_artifacts (принадлежит software update center), вставив корректную дату, после которой должны были появиться новые артефакты **lua_analyzer** и **lua_analyzer_linux**:

   select * from artifact where created_at > '2024-05-15';

При возникновении ошибки в ходе экспорта политики, содержащей правило, для которого неправильно вычислен id справочника, то в таблице policy_to_group в столбцу error_body появится запись вида:

```
{
 "result": {
  "status": "ERROR",
  "ruleID": "e45ba030-eb50-4467-b38c-4e63ccdc2ebc",
  "conditionID": "a1f2ae3b-1664-4909-9690-5110bb154b00",
  "dictionaryID": "c2893f39-38ea-401c-a732-436f3fd80e3a",
  "description": "Dictionary not found!"
 },
 "windows": null,
 "linux": null
}
```

dictionaryId – это id справочника, по которому выполнялся поиск значения.

Начиная с версии 0.4 и добавления IoC, один справочник может содержать несколько списков значений и body правила будет выглядеть так:

```
eventType = WmiExecMethod && (User includes \"Справочник номер 1.пользователи\") REACTION
 filter
```

Чтобы определить список значений однозначно, используется id из таблицы dictionary и id из таблицы dictionary_values. В случае ошибки в dictionaryID будет 2 uuid, например:

```
{
 "result": {
  "status": "ERROR",
  "ruleID": "e45ba030-eb50-4467-b38c-4e63ccdc2ebc",
  "conditionID": "a1f2ae3b-1664-4909-9690-5110bb154b00",
  "dictionaryID": "c2893f39-38ea-401c-a732-436f3fd80e3a - beca4260-9dfd-46ba-91d7-6e8c80419ccd",

  "description": "Dictionary not found!"
 },
 "windows": null,
 "linux": null
}
```

c2893f39-38ea-401c-a732-436f3fd80e3a – это id из таблицы dictionary.

beca4260-9dfd-46ba-91d7-6e8c80419ccd – это id из таблицы dictionary_values.

По этим двум id можно определить, какое значение было применено.

Приложение А. Настройка конфигурации концентраторов и анализатора EDR-агента

В этом разделе приведено описание настройки Solar EDR, в состав которого входят следующие компоненты: анализатор, концентраторы и сенсоры.

Для централизованного хранения путей, указываемых в конфигурационных файлах, используются переменные, значения которых указываются в переменных ОС. Названия переменных обрамляются знаком **%**, например: **%WINDIR%**.

Внимание!

Итоговые пути не сворачиваются в переменные окружения

А.1. Настройка конфигурации анализатора EDR

Анализатор EDR – компонент, который отвечает за обработку данных с концентраторов по заданным правилам (БРП) и их отправку в сетевую часть при срабатывании правила.

Правила представляют собой набор LUA-скриптов, обрабатывающих поток событий с концентраторов. Данные с концентратора – это событие, которое передается в виде текстовой строки, содержащей внутри JSON.

Обновление файла **Analyzer.lua** возможно только путем загрузки конфигураций через сервер Солар ПКОиР или при изменении БРП.

По умолчанию анализатор в соответствии с файлом **Analyzer.lua** получает события со всех концентраторов и отправляет их в сетевую часть.

Анализатор выполняет следующие задачи:

- фильтрация событий по заданным правилам (функция **negative** в **Analyzer.lua**);
- генерация инцидентов (функция **positive** в **Analyzer.lua**).

А.2. Настройка конфигурации концентраторов EDR

Концентратор EDR – компонент Solar EDR, обеспечивающий сбор и предварительную обработку событий с сенсоров по выделенной предметной области.

В поставке конфигурация каждого концентратора настроена на получение определенных событий. Также правила концентраторов настроены по умолчанию.

Внимание!

Изменение конфигурации подписки требует перезапуска концентратора, использующего данный конфигурационный файл.

Пример конфигурационного файла **config_for_XDR.json**:

```
{
 "configs": [
  {
   "config-file": {
    "eventsConfigs": [
     {
      "blackList": [
       "^\\s*echo\\s*$"
      ],
      "eventType": 40960,
      "whiteList": [
       "^\\s*test\\s*$",
       "^\\s*dir\\s*$"
      ]
     }
    ]
   },
   "config-type": "EventsConfigFromCmdSensorToOsCon"
  },
  {
   "config-file": {
    "eventsConfigs": [
     {
      "blackList": [],
      "eventType": 4100,
      "whiteList": []
     },
     {
      "blackList": [],
      "eventType": 16384,
      "whiteList": []
     },
     {
      "blackList": [],
      "eventType": 16385,
      "whiteList": []
     },
     {
      "blackList": [],
      "eventType": 16386,
      "whiteList": []
     },
     {
      "blackList": [],
      "eventType": 16387,
      "whiteList": []
     },
     {
      "blackList": [
       "^\\s*echo\\s*$"
      ],
      "eventType": 40960,
      "whiteList": [
       "^\\s*clear\\s*$",
       "^\\s*cls\\s*$"
      ]
     }
    ]
```

```
    },
    "config-type": "EventsConfigFromEtwSensorToOsCon"
  },
  {
    "config-file": {
      "eventsConfigs": [
        {
          "blackList": [],
          "whiteList": [
            "%WINDIR%\\*",
            "%PROGRAMFILES%\\*",
            "%PROGRAMFILES(X86)%\\*"
          ]
        },
        {
          "blackList": [],
          "eventType": 4099,
          "whiteList": []
        }
      ]
    },
    "config-type": "EventsConfigFromEtwSensorToProcCon"
  },
  {
    "config-file": {
      "eventsConfigs": [
        {
          "blackList": [],
          "whiteList": []
        },
        {
          "blackList": [],
          "eventType": 32768,
          "whiteList": []
        },
        {
          "blackList": [],
          "eventType": 32769,
          "whiteList": []
        }
      ],
      "sensorConfig": {
        "winEventLogConfig": {
          "clearSubscriptions": [
            "System",
            "Security",
            "Microsoft-Windows-PowerShell/Operational"
          ],
          "subscriptions": [
            {
              "filter": "Event/System[EventID=40962]",
              "source": "Microsoft-Windows-PowerShell/Operational"
            },
            {
              "filter": "*[System[(Level=2)]]",
              "source": "Security"
            }
          ]
```

```
      }
    }
  },
  "config-type": "EventsConfigFromEvtLogSensorToOsCon"
},
{
  "config-file": {
    "eventsConfigs": [
      {
        "blackList": [],
        "whiteList": [
          "%SYSTEMDRIVE%\\*",
          "%LOCALAPPDATA%\\*",
          "%APPDATA%\\*",
          "%ALLUSERSPROFILE%\\*",
          "%PROGRAMFILES%\\*",
          "%PROGRAMFILES(X86)%\\*",
          "%WINDIR%\\*",
          "\\Device\\NamedPipe*",
          "\\Device\\Mailslot*"
        ]
      },
      {
        "blackList": [],
        "eventType": 20480,
        "whiteList": []
      },
      {
        "blackList": [],
        "eventType": 20481,
        "whiteList": []
      },
      {
        "blackList": [],
        "eventType": 20482,
        "whiteList": []
      },
      {
        "blackList": [],
        "eventType": 20483,
        "whiteList": []
      },
      {
        "blackList": [],
        "eventType": 20484,
        "whiteList": []
      },
      {
        "blackList": [],
        "eventType": 20485,
        "whiteList": []
      },
      {
        "blackList": [],
        "eventType": 20486,
        "whiteList": []
      },
      {
```

```
        "blackList": [],
        "eventType": 20487,
        "whiteList": []
      },
      {
        "blackList": [],
        "eventType": 20488,
        "whiteList": []
      },
      {
        "blackList": [],
        "eventType": 20489,
        "whiteList": []
      },
      {
        "blackList": [],
        "eventType": 20490,
        "whiteList": []
      },
      {
        "blackList": [],
        "eventType": 20491,
        "whiteList": []
      },
      {
        "blackList": [],
        "eventType": 20492,
        "whiteList": []
      },
      {
        "blackList": [],
        "eventType": 20493,
        "whiteList": []
      },
      {
        "blackList": [],
        "eventType": 20494,
        "whiteList": []
      }
    ]
  },
  "config-type": "EventsConfigFromFsSensorToFsCon"
},
{
  "config-file": {
    "eventsConfigs": [
      {
        "blackList": [],
        "whiteList": [
          "%WINDIR%\\*",
          "%PROGRAMFILES%\\*",
          "%PROGRAMFILES(X86)%\\*"
        ]
      },
      {
        "blackList": [],
        "eventType": 4096,
        "whiteList": []
```

```
    },
    {
      "blackList": [],
      "eventType": 4097,
      "whiteList": []
    },
    {
      "blackList": [],
      "eventType": 4098,
      "whiteList": []
    }
  ],
  "sensorConfig": {
    "hideInjectConfig": {
      "hideInjectEnabled": true
    },
    "hookInjectConfig": {
      "blackList": [
        "%SYSTEMDRIVE%\\test\\*"
      ],
      "detailedConfig": [
        {
          "functionsList": [
            "NtQuerySystemInformation"
          ],
          "process": "%SYSTEMDRIVE%\\test\\notepad.exe"
        },
        {
          "functionsList": [
            "NtCreateThreadEx"
          ],
          "process": "%SYSTEMDRIVE%\\test\\2*.exe"
        },
        {
          "functionsList": [
            "NtQuerySystemInformation"
          ],
          "process": "%SYSTEMDRIVE%\\test\\3*.exe"
        }
      ],
      "functionsList": [
        "NtQuerySystemInformation",
        "NtCreateThreadEx",
        "NtSetContextThread",
        "NtQueueApcThread",
        "NtQueueApcThreadEx",
        "NtQueueApcThreadEx2",
        "NtProtectVirtualMemory",
        "NtMapViewOfSection"
      ],
      "hookInjectEnabled": true,
      "whiteList": [
        "%SYSTEMDRIVE%\\*"
      ]
    }
  },
  "config-type": "EventsConfigFromKernelSensorToProcCon"
```

```
},
{
  "config-file": {
    "eventsConfigs": [
      {
        "blackList": [
          "d_addr: 188.114.96.1/16"
        ],
        "whiteList": [
          "s_addr: 127.0.0.1",
          "d_addr: 127.0.0.1",
          "s_addr: 0.0.0.0/0",
          "d_addr: 0.0.0.0/0"
        ]
      },
      {
        "blackList": [],
        "eventType": 24576,
        "whiteList": []
      },
      {
        "blackList": [],
        "eventType": 24579,
        "whiteList": []
      },
      {
        "blackList": [],
        "eventType": 24580,
        "whiteList": []
      },
      {
        "blackList": [],
        "eventType": 24581,
        "whiteList": []
      }
    ]
  },
  "config-type": "EventsConfigFromNetSensorToNetCon"
},
{
  "config-file": {
    "eventsConfigs": [
      {
        "blackList": [
          "\\REGISTRY\\MACHINE\\SOFTWARE\\EDR*",
          "\\REGISTRY\\MACHINE\\system\\CurrentControlSet\\control\\securityproviders\\wdigest*"
        ],
        "whiteList": [
          "\\REGISTRY*",
          "\\REGISTRY\\MACHINE\\SOFTWARE\\Solar*Edr"
        ]
      },
      {
        "blackList": [],
        "eventType": 12288,
        "whiteList": []
      },
      {
```

```
      "blackList": [],
      "eventType": 12289,
      "whiteList": []
    },
    {
      "blackList": [],
      "eventType": 12290,
      "whiteList": []
    },
    {
      "blackList": [],
      "eventType": 12291,
      "whiteList": []
    },
    {
      "blackList": [],
      "eventType": 12292,
      "whiteList": []
    },
    {
      "blackList": [],
      "eventType": 12293,
      "whiteList": []
    },
    {
      "blackList": [],
      "eventType": 12294,
      "whiteList": []
    },
    {
      "blackList": [],
      "eventType": 12295,
      "whiteList": []
    },
    {
      "blackList": [],
      "eventType": 12296,
      "whiteList": []
    },
    {
      "blackList": [],
      "eventType": 12297,
      "whiteList": []
    },
    {
      "blackList": [],
      "eventType": 12298,
      "whiteList": []
    },
    {
      "blackList": [],
      "eventType": 12299,
      "whiteList": []
    },
    {
      "blackList": [],
      "eventType": 12300,
      "whiteList": []
```

```
        },
        {
          "blackList": [],
          "eventType": 12301,
          "whiteList": []
        },
        {
          "blackList": [],
          "eventType": 12302,
          "whiteList": []
        },
        {
          "blackList": [],
          "eventType": 12303,
          "whiteList": []
        },
        {
          "blackList": [],
          "eventType": 12304,
          "whiteList": []
        },
        {
          "blackList": [],
          "eventType": 12305,
          "whiteList": []
        },
        {
          "blackList": [],
          "eventType": 12306,
          "whiteList": []
        },
        {
          "blackList": [],
          "eventType": 12307,
          "whiteList": []
        },
        {
          "blackList": [],
          "eventType": 12308,
          "whiteList": []
        },
        {
          "blackList": [],
          "eventType": 12309,
          "whiteList": []
        }
      ]
    },
    "config-type": "EventsConfigFromRegSensorToRegCon"
  }
 ],
 "configuration_version": "0.3.1.0"
}
```


Описание элементов конфигурационного файла **config_for_XDR.json**:

configs – общий раздел конфигурации.

eventsConfigs – общая секция без eventType, но с blackList и whiteList. Секция применяется к событиям всех сенсоров данного раздела конфигурации.

config-file – раздел конфигурации, относящийся к определенной подписке на события (например, подписка на события от NET-сенсора к сетевому концентратору).

config-type – тип подписки на события, которые получает концентратор согласно настройкам в данном разделе конфигурации. Перечень типов подписок приведен в конце этого раздела.

eventsConfigs – блок описания blackList и whiteList.

blackList – список путей, события по которым сенсор будет получать даже если они указаны в whiteList.

whiteList – список путей, события по которым сенсор будет игнорировать.

- переменная s_addr. Означает «source address». В данном атрибуте можно указать только одно значение;
- переменная d_addr. Означает «delivery address». В данном атрибуте можно указать только одно значение;

Примеры IP-адресов, которые можно указывать в whiteList/blackList:

Варианты задания значений:

- IP адрес – s_addr: 10.201.31.210;
- IP адрес и порт – d_addr: 10.201.31.210:443.

Список IP-адресов, который определяется маской подсети – 192.168.101.0/26

Список IP-адресов с маской подсети и портом – 192.168.100.0/26:80

Примеры:

Фильтрация для всех событий для конкретного порта:

s_addr: 0.0.0.0/0:22

Фильтрация события для конкретного IP-адреса:

s_addr: 10.201.31.210

Фильтрация событий для конкретного IP-адреса и порта:

s_addr: 10.201.31.210:443

Фильтрация событий для пула IP-адресов:

s_addr: 10.201.31.0/26

Фильтрация событий для пула IP-адресов и порта:

s_addr: 10.201.31.0/26:443

sensorConfig – блок описания настроек сенсора.

injectEnabled – включение/отключение инжектирования.

Внимание!

Агент, начиная с версии 0.3.1, не поддерживает перехваты WinApi приложения Edge Legacy. Перехваты WinApi возможны только для Chromium-based Edge:

The new Microsoft Edge is based on Chromium and was released on January 15, 2020. It is compatible with all supported versions of Windows.
https://support.microsoft.com/en-us/microsoft-edge/download-the-new-microsoft-edge-based-on-chromium-0f4a3dd7-55df-60f5-739f-00010dba52cf

Microsoft stopped supporting Microsoft Edge Legacy on March 9, 2021. On April 13, 2021, Microsoft released a cumulative monthly security update which replaced Edge Legacy with the new Chromium-based Edge.

https://en.wikipedia.org/wiki/Microsoft_Edge

functionsList – список функций, вызовы которых перехватываются при инжектировании по умолчанию.

detailedConfig – список специализированных конфигураций инжектирования. Позволяет детально настроить список функций для инжектирования в определённые процессы. Состоит из блоков, содержащих атрибуты:

- **process** – маска полных имен процессов, для которых действует блок детальной настройки;
- **functionsList** – список функций, вызовы которых перехватываются при инжектировании в процессы, соответствующие блоку детальной настройки. Этот атрибут переписывает список функций, задаваемый по умолчанию.

subscriptions – массив, предназначенный для получения новых событий. Формат записей в массиве следующий:

- **source** – это источник (провайдер), из которого будут собираться события;
- **filter** – условие, по которому будут собираться события.

clearSubscriptions – массив, предназначенный для получения событий очистки журнала. Формат – строки с источниками (провайдерами), для которых требуется мониторинг очистки.

Примеры путей, которые можно указывать в blackList и whiteList:

- файлы, наименования которых удовлетворяют маске, например: **C:\Windows\System32\drivers*_text.exe**
- отдельные директории, например: **C:\Windows\System32\drivers***
- указанный файл, например: **C:\Windows\System32\drivers\text.exe**

- пути к веткам или ключам реестра, например: **\\REGISTRY\\MACHINE\\SOFTWARE\\Solar*Edr**

- пути для событий категории WMI-активность, например: **root\cimv2\Win32_Process**, где **root\cimv2** – это namespace, а **Win32_Process** – это class.

Символы ***** (отсутствие символов или несколько символов) и **?** (один символ) разрешены и позволяют создавать маску пути (см. примеры выше).

Для каждого сенсора в конфигурации описывается отдельный white/black-лист.

Конфигурация подписок концентраторов на сенсоры задается в файле конфигурации **config_for_XDR.json**:

- **EventsConfigFromNetSensorToNetCon** – настройка потока событий от NET-сенсора к сетевому концентратору;

- **EventsConfigFromFsSensorToFsCon** – настройка потока событий от FS-сенсора к файловому концентратору;

- **EventsConfigFromRegSensorToRegCon** – настройка потока событий от Reg-сенсора к концентратору реестра;

- **EventsConfigFromEtwSensorToOsCon** – настройка потока событий от OS-сенсора к концентратору операционной системы;

- **EventsConfigFromEtwSensorToProcCon** – настройка потока событий от ETW-сенсора к концентратору процессов;

- **EventsConfigFromKernelSensorToProcCon** – настройка потока событий от Proc-сенсора к концентратору процессов;

- **EventsConfigFromEvtLogSensorToOsCon** – настройка потока событий от EvtLog-сенсора к концентратору операционной системы.

Конфигурирование логирования/отладочной печати событий выполняется в разделе **EventsConfigFromEvtLogSensorToOsCon**. Состав событий определяется в файле **EventsDebugPrintConfig.json**, который находится в директории **C:\Program Files\SolarEDR\config**. Пример файла:

```
{
  "DebugPrintAnalyzerIncomingEvents": false,
  "DebugPrintAnalyzerGeneratedIncidents": false,
  "DebugPrintEventsSendingToServer": false,

  "DebugPrintEventsNetworkConcentrator": false,
  "DebugPrintEventsRegistryConcentrator": false,
  "DebugPrintEventsFilesystemConcentrator": false,
  "DebugPrintEventsProcessesConcentrator": false,
  "DebugPrintEventsOsConcentrator": false,

  "DebugPrintEventsEtwSensor": false,
  "DebugPrintEventsWinApiHookSensor": false,
  "UnexpandVarsForAllUsers": true
  }
```

Значения флагов:

- **DebugPrintAnalyzerIncomingEvents** – печать всех событий, поступающих в анализатор от концентраторов;
- **DebugPrintAnalyzerGeneratedIncidents** – печать инцидентов, генерируемых анализатором;
- **DebugPrintEventsSendingToServer** – печать событий, отправляемых на сервер;
- **DebugPrintEventsNetworkConcentrator** – печать событий, поступающих в сетевой концентратор;
- **DebugPrintEventsRegistryConcentrator** – печать событий, поступающих в концентратор реестра;
- **DebugPrintEventsFilesystemConcentrator** – печать событий, поступающих в концентратор файловой системы;
- **DebugPrintEventsProcessesConcentrator** – печать событий, поступающих в концентратор процессов;
- **DebugPrintEventsOsConcentrator** – печать событий, поступающих в концентратор ОС;
- **DebugPrintEventsEtwSensor** – печать событий, генерируемых в ETW-сенсоре;
- **DebugPrintEventsWinApiHookSensor** – печать событий, генерируемых в результате инжектирования;
- **UnexpandVarsForAllUsers** – раскрывает переменные окружения из настроек для всех пользователей.

Приложение В. Сведения о типах событий

В Табл.В.1 представлены типы событий, сгруппированные по категориям и источникам.

Табл. В.1. Типы событий

Источник	Категория	Тип события	Описание
Solar EDR Windows	Сетевая активность	TcpConnectionAttempted	Получение события установки tcp-соединения
		TcpDisconnect	Получение события разрыва связи по tcp-соединению
		UdpDataSent	Получение события отправки данных через udp
		UdpDataReceived	Получение события получения данных через udp
	Файловая система	FileCreate	Создание файла
		FileSetBasicInformation	Установка основной информации для файла
		FileSetDispositionInformation	Событие указания, должен ли файл быть удален. Используется для любых дескрипторов
		FileSetLinkInformation	Установка для файла ссылки на другой файл
		FileSetRenameInformation	Установка целевого имени, в которое должен быть переименован исходный файл
		FileSetPositionInformation	Установка позиции в файле, который был открыт
		FileSetAllocationInformation	Установка общего количества байт, которые должны быть выделены для файла
		FileSetEofInformation	Изменение содержимого файла путем добавления в файл информации
		FileSetValidDataLengthInformation	Установка допустимой длины данных в указанном файле
		FileRead	Чтение файла
		FileWrite	Запись в файл
		FileDeviceControl	Управление вводом-выводом драйвера устройства через DeviceIoControl или аналогично из ядра
		FileSetSecurity	Установка для файла разрешения безопасности для любого пользователя системы
		FileAcquireSectionSync	Получение события отображения файла в память при открытии
		FileReleaseSectionSync	Получение события отображения файла в память при закрытии
		FileOpen	Открытие файла

Источник	Категория	Тип события	Описание
		FileDelete	Удаление файла. Включает два варианта: • Открытие файла с флагом FILE_DELETE_ON_CLOSE (в этом случае устанавливается атрибут FileOpenedWithDeleteOnClose) • Установка отметки об удалении файла через FileDispositionInformation и FileDispositionInformationEx
	Процессы	ProcessCreate	Создание процесса в ОС
		ProcessExit	Завершение процесса в ОС
		ImageLoad	Загрузка бинарного файла (образа) в процесс (dll или exe)
		ImageUnload	Выгрузка бинарного файла (образа) из процесса (dll или exe)
		ProcessCreateElevated	Создание процесса с повышением привилегий в ОС
		CreateRemoteThread	Создание потока в виртуальном адресном пространстве другого процесса
		ProcessAccess	Создание/дублирование дескриптора для указанного объекта процесса
	LogOn/LogOff	UserLogon	Вход пользователя в ОС путем ввода логина и пароля
		UserLogoff	Выход пользователя из ОС
	Реестр	RegCreateKey	Создание ключа в реестре
		RegDeleteKey	Удаление ключа в реестре
		RegRenameKey	Изменение имени ключа в реестре
		RegSetValueKey	Сохранение данных в параметр ключа реестра
		RegDeleteValueKey	Удаление параметра ключа реестра
		RegEnumerateKey	Перечисление подразделов указанного открытого ключа реестра
		RegEnumerateValueKey	Перечисление значений для указанного открытого ключа реестра. Функция копирует одно имя индексированного значения и блок данных для ключа при каждом вызове
		RegCloseKey	Закрытие дескриптора для указанного раздела реестра
		RegQueryMultipleValueKey	Извлечение типа и данных для указанного имени значения, связанного с открытым разделом реестра
		RegOpenKey	Открытие указанного раздела реестра (без учета регистра)
		RegQueryValueKey	Извлечение типа и данных для списка имен значений, связанных с открытым ключом реестра

Источник	Категория	Тип события	Описание
		RegFlushKey	Запись в реестр всех атрибутов заданного открытого раздела реестра
		RegLoadKey	Создание подраздела в разделе реестра и загрузка данных из указанного куста реестра в этот подраздел
		RegUnloadKey	Выгрузка указанного раздела реестра и его подразделов из реестра
		RegGetKeySecurity	Извлечение копии дескриптора безопасности, защищающего указанный открытый раздел реестра
		RegSetKeySecurity	Задание безопасности открытого раздела реестра
		RegRestoreKey	Считывание сведений реестра в указанном файле и копирование их по указанному разделу
		RegSaveKey	Сохранение указанного ключа и всех его подразделов и значений в новом файле в стандартном формате
		RegReplaceKey	Замена файла, резервной копии раздела реестра, и всех его подразделов другим файлом. При следующем запуске системы ключ и подразделы имеют значения, хранящиеся в новом файле
		RegQueryKeyName	Возвращение списка следующих уровней подразделов и записей, расположенных в указанном подразделе в реестре
		RegSaveMergedKey	Возвращение сведений о двух поддеревьях реестра, для которых объединенное представление должно быть сохранено в файл
		RegSetInformationKey	Установка информации по ключу реестра
	WMI-активность	WmiExecMethod	Исполнение метода подсистемы WMI
		WmiExecQuery	Исполнение запроса через WMI
		WmiPutClass	Добавление нового класса WMI
		WmiDeleteClass	Удаление класса WMI
	Аудит/Самозащита	ConfigUpdate	Применение новой конфигурации/LUA
		UnauthorizedDbAccess	Попытка доступа к защищенному хранилищу
		HashDifference	Самозащита: компонент был модифицирован
		ServiceStart	Факт запуска сервиса агента
		ServiceStop	Факт остановки сервиса агента
		CommunicationStatus	Потеря/восстановление связи между компонентами агента
		ConnectionStatus	Потеря/восстановление связи с сервером (отдельно для каждого канала)

Источник	Категория	Тип события	Описание
		AgentRemoveStarted	Старт удаления агента
		AgentRemoveComplete	Результат операции удаления агента (успешно/неуспешно)
		AdamRemoveFailed	Неуспешный старт удаления ADAM
		DeactivationOn	Результат выполнения деактивации агента со статусом success/failure
		DeactivationOff	Результат выполнения активации агента (выхода из режима деактивации) со статусом success/failure
		AgentModificationAttempt	Попытка открытия бинарного файла агента с целью модификации/удаления/перемещения/переименования. Попытка переименования каталогов агента также обрабатывается самозащитой агента
	Журналы Windows	EventLogNewRecord	Получение события записи событий в журнал Windows
		EventLogClear	Очистка журнала Windows
	Перехваты WinApi	WinApiHook	Перехват WinAPI-вызовов через dll агента, инжектированную в сторонний процесс
	Консольные команды	ConsoleCommand	Перехват команд, вводимых/исполняемых в консолях CMD и Powershell
Solar NTA	Suricata	Alert	Негативное сетевое событие (сетевая атака, сетевая аномалия и т. д.), выявленное с помощью правил Suricata

Приложение С. Обязательные атрибуты событий Solar EDR Windows и Solar NTA

В Табл.С.1 представлен список обязательных атрибутов, которые присутствуют у любого события, полученного из источника Solar EDR Windows или Solar NTA.

Табл. С.1. Обязательные атрибуты событий Solar EDR Windows и Solar NTA

Атрибут	Назначение	Тип данных
ClientID	Идентификатор машины, с которой было получено событие	string
EventTime	Время начала операции (в UTC)	timestamp
EventTick	Время события в тиках от старта системы	int64
EventID	Внутренний ID события	uint32
EventType	Тип события	int64

Приложение D. Атрибуты событий Solar EDR Windows

В Табл.D.1 представлены атрибуты событий, полученных из источника Solar EDR Windows.

Табл. D.1. Атрибуты событий Solar EDR Windows

Атрибут	Назначение	Тип данных	Категория
RegValueDataSize	Размер буфера данных в байтах	unsigned	Реестр
RegEntryCount	Количество записей в массиве RegValueName	unsigned	
RegFileName	Имя файла	string	
RegHighKeyName	Имя ключа реестра одной ветки реестра	string	
RegKeyName	Имя ключа реестра	string	
RegLastWriteTime	Время последнего изменения ключа реестра	timestamp	
RegLowKeyName	Имя ключа реестра второй ветки реестра	string	
RegNewFileName	Имя файла с информацией реестра	string	
RegNewKeyName	Новое имя ключа (содержит полный путь к ключу)	string	
RegOldFileName	Имя файла, получающего резервную копию заменяемой информации реестра	string	
SecurityDescriptor	Дескриптор безопасности в формате SDDL	string	
SecurityInformation	Содержимое дескриптора	unsigned	
RegValueData	Данные значения	string	
RegValueName	Имя значения реестра	string	
RegValueType	Тип данных значения	string	
RegSourceFile	Имя подгружаемого файла реестра	string	
ConnectionId	Системный ID соединения (может быть равен 0)	unsigned	Сетевая активность
DestinationAddress	IP-адрес назначения	string	
DestinationPort	Порт назначения	unsigned	
NetPayloadSize	Размер полезных данных (payload) сетевого пакета	int64	
SourceAddress	IP-адрес инициатора соединения	string	
SourcePort	Порт инициатора соединения	unsigned	
FileStartOperationOffset	Начальное смещение при операции чтения/записи	unsigned	Файловая система
FileAllocationSize	Размер выделенного под файл места на устройстве	unsigned	
FileChangeTime	Время последнего изменения объекта ФС	timestamp	
FileCreationTime	Время создания объекта ФС	timestamp	
FileCurrentOffset	Смещение в байтах текущего указателя файла	unsigned	
FileDeleteFlag	Маркер удаления объекта ФС при закрытии всех дескрипторов	bool	
FileEndPosition	Позиция конца файла	unsigned	
FileAttributes	Атрибуты файла	unsigned	
FileIoControlCode	Код функции IOCTL	unsigned	
FileLockKey	Ключ блокировки диапазона байт файла, с которым происходит операция чтения/записи	unsigned	
FileLastAccessTime	Время последнего доступа к объекту ФС	timestamp	

Атрибут	Назначение	Тип данных	Категория
FileLastWriteTime	Время последней записи в объект ФС	timestamp	
FileDataLength	Длина диапазона байт при операции чтения/записи в файл	unsigned	
FileNewFilePath	Задаваемый путь файла/ссылки на файл	string	
FilePath	Полный путь с именем объекта ФС	string	
FileReplaceIfExistsFlag	Маркер необходимости замены существующего объекта при переименовании/создании жёсткой ссылки	bool	
SecurityDescriptor	Дескриптор безопасности объекта ФС в формате SDDL	string	
FileOperationStatus	Статус завершения операции (NTSTATUS)	unsigned	
FileStatusInfo	Атрибут результата выполнения операции (смысл зависит от типа операции)	unsigned	
FileValidDataLength	Допустимая длина данных файла	unsigned	
FileIsSectionNew	Является ли синхронизируемая секция вновь созданной	bool	
FileSectionPageProtection	Запрашиваемый тип защиты страниц секции	unsigned	
FileSectionSize	Возвращенный размер секции	unsigned	
FileSectionFlags	Атрибуты секции	unsigned	
FileSecDesReadAlig	Оптимальный размер эффективных операций чтения секции	unsigned	
FileOpenedWithDeleteOnClose	Атрибут, указывающий, что файл был открыт с флагом DELETE_ON_CLOSE	bool	
ImageHash	md5 хеш загружаемого модуля	string	Процессы
ImagePath	Путь до загружаемого модуля	string	
CreateElevatedProcessResult	Результат создания Elevated процесса (UAC) (op_status): true – успех, false – неудача, процесс не был создан	bool	
TargetProcessId	Идентификатор целевого процесса, в котором создается поток или к которому осуществляется доступ	unsigned	
ThreadId	Идентификатор потока, созданного в другом процессе	unsigned	
TargetProcessName	Полный путь процесса, в котором создается поток или к которому осуществляется доступ	string	
DesiredAccess	Запрошенная пользователем маска доступа при осуществлении доступа к процессу	unsigned	
OperationType	Тип операции, которая осуществляется с дескриптором. При создании дескриптора значение будет OB_OPERATION_HANDLE_CREATE (1), при дубликате дескриптора значение будет OB_OPERATION_HANDLE_DUPLICATE (2)	unsigned	
CallTrace	Трассировка вызовов процесса, который создает/дублирует дескриптор указанного объекта процесса. Каждая запись – это строка с форматом: *полный путь модуля* *адрес вызванной функции*	arrray	
ImageComments	Комментарии к загружаемой библиотеке	string	
ImageCompanyName	Название компании, выпустившей загружаемую библиотеку	string	

Атрибут	Назначение	Тип данных	Категория
ImageFileDescription	Описание к загружаемой библиотеке	string	
ImageFileVersion	Версия загружаемой библиотеки	string	
ImageInternalName	Внутреннее имя загружаемой библиотеки	string	
ImageLegalCopyright	Авторские права загружаемой библиотеки	string	
ImageLegalTragemark	Торговые знаки загружаемой библиотеки	string	
ImageOriginalFileName	Оригинальное имя загружаемой библиотеки	string	
ImagePrivateBuild	Приватный номер сборки загружаемой библиотеки	string	
ImageProductName	Имя продукта загружаемой библиотеки	string	
ImageProductVersion	Версия продукта загружаемой библиотеки	string	
ImageSpecialBuild	Специальный номер сборки загружаемой библиотеки	string	
ImageSignerName	Издатель подписи загружаемой библиотеки	string	
ImageSignValid	Валидна ли подпись загружаемой библиотеки	bool	
ImageHasSign	Есть ли подпись у загружаемой библиотеки	bool	
ImageTopCertIssuer	Издатель последнего сертификата загружаемой библиотеки	string	
ImageTopCertSubject	Субъект последнего сертификата загружаемой библиотеки	string	
ImageTopCertStartDate	Дата начала действия последнего сертификата загружаемой библиотеки	string	
ImageTopCertEndDate	Дата окончания действия последнего сертификата загружаемой библиотеки	string	
ImageTopCertSerial	Серийный номер последнего сертификата загружаемой библиотеки	string	
ImageRootCertIssuer	Издатель первого (корневого) сертификата загружаемой библиотеки	string	
ImageRootCertSubject	Субъект первого (корневого) сертификата загружаемой библиотеки	string	
ImageRootCertStartDate	Дата начала действия первого (корневого) сертификата загружаемой библиотеки	string	
ImageRootCertEndDate	Дата окончания действия первого (корневого) сертификата загружаемой библиотеки	string	
ImageRootCertSerial	Серийный номер первого (корневого) сертификата загружаемой библиотеки	string	
WmiNamespace	Пространство имен WMI	string	WMI-активность
WmiClass	WMI-класс	string	
WmiMethod	Метод WMI-класса	string	
WmiOperationId	Идентификатор операции WMI	int	
WmiClientMachine	На каком хосте выполнялась операция WMI	string	
WmiIsLocalOperation	Локально или удаленно вызвали	bool	
WmiMethodArgs	Аргументы операции	string	
Component	Наименование компонента	string	Аудит/Самозащита
OperationResult	Результат (success, failure)	string	
OperationDescription	Текстовое поле с описанием проблемы/логом (может быть пустым)	string	

Атрибут	Назначение	Тип данных	Категория
EventLogXmlEvent	Представление события журналов Windows в xml-формате (для событий очистки это поле – пустая строка)	string	Журналы Windows
EventLogSource	Провайдер, с которого пришло событие	string	
WinApiFuncName	Имя функции	string	Перехваты WinApi
WinApiResult	Результат выполнения	string	
WinApiArgs	Параметры WinAPI-вызова	array	
ConsoleName	Название консоли, в которой выполнялась команда CDM или Powershell	string	Консольные команды
ConsoleCommand	Команда, введенная в консоли	string	
CreatorProcessPath	Полный путь исполняемого файла процесса-создателя	string	Список общих атрибутов
CreatorProcessId	Идентификатор процесса-создателя операции	unsigned	
DesiredAccess	Запрашиваемые права (какие права были запрошены процессом, когда он осуществлял доступ к другим процессам) / Запрашиваемый доступ к объекту	unsigned	
UserDomain	Домен (или имя компьютера) пользователя, от имени которого выполняется процесс, либо произошло другое действие	string	
GrantedAccess	Предоставленные права (какие права были предоставлены) / Запрашиваемый доступ к объекту	unsigned	
SessionId	Номер сессии, в которой работает процесс, либо произошло другое действие. Значение по умолчанию 0	unsigned	
UserSID	SID пользователя, от имени которого выполняется процесс, либо произошло другое действие	string	
ProcessImageHash	md5 хеш от бинарника исполняемого файла процесса	string	
ParentImageHash	md5 хеш от бинарника исполняемого файла процесса родителя	string	
ProcessExitCode	Код завершения процесса	unsigned	
ProcessCreationTime	Время создания процесса	timestamp	
ParentProcessCmdLine	Командная строка родительского процесса	string	
ParentProcessId	PID родительского процесса	unsigned	
ProcessCmdLine	Командная строка процесса	string	
ProcessId	PID созданного процесса – Идентификатор процесса на агенте	unsigned	
ProcessPath	Полный путь исполняемого файла процесса	string	
ProcessTerminationTime	Время завершения процесса	timestamp	
Username	Имя пользователя, от которого выполняется процесс, либо произошло другое действие	string	
ParentProcessPath	Полный путь исполняемого файла процесса родителя	string	
CreatorProcessCmdLine	Командная строка процесса-создателя	string	
ParentProcessUserSID	SID пользователя, от имени которого выполняется родительский процесс	string	

Атрибут	Назначение	Тип данных	Категория
ParentProcessUserName	Имя пользователя, от которого выполняется родительский процесс	string	
ParentProcessUserDomain	Домен (или имя компьютера) пользователя, от имени которого выполняется родительский процесс	string	
IsLocalSession	Локальная сессия (true – локальная, false – дистанционная), в которой работает процесс, либо произошло другое действие	bool	
LogonId	Локальный уникальный идентификатор (LUID), который идентифицирует сеанс входа в систему. Значение по умолчанию: 0x3e7	string	
ProcessExecComments	Комментарии к исполняемому файлу	string	
ProcessExecCompanyName	Название компании, выпустившей исполняемый файл	string	
ProcessExecFileDescription	Описание к исполняемому файлу	string	
ProcessExecFileVersion	Версия исполняемого файла	string	
ProcessExecInternalName	Внутреннее имя исполняемого файла	string	
ProcessExecLegalCopyright	Авторские права исполняемого файла	string	
ProcessExecLegalTragemark	Торговые знаки исполняемого файла	string	
ProcessExecOriginalFileName	Оригинальное имя исполняемого файла	string	
ProcessExecPrivateBuild	Приватный номер сборки исполняемого файла	string	
ProcessExecProductName	Имя продукта исполняемого файла	string	
ProcessExecProductVersion	Версия продукта исполняемого файла	string	
ProcessExecSpecialBuild	Специальный номер сборки исполняемого файла	string	
ProcessSignerName	Издатель подписи исполняемого файла	string	
ProcessSignValid	Валидна ли подпись исполняемого файла	bool	
ProcessHasSign	Есть ли подпись у исполняемого файла	bool	
ProcessTopCertIssuer	Издатель последнего сертификата исполняемого файла	string	
ProcessTopCertSubject	Субъект последнего сертификата исполняемого файла	string	
ProcessTopCertStartDate	Дата начала действия последнего сертификата исполняемого файла	string	
ProcessTopCertEndDate	Дата окончания действия последнего сертификата исполняемого файла	string	
ProcessTopCertSerial	Серийный номер последнего сертификата исполняемого файла	string	
ProcessRootCertIssuer	Издатель первого (корневого) сертификата исполняемого файла	string	
ProcessRootCertSubject	Субъект первого (корневого) сертификата исполняемого файла	string	
ProcessRootCertStartDate	Дата начала действия первого (корневого) сертификата исполняемого файла	string	
ProcessRootCertEndDate	Дата окончания действия первого (корневого) сертификата исполняемого файла	string	
ProcessRootCertSerial	Серийный номер первого (корневого) сертификата исполняемого файла	string	

Приложение Е. Описание языка запросов, используемого при поиске сессий

В текущей версии Солар ПКОиР язык запросов, который используется при поиске сессий, основан на языке WireShark.

Следует отметить, что в запросе не указываются типы метаданных, весь текст запроса применяется ко всей цепочке метаданных сессии. Например, если цепочка выглядит как <СЕССИЯ-HTTP-TCP-IP>, то в запросе можно указывать любые поля типа метаданных из перечисленных: ip.srcaddr, tcp.dport, http.body и т. д. Для поиска по другим типам метаданных используется JSON SQL.

Условия в поисковых запросах задаются с помощью выражений и значений. Выражения, в свою очередь, представляют собой имя (или код) операции и ее аргументы. Значение – это второй операнд в операциях. Значение является константой и может быть числом, строкой или IPv4 адресом (с подсетью или без).

В Табл.Е.1 представлен список операций сравнения и логических операций, используемых для ввода поискового запроса, а также примеры их использования.

Табл. Е.1. Операции сравнения и логические операции

Описание	Оператор	Примеры использования
«равно»	• **eq** • **==**	• **tcp.dport eq 22** • **tcp.dport == 22**
«не равно»	• **neq** • **!=**	• **tcp.dport neq 22** • **tcp.dport != 22**
«больше»	• **gt** • **>**	• **http.response.code gt 200** • **http.response.code > 200**
«меньше»	• **lt** • **<**	• **http.response.code lt 200** • **http.response.code < 200**
«больше или равно»	• **gte** • **>=**	• **http.response.code gte 200** • **http.response.code >= 200**
«меньше или равно»	• **lte** • **<=**	• **http.response.code lte 200** • **http.response.code <= 200**
логическое «НЕ»	• **!** • **not**	• **!(tcp.dport eq 22)** • **NOT(tcp.dport eq 22)**
логическое «И»	• **&&** • **and**	• **(tcp.dport eq 22) AND (tcp.sport lt 1024)** • **(tcp.dport eq 22) && (tcp.sport lt 1024)**

Описание	Оператор	Примеры использования
логическое «ИЛИ»	• **||** • **or**	• **(tcp.dport eq 22) || (tcp.dport eq 23)** • **(tcp.dport eq 22) OR (tcp.dport eq 23)**
<аргумент 1> содержит <аргумент 2>	**contains**	• **http.url contains "session"** • **contains(http.url, "session")**

Приложение F. Операторы в условиях правил

Условия, задаваемые в решающих правилах, содержат:

- атрибут события;
- оператор;
- значение (зависит от атрибута события и оператора).

В Табл.F.1 представлен перечень операторов, которые используются в условиях правил.

Табл. F.1. Операторы в условиях правил

Описание	Оператор
«равно» (equals)	**==**
«не равно» (does not equals)	**!=**
«содержит» (contains – частичное совпадение без учета регистра)	**contains**
«не содержит» (not contains – частичное совпадение без учета регистра)	использовать **contains** с **&& !(...)** или **|| !(...)**
«начинается» (starts with)	**startsWith**
«заканчивается» (ends with)	**endsWith**
«входит» (includes – содержится в массиве значений)	**includes**
«не входит» (not includes – не содержится в массиве значений)	использовать **includes** с **&& !(...)** или **|| !(...)**
«пустое» (проверка на NULL)	**== null**
«не пустое» (проверка на NOT NULL)	**!= null**
«больше» (greater than)	**>**
«больше или равно» (greater than or equals to)	**>=**
«меньше» (less than)	**<**
«меньше или равно» (less than or equal to)	**<=**
«входит в интервал значений» (between)	**between [<значение_1>;<значение_2>]**
«не входит в интервал значений» (does not between)	использовать **between** с **&& !(...)** или **|| !(...)**
«истина» (is true)	**== true**
«не истина» (does not true)	заменяется на **== false**
«ложь» (is false)	**== false**

Пример условий:

attribute1 == value1 && attribute2 != very long value || intAttribute > 2 && !(dateAttribute <= 01-01-2024) || !(attribute4 between [2;10]) && attribute5 startsWith value6

Логический оператор (используется для связи условий между собой):

- **&&** – логическое «И»;
- **||** – логическое «ИЛИ»;
- **&& !(...)** – логическое «НЕ И»;
- **|| !(...)** – логическое «НЕ ИЛИ».

Приложение G. Тестирование стабильной работы агента Solar EDR Windows с прикладным ПО

Solar EDR Windows совместим со следующим ПО:

- 1С:Предприятие 8;
- 7-Zip (x64 edition);
- Adobe Acrobat Reader;
- Google Chrome;
- Kaspersky Endpoint Security для Windows;
- Microsoft Office Professional Plus 2019 - ru-ru: Excel, Word, PowerPoint, MS Teams, Outlook, OneDrive, Visio;
- Microsoft Visual C++ 2015-2019 Redistributable (x64);
- Microsoft Visual C++ 2015-2019 Redistributable (x86);
- PostgreSQL 9.4 (x86);
- PyCharm;
- Ассистент (для удаленного доступа);
- Telegram;
- WhatsApp;
- WinRAR;
- Агент addVisor;
- Dozor Endpoint Agent.

Приложение H. Регулярные выражения LUA

Регулярное выражение Lua Regular Expression (RegEx) – это последовательность символов, которая формирует шаблон поиска и используется для сопоставления комбинаций символов в строках. Регулярное выражение можно использовать для проверки того, содержит ли строка указанный шаблон поиска или нет. В отличие от других языков, регулярное выражение lua отличается от других, оно более ограничено и имеет другой синтаксис.

Программирование на Lua предлагает набор функций, которые позволяют искать соответствие в строке, как указано ниже:

find(string, pattern [, init [, plain]]): функция возвращает начальный и конечный индекс соответствия шаблону в строке.

match(string, pattern [, index]): функция сопоставляет шаблон, как только сопоставление начинается с заданного индекса.

match(string, pattern): функция возвращает функцию, которая выполняет итерацию по всем совпадениям с шаблоном в строке.

gsub(string, pattern, repl [, n]): функция используется для замены соответствующей строки подстроками, a n указывает количество замен.

Метасимволы регулярных выражений Lua

Программирование на Lua предлагает набор метасимволов, специальных последовательностей и наборов, которые имеют особое значение, как указано ниже:

. – : Это метасимвол, который соответствует всем символам.

%a: Это специальная последовательность, которая соответствует всем буквам.

%l: Это специальная последовательность, которая соответствует всем строчным буквам.

%u: Это специальная последовательность, которая соответствует всем прописным буквам.

%d: Это специальная последовательность, которая соответствует всем цифрам.

%s: Это специальная последовательность, которая соответствует всем пробельным символам.

%x: Это специальная последовательность, которая соответствует всем шестнадцатеричным цифрам.

%p: Это специальная последовательность, которая соответствует всем знакам препинания.

%g: Это специальная последовательность, которая соответствует всем печатаемым символам, кроме пробела.

%c: Это специальная последовательность, которая соответствует всем управляющим символам.

[set]: Это набор, который соответствует классу, который является объединением всех символов в set.

[^set]: Это специальная последовательность, которая соответствует дополнению set.

+: Это случайное совпадение, которое соответствует 1 или более вхождениям предыдущего класса символов.

*: Это случайное совпадение, которое соответствует 0 или более вхождениям предыдущего класса символов.

?: Это точное совпадение, которое соответствует 0 или 1 вхождению предыдущего класса символов.

– -: Это отложенное совпадение, которое соответствовало 0 или более вхождениям предыдущего класса символов.

Пример кода:

```
-- create string to match pattern
str = 'Apple'
print( "The string is : ", str)
-- 'pl' match in string
print( "string.find( str, 'pl') : ", string.find( str, 'pl'))
-- 'lua' will not be match in string
print( "string.find( str, 'lua') : ", string.find( str, 'lua'))
-- e.. match e and any two characters
print( "string.find( 'Hello', 'e..') : ", string.find( "Hello", 'e..'))
-- match 3 sequence of digit
print( "string.match(\"Hello, 123 \", '%d%d%d') : ", string.match("Hello, 123 ", '%d%d%d'))
--
print( "string.match('banana', '[na][an]') : ", string.match("banana", '[na][an]'))
-- you can specify a range of characters using -
print( "string.match('123', '[0-9]') : ", string.match("123", '[0-9]'))
-- Repetition examples
print( "string.match('Apples', 'Apples?') : ", string.match("Apples", 'Apples?'))
print( "string.match('Apple', 'Apples?') : ", string.match("Apple", 'Apples?'))
print( "string.match('Apple', 'Apples') : ", string.match("Apple", 'Apples'))
print( "string.match('abcd', 'a.*') : ", string.match("abc", 'a.*'))
-- $ matches the end of the string
print( "string.match('abcd', 'a.-$') : ", string.match("abcd", 'a.-$'))
-- .- part matches nothing
print( "string.match('abcd', 'a.-$') : ", string.match("abcd", 'a.-'))
-- ^ matches the start of the string
print( "string.match('abcd', '^.-b') : ", string.match("abcd", '^.-b'))
-- gsub() example
print( "string.gsub('Hello!, John', 'John', 'Johny') : ", string.gsub("Hello!, John", "John", "Johny"))
```

Результат:

```
The string is :         Apple
string.find( str, 'pl') :       3       4
string.find( str, 'lua') :      nil
string.find( 'Hello', 'e..') :  2       4
string.match("Hello, 123 ", '%d%d%d') :         123
string.match('banana', '[na][an]') :    an
string.match('123', '[0-9]') :  1
string.match('Apples', 'Apples?') :     Apples
string.match('Apple', 'Apples?') :      Apple
string.match('Apple', 'Apples') :       nil
string.match('abcd', 'a.*') :   abc
string.match('abcd', 'a.-$') :  abcd
string.match('abcd', 'a.-$') :  a
string.match('abcd', '^.-b') :  ab
string.gsub('Hello!, John', 'John', 'Johny') :  Hello!, Johny   1
```

Рис. H.1.

В приведенной выше lua-программе, присутствуют примеры сопоставления с образцом с помощью регулярного выражения, где используются функции **find()**, **match()** и **gsub().**

Функция **find()** используется для проверки того, найден ли шаблон или нет. Если шаблон найден, то возвращает начальную и конечную позицию шаблона, найденного в строке. Если шаблон не найден, то возвращает «nil» в качестве выходных данных.

Функция **match()** используется для сопоставления с шаблоном и возврата совпадающей группы из строки. В приведенном выше примере строка – «Привет, 123», а шаблон – «%d%d%d» (который соответствует трем следующим цифрам), поэтому здесь совпадающая строка – «123», которая отображается в выходных данных.

Затем используется функция **gsub()**, которая соответствует шаблону (второй параметр), и соответствующая строка заменяется третьей строкой, передаваемой как «Johny». Выходные данные этого метода возвращают строку (с совпадающей заменой) и число замен. В выходных данных это значение равно «1», поскольку совпало только одно вхождение.

Лист контроля версий

21/08/2024-15:20