ООО «Интеллектуальная безопасность»

«УТВЕРЖДАЮ»

Генеральный директор

ООО «Интеллектуальная безопасность»

_____ Р.Г. Рахметов

М.П.

«____» _____ 2022 г.

Программный комплекс «Security Vision Security Orchestration, Automation and Response»

Руководство по эксплуатации

На 52 листах

Москва

2022

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

В настоящем документе приведено описание основных операций, выполняемых пользователем Security Vision – Security Orchestration, Automation and Response (SOAR). Документ содержит описание работы и использования Системы, в том числе включает общее описание программы, условия, необходимые для корректной работы Системы, описание операций, доступных Пользователю в интерфейсе Системы.

Разработчиком программного обеспечения Security Vision SOAR является российская компания. Программный комплекс не содержит компонентов иностранного производства

2 НАЗНАЧЕНИЕ И ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ СИСТЕМЫ

Система является многофункциональным инструментом автоматизации деятельности по реагированию на инциденты информационной безопасности в организации. Обращение пользователя с системой происходит посредством портала SV.

Система обеспечивает выполнение следующих функций:

- Управление жизненным циклом инцидентов информационной безопасности;
- Взаимодействие с внешними системами;
- Управление активами;
- Управление визуализацией на географической карте;
- Формирование отчётов по информационной безопасности;
- Визуализация данных о состоянии информационной безопасности;
- Управление документами, регламентирующими порядок обеспечения информационной безопасности предприятия;
- Разделение пользователей портала по контентно-ролевой модели, согласно выполняемым ими функциям;
- Помощь в принятии решений по возникающим проблемам информационной безопасности;

Управление жизненным циклом инцидентов информационной безопасности является основной функцией системы и включает в себя автоматизацию следующих процессов:

- Регистрация инцидента информационной безопасности
- Определение контекста инцидента
- Назначение ответственного за инцидент
- Контроль процесса обработки инцидента информационной безопасности

Управление активами осуществляется посредством соответствующего модуля. Данный функционал позволяет производить учет активов различных типов для дальнейшего формирования области оценки риска с включением соответствующих активов.

Формирование отчетов и визуализация данных о рисках кибербезопасности осуществляется посредством модуля аналитики и отчетности.

Разделение пользователей портала по контентно-ролевой модели осуществляется посредством присвоения каждому пользователю одной или нескольких ролей, обладающих соответствующими разрешениями.

3 ОПИСАНИЕ ОСНОВНЫХ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ ПОРТАЛА SECURITY VISION

3.1 Интерфейс Портала Security Vision

3.1.1 Окно входа пользователя

Для входа на портал Security Vision необходимо ввести в адресной строке браузера https://sv-soar-app. После входа на сайт Портала Security Vision выводится страница входа пользователя (Рис. 3-1):

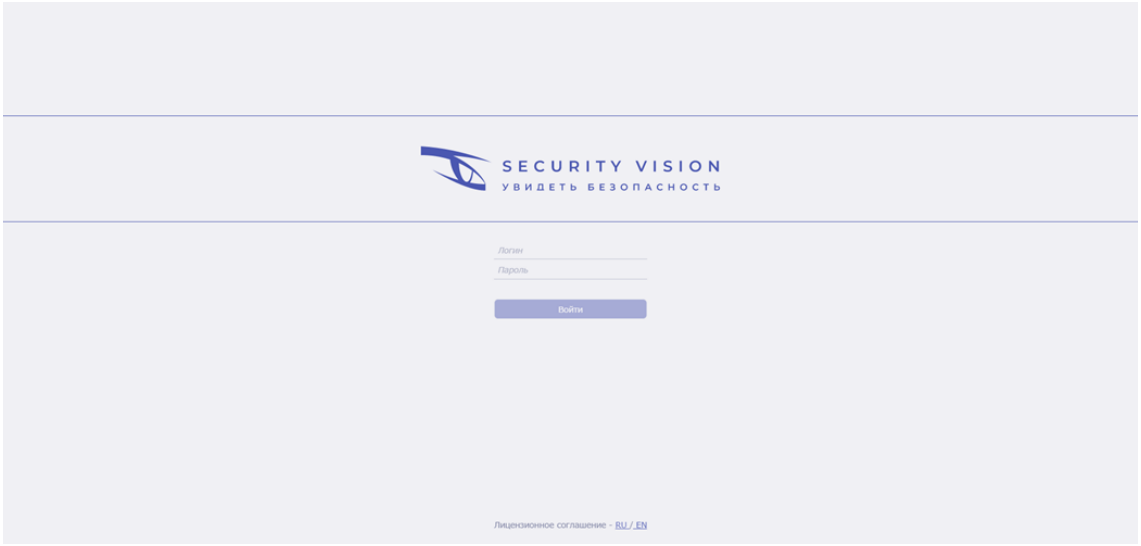


Рис. 3-1 Окно входа в систему

На данной странице необходимо указать корректное имя пользователя и пароль для входа в систему.

3.2 Основное меню

Портал Security Vision имеет модульную структуру. Вызов списка модулей осуществляется нажатием пиктограммы Security Vision, расположенной сверху слева. Переход между модулями осуществляется через основное меню модулей (Рисунок 3-2).

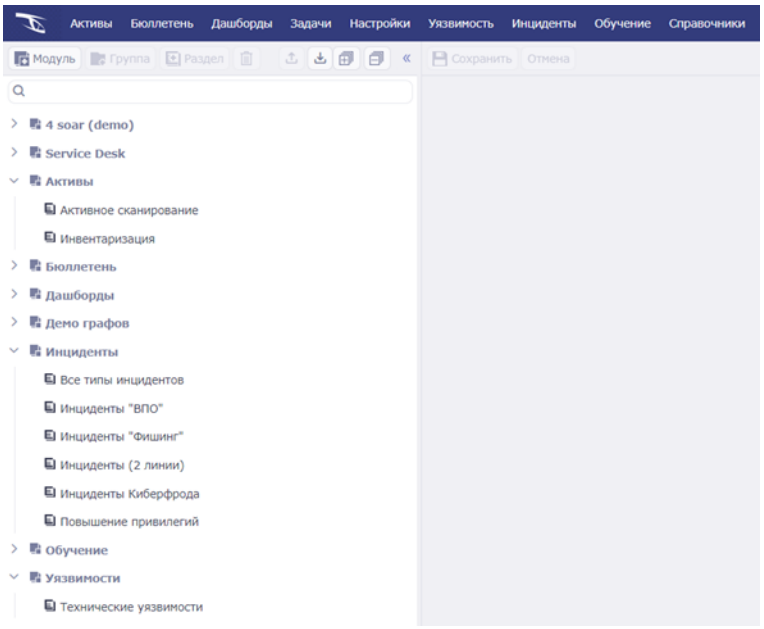


Рисунок 3-2 – Основное меню

В правом верхнем углу страницы Портала отображаются значки ленты уведомлений, карточки текущего пользователя и глобального поиска. Если нажать на имя текущего пользователя, то появится область (Рис. 3-3), в которой можно открыть секции:

- «Лицензия и поддержка» - для просмотра уровня текущей лицензии и даты окончания действия поддержки;
- «Справка» - для открытия секции просмотра справочной информации по Порталу;
- «Обратная связь» – для отправки писем-пожеланий;
- Данные текущего пользователя;
- «Профиль» - редактирование профиля пользователя и редактирование подписки на оповещения;
- «Выход» - для осуществления выхода из Портала;
- Группы – список групп пользователей, в которые входит данный сотрудник.

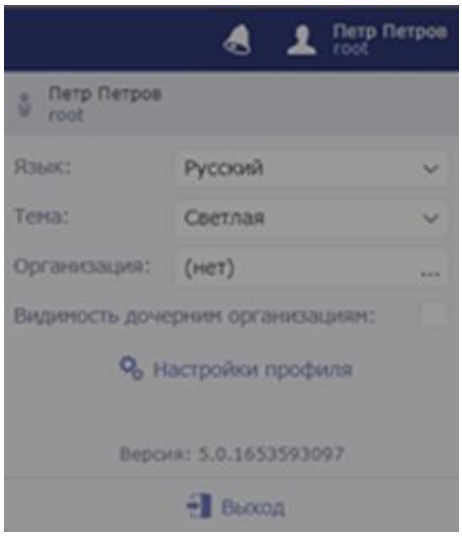


Рис. 3-3 Информация о текущем пользователе

При переходе в редактирование профиля пользователя открывается секция с двумя вкладками

- Данные пользователя (Рис. 3-4);
- Оповещение (Рис. 3-5)

В «Данных пользователя» происходит редактирование параметров учётной записи: ФИО, контактные данные, смена пароля и редактирование фотографии пользователя.

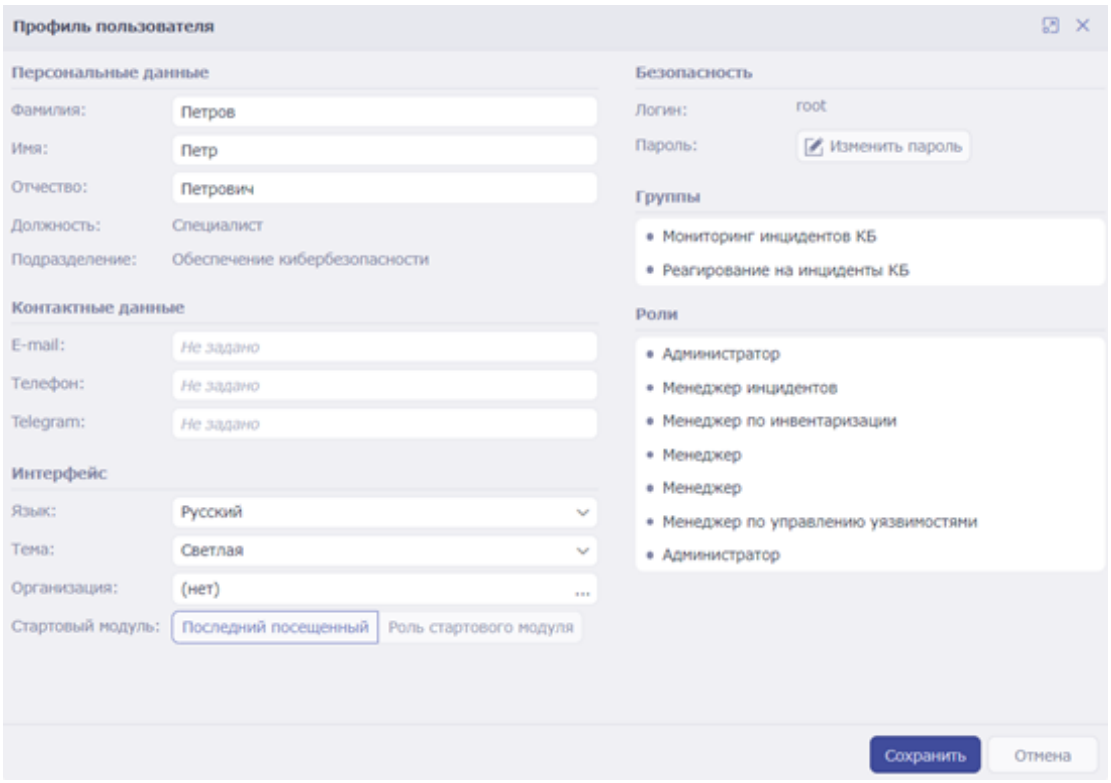


Рис. 3-4 Секция «Данные пользователя»

В «Оповещении» настраивается подписка на события и способы оповещения об этих событиях.

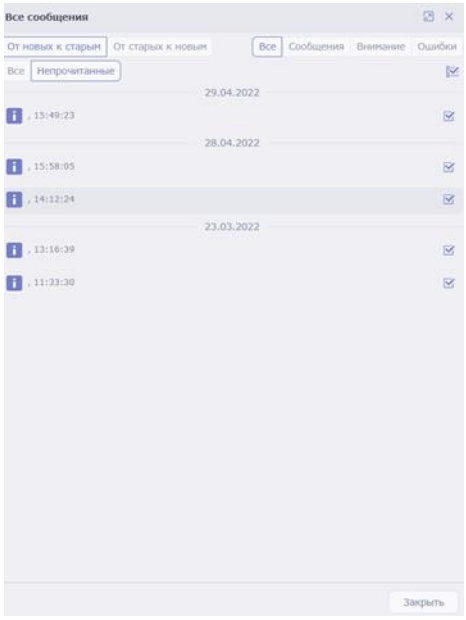


Рис. 3-5 Секция «Оповещение»

3.3 ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

В Таблица 3.1 перечислены основные функции системы и выполняемые в рамках этих функций пользовательские задачи.

Таблица 3.1 – Основные функциональные возможности системы

Задача	Описание
Управление активами	
Активное сканирование	Данная функция позволяет автоматизировать процесс инвентаризации активов и построения карты активов
Идентификация нераспознанного объекта	
Категорирование активов	
Прохождение жизненного цикла	
Обогащение сведений по активу	
Управление уязвимостями	
Загрузка CVE, БДУ ФСТЭК и бюллетеней Microsoft	Данная функция позволяет автоматизировать процесс аналитики существующих уязвимостей и процедур по устранению.
Настройка подтверждения выполнения заявки на устранение	
Настройка внешних сервисов Service Desk	
Настройка политики устранения	
Включение политики устранения	
Настройка аналитических сервисов	
Сканирование уязвимостей	
Управление жизненным циклом инцидентов информационной безопасности	
Регистрация инцидента информационной безопасности	Данная функция позволяет автоматизировать процесс обработки инцидента информационной безопасности.
Определение контекста инцидента	
Назначение ответственного за инцидент	
Контроль процесса обработки инцидента информационной безопасности	
Импорт и экспорт данных	
Экспорт данных	
Импорт данных	

3.3.1 Описание функции «Управление активами».

Данная функция позволяет автоматизировать процесс инвентаризации активов и построения карты активов.

В главном меню в зависимости от роли пользователю доступны следующие разделы модуля:

- Активы — модуль с доступом ко всем настройкам сканирования, идентификации и инвентаризации.
- Мои активы — раздел с перечнем активов, закрепленных за определенным владельцем.

Модуль «Активы» предназначен для работы с активами организации (просмотра, создания и редактирования). Внешний вид меню модуля «Активы» представлен на рисунке 3-6.

В разделе «Активы» отображается перечень активов и интерфейс взаимодействия с ними.

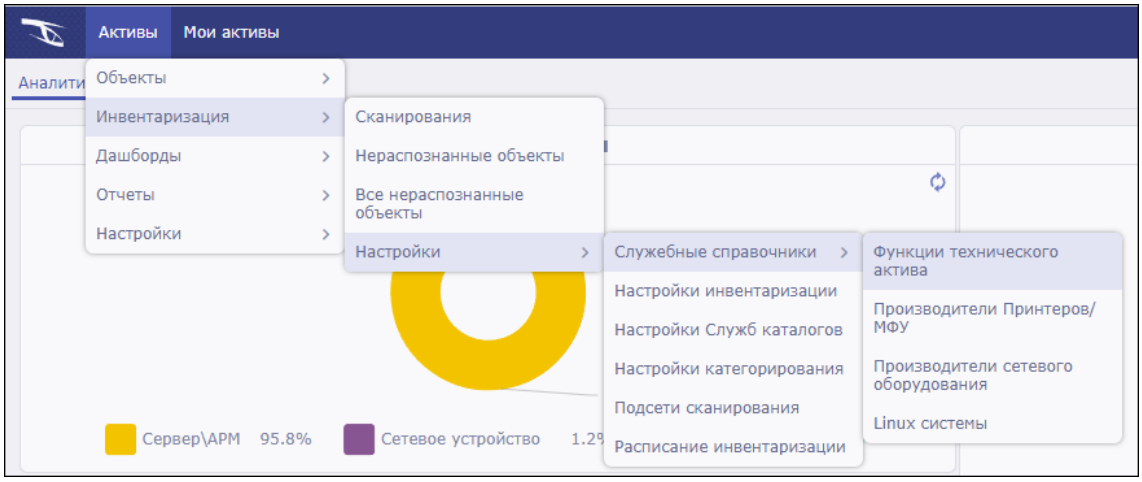


Рисунок 3-6 – Внешний вид вкладки "Активы"

3.3.1.1 Активное сканирование

Активное сканирование выполняет поиск активов в определенной подсети. Информация о сканируемой подсети выбирается из справочника. По каждой записи в справочнике запускается рабочий процесс по сканированию. Данный рабочий процесс запускается автоматически по расписанию или, при необходимости, вручную. Перед сканированием следует добавить подсети в раздел модуля — см. пояснение ниже в разделе Подготовка к сканированию.

3.3.1.1.1 Подготовка к сканированию

Перед сканированием следует добавить целевую подсеть в раздел **Активы → Инвентаризация → Настройки → Подсети сканирования**.

Чтобы добавить подсеть:

1) Откройте раздел **Активы → Инвентаризация → Настройки → Подсети сканирования**.
2) Нажмите кнопку **Добавить элемент** и заполните форму, как на рисунке ниже. В данной записи указывается диапазон сканируемой сети, тип сканирования и перечень портов SSH, WinRM, HTTP, UDP, TCP. Порты указываются через запятую. Следует указывать все нестандартные порты, используемые для доступа к активам в целевой подсети.
3) После сохранения записи автоматически запустится процесс сканирования.

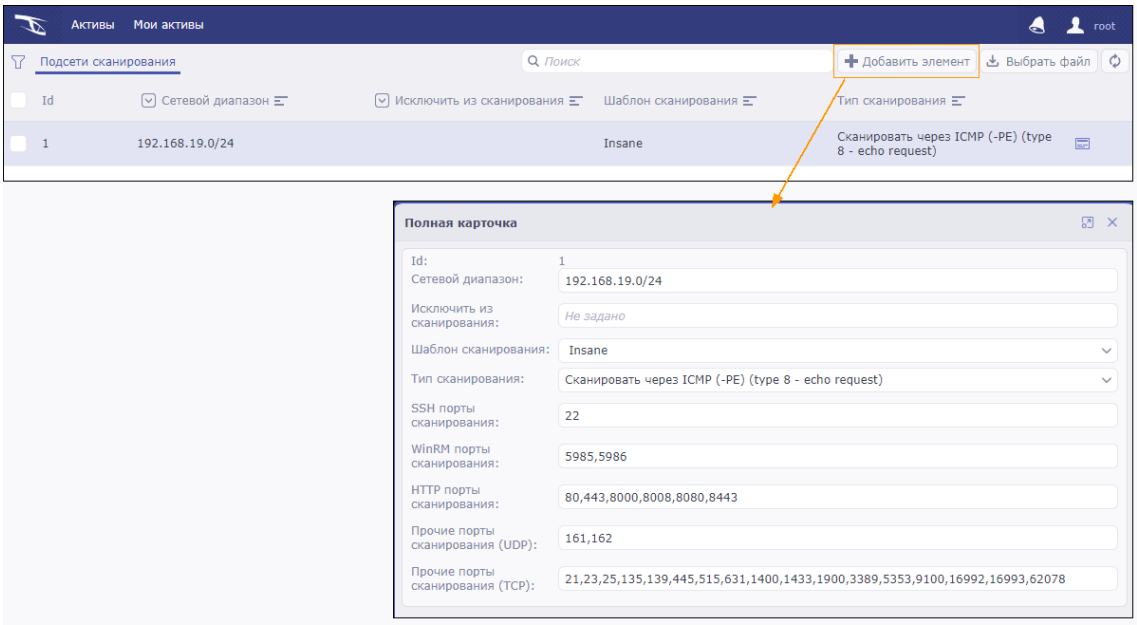


Рисунок 3-7 – Добавление подсети для сканирования

3.3.1.1.2 Процесс сканирования

Порядок активного сканирования следующий:

1) По расписанию *Расписание сетевого сканирования* автоматически запускается рабочий процесс *Создать Сетевое сканирование из справочника*. Расписание доступно для редактирования в разделе **Активы → Инвентаризация → Настройки → Расписание инвентаризации**. Предусмотрена возможность запустить сканирование, не дожидаясь срабатывания рабочего процесса *Создать Сетевое сканирование из справочника* по расписанию. Для этого в расписании нажмите кнопку **Выполнить сейчас**.
2) Рабочий процесс *Создать Сетевое сканирование из справочника* выполняет одну автоматическую транзакцию по созданию объекта *Сетевое сканирование*. Данная транзакция содержит действие *Создать сканирование из справочника*. В результате

работы действия создаются объекты типа *Сетевое сканирование* на базе записей из справочника *Подсети сканирования*: количество создаваемых объектов будет равно количеству записей в справочнике. В создаваемых объектах заполняются свойства: Сетевой диапазон, Тип сканирования, SSH порты, WinRM порты и т.д. Созданные объекты типа *Сетевое сканирование* доступны для просмотра в разделе **Активы → Инвентаризация → Сканирования**.

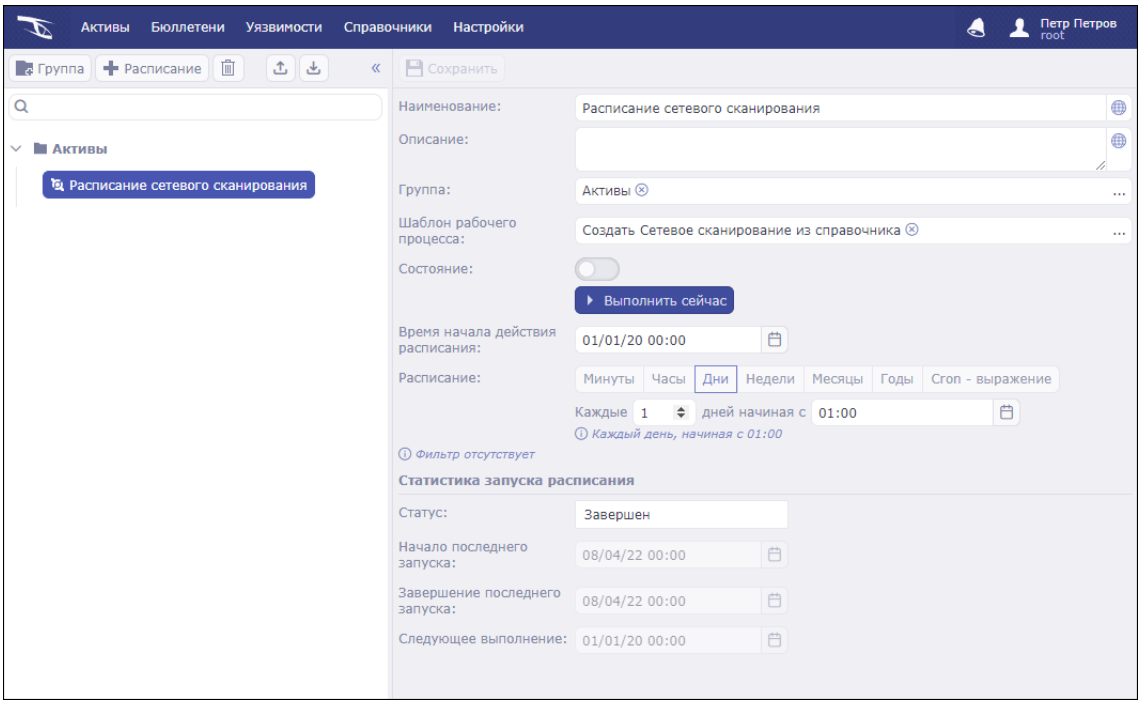


Рисунок 3-8 – Расписание сетевого сканирования

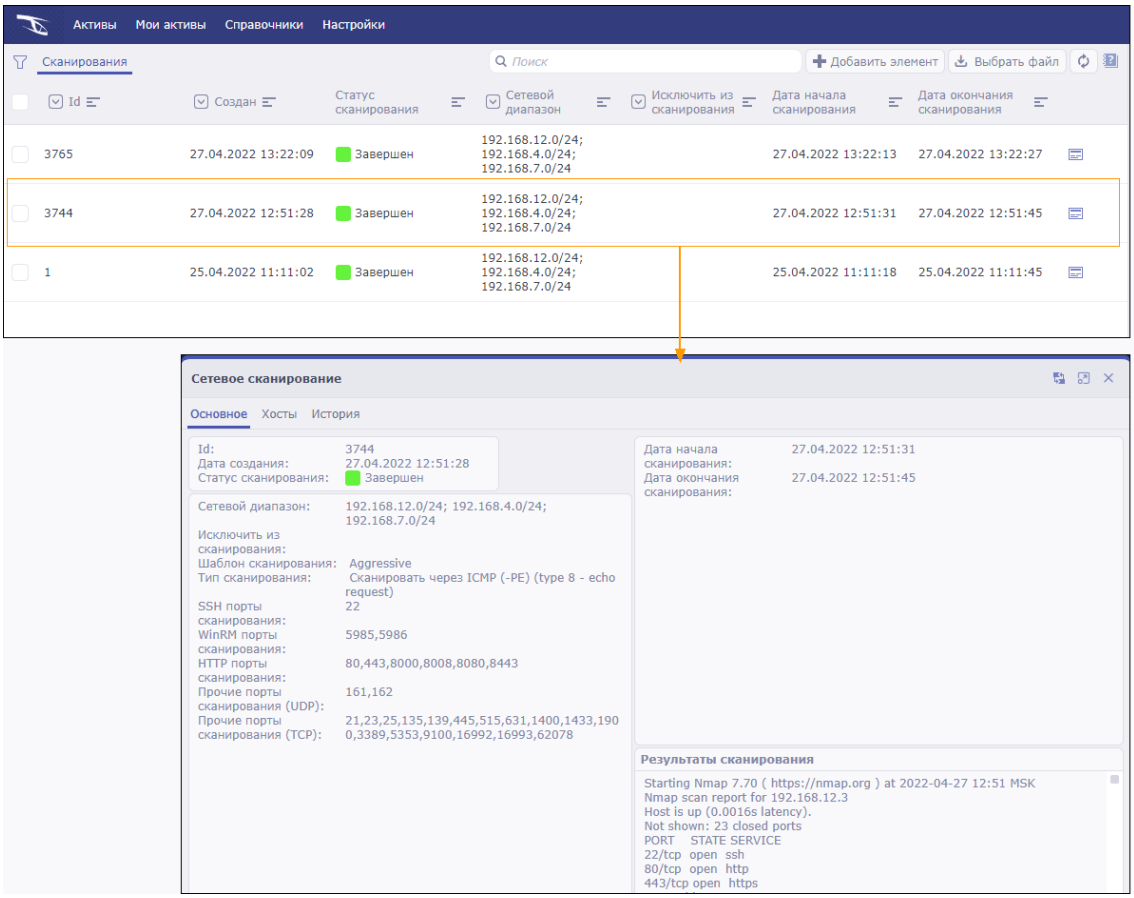


Рисунок 3-9 – Созданные объекты типа Сетевое сканирование

3) Автоматически запускается рабочий процесс *Сканирование подсети* для каждого созданного объекта *Сканирование*. Выполняется сканирование сетевых диапазонов на базе созданных объектов *Сканирования*. В результате сканирования создаются объекты типа *Нераспознанный объект*. Созданные объекты типа *Нераспознанный объект* доступны для просмотра в разделе **Активы → Инвентаризация → Нераспознанные объекты** или в разделе **Активы → Инвентаризация → Все нераспознанные объекты**. В разделе **Нераспознанные объекты** приводятся только те объекты, которые не распознаны на текущий момент. В разделе **Все нераспознанные объекты** приводятся все объекты, которые распознаны и не распознаны.
4) Автоматически запускается рабочий процесс Идентификация нераспознанного объекта для каждого созданного *Нераспознанного объекта*.

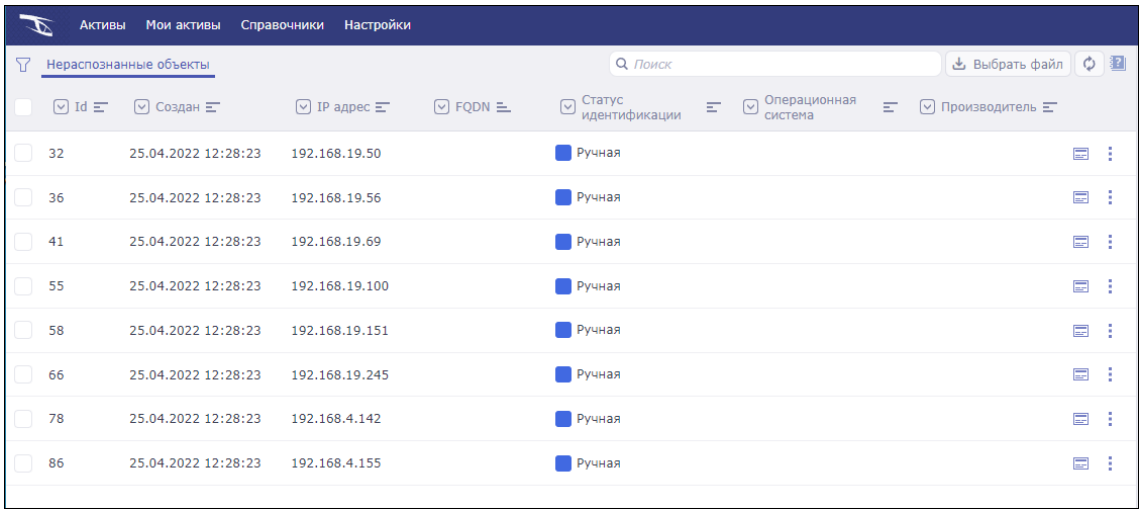


Рисунок 3-10 – Созданные объекты типа Нераспознанный объект

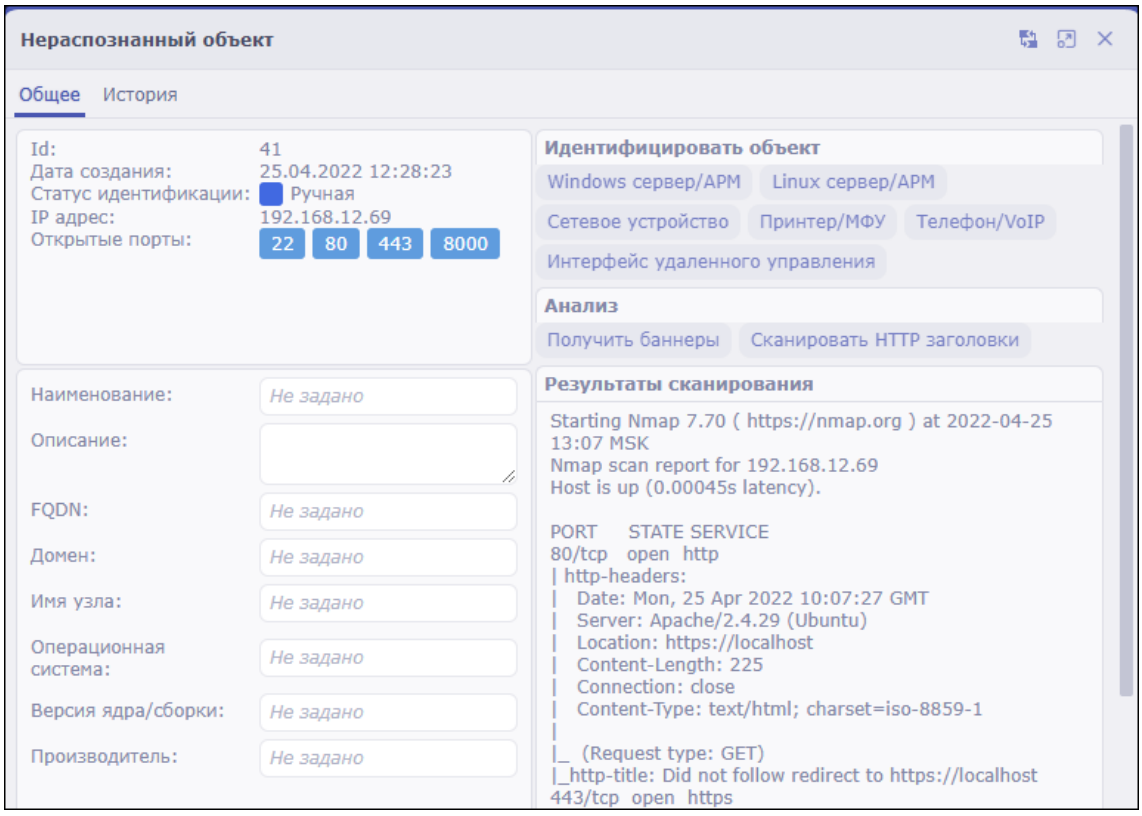


Рисунок 3-11 – Полная карточка объекта типа Нераспознанный объект

3.3.1.2 Идентификация нераспознанного объекта

Данный процесс идентификации автоматически запускается только для нераспознанных объектов, полученных в результате активного сканирования. Предусмотрена возможность идентификации нераспознанного объекта вручную — см. раздел Запуск идентификации вручную.

3.3.1.2.1 Процесс идентификации

Порядок идентификации объекта следующий:

1) Нераспознанный объект проверяется на наличие определенных параметров, по которым идентифицируется объект: определенный порт, имя узла, активная сессия RDP и т.д. Для идентификации некоторых объектов используются предзаполненные служебные справочники.
2) После успешной идентификации автоматически создается объект соответствующего типа: Windows АРМ, Windows сервер, Linux сервер, сетевое устройство, принтер/МФУ, Телефон/VoIP, удаленный интерфейс, другое устройство. В созданные объекты записывается информация, полученная в результате идентификации. Если объект не был идентифицирован автоматически, то в карточке нераспознанного объекта будут доступны кнопки для идентификации объекта вручную. Созданные идентифицированные объекты доступны в группе разделов **Активы → Объекты → Оборудование** (см. ниже рисунок).
3) После идентификации автоматически запускается рабочий процесс Инвентаризация Сервера/АРМ.

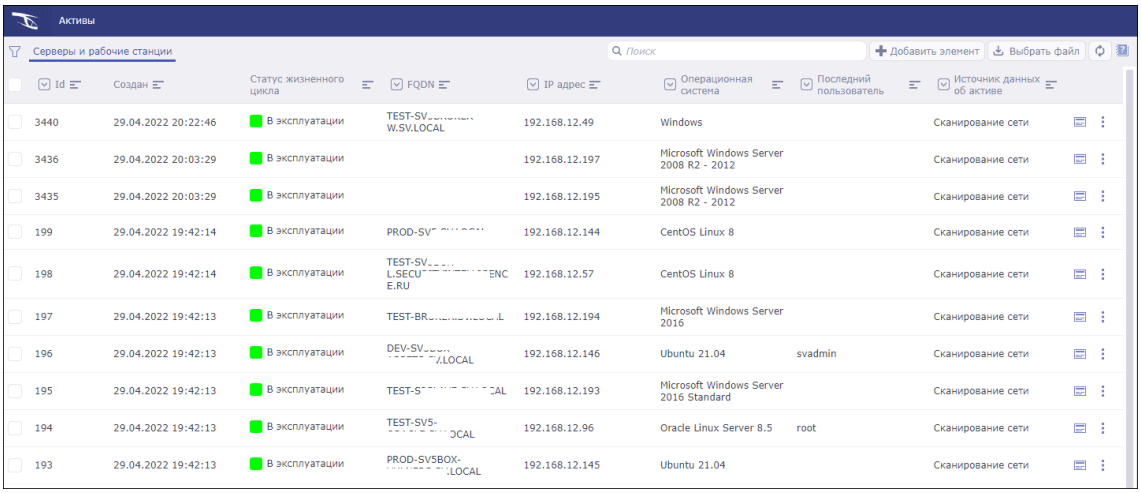


Рисунок 3-12 – Созданные идентифицированные объекты

3.3.1.2.2 Запуск идентификации вручную

Чтобы запустить идентификацию вручную:

1) Откройте раздел **Активы → Инвентаризация → Нераспознанные объекты**.
2) Откройте карточку нераспознанного объекта.
3) Нажмите соответствующую кнопку для идентификации объекта в качестве Windows сервер, Linux сервер и т.д. Кнопки **Получить баннеры** и **Сканировать HTTP заголовки** предназначены для получения данных из баннеров или HTTP-заголовков для последующей идентификации активов. После нажатия на кнопку следует указать

порты, которые необходимо сканировать. Порты следует вводить через запятую. Примеры идентификации по баннерам и HTTP-заголовкам:

— В полученных баннерах выполняется поиск ключевого слова *win** или *ubuntu*, на основании которого идентифицируется сервер или АРМ под управлением ОС семейства Windows или Linux. Найденное ключевое слово сравнивается со значениями из служебного справочника Linux системы.

— В полученных HTTP-заголовках выполняется поиск ключевого слова *IIS* или *NGINX*, на основании которого идентифицируется сервер под управлением ОС семейства Windows или Linux.

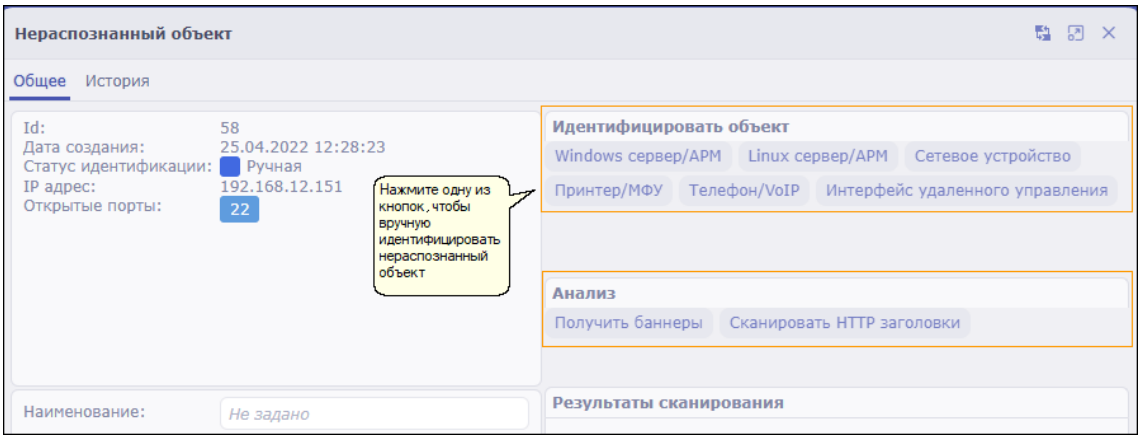


Рисунок 3-13 – Запуск идентификации вручную

3.3.1.3 Категорирование активов

Категорирование активов выполняется автоматически по предзаполненному справочнику **Настройки категорирования**. Категория актива определяется по его IP-адресу. В записи справочника указывается начало и конец диапазона IP-адресов и соответствующие ему категории по следующим признакам: *Конфиденциальность, Целостность, Доступность, Критичность*. Таким образом, при вхождении IP-адреса актива в определенный диапазон автоматически определяется его категория по справочнику.

Категорирование актива вручную выполняет пользователь с полномочиями роли *Владелец системы*. Категория указывается на вкладке **Бизнес-параметры** в карточке актива — см. ниже раздел Просмотр детальной информации.

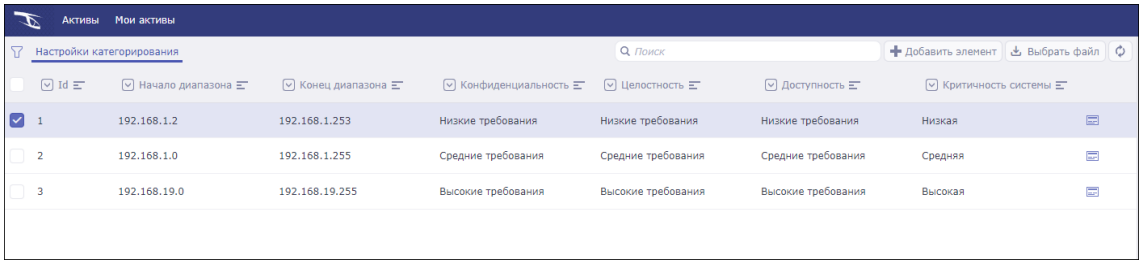


Рисунок 3-14 – Справочник Настройки категорирования

3.3.1.4 Прохождение жизненного цикла

После инвентаризации и категорирования актив проходит жизненный цикл по следующим этапам: *Новый, На категорировании, В эксплуатации, Сломан, В ремонте, На складе, Выведен из эксплуатации*. Жизненный цикл актива проходит по рабочему процессу *Жизненный цикл устройства*, расположенному в группе **Активы**, подгруппе **Жизненный цикл**.

Чтобы установить этап жизненного цикла в активе:

1) Откройте карточку актива, в котором следует установить определенный этап жизненного цикла. Инвентаризированные активы доступны в группе разделов **Активы → Объекты → Оборудование**;
2) На вкладке **Основные** нажмите на кнопку перевода актива на следующий этап.

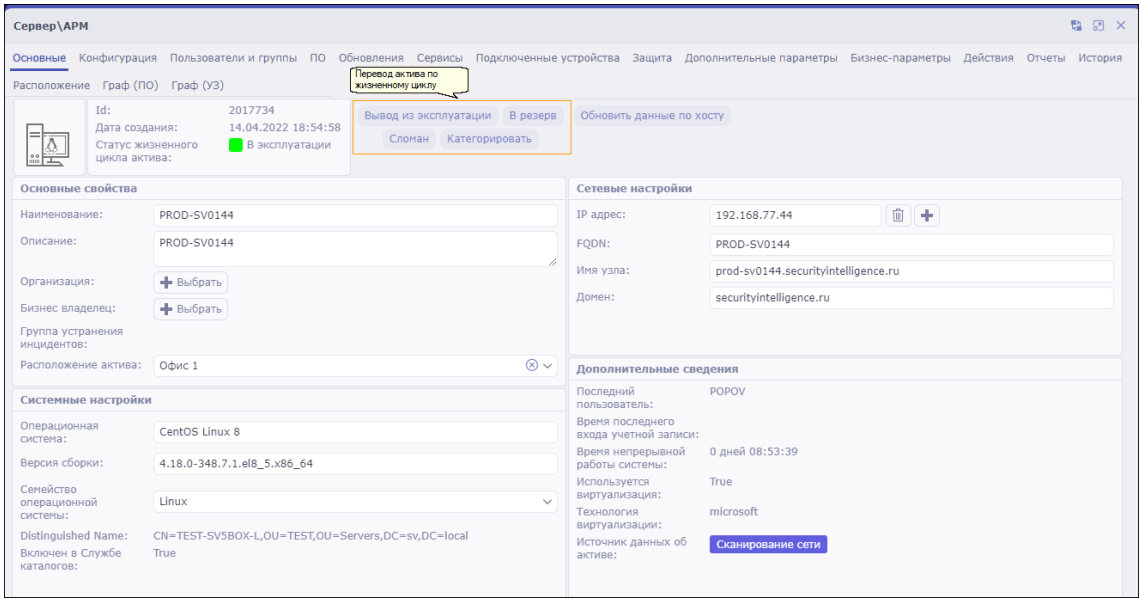


Рисунок 3-15 – Установка этапа жизненного цикла актива

3.3.1.5 Обогащение активов

Предусмотрена возможность вручную запустить обогащение данных по активу из его полной карточки:

- Данные по хосту
- Данные по конфигурации (ЦПУ и оперативная память)
- Данные по учетным записям пользователей
- Данные о программном обеспечении
- Дополнительные параметры

Инвентаризированные активы доступны в группе разделов **Активы** → **Объекты** → **Оборудование**.

Автоматическое обогащение данных активов выполняется только при сканировании объектов из внешних источников — см. раздел Получение данных из внешних источников.

3.3.1.5.1 Данные по хосту

Обновление данных по хосту запускается в полной карточке объекта на вкладке **Основные**. Обновляются данные по сетевым настройкам актива, системным настройкам и пользовательских сессиях.

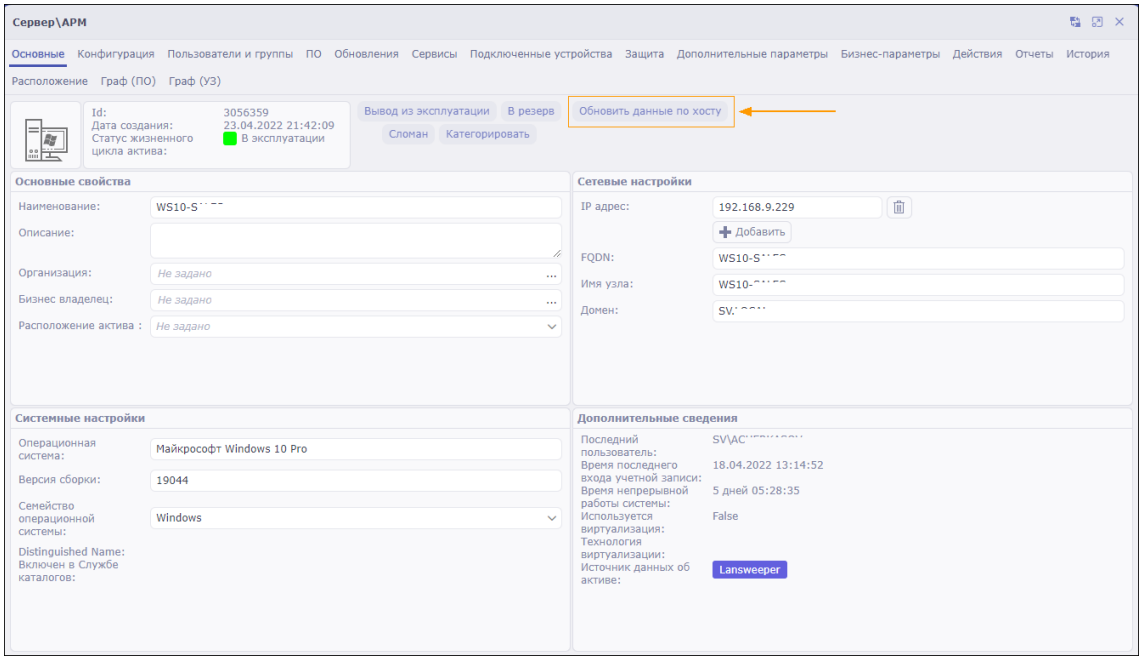


Рисунок 3-16 – Запуск обновления данных по хосту

3.3.1.5.2 Данные по конфигурации

Обновление данных по конфигурации актива запускается в полной карточке объекта на вкладке **Конфигурация**. Обновляются данные по текущей загрузке центрального процессора и оперативной памяти актива, а также данные по жестким дискам, сетевым интерфейсам. После инвентаризации данные по загрузке центрального процессора и оперативной памяти не заполняются, так как параметры имеют динамическое значение.

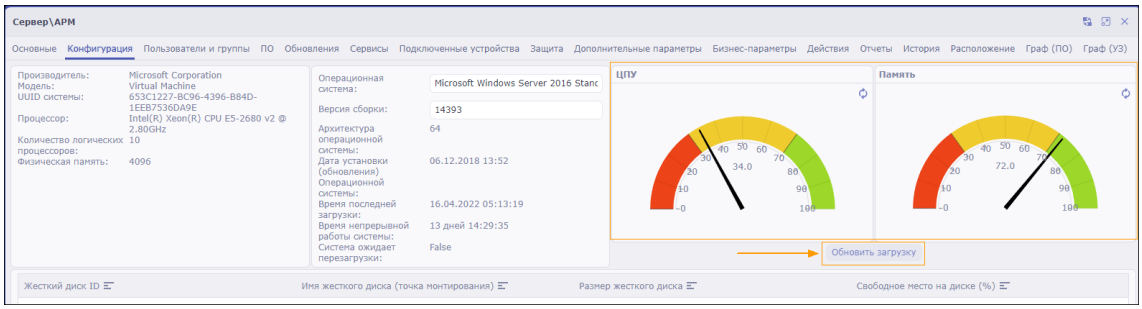


Рисунок 3-17 – Запуск обновления данных по конфигурации актива

3.3.1.5.3 Данные по учетным записям пользователей

Обновление данных об учетных записях пользователей актива запускается в полной карточке объекта на вкладке **Пользователи и группы**.

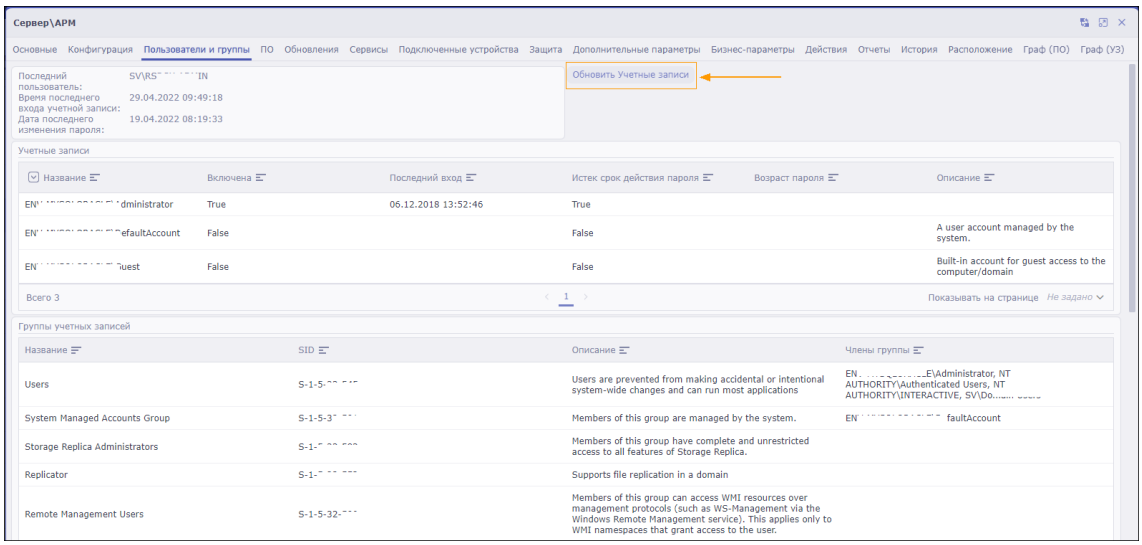


Рисунок 3-18 – Запуск обновления данных об учетных записях пользователей актива

3.3.1.5.4 Данные о программном обеспечении

Обновление данных по установленному программному обеспечению актива запускается в полной карточке объекта на вкладке **ПО**.

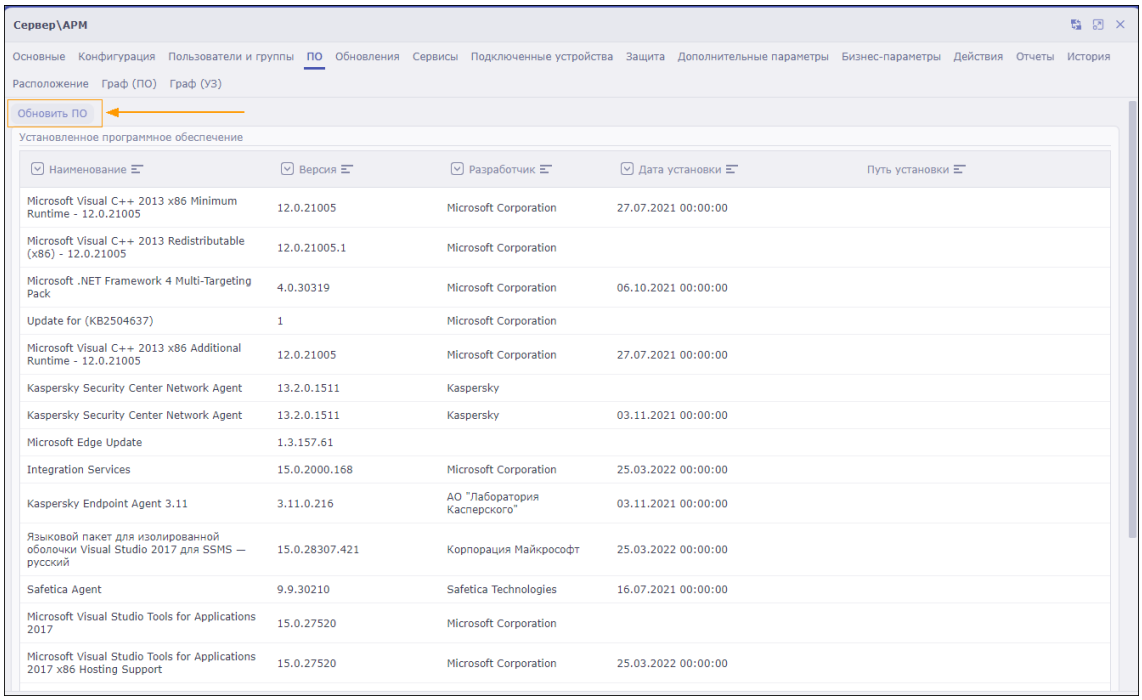


Рисунок 3-19 – Запуск обновления данных о ПО актива

3.3.1.5.5 Дополнительные параметры

Обновление данных по сетевым портам актива запускается в полной карточке объекта на вкладке **Дополнительные параметры**. Обновляются данные по портам актива, а также данные о локализации и часовом поясе актива.

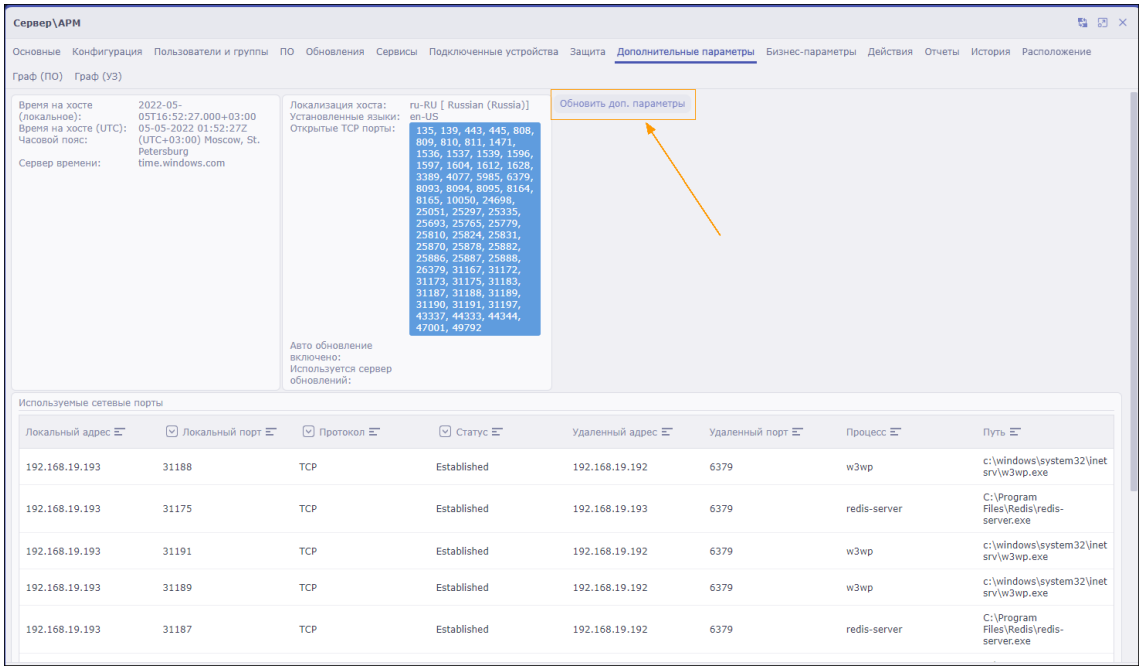


Рисунок 3-20 – Запуск обновления данных о дополнительных параметрах актива

3.3.2 Описание функции «Управление уязвимостями».

3.3.2.1 Загрузка CVE, БДУ ФСТЭК и бюллетеней Microsoft

Перед запуском получения данных по уязвимостям следует загрузить в Модуль CVE и бюллетени из БДУ ФСТЭК, баз NVD и Microsoft. Бюллетени и CVE выгружаются автоматически по расписанию. Преднастроенные расписания доступны для редактирования в разделе **Уязвимости → Настройки → Расписание загрузки данных**. Выгруженные CVE и бюллетени будут доступны в разделах **Уязвимости → Бюллетени → Бюллетени обновлений безопасности, Уязвимости → Технические уязвимости → Уязвимость CVE/Уязвимость БДУ ФСТЭК**. Выгруженные CVE и бюллетени будут привязываться к соответствующей уязвимости, выгруженной из внешнего источника (сканера уязвимостей).

Чтобы вручную запустить загрузку:

1) Откройте раздел **Уязвимости → Настройки → Расписание загрузки данных**.
2) Выберите необходимое расписание: *Загрузка бюллетеней (полная), Загрузка бюллетеней (API), CVE и БДУ ФСТЭК.*
3) Нажмите кнопку **Выполнить сейчас**. В модуль загрузятся актуальные CVE и бюллетени из внешних баз.

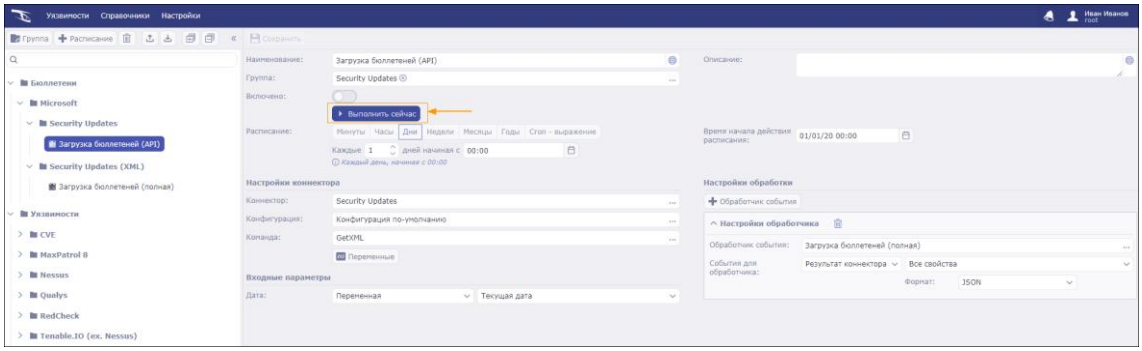


Рисунок 3-21 – Расписание для загрузки бюллетеней Microsoft

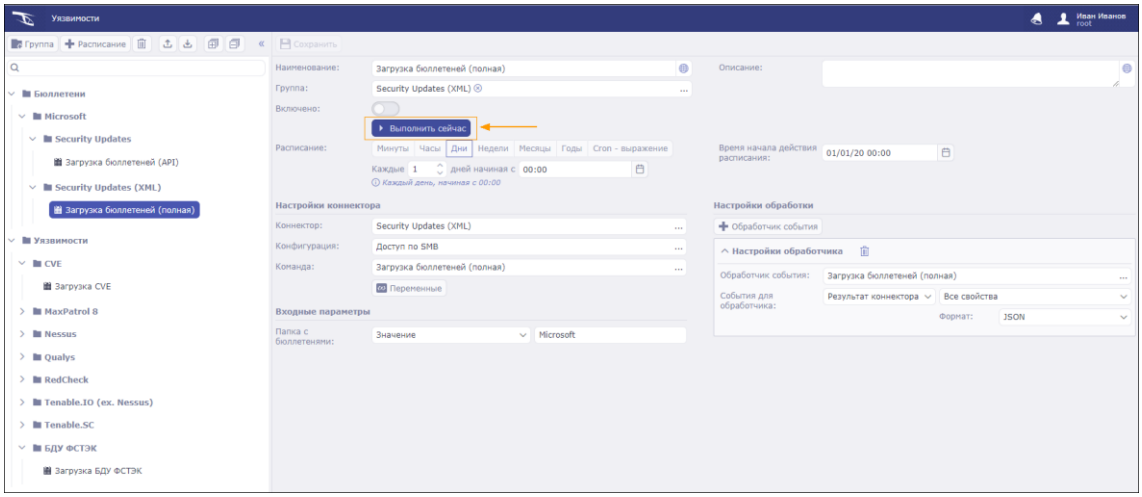


Рисунок 3-22 – Расписание для загрузки бюллетеней Microsoft

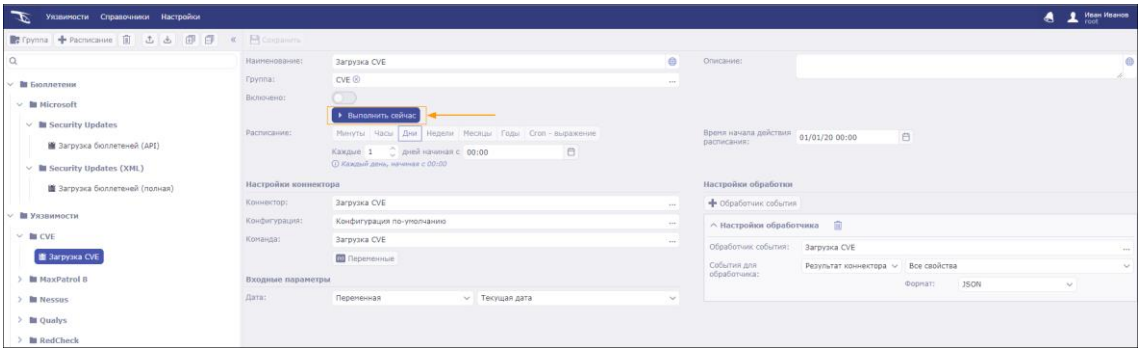


Рисунок 3-23 – Расписание для загрузки CVE

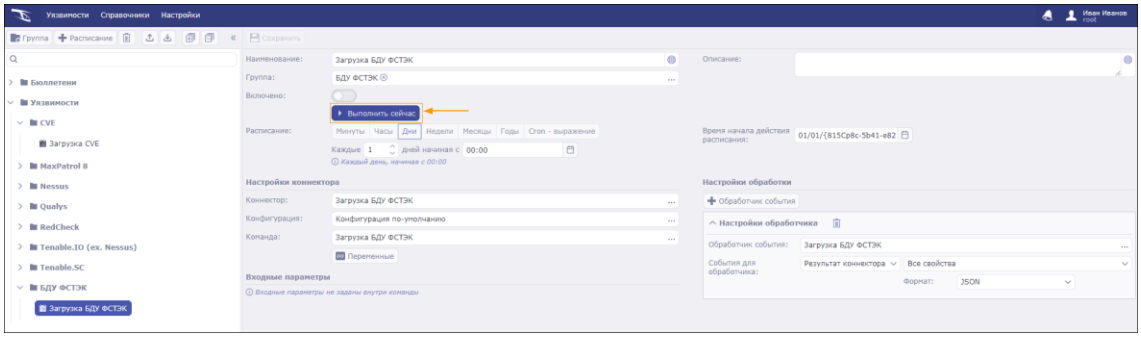
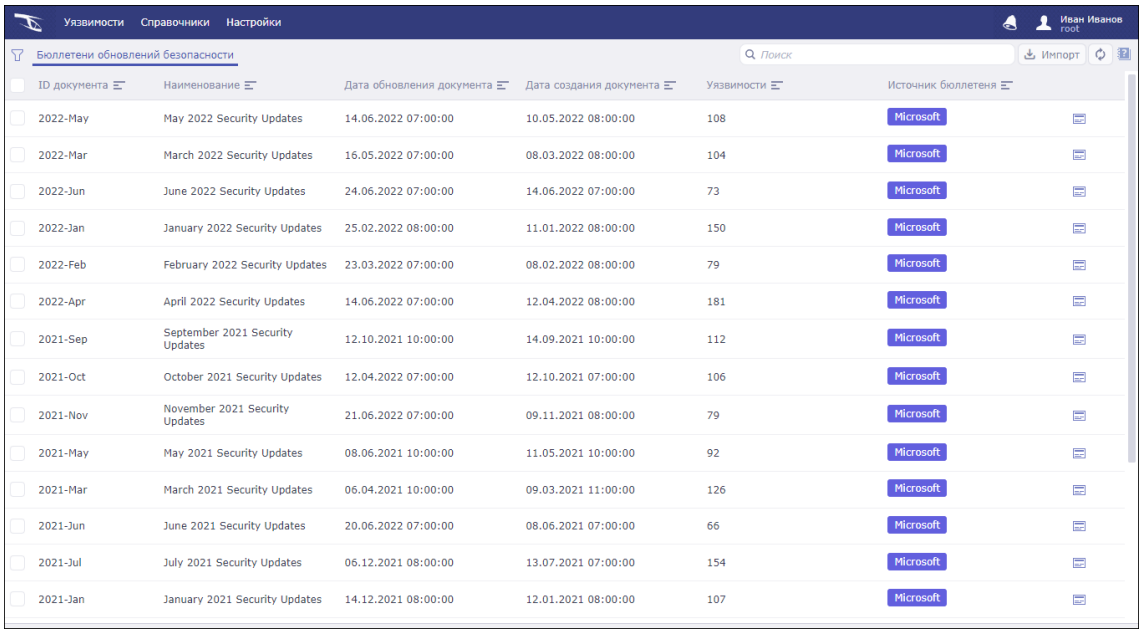


Рисунок 3-24 – Расписание для загрузки БДУ ФСТЭК

3.3.2.1.1 Бюллетени Microsoft

В разделе **Уязвимости → Бюллетени → Бюллетени обновлений безопасности** приводится перечень выгруженных бюллетеней из базы Microsoft. Из карточки бюллетеня доступны уязвимости, которые описываются в рамках данного бюллетеня, и продукты, которые подвержены данным уязвимостям. Из карточки уязвимости доступны соответствующие продукты, угрозы, оценки, исправления. Перечень выгруженных из базы Microsoft исправлений доступен в разделе **Уязвимости → Бюллетени → Исправления**.



ID документа	Наименование	Дата обновления документа	Дата создания документа	Уязвимости	Источник бюллетеня
2022-May	May 2022 Security Updates	14.06.2022 07:00:00	10.05.2022 08:00:00	108	Microsoft
2022-Mar	March 2022 Security Updates	16.05.2022 07:00:00	08.03.2022 08:00:00	104	Microsoft
2022-Jun	June 2022 Security Updates	24.06.2022 07:00:00	14.06.2022 07:00:00	73	Microsoft
2022-Jan	January 2022 Security Updates	25.02.2022 08:00:00	11.01.2022 08:00:00	150	Microsoft
2022-Feb	February 2022 Security Updates	23.03.2022 07:00:00	08.02.2022 08:00:00	79	Microsoft
2022-Apr	April 2022 Security Updates	14.06.2022 07:00:00	12.04.2022 08:00:00	181	Microsoft
2021-Sep	September 2021 Security Updates	12.10.2021 10:00:00	14.09.2021 10:00:00	112	Microsoft
2021-Oct	October 2021 Security Updates	12.04.2022 07:00:00	12.10.2021 07:00:00	106	Microsoft
2021-Nov	November 2021 Security Updates	21.06.2022 07:00:00	09.11.2021 08:00:00	79	Microsoft
2021-May	May 2021 Security Updates	08.06.2021 10:00:00	11.05.2021 10:00:00	92	Microsoft
2021-Mar	March 2021 Security Updates	06.04.2021 10:00:00	09.03.2021 11:00:00	126	Microsoft
2021-Jun	June 2021 Security Updates	20.06.2022 07:00:00	08.06.2021 07:00:00	66	Microsoft
2021-Jul	July 2021 Security Updates	06.12.2021 08:00:00	13.07.2021 07:00:00	154	Microsoft
2021-Jan	January 2021 Security Updates	14.12.2021 08:00:00	12.01.2021 08:00:00	107	Microsoft

Рисунок 3-25 – Перечень выгруженных бюллетеней Microsoft

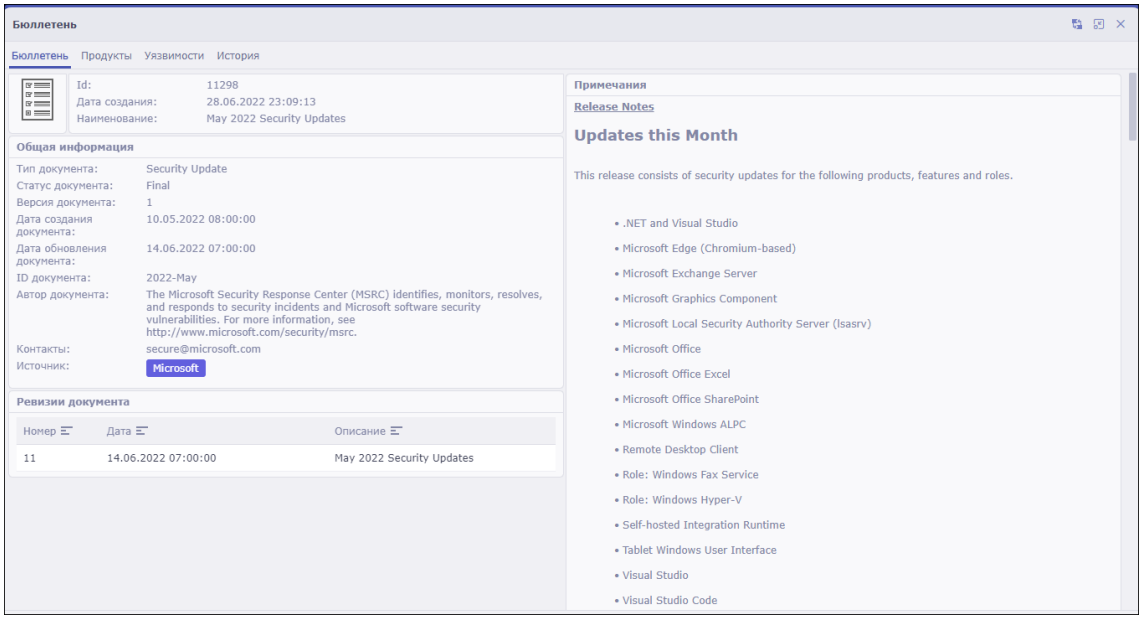


Рисунок 3-26 – Карточка бюллетеня Microsoft

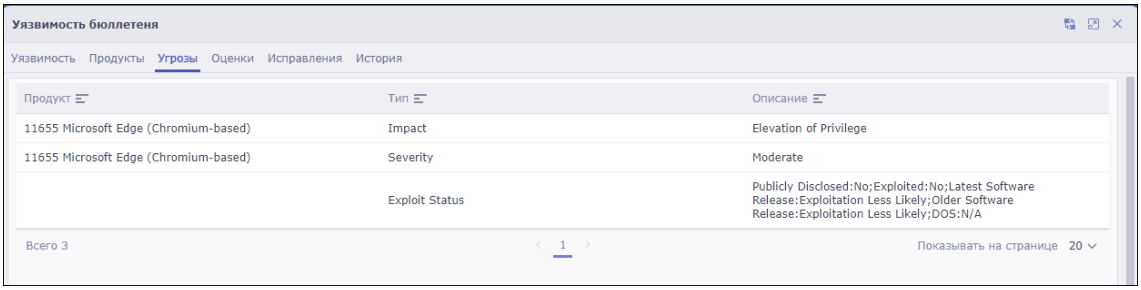


Рисунок 3-27 – Карточка уязвимости. Угрозы

3.3.2.2 Настройка подтверждения выполнения заявки на устранение

Настройка позволяет вычислять плановую дату подтверждения выполнения заявки. В зависимости от настройки к дате решения будет добавляться определенный срок подтверждения. Таким образом будет вычисляться плановая дата подтверждения выполненной заявки.

Чтобы настроить срок подтверждения:

1) Откройте раздел **Уязвимости → Настройки → Настройки подтверждения заявок**;
2) Откройте преднастроенную запись настроек подтверждения заявок и укажите необходимое значение в поле **Срок подтверждения при наличии отчета о сканировании** (см. ниже рисунок). Указанная дата будет добавляться к дате решения заявки.

В результате в выполненных заявках будет отображаться актуальная плановая дата подтверждения.

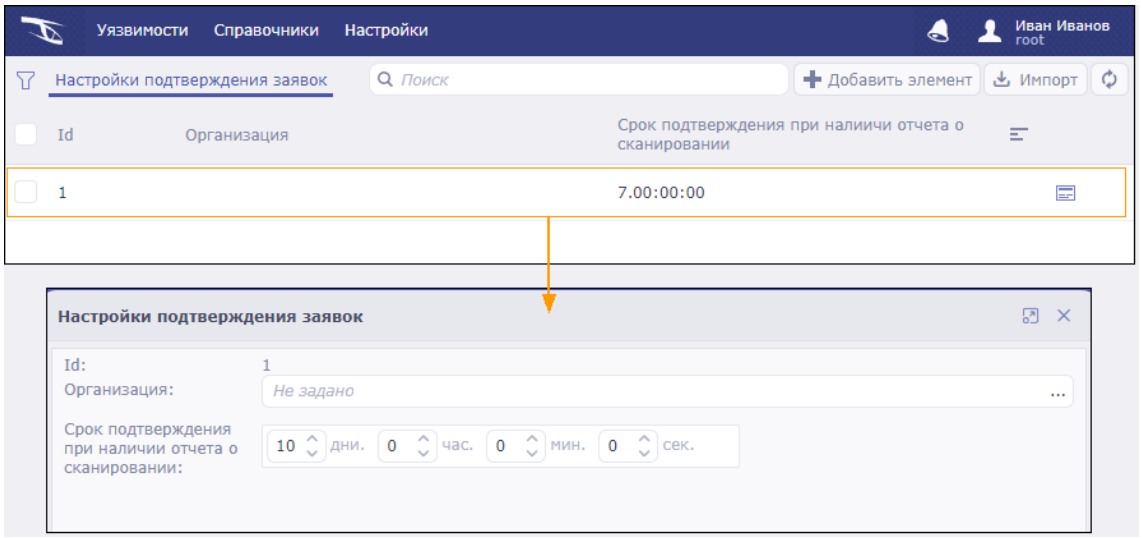


Рисунок 3-28 – Настройка подтверждения заявок

3.3.2.3 Настройка внешних сервисов Service Desk

Интеграция с внешними сервисами Service Desk позволяет автоматически создавать задачи на устранение в сторонних сервисах и отслеживать статус их выполнения. Таким образом при создании в Модуле заявки на устранение автоматически будет создаваться заявка во внешнем сервисе Jira.

Чтобы настроить сервис Service Desk:

1) Откройте раздел **Настройки → Коннекторы → Коннекторы**;
2) Раскройте группу *Service Desk* и выберите коннектор *Jira*;
3) Откройте конфигурацию подключения и укажите настройки по аналогии: введите адрес сервера Jira, логин и пароль;
4) Откройте раздел **Уязвимости → Настройки → Настройки внешних сервисов Service Desk**;
5) Откройте преднастроенную запись настройки сервиса.
6) Укажите следующие параметры:

— *Название внешнего сервиса* — наименование сервиса, в котором будут создаваться заявки.

— *ID группы реагирования* — название проекта в Jira, в рамках которого будут создаваться заявки в Jira.

— *Признак Включен* — если признак включен, то во внешнем сервисе Jira будет автоматически создаваться задача по каждой заявке, созданной в Модуле. Если признак выключен, то заявки не будут создаваться во внешнем сервисе.

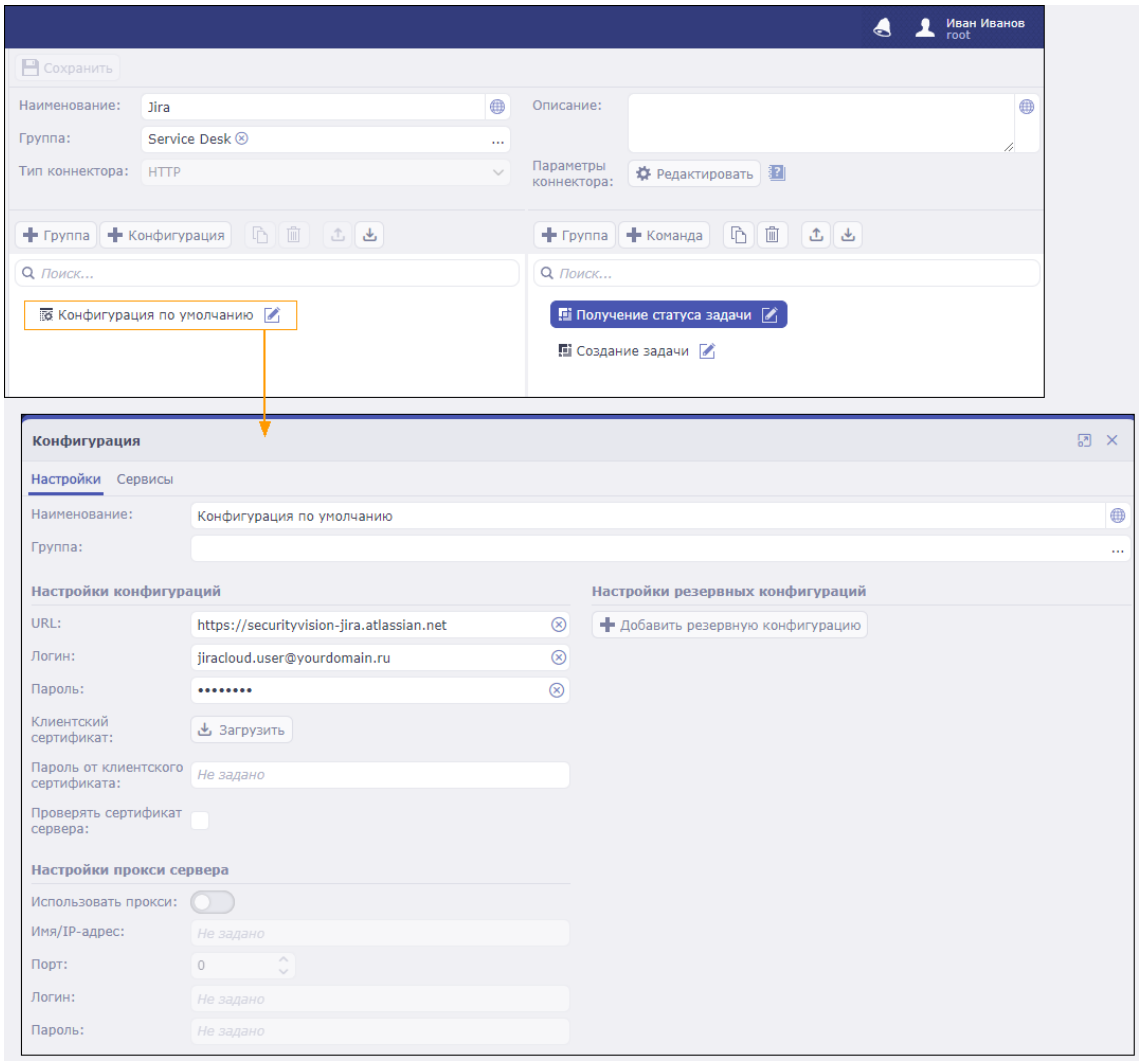


Рисунок 3-29 – Настройка подключения к сервису Service Desk

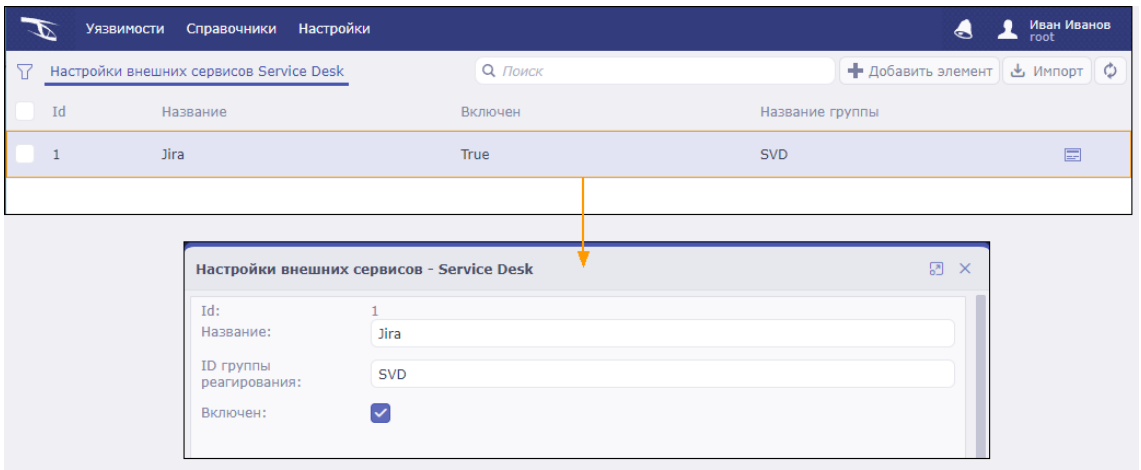


Рисунок 3-30 – Включение сервиса Service Desk

3.3.2.4 Настройка политики устранения

Политика устранения определяет SLA в заявке на устранение уязвимости.

Пользователю доступны следующие политики устранения:

— Вручную — значение SLA будет устанавливаться в карточку заявки на устранение вручную пользователем.
— CVSS + Параметры актива — значение SLA будет автоматически устанавливаться в карточку заявки на устранение на базе данных из записей раздела **Настройки политики устранения уязвимостей (CVSS + Актив)**.
— Дерево решений — значение SLA будет автоматически устанавливаться в карточку заявки на устранение посредством запуска определенных транзакций рабочего процесса.

Перед использованием политики устранения следует выполнить следующие действия:

1) Выбрать одну из политик устранения — см. выше доступные политики.
2) Настроить выбранную политику устранения — см. разделы Настройка политики устранения — CVSS + Актив и Настройка политики устранения — Дерево решений.
3) Включить политику устранения для последующего применения — см. раздел Включение политики устранения.

3.3.2.4.1 Политика устранения — CVSS + Актив

Политика устранения уязвимости реализуется посредством установки определенного SLA в карточку уязвимости. Пользователю доступна возможность настройки политики устранения CVSS + Актив.

Чтобы настроить политику устранения:

1) Перейдите в раздел **Уязвимости → Настройки → Настройки политики устранения уязвимостей (CVSS + Актив)**;
2) Укажите следующие параметры в карточке каждого правила: *CVSS Score*, *Конфиденциальность*, *Доступность*, *Целостность*, *Критичность*, *Приоритет правила*;
3) Сохраните изменения. Таким образом настроена политика создания заявок на устранение с определенным SLA.

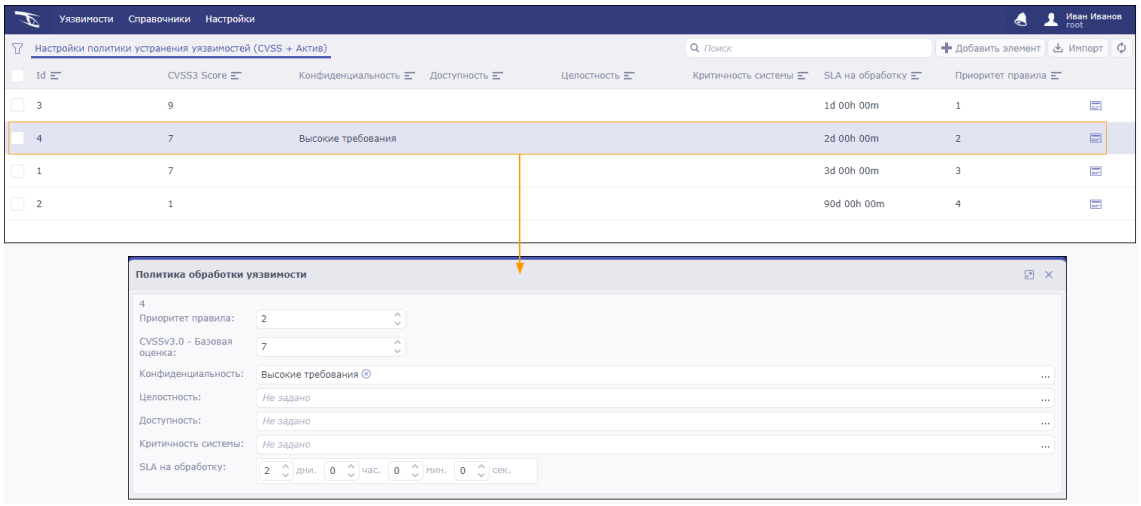


Рисунок 3-31 – Настройки политики устранения уязвимостей (CVSS+Актив)

3.3.2.4.2 Политика устранения — Дерево решений

Политика устранения уязвимости реализуется посредством установки определенного SLA в карточку уязвимости. Для реализации данной политики следует настроить шаблон рабочего процесса *Политика устранения - Дерево решений*. Все транзакции шаблона рабочего процесса автоматические. При срабатывании условий перехода выполняется соответствующая транзакция. В результате выполнения транзакции устанавливается определенный SLA в карточку уязвимости.

Чтобы настроить политику устранения:

1) Перейдите в раздел **Настройки → Рабочие процессы → Шаблоны рабочих процессов**;
2) В корне группы *Уязвимости* выберите рабочий процесс *Политика устранения - Дерево решений*;
3) Отредактируйте транзакции рабочего процесса: укажите условия перехода и заполните действия *Установить SLA* в каждой транзакции. Также можно добавить свои транзакции — см. руководство администратора, раздел Рабочие процессы.

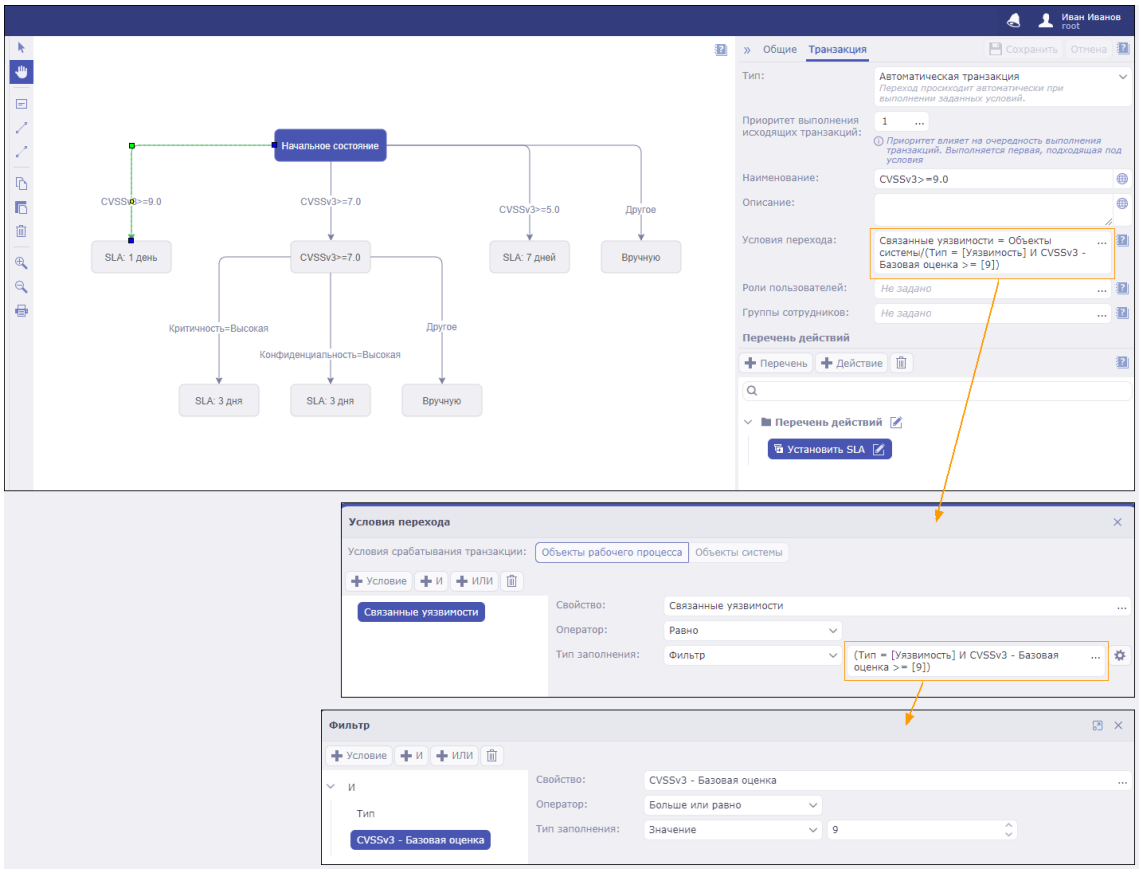


Рисунок 3-32 – Шаблон рабочего процесса для реализации политики устранения

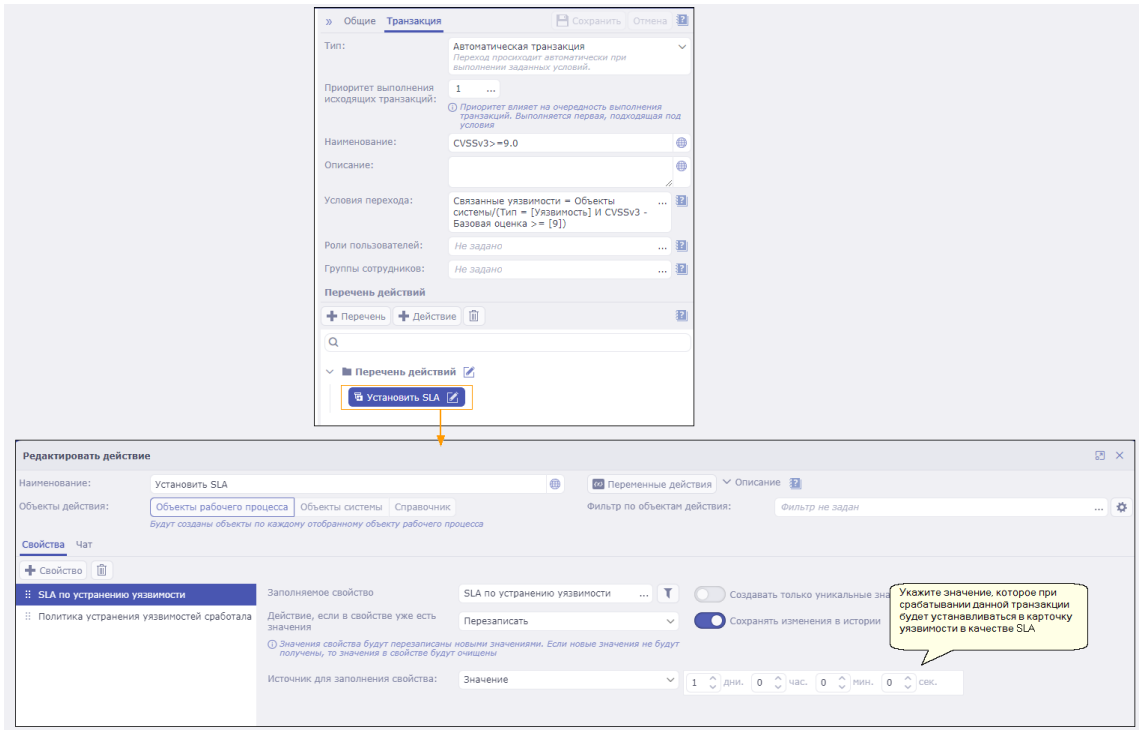


Рисунок 3-33 – Настройки действия Установить SLA

3.3.2.5 Включение политики устранения

Чтобы одна из настроенных политик (Политика устранения уязвимостей (CVSS + Актив), Политика устранения - Дерево решений, Вручную) применялась ко всем создаваемым заявкам на устранение следует ее включить в соответствующем разделе Модуля.

Чтобы применить политику устранения:

1) Открыть раздел **Уязвимости → Настройки → Политика устранения уязвимостей**;
2) Выбираем политику в одноименном поле: например, указываем политику устранения — *CVSS+Параметры актива*;
3) Таким образом для всех заявок на устранение будет применяться данная политика устранения — *CVSS+Параметры актива*.

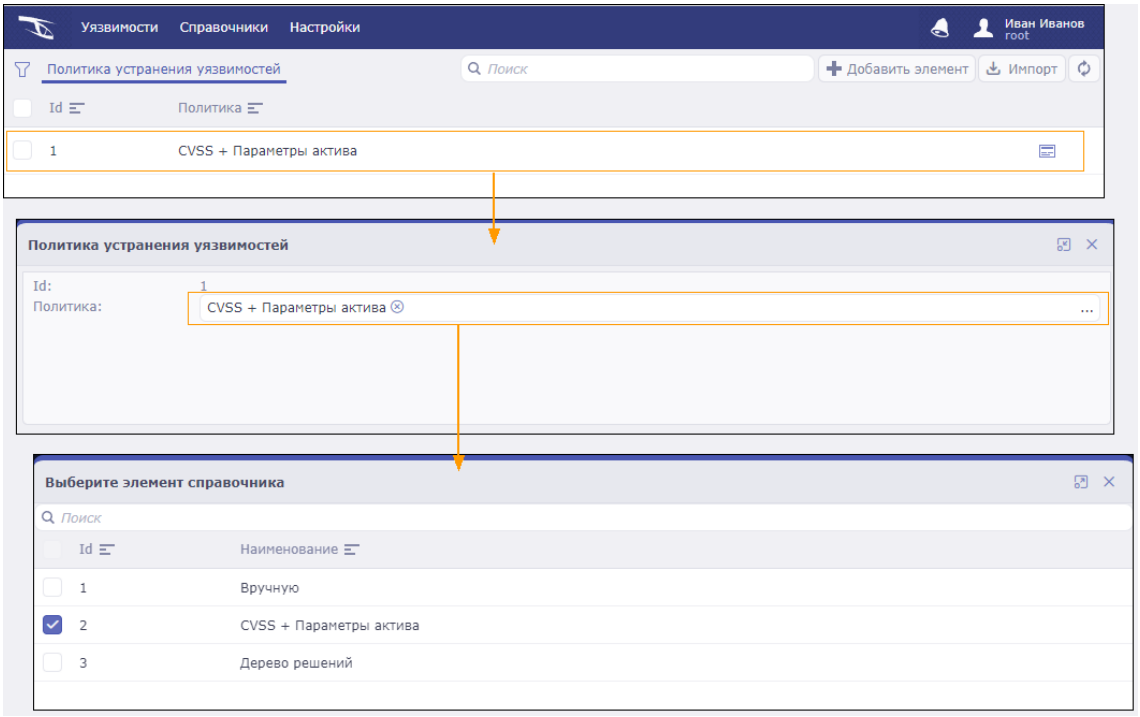


Рисунок 3-34 – Включение определенной политики устранения

3.3.2.6 Настройка аналитических сервисов

Аналитические сервисы используются для более глубокого анализа уязвимости. По нажатию кнопки **Обновить данные из внешних источников** в карточке уязвимости на вкладке **Анализ** выполняется запрос к внешним сервисам, которые возвращают описание соответствующей уязвимости из своей базы. В качестве исходного значения передается код уязвимости, по которой требуется получить соответствующую CVE.

Чтобы настроить аналитический сервис:

1) Откройте раздел **Уязвимости → Настройки → Настройки аналитических сервисов**;
2) Откройте преднастроенную запись настроек аналитических сервисов, в которой следует указать API ключ и установить признак *Включен*. API ключ необходимо указывать для авторизации запроса в сервисе.

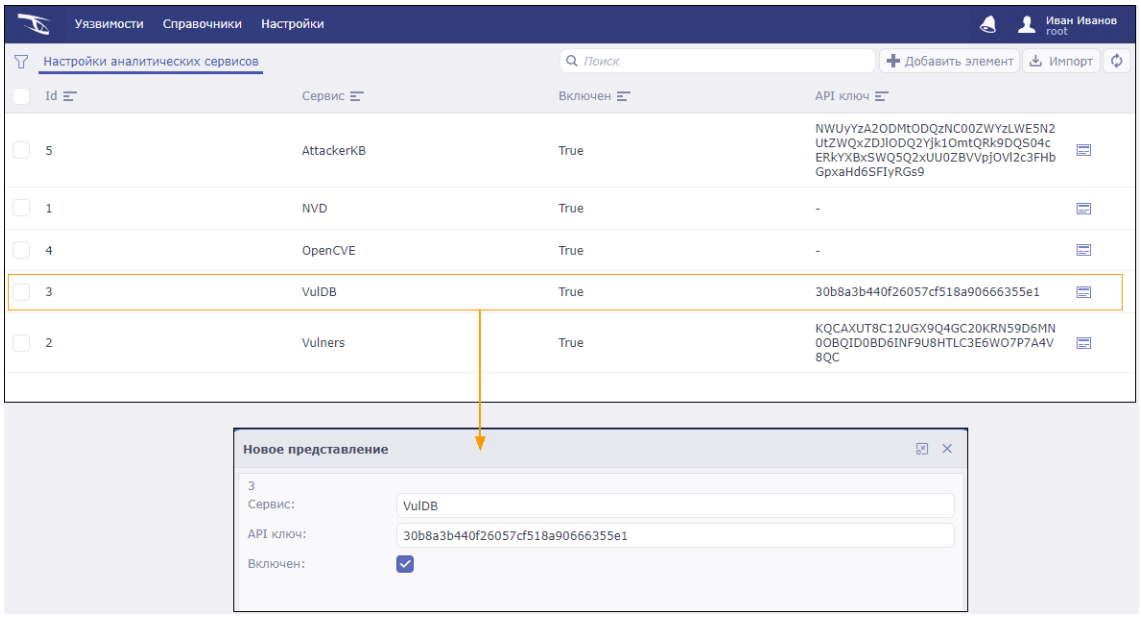


Рисунок 3-35 – Настройка аналитических сервисов

3.3.2.7 Сканирование уязвимостей

Получение данных по уязвимостям запускается автоматически по расписанию посредством преднастроенных расписаний или вручную. Преднастроенные расписания доступны в разделе Модуля **Уязвимости → Настройки → Расписание загрузки данных**. Каждое расписание доступно для редактирования. Подключение к внешним источникам (сканерам уязвимостей) осуществляется с помощью коннекторов: MaxPatrol 8, Nessus (XML), Qualys (API), Qualys (XML), RedCheck (API), RedCheck (DB), RedCheck (XML), Tenable.IO (ex. Nessus), Tenable.SC (см. раздел Настройка сканеров уязвимостей).

Полученная информация проходит нормализацию (парсинг) и затем на базе обработанных данных в группе разделов **Уязвимости → Технические уязвимости → Уязвимости** создаются уязвимости, к которым привязываются детали обнаружения и заявки на устранение. Также к созданным уязвимостям привязываются соответствующие CVE, БДУ ФСТЭК и бюллетени Microsoft, полученные из внешних источников. В карточке также отображаются связанные уязвимости, полученные из сканера по соответствующему активу. Информация по уязвимости загружается из соответствующей CVE из внешней базы NVD.

3.3.3 Описание функции «Управление жизненным циклом инцидентов информационной безопасности».

Данная функция позволяет автоматизировать процесс обработки инцидента информационной безопасности.

3.3.3.1 Задача «Регистрация инцидента информационной безопасности».

Операция 1. Автоматическая регистрация инцидента информационной безопасности.

Условия выполнения операции: Автоматическая регистрация инцидента производится при условии регистрации инцидента в ядре системы в соответствии с правилами корреляции

Подготовка: подготовительные действия предполагают настройку правил корреляции в ядре системы. Подробная информация о настройке правил корреляции содержится в документации на SIEM, используемую в качестве ядра системы.

Действия пользователя: действия не требуются, необходимые поля заполняются автоматически на основе данных от ядра.

Результат: результатом является созданная заявка типа «Инцидент». Созданные заявки группируются в перечень заявок и отображаются в разделе «Заявки»

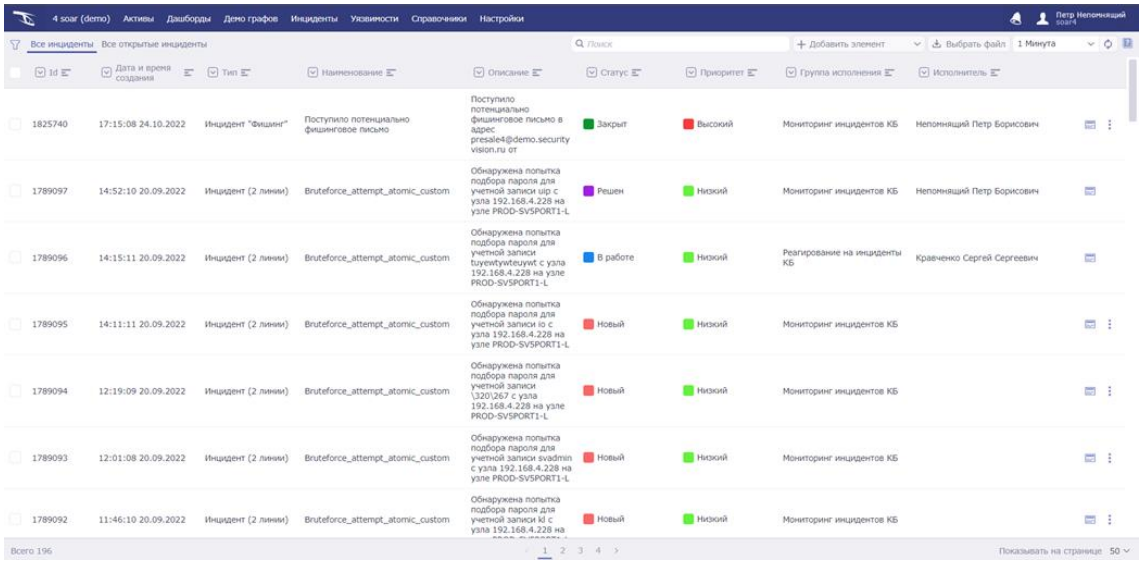


Рисунок 3-36

Операция 2. Ручная регистрация инцидента информационной безопасности.

Условия выполнения операции: в организации созданы условия для приема обращений от сотрудников. Работникам назначены роли согласно выполняемым ими функциям. Подробнее о назначении ролей пользователей в соответствующем разделе.

Действия пользователя: для того, чтобы зарегистрировать новый инцидент в системе, необходимо создать заявку соответствующего типа. В системе встроены 3 типа заявки для обработки инцидента:

1. «Инцидент». Данная заявка с соответствующим рабочим процессом реализует линейный сценарий обработки инцидента.

2. «Инцидент с распределением». Данная заявка с соответствующим рабочим процессом реализует сценарий обработки инцидента, в рамках которого осуществляется распределение инцидентов по зонам ответственности для последующей обработки.

3. «Инцидент (3 линии)». Данная заявка с соответствующим рабочим процессом реализует сценарий обработки инцидента, в рамках которого осуществляется последовательная эскалация инцидента и его передача на более высокий уровень обработки.

Детальная информация о каждом из перечисленных типов заявок, а также описание различий между ними представлена в Приложении А.

Для создания новой заявки необходимо нажать кнопку «Добавить заявку» в левом верхнем углу интерфейса заявок. При нажатии кнопки «Добавить заявку» откроется список с доступными типами заявок для создания (см. Рисунок 3-37). В данном списке необходимо выбрать нужный тип заявки. Откроется карточка создаваемой заявки.

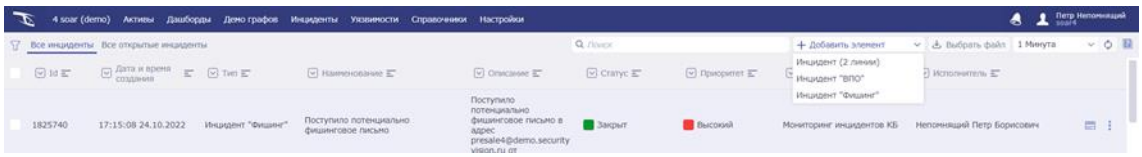


Рисунок 3-37 – Добавление заявки в Систему

В карточке создаваемой заявки необходимо внести информацию в свойства заявки, отмеченные как обязательные для заполнения, а также, при необходимости, внести информацию в другие свойства заявки, доступные для редактирования. После внесения всей информации необходимо нажать кнопку «Сохранить». Заявка будет создана в Системе, и заполненные пользователем свойства будут сохранены.

Общий вид карточки инцидента представлен на рисунке 3-38. На карточке имеется 3 вкладки:

- Основные – на вкладке размещены поля, отображающие свойства инцидента;
- Связи – на вкладке отображаются все связанные заявки;
- История – на вкладке отображается история изменения свойств заявки.

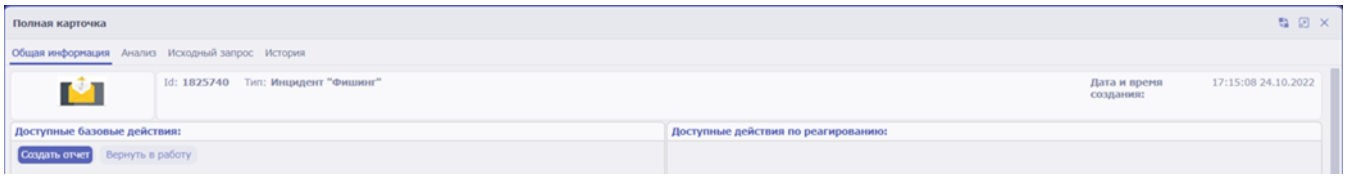


Рисунок 3-38 – Карточка инцидента

Поля на вкладке «Основные» распределены по следующим разделам:

1. Основная информация. Раздел содержит информацию, идентифицирующую данный инцидент:

- ID;
- Тип заявки Инцидент
- Время создания;
- Источник информации об инциденте;
- Сообщающее лицо;

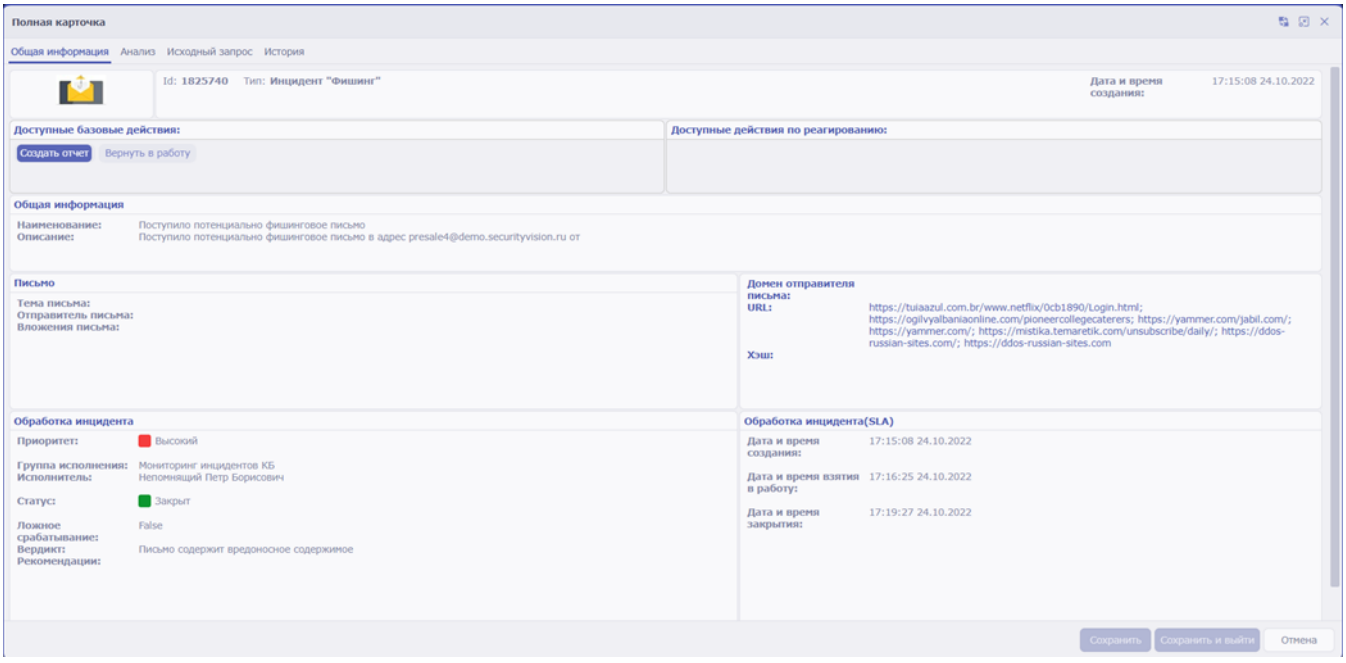


Рисунок 3-39 – Раздел «Основная информация»

2. Детали инцидента. В данном разделе расположены поля, позволяющие детализировать информацию об инциденте:

- Дата возникновения события
- Дата обнаружения
- Дата сообщения об инциденте
- Продолжительность инцидента

- Отметка о завершенности инцидента

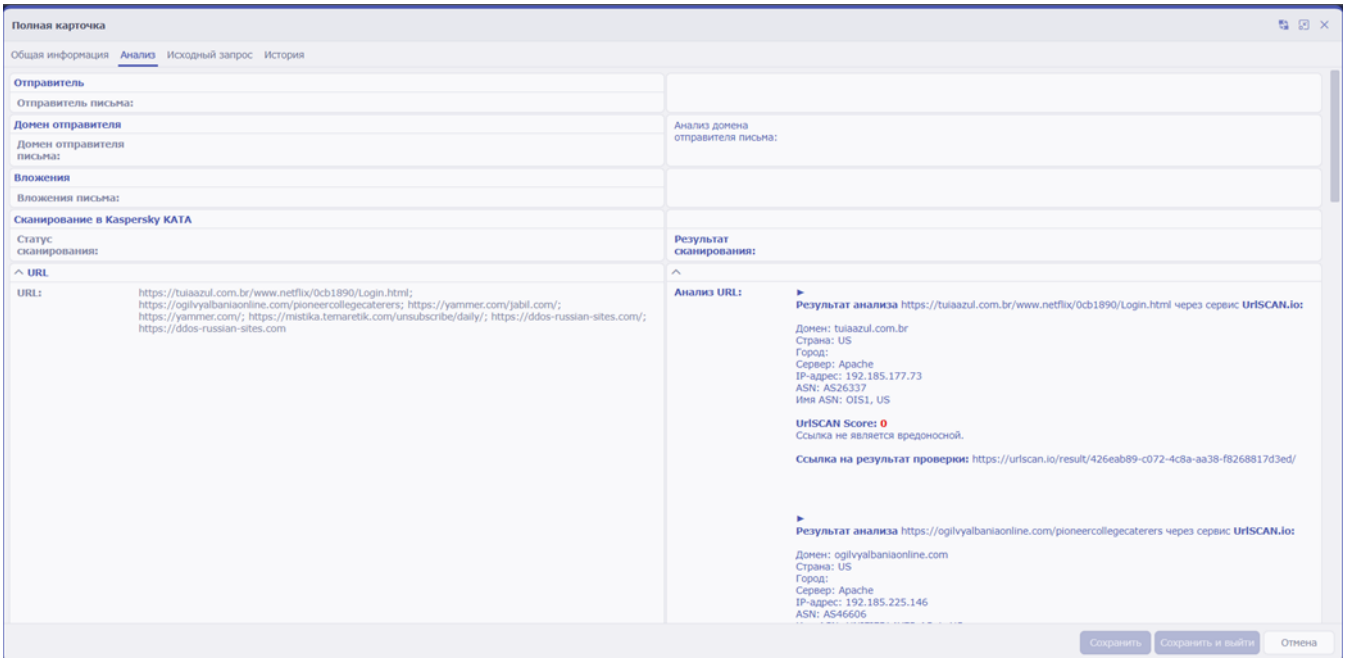


Рисунок 3-40 – Раздел «Детали инцидента»

Результат: результатом является созданная заявка типа «Инцидент». Созданные заявки группируются в перечень заявок и отображаются в разделе «Заявки»

Операция 3. Просмотр перечня инцидентов

Действия пользователя: для просмотра инцидентов необходимо выбрать в основном меню «Заявки» и далее выбрать пункт «Заявки» (Рисунок 3-41).

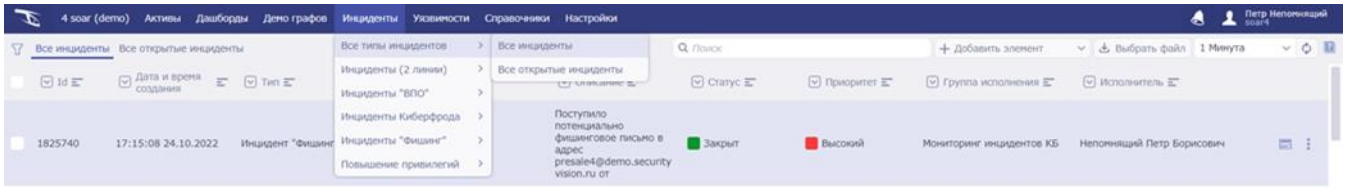


Рисунок 3-41 – Основное меню веб-интерфейса Портала Security Vision

После этого откроется таблица открытых заявок (Рисунок 3-42). В таблице отображаются основные параметры каждой заявки. Таблицу можно отсортировать по одному из параметров кликом на название параметра.

Рисунок 3-42 – Таблица заявок типа «Инцидент»

В левом нижнем углу происходит навигация по страницам таблицы. В левом верхнем углу находится кнопка для создания новой заявки пользователем, нажатие на нее откроет форму управления заявкой.

В таблице «Инциденты» выводятся следующие параметры:

- Id – уникальный идентификатор заявки в системе;
- Наименование – название инцидента. Заполняется пользователем вручную при создании инцидента или автоматически;
- Описание – описание инцидента, введенное пользователем
- Приоритет – отображает приоритет инцидента. Может принимать значения «Высокий», «Средний», «Низкий»;
- Статус заявки – текущее состояние инцидента в его жизненном цикле. Может иметь значения:
  - «Новый» – заявка создана и еще не взята в работу;
  - «В работе» – инцидент обрабатывается;
  - «Закрыт» – инцидент закрыт, дальнейшее изменение недоступно;
- Группа исполнения – группа сотрудников, ответственных за обработку инцидента;

Для просмотра подробной информации по заявке и совершения действий с ней нужно дважды кликнуть на заявку в таблице. Это откроет форму управления заявкой.

3.3.3.2 Задача «Определение контекста инцидента».

Операция 1. Заполнение сведений об инциденте.

Условия: Пользователь входит в группу, наделенную правами редактирования информации об инциденте.

Подготовка: необходимо открыть карточку созданной заявки типа «Инцидент». Для открытия карточки заявки из перечня заявок необходимо выбрать строку таблицы перечня заявок с необходимой заявкой и выполнить двойной клик левой кнопки мыши. Откроется карточка заявки.

Действия пользователя: Пользователь может заполнить все доступные для редактирования поля карточки заявки в соответствии с допустимыми значениями. Недоступные поля карточки выделяются серым цветом.

Результат: в зависимости от выбранного типа инцидента после заполнения полей станут доступными элементы управления, инициирующие перевод заявки на следующий этап рабочего процесса.

3.3.3.3 Импорт и экспорт данных

Предусмотрена возможность импорта и экспорта данных: шаблонов рабочих процессов, коннекторов, справочников, типов объектов и т.д. Данные выгружаются в виде ZIP-архива. Каждый ZIP-архив содержит JSON-документ с описанием выгруженной сущности. Загружать на Платформу можно только ZIP-архив с JSON-документом. Автором импортируемых данных будет тот пользователь, который выгружал данные. Таким образом данная функция позволяет быстро перенести настроенные сущности с одного стенда Платформы на другой.

Порядок действий для импорта и экспорта данных см. в разделах:

- Экспорт данных
- Импорт данных
  - Импорт данных из консоли

При запуске импорта или экспорта запускается асинхронное задание, статус которого можно отслеживать в модальном окне или через панель в правом верхнем углу экрана: если закрыть модальное окно или нажать на кнопку **Выполнять в фоновом режиме**, то прогресс по заданию переместится в данную панель — см. ниже рисунки. При экспорте справочника или группы справочников можно выбрать опцию **Экспортировать данные** — будут выгружены все записи справочника с сохранением их порядка по идентификатору.

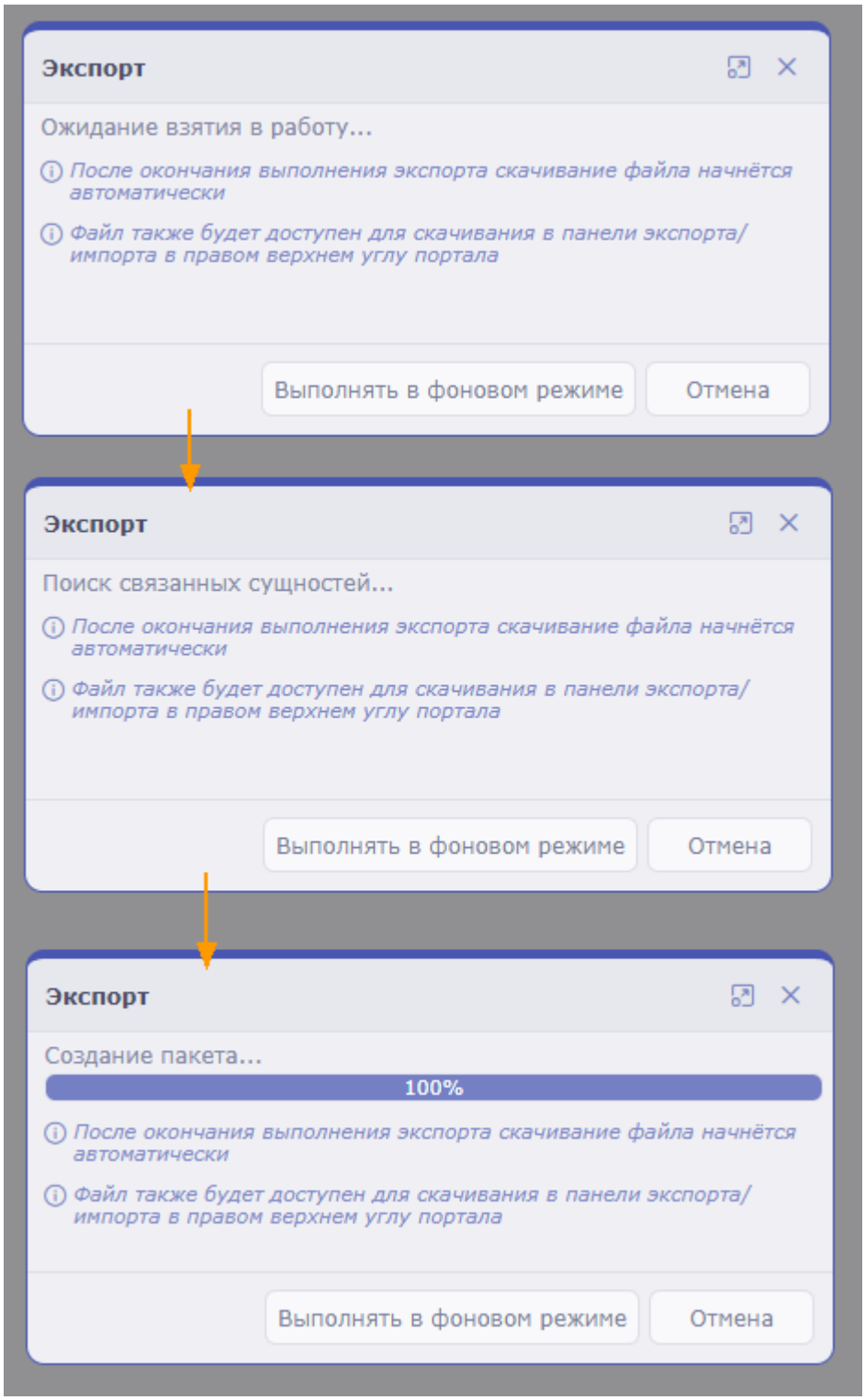

Экспорт
Ожидание взятия в работу...
После окончания выполнения экспорта скачивание файла начнётся автоматически
Файл также будет доступен для скачивания в панели экспорта/импорта в правом верхнем углу портала
Выполнять в фоновом режиме
Отмена
Экспорт
Поиск связанных сущностей...
После окончания выполнения экспорта скачивание файла начнётся автоматически
Файл также будет доступен для скачивания в панели экспорта/импорта в правом верхнем углу портала
Выполнять в фоновом режиме
Отмена
Экспорт
Создание пакета...
100%
После окончания выполнения экспорта скачивание файла начнётся автоматически
Файл также будет доступен для скачивания в панели экспорта/импорта в правом верхнем углу портала
Выполнять в фоновом режиме
Отмена

Рисунок 3-43 – Экспорт данных

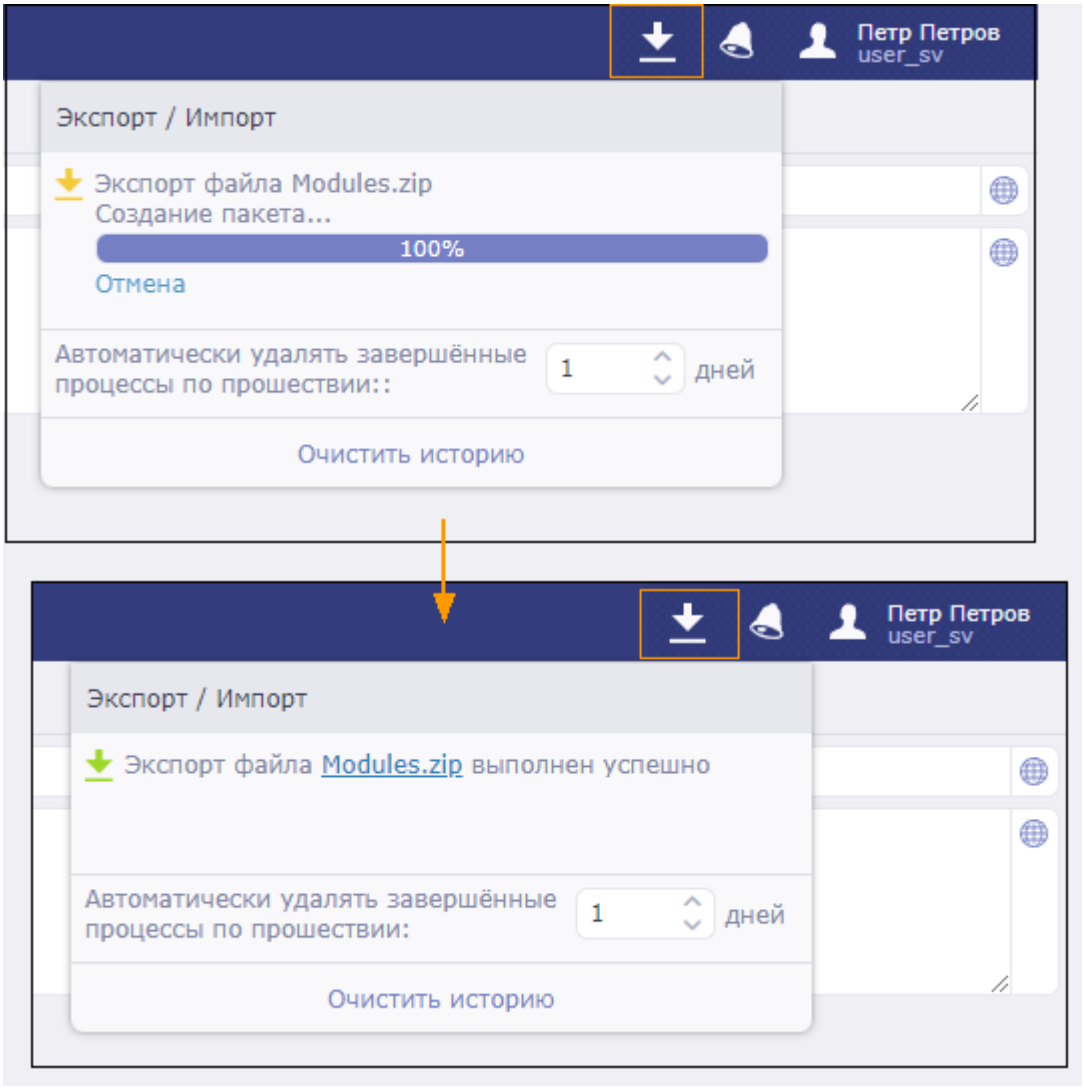


Рисунок 3-44 – Экспорт данных в фоновом режиме

3.3.3.3.1 Экспорт данных

Чтобы экспортировать данные:

1) Откройте раздел с настроенной сущностью.
2) Выберите сущность (шаблон рабочего процесса, коннектор, справочник). Выгружать можно отдельно сущности или их группы.
3) Нажмите кнопку экспорта данных — см. рисунок 3-67.
4) На локальный диск выгрузится ZIP-архив с документом JSON, описывающим настроенную сущность.

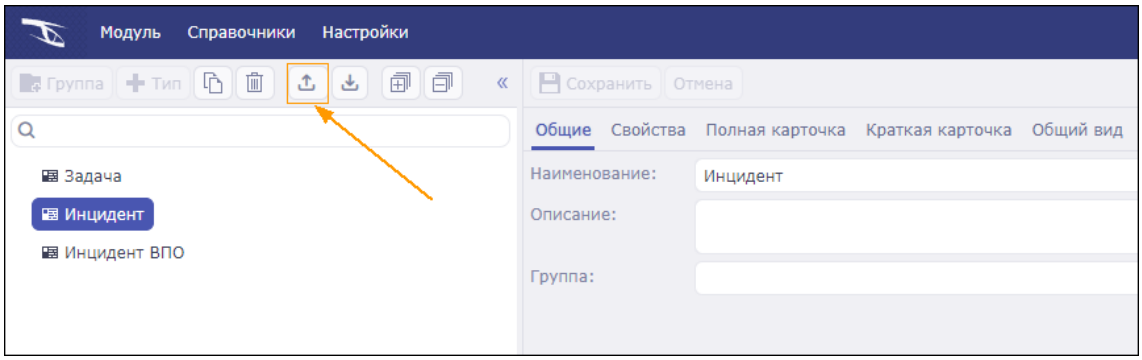


Рисунок 3-45 – Выгрузить настроенный тип объектов

Таблица 3.2 –Зависимости экспортируемых данных

Экспортируемые данные	**Зависимости**
Рабочие процессы	
Шаблон рабочего процесса	Вне зависимости от действий вместе с шаблоном рабочего процесса выгружаются следующие данные: — Группы пользователей и роли пользователей, которым доступны транзакции из шаблона рабочего процесса; — Типы данных объектов; — Свойства данных объектов (общие настройки, формы ввода и вывода). В зависимости от действий в шаблоне рабочего процесса выгружаются дополнительно следующие данные: — Отчеты и все его настройки (виджеты, входные параметры); — Другие запускаемые рабочие процессы и их типы объектов, свойства объектов (формы ввода и вывода); — Запускаемые коннекторы и все его настройки (конфигурации подключения, команды, входные параметры команд).
Расписание запуска рабочего процесса	— Рабочие процессы, шаблон которых указан в расписании, и все сопутствующие рабочему процессу зависимости — см. выше шаблон рабочего процесса. — Типы объектов, отобранных по фильтру расписания; — Свойства объектов (общие настройки, формы ввода и вывода), отобранных по фильтру расписания.

Экспортируемые данные	Зависимости
Объекты Платформы	
Созданные объекты	Выгружаются дополнительно: — Типы выбранных объектов — см. пункт тип объектов. — Свойства выбранных объектов — см. пункт свойство объектов. Если в объекте есть свойство типа Ссылка на справочник, то выгружаются дополнительно следующие данные: — Настройки справочника, на который указывает свойство; — Записи данного справочника, выбранные в качестве значения свойства. Если в объекте есть свойство типа Ссылка на объект, то выгружаются дополнительно следующие данные: — Тип объекта, на который указывает свойство; — Объекты данного типа, выбранные в качестве значения свойства; — Свойства данных объектов (общие настройки, формы ввода и вывода).
Свойство объектов	Вне зависимости от типа свойства: — Общие настройки; — Формы ввода и вывода. Если свойство типа Ссылка на справочник, то выгружаются дополнительно следующие данные: — Настройки справочника, на который указывает свойство. Если свойство типа Ссылка на объект, то выгружаются дополнительно следующие данные: — Тип объекта, на котороый указывает свойство; — Свойства данных объектов (общие настройки, формы ввода и вывода).
Тип объектов	Если в типе объекта есть свойство типа Ссылка на справочник, то выгружаются дополнительно следующие данные:

Экспортируемые данные	Зависимости
	— Настройки справочника, на который указывает свойство. Если в типе объекта есть свойство типа Ссылка на объект, то выгружаются дополнительно следующие данные: — Тип объектов; — Свойства данного типа объектов (общие настройки, формы ввода и вывода). Если в типе объекта настроены правила видимости и доступности, автозаполнения или валидации, то выгружаются дополнительно следующие данные: — Группы пользователей и роли пользователей, к которым применяются данные правила.
События	
Обработчик событий	Если в действиях обработчика создается объект, то выгружаются дополнительно следующие данные: — Тип объекта; — Все свойства объекта выбранного типа; — Рабочие процессы для новых объектов и все сопутствующие рабочему процессу зависимости — см. выше шаблон рабочего процесса Если в действиях обработчика создается событие, то выгружаются дополнительно следующие данные: — Тип события (общие настройки и свойства типа события).
Расписание	— Запускаемые коннекторы и все его настройки (конфигурации подключения, команды, входные параметры команд). — Заполняемые обработчики событий и все сопутствующие обработчикам зависимости — см. выше обработчик событий.
Тип событий	Нет зависимостей.
Модули	

Экспортируемые данные	Зависимости
Модуль	Дополнительно выгружаются группы, разделы выбранного модуля и все сопутствующие группе и разделу зависимости — см. пункты группа и раздел.
Раздел	— Роли пользователей, которым доступно представление раздела модуля. — Тип объекта системы и все сопутствующие зависимости типу объекта системы — см. выше тип объектов. — Рабочие процессы, запускаемые для данного типа в рамках данного модуля (при наличии таких). Также все сопутствующие рабочему процессу зависимости — см. выше шаблон рабочего процесса. — Разделы модулей, на которые указывают быстрые ссылки (при наличии таких). Также все сопутствующие разделу модуля зависимости — см. текущий пункт.
Группа	Дополнительно выгружаются родительский модуль, разделы выбранной группы и все сопутствующие группе и модулю зависимости — см. пункты модуль и раздел.
Роли	
Роль	Дополнительно выгружаются сущности, к которым выдан доступ в соответствии с полномочиями роли: — Модули и все сопутствующие зависимости — см. пункт модуль. — Справочники и все сопутствующие зависимости — см. пункт справочник.
Группа ролей	Все роли из группы и все сопутствующие роли зависимости — см. пункт роль.
Справочники	
Справочник (настройки)	Дополнительно выгружаются следующие данные: — Группы сотрудников, для которых настроено правило валидации. Также все сопутствующие зависимости.

Экспортируемые данные	Зависимости
	Если в справочнике есть свойство типа Ссылка на справочник, то дополнительно выгружаются следующие данные: — Настройки и записи справочника, на который указывает свойство.
Группа справочников	Все справочники из группы и все сопутствующие справочнику зависимости — см. пункт справочник.
Записи справочника	Дополнительно выгружаются: — Настройки справочника, в котором хранятся выбранные записи — см. пункт справочник (настройки). Если в справочнике есть свойство типа Ссылка на справочник, то дополнительно выгружаются следующие данные: — Настройки справочника, на который указывает свойство.
Коннекторы	
Коннектор	Нет зависимостей.
Конфигурация подключения коннектора	Нет зависимостей.
Команда коннектора	Нет зависимостей.
Сервис коннекторов	Дополнительно выгружаются сервисы коннекторов, которые связаны с текущим сервисом коннекторов.
Группа коннекторов	Все коннекторы из группы и все сопутствующие коннекторам зависимости — см. пункт коннектор.
Виджеты	
Виджет	— Выбранные Свойства объектов и все сопутствующие зависимости — см. пункт свойство объектов. — Анимации (нет зависимостей). — Стрелки (нет зависимостей). — Изображения для карты (нет зависимостей).

Экспортируемые данные	Зависимости
	— Иконки (нет зависимостей). — Дашборды — см. пункт дашборд. — Раздел модуля — см. пункт раздел модуля. — Связанные виджеты и все сопутствующие виджетам зависимости — см. текущий пункт.
Группа виджетов	Все виджеты из группы и все сопутствующие виджетам зависимости — см. пункт виджет.
Дашборды	
Дашборд	Все виджеты из блоков с типом содержимого *Виджет* и все сопутствующие виджетам зависимости — см. пункт виджет. Если входные параметры дашборда имеют тип свойства *Ссылка на справочник* или *Ссылка на объект*, то дополнительно выгружаются следующие данные: — Для *свойства типа Ссылка на справочник*: o Настройки справочника, на который указывает свойство. — Для *свойства типа Ссылка на объект*: o Тип объекта, на который указывает свойство; o Свойства данных объектов (общие настройки, формы ввода и вывода).
Группы дашбордов	Все дашборды из группы и все сопутствующие дашбордам зависимости — см. пункт дашборд.
Отчеты	
Отчет	Все виджеты из блоков с типом содержимого *Виджет* и все сопутствующие виджетам зависимости — см. пункт виджет. Если входные параметры отчета имеют тип свойства *Ссылка на справочник* или *Ссылка на объект*, то дополнительно выгружаются следующие данные: — Для *свойства типа Ссылка на справочник*:

Экспортируемые данные	Зависимости
	○ Настройки справочника, на который указывает свойство. — Для *свойства типа Ссылка на объект*: ○ Тип объекта, на который указывает свойство; ○ Свойства данных объектов (общие настройки, формы ввода и вывода).
Группа отчетов	Все отчеты из группы и все сопутствующие отчетам зависимости — см. пункт отчет.
Изображения	
Изображение	Нет зависимостей.
Группа изображений	Все изображения из группы.
Иконки	
Иконка	Нет зависимостей.
Группа иконок	Все иконки из группы.
Анимации	
Анимация	Нет зависимостей.
Группа анимаций	Все анимации из группы.

3.3.3.3.2 Импорт данных

Чтобы импортировать данные:

1) Зайдите на стенд Платформы, на который следует загрузить данные.
2) Откройте раздел Платформы, в который следует загрузить данные.
3) Нажмите кнопку импорта данных и укажите ZIP-архив с JSON-документом, описывающим настроенную сущность — см. рисунок 3-68.
4) Таким образом в Платформу импортируется указанная сущность.

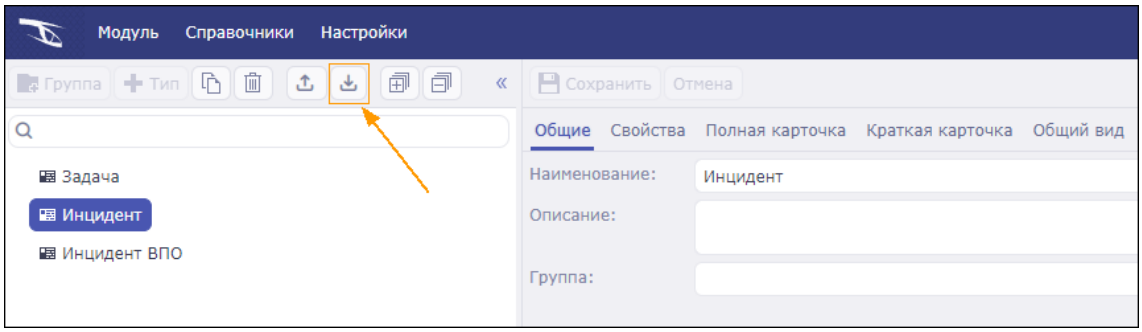


Рисунок 3-46 – Загрузить тип объектов

3.3.3.3.3 Импорт данных из консоли

Импортировать данные на Платформу можно также через командную строку. Данная операция выполняется посредством приложения ImportTool.

Чтобы импортировать данные через командную строку:

1) Открыть командную строку на сервере.
2) Запустить приложение SecurityVision.ImportTool, на вход которому передать zip архив с импортируемыми данными. Пример команды для сервера под управлением CentOS приведен ниже:

```
sudo ./SecurityVision.ImportTool ./archive.zip
```

3) Таким образом данные импортированы на Платформу.

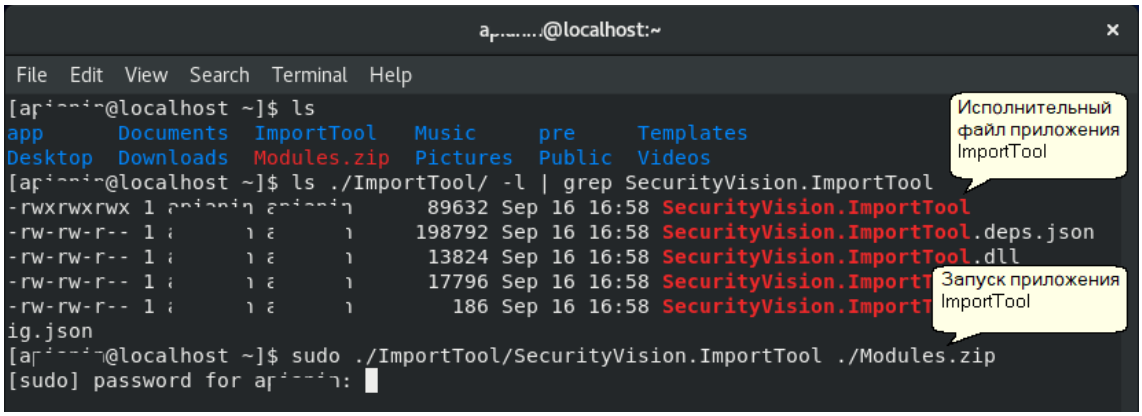


Рисунок 3-47 – Пример импорта данных через командную строку

ПРИЛОЖЕНИЕ А. ОПИСАНИЕ РАБОЧИХ ПРОЦЕССОВ ОБРАБОТКИ ИНЦИДЕНТА

В системе предусмотрено три типа заявок по обработке инцидентов и соответствующих рабочих процессов.

1. Заявка типа «Инцидент с распределением». Данная заявка с соответствующим рабочим процессом реализует сценарий обработки инцидента, в рамках которого осуществляется распределение инцидентов по зонам ответственности для последующей обработки. Данный тип заявки предполагает создание задачи по реагированию на инцидент. Задача по реагированию представляет собой заявку типа «Задача» и в совокупности с соответствующим рабочим процессом позволяет контролировать выполнение действий по реагированию на инцидент.
2. Заявка типа «Инцидент (3 линии)». Данная заявка с соответствующим рабочим процессом реализует сценарий обработки инцидента, в рамках которого осуществляется последовательная эскалация инцидента и его передача на более высокий уровень обработки. На каждом уровне обработки предусмотрено формирование задачи на обработку инцидента. Задача по обработке представляет собой заявку типа «Задача» и в совокупности с соответствующим рабочим процессом позволяет контролировать выполнение действий по обработке инцидента. В зависимости от этапа рабочего процесса обработки инцидента, на котором формируется задача, может формироваться задача типа «Анализ» или «Реагирование»

Описание рабочего процесса обработки заявки типа «Инцидент с распределением».

1. Началом рабочего процесса является момент создания заявки типа «Инцидент с распределением» в системе управления заявками. Заявка данного типа может быть создана как автоматически на основании данных ядра системы, так и вручную пользователем.

При создании заявки заполняется базовая информация об инциденте. Обязательными для заполнения на данном этапе являются следующие поля:

- Наименование
- Источник информации об инциденте

Также заполняется информация о связанных активах.

2. На этапе идентификации производится определение контекста инцидента, критичности, зоны ответственности. После заполнения всей известной информации об инциденте

осуществляется его передача специалисту в соответствии с зоной ответственности. На данном этапе обязательными для заполнения являются следующие поля:

- Описание
- Опасность события ИБ
- Группа исполнения

На этапе идентификации также возможно отметить инцидент как ложноположительный или признать событие легитимным, т.е. не являющимся инцидентом ИБ.

В случае, если инцидент отмечен как ложноположительный, осуществляется переход к действиям по обработке ложного срабатывания.

Если определено, что событие вызвано легитимным действием, появляется возможность закрытия заявки и прекращения работы с инцидентом с соответствующей пометкой.

3. Далее осуществляется взятие инцидента в работу специалистом, входящим в группу исполнения.

4. Уточнение информации об инциденте. На данном этапе происходит обогащение и актуализация данных об инциденте.

На данном этапе инцидент также может быть отмечен как ложноположительный. В этом случае осуществляется переход к действиям по обработке ложного срабатывания.

Если в ходе уточнения информации, инцидент подтвержден, осуществляется проверка, есть ли соответствующий план реагирования. Если план имеется, осуществляется переход к реагированию на инцидент. Если плана обработки нет, осуществляется переход к определению действий по реагированию. После того, как действия по реагированию определены, осуществляется переход к реагированию на инцидент.

5. Дальнейшие действия рабочего процесса предполагают создание задачи по реагированию на инцидент. На данном этапе пользователем формируется заявка типа «Задача» по реагированию. В новую заявку передаются данные об ответственном сотруднике и группе исполнения, описание инцидента, перечень планируемых действий и сроки их выполнения.

Действия с созданной заявкой выполняются в соответствии с рабочим процессом заявки типа «Задача».

После выполнения всех требуемых действий и закрытия всех связанных заявок типа «Задача» осуществляется переход на следующий этап рабочего процесса.

7. Анализ инцидента. На данном этапе выполняются действия по анализу инцидента, а также, если необходимо, создается задача на выполнение действий, направленных на предотвращение повторного возникновения инцидента или настройку правил выявления инцидентов. Создание данной задачи аналогично созданию задачи по реагированию.

Когда все действия из связанной заявки выполнены, статус основной заявки устанавливается в «Обработка завершена». В поле «Время завершения обработки» устанавливается текущее время.

Если действия всех связанных заявок выполнены, заполнены все обязательные поля, инцидент может быть закрыт.

Описание рабочего процесса обработки заявки типа «Инцидент (3 линии)»

1. Началом рабочего процесса является момент создания заявки типа «Инцидент» в системе управления заявками. Заявка данного типа может быть создана как автоматически на основании данных ядра системы, так и вручную пользователем.

При создании заявки заполняется базовая информация об инциденте. Обязательными для заполнения на данном этапе являются следующие поля:

- Наименование
- Источник информации об инциденте

Также заполняется информация о связанных активах.

2. После идентификации события осуществляется прием события в работу специалистом 1й линии.

3. После принятия события в работу, осуществляется формирование задачи на мониторинг события. Пользователем формируется связанная заявка типа «Задача». В новую заявку передаются данные об ответственном сотруднике и группе исполнения, описание события, перечень планируемых действий и сроки их выполнения. В рамках созданной задачи производятся действия по сбору дополнительной информации о событии, выявлению ложного срабатывания систем, определению контекста инцидента, критичности, зоны ответственности. На данном этапе обязательными для заполнения являются следующие поля:

- Описание
- Опасность события ИБ
- Группа исполнения

- Исполнитель
- Категория инцидента

Дальнейший переход по рабочему процессу осуществляется только при заполнении перечисленных полей.

4. Обработка результатов мониторинга. На данном этапе в карточку события вносится дополнительная информация, полученная в ходе мониторинга. В случае, если инцидент отмечен как ложноположительный, осуществляется переход к действиям по обработке ложного срабатывания. В случае, если определено, что событие не является угрозой ИБ, осуществляется закрытие заявки с внесением соответствующей пометки. В случае, если определено, что событие представляет угрозу, осуществляется определение приоритета и критичности события и дальнейшая передача события на обработку 2й линии.

5. Далее событие может быть взято в работу сотрудником, определенным как исполнитель в заявке. На данном этапе происходит обогащение информации о событии. Если определено, что событие не является инцидентом, формируется задача на исследование и обработку события.

7. Если определено, что предпринятые на предыдущем этапе действия были эффективны и угроза нейтрализована, осуществляется закрытие заявки.

8. Если угроза остается, инцидент подтвержден, осуществляется дальнейшее обогащение информации об инциденте, уточнение категории и критичности инцидента. После заполнения обязательных полей появляется возможность передачи заявки в обработку 3й линии.

9. Далее событие может быть взято в работу сотрудником, определенным как исполнитель в заявке. На данном этапе происходит анализ инцидента специалистами 3й линии. Если установлено, что инцидент является критичным, осуществляется передача инцидента группе реагирования.

11. Дальнейшие действия предполагают создание задачи на реагирование. В новую заявку передаются данные об ответственном сотруднике и группе исполнения, описание инцидента, перечень планируемых действий и сроки их выполнения. Действия с созданной заявкой выполняются в соответствии с рабочим процессом заявки типа «Задача».

12. После завершения действий по реагированию и закрытия связанных заявок заполняются результаты обработки инцидента. Осуществляется переход к анализу инцидента.

13. Анализ. На данном этапе выполняются действия по анализу инцидента, а также, если необходимо, создается задача на выполнение действий, направленных на предотвращение повторного возникновения инцидента или настройку правил выявления инцидентов. Создание данной задачи аналогично созданию задачи по реагированию.

14. Если завершены все действия по обработке инцидента, заявка может быть закрыта/