ООО «Интеллектуальная автоматизация»

«УТВЕРЖДАЮ»

Генеральный директор

ООО «Интеллектуальная автоматизация»

_____ Р.Г. Рахметов

М.П.

«____» _____ 2023 г.

Программный комплекс «One Vision: Платформа автоматизации ИТ-процессов»

Руководство по эксплуатации

На 31 листах

Москва

2023

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

В настоящем документе приведено описание основных операций, выполняемых пользователем One Vision: Платформа автоматизации ИТ-процессов. 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 One Vision 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 web-портала.

Система обеспечивает выполнение следующих функций:

- 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 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 ONE VISION

3.1 Интерфейс Портала One Vision

Портал One Vision имеет модульную структуру. Вызов списка модулей осуществляется нажатием пиктограммы One Vision, расположенной сверху слева. Переход между модулями осуществляется через основное меню модулей (Рисунок 3-1).

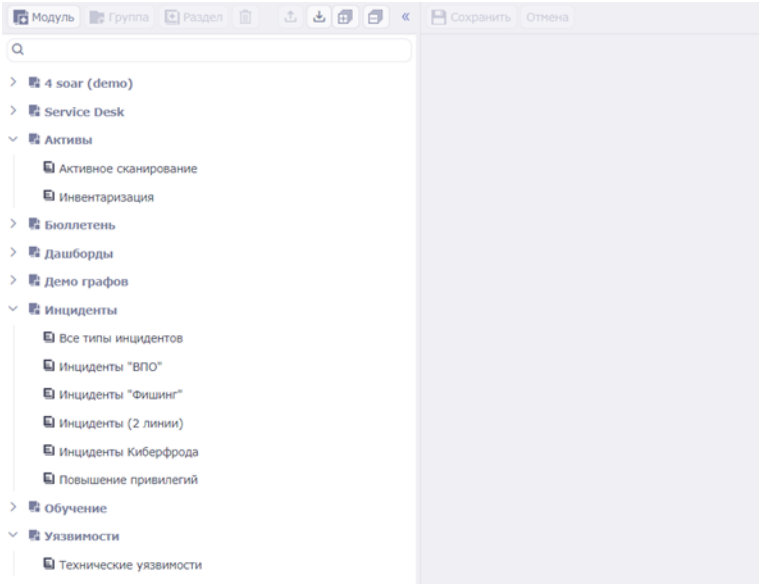


Рисунок 3-1 – Основное меню

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. 3-2), 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.

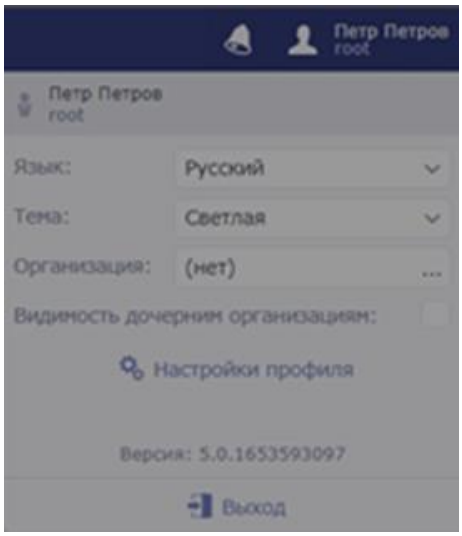


Рис. 3-2 Информация о текущем пользователе

При переходе в редактирование профиля пользователя открывается секция с двумя вкладками

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

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

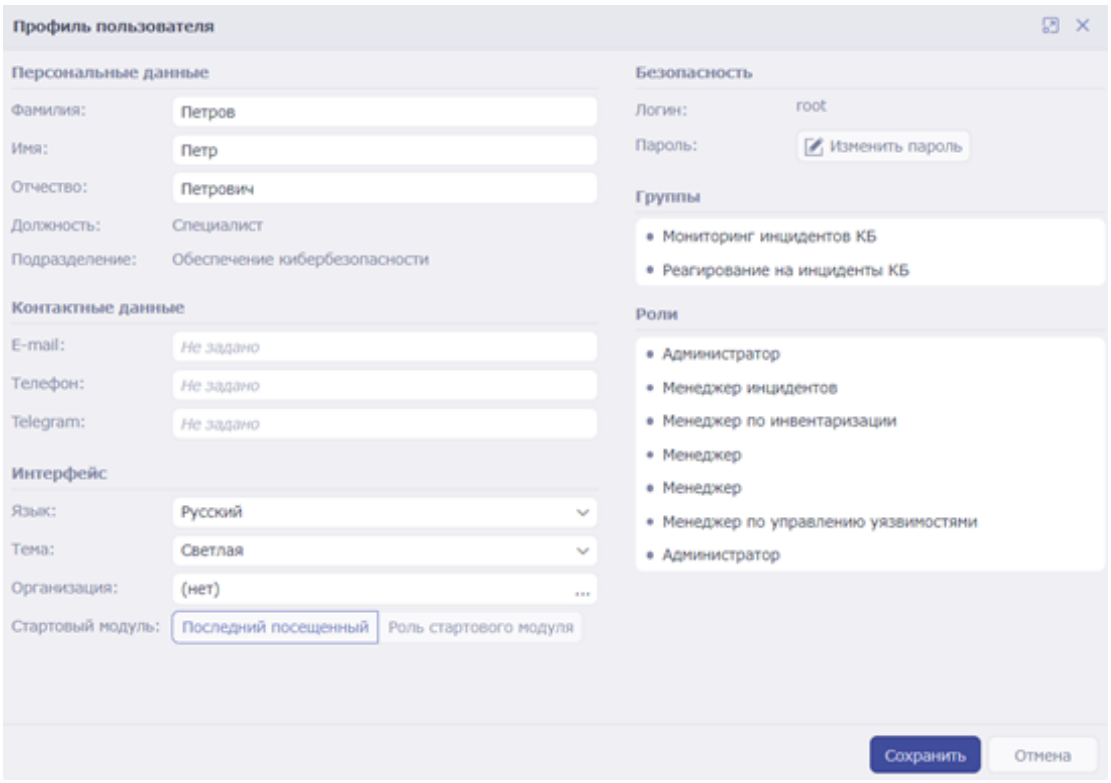


Рис. 3-3 Секция «Данные пользователя»

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

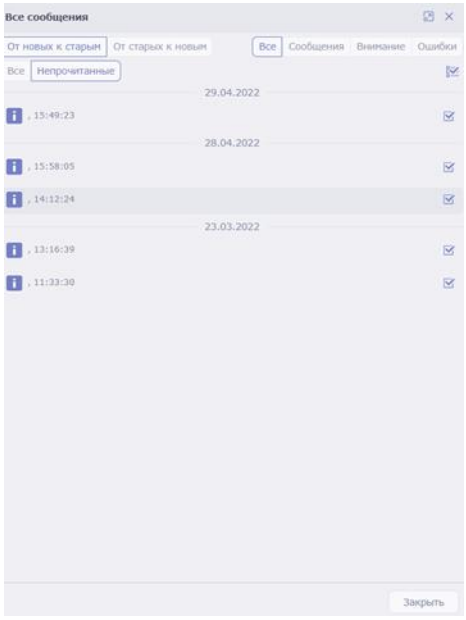


Рис. 3-4 Секция «Оповещение»

3.2 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
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	
Экспорт данных	
Импорт данных	

3.2.1 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.

3.2.1.1 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.

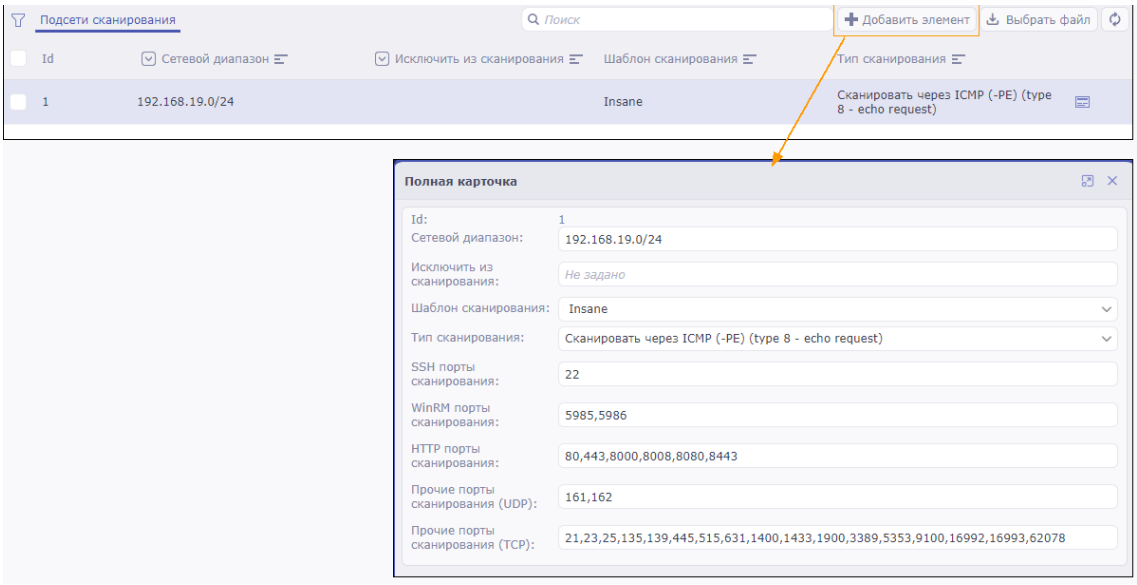


Рисунок 3-5 – Добавление подсети для сканирования

3.2.1.2 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**.

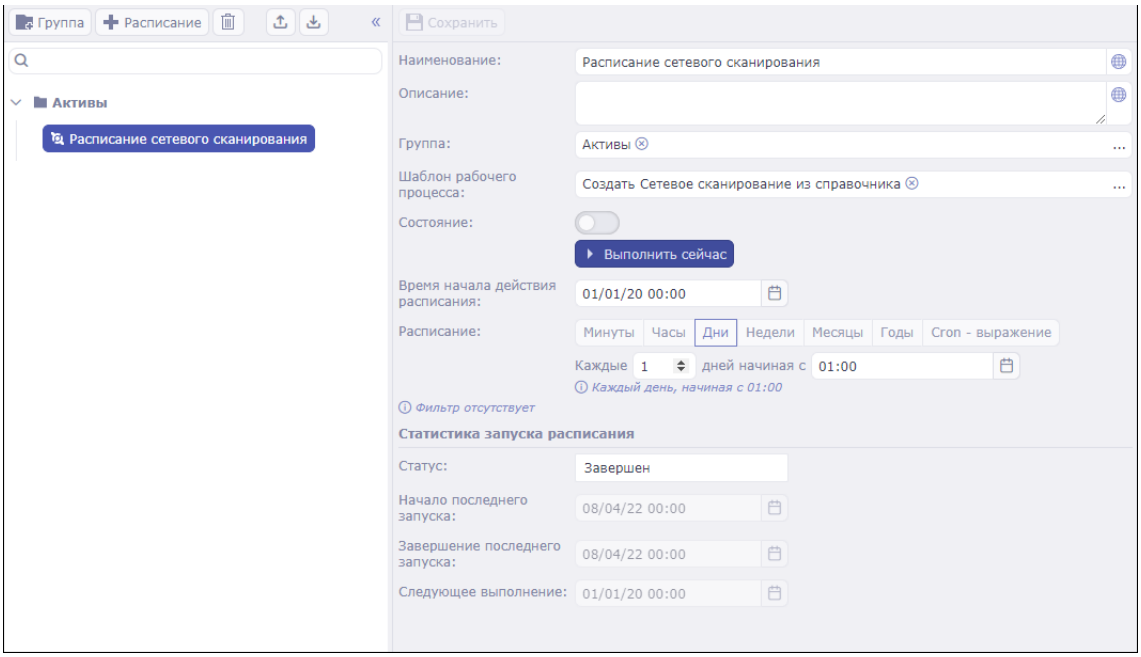


Рисунок 3-6 – Расписание сетевого сканирования

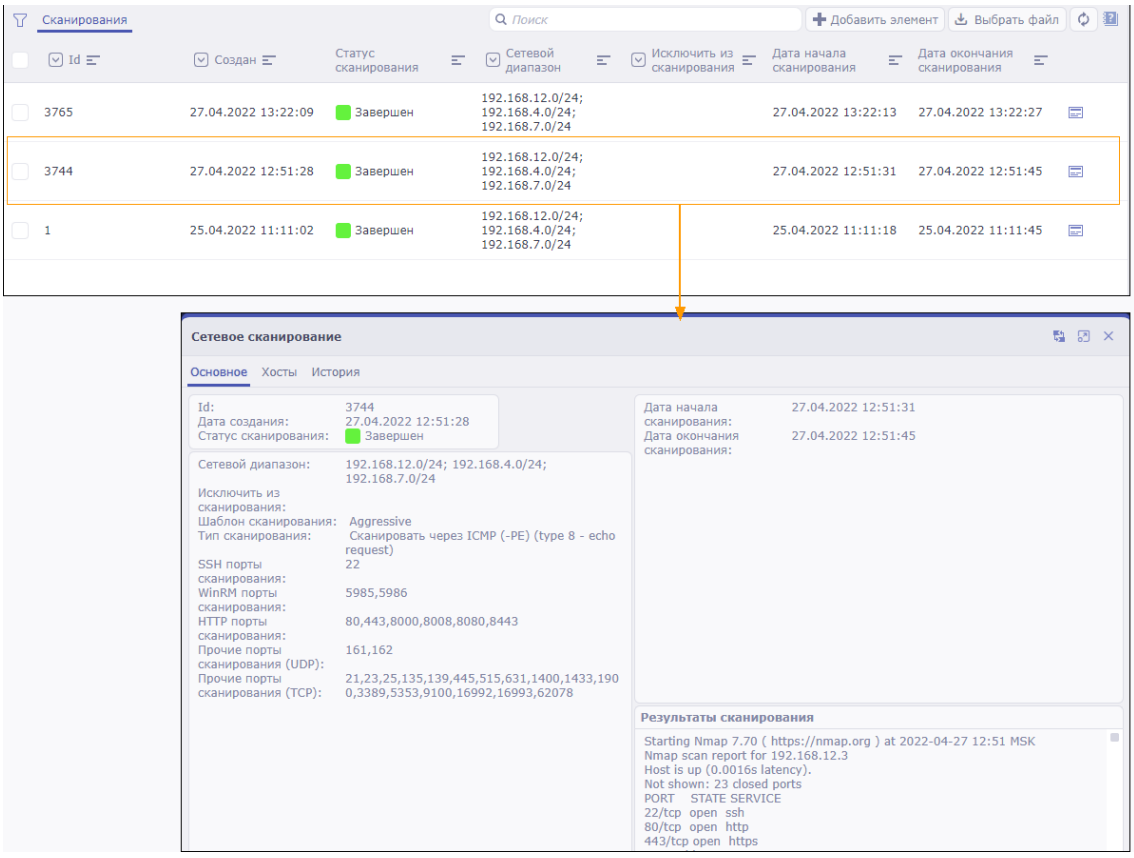


Рисунок 3-7 – Созданные объекты типа Сетевое сканирование

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*.

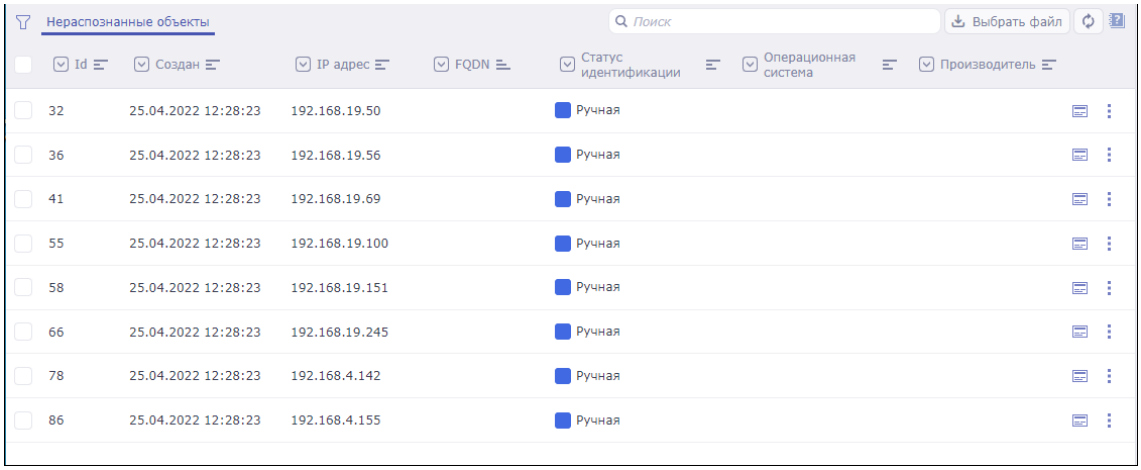


Рисунок 3-8 – Созданные объекты типа Нераспознанный объект

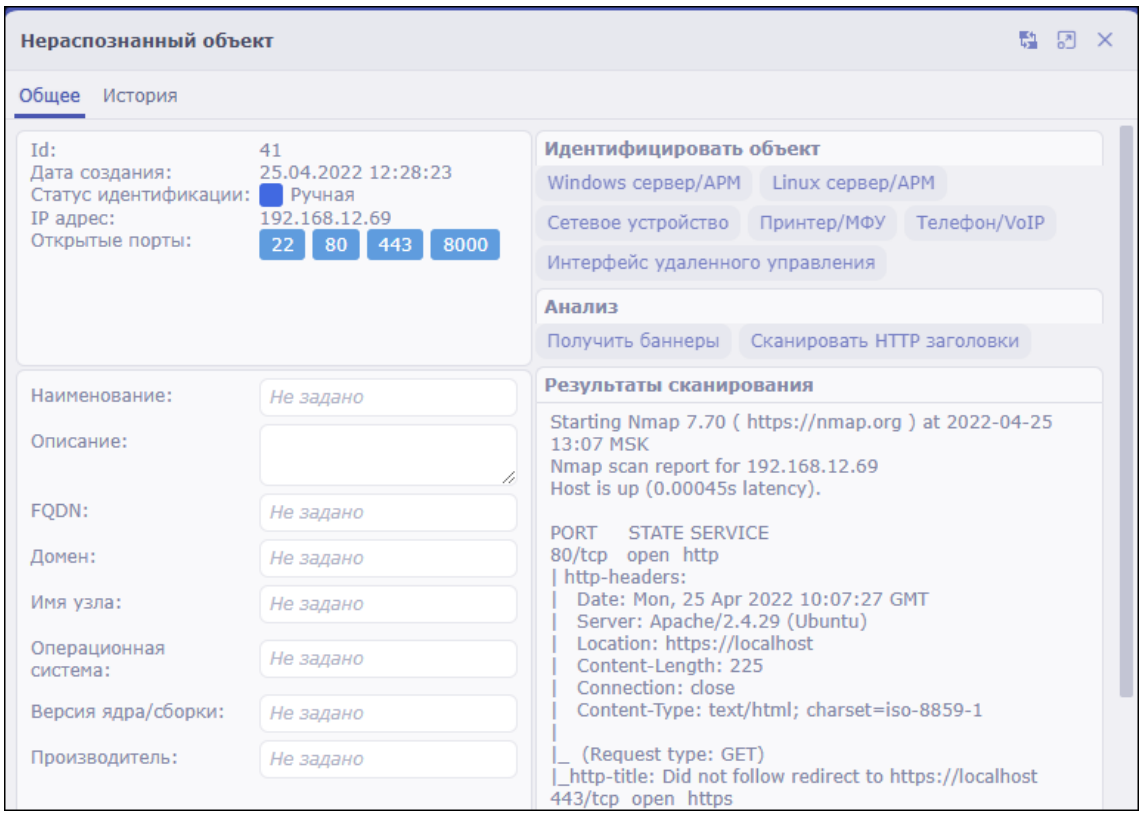


Рисунок 3-9 – Полная карточка объекта типа Нераспознанный объект

3.2.2 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.

3.2.2.1 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.

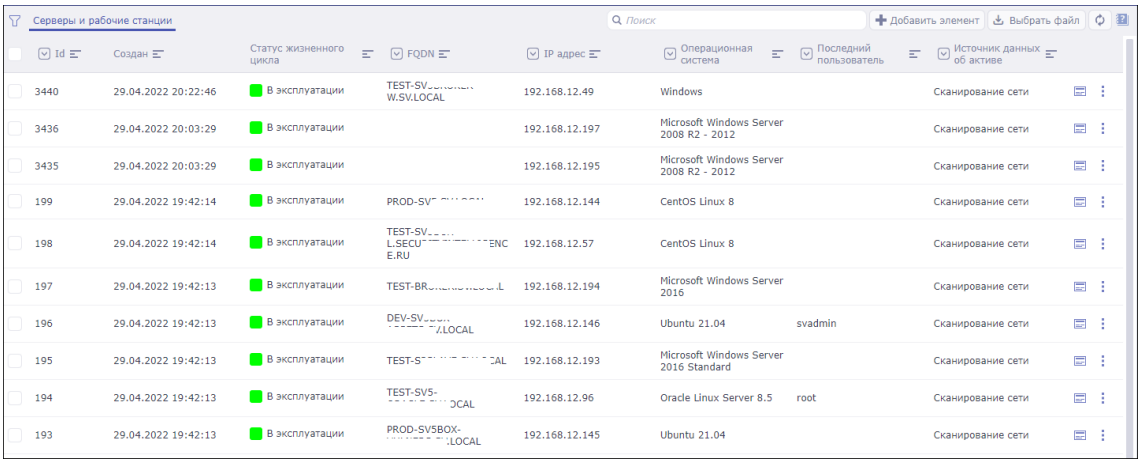


Рисунок 3-10 – Созданные идентифицированные объекты

3.2.2.2 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.

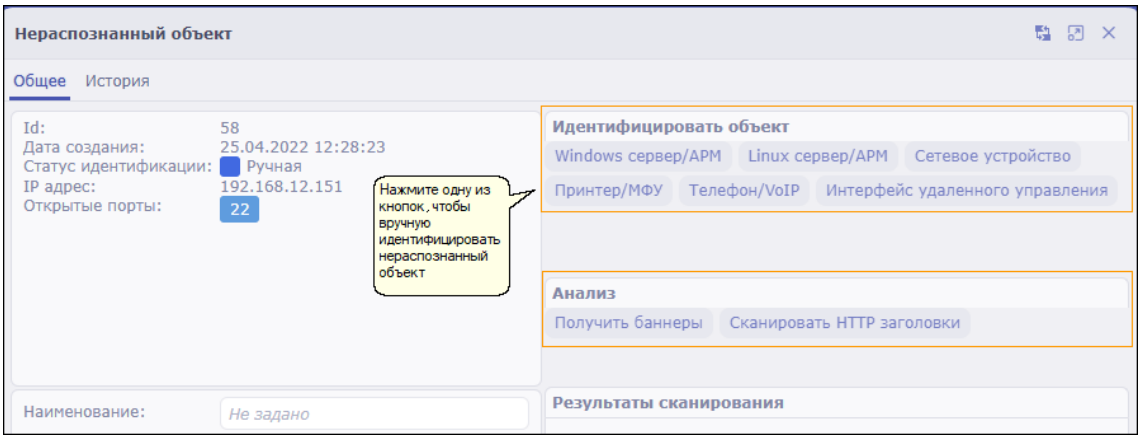


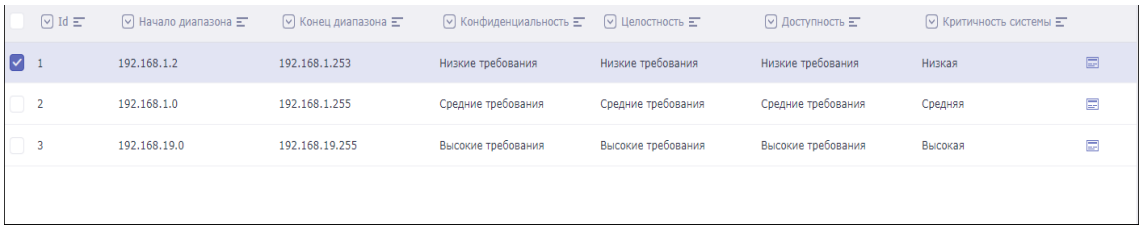
Рисунок 3-11 – Запуск идентификации вручную

3.2.3 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.



Id	Начало диапазона	Конец диапазона	Конфиденциальность	Целостность	Доступность	Критичность системы
1	192.168.1.2	192.168.1.253	Низкие требования	Низкие требования	Низкие требования	Низкая
2	192.168.1.0	192.168.1.255	Средние требования	Средние требования	Средние требования	Средняя
3	192.168.19.0	192.168.19.255	Высокие требования	Высокие требования	Высокие требования	Высокая

Рисунок 3-12 – Справочник Настройки категорирования

3.2.4 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.

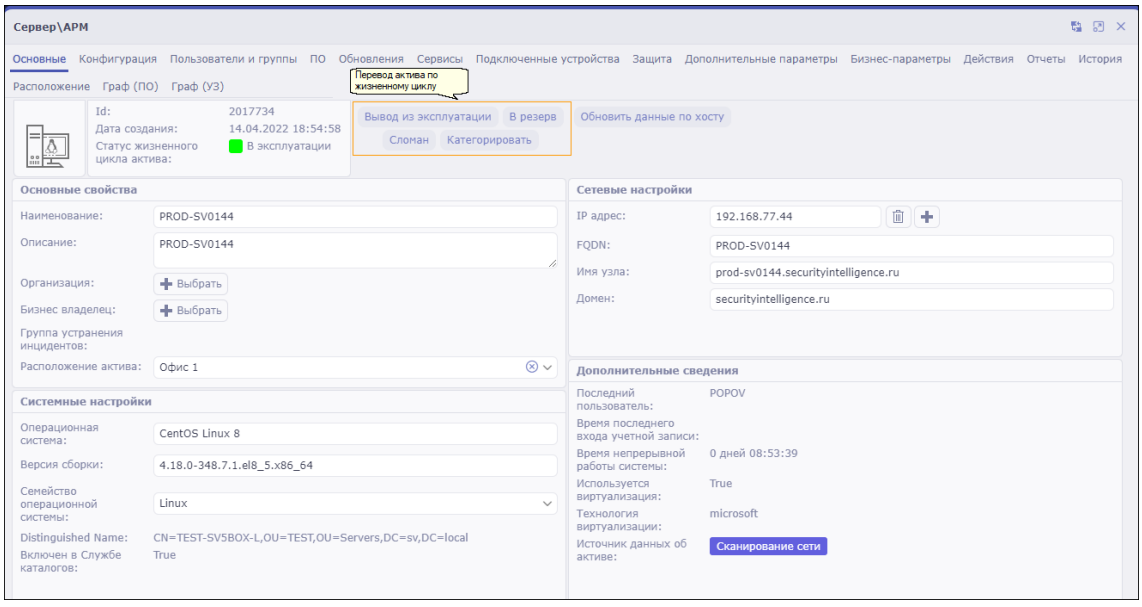


Рисунок 3-13 – Установка этапа жизненного цикла актива

3.2.5 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.

3.2.5.1 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.

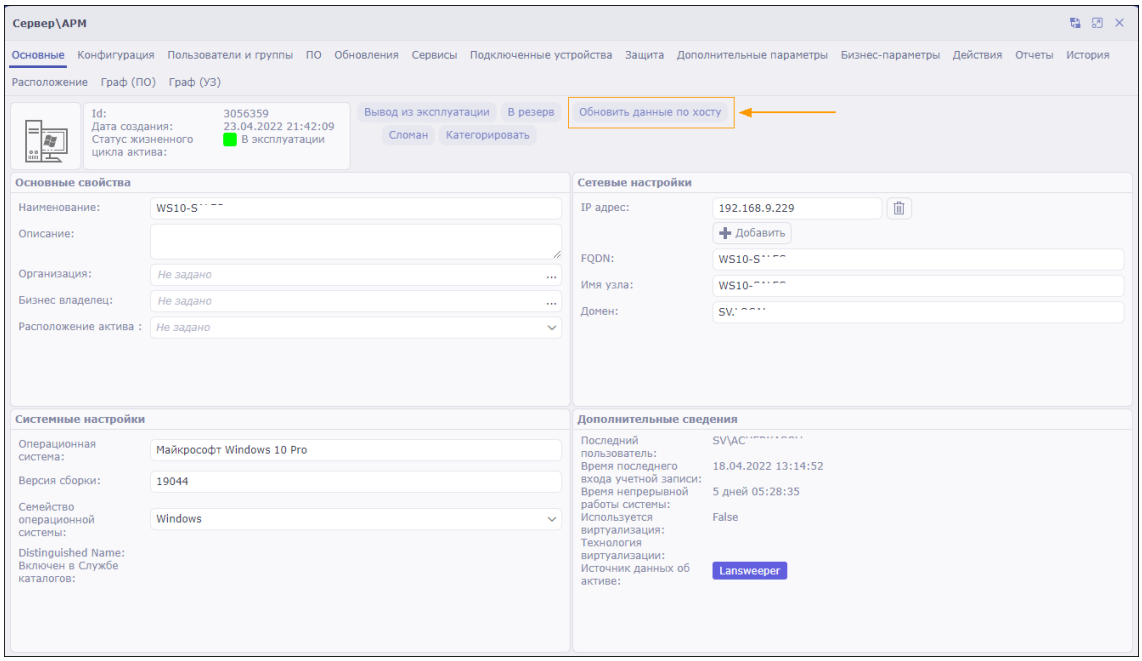


Рисунок 3-14 – Запуск обновления данных по хосту

3.2.5.2 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.

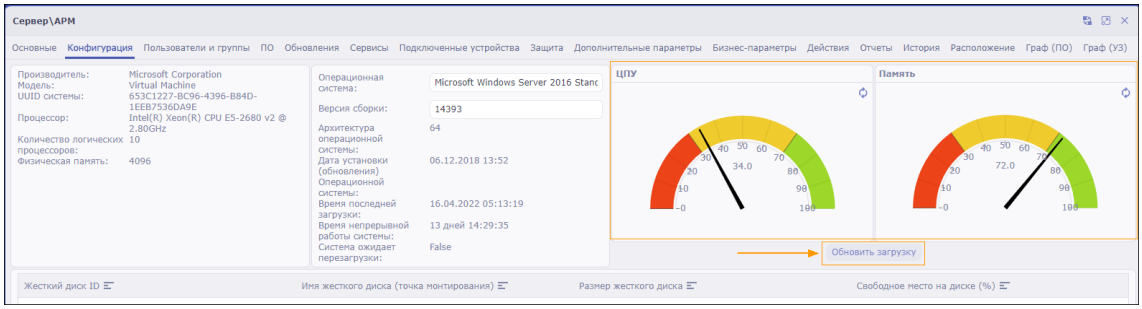


Рисунок 3-15 – Запуск обновления данных по конфигурации актива

3.2.5.3 Данные по учетным записям пользователей

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

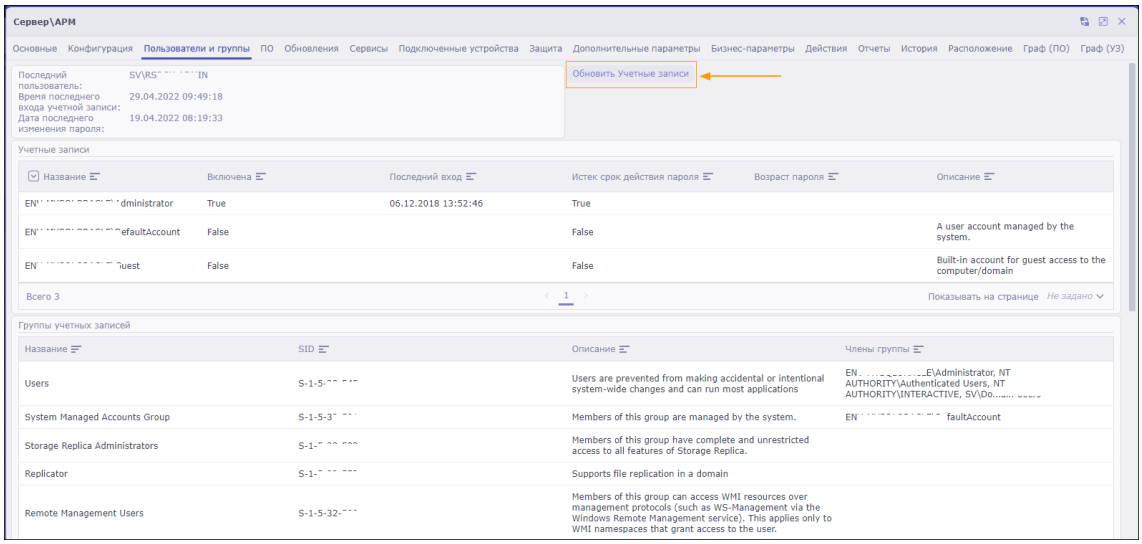


Рисунок 3-16 – Запуск обновления данных об учетных записях пользователей актива

3.2.5.4 Данные о программном обеспечении

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

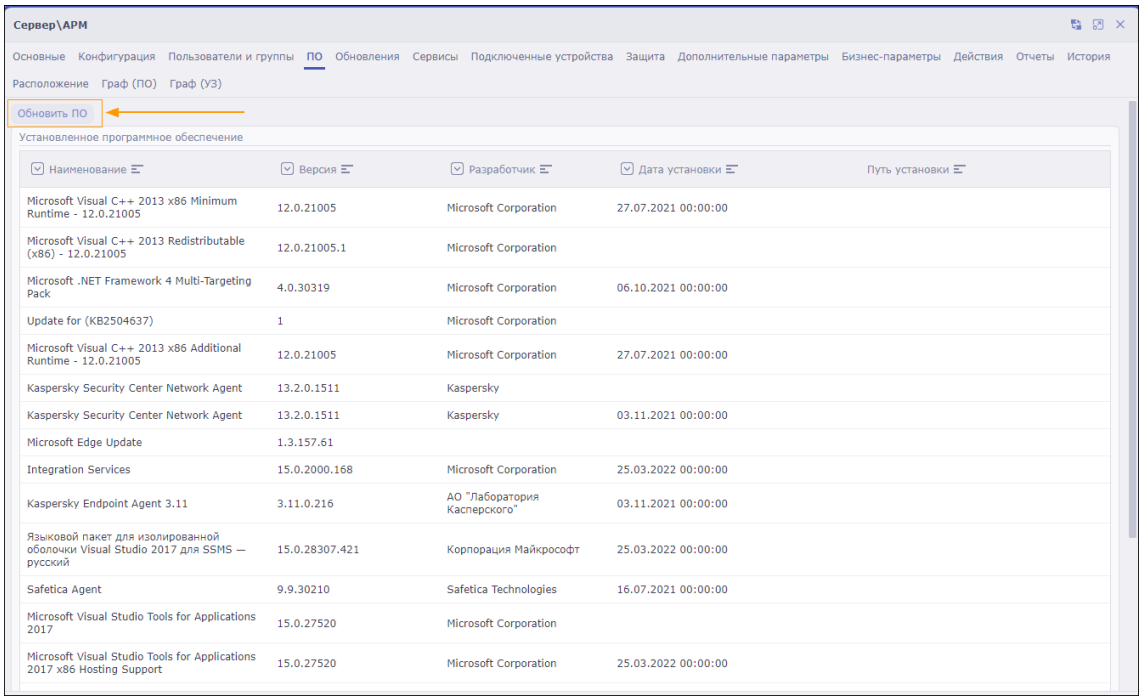


Рисунок 3-17 – Запуск обновления данных о ПО актива

3.2.5.5 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.

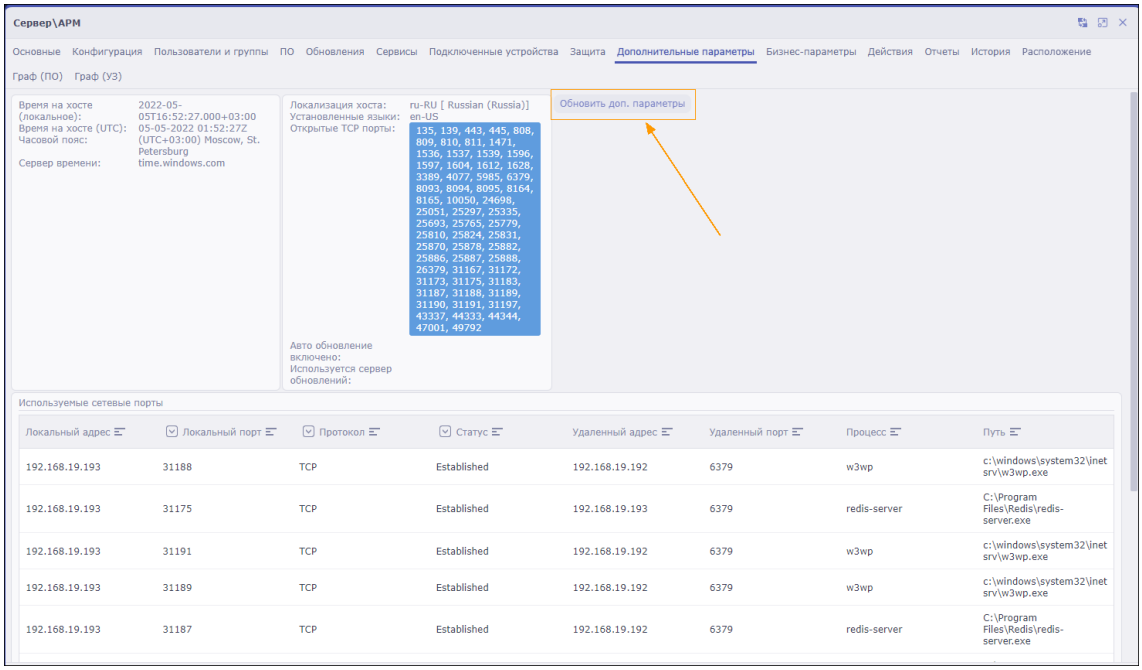


Рисунок 3-18 – Запуск обновления данных о дополнительных параметрах актива

3.2.6 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.

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.

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.

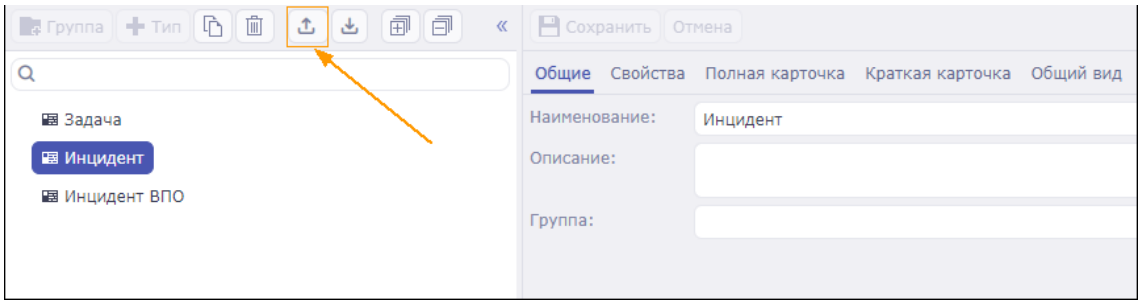


Рисунок 3-19 – Выгрузить настроенный тип объектов

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.
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;

Экспортируемые данные	Зависимости
	— 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: — 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:

Экспортируемые данные	Зависимости
	— 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	
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

Экспортируемые данные	Зависимости
	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. 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:

Экспортируемые данные	Зависимости
	— 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). — 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.

Экспортируемые данные	Зависимости
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*: 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).
Группа отчетов	Все отчеты из группы и все сопутствующие отчетам зависимости — см. пункт отчет.

Экспортируемые данные	Зависимости
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.

3.2.7 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.

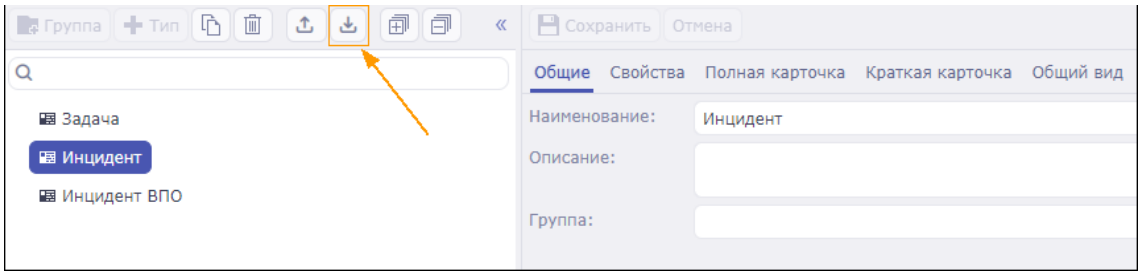


Рисунок 3-20 – Загрузить тип объектов

3.2.7.1 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 OneVision.ImportTool, на вход которому передать zip архив с импортируемыми данными. Пример команды для сервера под управлением CentOS приведен ниже:

```
sudo ./OneVision.ImportTool ./archive.zip
```

3) Таким образом данные импортированы на Платформу.

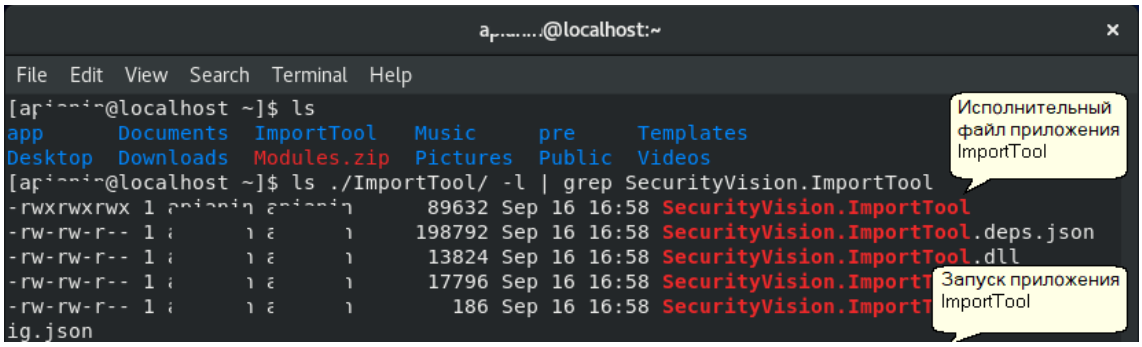


Рисунок 3-21 – Пример импорта данных через командную строку

3.2.8 Разделение пользователей портала по контентно-ролевой модели, согласно выполняемым ими функциям

Данная функция обеспечивает реализацию ролевой модели разграничения доступа, с возможностью задавать разрешения для просмотра данных и/или использования определенного функционала.

В системе предустановлены следующие роли:

- Администратор. Пользователь, обладающий данной ролью, обеспечивает полноценное функционирование системы
- Пользователь. Выполняет работы по обеспечению информационной безопасности организации в соответствии с возложенными на него обязанностями

Сотрудники, обладающие ролью Администратора, обладают следующими правами:

– Управление инцидентами:

- Просмотр типов заявок;
- Управление типами заявок;
- Просмотр свойств заявок;
- Управление свойствами заявок;

- Просмотр рабочих процессов;
- Управление рабочими процессами.

- Управление активами:
  - Просмотр типов активов;
  - Управление типами активов;
  - Просмотр свойств активов;
  - Управление свойствами активов;
- Управление отчетами:
  - Создание шаблонов отчетов;
  - Управление шаблонами отчетов.
- Визуализация данных и состояния:
  - Управление шаблонами дашбордов;
  - Управление источниками данных.
- Управление доступом:
  - Просмотр пользователей Платформы;
  - Управление пользователями Платформы;
  - Управление ролями пользователей.
- Управление оповещением:
  - Управление каналами связи оповещения;
  - Управление пользовательскими событиями оповещения;

Сотрудники организации, обладающие ролью Пользователя Платформы, обладают следующими правами:

- Управление инцидентами:
  - Просмотр инцидентов;
  - Управление инцидентами в соответствии с рабочим процессом.
- Управление активами:
  - Просмотр активов;
  - Создание активов;
  - Управление активами;
  - Просмотр диаграмм связей активов;

    - Управление диаграммами связей активов;
- Управление отчетами:
    - Создание отчетов.
- Визуализация данных и состояния:
    - Формирование и просмотр дашбордов.

ПРИЛОЖЕНИЕ А. ЭКСПОРТ В ФОНОВОМ РЕЖИМЕ

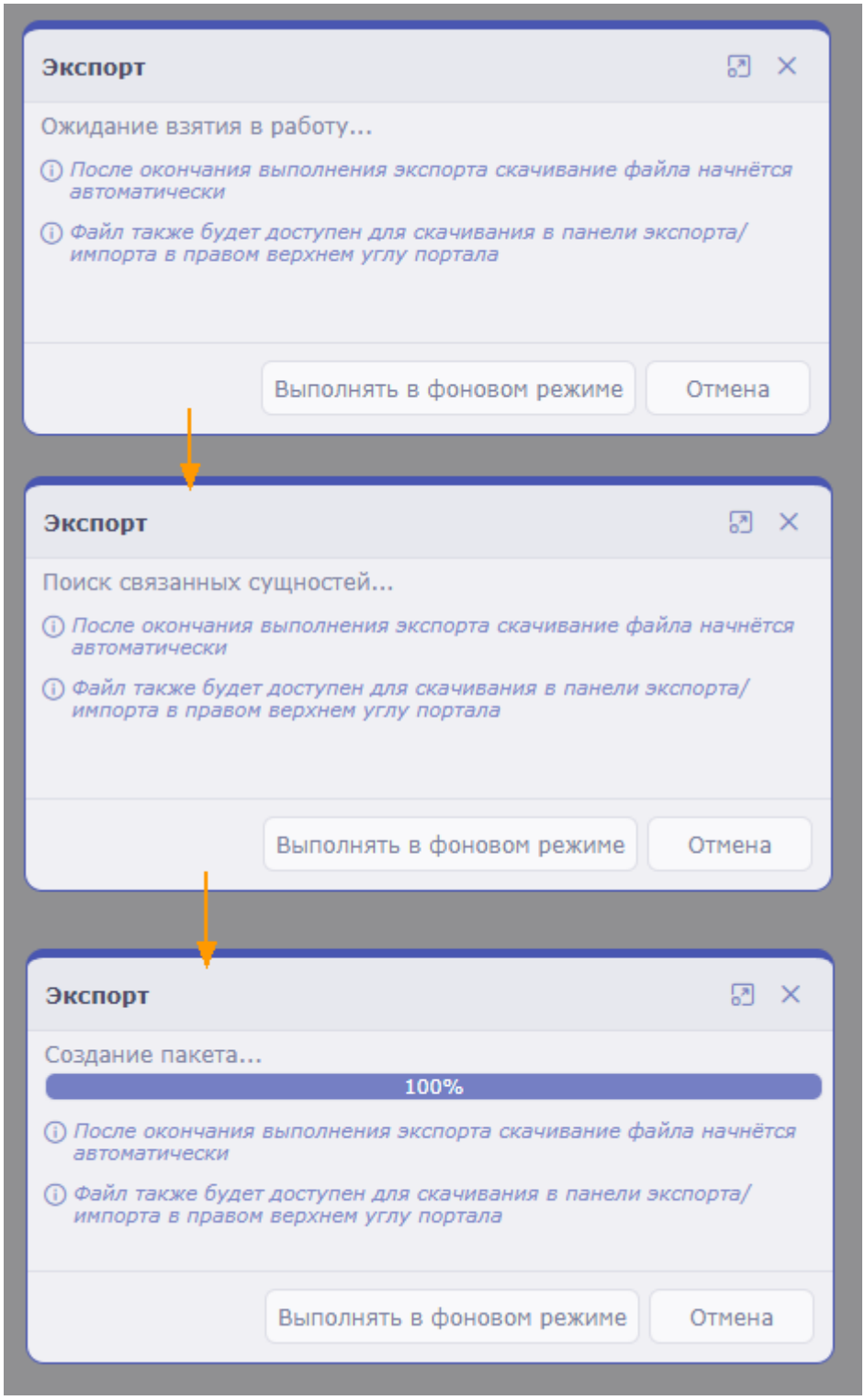


Рисунок 0-1 – Экспорт данных

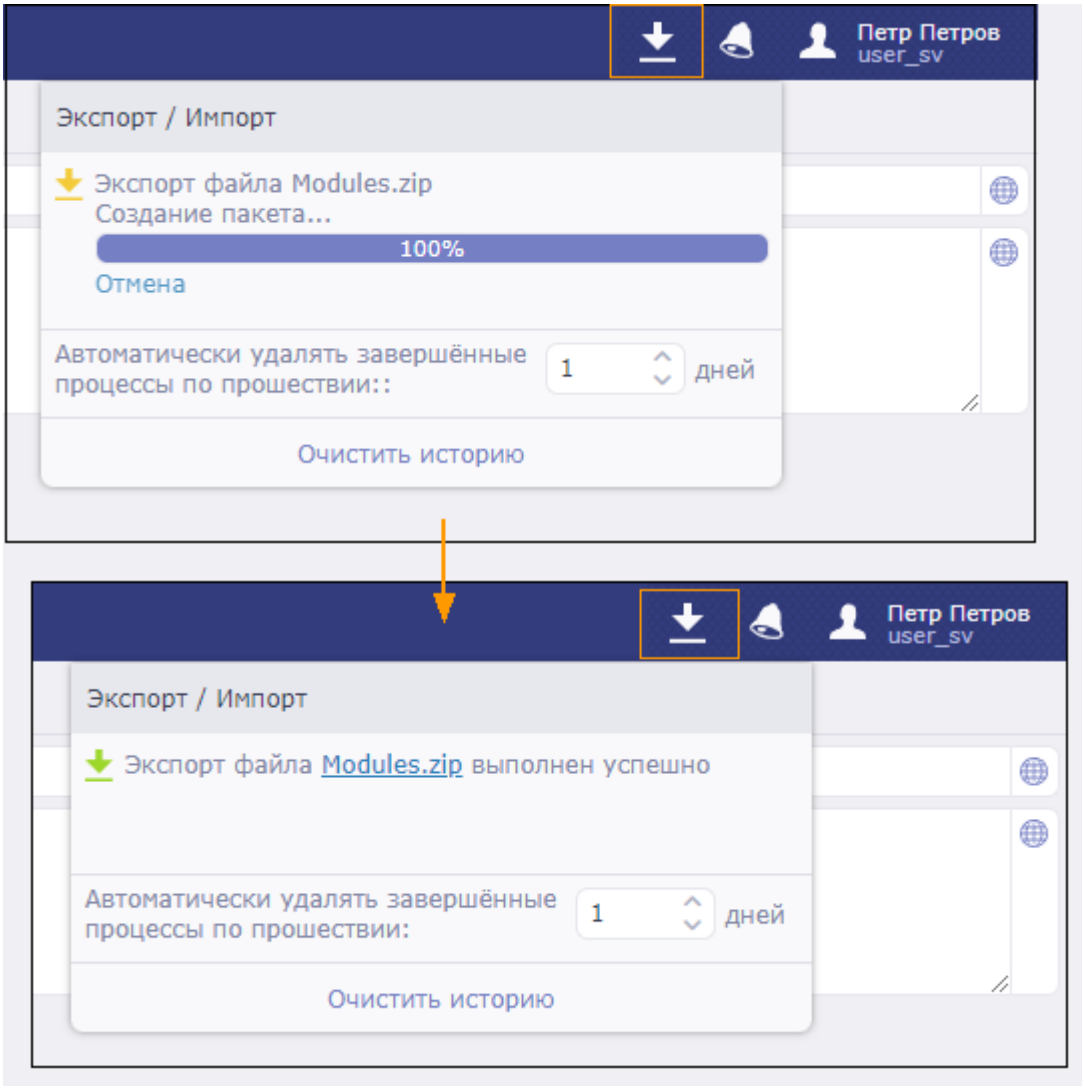


Рисунок 0-2 – Экспорт данных в фоновом режиме

ПРИЛОЖЕНИЕ Б. ОПИСАНИЕ РАБОЧИХ ПРОЦЕССОВ ОБРАБОТКИ ИНЦИДЕНТА

Описание рабочего процесса заявки типа «Простой инцидент»

1. Началом рабочего процесса является момент создания заявки типа «Простой 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 основная информация об инциденте. Обязательными для заполнения на данном этапе являются следующие поля:

- Наименование
- Источник информации об инциденте

Также заполняется информация о связанных активах.

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

2. На этапе идентификации инцидента осуществляется прием инцидента в работу специалистом, определение контекста инцидента, критичности, зоны ответственности. На данном этапе обязательными для заполнения являются следующие поля:

- Описание;
- Опасность;
- Исполнитель;

На этапе идентификации также возможно отметить инцидент как ложноположительный.

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

4. На этапе реагирования осуществляется взятие инцидента в работу исполнителем, статус заявки меняется на «В работе».

После выполнения действий по реагированию и внесения соответствующей информации в поле «Предпринятые меры», осуществляется переход на следующий этап рабочего процесса и устанавливается статус «Обработка завершена».

5. На этапе анализа выполняются действия по анализу инцидента

После завершения анализа инцидента и выполнения необходимых действий, инцидент может быть закрыт, статус заявки устанавливается в «Закрыт».