INNOSTAGE

ПРОГРАММНЫЙ ПРОДУКТ СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ NEXTSTAGE SECURITY PLATFORM: NEXTSTAGE IRP

Руководство пользователя

2020

АННОТАЦИЯ

Данный документ предназначен для пользователей программного продукта «Система управления информационной безопасностью **NextSTage Security Platform: NextStage IRP**» (далее - **NextStage IRP**) и включает описание функционала графического интерфейса данного программного продукта, а также механизм работы с учетными карточками объектов и операции, которые выполняют пользователи при работе с **NextStage IRP.**

СОДЕРЖАНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение и условия применения

Программный продукт **NextStage IRP** предназначен для автоматизации процессов регистрации инцидентов ИБ, а также реагирования на них, управления ИТ-активами, формирования и отображения динамической отчетности, организации взаимодействия с Национальным координационным центром по компьютерным инцидентам (далее - НКЦКИ).

NextStage IRP обеспечивает автоматизацию следующих функций:

- управление инцидентами ИБ в части их ручной и автоматической регистрации, назначения ответственных, редактирования учетных карточек, фиксации результатов реагирования и расследования;
- реализация автоматических сценариев реагирования на инциденты ИБ;
- управление ИТ-активами;
- сбор информации об используемых ИТ-активах посредством сканирования сети организации;
- выгрузка проектов файлов для дальнейшей передачи в НКЦКИ в соответствии с форматами представления сведений в НКЦКИ;
- отображение сводных статистических и детальных данных об инцидентах ИБ и используемых ИТ-активах на информационных панелях (дашбордах).

1.2 Перечень функциональных модулей

Программный продукт **NextStage IRP** включает следующие функциональные модули:

- Личный кабинет пользователя **NextStage IRP** (далее – Личный кабинет пользователя);
- Модуль сканирования сети;
- Модуль визуализации;
- Модуль выполнения управляющих воздействий (оркестрации).

2 ОБЩИЕ ИНСТРУКЦИИ ПО ИСПОЛЬЗОВАНИЮ ЛИЧНОГО КАБИНЕТА ПОЛЬЗОВАТЕЛЯ NEXTSTAGE IRP

Графический пользовательский интерфейс Личного кабинета пользователя представляет собой веб-приложение, которое выполняется на автоматизированном рабочем месте пользователя.

2.1 Программно-аппаратные требования

Для работы с Личным кабинетом пользователя рекомендуется использовать автоматизированное рабочее место со следующими аппаратными требованиями:

1) Монитор с разрешением 1920x1080, масштабирование дисплея 100%.
2) Диагональ экрана от 17".

Для настройки расширения экрана необходимо выполнить следующие действия[1]:

1) В меню Пуск выбрать раздел «Параметры».
2) В открывшейся форме выбрать раздел «Система» и подраздел «Дисплей».
3) В открывшейся форме (Рисунок 2.1) в разделе «Расширение экрана» выбрать значение 1920x1080 из выпадающего списка.

[1] Действия по настройке описаны для операционной системы MS Windows 10.

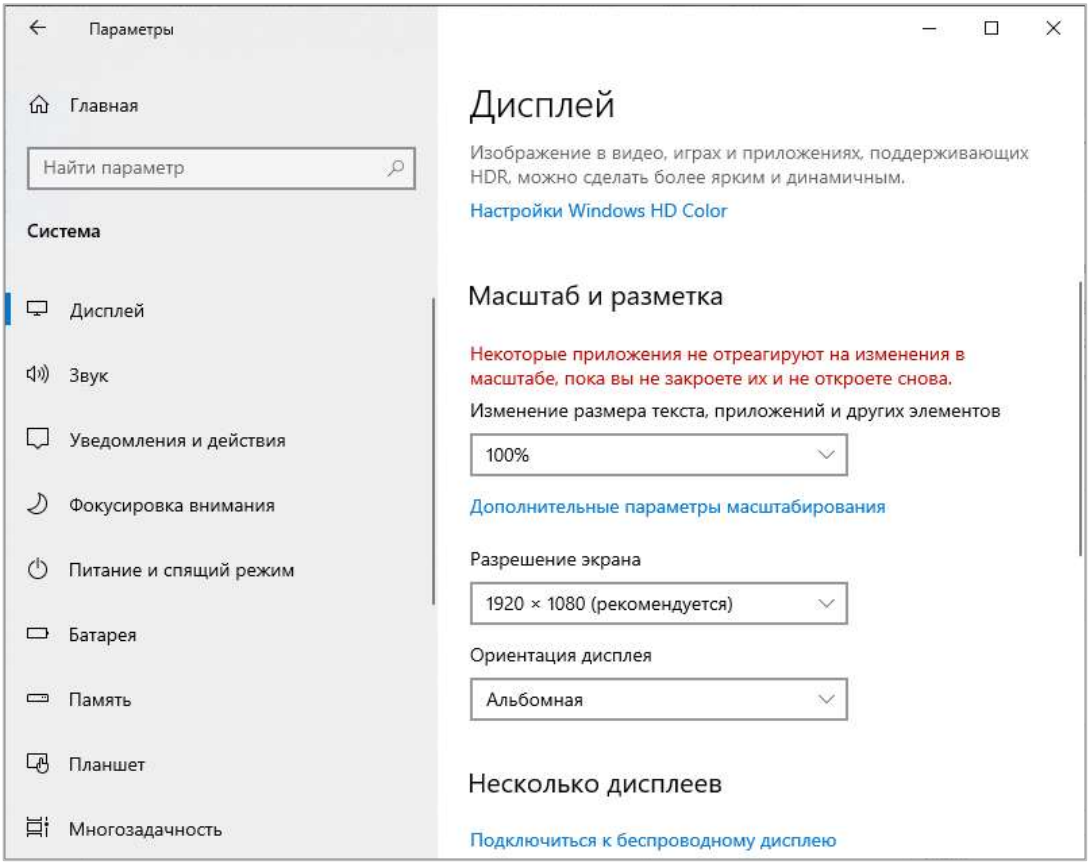

Рисунок 2.1 – Форма настройки расширения экрана

Для настройки масштабирования дисплея необходимо выполнить следующие действия[2]:

1) В меню пуск выбрать раздел «Параметры».

2) В открывшейся форме выбрать раздел «Система» и подраздел «Дисплей».

3) В открывшейся форме (Рисунок 2.2) в разделе «Изменение размера текста, приложений и других элементов» выбрать значение 100% из выпадающего списка.

[2] Действия для настройки описаны для операционной системы MS Windows 10.

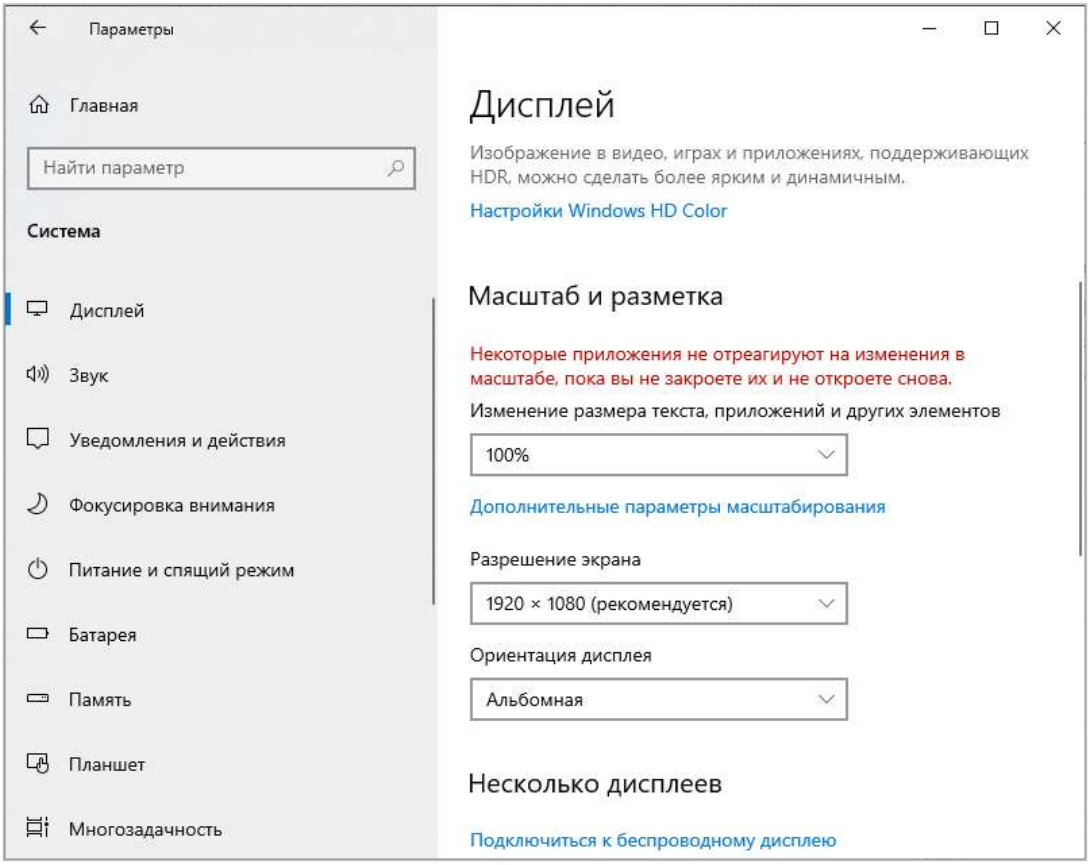

Рисунок 2.2 – Форма настройки масштабирования дисплея

В качестве веб-обозревателя рекомендуется использовать Google Chrome 87 версии или Internet Explorer 11 версии.

2.2 Вход в графический интерфейс пользователя

Для входа в Личный кабинет пользователя необходимо выполнить следующие действия:

1) На рабочей станции запустить веб-обозреватель.

2) В адресной строке веб-обозревателя указать адрес Личного кабинета пользователя (адрес формируется при настройке программного продукта администратором).

3) В открывшейся форме (Рисунок 2.3) указать данные учетной записи пользователя и осуществить вход в Личный кабинет пользователя, нажав на кнопку «**Войти**». Для получения первоначального логина и пароля необходимо обратиться к администратору программного продукта.

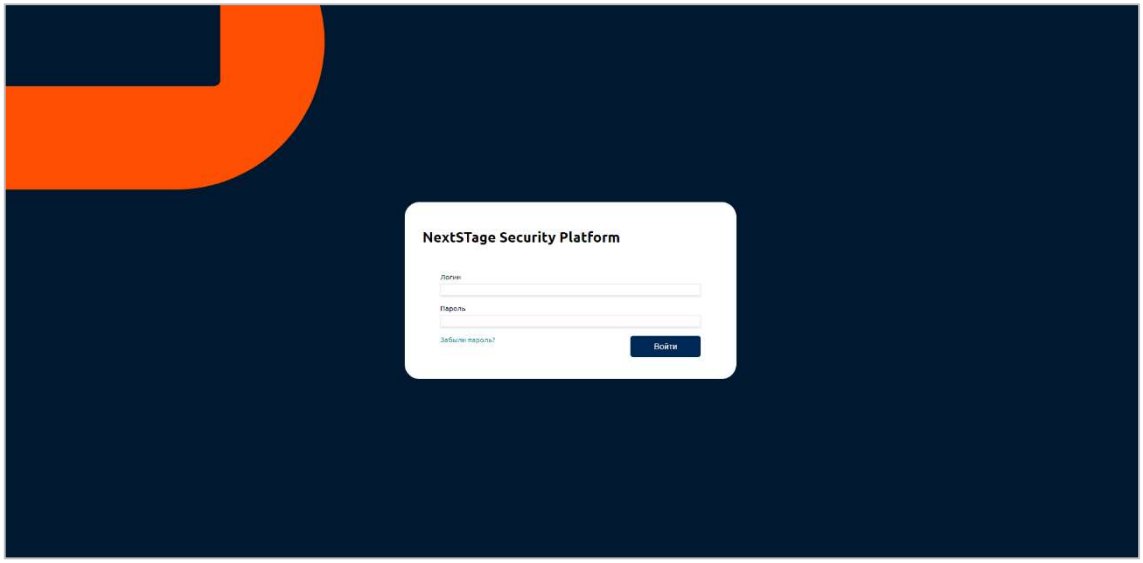

Рисунок 2.3 – Форма входа в Систему

Для выхода из Личного кабинета пользователя необходимо нажать на кнопку , расположенную в правой верхнем углу экранной формы.

2.3 Восстановление пароля пользователя

Для изменения пароля необходимо на форме входа в Личный кабинет пользователя нажать на ссылку «**Забыли пароль?**». Откроется форма (Рисунок 2.4) для ввода адреса электронной почты.

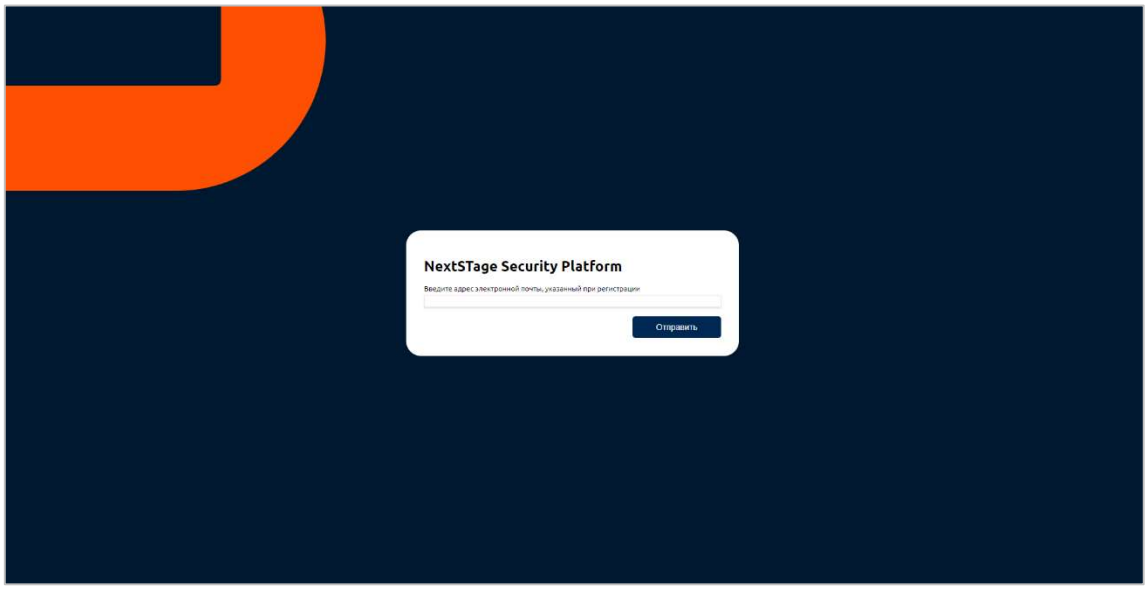

Рисунок 2.4 – Форма восстановления пароля

После ввода адреса электронной почты и нажатии на кнопку «**Отправить**», на указанный адрес придет письмо со ссылкой на восстановление пароля. Для изменения пароля необходимо перейти по ссылке из письма и ввести новый пароль.

2.4 Описание графического интерфейса пользователя

Графический интерфейс Личного кабинета пользователя состоит из следующих частей:

1) Главное меню (Рисунок 2.5) располагается в левой части экранной формы и позволяет получить доступ к основным функциям Системы.

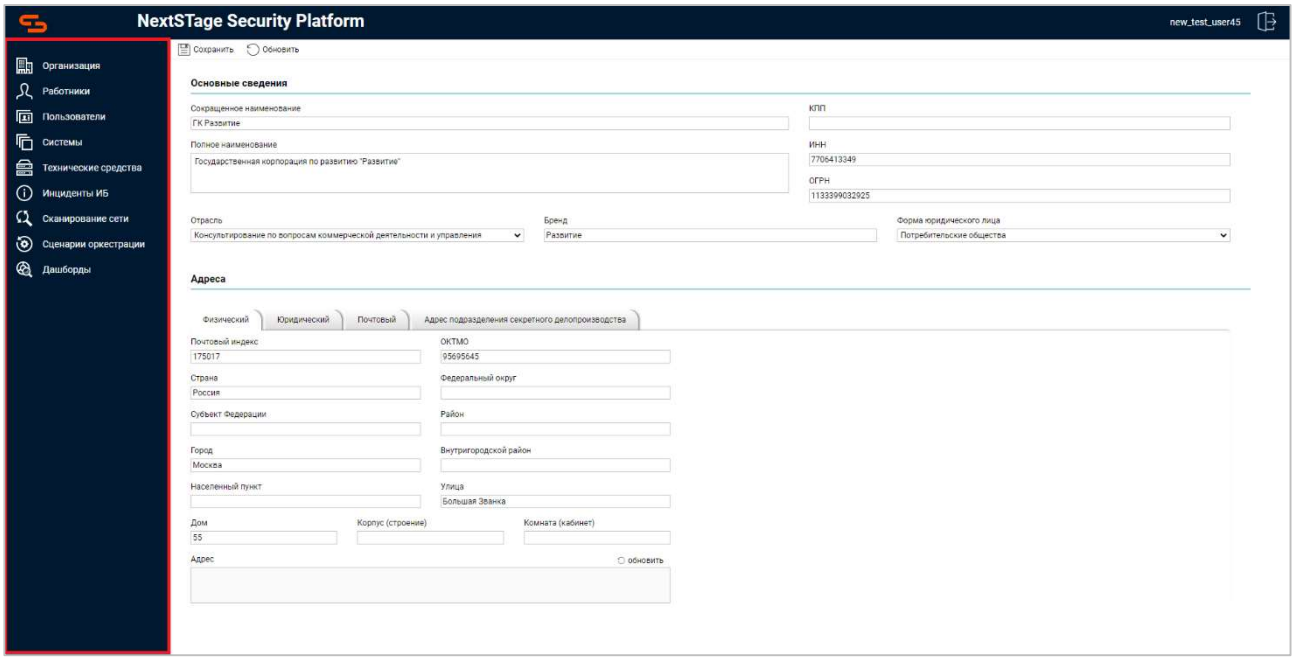

Рисунок 2.5 – Главное меню

2) Рабочая область (Рисунок 2.6) позволяет осуществлять работу с объектами Системы.

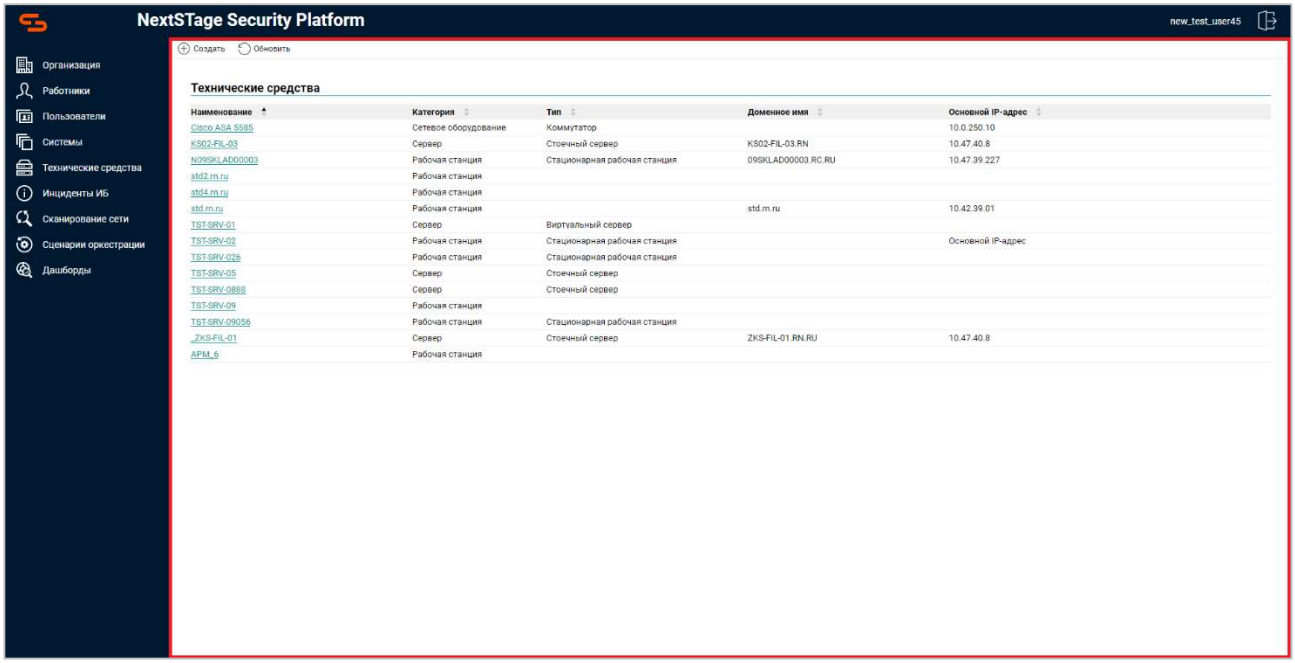

Рисунок 2.6 – Рабочая область

3) Строка меню (Рисунок 2.7) позволяет осуществлять определенные действия с объектами Системы.

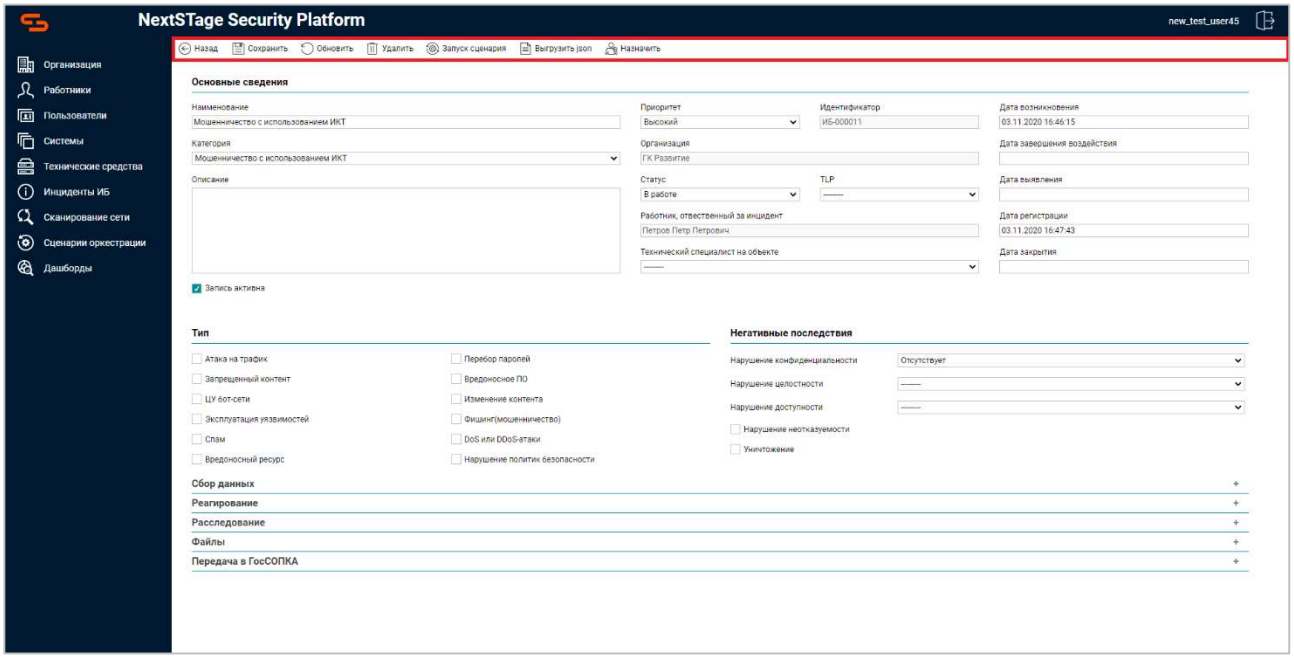

Рисунок 2.7 – Строка меню

2.5 Описание работы со стандартными полями

В Системе используются следующие основные типы полей:

1) Текстовое поле (Рисунок 2.8) предназначено для ввода небольшого объема текста без переноса строк.

Рисунок 2.8 – Вид текстового поля

Информация в данное поле вводится простым текстовым вводом. На длину поля установлено ограничение.

Для некоторых атрибутов объектов в текстовом поле доступна дополнительная функция «Заполнить» для заполнения значения из справочника. Для вызова функции «Заполнить» необходимо нажать кнопку «**Заполнить**» (☰) рядом с заполняемым полем. В появившейся форме поиска необходимо указать критерии поиска и нажать кнопку «**Поиск**» (Рисунок 2.9). Для изменения условий поиска необходимо нажать на кнопку «**Изменить фильтр**».

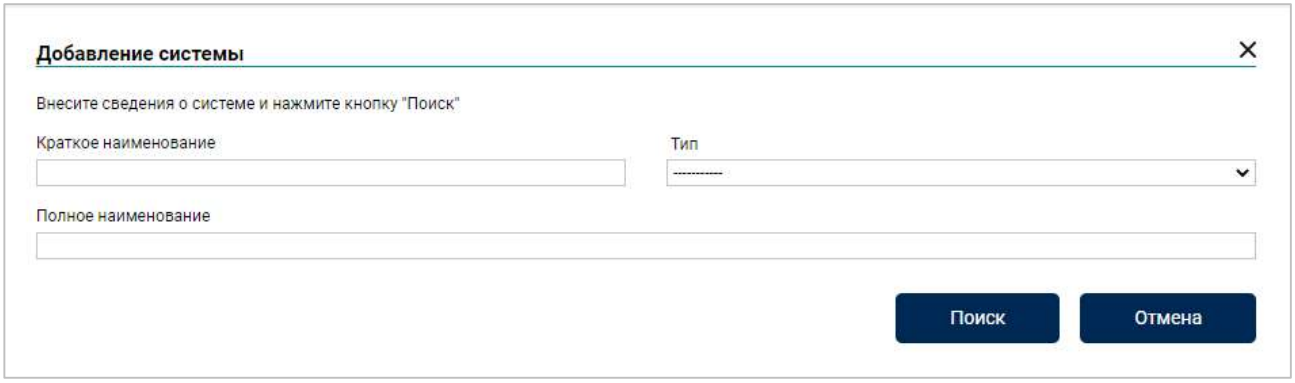

Рисунок 2.9 – Пример формы выбора критериев поиска

В появившемся окне (Рисунок 2.10) необходимо выбрать необходимую запись двойным щелчком левой кнопкой мыши.

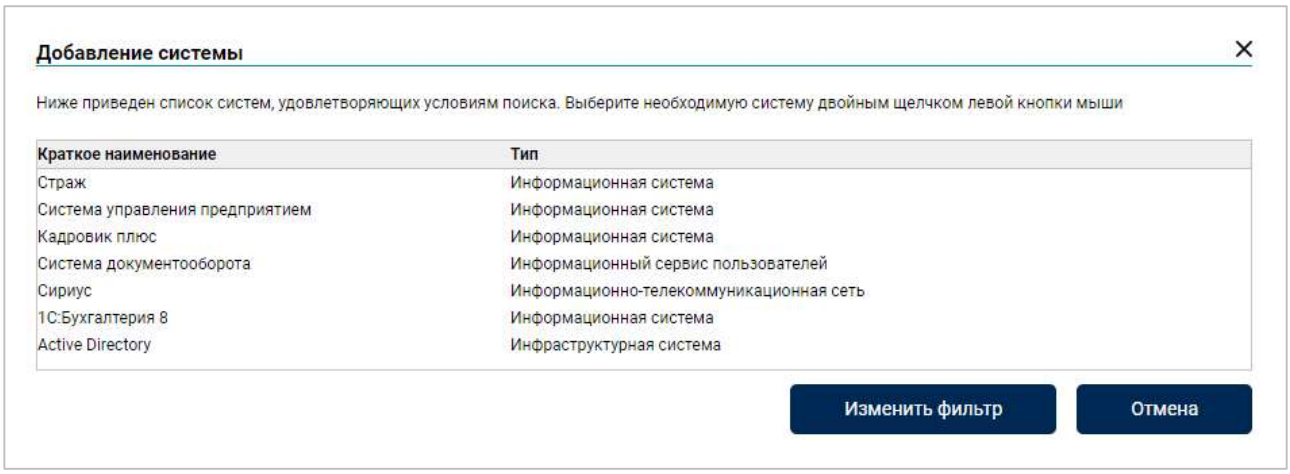

Рисунок 2.10 – Пример формы выбора объекта

2) Многострочное текстовое поле (Рисунок 2.11). Информация в данное поле вводится простым текстовым вводом. При вводе больших текстовых данных в поле появляется прокрутка.

Рисунок 2.11 –Вид текстового поля

3) Поле с выпадающим списком (Рисунок 2.12).

Рисунок 2.12 – Вид поля с выпадающем списком

Для данного поля предусмотрена возможность выбора значения поля из выпадающего списка.

4) Поле - чек-бокс (флаговое поле). Для данного поля доступны два состояния: ☑ включено (обозначает ответ «Да») и ☐ выключено (обозначает ответ «Нет»);

5) Радиокнопка. Данное поле позволяет выбрать один пункт из определенного набора. Для поля доступны два состояния: включено (обозначает ответ «Да») и выключено (обозначает ответ «Нет»);

6) Поле с типом «Дата и время». Данное поле в Системе заполняется в формате ДД.ММ.ГГГГ ЧЧ:ММ:СС, например, 07.04.2020 13:15:30. Для заполнения значения поля с типом «Дата и время» используется календарь (Рисунок 2.13).

Рисунок 2.13 – Календарь

Для вызова календаря необходимо нажать на заполняемое поле. Описание элементов календаря приведено в таблице ниже (Таблица 2.1).

Таблица 2.1 – Описание элементов календаря

Элемент календаря	Описание
	Элемент используется для выбора месяца и года
	Элемент используется для выбора даты
	Элемент используется для выбора времени (верхний бегунок служит для указания часа, нижний бегунок служит для указания минуты).

2.6 Описание работы с таблицами

В Системе используются следующие основные типы таблиц:

1) Таблица с простым вводом (Рисунок 2.14). В данной таблице поля доступны для редактирования. Работа с полями осуществляется в соответствии с п. 2.5 настоящего документа.

Рисунок 2.14 – Пример таблицы с простым вводом

Для добавления новой строки в данную таблицу необходимо нажать на кнопку «**Добавить**» (+).

Для удаления объектов необходимо проставить галочки около необходимых объектов и нажать на кнопку «**Удалить**» (🗑).

2) Таблица с возможностью добавления объектов из базы данных (Рисунок 2.15). Объекты данной таблицы добавляются с помощью вызываемого мастера и не редактируются непосредственно в таблице.

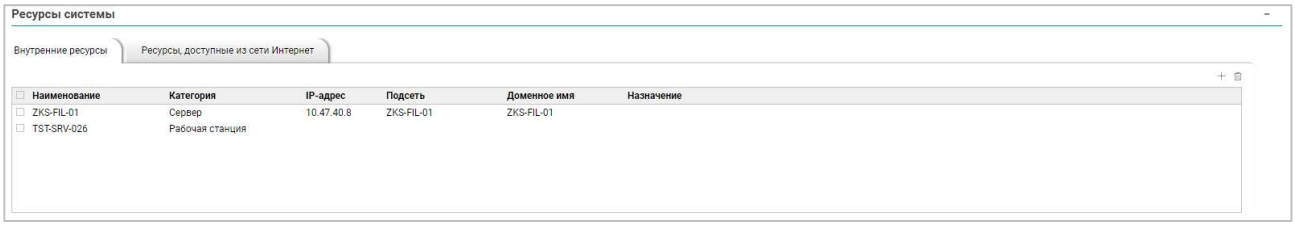

Рисунок 2.15 – Пример таблицы с выбором объектов

Для добавления нового объекта в данную таблицу необходимо нажать на кнопку +. Откроется мастер добавления объекта. В зависимости от типа добавляемого объекта в мастере можно создать новый объект и (или) осуществить поиск существующего объекта.

Для создания нового объекта добавления его в таблицу и перехода к добавлению следующего необходимо заполнить поля на форме и нажать кнопку «**Создать**». Для создания

нового объекта добавления его в таблицу и возврата в учетную карточку объекта необходимо заполнить поля на форме и нажать кнопку «**Создать и завершить**».

Для поиска объекта в базе данных необходимо заполнить известные поля и нажать на кнопку «Поиск». Откроется окно со списком объектов, удовлетворяющих условиям поиска. Для добавления объектов необходимо выбрать их из перечня и нажать на кнопку «**Добавить**». Для изменения условий поиска необходимо нажать на кнопку «**Изменить фильтр**».

Для удаления объектов необходимо проставить галочки около необходимых объектов и нажать на кнопку «**Удалить**» (🗑).

2.7 Описание работы с учетными карточками объектов Системы

В интерфейсе Системы доступны функции учета и ведения учетных карточек следующих объектов:

- организация;
- работники;
- системы;
- технические средства;
- инциденты ИБ.

2.7.1 Редактирование учетной карточки организации

Для перехода к учетной карточке организации (Рисунок 2.16) необходимо в главном меню выбрать раздел «Организация». Поля учетной карточки организации заполняются в соответствии с пунктом 2.5 настоящего документа.

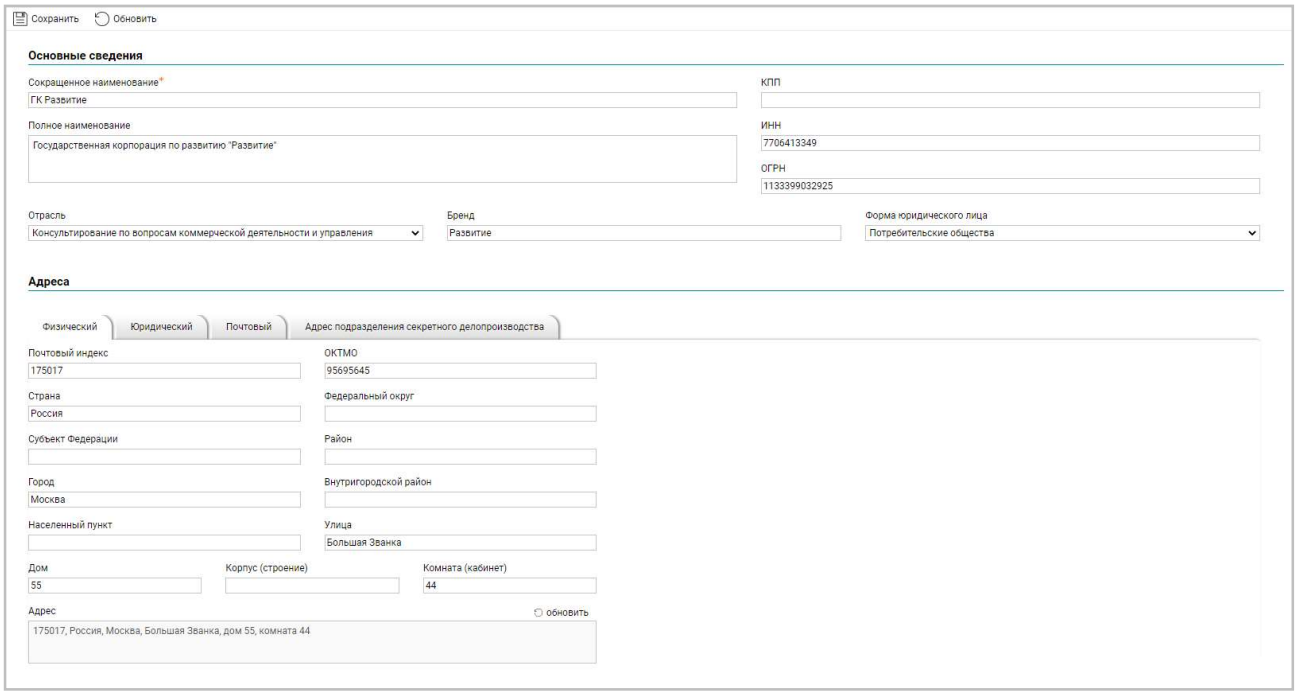

Рисунок 2.16 – Учетная карточка организации

Обязательные поля учетной карточки организации отмечены знаком «*».

Для сохранения внесенных в учетную карточку изменений необходимо нажать на кнопку «**Сохранить**» в строке меню.

Для обновления учетной карточки организации (в том числе возврата к сохраненным значениям полей) необходимо нажать на кнопку «**Обновить**».

2.7.2 Просмотр перечня, создание и редактирование учетных карточек работников

Для просмотра перечня учетных карточек работников необходимо в главном меню выбрать раздел «Работники». Откроется перечень учетных карточек работников (Рисунок 2.17).

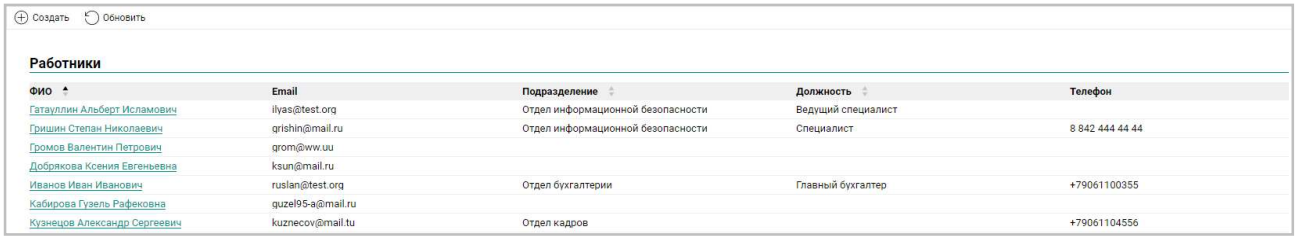

Рисунок 2.17 – Перечень работников

Для перехода к учетной карточке работника необходимо выбрать (щелкнув левой кнопкой мыши) соответствующую строку перечня. Откроется учетная карточка работника (Рисунок 2.18).

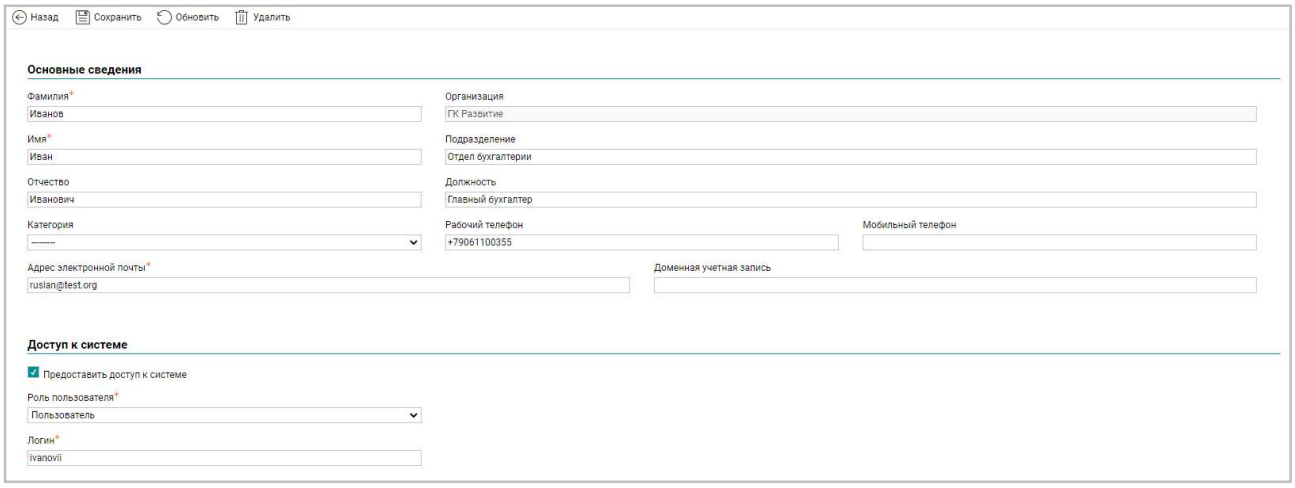

Рисунок 2.18 – Учетная карточка работника

Для обновления элементов перечня необходимо нажать на кнопку «**Обновить**».

Для создания учетной карточки работника необходимо нажать на кнопку «**Создать**». Откроется новая учетная карточка работника (Рисунок 2.19).

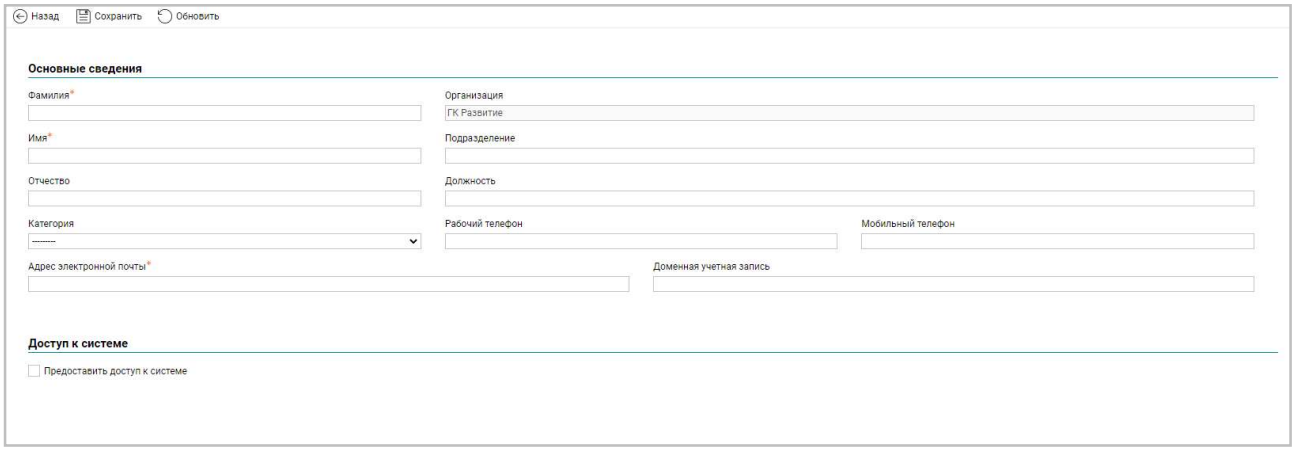

Рисунок 2.19 – Новая учетная карточка работника

Поля учетной карточки работника заполняются в соответствии с пунктом 2.5 настоящего документа.

Обязательные поля учетной карточки работника отмечены знаком «*».

Для создания учетной карточки работника и (или) сохранения внесенных в учетную карточку изменений необходимо нажать на кнопку «**Сохранить**» в строке меню.

Для возврата к перечню работников необходимо нажать на кнопку «**Назад**». Для обновления учетной карточки работника необходимо нажать на кнопку «**Обновить**». Для удаления учетной карточки работника необходимо нажать на кнопку «**Удалить**». Для восстановления ошибочно удаленной карточки работника необходимо обратиться к администратору.

2.7.3 Просмотр перечня, создание и редактирование учетных карточек систем

Для просмотра перечня учетных карточек систем необходимо в главном меню выбрать раздел «Системы». Откроется перечень учетных карточек систем (Рисунок 2.20).

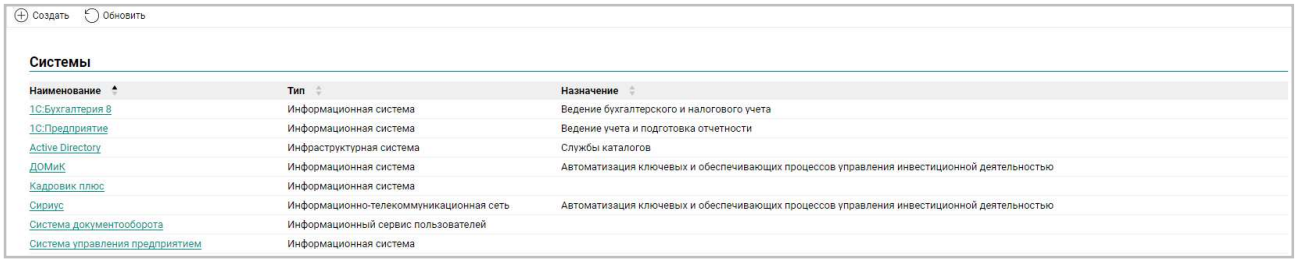

Рисунок 2.20 – Перечень систем

Для перехода к учетной карточке системы необходимо выбрать (щелкнув левой кнопкой мыши) соответствующую строку перечня. Откроется учетная карточка системы (Рисунок 2.21).

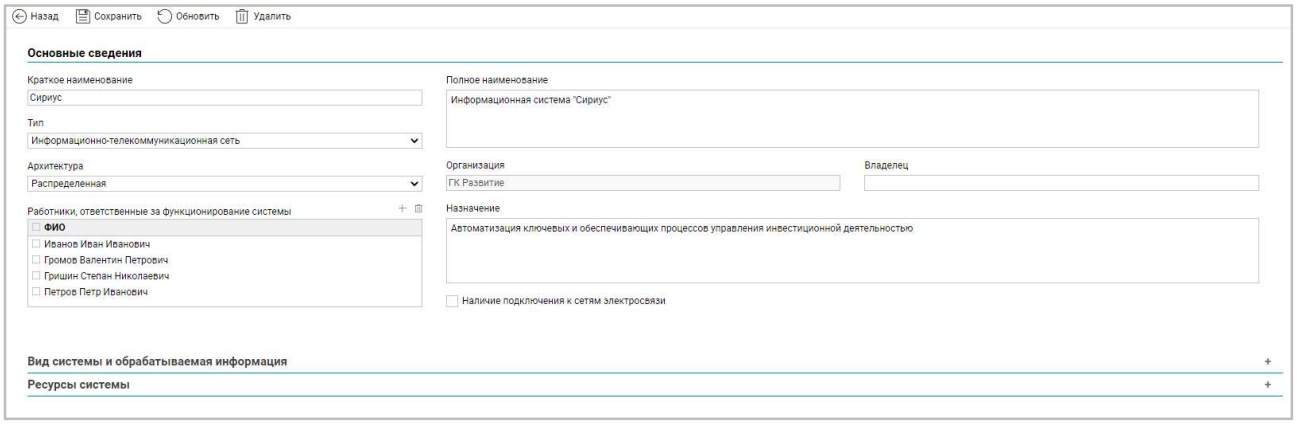

Рисунок 2.21 – Учетная карточка системы

Для обновления элементов перечня необходимо нажать на кнопку «**Обновить**».

Для создания учетной карточки системы необходимо нажать на кнопку «**Создать**». Откроется новая учетная карточка системы (Рисунок 2.22).

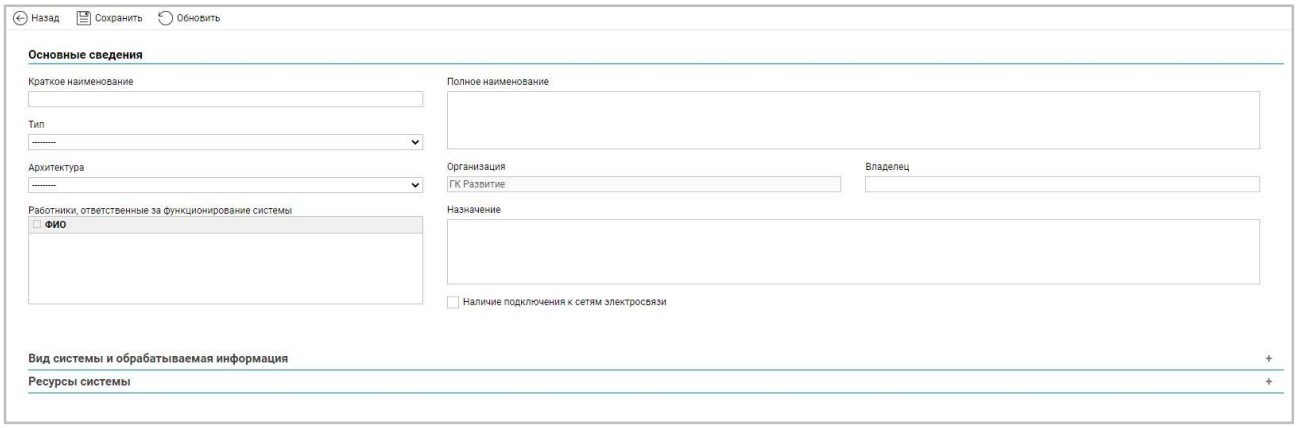

Рисунок 2.22 – Новая учетная карточка системы

Поля учетной карточки системы заполняются в соответствии с пунктом 2.5 настоящего документа.

Обязательные поля учетной карточки системы отмечены знаком «*».

Для создания учетной карточки системы и (или) сохранения внесенных в учетную карточку изменений необходимо нажать на кнопку «**Сохранить**» в строке меню.

Для возврата к перечню систем необходимо нажать на кнопку «**Назад**». Для обновления учетной карточки системы необходимо нажать на кнопку «**Обновить**». Для удаления учетной карточки системы необходимо нажать на кнопку «**Удалить**». Для восстановления ошибочно удаленной карточки системы необходимо обратиться к администратору.

В учетной карточке системы доступны для заполнения следующие разделы:

1) Раздел «**Основные сведения**» (Рисунок 2.23), в котором приводится общая информация о системе. Поля данного раздела заполняются в соответствии с пунктом 2.5 настоящего документа.

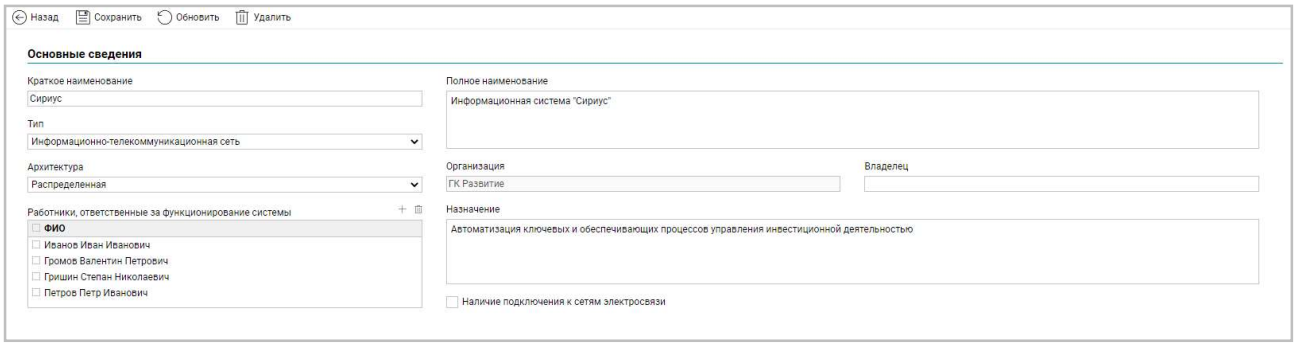

Рисунок 2.23 – Раздел «Основные сведения»

2) Раздел «**Вид системы и обрабатываемая информация**» (Рисунок 2.24), в котором указывается, является ли система объектом КИИ, ИСПДн, АСУ ТП, ГИС или АС, классифицируемой в соответствии с РД Гостехкомиссии России, результаты соответствующей классификации, а также характеристики обрабатываемой в системе информации. Поля данного раздела заполняются в соответствии с пунктом 2.5 настоящего документа.

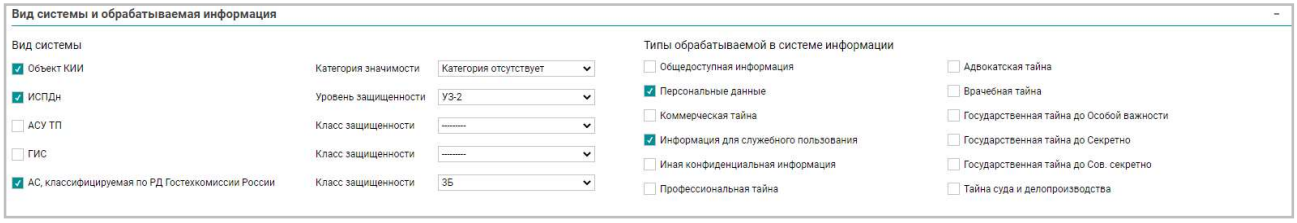

Рисунок 2.24 – Раздел «Вид системы и обрабатываемая информация»

3) Раздел «**Ресурсы системы**», в котором:

– во вкладке «Внутренние ресурсы» в таблице указываются технические средства, которые используются в системе (Рисунок 2.25). Внутренние ресурсы можно добавлять в таблицу только после создания учетной карточки системы (после первого нажатия на кнопку «**Сохранить**»).

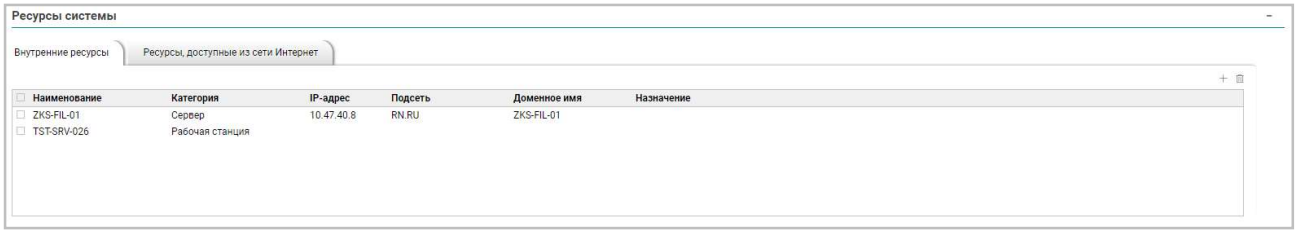

Рисунок 2.25 – Раздел «Ресурсы системы» вкладка «Внутренние ресурсы»

Для добавления внутренних ресурсов в таблицу необходимо нажать на кнопку «**Добавить**» (+). Откроется мастер добавления ресурсов (Рисунок 2.26), в котором необходимо заполнить известные поля и нажать на кнопку «**Поиск**».

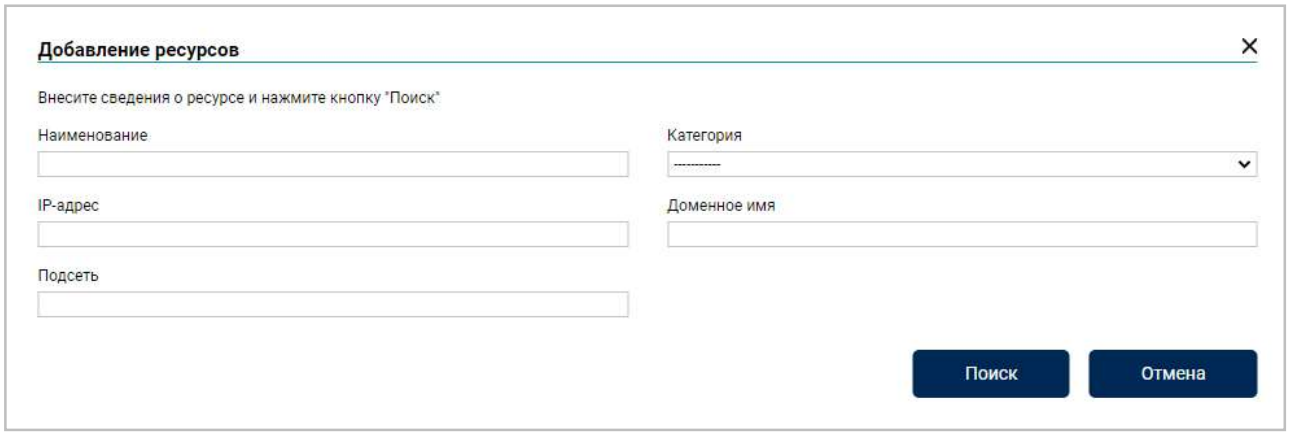

Рисунок 2.26 – Мастер добавления ресурсов

Откроется окно со списком ресурсов, удовлетворяющих условиям поиска (Рисунок 2.27). Для добавления ресурсов необходимо выбрать их из перечня и нажать на кнопку «**Добавить**». Для изменения условий поиска необходимо нажать на кнопку «**Изменить фильтр**».

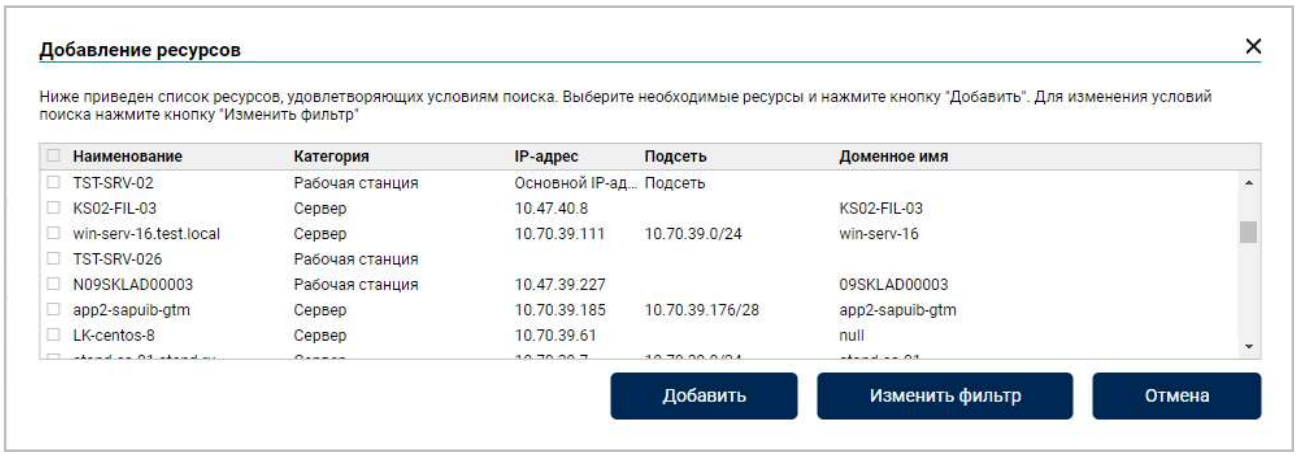

Рисунок 2.27 – Результаты поиска внутренних ресурсов

– во вкладке «Ресурсы, доступные из сети Интернет» в таблице указываются адреса системы, маршрутизируемые из сети Интернет (Рисунок 2.28). Ресурсы, доступные из сети Интернет, можно добавлять в таблицу только после создания учетной карточки системы (после первого нажатия на кнопку «**Сохранить**»).

Рисунок 2.28 – Раздел «Ресурсы системы» вкладка «Ресурсы, доступные из сети Интернет»

Для добавления ресурсов, доступных из сети Интернет, в таблицу необходимо нажать на кнопку «**Добавить**» (+). Откроется мастер добавления ресурсов (Рисунок 2.29).

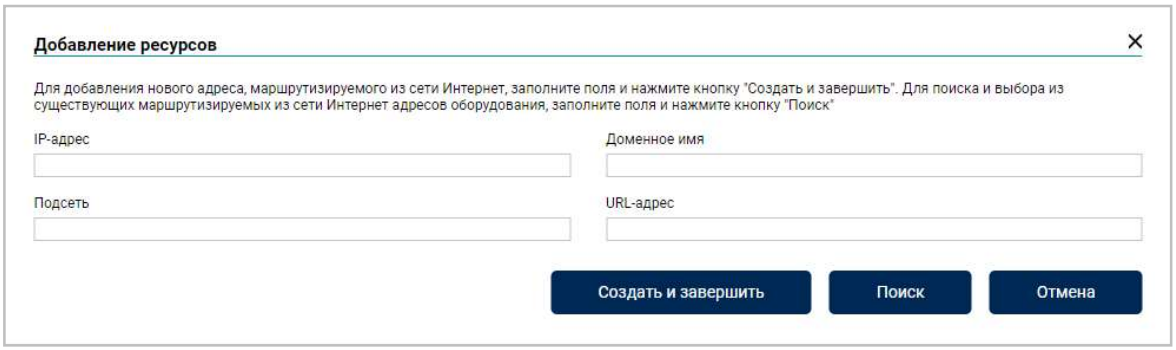

Рисунок 2.29 – Мастер добавления ресурса, доступного из сети Интернет

Для добавления ресурса, доступного из сети Интернет, необходимо заполнить хотя бы одно поле и нажать на кнопку «**Создать и завершить**».

Для поиска и выбора из уже созданных в Системе адресов технических средств, необходимо заполнить известные поля и нажать на кнопку «**Поиск**». Откроется окно со списком ресурсов, удовлетворяющих условиям поиска (Рисунок 2.30).

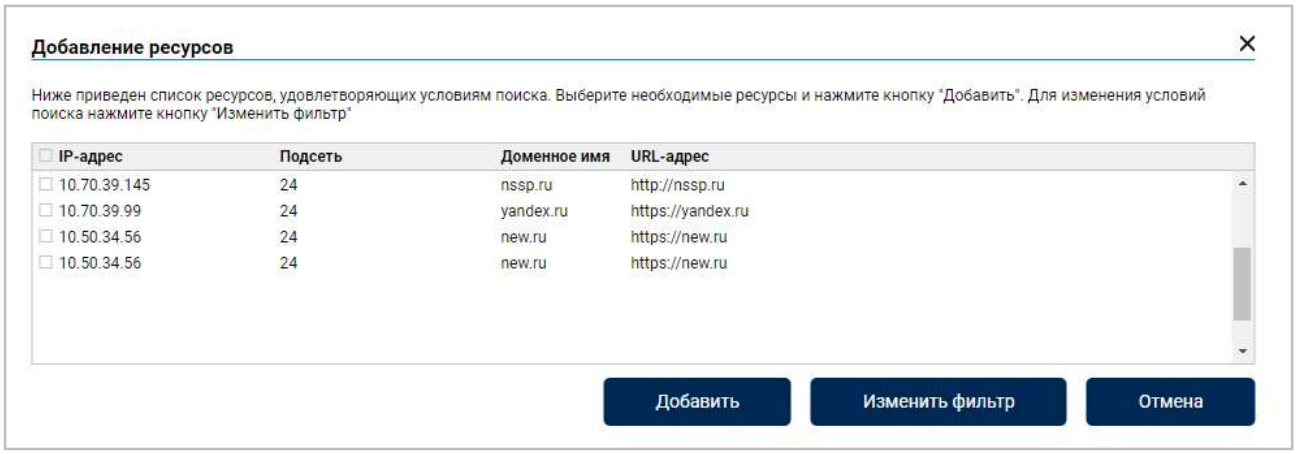

Рисунок 2.30 – Результаты поиска ресурсов, доступных из сети Интернет

Для добавления ресурсов необходимо выбрать их из перечня и нажать на кнопку «**Добавить**». Для изменения условий поиска необходимо нажать на кнопку «**Изменить фильтр**».

2.7.4 Просмотр перечня, создание и редактирование учетных карточек технических средств

Для просмотра перечня учетных карточек технических средств необходимо в главном меню выбрать раздел «Технические средства». Откроется перечень учетных карточек технических средств (Рисунок 2.31).

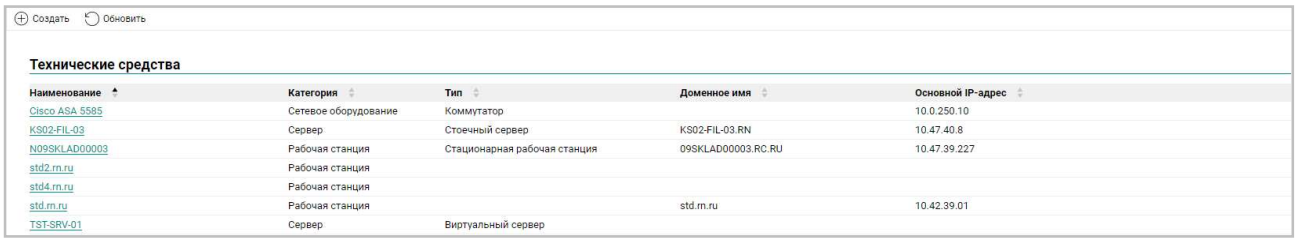

Рисунок 2.31 – Перечень технических средств

Для перехода к учетной карточке технического средства необходимо выбрать (щелкнув левой кнопкой мыши) соответствующую строку перечня. Откроется учетная карточка технического средства (Рисунок 2.32).

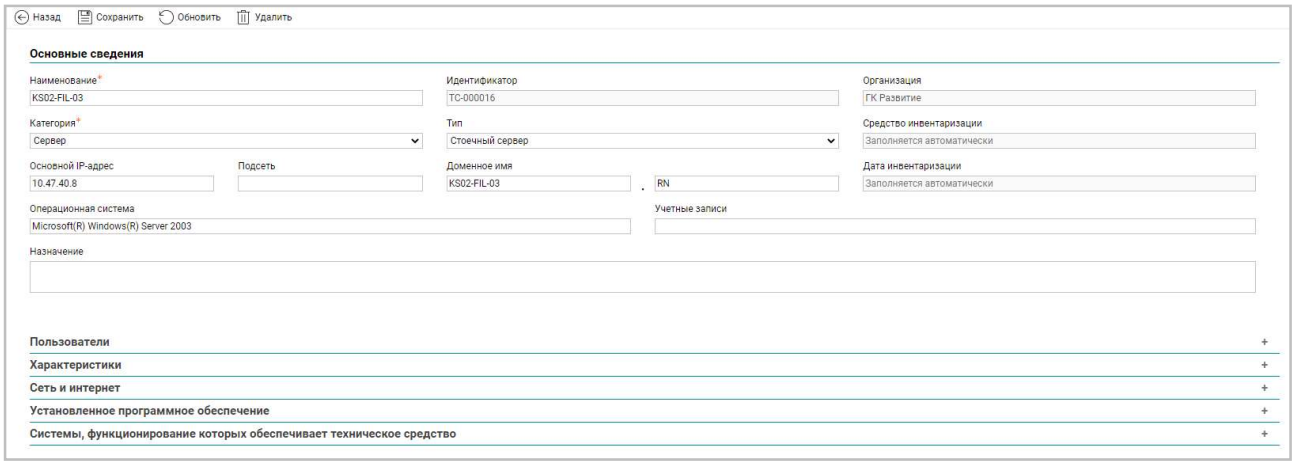

Рисунок 2.32 – Учетная карточка технического средства

Для обновления элементов перечня необходимо нажать на кнопку «**Обновить**».

Для создания учетной карточки технического средства необходимо нажать на кнопку «**Создать**». Откроется новая учетная карточка технического средства (Рисунок 2.33).

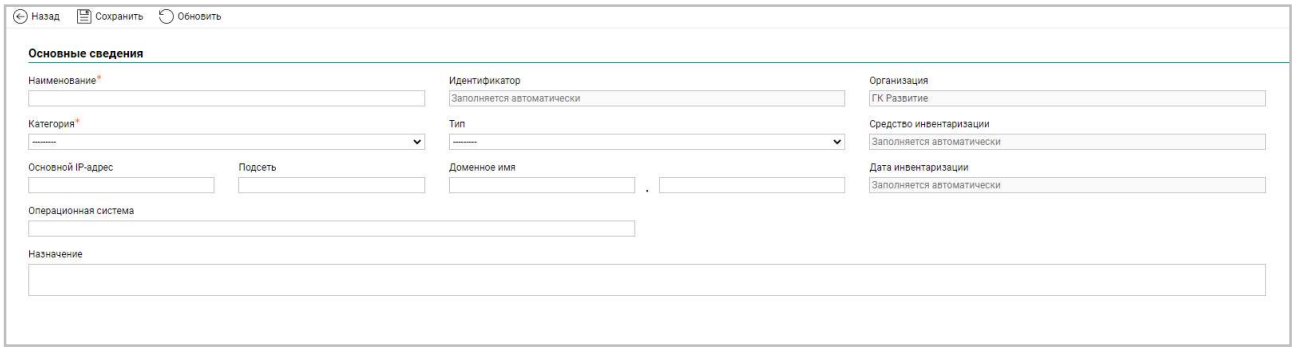

Рисунок 2.33 – Новая учетная карточка технического средства

Поля учетной карточки технического средства заполняются в соответствии с пунктом 2.5 настоящего документа.

Обязательные поля учетной карточки технического средства отмечены знаком «*».

Для создания учетной карточки технического средства и (или) сохранения внесенных в учетную карточку изменений необходимо нажать на кнопку «**Сохранить**» в строке меню.

Для возврата к перечню технических средств необходимо нажать на кнопку «**Назад**». Для обновления учетной карточки технического средства необходимо нажать на кнопку «**Обновить**». Для удаления учетной карточки технического средства необходимо нажать на

кнопку «**Удалить**». Для восстановления ошибочно удаленной карточки технического средства необходимо обратиться к администратору.

В Системе доступны для создания следующие категории учетных карточек технических средств:

– рабочая станция;
– сервер;
– сетевое оборудование;
– периферийное оборудование;
– категория не определена.

В учетных карточках технических средств всех категорий доступен для заполнения раздел «**Основные сведения**» (Рисунок 2.34). В данном разделе приводится общая информация о техническом средстве. Поля «Идентификатор», «Средство инвентаризации» и «Дата инвентаризации» заполняются автоматически, остальные поля данного раздела заполняются в соответствии с пунктом 2.5 настоящего документа.

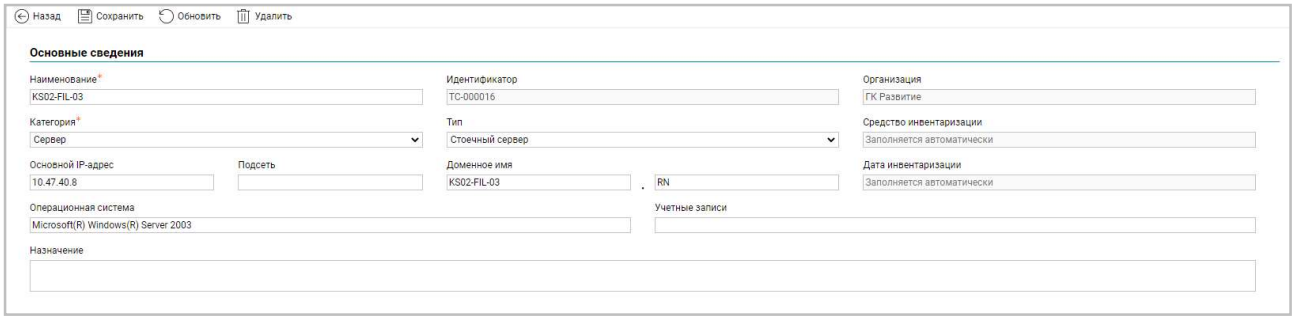

Рисунок 2.34 – Раздел «Основные сведения»

В учетных карточках технических средств категории рабочая станция и сервер доступны для заполнения следующие дополнительные разделы:

1) Раздел «**Пользователи**» (Рисунок 2.35, Рисунок 2.36), в котором приводится информация об учетных записях и группах пользователей технического средства. Таблицы данного раздела заполняются в соответствии с п. 0 настоящего документа.

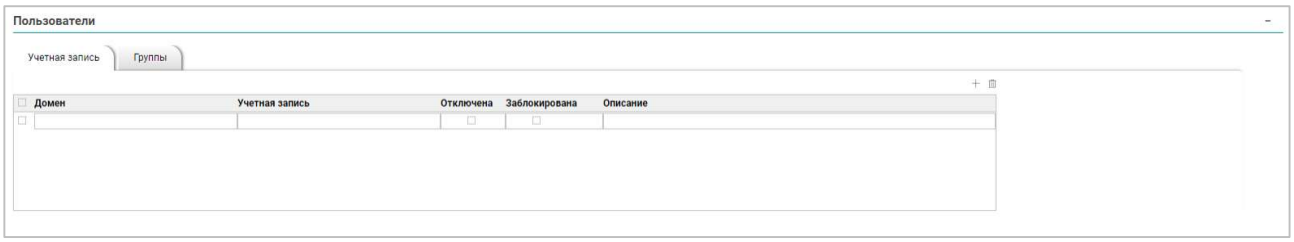

Рисунок 2.35 – Раздел «Пользователи» вкладка «Учетные записи»

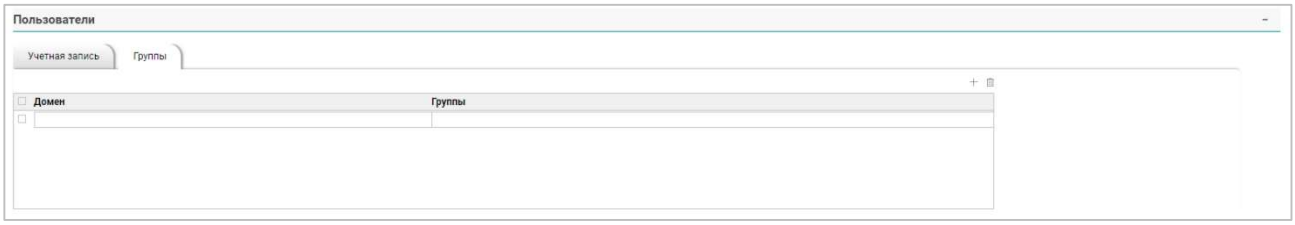

Рисунок 2.36 – Раздел «Пользователи» вкладка «Группы»

2) Раздел «**Характеристики**» (Рисунок 2.37), в котором приводится информация об основных характеристиках технического средства. Поля «Объем оперативной памяти», «Емкость дисков» заполняются автоматически, остальные поля данного раздела заполняются в соответствии с пунктом 2.5 настоящего документа.

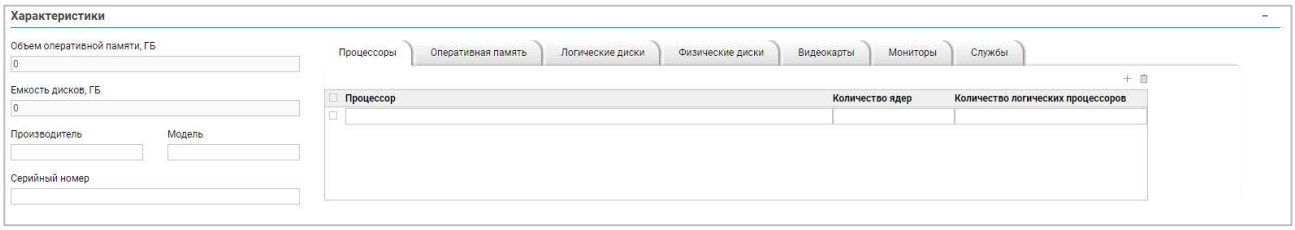

Рисунок 2.37 – Раздел «Характеристики»

– во вкладке «Процессоры» (Рисунок 2.38) приводится информация о характеристиках процессоров технического средства. Таблица данного раздела заполняется в соответствии с п. 2.6 настоящего документа.

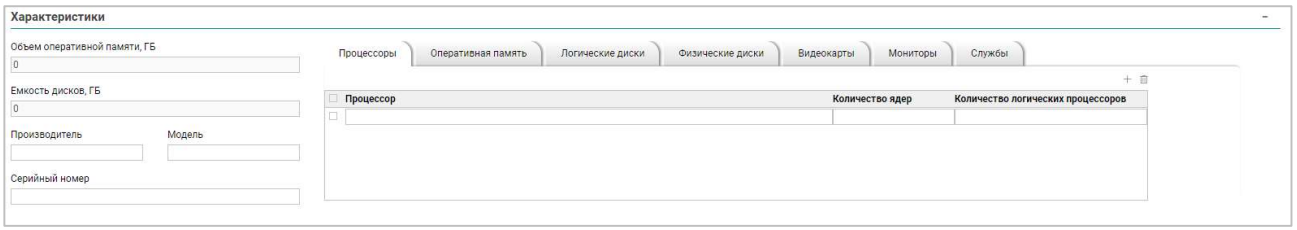

Рисунок 2.38 – Раздел «Характеристики» вкладка «Процессоры»

– во вкладке «Оперативная память» (Рисунок 2.39) приводится информация о производителе и объеме оперативной памяти технического средства. Таблица данного раздела заполняется в соответствии с п. 2.6 настоящего документа.

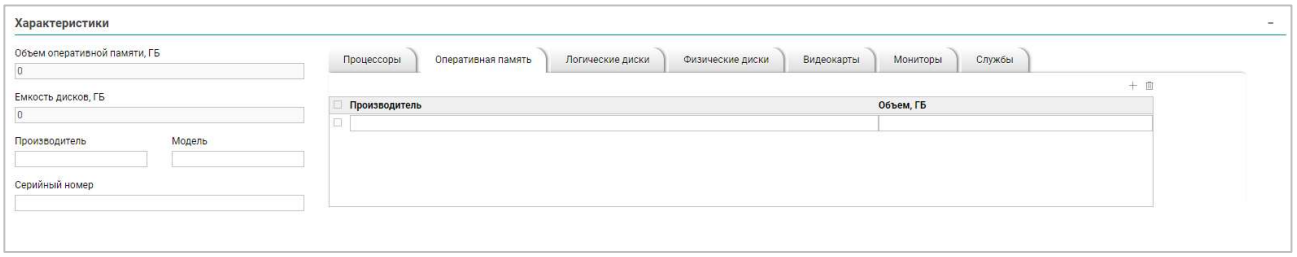

Рисунок 2.39 – Раздел «Характеристики» вкладка «Оперативная память»

– во вкладке «Логические диски» (Рисунок 2.40) приводится информация о логических дисках технического средства. Таблица данного раздела заполняется в соответствии с п. 2.6 настоящего документа.

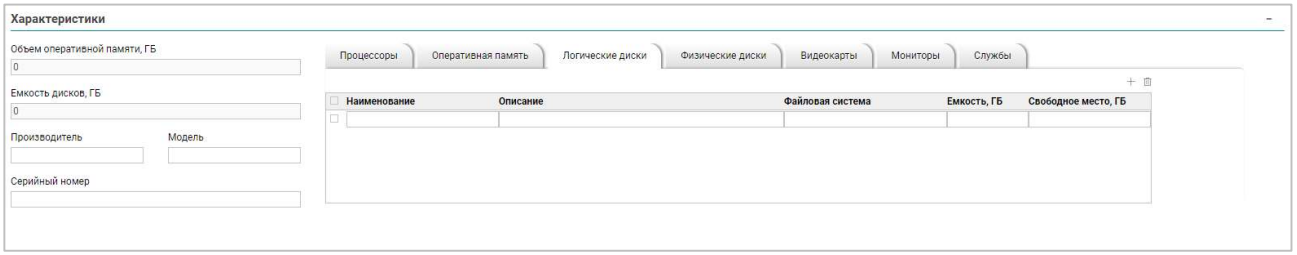

Рисунок 2.40 – Раздел «Характеристики» вкладка «Логические диски»

– во вкладке «Физические диски» (Рисунок 2.41) приводится информация о физических дисках технического средства. Таблица данного раздела заполняется в соответствии с п. 2.6 настоящего документа.

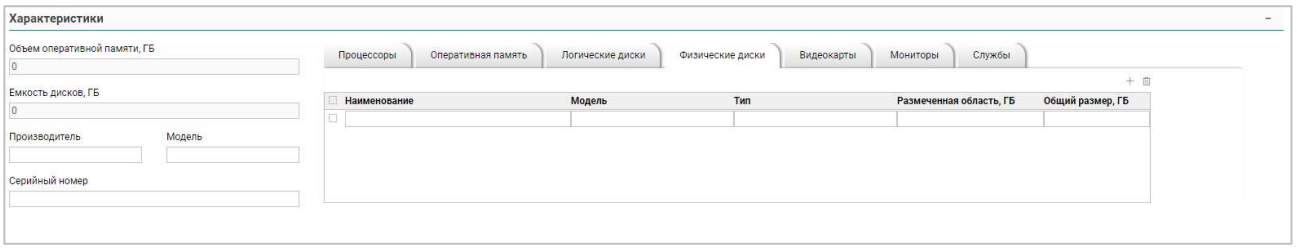

Рисунок 2.41 – Раздел «Характеристики» вкладка «Физические диски»

– во вкладке «Видеокарты» (Рисунок 2.42) приводится информация о видеокартах, установленных на техническом средстве. Таблица данного раздела заполняется в соответствии с п. 2.6 настоящего документа.

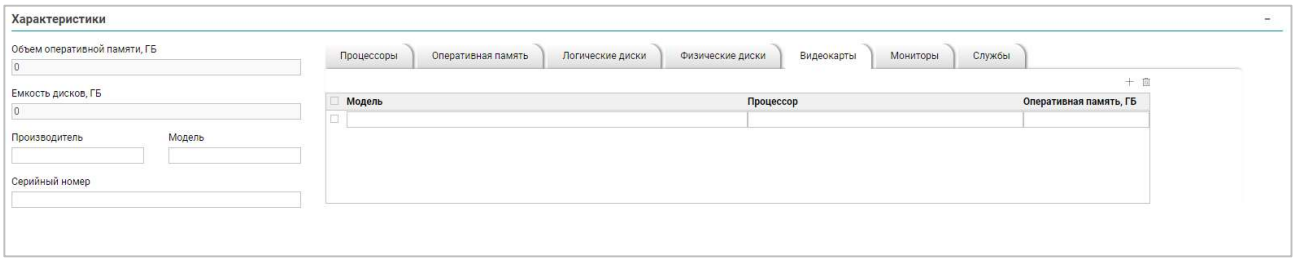

Рисунок 2.42 – Раздел «Характеристики» вкладка «Видеокарты»

– во вкладке «Мониторы» (Рисунок 2.43) приводится информация о мониторах, подключенных к техническому средству. Таблица данного раздела заполняется в соответствии с п. 2.6 настоящего документа.

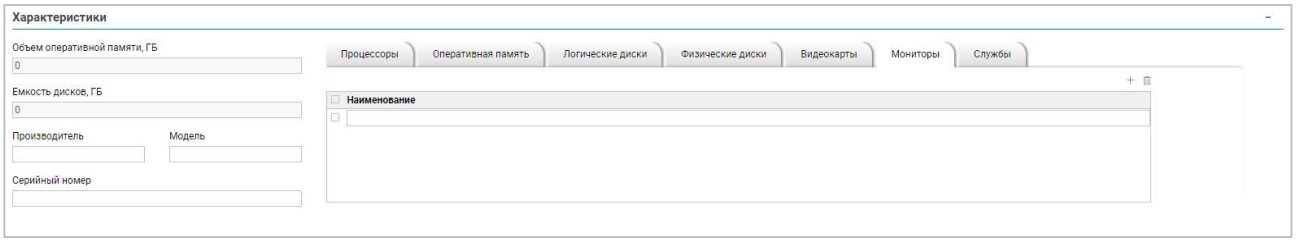

Рисунок 2.43 – Раздел «Характеристики» вкладка «Мониторы»

– во вкладке «Службы» (Рисунок 2.44) приводится информация о службах, запущенных на техническом средстве. Таблица данного раздела заполняется в соответствии с п. 2.6 настоящего документа.

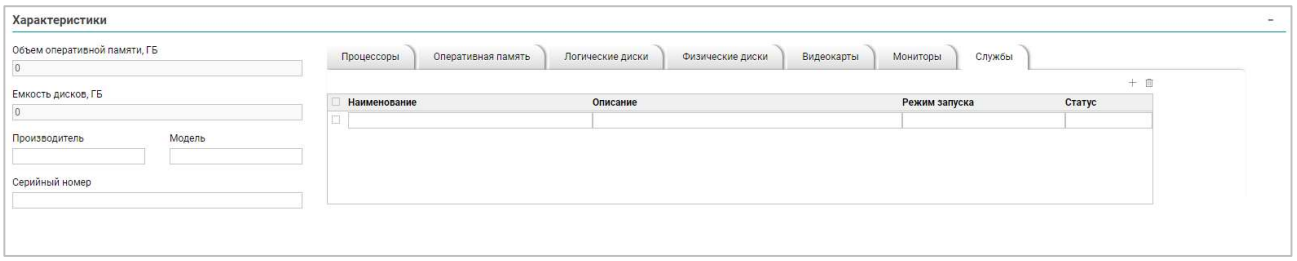

Рисунок 2.44 – Раздел «Характеристики» вкладка «Службы»

3) Раздел «**Сеть и Интернет**», в котором:

– во вкладке «Адреса, доступные из сети Интернет» в таблице указываются внешние адреса технического средства (Рисунок 2.45). Адреса, доступные из сети Интернет, можно добавлять в таблицу только после создания учетной карточки технического средства (после первого нажатия на кнопку «**Сохранить**»).

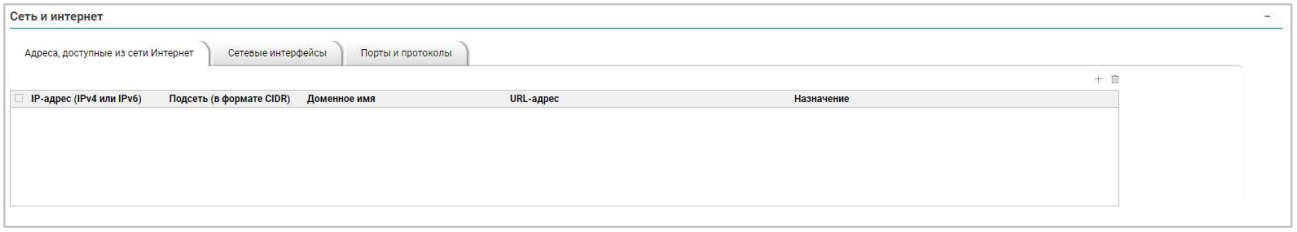

Рисунок 2.45 – Раздел «Сеть и Интернет» вкладка «Адреса, доступные из сети Интернет»

Для добавления в таблицу адресов, доступных из сети Интернет, необходимо нажать на кнопку «**Добавить**» (+). Откроется мастер добавления ресурсов (Рисунок 2.46).

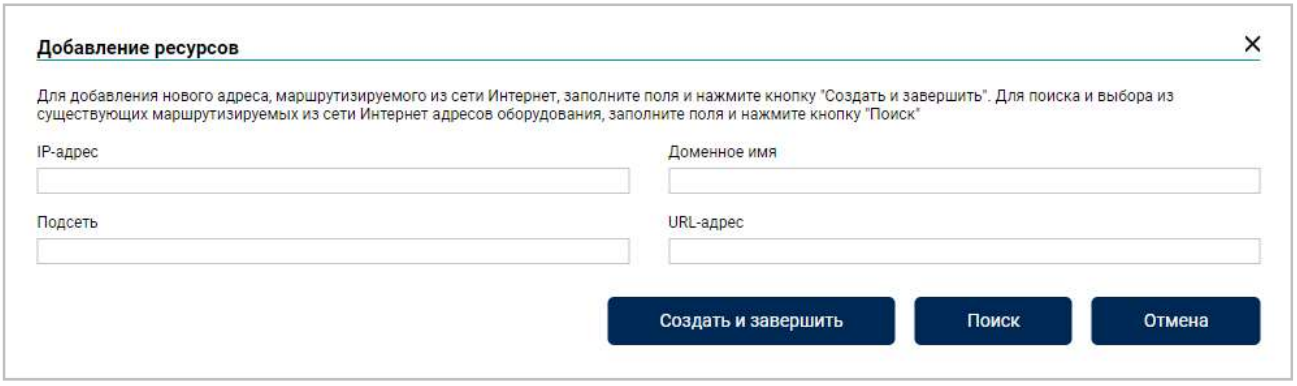

Рисунок 2.46 – Мастер добавления ресурсов

Для добавления адреса, доступного из сети Интернет, необходимо заполнить хотя бы одно поле и нажать на кнопку «**Создать**».

Для поиска и выбора из уже созданных в Системе адресов, необходимо заполнить известные поля и нажать на кнопку «**Поиск**». Откроется окно (Рисунок 2.47) со списком ресурсов, удовлетворяющих условиям поиска. Для добавления ресурсов необходимо выбрать их из перечня и нажать на кнопку «**Добавить**». Для изменения условий поиска необходимо нажать на кнопку «**Изменить фильтр**».

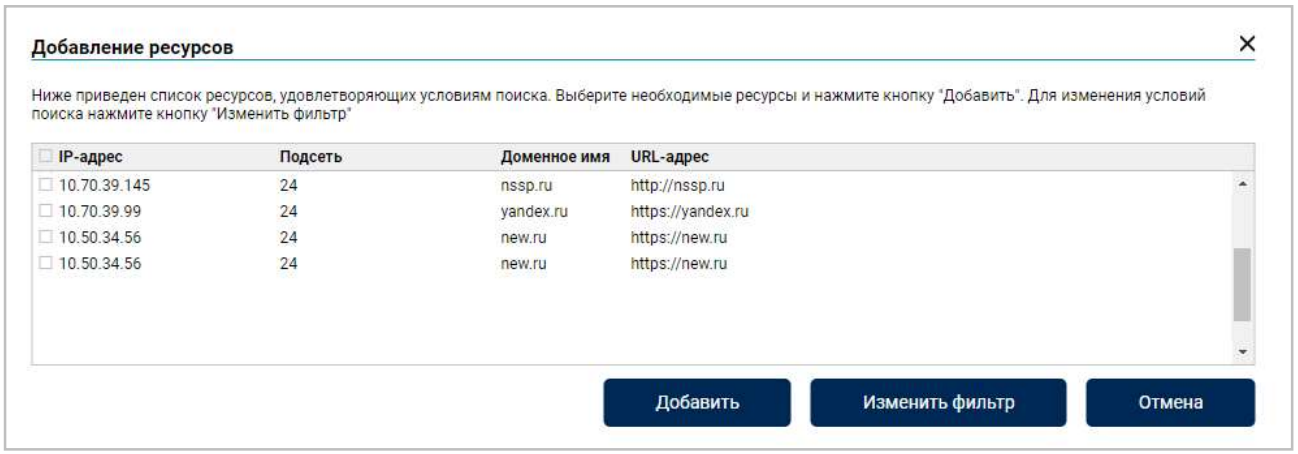

Рисунок 2.47 –Результаты поиска ресурсов

– во вкладке «Сетевые интерфейсы» (Рисунок 2.48) приводится информация о сетевых интерфейсах технического средства. Таблица данного раздела заполняется в соответствии с п. 2.6 настоящего документа.

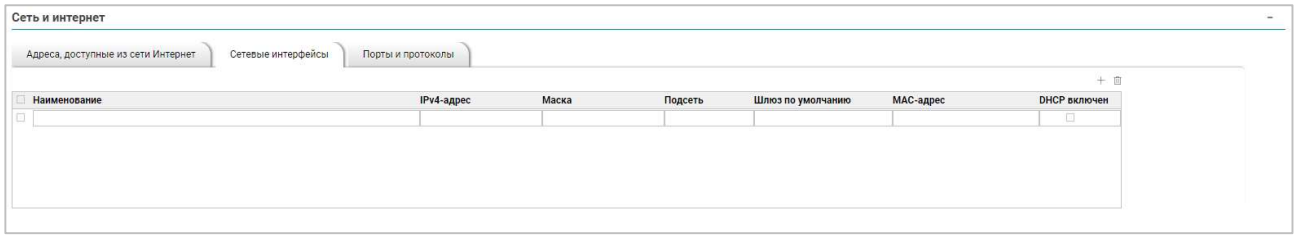

Рисунок 2.48 – Раздел «Сеть и Интернет» вкладка «Сетевые интерфейсы»

– во вкладке «Порты и протоколы» (Рисунок 2.49) приводится информация о сетевых портах и протоколах, статусах портов технического средства. Таблица данного раздела заполняется в соответствии с п. 2.6 настоящего документа.

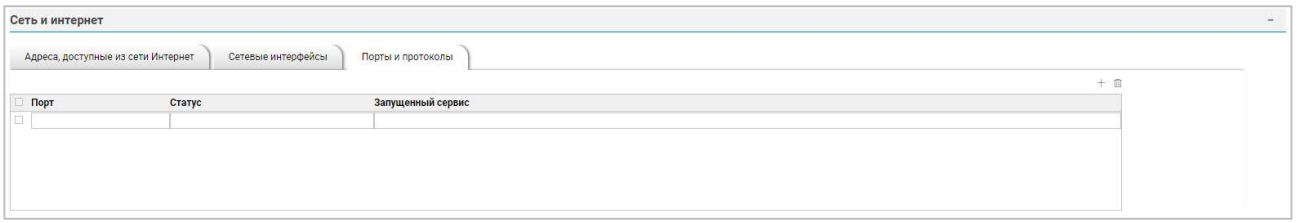

Рисунок 2.49 – Раздел «Сеть и Интернет» вкладка «Порты и протоколы»

4) Раздел «**Установленное программное обеспечение**» (Рисунок 2.50), в котором приводится информация об установленном на техническом средстве программном обеспечении. Таблица данного раздела заполняется в соответствии с п. 2.6 настоящего документа.

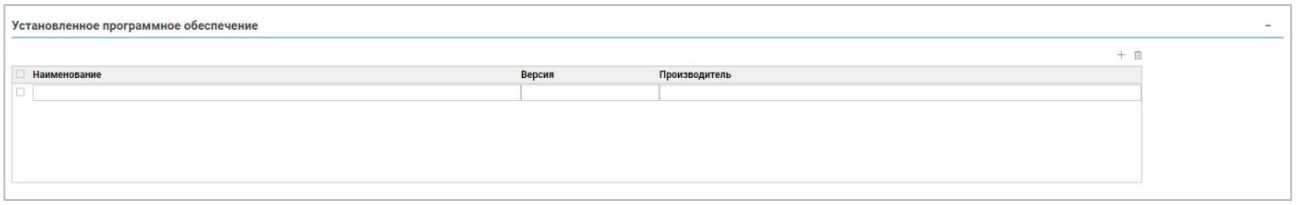

Рисунок 2.50 – Раздел «Установленное программное обеспечение»

– Раздел «**Системы, функционирование которых обеспечивает техническое средство**», в котором указываются системы, функционирование которых обеспечивает техническое средство (Рисунок 2.51). Системы можно добавлять в таблицу только после создания учетной карточки технического средства (после первого нажатия на кнопку «**Сохранить**»).

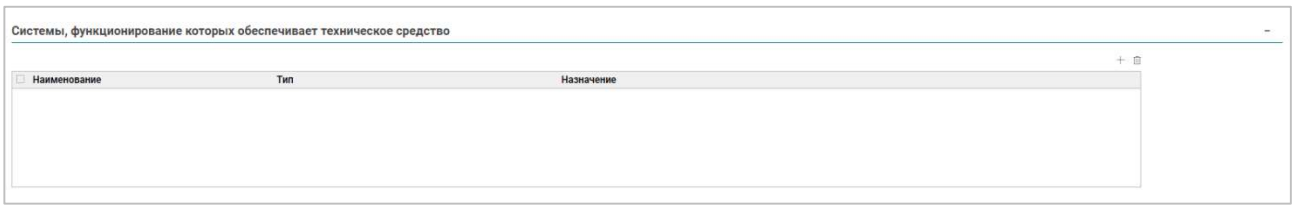

Рисунок 2.51 – Раздел «Системы, функционирование которых обеспечивает техническое средство»

Для добавления систем в таблицу необходимо нажать на кнопку «**Добавить**» (+). Откроется мастер добавления систем (Рисунок 2.52), в котором необходимо заполнить известные поля и нажать на кнопку «**Поиск**».

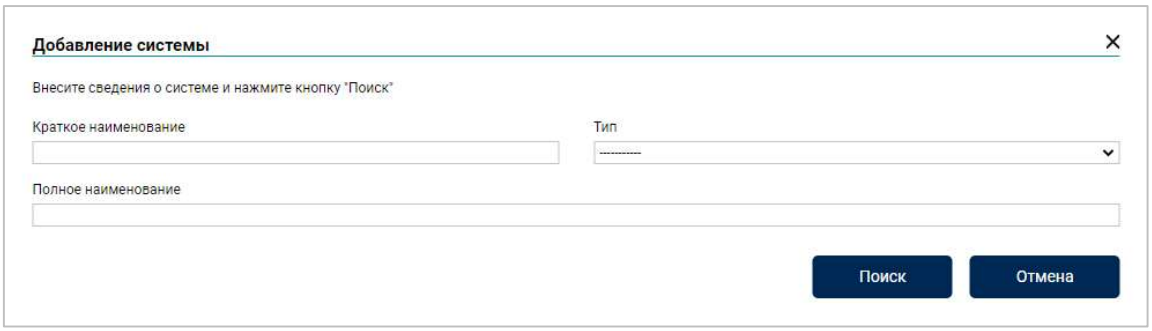

Рисунок 2.52 – Мастер добавления систем

Откроется окно (Рисунок 2.53) со списком систем, удовлетворяющих условиям поиска. Для добавления систем необходимо выбрать их из перечня и нажать на кнопку «**Добавить**». Для изменения условий поиска необходимо нажать на кнопку «**Изменить фильтр**».

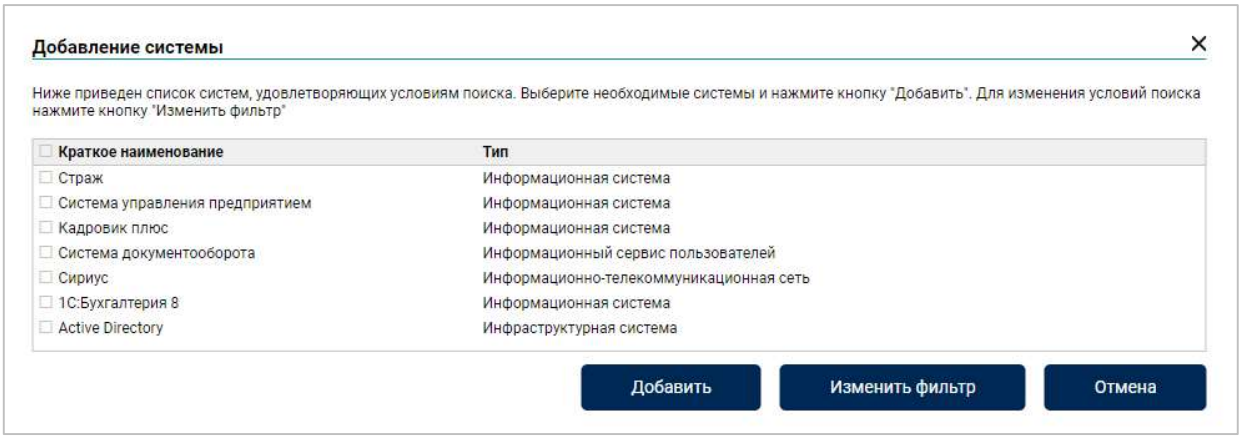

Рисунок 2.53 – Результаты поиска систем

2.7.5 Работа с инцидентами ИБ

2.7.5.1 Автоматическая регистрация инцидента ИБ

Описание настройки автоматической регистрации инцидентов ИБ из xml-файлов, выгружаемых из SIEM-систем, приведено в документе «Программный продукт Система

управления информационной безопасностью NextSTage Security Platform: NextStage IRP. Руководство администратора».

2.7.5.2 Просмотр перечня, создание и редактирование учетных карточек инцидентов ИБ

Для просмотра перечня учетных карточек инцидентов ИБ необходимо в главном меню выбрать раздел «Инциденты ИБ». Откроется перечень учетных карточек инцидентов ИБ (Рисунок 2.54).

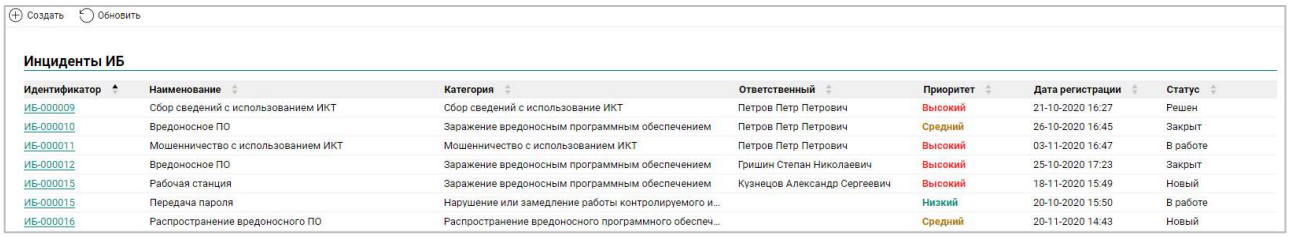

Рисунок 2.54 – Перечень инцидентов ИБ

Для перехода к учетной карточке инцидента ИБ необходимо выбрать (щелкнув левой кнопкой мыши) соответствующую строку перечня. Откроется учетная карточка инцидента ИБ (Рисунок 2.55).

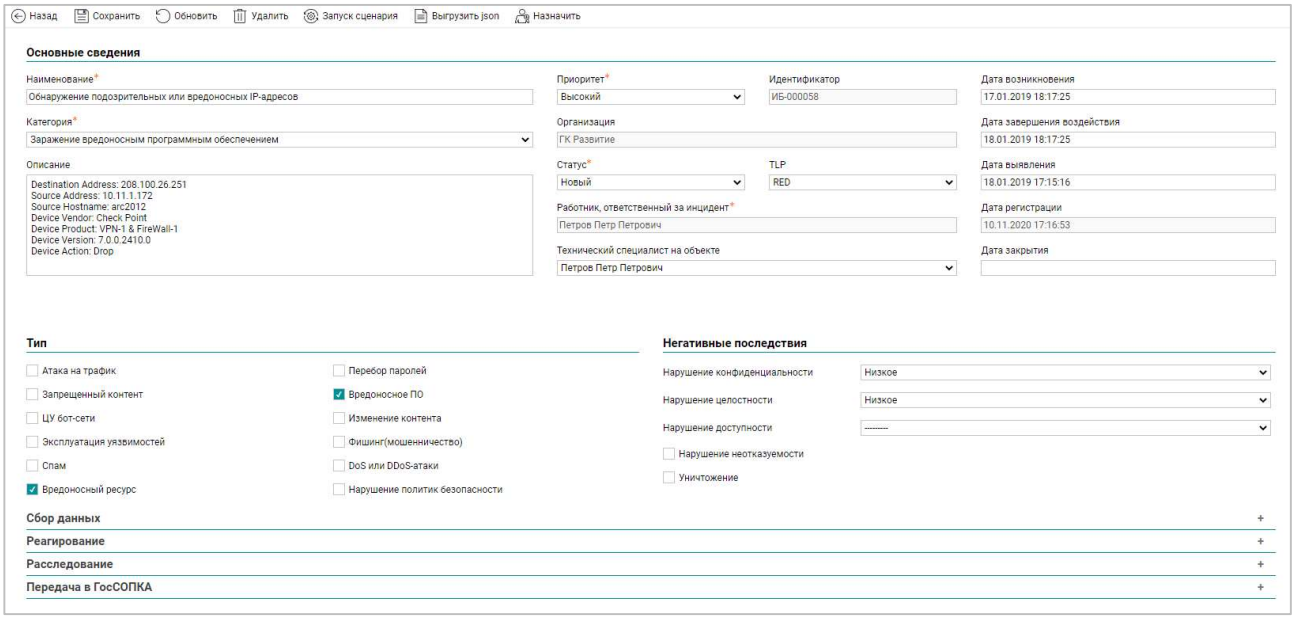

Рисунок 2.55 – Учетная карточка инцидента ИБ

Для обновления элементов перечня необходимо нажать на кнопку «**Обновить**».

Для создания учетной карточки инцидента ИБ необходимо нажать на кнопку «**Создать**». Откроется новая учетная карточка инцидента ИБ (Рисунок 2.56).

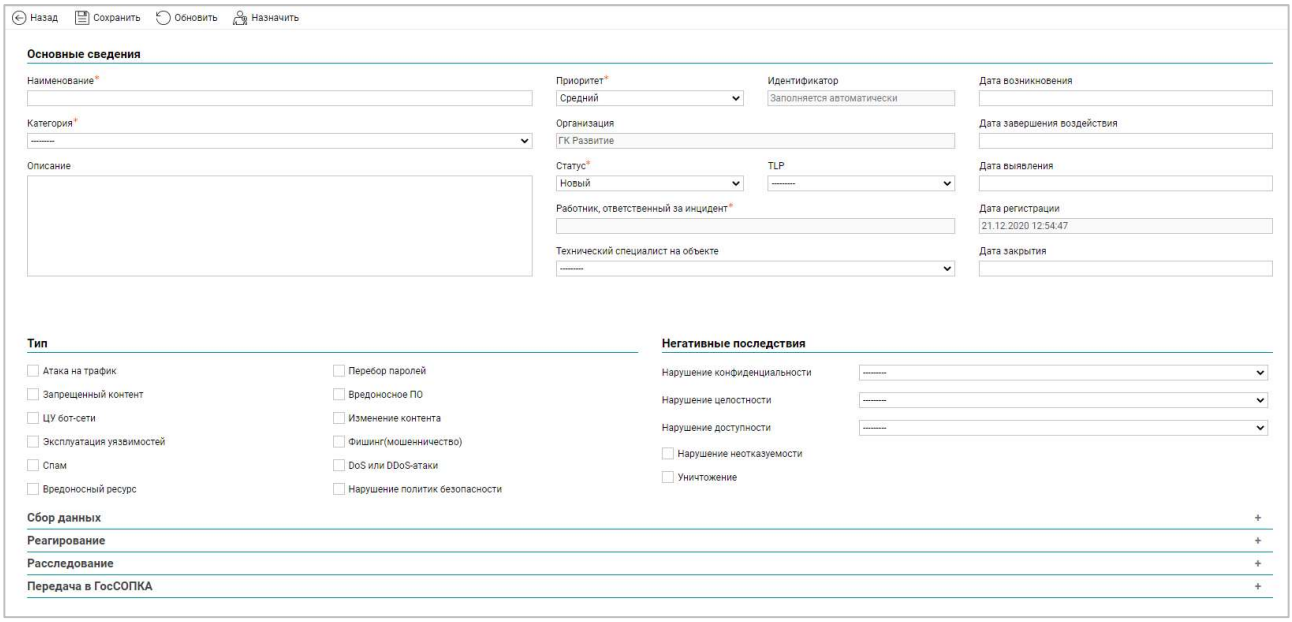

Рисунок 2.56 – Новая учетная карточка инцидента ИБ

Поля учетной карточки инцидента ИБ заполняются в соответствии с пунктом 2.5 настоящего документа.

Обязательные поля учетной карточки инцидента ИБ отмечены знаком «*».

Для создания учетной карточки инцидента ИБ и (или) сохранения внесенных в учетную карточку изменений необходимо нажать на кнопку «**Сохранить**» в строке меню.

Для возврата к перечню инцидентов ИБ необходимо нажать на кнопку «**Назад**».

Для обновления учетной карточки инцидента ИБ необходимо нажать на кнопку «**Обновить**».

Для удаления учетной карточки инцидента ИБ необходимо нажать на кнопку «**Удалить**». Для восстановления ошибочно удаленной карточки инцидента ИБ необходимо обратиться к администратору.

В учетной карточке инцидента ИБ доступны для заполнения следующие разделы:

1) Раздел «**Основные сведения**» (Рисунок 2.57). В данном разделе приводится общая информация об инциденте ИБ. Поля «Идентификатор», «Дата регистрации»

заполняются автоматически, остальные поля данного раздела заполняются в соответствии с пунктом 2.5 настоящего документа.

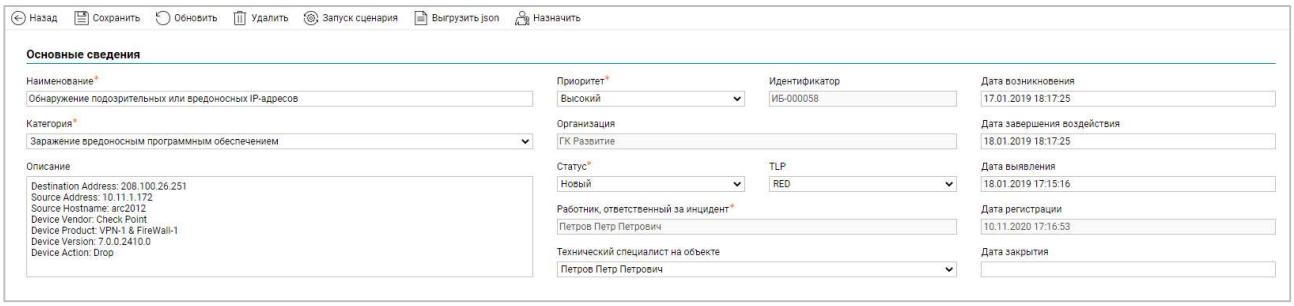

Рисунок 2.57 – Раздел «Основные сведения»

2) Раздел «**Тип**» (Рисунок 2.58), в котором указываются типы, к которым относится инцидент ИБ. Поля данного раздела заполняются в соответствии с пунктом 2.5 настоящего документа.

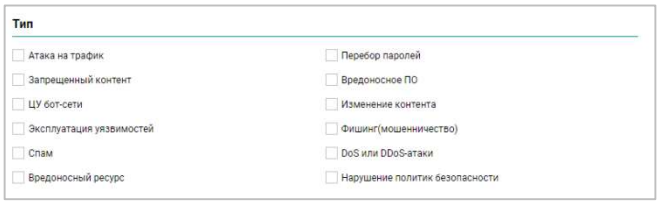

Рисунок 2.58 – Раздел «Тип»

3) Раздел «**Негативные последствия**» (Рисунок 2.59), в котором указывается, к каким негативным последствиям привел инцидент ИБ.

Рисунок 2.59 – Раздел «Негативные последствия»

4) Раздел «**Сбор данных**», в котором:

– во вкладке «Источник выявления» указываются сведения об источнике выявления инцидента ИБ (Рисунок 2.60). Поля данного раздела заполняются в соответствии с пунктом 2.5 настоящего документа.

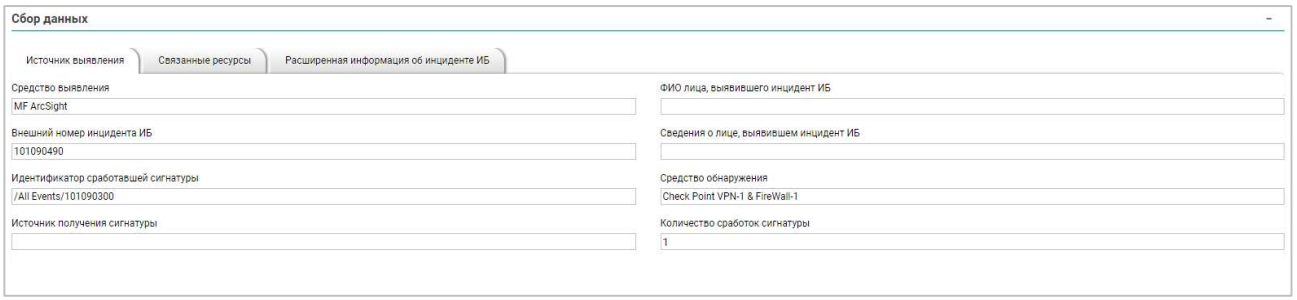

Рисунок 2.60 – Раздел «Сбор данных» вкладка «Источник выявления»

– во вкладке «Связанные ресурсы» (Рисунок 2.61) приводятся сведения о пострадавшей системе, пострадавших ресурсах и источниках инцидента ИБ.

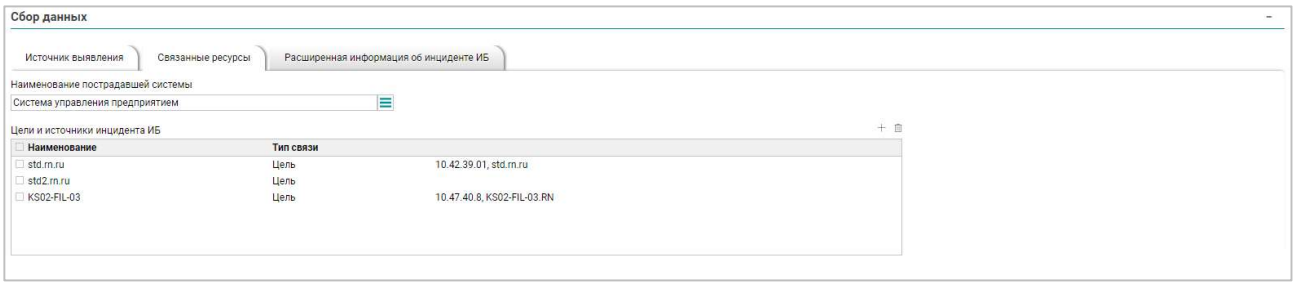

Рисунок 2.61 – Раздел «Сбор данных» вкладка «Связанные ресурсы»

В таблице «Список ресурсов, связанных с инцидентом ИБ» указываются пострадавшие ресурсы и источники инцидента ИБ. Пострадавшие ресурсы и источники инцидента ИБ можно добавлять в таблицу только после создания учетной карточки инцидента ИБ (после первого нажатия на кнопку «**Сохранить**»).

Для добавления пострадавших ресурсов в таблицу необходимо нажать на кнопку «**Добавить**» (+). Откроется мастер добавления ресурсов (Рисунок 2.62), в котором необходимо выбрать в поле «Тип связи» значение «Цель», заполнить известные поля и нажать на кнопку «**Поиск**». Откроется окно со списком ресурсов, удовлетворяющих условиям поиска. Для добавления ресурсов необходимо выбрать их из перечня и нажать на кнопку «**Добавить**». Для изменения условий поиска необходимо нажать на кнопку «**Изменить фильтр**».

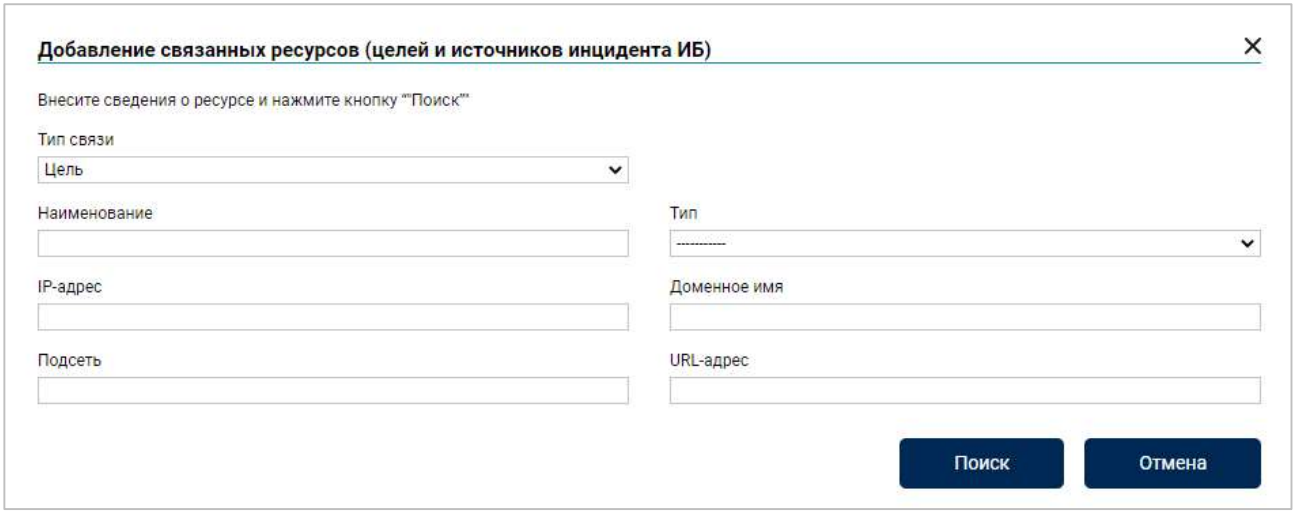

Рисунок 2.62 – Мастер добавления ресурсов

Для добавления источника инцидента ИБ в таблицу необходимо нажать на кнопку «**Добавить**» (+). Откроется мастер добавления источников (Рисунок 2.63), в котором необходимо выбрать в поле «Тип связи» значение «Источник», заполнить известные поля и нажать на кнопку «**Создать и Завершить**». Для перехода к созданию следующего источника инцидента ИБ нажать на кнопку «**Создать**».

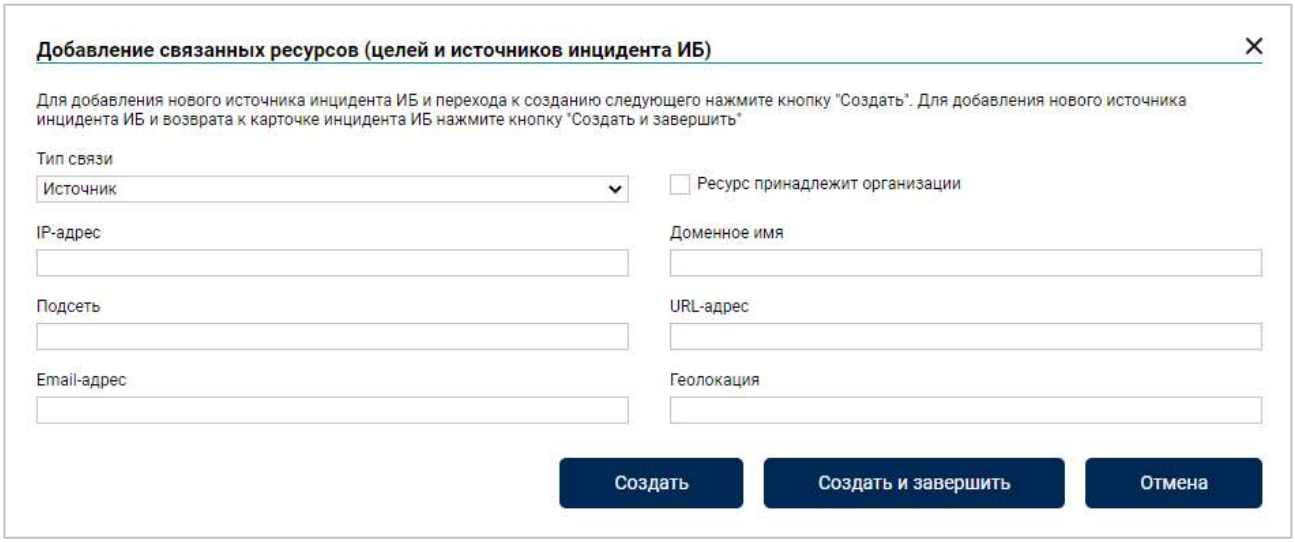

Рисунок 2.63 – Мастер добавления источников

Для добавления пострадавшей системы необходимо нажать на кнопку Заполнить( ) рядом с полем «Наименование системы». Откроется мастер добавления системы (Рисунок 2.64), в котором необходимо заполнить известные поля и нажать на кнопку «**Поиск**».

Откроется окно со списком систем, удовлетворяющих условиям поиска. Для добавления системы необходимо выбрать ее из перечня. Для изменения условий поиска необходимо нажать на кнопку «**Изменить фильтр**».

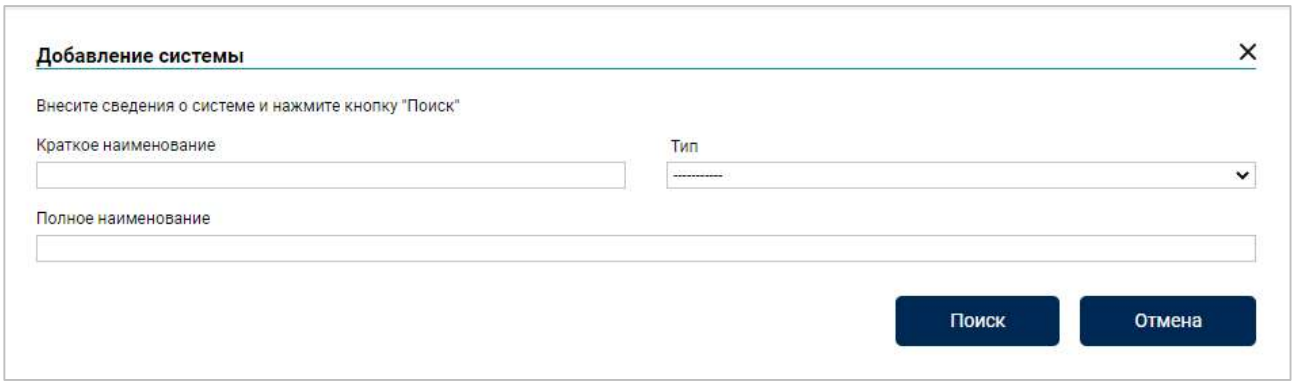

Рисунок 2.64 – Мастер добавления системы

– во вкладке «Расширенная информация об инциденте ИБ» (Рисунок 2.65) приводятся дополнительные поля, характеризующие инцидент ИБ в зависимости от его типа. Данная вкладка доступна, если в разделе «Тип» выбран хотя бы один тип инцидента ИБ. Поля и таблицы данного раздела заполняются в соответствии с пунктом 2.5 настоящего документа.

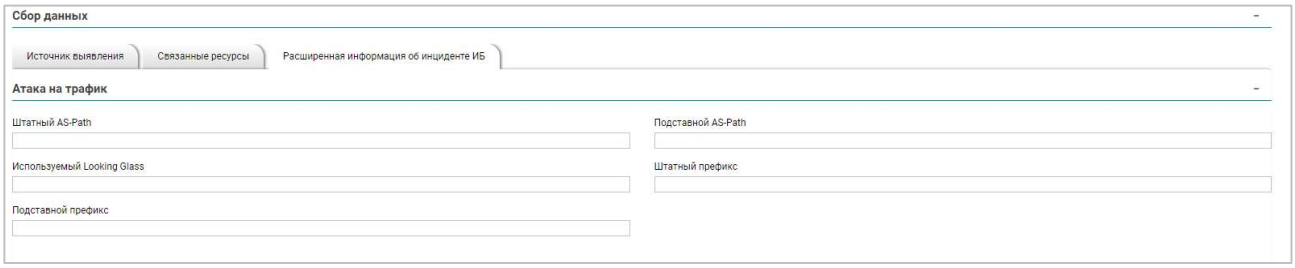

Рисунок 2.65 – Раздел «Сбор данных» вкладка «Расширенная информация об инциденте ИБ»

5) Раздел «**Реагирование**» (Рисунок 2.66), в котором указываются результаты выполнения работ по реагированию на инцидент ИБ. Перечень запущенных в рамках решения инцидента ИБ сценариев недоступен для редактирования, остальные поля данного раздела заполняются в соответствии с пунктом 2.5 настоящего документа.

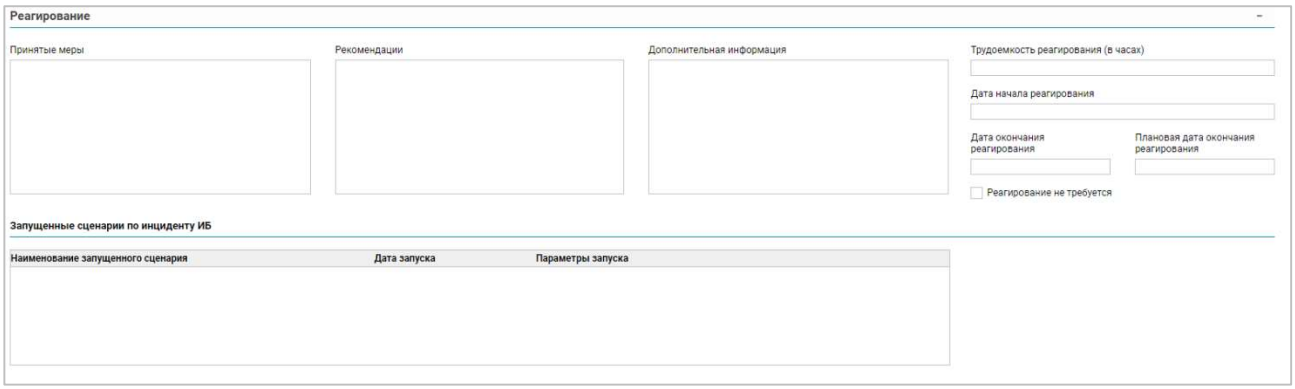

Рисунок 2.66 – Раздел «Реагирование»

6) Раздел «**Расследование**» (Рисунок 2.67), в котором приводятся результаты выполнения работ по расследованию инцидента ИБ. Поля данного раздела заполняются в соответствии с пунктом 2.5 настоящего документа.

Рисунок 2.67 – Раздел «Расследование»

7) Раздел «**Передача в ГосСОПКА**» (Рисунок 2.68), в котором указывается дополнительная информация об инциденте ИБ для передачи в НКЦКИ. Поля данного раздела заполняются в соответствии с пунктом 2.5 настоящего документа.

Рисунок 2.68 – Раздел «Передача в ГосСОПКА»

2.7.5.3 Переназначение инцидента ИБ

Для переназначения инцидента ИБ необходимо нажать на кнопку «**Назначить**» в строке меню учетной карточки инцидента ИБ. Откроется мастер переназначения инцидента ИБ (Рисунок 2.69), в котором необходимо выбрать из перечня ответственного и нажать на кнопку «**Завершить**».

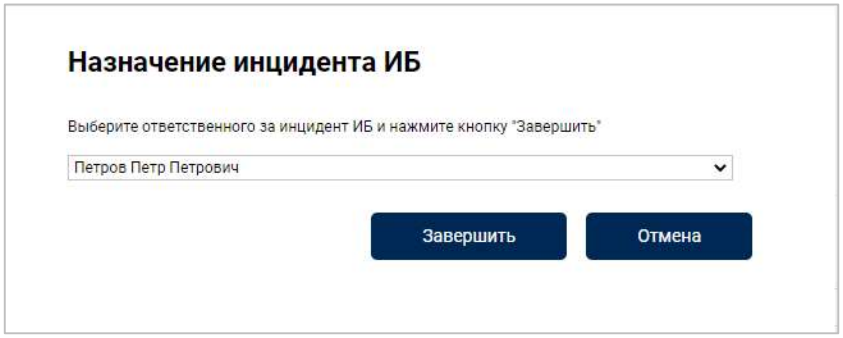

Рисунок 2.69 – Мастер переназначения инцидента ИБ

2.7.5.4 Запуск сценария

Для запуска сценария реагирования на инцидент ИБ необходимо нажать на кнопку «**Запустить сценарий**» в строке меню учетной карточки инцидента ИБ. Откроется мастер (Рисунок 2.70), в котором необходимо выбрать из перечня сценарий, проверить параметры запуска и нажать на кнопку «**Запустить**».

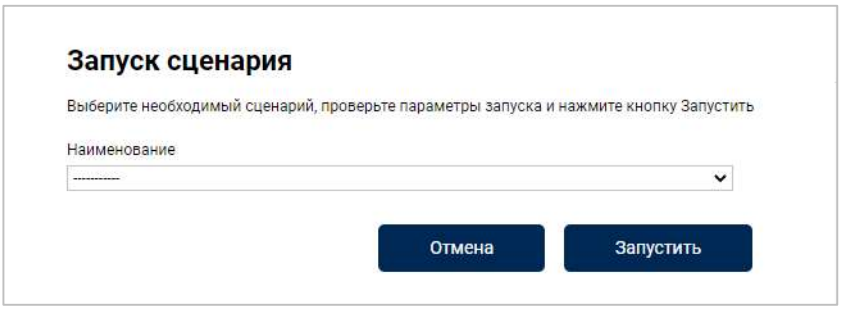

Рисунок 2.70 – Мастер запуска сценария

Параметры запуска подгружаются из карточки инцидента ИБ:

1) Для сценариев «Блокировка учетной записи в AD», «Разблокировка учетной записи в AD», «Сброс пароля пользователя в AD» в качестве параметра запуска используется значение поля «Учетная запись» в блоке «Нарушение политик безопасности» вкладки

«Расширенная информация об инциденте ИБ» раздела «Сбор данных» (данный блок доступен для редактирования при выборе типа инцидента ИБ «Нарушение политик безопасности»).

2) Для сценария «Запуск сканирования KSC» в качестве параметра запуска используется доменное имя технического средства, указанного в таблице «Цели и источники инцидента ИБ» вкладки «Связанные ресурсы» раздела «Сбор данных».

3) Для сценария «Блокировка hash (md5, sha256) в KSC» в качестве параметра запуска используется hash-сумма вредоносного файла, указанная в таблице «Образцы вредоносного ПО» блока «Вредоносное ПО» вкладки «Расширенная информация об инциденте ИБ» раздела «Сбор данных» (данный блок доступен для редактирования при выборе типа инцидента ИБ «Вредоносное ПО»).

Для редактирования параметров запуска необходимо нажать на кнопку «**Отмена**», изменить параметры в карточке инцидента ИБ и нажать на кнопку «**Запустить сценарий**» повторно.

2.7.5.5 Выгрузка JSON-файла

Для выгрузки JSON-файла необходимо нажать на кнопку «**Выгрузить json**» в строке меню учетной карточки инцидента ИБ.

Перед открытием файла учетная карточка инцидента ИБ будет сохранена в базе данных.

В случае, если в учетной карточке не заполнена информация, обязательная для отправки файла в НКЦКИ, откроется всплывающее окно с уведомлением об ошибке. Для выгрузки json-файла с незаполненной обязательной информацией необходимо нажать на кнопку «**Завершить**». Для возврата к карточке инцидента ИБ и просмотра перечня незаполненных обязательных полей необходимо нажать на кнопку «**Отмена**». Перечень незаполненных полей будет отражен в окне «требуется заполнить поля» в левой части рабочей области (под главным меню).

3 ОБЩИЕ ИНСТРУКЦИИ ПО ИСПОЛЬЗОВАНИЮ ГРАФИЧЕСКОГО ИНТЕРФЕЙСА МОДУЛЯ ВИЗУАЛИЗАЦИИ

Для перехода к просмотру информационной панели в модуле визуализации необходимо в главном меню личного кабинета пользователя выбрать раздел «Дашборды». Откроется графический интерфейс модуля визуализации с информационной панелью по инцидентам ИБ и активам.

На информационной панели по инцидентам ИБ и активам доступны следующие разделы:

1) Раздел «Инциденты ИБ» (Рисунок 3.1), в котором представлена статистика по инцидентам ИБ в виде графиков и перечней:

- Общее количество зарегистрированных инцидентов ИБ;
- Количество просроченных инцидентов ИБ;
- Количество инцидентов ИБ, которые привели к негативным последствиям;
- Распределение инцидентов ИБ по статусам;
- Негативные последствия;
- Распределение инцидентов ИБ по приоритетам;
- Процент соблюдения сроков реагирования на инциденты ИБ;
- Среднее время реагирования на инциденты ИБ по приоритетам (в часах);
- Категории инцидентов ИБ;
- Динамика регистрации инцидентов ИБ;
- Источники инцидентов ИБ (по учетным записям);
- Источники инцидентов ИБ (по email);
- Системы, затронутые инцидентами ИБ;
- Технические средства, затронутые инцидентами ИБ;
- Распределение инцидентов ИБ по ответственным.

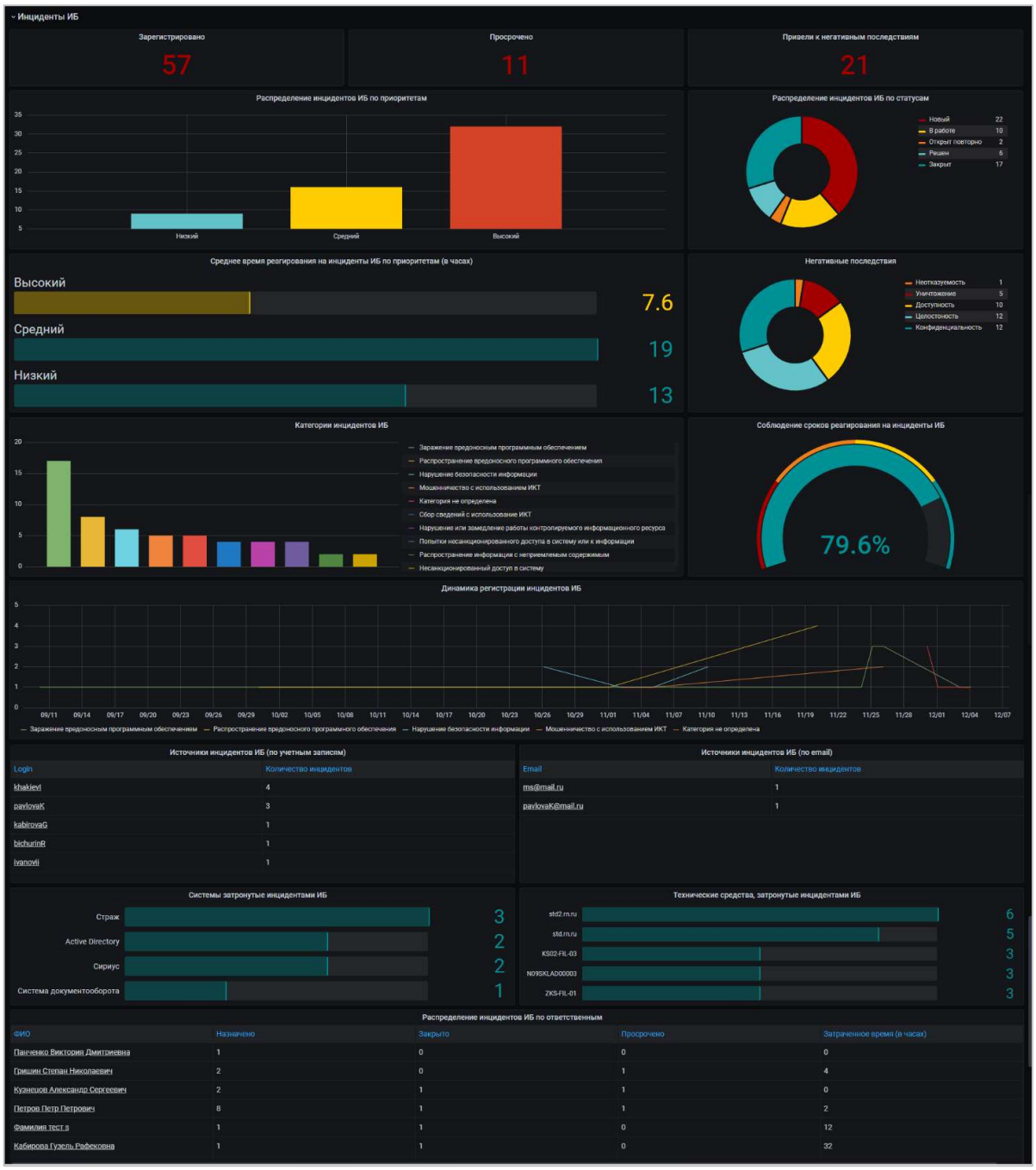

Рисунок 3.1 – Раздел «Инциденты ИБ»

Для метрик «Общее количество зарегистрированных инцидентов ИБ», «Количество просроченных инцидентов ИБ», «Количество инцидентов ИБ, которые привели к негативным последствиям» доступна функция по переходу к окну с перечнем соответствующих инцидентов ИБ. Для перехода к перечню инцидентов ИБ необходимо нажать на числовой показатель и щелкнуть по появившейся ссылке.

Для таблиц «Источники инцидентов ИБ (по учетным записям)», «Источники инцидентов ИБ (по email)» доступна функция по переходу к окну с перечнем соответствующих инцидентов ИБ. Для перехода к перечню инцидентов ИБ необходимо щелкнуть левой кнопкой мыши по ссылке в первом столбце таблицы.

2) Раздел «Активы» (Рисунок 3.2), в котором представлена статистка по ИТ-активам в виде следующих графиков:

– Общее количество информационных систем
– Общее количество технических средств
– Процент технических средств, обновленных автоматически
– Распределение технические средств по категориям
– Распределение информационных систем по типам
– Используемые операционные системы

Для показателей «Общее количество информационных систем», «Общее количество технических средств» доступна функция по переходу к окну с перечнем информационных систем и к окну технических средств соответственно. Для перехода к окну с перечнем активов необходимо нажать на числовой показатель и щелкнуть по появившейся ссылке.

Рисунок 3.2 – Раздел «Активы»

4 ОБЩИЕ ИНСТРУКЦИИ ПО ИСПОЛЬЗОВАНИЮ МОДУЛЯ СКАНИРОВАНИЯ СЕТИ

4.1 Настройка модуля сканирования сети

Описание настроек модуля сканирования сети приведено в документе «Программный продукт Система управления информационной безопасностью NextSTage Security Platform: NextStage IRP. Руководство администратора».

4.2 Запуск сканирования сети

Для перехода к запуску сканирования сети организации необходимо в главном меню личного кабинета пользователя выбрать раздел «Сканирование сети». Откроется форма запуска сканирования (Рисунок 4.1).

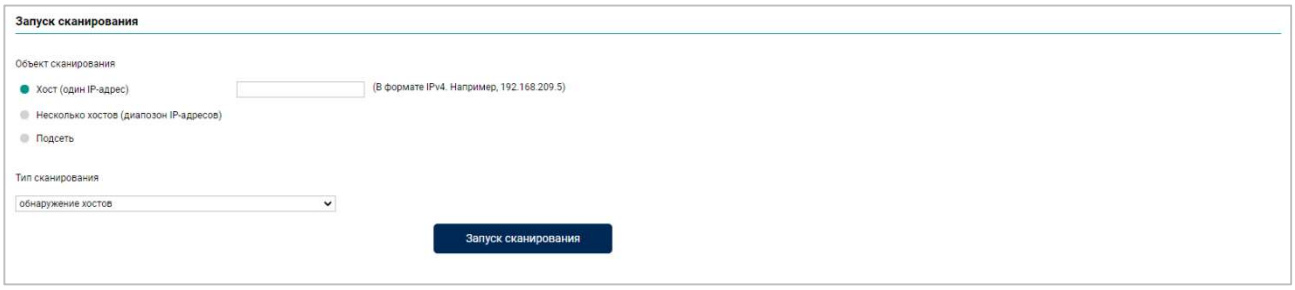

Рисунок 4.1 – Форма запуска сканирования сети

Поля формы запуска сканирования сети заполняются в соответствии с пунктом 2.5 настоящего документа.

Для запуска сканирования необходимо указать объект, тип сканирования и нажать на кнопку «**Запустить сканирование**».

Важно! *Для обеспечения возможности добавления сведений по портам в учетную карточку технического средства Личного кабинета пользователя необходимо, чтобы по данному техническому средству хотя бы единожды запускался тип сканирования «Сбор информации по хостам».*

Результаты сканирования сохраняются в Личном кабинете пользователя в виде учетных карточек технических средств (Рисунок 4.2) с указанием даты и средства инвентаризации.

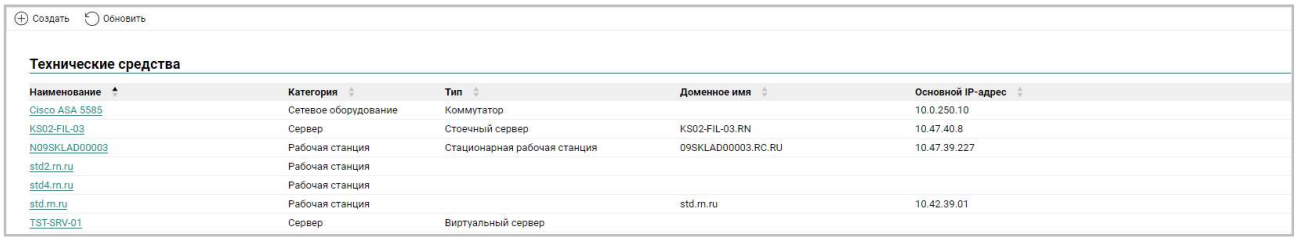

Рисунок 4.2 – Результаты сканирования

5 ДЕЙСТВИЯ ПРИ ВОЗНИКНОВЕНИИ ОШИБОК И НЕИСПРАВНОСТЕЙ

При возникновении ошибок и неисправностей в работе программного продукта необходимо обновить страницу с помощью комбинации клавиш Ctrl+Shift+R и повторно проделать ранее выполненные действия. При повторном появлении ошибки необходимо обратиться к администратору программного продукта, описать ему действия, при которых были выявлены проблемы и ошибки, а также вводимые данные, и предоставить скриншоты появляющихся ошибок.

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

Сокращение	Полное наименование
JSON	JavaScript Object Notation
MS	Microsoft
SIEM	Security information and event management
XML	Extensible Markup Language
АС	Автоматизированная система
АСУ ТП	Автоматизированная система управления технологическим процессом
ГИС	Государственная информационная система
ИБ	Информационная безопасность
ИТ	Информационные технологии
ИС	Информационная система
ИСПДн	Информационная система персональных данных
КИИ	Критическая информационная инфраструктура
НКЦКИ	Национальный координационный центр по компьютерным инцидентам

ПЕРЕЧЕНЬ ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

Термин	Определение
JSON	Текстовый формат представления данных, предназначенный для обмена данными
Автоматизированное рабочее место	Программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида
Информационная панель	Визуальное представление данных, сгруппированных по одному или нескольким направлениям деятельности на одном экране
Объект базы данных	Совокупность атрибутов, информация о которых хранится в базе данных Системы
Учетная карточка	Документ, содержащий формальное определение параметров функционирования и состава объектов базы данных