Программный комплекс «Модель прогноза состояния информационной безопасности» (далее ПК «МПСИБ»)

Руководство пользователя

Оглавление

1. Общие сведения

Программный комплекс «Модель прогноза состояния информационной безопасности» (далее ПК «МПСИБ» или ПК) предназначен для прогнозирования тенденций атак и инцидентов, отражения развития состояния ИБ на период 3 года, ведения реестра информационных активов, идентификации и приоритизации угроз и рисков ИБ, фиксации мероприятий по минимизации рисков ИБ.

2. Ролевая модель

Действия пользователей ПК «МПСИБ» определяются ролевой моделью, согласно установленных прав пользователей для выполнения конкретных действий и их ограничений.

В рамках ролевой модели существуют следующие типы ролей:

1) Владелец процесса:

- имеет доступ на просмотр данных разделов «Стартовая страница», «Аналитика», «Справочники», «Сводный отчет», «Статистика прошлых лет», «Реестр ИА», «Реестр рисков», «Матрица» и их подразделов;
- согласовывает реестр рисков в разделе «Реестр рисков».

Пользователь не имеет возможности ввода данных.

2) Специалист службы ИТ и ИБ:

- имеет доступ на просмотр данных разделов «Стартовая страница», «Аналитика», «Справочники», «Сводный отчет», «Статистика прошлых лет», «Реестр ИА», «Реестр рисков», «Матрица» и их подразделов;
- - загружает аналитические данные в раздел «Аналитика», актуализирует и загружает справочники в разделе «Справочники»;
- - формирует перечень угроз ИБ;
- - формирует реестр рисков;
- - осуществляет ручной ввод в карточке риска в подразделе «Риски» («Реестр ИА», карточка ИА).

Пользователь не имеет доступа к согласованию реестра рисков в разделе «Реестр рисков».

3) Аналитик / Риск-менеджер:

- имеет доступ на просмотр данных разделов «Стартовая страница», «Аналитика», «Справочники», «Сводный отчет», «Статистика прошлых лет», «Реестр ИА», «Реестр рисков», «Матрица» и их подразделов;

Пользователь не имеет возможности ввода данных и согласования реестра рисков ИБ.

4) Администратор:

- имеет доступ к разделу «Администрирование»;
- заводит отчетный период (год);
- открывает версию ОЛ для возможности внесения корректировок перечня угроз и оценки рисков ИБ для специалиста ИБ/ИТ и ИБ.

На основании определённой пользовательской роли и соответствующих ей прав, создается учётная запись пользователя.

3. Работа с данными

Программный комплекс работает с данными в виде файлов формата XLSX и CSV. Особенности загрузки данных в программный комплекс и выгрузки данных из него описаны далее.

3.1. Справочники ФСТЭК

Для выполнения корректного анализа и прогнозирования угроз и рисков ИБ в ПК должна учитываться актуальная информация об угрозах и уязвимостях, предоставляемая в свободном доступе на портале ФСТЭК.
Данные, содержащие сведения об угрозах безопасности информации, размещены на странице https://bdu.fstec.ru/threat
Данные, содержащие сведения об уязвимостях, размещены на странице https://bdu.fstec.ru/vul
Процесс получения и применения этих данных описан в разделе настоящего документа **7. Справочники**.

3.2. Аналитические отчеты

Данные «Аналитика_ИА» и «Аналитика_Инциденты» — это отчеты, наполняемые специфическими данными в сторонней системе «Цифровой помощник» или вручную, являются основой для анализа и прогнозирования, загружаемые в ПК в формате XLSX.

3.2.1. Версии аналитических отчетов

Версия отчетов, или версия данных, может иметь статус «Закрыта» и «Открыта».
Версии со статусом «Закрыта» — это данные отчетов, которые прошли обработку в карточках ИА раздела **Реестр ИА** и были согласованы в разделе **Реестр рисков**. Количество «закрытых» версий соответствует числу согласованных реестров рисков.
Версия со статусом «Открытая» — это текущая загруженная версия, по которой не пройдены или не завершены этапы анализа данных и не пройдена стадия согласования в Реестре рисков.
При загрузке аналитических отчетов «Аналитика_ИА», «Аналитика_Инциденты» в разделе **Аналитика** отражается запись с её названием в формате «дд.мм.гггг чч.мм» и статусом «Открыта».
Пока версия открыта, каждая последующая загрузка аналитических отчетов будет подгружаться в данную версию, т.е. будут изменяться данные по ИА, атакам и инцидентам согласно данным последних загруженных файлом отчетов.

ВАЖНО: Обязательным условием для загрузки аналитических отчетов «Аналитика_ИА», «Аналитика_Инциденты» за текущий отчетный период является открытие соответствующего периода Администратором ПК МПСИБ.

3.2.2. Требования к заполнению версий аналитических отчетов данными

«Аналитика_ИА» содержат данные об информационных системах (ИС), распределённых по видам. Особенности внесения данных изложены далее.

ИСПДн

Данными заполняются следующие столбцы:

- Регион присутствия компании;
- Отрасль;
- Локальное расположение ИА;
- Уникальный номер ИА обследования/оценки ИТ-инфраструктуры;
- Наименование ИСПДн/ГИС/МИС/Другой ИС/АСУ/ЦОД/Серверная/ИТС/ОКИИ;
- Отнесение информационного объекта к ОКИИ;
- Тип ИА;
- Вид ИА;
- Идентификатор ценности ИА;
- Сертификация / аттестация ФСТЭК;
- Название ПО;
- Разработчик / Вендор;
- Назначение;
- Наименование ОС (может быть не заполнено в соответствии со справочником ФСТЭК);
- Прикладное ПО (может быть не заполнено в соответствии со справочником ФСТЭК);
- Вендор ПО (может быть не заполнено в соответствии со справочником ФСТЭК);
- Версия ПО;
- Состав ПДн;
- Объем ПДн;
- Субъекты ПДн;
- Тип актуальных угроз;
- Определение уровня защищенности ПДн;
- Категория значимости ОКИИ;
- Ввод в промышленную эксплуатацию;
- Планируемый вывод из эксплуатации;
- Наличие ТП;
- Тип ТП;

- SLA: время реагирования, в т.ч для аутсорсинга.

Данными не заполняются следующие столбцы:

- Класс ГИС;
- Масштаб ГИС;
- Уровень значимости ИС;
- Группа защищенности (АСУ);
- Тип информации (АСУ);
- Класс (АСУ);
- Уровень конфиденциальности (АСУ);
- Инструмент мониторинга / надежности функционирования.

ГИС/МИС

Данными заполняются следующие столбцы:

- Регион присутствия компании;
- Отрасль;
- Локальное расположение ИА;
- Уникальный номер ИА обследования/оценки ИТ-инфраструктуры;
- Наименование ИСПДн/ГИС/МИС/Другой ИС/АСУ/ЦОД/Серверная/ИТС/ОКИИ;
- Отнесение информационного объекта к ОКИИ;
- Тип ИА;
- Вид ИА;
- Идентификатор ценности ИА;
- Сертификация / аттестация ФСТЭК;
- Название ПО;
- Разработчик / Вендор;
- Назначение;
- Наименование ОС (может быть не заполнено в соответствии со справочником ФСТЭК);
- Прикладное ПО (может быть не заполнено в соответствии со справочником ФСТЭК);
- Вендор ПО (может быть не заполнено в соответствии со справочником ФСТЭК);
- Версия ПО;
- Класс ГИС;
- Масштаб ГИС;
- Уровень значимости ИС;
- Категория значимости ОКИИ;
- Ввод в промышленную эксплуатацию;
- Планируемый вывод из эксплуатации;
- Ввод в эксплуатацию, месяц/год;

- Вывод из эксплуатации, месяц/год;
- Наличие ТП;
- Тип ТП;
- SLA: время реагирования, в т.ч для аутсорсинга.

Данными не заполняются следующие столбцы:

- Состав ПДн;
- Объем ПДн;
- Субъекты ПДн;
- Тип актуальных угроз;
- Определение уровня защищенности ПДн;
- Группа защищенности (АСУ);
- Тип информации (АСУ);
- Класс (АСУ);
- Уровень конфиденциальности (АСУ);
- Инструмент мониторинга / надежности функционирования.

Другие ИС

Данными заполняются следующие столбцы:

- Регион присутствия компании;
- Отрасль;
- Локальное расположение ИА;
- Уникальный номер ИА обследования/оценки ИТ-инфраструктуры;
- Наименование ИСПДн/ГИС/МИС/Другой ИС/АСУ/ЦОД/Серверная/ ИТС/ОКИИ;
- Отнесение информационного объекта к ОКИИ;
- Тип ИА;
- Вид ИА;
- Идентификатор ценности ИА;
- Сертификация / аттестация ФСТЭК;
- Название ПО;
- Разработчик / Вендор;
- Назначение;
- Наименование ОС (может быть не заполнено в соответствии со справочником ФСТЭК);
- Прикладное ПО(может быть не заполнено в соответствии со справочником ФСТЭК);
- Вендор ПО (может быть не заполнено в соответствии со справочником ФСТЭК);
- Версия ПО;
- Уровень значимости ИС;
- Категория значимости ОКИИ;

- Ввод в промышленную эксплуатацию;
- Планируемый вывод из эксплуатации;
- Наличие ТП;
- Тип ТП;
- SLA: время реагирования, в т.ч для аутсорсинга.

Данными **не заполняются** следующие столбцы:

- Состав ПДн;
- Объем ПДн;
- Субъекты ПДн;
- Тип актуальных угроз;
- Определение уровня защищенности ПДн;
- Класс ГИС;
- Масштаб ГИС;
- Группа защищенности (АСУ);
- Тип информации (АСУ);
- Класс (АСУ);
- Уровень конфиденциальности (АСУ);
- Инструмент мониторинга / надежности функционирования.

АСУ

Данными заполняются следующие столбцы:

- Регион присутствия компании;
- Отрасль;
- Локальное расположение ИА;
- Уникальный номер ИА обследования/оценки ИТ-инфраструктуры;
- Наименование ИСПДн/ГИС/МИС/Другой ИС/АСУ/ЦОД/Серверная/ ИТС/ОКИИ;
- Отнесение информационного объекта к ОКИИ;
- Тип ИА;
- Вид ИА;
- Идентификатор ценности ИА;
- Сертификация / аттестация ФСТЭК;
- Название ПО;
- Разработчик / Вендор;
- Назначение;
- Наименование ОС (может быть не заполнено в соответствии со справочником ФСТЭК);
- Прикладное ПО (может быть не заполнено в соответствии со справочником ФСТЭК);
- Вендор ПО (может быть не заполнено в соответствии со справочником ФСТЭК);

- Версия ПО;
- Группа защищенности (АСУ);
- Тип информации (АСУ);
- Класс (АСУ);
- Уровень конфиденциальности (АСУ);
- Категория значимости ОКИИ;
- Ввод в промышленную эксплуатацию;
- Планируемый вывод из эксплуатации;
- Наличие ТП;
- Тип ТП;
- SLA: время реагирования, в т.ч для аутсорсинга.

Данными не заполняются следующие столбцы:

- Состав ПДн;
- Объем ПДн;
- Субъекты ПДн;
- Тип актуальных угроз;
- Определение уровня защищенности ПДн;
- Класс ГИС;
- Масштаб ГИС;
- Уровень значимости ИС;
- Инструмент мониторинга / надежности функционирования.

Другие АСУ

Данными заполняются следующие столбцы:

- Регион присутствия компании;
- Отрасль;
- Локальное расположение ИА;
- Уникальный номер ИА обследования/оценки ИТ-инфраструктуры;
- Наименование ИСПДн/ГИС/МИС/Другой ИС/АСУ/ЦОД/Серверная/ ИТС/ОКИИ;
- Отнесение информационного объекта к ОКИИ;
- Тип ИА;
- Вид ИА;
- Идентификатор ценности ИА;
- Сертификация / аттестация ФСТЭК
- Название ПО;
- Разработчик / Вендор
- Назначение
- Наименование ОС;
- Прикладное ПО;
- Вендор ПО;

- Версия ПО;
- Группа защищенности (АСУ);
- Тип информации (АСУ);
- Класс (АСУ);
- Уровень конфиденциальности (АСУ);
- Категория значимости ОКИИ;
- Ввод в промышленную эксплуатацию;
- Планируемый вывод из эксплуатации;
- Наличие ТП;
- Тип ТП;
- SLA: время реагирования, в т.ч для аутсорсинга.

Данными **не заполняются** следующие столбцы:

- Состав ПДн;
- Объем ПДн;
- Субъекты ПДн;
- Тип актуальных угроз;
- Определение уровня защищенности ПДн;
- Класс ГИС;
- Масштаб ГИС;
- Уровень значимости ИС;
- Инструмент мониторинга / надежности функционирования.

ЦОД

Данными заполняются следующие столбцы:

- Регион присутствия компании;
- Отрасль;
- Локальное расположение ИА;
- Уникальный номер ИА обследования/оценки ИТ-инфраструктуры;
- Наименование ИСПДн/ГИС/МИС/Другой ИС/АСУ/ЦОД/Серверная/ ИТС/ОКИИ;
- Отнесение информационного объекта к ОКИИ;
- Тип ИА;
- Вид ИА;
- Идентификатор ценности ИА;
- Сертификация / аттестация ФСТЭК
- Категория значимости ОКИИ (если присвоен статус ОКИИ);
- Инструмент мониторинга / надежности функционирования;
- Ввод в промышленную эксплуатацию;
- Планируемый вывод из эксплуатации;
- Наличие ТП;
- Тип ТП;

- SLA: время реагирования, в т.ч. для аутсорсинга.

Данными не заполняются следующие столбцы:

- Название ПО;
- Разработчик / Вендор;
- Назначение;
- Наименование ОС;
- Прикладное ПО;
- Вендор ПО;
- Версия ПО;
- Состав ПДн;
- Объем ПДн;
- Субъекты ПДн;
- Тип актуальных угроз;
- Определение уровня защищенности ПДн;
- Класс ГИС;
- Масштаб ГИС;
- Уровень значимости ИС;
- Группа защищенности (АСУ);
- Тип информации (АСУ);
- Класс (АСУ);
- Уровень конфиденциальности (АСУ).

Серверная

Данными заполняются следующие столбцы:

- Регион присутствия компании;
- Отрасль;
- Локальное расположение ИА;
- Уникальный номер ИА обследования/оценки ИТ-инфраструктуры;
- Наименование ИСПДн/ГИС/МИС/Другой ИС/АСУ/ЦОД/Серверная/ ИТС/ОКИИ;
- Отнесение информационного объекта к ОКИИ;
- Тип ИА;
- Вид ИА;
- Идентификатор ценности ИА;
- Сертификация / аттестация ФСТЭК
- Категория значимости ОКИИ (если присвоен статус ОКИИ);
- Инструмент мониторинга / надежности функционирования;
- Ввод в промышленную эксплуатацию;
- Планируемый вывод из эксплуатации;
- Наличие ТП;
- Тип ТП;

- SLA: время реагирования, в т.ч. для аутсорсинга.

Данными не заполняются следующие столбцы:

- Название ПО;
- Разработчик / Вендор;
- Назначение;
- Наименование ОС;
- Прикладное ПО;
- Вендор ПО;
- Версия ПО;
- Состав ПДн;
- Объем ПДн;
- Субъекты ПДн;
- Тип актуальных угроз;
- Определение уровня защищенности ПДн;
- Класс ГИС;
- Масштаб ГИС;
- Уровень значимости ИС;
- Группа защищенности (АСУ);
- Тип информации (АСУ);
- Класс (АСУ);
- Уровень конфиденциальности (АСУ).

ИТС

Данными заполняются следующие столбцы:

- Регион присутствия компании;
- Отрасль;
- Локальное расположение ИА;
- Уникальный номер ИА обследования/оценки ИТ-инфраструктуры;
- Наименование ИСПДн/ГИС/МИС/Другой ИС/АСУ/ЦОД/Серверная/ ИТС/ОКИИ;
- Отнесение информационного объекта к ОКИИ;
- Тип ИА;
- Вид ИА;
- Идентификатор ценности ИА;
- Сертификация / аттестация ФСТЭК
- Категория значимости ОКИИ (если присвоен статус ОКИИ);
- Инструмент мониторинга / надежности функционирования;
- Ввод в промышленную эксплуатацию;
- Планируемый вывод из эксплуатации;
- Наличие ТП;
- Тип ТП;

- SLA: время реагирования, в т.ч. для аутсорсинга.

Данными не заполняются следующие столбцы:

- Название ПО;
- Разработчик / Вендор;
- Назначение;
- Наименование ОС;
- Прикладное ПО;
- Вендор ПО;
- Версия ПО;
- Состав ПДн;
- Объем ПДн;
- Субъекты ПДн;
- Тип актуальных угроз;
- Определение уровня защищенности ПДн;
- Класс ГИС;
- Масштаб ГИС;
- Уровень значимости ИС;
- Группа защищенности (АСУ);
- Тип информации (АСУ);
- Класс (АСУ);
- Уровень конфиденциальности (АСУ).

4. Начало работы в программном комплексе

Для начала работы с ПК «МПСИБ» необходимо открыть в браузере страницу входа.
В открывшемся окне аутентификации в соответствующих полях необходимо указать логин и пароль пользователя (**Ошибка! Источник ссылки не найден.**).

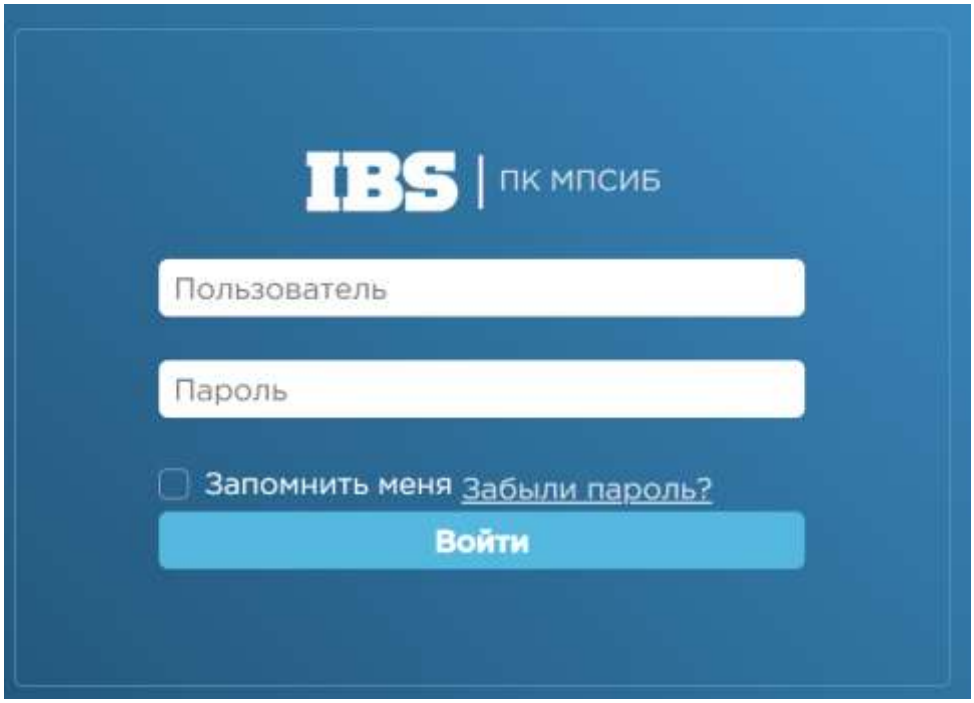


Рисунок 1 Окно аутентификации

Обратите внимание!

Сложность пароля должна соответствовать актуальным требованиям безопасности, рекомендованная длина пароля - не менее 12 символов.

Количество попыток ввода пароля ограниченно. После 3 неудачных попыток учетная запись блокируется. Для ее восстановления необходимо обратиться к системному администратору.

В результате корректной аутентификации отобразится стартовая страница ПК (**Ошибка! Источник ссылки не найден.**).

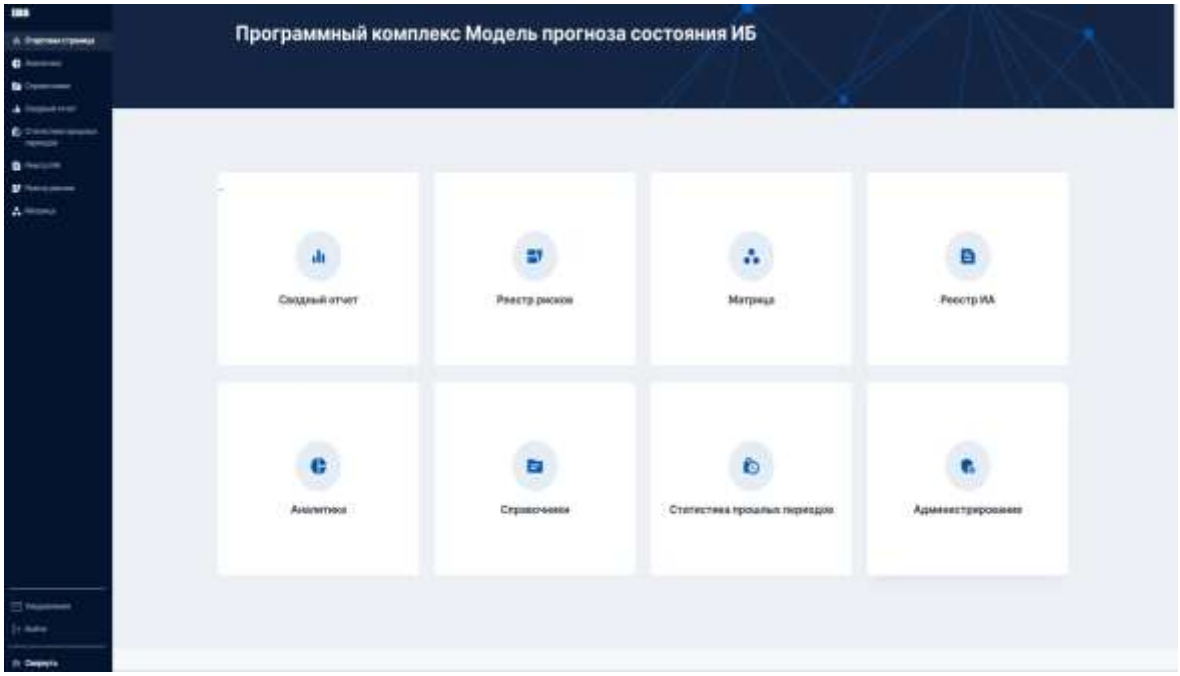


Рисунок 2 Стартовая страница

На стартовой странице доступны следующие наборы элементов интерфейса:

1. Боковая панель — отображает основное меню ПК.
2. Область просмотра данных — отображает состав разделов.
3. Кнопка «Уведомления» — позволяет открыть блок «Системные сообщения», содержащий список событий ПК и элементы управления (Рисунок 3).

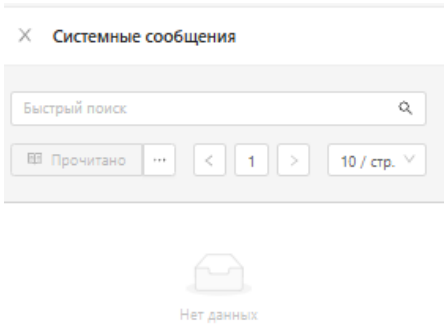


Рисунок 3 Окно системных сообщений

4. Кнопка «Свернуть» — позволяет сворачивать и разворачивать боковую панель.
5. Кнопка «Выйти» — позволяет закрыть сессию.

Для перехода в интересующий раздел ПК следует кликнуть на его название в боковом меню или в области просмотра данных.

Обратите внимание: состав доступных разделов ПК определяется ролью пользователя!

5. Раздел «Администрирование»

Раздел доступен только пользователям с ролью Администратор.
Администратор может открывать версии аналитических отчетов и новые периоды.

5.1. Открытие версий аналитических отчетов

По требованию Владельца процесса Администратор может открывать версии аналитических отчетов, которые прошли согласование и имеют статус «Закрыта».
Сведения о процессах согласования содержатся в разделе **11. Реестр рисков**.
Для изменения статуса версии аналитического отчета на «Открыта» необходимо выполнить следующие действия:

1. На вкладке **Версии** в поле раскрывающегося списка «Версия» следует выбрать необходимую версию аналитического отчета. В расположенной ниже таблице отобразятся сведения о выбранной версии. (Рисунок 4).

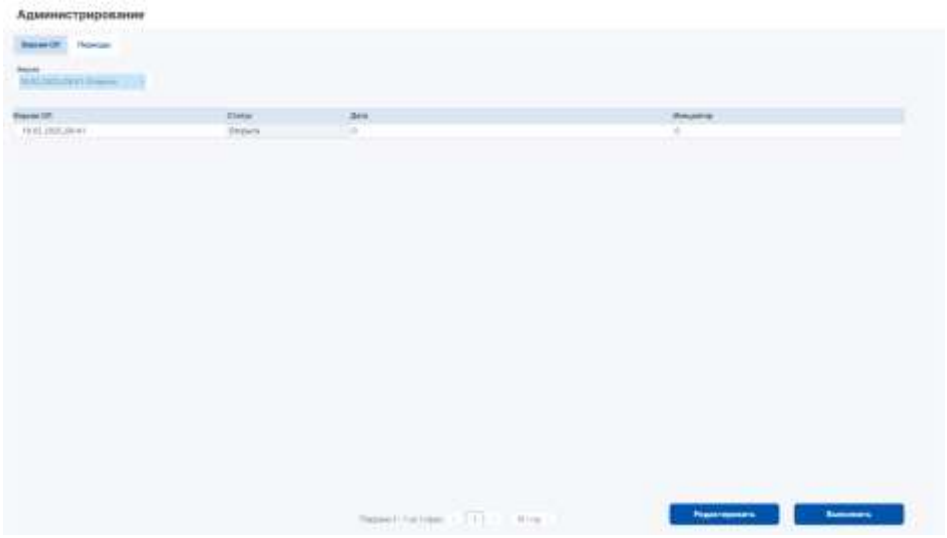


Рисунок 4 Окно выбора версии аналитического отчета

1. Для изменения статуса версии следует нажать на кнопку **Редактировать** и в ячейке столбца **Статус** изменить значение на **Открыта**.
2. Для сохранения изменения статуса следует последовательно нажать на кнопки **Выполнить** и **Выйти**.

В результате изменения статуса версии аналитического отчета станут доступны для внесения корректировок и изменений карточки ИА в части угроз и рисков ИБ.
Описание работы с аналитическими отчетами содержится в разделах **3.2 Аналитические отчеты** и **6. Аналитика**.

5.2. Открытие новых периодов

Администратор может выполнить открытие нового периода (календарный год) для формирования прогноза угроз ИБ и отчета по рискам ИБ.

Для открытия нового периода необходимо выполнить следующие действия:

1. Открыть вкладку **Периоды** (Рисунок 5).
2. В поле **Новый отчетный период** указать или выбрать из списка конкретный календарный год.
3. Нажать кнопку **Добавить период**.

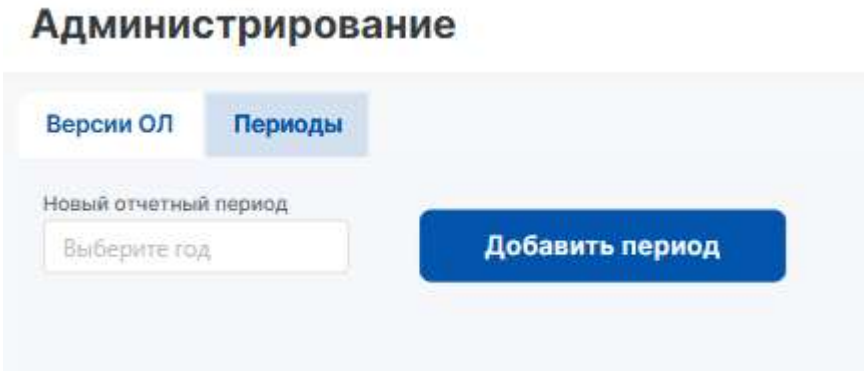


Рисунок 5 Раздел администратора, открытие нового периода

6. Раздел «Аналитика»

В разделе отображается список версий загрузок аналитических отчетов «Аналитика_ИА» и «Аналитика_Инциденты» (Рисунок 6).

Рисунок 6 Раздел Аналитика, загруженные аналитические отчеты

На основании набора данных возможно проведение анализа состояния ИБ, прогнозирование атак и инцидентов, выявление уязвимостей ИА, идентификация угроз и рисков ИБ.

ВАЖНО: на стадии загрузки файлов «Аналитика_ИА» и «Аналитика_Инциденты» проверять загрузившийся материал: перечень ИА, наличие всех характеристик ИА и информации по кибератакам и инцидентам, чтобы данные были загружены корректно и в полном объеме.

6.1. Загрузка аналитических отчетов

Для того чтобы загрузить набор данных необходимо выполнить следующие действия:

1. Нажать кнопку **Загрузить данные**.

- В открывшемся окне **Шаг 1. Загрузить реестр ИА** (Рисунок 7) нажать на центр экрана.

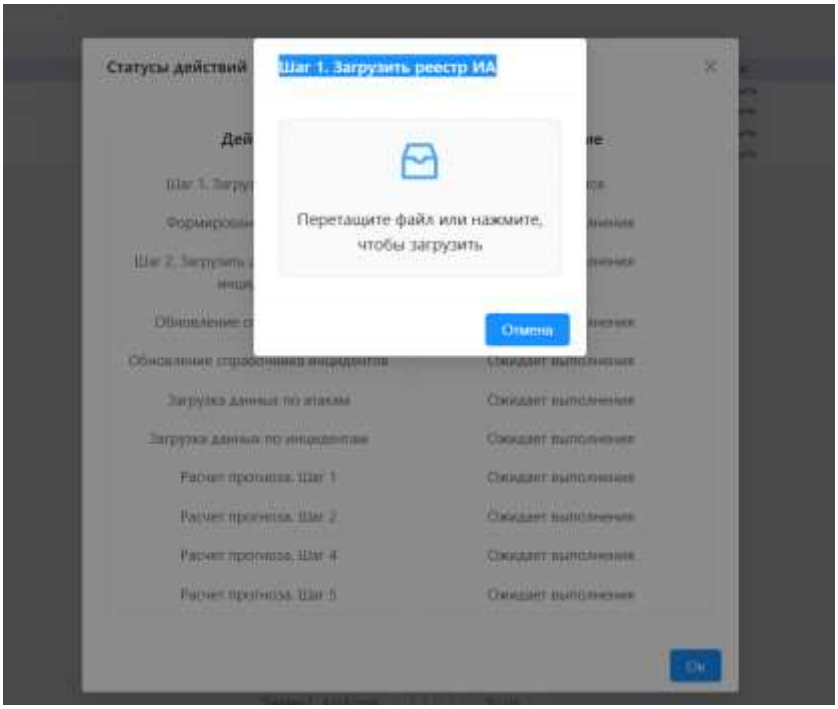


Рисунок 7 Шаг 1. Окно загрузки реестра ИА «Аналитика_ИА»

- В открывшемся окне поиска сохранённых загрузочных файлов выбрать файл *Аналитика_ИА* (Рисунок 8).

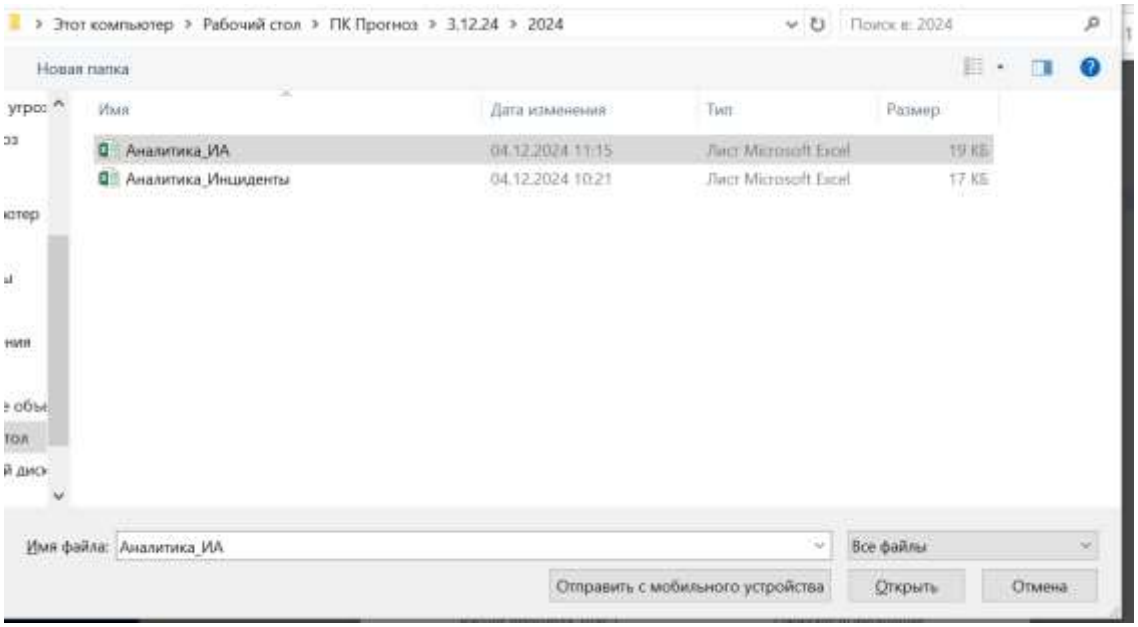


Рисунок 8 Папка с подготовленными к загрузке отчетами «Аналитика_ИА», «Аналитика_Инциденты». Выбор реестра ИА

- По окончании загрузки в окне **Статусы загрузки** должны отобразиться сообщения:

  Шаг 1. Загрузить реестр ИА - Выполнено/Выполнено с предупреждением

  Формирование реестра ИА – Выполнено/Выполнено с предупреждением

- После удачной загрузки данных по ИА откроется окно **Шаг 2. Загрузить данные по атакам и инцидентам** (Рисунок 9).

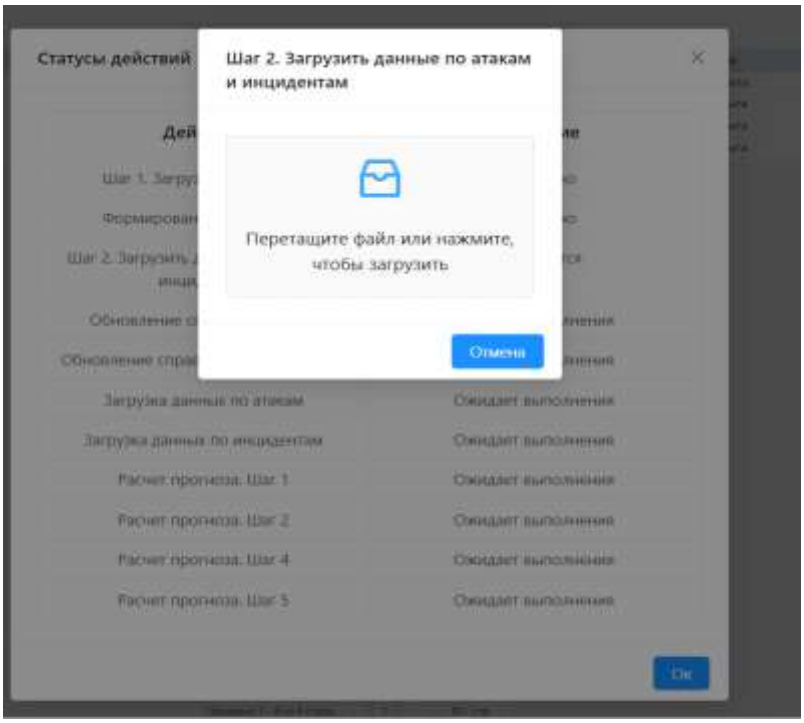


Рисунок 9 Шаг 2. Окно загрузки «Аналитика_Инциденты»

- В открывшемся окне поиска сохранённых загрузочных файлов следует выбрать файл *Аналитика_Инциденты* (Рисунок 10).

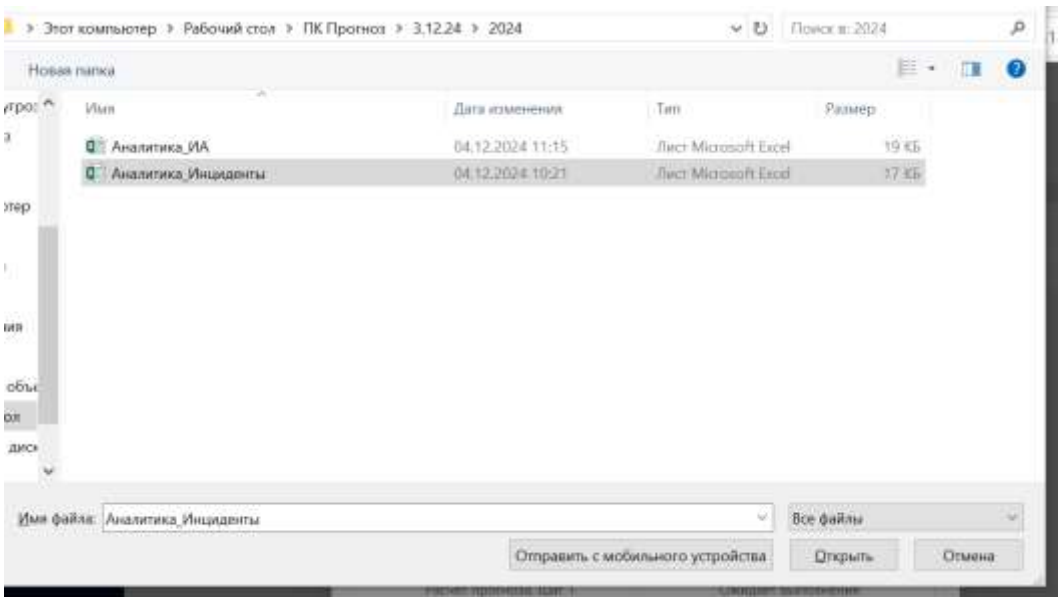


Рисунок 10 Папка с подготовленными к загрузке отчетами «Аналитика_ИА», «Аналитика_Инциденты». Выбор отчета по атакам и инцидентам

- По окончании загрузки в окне **Статусы загрузки** должно отобразиться (Рисунок 11):

Шаг 2. Загрузить данные по атакам и инцидентам – Выполнено/Выполнено с предупреждением

Обновление справочника атак - Выполнено/Выполнено с предупреждением

Обновление справочника инцидентов - Выполнено/Выполнено с предупреждением

Загрузка данных по атакам - Выполнено/Выполнено с предупреждением

Загрузка данных по инцидентам - Выполнено/Выполнено с предупреждением

Расчет прогноза. Шаг 1 - Выполнено/Выполнено с предупреждением

Расчет прогноза. Шаг 2 - Выполнено/Выполнено с предупреждением

Расчет прогноза. Шаг 4 - Выполнено/Выполнено с предупреждением

Расчет прогноза. Шаг 5 – Выполнено/Выполнено с предупреждением

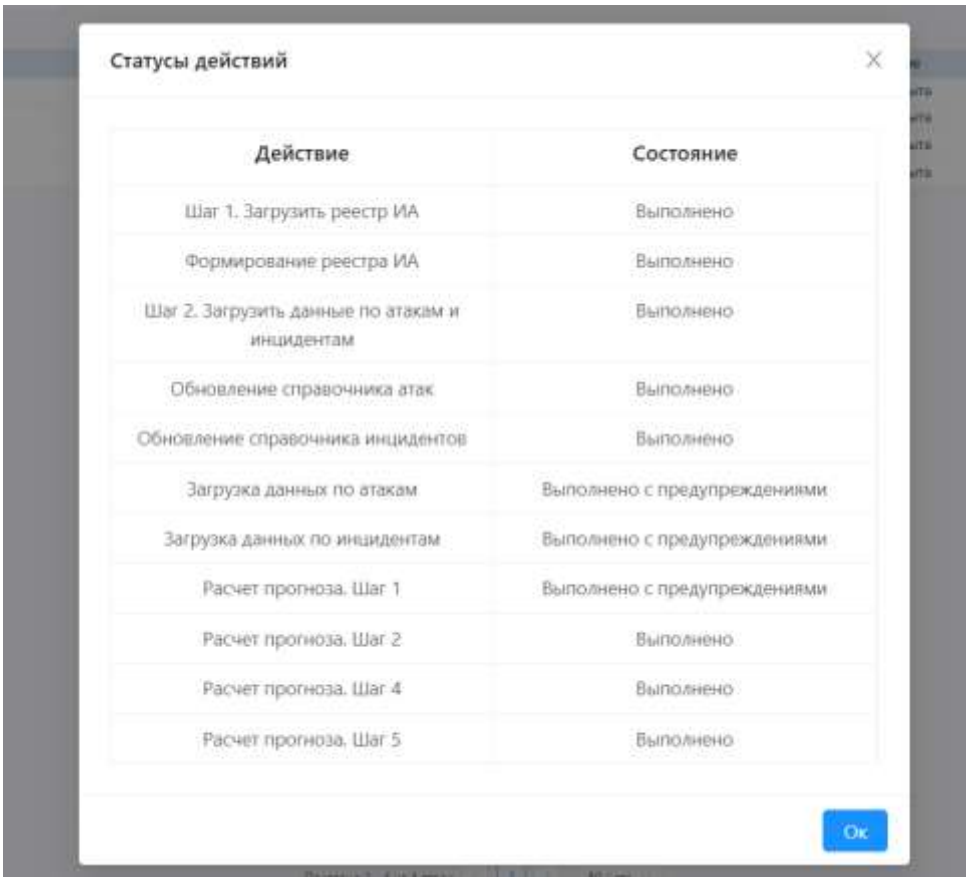


Рисунок 11 Статусы загрузки аналитических отчетов

- Далее следует нажать кнопку **Открытие версии для анализа угроз ИБ** и в открывшемся окне **Выбрать файл Аналитика_ИА.xlsx** нажать на центр экрана (Рисунок 12).

  Открытие версии для анализа угроз ИБ – это обозначение версии аналитического отчета за тот год, после которого начнет выстраиваться прогноз атак и инцидентов.

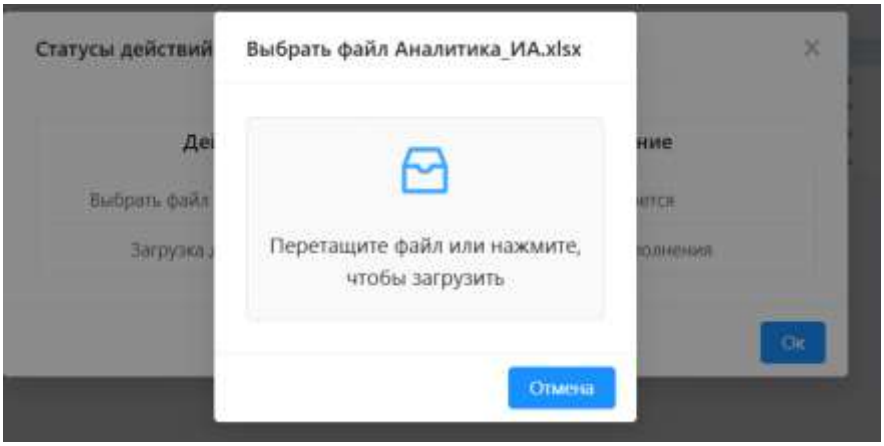


Рисунок 12 Открытие версии для анализа угроз ИБ

- Выбрать файл *Аналитика_Инциденты* (Рисунок 13).

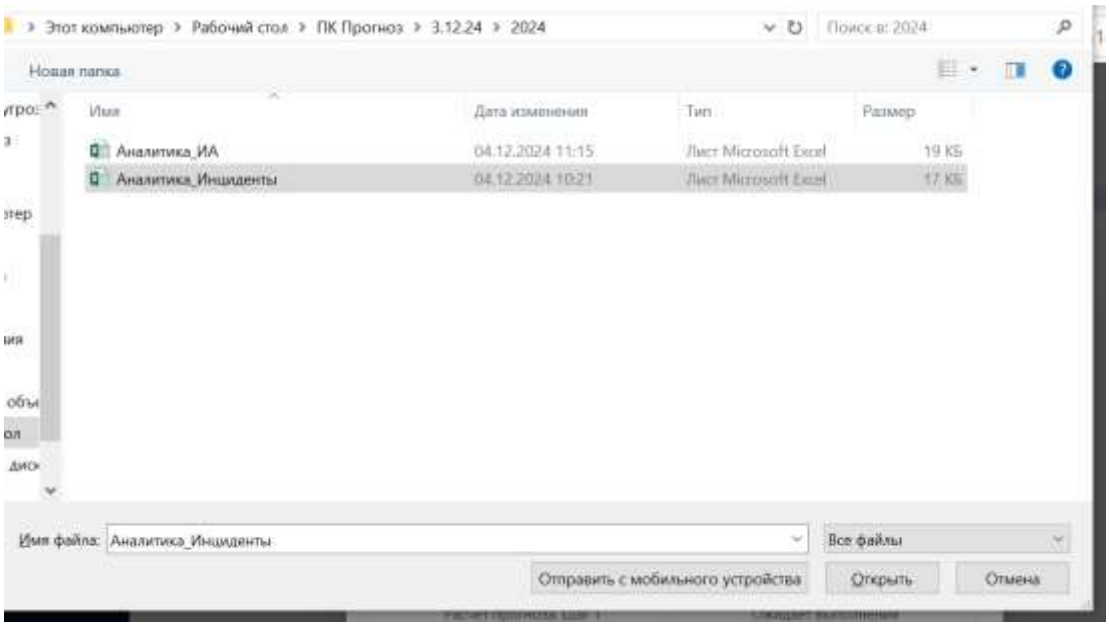


Рисунок 13 Папка с подготовленными к загрузке отчетами «Аналитика_ИА», «Аналитика_Инциденты»

- По окончании загрузки в окне **Статусы загрузки** должно отобразиться (Рисунок 14):

  Выбрать файл Аналитика_ИА.xlsx - Выполнено/Выполнено с предупреждением

  Загрузка данных по ИА – Выполнено/Выполнено с предупреждением

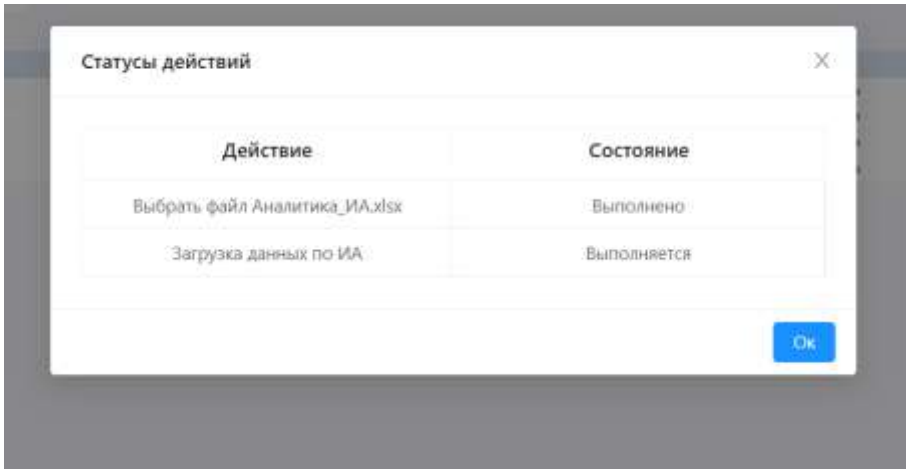


Рисунок 14 Окно статусов загрузки аналитических отчетов для открытия версии

Аналитические данные загружены успешно. Корректно сформированы графики и отчеты в разделах **Сводный отчет** и **Статистика прошлых периодов**.

После завершения загрузки данных актуальная версия аналитического отчета будет добавлена в общий перечень версий в разделе «Аналитика» со статусом «Открыта». Для её просмотра необходимо кликнуть на наименование. Откроется окно из двух вкладок «Характеристики ИА» (Рисунок 15). и «Описание инцидентов по ИА». (Рисунок 16) соответствующих по формату и содержанию ранее описанным аналитическим отчетам «Аналитика_ИА» и «Аналитика_Инциденты».

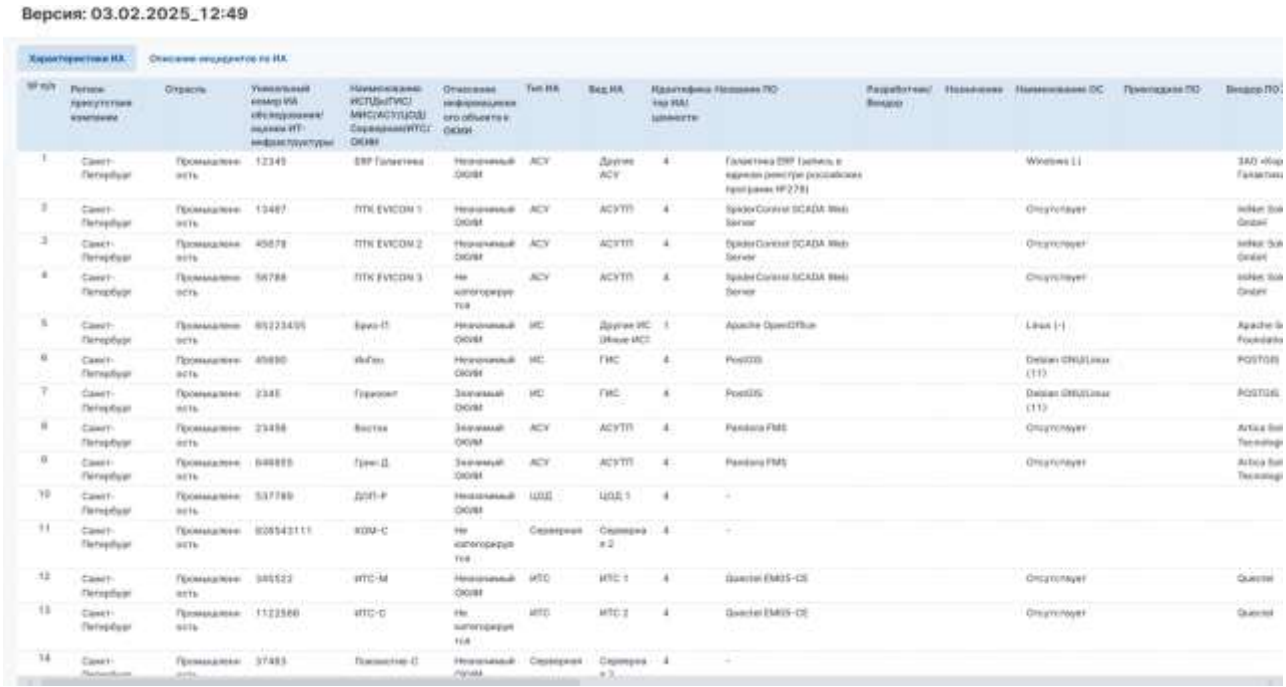


Рисунок 15 6.1.Вкладка «Характеристики ИА»

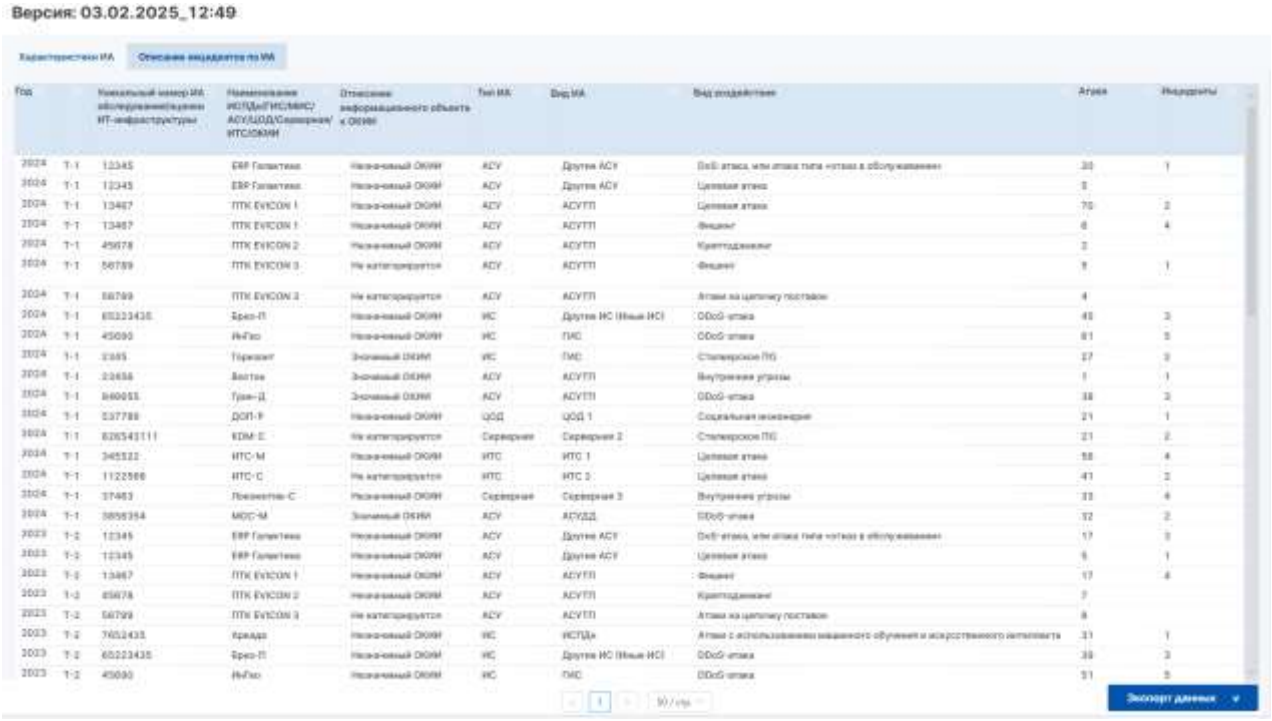


Рисунок 16 Вкладка «Описание инцидентов по ИА»

Данные по атакам и инцидентам — это фактические данные за обследуемый период. При первичной загрузке количество обследований должно отражать данные не менее, чем за 3 года. (Для наиболее точного прогноза рекомендуемый период обследования — 10 лет).

Для экспорта данных таблицы в файл формата XLSX следует нажать на кнопку **Экспорт данных** в правой нижней части экрана.

7. Раздел «Справочники»

Раздел содержит подразделы:

1) Перечень угроз ФСТЭК**;**
2) Перечень обнаруженных уязвимостей ИА**;**
3) Оценка критичности информационного актива**.**

7.1. Перечень угроз ФСТЭК

В разделе отображается таблица с перечнем угроз ИБ, загруженная с портала ФСТЭК (Рисунок 17).

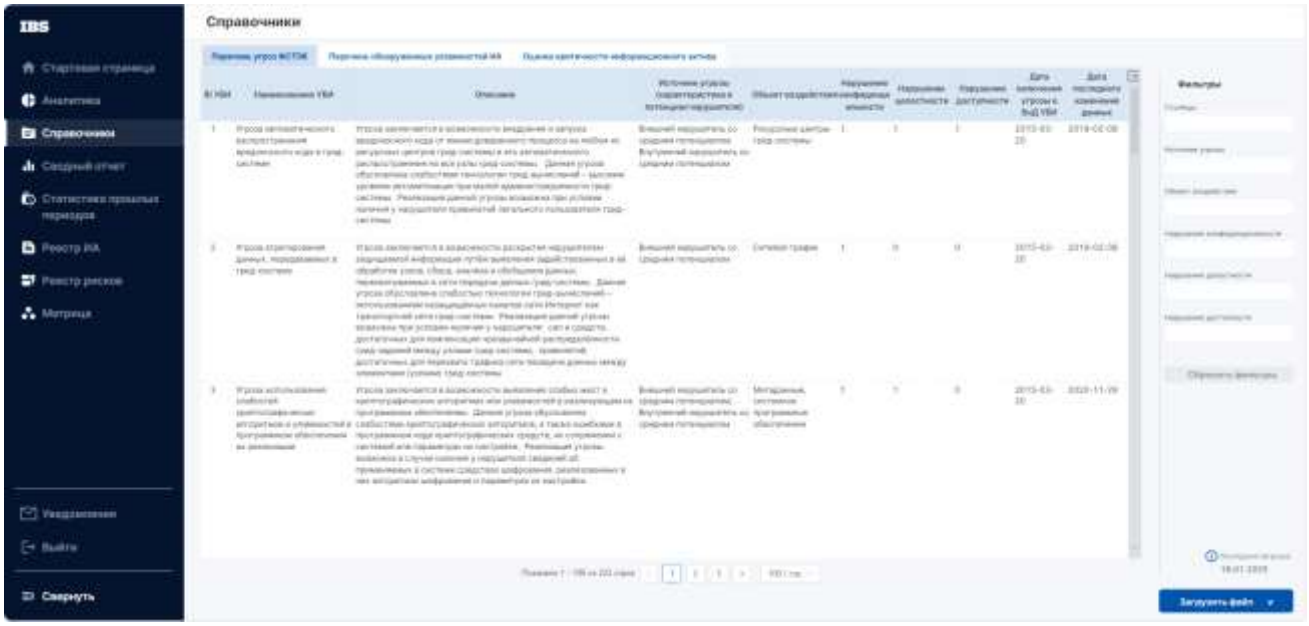


Рисунок 17 Подраздел «Перечень угроз ФСТЭК»

Данные в таблице могут быть отфильтрованы с помощью инструментов, размещенных на боковой панели.

Для загрузки актуального справочника угроз необходимо нажать кнопку «Загрузить файл» и в открывшемся окне выбрать, предварительно подготовленный парсером справочников ФСТЭК файл *thrlist_info.csv* (Рисунок 18).

Дата обновления загрузки отображается в правом нижнем углу.

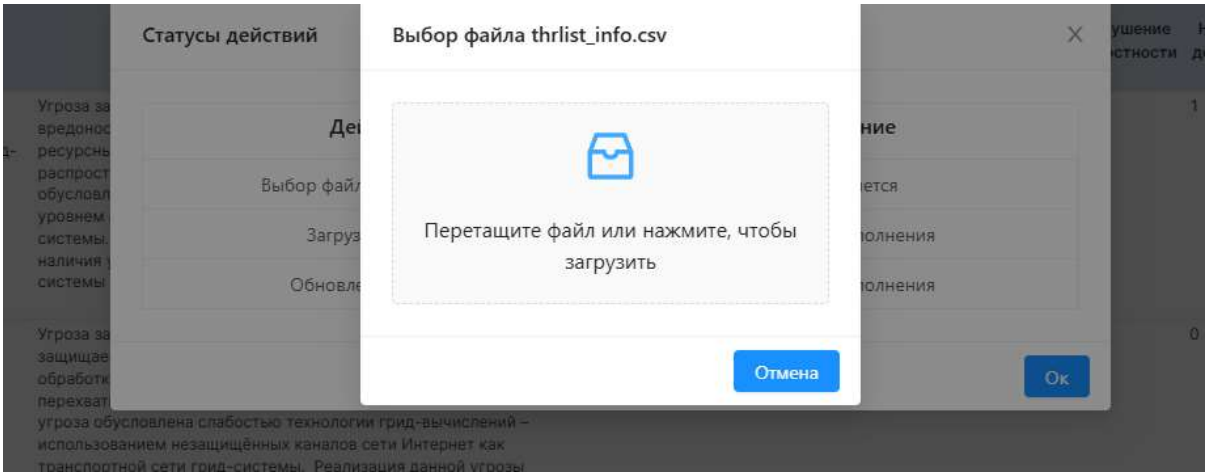


Рисунок 18 Окно загрузки справочника угроз ФСТЭК

После завершения загрузки информация в таблице будет обновлена в соответствии с данными из файла *thrlist_info.csv* и доступна для дальнейшей работы.

7.2. Перечень обнаруженных уязвимостей ИА

В подразделе отражается перечень обнаруженных уязвимостей ИА (Рисунок 19).

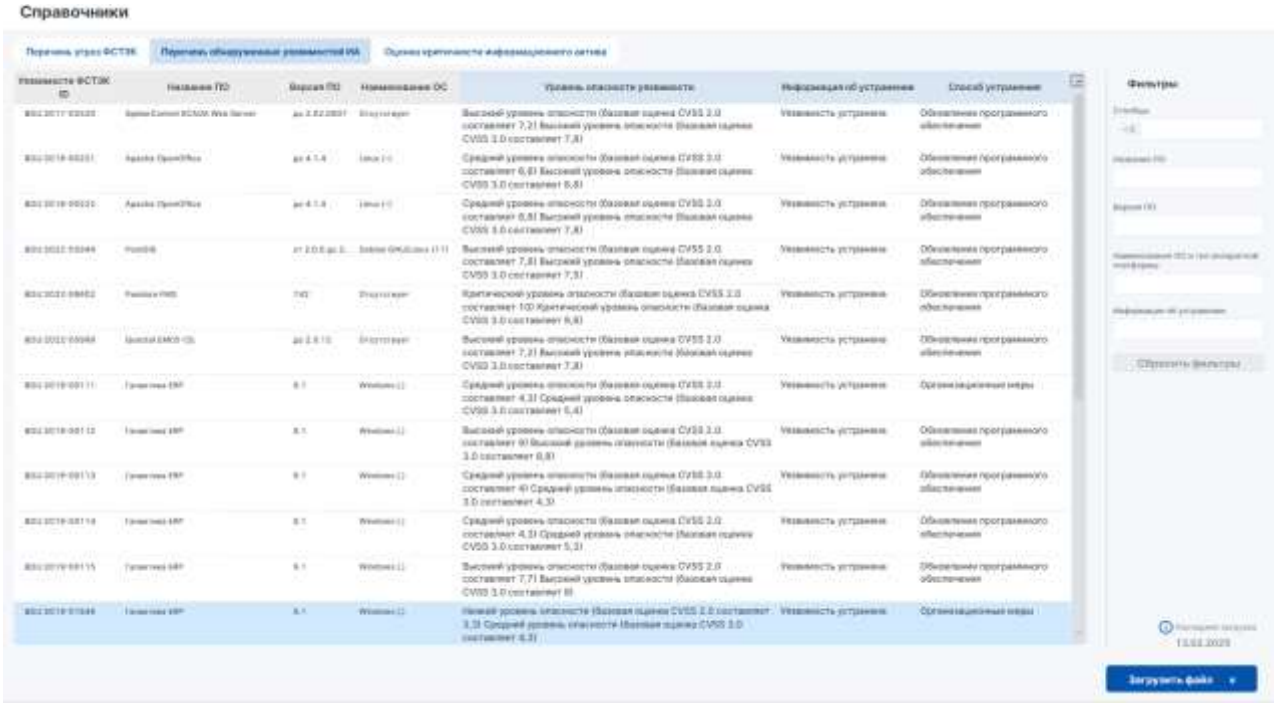


Рисунок 19 Подраздел «Перечень обнаруженных уязвимостей ИА»

Данные в таблице могут быть отфильтрованы с помощью инструментов, размещенных на боковой панели.

Для актуализации данных необходимо нажать кнопку **Загрузить файл** и в открывшемся окне поочередно выбрать предварительно сформированные парсером справочника ФСТЭК файлы (Рисунок 20):

- *meta_data_info*;

- *thrlist_info*;
- *title_OS*;
- *version_PO*;
- *vendor_PO.*

Дата обновления загрузки отображается в правом нижнем углу.

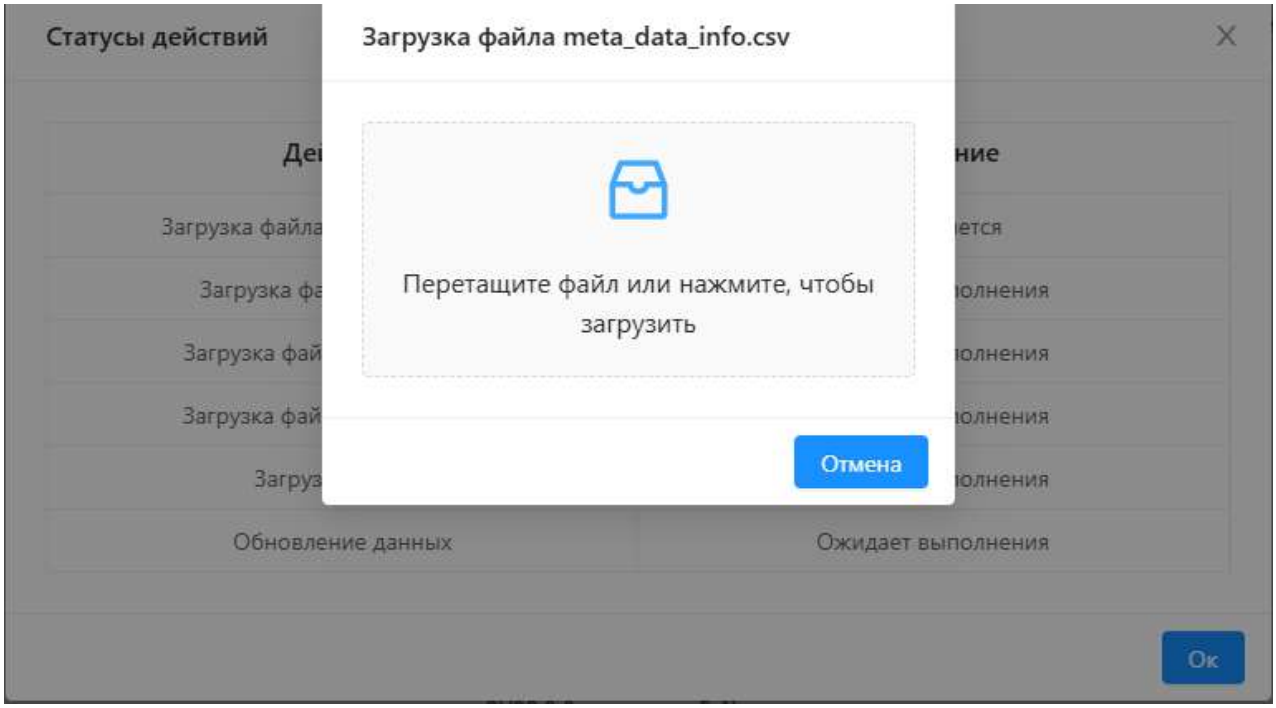


Рисунок 20 Окно загрузки справочника уязвимостей ФСТЭК

После завершения загрузки информация в таблице будет обновлена в соответствии с загруженными данными и доступна для дальнейшей работы.

7.3. Оценка критичности информационного актива

В подразделе отражается таблица с данными о критичности информационного актива. Для изменения значений в таблице следует нажать кнопку «Редактировать» (Рисунок 21).

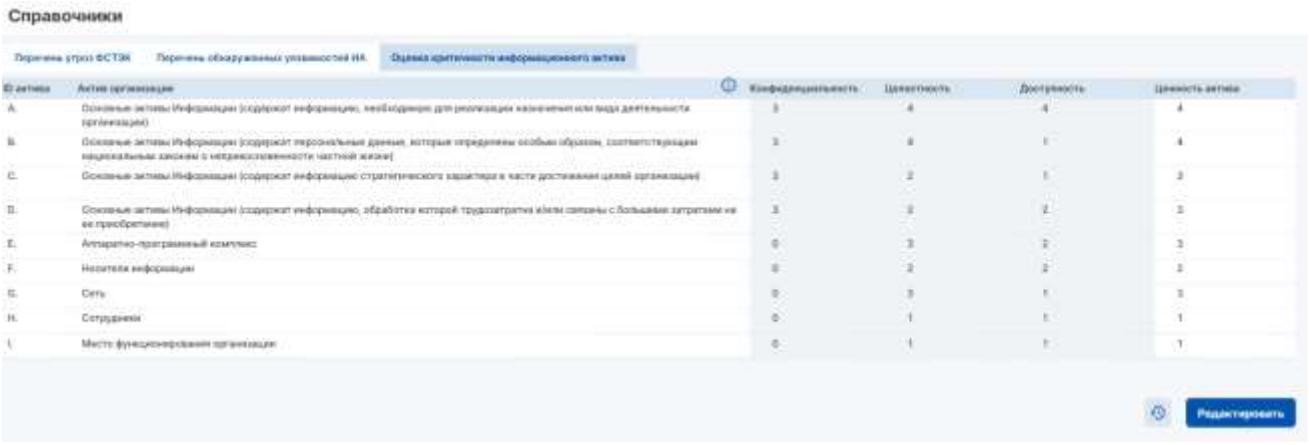
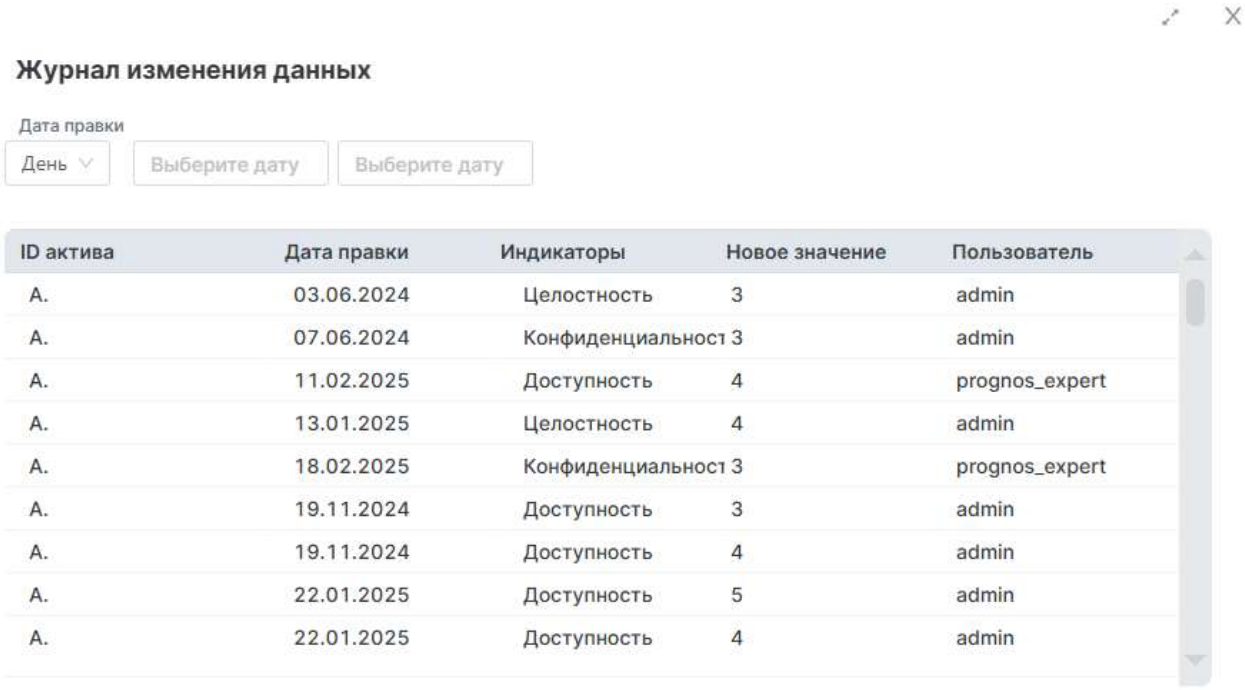


Рисунок 21 Подраздел «Оценка критичности ИА»

Для сохранения внесенных изменений следует нажать кнопку «Выйти».

В таблице «Журнал изменения данных», открываемой кнопкой , отображается история внесенных правок (Рисунок 22).



ID актива	Дата правки	Индикаторы	Новое значение	Пользователь
A.	03.06.2024	Целостность	3	admin
A.	07.06.2024	Конфиденциальност	3	admin
A.	11.02.2025	Доступность	4	prognos_expert
A.	13.01.2025	Целостность	4	admin
A.	18.02.2025	Конфиденциальност	3	prognos_expert
A.	19.11.2024	Доступность	3	admin
A.	19.11.2024	Доступность	4	admin
A.	22.01.2025	Доступность	5	admin
A.	22.01.2025	Доступность	4	admin

Рисунок 22 Журнал изменения данных

8. Раздел «Сводный отчет»

В разделе отражаются графики, отчеты с прогнозом кибератак и инцидентов в разрезе 6 лет, формируемые на основе фактических данных за прошлые годы и в виде прогноза на 3 года вперед.

8.1. График

В подразделе отражаются графики (Рисунок 23):

- Динамика инцидентов в общем объеме кибератак, ед.;
- Соотношение кибератак и инцидентов, %;
- Динамика кибератак по ИСПДн, ГИС, АСУТП, ЦОД, Серверной, ИТС, ед.;
- Динамика кибератак в разрезе по ИС, АСУ, ЦОД, Серверные, ИТС, ед.

Рисунок 23 Подраздел «График»

На графиках возможен выборочный просмотр динамики по типам ИА. Уточненные данные станут доступны при выборе конкретного показателя на легенде графиков (Рисунок 24).

Рисунок 24 Легенда графиков

При наведении курсора на цветные области графиков отображаются сведения о конкретных числовых показателях.

8.2. Отчет

В подразделе отражается отчет (Рисунок 25), сформированный на основе фактических данных об атаках и инцидентах за предыдущие 3 года в разрезе ИА, а также прогноз на 3 года вперед.

Рисунок 25 Подраздел «Отчет»

При выборе конкретного значения в ячейке столбца «Вид воздействия» отразится график динамики инцидентов в общем объеме кибератак.
Доступна возможность фильтрации данных по признакам, выбираемым в соответствующих полях раскрывающихся списков.

8.3. Анализ

В подразделе отражается отчет (Рисунок 266), сформированный на основе фактических данных об атаках и инцидентах за предыдущие 3 года, а также прогноз на 3 года вперед.

Обследуемые ИА разбиваются на группы:

- Значимый ОКИИ;
- Незначимый ОКИИ;
- Не категорируется.

Внутри каждой такой группы ИА разбиваются на типы:

- АСУ;

- ИС;
- ЦОД;
- Серверная;
- ИТС.

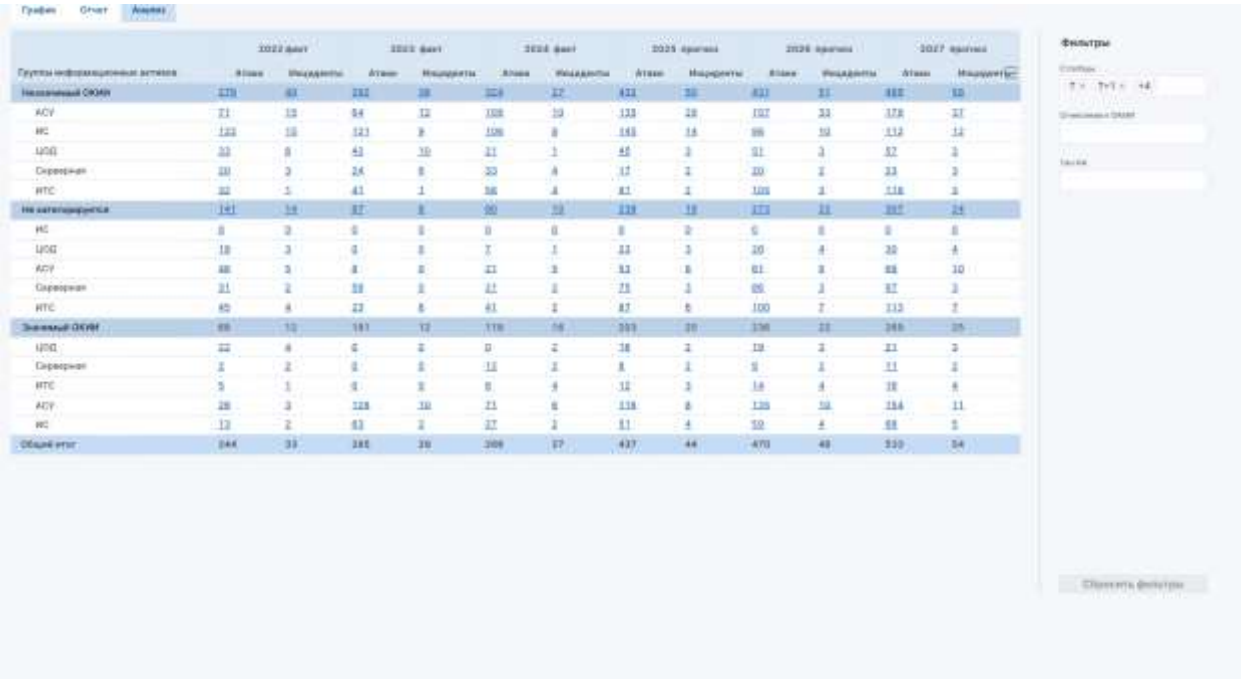


Рисунок 266 Подраздел «Анализ»

Для получения подробных сведений об атаках и инцидентах следует выбрать конкретное значение количества атак или инцидентов в соответствующей ячейке отчета. В результате отразится таблица с данными по ИА и связанными с ними атаками или инцидентами (Рисунок 277). Источником данных служат сведения раздела **Аналитика**.

Рисунок 277 Отчет по атакам и инцидентам

Доступна возможность фильтрации данных по признакам, выбираемым в соответствующих полях раскрывающихся списков.

9. Раздел «Статистика прошлых периодов»

В разделе отражается аналитические данные прошлых периодов (факт) по атакам и инцидентам на анализируемые ИА в виде графиков и таблиц в подразделах **График**, **Отчет**, **Анализ**.

9.1. График

В разделе отображаются графики (Рисунок 282828):

- Динамика инцидентов в общем объеме кибератак, ед.;
- Соотношение кибератак и инцидентов, %;
- Динамика кибератак по ИСПДн, ГИС, АСУТП, ЦОД, Серверной, ИТС, ед.;
- Динамика кибератак в разрезе по ИС, АСУ, ЦОД, Серверные, ИТС, ед.

Рисунок 2828 Окно подраздела «Графики»

На графиках возможен выборочный просмотр динамики по типам ИА. Уточненные данные станут доступны при выборе конкретного показателя на легенде графиков путем двойного клика (Рисунок).

Рисунок 29 Легенда графиков

При наведении курсора на цветные области графиков отображаются сведения о конкретных числовых показателях.

9.2. Отчет

В разделе отражается отчет (Рисунок 290), сформированный на основе фактических данных об атаках и инцидентах в разрезе ИА.

Рисунок 290 Окно подраздела «Отчет»

Доступна возможность фильтрации данных по годам, типу и виду ИА в правом верхнем поле.

9.3. Анализ

В разделе отражается отчет (Рисунок 301), сформированный на основании фактических данных об атаках и инцидентах в разрезе ИА по признаку отнесения к ОКИИ.

Обследуемые ИА разбиваются на группы:

- Значимый ОКИИ;
- Незначимый ОКИИ;
- Не категорируется.

Внутри каждой группы ИА разбиваются на типы:

- АСУ;
- ИС;
- ЦОД;

- Серверная;
- ИТС.

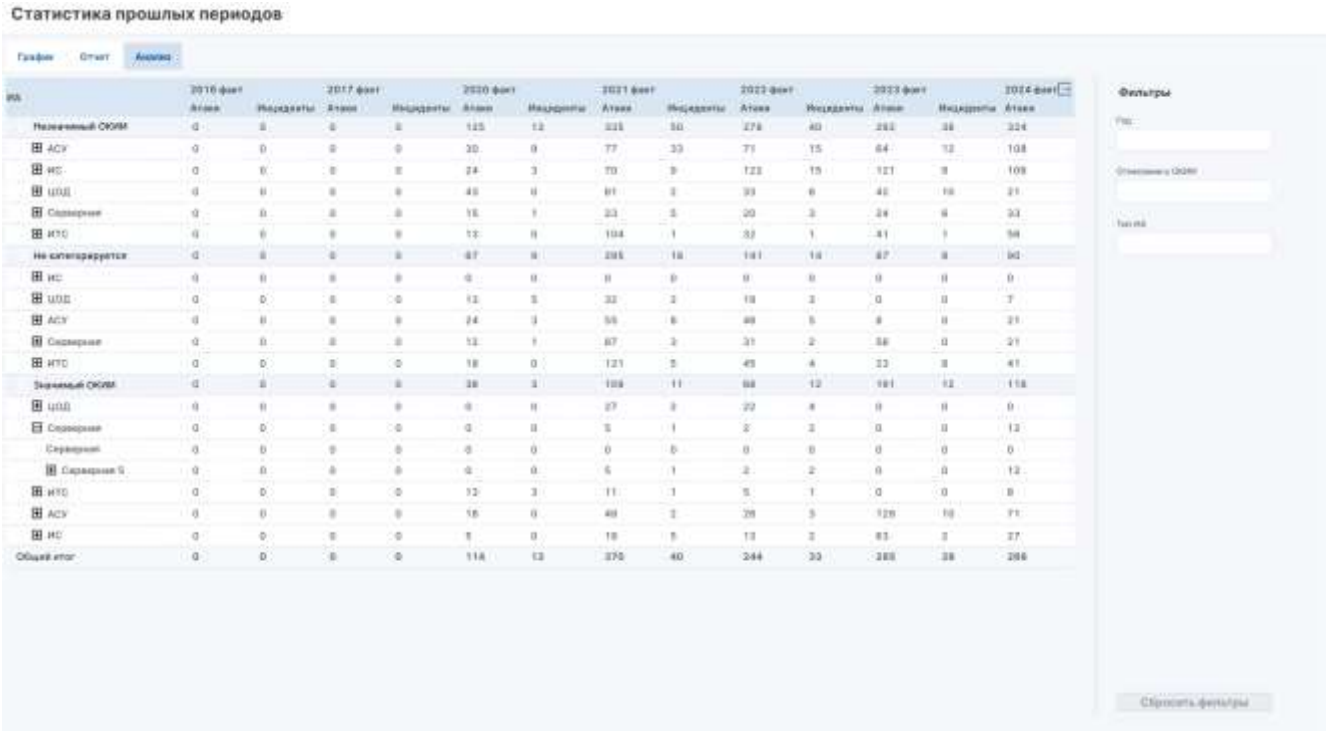


Рисунок 301 Окно подраздела «Анализ»

Для получения подробных сведений об атаках и инцидентах по определенной группе ИА, следует кликнуть на интересующее значение количества атак или инцидентов в соответствующей ячейке отчета. В результате, откроется таблица с данными по ИА и оказываемым на них атакам и инцидентам (**Ошибка! Источник ссылки не найден.**2). Источником данных служат сведения раздела «Аналитика».

Рисунок 312 Окно отчета по атакам и инцидентам

Доступна возможность фильтрации данных по признакам, выбираемым в соответствующих полях раскрывающихся списков.

10. Раздел «Реестр ИА»

В разделе отражается перечень ИА, сформированный при загрузке в разделе «Аналитика» аналитического отчета «Аналитика_ИА», в части перечня ИА, и аналитического отчета «Аналитика_Инциденты», в части учета атак и инцидентов на ИА в индивидуальном порядке. (**Ошибка! Источник ссылки не найден.**3).

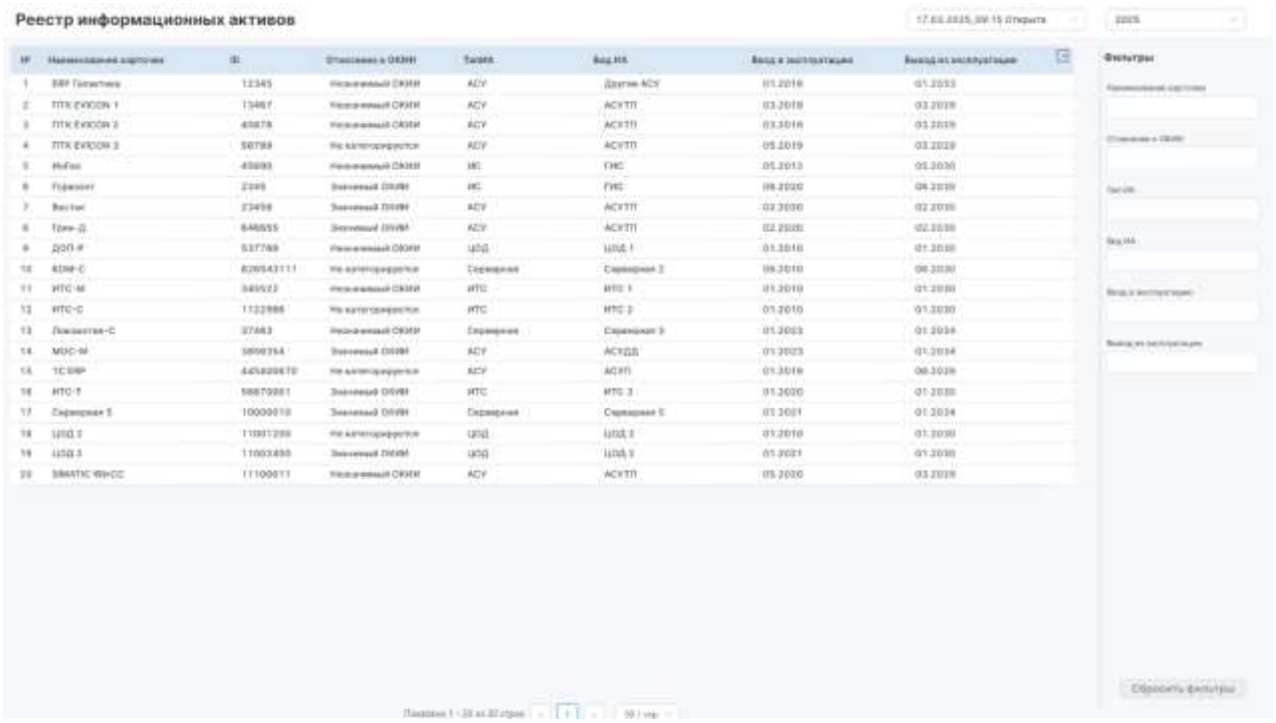


Рисунок 323 Окно раздела «Реестр ИА»

В правой части панели доступна возможность фильтрации данных по признакам в соответствующих полях раскрывающихся списков.

Для просмотра данных отдельно по каждому активу необходимо кликнуть на наименование ИА. Откроется карточка информационного актива.

Каждая карточка содержит подразделы:

1) Статистика кибератак**;**
2) Описание инцидентов**;**
3) Угрозы**;**
4) Риски**.**

10.1. Статискика кибератак

В подразделе «Статистика кибератак» можно увидеть динамику атак и инцидентов в разрезе 6 лет, техническую характеристику ИА, дату его ввода и вывода из эксплуатации (Рисунок 334).

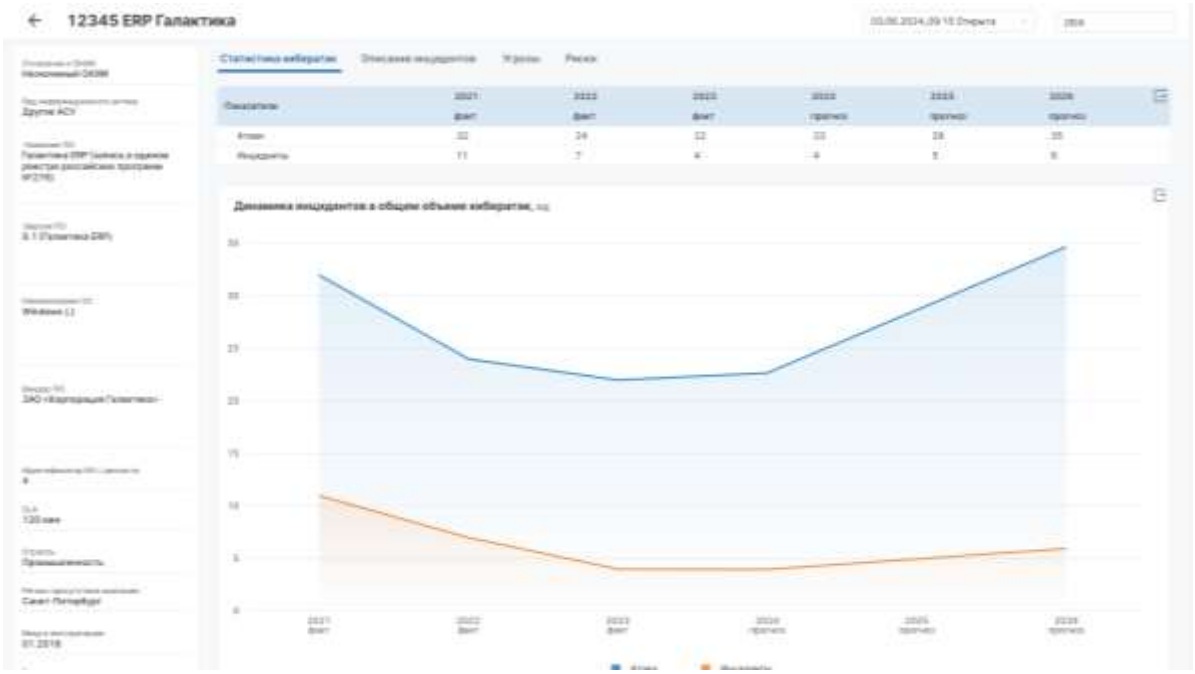


Рисунок 334 Карточка ИА, Статистика кибератак

10.2. Описание инцидентов

В подразделе «Описание инцидентов» собирается статистика атак и инцидентов в разрезе по виду воздействия. Также ниже специалист ИБ/ИТ и ИБ заполняет раздел «Характеристика инцидентов» (Рисунок 345).

Для внесения данных по характеристикам инцидентов следует нажать кнопку «Редактировать» и заполнить данные о длительности, масштабе инцидента, тактике нарушителя.

Для сохранения введённых данных необходимо нажать кнопку «Выйти».

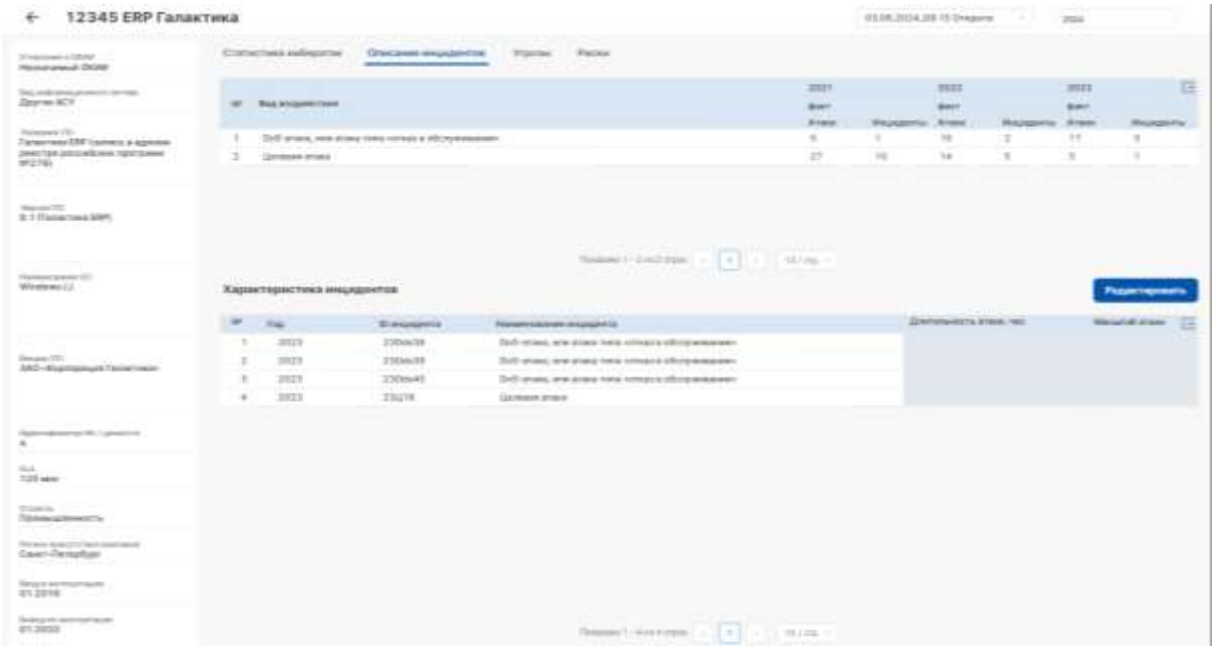


Рисунок 345 Карточка ИА, Описание инцидентов

10.3. Угрозы

В подразделе «Угрозы» следует указать, какие угрозы на данный момент характерны для рассматриваемого ИА (Рисунок 356).

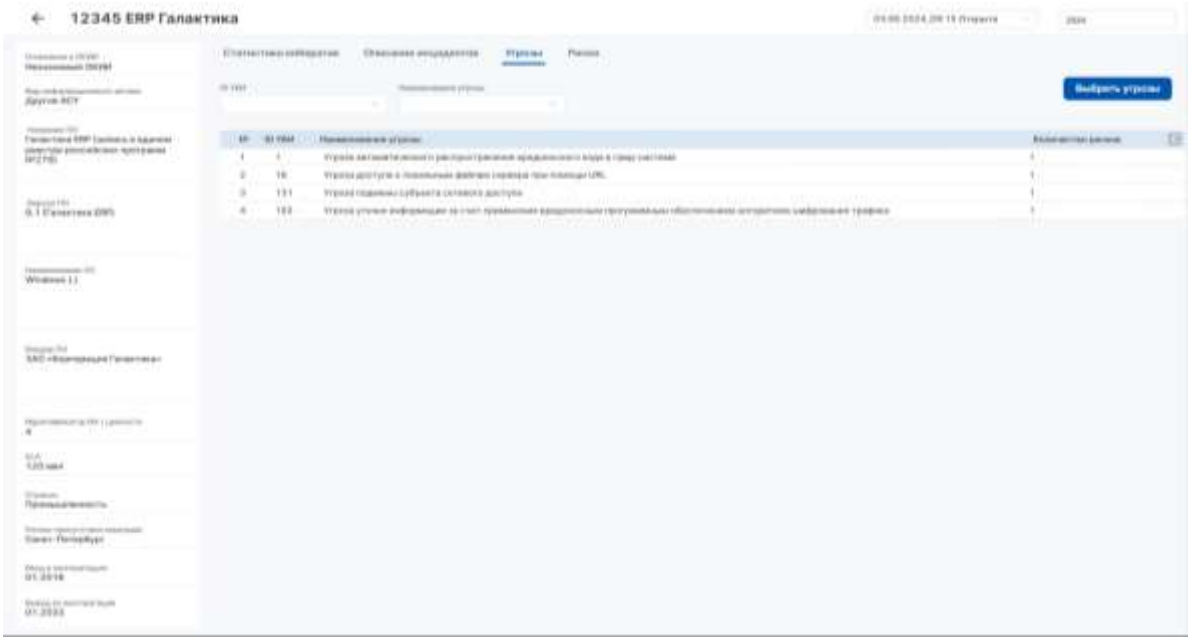


Рисунок 356 Определение угроз ИБ в карточке ИА

Для формирования перечня угроз ИБ, присущих рассматриваемому информационному активу, путем первичной идентификации необходимо выполнить следующие действия:

1. Нажать кнопку «Выбрать угрозы» и в открывшемся окне выбрать соответствующую ИА угрозу/перечень угроз ИБ проставив галочки в крайнем правом столбце.
2. При закрытии окна выбора угроз ИБ, выбранные позиции сохраняются.
3. Для удаления или замены выбранных позиций угроз необходимо снова нажать кнопку «Выбрать угрозы», снять галочки с ранее выбранных угроз ИБ и проставить более подходящие. Далее закрыть окно и свериться, что позиции по угрозам ИБ отражаются корректно.

10.4. Риски

Дальнейшим шагом анализа данных будет определение рисков ИБ, их анализ, оценка как следствие угроз ИБ.
Для этого необходимо кликнуть на угрозу ИБ, после чего откроется подраздел «Риски» (Рисунок 367).

Рисунок 367 Подраздел «Риски», карточка ИА

Для формирования перечня рисков ИБ выполнить следующие действия:

1. Нажать кнопку «Выбрать риски» и в открывшемся окне с перечнем рисков ИБ выбрать соответствующую позицию, проставив галочки в крайнем правом столбце (Рисунок 38).
2. При закрытии окна выбора рисков ИБ, выбранные позиции сохраняются.
3. Проделать шаг 1 и 2 для каждой угрозы ИБ для рассматриваемого ИА.

Для удаления или замены выбранных позиций рисков необходимо снова нажать кнопку «Выбрать риски», снять галочки с ранее выбранных позиций и проставить более подходящие. Далее закрыть окно и свериться, что данные отражаются корректно.

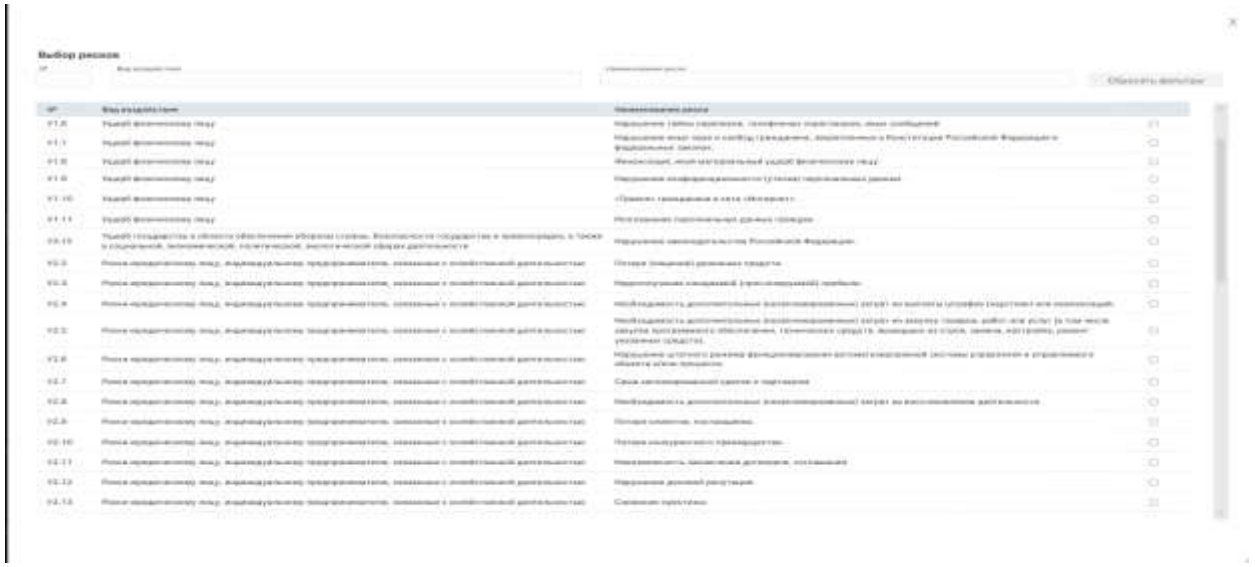


Рисунок 38 Окно перечня рисков ИБ

По окончании обработки каждой угрозы сформируется перечень рисков по рассматриваемому ИА.
Для заполнения характеристик выбранных рисков ИБ необходимо заполнять поочередно карточки самих рисков.

10.5. Карточка риска

Выбрать риск, кликнув на его наименование. В открывшемся окне (Рисунок 39) необходимо заполнить информацию:

- «Вероятность возникновения» и нажать на значок расчета оценки риска,
- «Затраты на мероприятия»,
- «Вероятный ущерб»,
- «Внешние факторы»,
- «Внутренние факторы»,
- «Описание мероприятий».

Для этого необходимо нажать на кнопку «Редактировать» в правом верхнем углу. По окончании ввода данных и их сохранения нажать кнопку «Выйти».

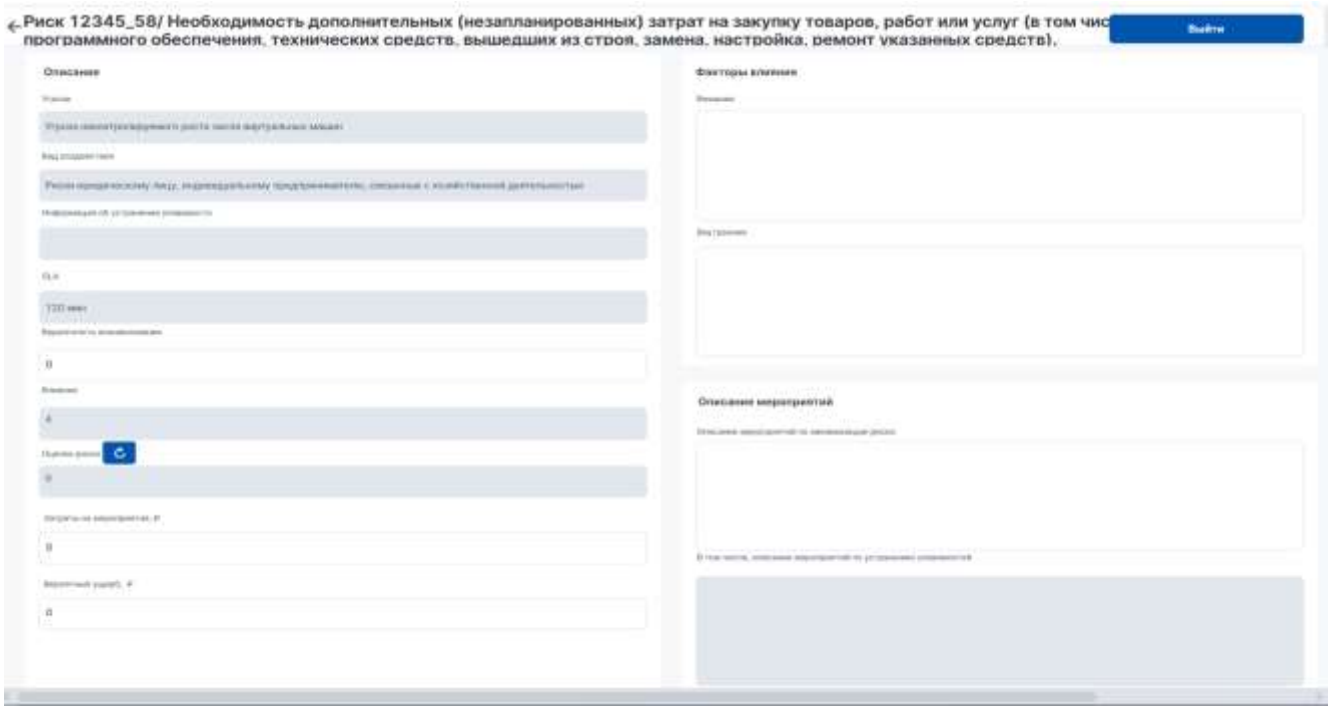


Рисунок 39 Карточка риска

При заполнении карточки риска можно наблюдать задвоение активных разделов в меню Реестр ИА и Реестр рисков это происходит, так как данные этих разделов взаимосвязаны.

Из карточки риска можно вернуться к списку всех карточек рисков в разделе Реестр ИА нажав на стрелку назад в системе. Или перейти в раздел Реестр рисков через кнопку в меню.

11. Раздел «Реестр рисков»

В разделе «Реестр рисков» (Рисунок 0) отражается перечень выявленных рисков ИБ в процессе анализа состояния ИА, затраты на проведения мероприятий для обеспечения ИБ и сумма ущерба.

Цвет индикатора риска указывает на категорию критичности, в которую попадает данный риск.

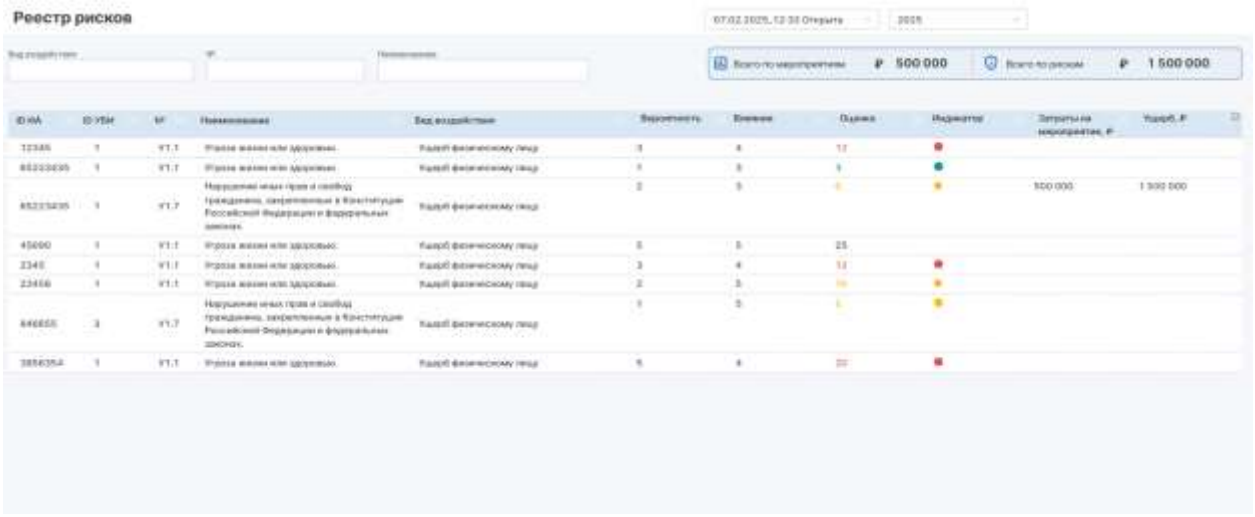


Рисунок 40 Окно Реестра рисков

Информацию о риске можно отредактировать, внеся соответствующие изменения в его карточке (п. 10.5). После внесения конечных корректировок рисков, сформированный реестр рисков ИБ требует согласования руководителем подразделения ИБ/ИТ и ИБ (владельцем процесса).

12. Раздел «Матрица рисков»

В разделе отражается матрица рисков.

Данные будут отображаться на матрице, если актуальная информация о рисках и угрозах подгружена и внесена в разделах **Аналитика**, **Реестр рисков**, **Реестр ИА** и обновлены данные ФСТЭК в разделе **Справочники** (Рисунок 371).

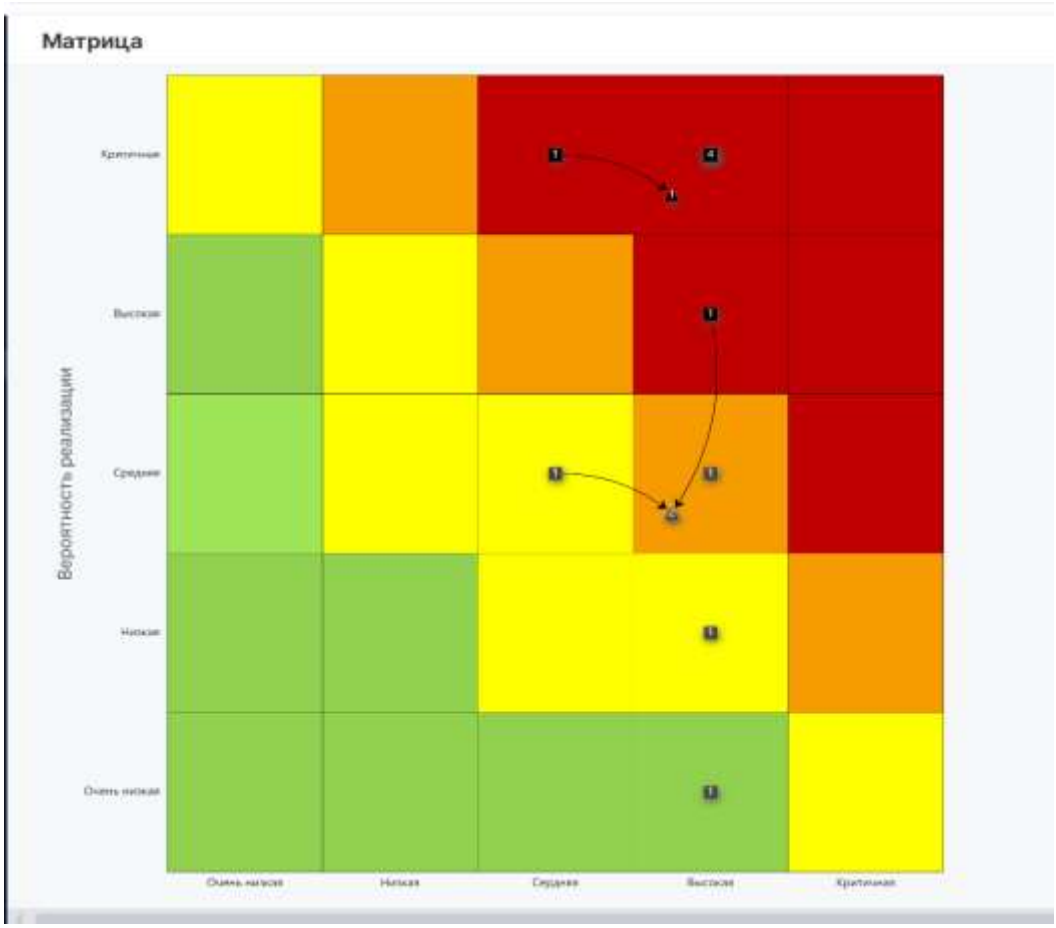


Рисунок 371 Матрица рисков

Доступна возможность фильтрации данных по признакам, выбираемым в соответствующих полях раскрывающихся списков.