



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

**Руководство пользователя**

## Оглавление

1.	Общие сведения.....	3
2.	Ролевая модель.....	4
3.	Работа с данными .....	5
3.1.	Справочники ФСТЭК.....	5
3.2.	Аналитические отчеты.....	5
3.2.1.	Версии аналитических отчетов.....	5
3.2.2.	Требования к заполнению версий аналитических отчетов данными.....	6
4.	Начало работы в программном комплексе.....	15
5.	Раздел «Администрирование» .....	17
5.1.	Открытие версий аналитических отчетов.....	17
5.2.	Открытие новых периодов.....	18
6.	Раздел «Аналитика» .....	19
6.1.	Загрузка аналитических отчетов.....	19
7.	Раздел «Справочники» .....	26
7.1.	Перечень угроз ФСТЭК.....	26
7.2.	Перечень обнаруженных уязвимостей ИА.....	27
7.3.	Оценка критичности информационного актива .....	28
8.	Раздел «Сводный отчет» .....	30
8.1.	График.....	30
8.2.	Отчет .....	31
8.3.	Анализ.....	31
9.	Раздел «Статистика прошлых периодов» .....	33
9.1.	График.....	33
9.2.	Отчет .....	34
9.3.	Анализ.....	34
10.	Раздел «Реестр ИА» .....	36
10.1.	Статистика кибератак.....	36
10.2.	Описание инцидентов.....	37
10.3.	Угрозы .....	38
10.4.	Риски .....	39
10.5.	Карточка риска .....	40
11.	Раздел «Реестр рисков» .....	42
12.	Раздел «Матрица рисков».....	43

## **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 установленным правам 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.**).

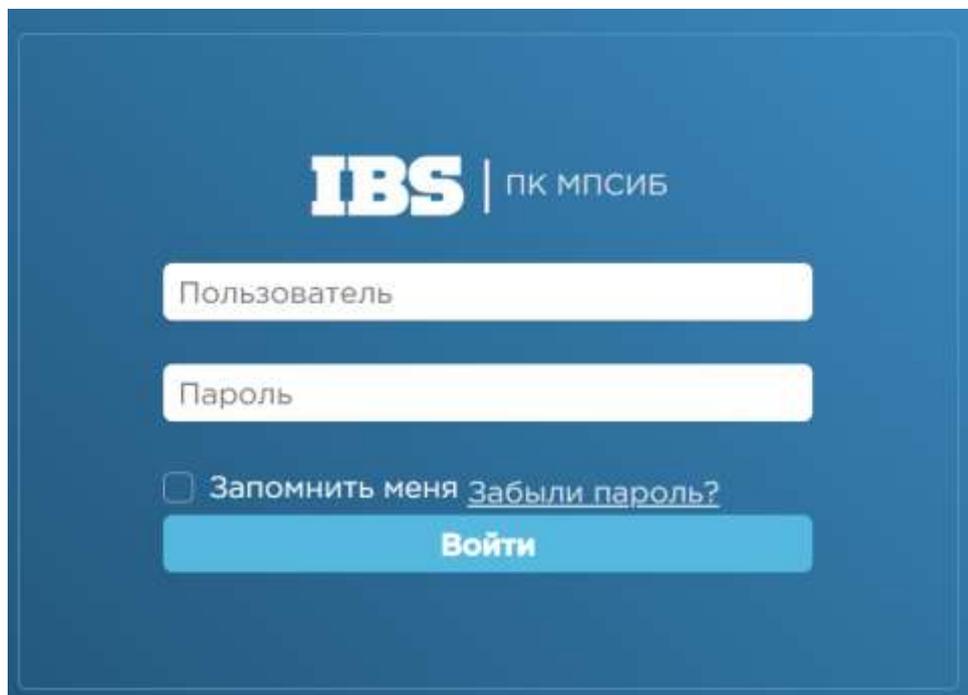


Рисунок 1 Окно аутентификации

Обратите внимание!

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

Количество попыток ввода пароля ограничено. 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.**).

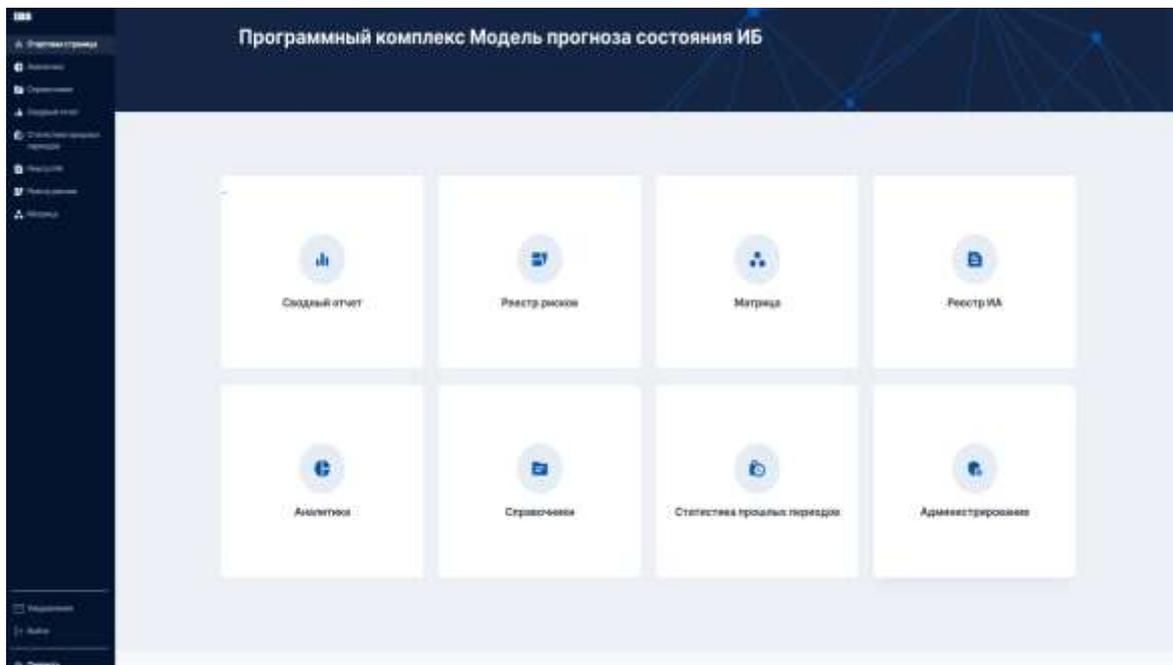


Рисунок 2 Стартовая страница

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).

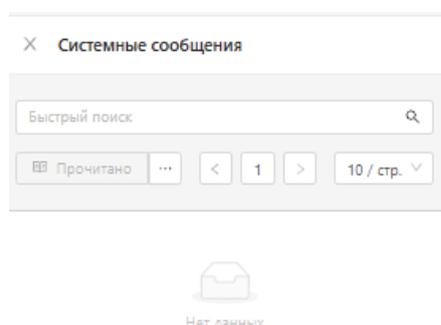


Рисунок 3 Окно системных сообщений

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 «Закрота».

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).

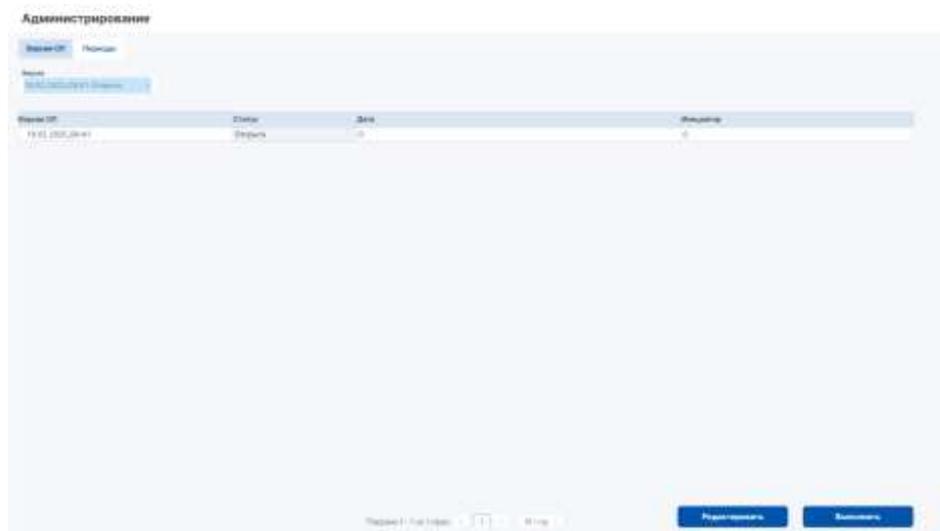


Рисунок 4 Окно выбора версии аналитического отчета

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**.

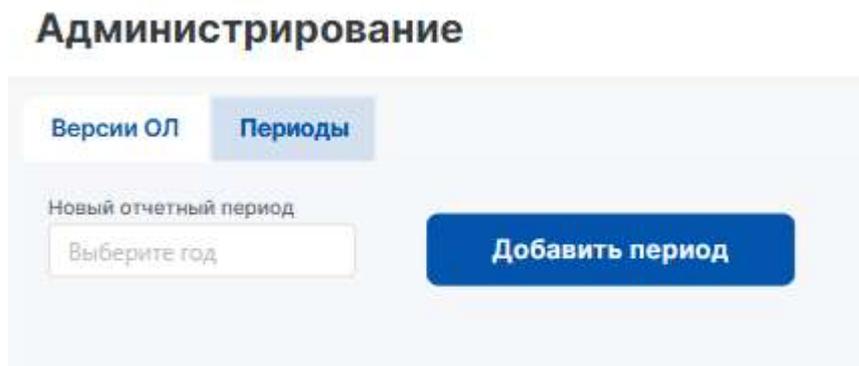


Рисунок 5 Раздел администратора, открытие нового периода

## 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 загруженный 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.

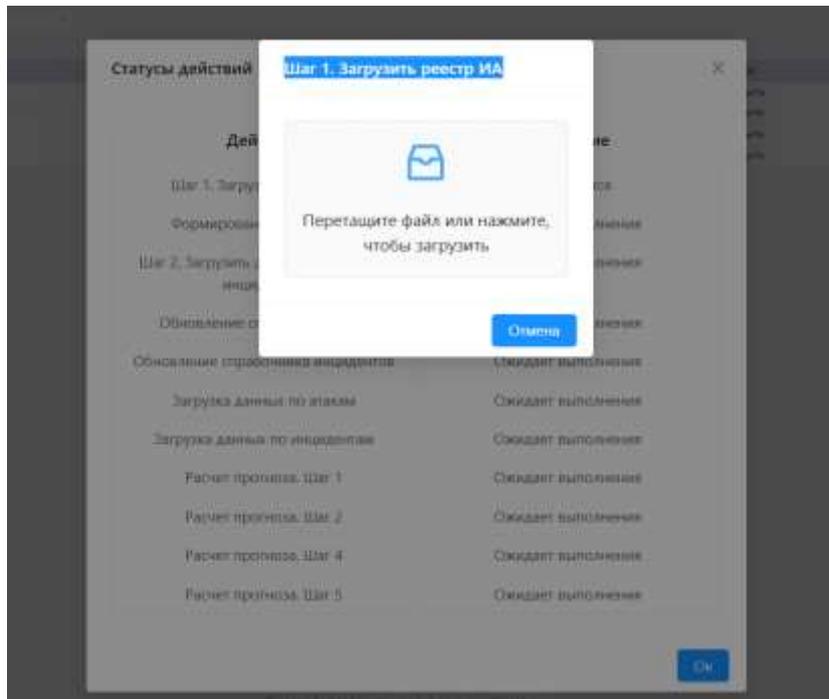


Рисунок 7 Шаг 1. Окно загрузки реестра ИА «Аналитика\_ИА»

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

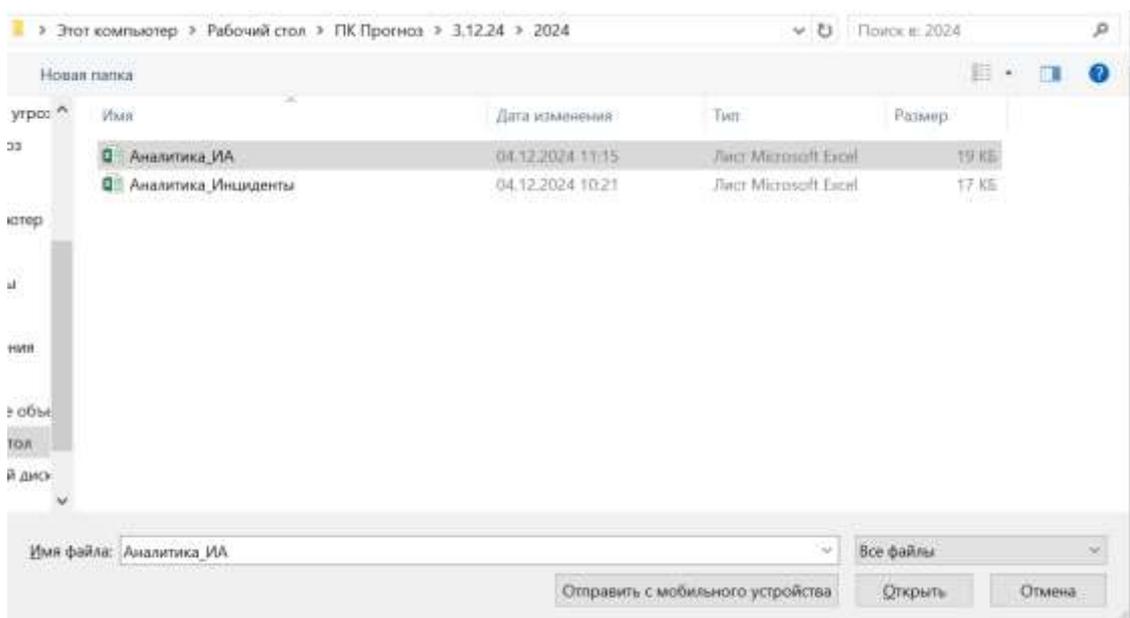


Рисунок 8 Папка с подготовленными к загрузке отчетами «Аналитика\_ИА», «Аналитика\_Инциденты». Выбор реестра ИА

- 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).

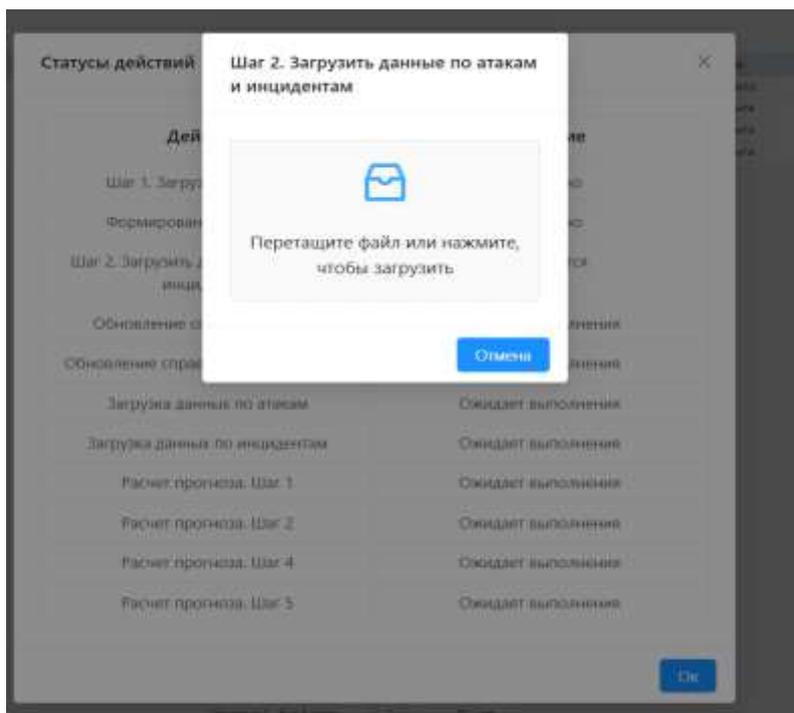


Рисунок 9 Шаг 2. Окно загрузки «Аналитика\_Инциденты»

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

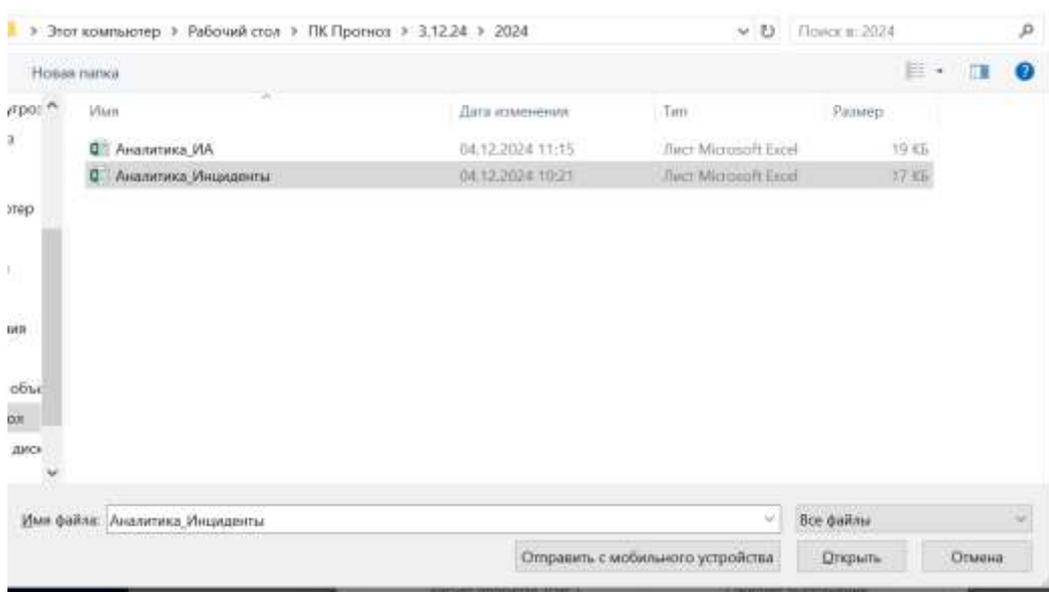


Рисунок 10 Папка с подготовленными к загрузке отчетами «Аналитика\_ИА», «Аналитика\_Инциденты». Выбор отчета по атакам и инцидентам

- 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*

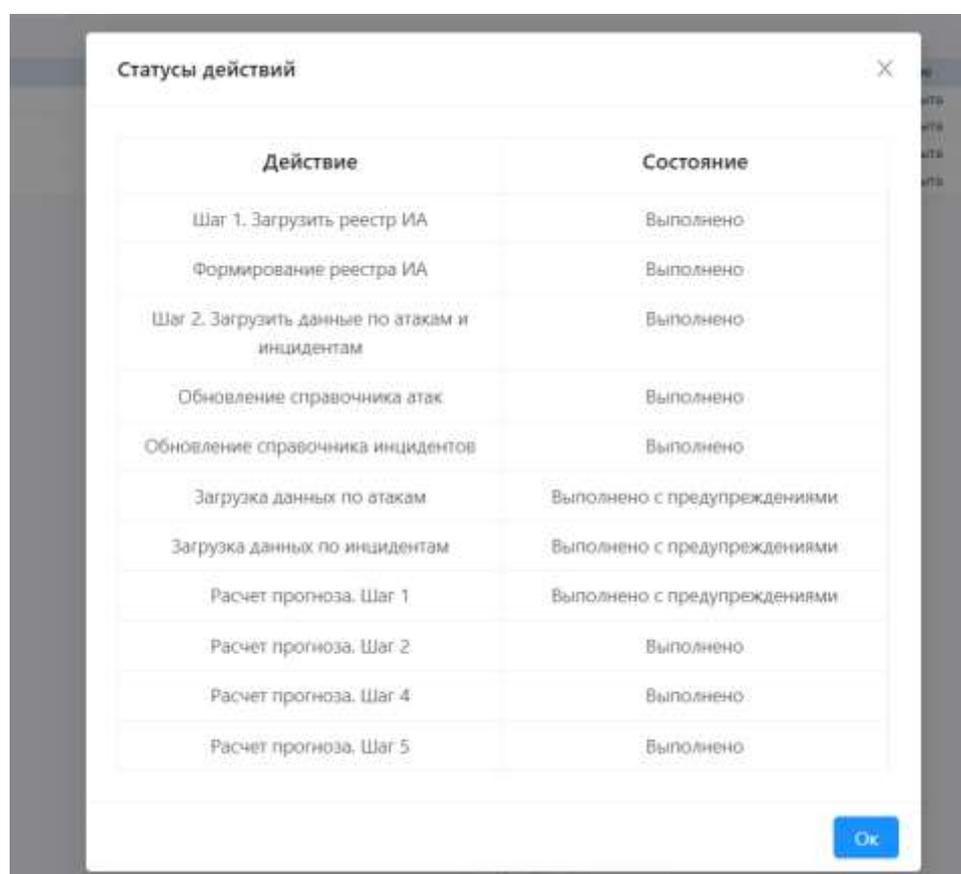
*Загрузка данных по инцидентам - Выполнено/Выполнено с предупреждением*

*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*



Действие	Состояние
Шаг 1. Загрузить реестр ИА	Выполнено
Формирование реестра ИА	Выполнено
Шаг 2. Загрузить данные по атакам и инцидентам	Выполнено
Обновление справочника атак	Выполнено
Обновление справочника инцидентов	Выполнено
Загрузка данных по атакам	Выполнено с предупреждениями
Загрузка данных по инцидентам	Выполнено с предупреждениями
Расчет прогноза. Шаг 1	Выполнено с предупреждениями
Расчет прогноза. Шаг 2	Выполнено
Расчет прогноза. Шаг 4	Выполнено
Расчет прогноза. Шаг 5	Выполнено

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.

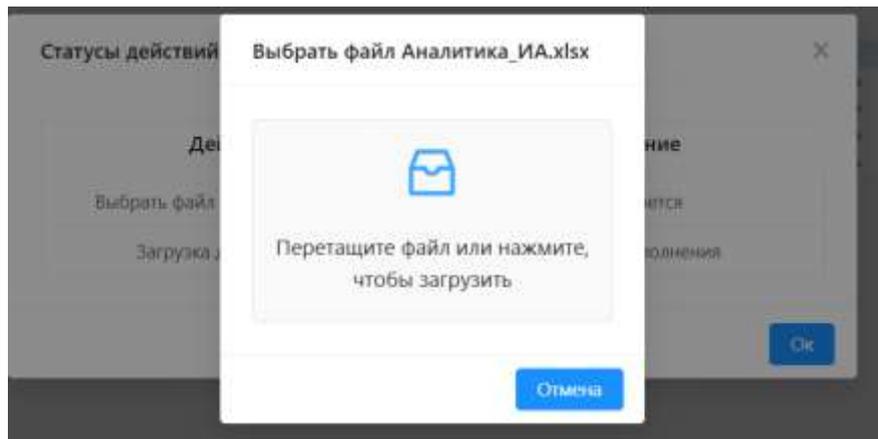


Рисунок 12 Открытие версии для анализа угроз ИБ

- Выбрать файл *Аналитика\_Инциденты* (Рисунок 13).

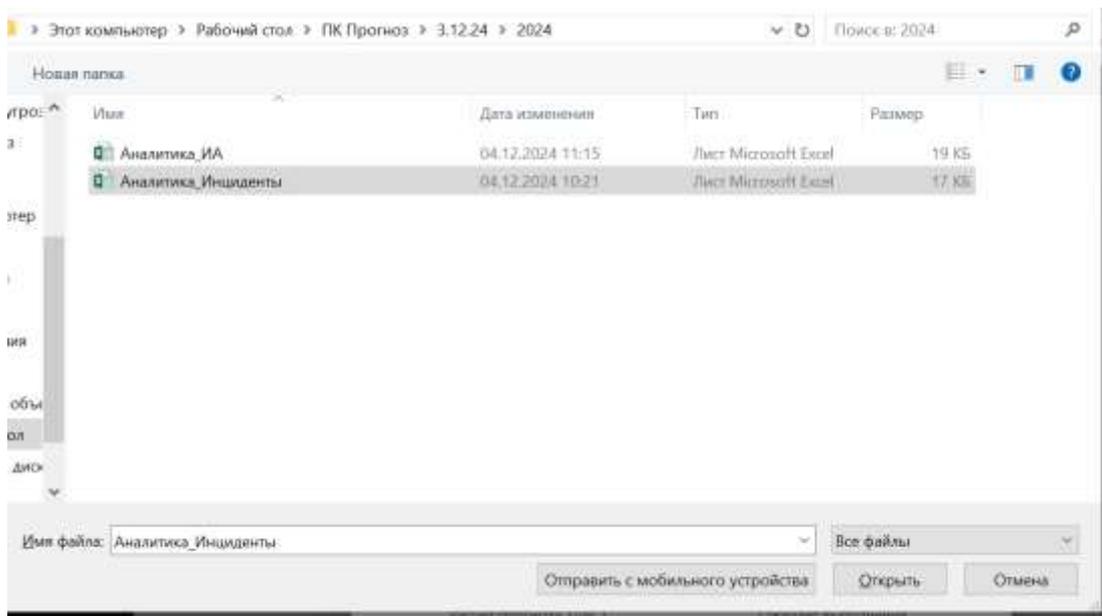


Рисунок 13 Папка с подготовленными к загрузке отчетами «Аналитика\_ИА», «Аналитика\_Инциденты»

- 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*



Год	Категория	Уникальный номер ИА	Наименование ИА	Источники информации	Тип ИА	Вид ИА	Вид инцидента	Атаки	Инциденты
2024	1-1	12345	ERP Газпром	Национальный ООИИ	АСУ	Другие АСУ	DoS-атака, или атака типа «человек в обмороке»	30	1
2024	1-1	12345	ERP Газпром	Национальный ООИИ	АСУ	Другие АСУ	Целевая атака	3	
2024	1-1	13456	ПТК EVICOM 1	Национальный ООИИ	АСУ	АСУП	Целевая атака	70	2
2024	1-1	13456	ПТК EVICOM 1	Национальный ООИИ	АСУ	АСУП	Фишинг	6	4
2024	1-1	45678	ПТК EVICOM 2	Национальный ООИИ	АСУ	АСУП	Криптоджекинг	2	
2024	1-1	56789	ПТК EVICOM 3	Не категоризируется	АСУ	АСУП	Фишинг	9	1
2024	1-1	56789	ПТК EVICOM 3	Не категоризируется	АСУ	АСУП	Атаки на цепочку поставок	4	
2024	1-1	60223435	Брау-П	Национальный ООИИ	ИС	Другие ИС (иные ИС)	DoS-атака	49	3
2024	1-1	45090	И-Рис	Национальный ООИИ	ИС	ПИС	DoS-атака	61	3
2024	1-1	2345	Терминал	Зональный ООИИ	ИС	ПИС	Спам-рассылка	27	2
2024	1-1	23456	Валтае	Зональный ООИИ	АСУ	АСУП	Внутренние угрозы	1	1
2024	1-1	840055	Тран-Д	Зональный ООИИ	АСУ	АСУП	DoS-атака	38	3
2024	1-1	237798	ДОП-Р	Национальный ООИИ	СДБ	СДБ 1	Созданные инциденты	21	1
2024	1-1	826543111	КДМ-Е	Не категоризируется	Серверные	Серверные 2	Спам-рассылка	21	2
2024	1-1	345522	ИТС-М	Национальный ООИИ	ИТС	ИТС 1	Целевая атака	58	4
2024	1-1	1122566	ИТС-С	Не категоризируется	ИТС	ИТС 2	Целевая атака	41	3
2024	1-1	37453	Львовичи-С	Национальный ООИИ	Серверные	Серверные 3	Внутренние угрозы	13	4
2024	1-1	3855354	МОС-М	Зональный ООИИ	АСУ	АСУСД	DoS-атака	52	2
2023	1-2	12345	ERP Газпром	Национальный ООИИ	АСУ	Другие АСУ	DoS-атака, или атака типа «человек в обмороке»	17	3
2023	1-2	12345	ERP Газпром	Национальный ООИИ	АСУ	Другие АСУ	Целевая атака	6	1
2023	1-2	13456	ПТК EVICOM 1	Национальный ООИИ	АСУ	АСУП	Фишинг	17	4
2023	1-2	45678	ПТК EVICOM 2	Национальный ООИИ	АСУ	АСУП	Криптоджекинг	7	
2023	1-2	56789	ПТК EVICOM 3	Не категоризируется	АСУ	АСУП	Атаки на цепочку поставок	6	
2023	1-2	7402433	Брауде	Национальный ООИИ	ИС	ИС(Д)	Атаки с использованием вредоносного программного обеспечения и вредоносного кода	31	1
2023	1-2	60223435	Брау-П	Национальный ООИИ	ИС	Другие ИС (иные ИС)	DoS-атака	39	3
2023	1-2	45090	И-Рис	Национальный ООИИ	ИС	ПИС	DoS-атака	51	3

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).

ID ИА	Наименование УИ	Описание	Влияние угрозы (оценочная информация)	Уровень воздействия информации	Критичность	Нарушение целостности	Нарушение доступности	Дата появления угрозы в ФСТЭК	Дата последнего обновления данных
1	Угроза целостности информации в граф. системе	Угроза целостности информации в граф. системе возникает в результате воздействия вредоносного ПО на граф. систему. Данное угроза обусловлена наличием уязвимостей в граф. системе. Реализация данной угрозы возможна при условии наличия у злоумышленника доступа к граф. системе.	Влияние угрозы: нарушение целостности информации.	Высокий уровень	1	1	1	2019-01-20	2019-02-03
2	Угроза целостности информации в граф. системе	Угроза целостности информации в граф. системе возникает в результате воздействия вредоносного ПО на граф. систему. Данное угроза обусловлена наличием уязвимостей в граф. системе. Реализация данной угрозы возможна при условии наличия у злоумышленника доступа к граф. системе.	Влияние угрозы: нарушение целостности информации.	Высокий уровень	1	1	1	2019-01-20	2019-02-03
3	Угроза целостности информации в граф. системе	Угроза целостности информации в граф. системе возникает в результате воздействия вредоносного ПО на граф. систему. Данное угроза обусловлена наличием уязвимостей в граф. системе. Реализация данной угрозы возможна при условии наличия у злоумышленника доступа к граф. системе.	Влияние угрозы: нарушение целостности информации.	Высокий уровень	1	1	1	2019-01-20	2019-02-03

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.

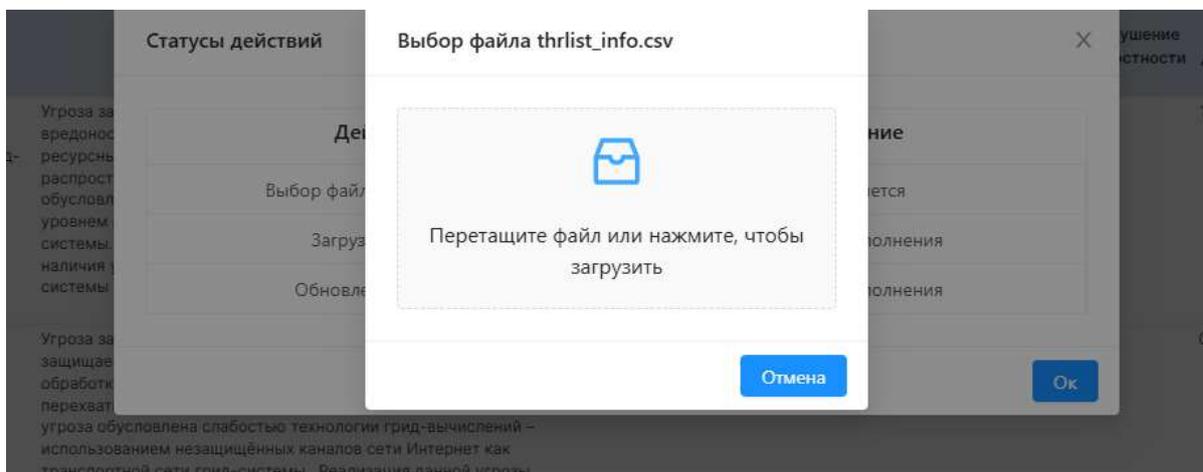


Рисунок 18 Окно загрузки справочника угроз ФСТЭК

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).

Справочники

Перечень угроз ФСТЭК | **Перечень обнаруженных уязвимостей ИА** | Оценка критичности информационных систем

Уязвимость ФСТЭК ID	Название ПО	Версия ПО	Наименование ОС	Уровень опасности уязвимости	Информация об устранении	Способ устранения
802-2019-00202	Apple Safari 525.00. Web Browser	до 2.02.2007	macOS	Высокий уровень опасности (Базовая оценка CVSS 2.0 составляет 7,2) Высокий уровень опасности (Базовая оценка CVSS 3.0 составляет 7,8)	Уязвимость устранена	Обновления программного обеспечения
802-2019-00201	Apple QuickTime	до 4.7.4	macOS	Средний уровень опасности (Базовая оценка CVSS 2.0 составляет 6,6) Высокий уровень опасности (Базовая оценка CVSS 3.0 составляет 6,8)	Уязвимость устранена	Обновления программного обеспечения
802-2019-00200	Apple QuickTime	до 4.7.4	macOS	Средний уровень опасности (Базовая оценка CVSS 2.0 составляет 6,6) Высокий уровень опасности (Базовая оценка CVSS 3.0 составляет 7,8)	Уязвимость устранена	Обновления программного обеспечения
802-2019-00199	Apple	от 2.0.0 до 2.0	Apple OS (Mac OS X)	Высокий уровень опасности (Базовая оценка CVSS 2.0 составляет 7,8) Высокий уровень опасности (Базовая оценка CVSS 3.0 составляет 7,3)	Уязвимость устранена	Обновления программного обеспечения
802-2019-00198	Apple	7.0	macOS	Критический уровень опасности (Базовая оценка CVSS 2.0 составляет 10) Критический уровень опасности (Базовая оценка CVSS 3.0 составляет 8,8)	Уязвимость устранена	Обновления программного обеспечения
802-2019-00196	Apple macOS OS	до 2.0.10	macOS	Высокий уровень опасности (Базовая оценка CVSS 2.0 составляет 7,2) Высокий уровень опасности (Базовая оценка CVSS 3.0 составляет 7,8)	Уязвимость устранена	Обновления программного обеспечения
802-2019-00111	Галерея ERP	8.0	Windows	Средний уровень опасности (Базовая оценка CVSS 2.0 составляет 4,3) Средний уровень опасности (Базовая оценка CVSS 3.0 составляет 6,4)	Уязвимость устранена	Организационные меры
802-2019-00112	Галерея ERP	8.0	Windows	Высокий уровень опасности (Базовая оценка CVSS 2.0 составляет 9) Высокий уровень опасности (Базовая оценка CVSS 3.0 составляет 8,8)	Уязвимость устранена	Обновления программного обеспечения
802-2019-00113	Галерея ERP	8.0	Windows	Средний уровень опасности (Базовая оценка CVSS 2.0 составляет 4,3) Средний уровень опасности (Базовая оценка CVSS 3.0 составляет 4,3)	Уязвимость устранена	Обновления программного обеспечения
802-2019-00114	Галерея ERP	8.0	Windows	Средний уровень опасности (Базовая оценка CVSS 2.0 составляет 4,3) Средний уровень опасности (Базовая оценка CVSS 3.0 составляет 5,3)	Уязвимость устранена	Обновления программного обеспечения
802-2019-00115	Галерея ERP	8.0	Windows	Высокий уровень опасности (Базовая оценка CVSS 2.0 составляет 7,7) Высокий уровень опасности (Базовая оценка CVSS 3.0 составляет 8)	Уязвимость устранена	Обновления программного обеспечения
802-2019-01049	Галерея ERP	8.0	Windows	Низкий уровень опасности (Базовая оценка CVSS 2.0 составляет 3,3) Средний уровень опасности (Базовая оценка CVSS 3.0 составляет 6,3)	Уязвимость устранена	Организационные меры

Фильтры: Поиск, Сортировка, Страницы (1), Информационная система, Информация об устранении, Скрыть неактивные

13.02.2023

Загрузить файл

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.

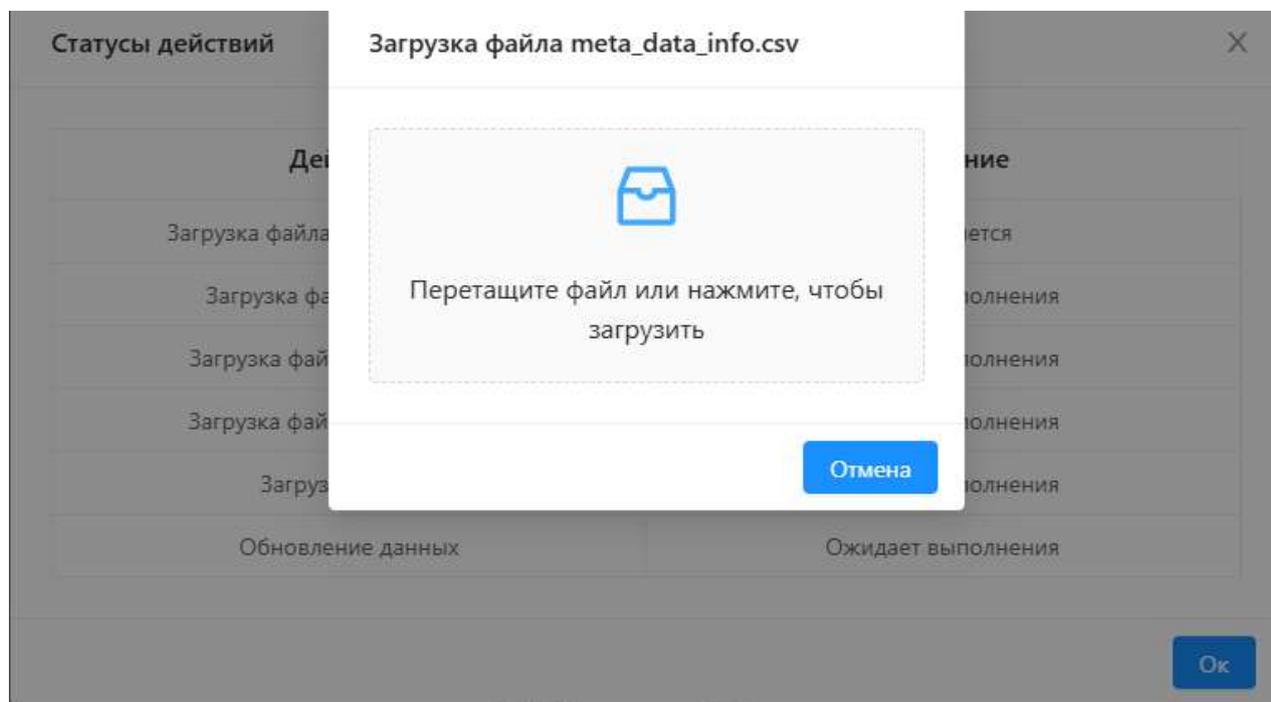


Рисунок 20 Окно загрузки справочника уязвимостей ФСТЭК

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).

Справочники

Перечень групп ССТЭИ    Перечень обнаруженных уязвимостей ИИ.    **Оценка критичности информационного актива**

ID актива	Актив организации	Конфиденциальность	Целостность	Доступность	Ценность актива
A.	Основные данные Информации (содержит информацию, необходимую для реализации ключевых или вида деятельности организации)	3	4	4	4
B.	Основные данные Информации (содержит персональные данные, которые определены особым образом, соответствующими национальным законам о неприкосновенности частной жизни)	3	3	1	4
C.	Основные данные Информации (содержит информацию стратегического характера в части достижения целей организации)	3	2	1	3
D.	Основные данные Информации (содержит информацию, обработка которой трудозатратна и/или связана с большими затратами на ее приобретение)	3	2	2	3
E.	Аппаратно-программный комплекс	0	3	2	3
F.	Носители информации	0	2	2	2
G.	Сеть	0	3	1	3
H.	Сотрудники	0	1	1	1
I.	Места функционирования организации	0	1	1	1

 [Редактировать](#)

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).

### Журнал изменения данных

Дата правки

День ▾

Выберите дату

Выберите дату

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

Наименование информационного ресурса	Вид воздействия	2022 факт		2023 факт		2024 факт		2025 прогноз		2026 прогноз		2027 прогноз	
		Атаки	Инциденты	Атаки	Инциденты	Атаки	Инциденты	Атаки	Инциденты	Атаки	Инциденты	Атаки	Инциденты
ТС ЭБР	Целевая атака	12	1			12	4	16	3	16	4	20	4
ТС ЭБР	Внутренние угрозы							3		3		3	
Архив	Атаки с использованием поданного обфускированного и анонимизированного источника	24	3	21	1								
Бере-П	DDoS-атака	41	5	38	3	45	3	60	5				
Восток	Внутренние угрозы	2	2	75	4	1	1	47	2	54	3	61	3
Лужанск	Ставарское ПО	13	5	63	1	23	2	61	4	58	4	68	5
Прин-Д	DDoS-атака	24	1	20	1	30	3	68	4	56	3	64	4
ДОП-Р	Социальная инженерия	20	3	15	1	21	1	43	3	31	3	37	3
ДОП-Р	SQL-инъекция (включая код SQL)	11	1	27	1								
ИМ/С	DDoS-атака	57	7	51	5	61	4	84	8	88	10	112	12
ИТС-М	Целевая атака	32	1	41	1	58	4	91	2	103	3	118	1
ИТС-С	Целевая атака	49	4	23	1	41	3	67	6	100	2	112	7
ИТС-Т	Целевая атака	5	1			6	4	8	2	7	3	5	3
ИТС-Т	Внутренние угрозы							7	1	7	1	4	1
КДМ-Е	КЭД (вебсайтовый скрэтчис или злоумышленник неавторизованный пользователь)	20	3	21	1								
КДМ-С	Ставарское ПО	21	3	26	1	21	2	75	2	88	3	97	3
Ленинград-С	Целевая атака			1				1		1		3	
Ленинград-С	Внутренние угрозы					23	4	18	2	15	2	22	3
МОС-М	Целевая атака			15	1			8		7		6	
МОС-М	DDoS-атака					22	2	10		18	1	21	1

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 категоризируется.

Внутри каждой такой группы ИА разбиваются на типы:

- АСУ;

- ИС;
- ЦОД;
- Серверная;
- ИТС.

Группы информационных активов	2022 факт		2023 факт		2024 факт		2025 прогноз		2026 прогноз		2027 прогноз	
	Атаки	Инциденты	Атаки	Инциденты	Атаки	Инциденты	Атаки	Инциденты	Атаки	Инциденты	Атаки	Инциденты
<b>Национальный ОКИН</b>	170	61	231	28	228	27	431	26	831	21	382	10
АСУ	21	12	64	12	108	19	133	28	107	21	178	21
ИС	123	18	121	8	108	8	163	18	88	18	112	14
ЦОД	23	8	61	10	21	1	28	2	21	3	27	2
Серверная	20	3	24	8	30	8	17	1	20	2	23	3
ИТС	22	5	41	1	38	8	82	1	105	2	118	3
<b>Не категоризованы</b>	141	18	27	2	30	18	118	18	272	11	207	24
ИС	8	2	8	8	8	8	2	8	8	8	8	8
ЦОД	18	3	8	8	7	1	23	3	20	8	20	8
АСУ	88	3	8	8	21	2	33	8	61	8	88	10
Серверная	21	2	28	2	21	2	28	2	25	2	27	2
ИТС	42	8	22	8	41	2	47	8	100	7	112	7
<b>Земельный ОКИН</b>	88	10	181	12	118	16	209	20	178	21	285	25
ЦОД	22	8	8	8	8	2	18	2	18	2	21	3
Серверная	2	2	8	8	12	2	8	2	8	2	11	2
ИТС	5	1	8	2	8	8	12	2	18	8	18	8
АСУ	28	3	128	18	21	8	118	8	128	18	188	11
ИС	12	2	83	2	27	2	11	4	52	8	58	5
<b>Общий итог</b>	344	33	385	28	308	27	437	44	470	48	520	34

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**.

ID	NAME	Статус (в ОКИН)	Тип атаки	Вид ИА	Вид инцидента	2023
4345	Гиринск	Национальный ОКИН	ИС	ИТС	Категория ИС	18

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 отражаются 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.

Статистика прошлых периодов

График Отчет Анализ

ИА	Кибератака	2020 факт		2021 факт		2022 факт		2023 факт		2024 факт	
		Атаки	Инциденты								
БРР Газетика	DDoS-атака, атака типа колосс в обслуживании	7	2	5	1	10	2	17	3	20	1
БРР Газетика	Целевая атака	3	1	27	10	14	5	5	1	5	
ПТК EVISON 1	Целевая атака	5	1							70	2
ПТК EVISON 1	Фишинг			21	17	12	3	17	4	6	4
ПТК EVISON 2	Кредитование	3	1	2	1	4	1	7		2	
ПТК EVISON 3	Фишинг									5	1
ПТК EVISON 3	Атаки на цепочку поставок	12	1	37	4	34	4	6		4	
Арсел	Атаки с использованием надписей обучения и искусственного интеллекта	3		16	3	24	3	31	1		
Банд-П	DDoS-атака	12	1	16	2	41	5	39	2	43	2
ИвГен	DDoS-атака	9	2	36	4	57	7	51	5	61	5
Гармакт	Спам-розыгрыш (П)	5		18	5	13	2	63	2	27	2
Бустан	Внутренние угрозы	18		32	1	2	2	75	4	1	1
Гран-Д	DDoS-атака			16	1	24	1	38	5	38	3
ДОП-Р	Социальный инженеринг	43		34	1	20	3	15	5	21	1
ДОП-Р	SQL-инъекция (внедрение кода SQL)			27	1	13	3	27	0		
КОМ-Е	XSS (инъекционный скриптинг) или применение несовместимых стандартов	16	1	23	5	20	3	21	6		
КОМ-С	Спам-розыгрыш (П)	12	1	47	3	21	2	56		21	2
ИТС-М	Целевая атака	13		104	1	32	1	41	1	56	4
ИТС-С	Целевая атака	10		121	5	45	4	23	8	41	2
Ливонские-С	Целевая атака							1			
Ливонские-С	Внутренние угрозы									33	4
МОС-М	Целевая атака							12	1		
МОС-М	DDoS-атака									32	2
ТС-БРР	Целевая атака			16	4	12	1			12	4
ТС-БРР	Внутренние угрозы	13	2								
ИТС-Т	Целевая атака					5	1			6	4
ИТС-Т	Внутренние угрозы	13	3	11	1						

Фильтры

Поиск

Сбросить фильтры

Показано 1 - 34 из 34 стр. 1 / 1 стр.

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 категоризируется.

Внутри каждой группы ИА разбиваются на типы:

- АСУ;
- ИС;
- ЦОД;

- Серверная;
- ИТС.

Статистика прошлых периодов

График Стат Анализ

ИА	2016 факт		2017 факт		2020 факт		2021 факт		2022 факт		2023 факт		2024 факт	
	Атаки	Инциденты												
Полочный ООМ	0	0	0	0	125	12	223	30	279	40	292	38	324	
АСУ	0	0	0	0	30	0	77	33	71	15	64	52	108	
ИТС	0	0	0	0	24	3	70	0	123	19	121	0	109	
ЦОД	0	0	0	0	43	0	81	2	33	0	40	10	31	
Сетевые	0	0	0	0	16	1	23	2	20	3	24	0	33	
ИТС	0	0	0	0	12	0	104	1	32	1	41	1	50	
Не классифицируется	0	0	0	0	87	0	205	18	141	14	87	0	90	
ИТС	0	0	0	0	0	0	0	0	0	0	0	0	0	
ЦОД	0	0	0	0	12	0	32	2	18	3	0	0	7	
АСУ	0	0	0	0	24	1	55	0	49	5	0	0	31	
Сетевые	0	0	0	0	12	1	87	2	31	2	38	0	21	
ИТС	0	0	0	0	18	0	121	0	45	4	22	0	41	
Значный ООМ	0	0	0	0	38	3	109	11	68	12	101	12	118	
ЦОД	0	0	0	0	0	0	27	0	22	0	0	0	0	
Сетевые	0	0	0	0	0	0	5	1	2	2	0	0	12	
Серверный	0	0	0	0	0	0	0	0	0	0	0	0	0	
Серверный S	0	0	0	0	0	0	5	1	2	2	0	0	12	
ИТС	0	0	0	0	12	3	11	1	5	1	0	0	0	
АСУ	0	0	0	0	16	0	48	2	28	2	128	10	71	
ИТС	0	0	0	0	1	0	18	0	12	2	83	0	27	
Общий итог	0	0	0	0	118	13	370	40	244	33	285	38	286	

Фильтры

ИТС

Значный ООМ

ИТС

Скрыть фильтры

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».

ИА	ИАМ	Описание к ИАМ	Тип атаки	Вид ИА	Вид инцидента	Атаки	Инциденты
ИТС	Горюхи	Значный ООМ	ИТС	ИТС	Сетевые ИА	18	0

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).**

№	Наименование актива	ID	Статус в ОДН	Тип	Вид ИА	Вид в эксплуатации	Вывод из эксплуатации
1	БФР Газетная	12345	Нормальный ОКН	АСУ	Другие АСУ	01.2016	01.2023
2	ПТК ЕУКСОН 1	13456	Нормальный ОКН	АСУ	АСУТП	03.2018	03.2019
3	ПТК ЕУКСОН 2	45678	Нормальный ОКН	АСУ	АСУТП	03.2018	03.2019
4	ПТК ЕУКСОН 3	56789	Не категоризован	АСУ	АСУТП	05.2019	03.2020
5	МГЭ	45690	Нормальный ОКН	ИС	ГИС	05.2013	01.2020
6	Губернет	2345	Зачесный ОКН	ИС	ГИС	08.2020	08.2020
7	Вестел	23456	Зачесный ОКН	АСУ	АСУТП	02.2020	02.2020
8	Три-Д	646955	Зачесный ОКН	АСУ	АСУТП	02.2020	02.2020
9	ДЭП Р	537769	Нормальный ОКН	ЦОД	ЦОД 1	01.2010	01.2020
10	КЭМ-С	820543111	Не категоризован	Серверная	Серверная Э	08.2010	06.2020
11	ИТС-М	345622	Нормальный ОКН	ИТС	ИТС 1	01.2010	01.2020
12	ИТС-С	1122888	Не категоризован	ИТС	ИТС 2	01.2010	01.2020
13	Линкстек-С	37883	Нормальный ОКН	Серверная	Серверная Э	01.2020	01.2024
14	МЭС-М	3899334	Зачесный ОКН	АСУ	АСУЭД	01.2023	01.2024
15	ТСВР	445622870	Не категоризован	АСУ	АСУП	01.2018	06.2020
16	ИТС-Т	88979281	Зачесный ОКН	ИТС	ИТС 3	01.2020	01.2020
17	Скарелка Б	10000010	Зачесный ОКН	Серверная	Серверная Э	01.2021	01.2024
18	ЦОД 1	11001200	Не категоризован	ЦОД	ЦОД 1	01.2010	01.2020
19	ЦОД 2	11003490	Зачесный ОКН	ЦОД	ЦОД 2	01.2021	01.2020
20	ВМАТС ФНС	11000011	Нормальный ОКН	АСУ	АСУТП	05.2020	03.2019

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. Статистика 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 введенных данных необходимо нажать кнопку «Выйти».

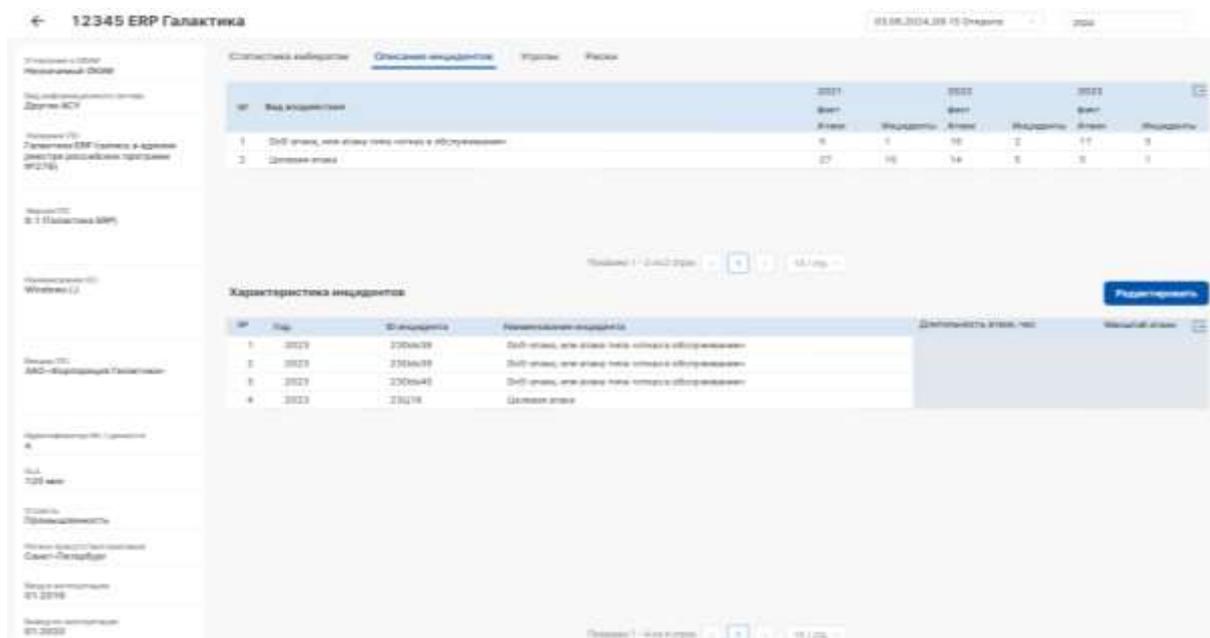


Рисунок 345 Карточка ИА, Описание инцидентов

### 10.3. Угрозы

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

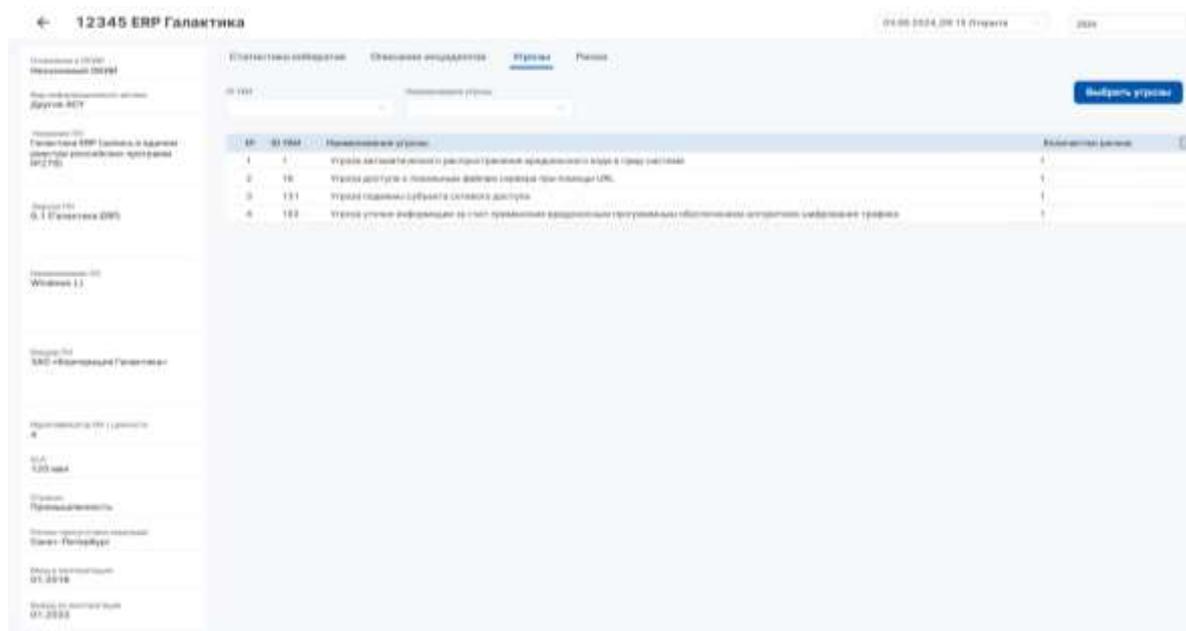


Рисунок 356 Определение угроз ИБ в карточке ИА

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. Прodelать 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.

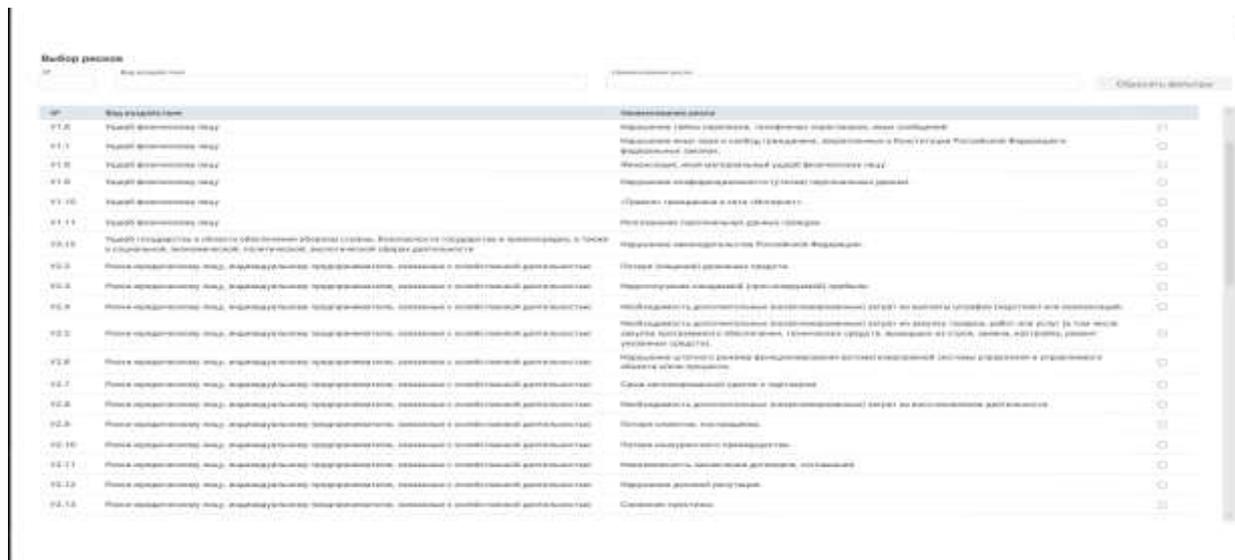


Рисунок 38 Окно перечня рисков ИБ

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».

← Риск 12345\_58 / Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств), Выйти

<p><b>Описание</b></p> <p>Имя:</p> <p>Услуга по техническому обслуживанию серверов в серверной комнате</p> <p>Инициатор:</p> <p>Управляющему ИТД, подразделению поддержки, связанное с хозяйственной деятельностью</p> <p>Информация об уровне риска:</p> <p>С/к:</p> <p>УЗП (кв):</p> <p>Временной период:</p> <p>0</p> <p>Классификация:</p> <p>4</p> <p>Статус риска:</p> <p>0</p> <p>Нормативная стоимость, Р:</p> <p>0</p> <p>Фактический ущерб, Р:</p> <p>0</p>	<p><b>Факторы влияния</b></p> <p>Пояснение:</p> <p>Инструменты:</p> <p>Описание мероприятий:</p> <p>Описание мероприятий по снижению риска:</p> <p>0 на время, включая мероприятия по управлению рисками</p>
---	--

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.

ID ИА	ID ИБ	ИД	Наименование	Исходдействие	Вероятность	Влияние	Сумма	Индикатор	Затраты на мероприятия, ₽	Ущерб, ₽
12385	1	У1.1	Угроза жизни или здоровья	Разруб физическому лицу	3	4	12	🔴		
8523205	1	У1.1	Угроза жизни или здоровья	Разруб физическому лицу	3	3	9	🟢		
8523205	1	У1.2	Нарушение прав граждан Российской Федерации и иностранных граждан	Разруб физическому лицу	2	5	10	🟡	500 000	1 500 000
45690	1	У1.1	Угроза жизни или здоровья	Разруб физическому лицу	3	5	15	🔴		
2345	1	У1.1	Угроза жизни или здоровья	Разруб физическому лицу	2	4	8	🔴		
23456	1	У1.1	Угроза жизни или здоровья	Разруб физическому лицу	2	3	6	🟡		
846855	3	У1.2	Нарушение прав граждан Российской Федерации и иностранных граждан	Разруб физическому лицу	1	5	5	🟡		
3856354	1	У1.1	Угроза жизни или здоровья	Разруб физическому лицу	3	4	12	🔴		

Рисунок 40 Окно Реестра рисков

Информацию о риске можно отредактировать, внося 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).

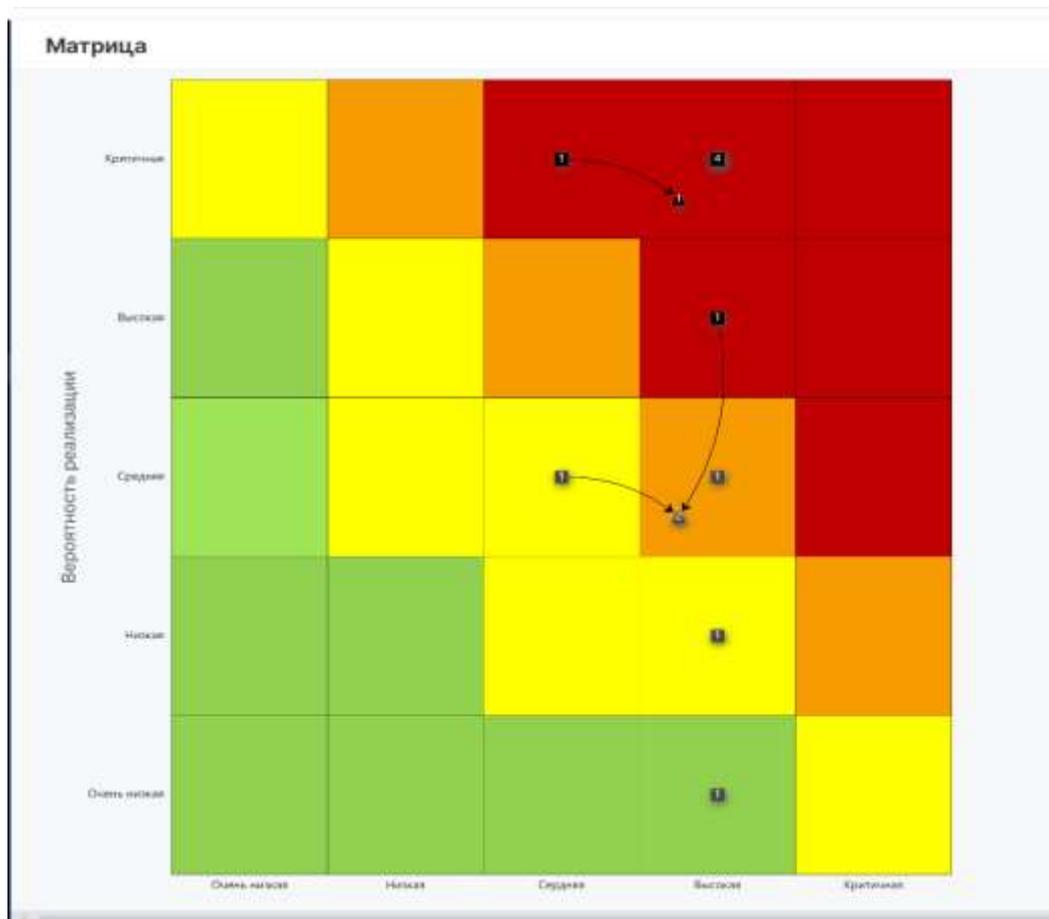


Рисунок 371 Матрица рисков

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