

**«СИСТЕМА АВТОМАТИЗАЦИИ  
ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ»**

**Управление компьютерными инцидентами ИБ и нештатными ситуациями**

Руководство пользователя

# Содержание

<b>1. Общие положения.....</b>	<b>4</b>
1.1. Термины, определения, сокращения.....	4
1.2. Общие сведения.....	4
1.3. Назначение модуля.....	4
<b>2. Описание ролевой модели.....</b>	<b>5</b>
<b>3. Начало работы с модулем.....</b>	<b>6</b>
<b>4. Описание интерфейсов пользователей.....</b>	<b>7</b>
4.1. Рабочая область Эксперта УКИНС.....	7
4.2. Рабочая область Ответственного за инцидент.....	12
4.3. Рабочая область Руководства САОБ.....	17
4.4. Рабочая область Участника ГРИИБ.....	23
4.5. Рабочая область Оператора-диспетчера.....	26
<b>5. Сценарии работы пользователей.....</b>	<b>27</b>
5.1. Работа со справочниками.....	27
5.1.1. Справочник «Классификация инцидентов».....	27
5.1.2. Справочник «Виды инцидента».....	31
5.1.3. Справочник «Реагирование на инциденты ИБ».....	32
5.1.4. Справочник «Время реагирования».....	36
5.1.5. Справочник «Угрозы».....	36
5.1.6. Справочник «Категории нарушений».....	38
5.1.7. Справочник «Правила корреляции».....	38
5.1.8. Справочник «Виды нештатной ситуации».....	40
5.1.9. Справочник «Реагирование на нештатные ситуации».....	43
5.2. Формирование группы реагирования на инциденты ИБ.....	45
5.2.1. Добавление участника ГРИИБ.....	46
5.2.2. Редактирование информации об участнике ГРИИБ.....	46
5.3. Управление событиями информационной безопасности.....	47
5.3.1. Создание записи о событии информационной безопасности.....	48
5.3.2. Редактирование записи о событии информационной безопасности.....	50
5.3.3. Формирование отчетных форм о событии информационной безопасности.....	51
5.3.4. Обработка события информационной безопасности.....	51
5.3.5. Групповая обработка событий информационной безопасности.....	53

5.4. Управление инцидентами информационной безопасности.....	54
5.4.1. Создание записи об инциденте информационной безопасности.....	55
5.4.2. Редактирование записи об инциденте информационной безопасности.....	57
5.4.3. Формирование отчетных форм об инциденте информационной безопасности.....	61
5.4.4. Перевод инцидента в статус «Не является инцидентом».....	61
5.4.5. Формирование плана реагирования на инцидент информационной безопасности.....	63
5.5. Мониторинг и контроль управления инцидентами ИБ.....	75
5.6. Управление нештатными ситуациями.....	76
5.6.1. Создание записи о нештатной ситуации.....	76
5.6.2. Редактирование записи о нештатной ситуации.....	77
5.6.3. Формирование плана реагирования на нештатную ситуацию.....	80
5.6.4. Работа с задачами по реагированию и расследованию нештатной ситуации.....	80
5.6.5. Загрузка документов.....	80
5.6.6. Завершение реагирования и расследования нештатной ситуации.....	81
5.6.7. Завершение обработки нештатной ситуации.....	81
5.6.8. Возврат нештатной ситуации в работу.....	82

# **1. Общие положения**

## **1.1. Термины, определения, сокращения**

В настоящем руководстве использованы следующие сокращения:

ГРИИБ – группа реагирования на инциденты ИБ.

ИБ – информационная безопасность.

САОБ – система автоматизации обеспечения безопасности.

## **1.2. Общие сведения**

Настоящее руководство пользователя устанавливает порядок работы с модулем «Управление компьютерными инцидентами ИБ и нештатными ситуациями» (далее – модуль УКИНС).

Модуль УКИНС предназначен для автоматизации процесса управления инцидентами ИБ:

- регистрации, обработки и учета событий, инцидентов ИБ и нештатных ситуаций;
- выгрузки отчетных форм по событиям и инцидентам ИБ.

## **1.3. Назначение модуля**

Модуль УКИНС предназначен для автоматизации процедур регистрации инцидентов ИБ, проведения расследования и (или) реагирования на инциденты ИБ, проведения оценки и анализа инцидента ИБ, закрытия инцидента ИБ по итогам проведения работ в эксплуатирующей организации, формирования отчетных форм по инцидентам и событиям ИБ.

Модуль УКИНС предназначен для выполнения следующих функций:

- формирование группы реагирования на инциденты ИБ;
- регистрация и учёт событий и инцидентов ИБ;
- обработка событий и инцидентов ИБ, управление процессом реагирования и расследования инцидентов ИБ;
- выполнение задач по реагированию и расследованию инцидентов ИБ;
- формирование типовых сценариев по реагированию и расследованию инцидентов ИБ;
- анализ статистических данных.

## 2. Описание ролевой модели

В модуле УКИНС предусмотрены следующие роли пользователей:

- Эксперт УКИНС;
- Участник ГРИИБ;
- Ответственный за инцидент ИБ;
- Руководство САОБ;
- Оператор-диспетчер ИБ.

Участие ролей пользователей в выполнении функций модуля УКИНС приведено в [Таблица 1](#).

Табл. 1. Участие ролей пользователей в выполнении функций модуля УКИНС

Участие в функциях	Роль				
	Эксперт УКИНС	Участник ГРИИБ	Ответственный за инцидент ИБ	Руководство САОБ	Оператор-диспетчер ИБ
Формирование группы реагирования на инциденты ИБ	+	-	-	+	-
Регистрация и учёт событий, инцидентов ИБ и нештатных ситуаций	-	-	+	+	+
Обработка событий, инцидентов ИБ и нештатных ситуаций, управление процессом реагирования и расследования инцидентов ИБ	-	-	+	+	-
Выполнение задач по реагированию и расследованию инцидентов ИБ и нештатных ситуаций	-	+	-	-	-
Формирование типовых сценариев по реагированию и расследованию инцидентов ИБ и нештатных ситуаций	+	-	+	+	-
Анализ статистических данных	-	-	-	+	-

### 3. Начало работы с модулем

Для начала работы с модулем УКИНС выполните следующие действия:

1. Откройте браузер.
2. В адресной строке браузера укажите адрес, по которому расположен Ваш экземпляр платформы.
3. На странице аутентификации введите логин и пароль Вашей учетной записи.
4. Нажмите кнопку «Войти». Откроется рабочая область, соответствующая роли, в которой находится пользователь.

## 4. Описание интерфейсов пользователей

### 4.1. Рабочая область Эксперта УКИНС

Для перехода к рабочей области нажать на логотип в левом верхнем углу.

Рабочая область пользователя с ролью «Эксперт УКИНС» ([Рисунок 1](#)) предназначена для отображения основной статистической информации о зарегистрированных событиях и инцидентах.

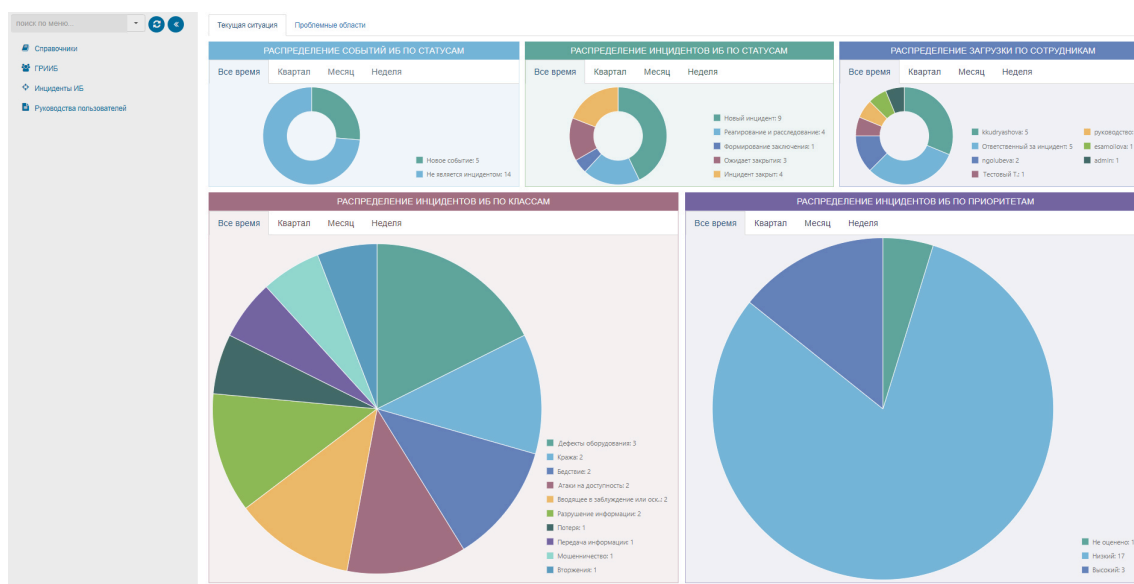


Рис. 1. Рабочая область Эксперта УКИНС

Рабочая область состоит из следующих информационных панелей:

#### 1. Информационная панель «Текущая ситуация» ([Рисунок 2](#)).

Для того чтобы перейти к информационной панели, необходимо на стартовой странице пользователя перейти на вкладку «Текущая ситуация».

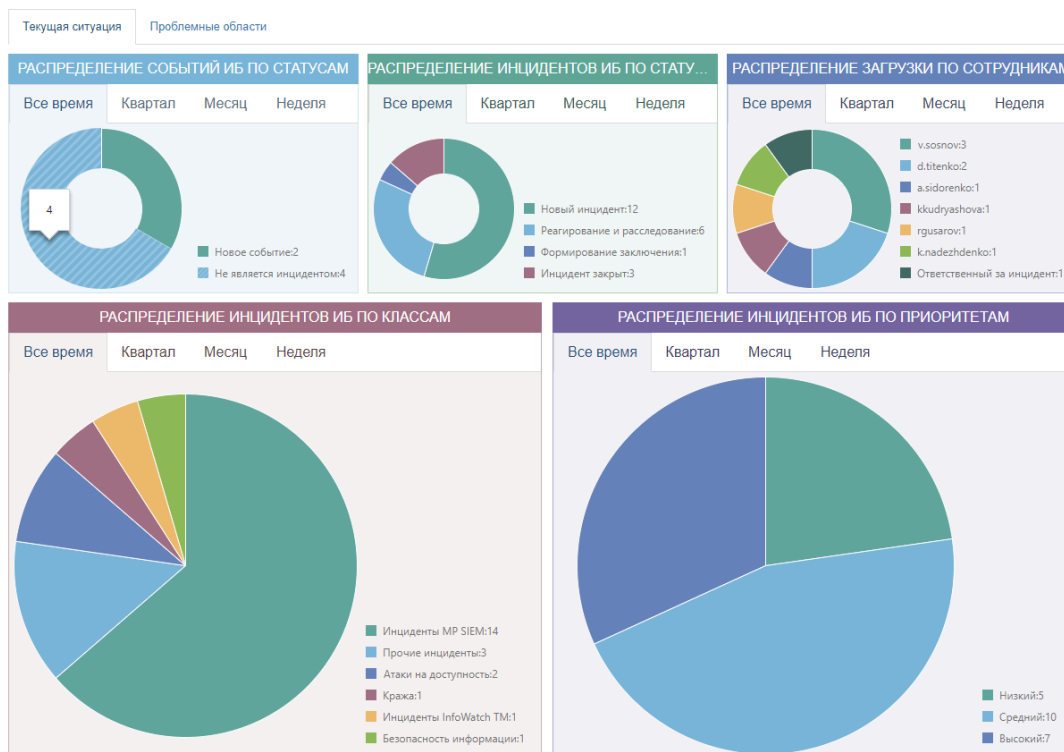


Рис. 2. Информационная панель «Текущая ситуация»

Информационная панель отображает сведения о распределении зарегистрированных событий и инцидентов ИБ по статусам, инцидентов по ответственным, а также по классам и приоритетам в различных разрезах временных интервалов.

## 2. Информационная панель «Проблемные области» (Рисунок 3).

Для того чтобы перейти к информационной панели, необходимо на стартовой странице пользователя перейти на вкладку «Проблемные области».



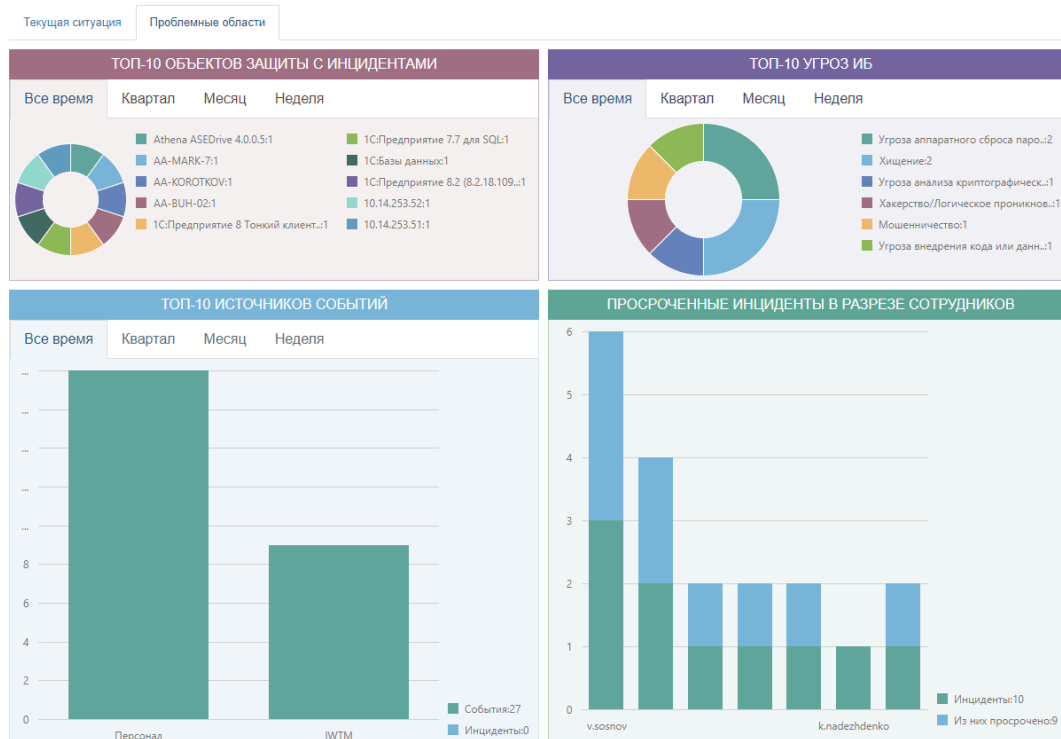


Рис. 3. Информационная панель «Проблемные области»

Информационная панель отображает сведения о проблемных объектах защиты, частых угрозах ИБ и источниках событий в различных разрезах временных интервалов. Также на панели отображается статистика распределения просроченных инцидентов по ответственным.

### 3. Информационная панель «Справочники» (Рисунок 4).

Для того чтобы перейти к информационной панели, необходимо в боковом меню пользователя выбрать пункт «Справочники».

Справочники УИ

Классификация инцидентов | Сценарии реагирования | Угрозы | Виды инцидентов | Категории нарушений | Правила корреляции | Времени реагирования

Подклассы инцидента

Наименование	Приоритет	Сценарий	
Q	Q	Q	
нет значения			
Спам	Низкий	тестовый сценарий	✗
Навязчивые агрессивные действия	Низкий	Сетевые мероприятия	✗
Несанкционированная сетевая активность			✗
Атаки на доступность			
DoS (Deny of Service – отказ в обслуживании)	Средний	Мероприятия по антивирусной защите	✗
DDoS (Distributed Deny of Service – распределенный отказ в обслуживании)	Низкий		✗
Саботаж	Низкий		✗
Бедствие			
Бедствие	Высокий		✗
Безопасность информации			
Несанкционированный доступ к информации. Разглашение	Высокий	Мероприятия по реагированию на несанкционированный доступ	✗
Несанкционированная модификация информации. Разрушение	Высокий	Мероприятия по реагированию на несанкционированный доступ	✗
Безопасность контента (Продолжение на следующей странице)			

Всего записей: 137 | 1 | из 14

Рис. 4. Информационная панель «Справочники»

Информационная панель содержит вкладки с данными справочников Модуля УКИНС (списки классов и подклассов инцидентов, типовые сценарии реагирования, перечень видов инцидентов, угроз ИБ, правил корреляции и таблицу времени реагирования в зависимости от приоритета инцидента).

#### 4. Информационная панель «ГРИИБ» (Рисунок 5).

Для того чтобы перейти к информационной панели, необходимо в боковом меню пользователя выбрать пункт «ГРИИБ».

Группа реагирования на инциденты ИБ и нештатные ситуации

Руководитель ГРИИБ

Колпаков М.С., Аналитик, Новая организация

Работники\*

+ ↺ 🔍 Искать.

Фамилия И.О.	Должность	email	
Кудряшова К.А.	Начальник отдела	kkudryashova@ussc.ru	✖

5 10 20 50 < 1 из 1 >

\*Пользователи, добавленные в группу реагирования, могут быть назначены ответственными за выполнения мероприятий по реагированию и расследованию

Сохранить

Рис. 5. Информационная панель «ГРИИБ»

Информационная панель содержит список работников, входящих в группу реагирования на инцидент ИБ. Двойной щелчок левой кнопкой мыши по записи работника открывает карточку с подробной информацией о работнике.

#### 5. Информационная панель «Реестр инцидентов ИБ» (Рисунок 6).

Для того чтобы перейти к информационной панели, необходимо в боковом меню пользователя выбрать пункт «Инциденты ИБ».

Реестр инцидентов ИБ

НовыеВ работеОбработанные

Новый инцидент

Дата и время возникновения...

Номер

Наименование

Подкласс

Приоритет

Источник

Ответственный

Q

Q

Q

Q

Q

Q

08.11.2021 15:54:20

08.25.08/ИИБ/4

Вирус на ПК с КТ

Компьютерный вирус

Средний

Персонал

ozib

03.11.2021 10:25:22

08.25.08/ИИБ/2

Кража носителя данных

Кража носителя данных

Низкий

Персонал

Кудряшова К.

5102050

Всего записей: 2

1

из 1

Не является инцидентом

Информационная панель содержит список инструкций по модулям системы доступных для загрузки.

ИНСТРУКЦИИ ПО МОДУЛЯМ		
Наименование	Инструкция	Дата обновления
Руководство пользователя УКИНС	САОБ_УКИНС.pdf	15.08.2022
Руководство пользователя модуль взаимодействия с НКЦКИ	САОБ_Модуль взаимодействия с НКЦКИ.pdf	15.08.2022
Руководство пользователя УДИБ	САОБ_УДИБ.pdf	15.08.2022
Руководство пользователя УИВИБ	САОБ_УИВИБ.pdf	15.08.2022
Руководство пользователя УКСБ	САОБ_УКСБ.pdf	15.08.2022
Руководство пользователя УМОИБ	САОБ_УМОИБ.pdf	15.08.2022
Руководство пользователя УУУИБ	САОБ_УУУИБ.pdf	15.08.2022
Руководство пользователя УКО	САОБ_УКО.pdf	15.08.2022

Рис. 7. Информационная панель «Руководства пользователей»

## 4.2. Рабочая область Ответственного за инцидент

Для перехода к рабочей области нажать на логотип в левом верхнем углу.

Рабочая область пользователя с ролью «Ответственный за инцидент ИБ» (Рисунок 8) предназначена для отображения основной информации о зарегистрированных событиях и инцидентах, назначенных на данного пользователя.

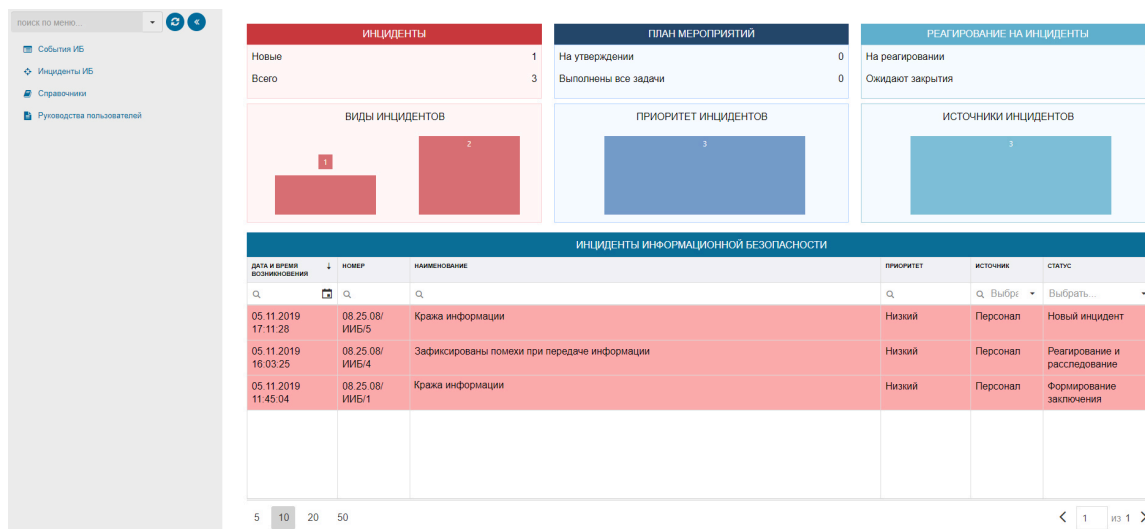


Рис. 8. Рабочая область Ответственного за инцидент

Рабочая область состоит из следующих виджетов:

1. Виджет «Инциденты информационной безопасности» (Рисунок 9).

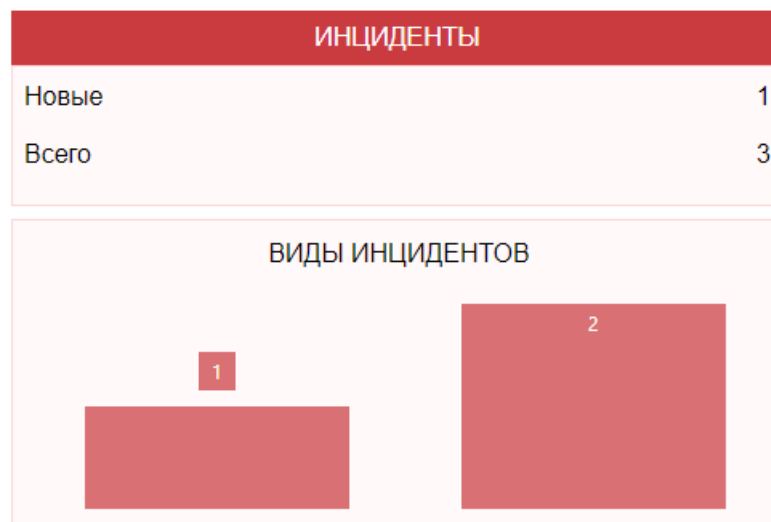


Рис. 9. Виджет «Инциденты информационной безопасности»

Виджет содержит данные о инцидентах ИБ, за которые ответственен пользователь. В верхней части отображается счетчик новых инцидентов ИБ, требующих обработки, и общее количество инцидентов ИБ, назначенных на пользователя. Нижний график содержит информацию о распределении инцидентов ИБ по видам.

2. Виджет «План мероприятий и приоритет инцидентов» (Рисунок 10).



Рис. 10. Виджет «План мероприятий и приоритет инцидентов»

Виджет содержит данные об инцидентах ИБ, за которые ответственен пользователь. В верхней части отображается счётчик новых инцидентов ИБ, требующих обработки, и общее количество инцидентов ИБ, назначенных на пользователя. Нижний график содержит информацию о распределении инцидентов ИБ по приоритетам реагирования.

3. Виджет «Реагирование на инциденты» (Рисунок 11).

Виджет содержит данные об инцидентах ИБ, находящихся в обработке. В верхней части отображается счетчик инцидентов ИБ, находящихся на реагировании,

и счётчик инцидентов ИБ, ожидающих закрытия. Нижний график содержит информацию о распределении инцидентов ИБ по источникам.



Рис. 11. Виджет «Реагирование на инциденты»

#### 4. Таблица «Инциденты информационной безопасности» (Рисунок 12).

Таблица содержит список инцидентов ИБ, за которые ответственен пользователь. Цветом выделены незакрытые инциденты с истёкшим сроком реагирования. Двойной щелчок левой кнопкой мыши по записи инцидента открывает его карточку.

ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ						
Дата и время возникновения	Номер	Наименование	Приоритет	Источник	Статус	
05.11.2019 17:11:28	08.25.08/ИИБ/5	Кража информации	Высокий	Техничес... средства	Новый инцидент	
05.11.2019 16:03:25	08.25.08/ИИБ/4	Зафиксированы помехи при передаче информации	Низкий	Персонал	Реагирование и расследование	
05.11.2019 11:45:04	08.25.08/ИИБ/1	Кража информации	Низкий	Персонал	Формирование заключения	

5 10 20 50 < 1 из 1 >

Рис. 12. Таблица «Инциденты информационной безопасности»

#### 5. Информационная панель «Реестр событий ИБ» (Рисунок 13).

Для того чтобы перейти к информационной панели, необходимо в боковом меню пользователя выбрать пункт «События ИБ».

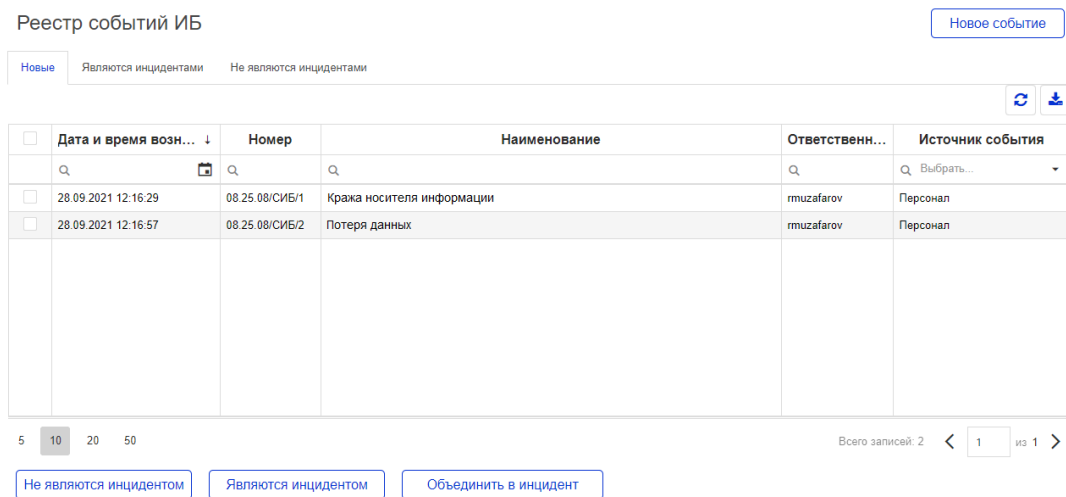


Рис. 13. Информационная панель «Реестр событий ИБ»

На соответствующих вкладках панели отображается список новых событий ИБ, список событий ИБ, являющихся и не являющихся инцидентами. В реестре событий доступно создание новых событий, перевод событий в инцидент для дальнейшей обработки и перевод в не являющиеся инцидентами. Двойной щелчок левой кнопкой мыши по записи события открывает его карточку.

#### 6. Информационная панель «Реестр инцидентов ИБ» (Рисунок 14).

Для того чтобы перейти к информационной панели, необходимо в боковом меню пользователя выбрать пункт «Инциденты ИБ».

На соответствующих вкладках панели отображается список инцидентов ИБ, за которые ответственен пользователь, разделённых по статусам: новые, в работе и обработанные (закрытые) инциденты. В реестре инцидентов ИБ доступно создание новых инцидентов и перевод в не являющиеся инцидентами. Цветом выделены инциденты с истёкшим сроком реагирования. Двойной щелчок левой кнопкой мыши по записи инцидента открывает его карточку.





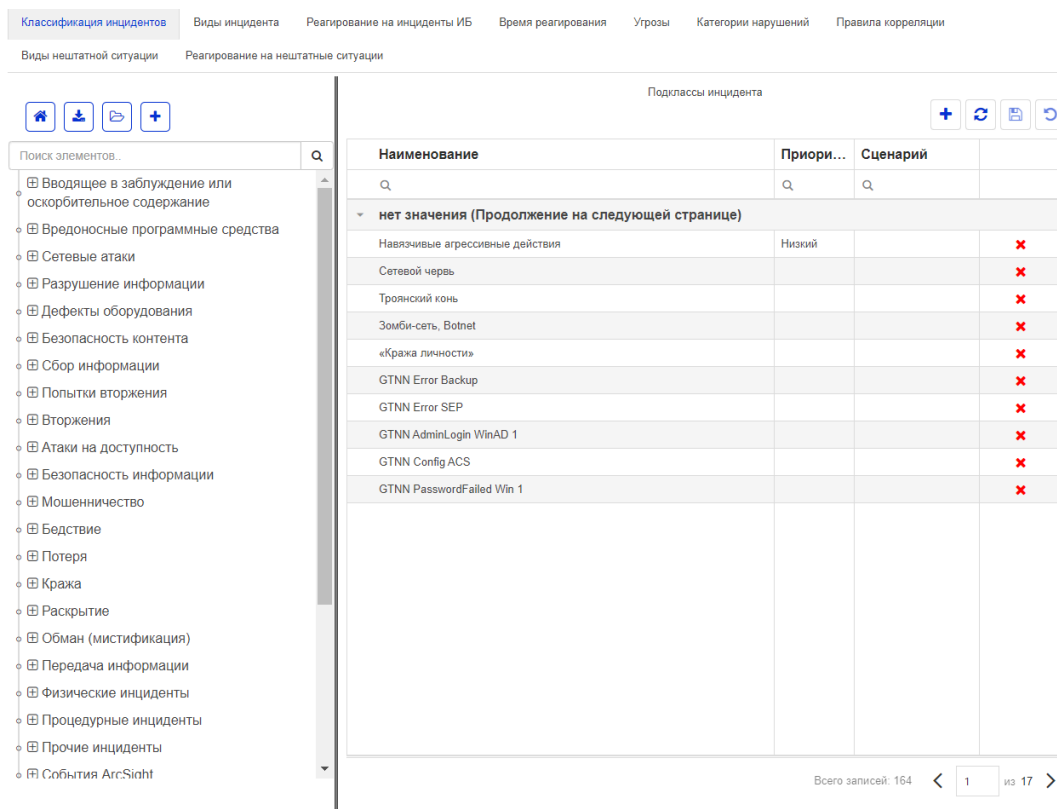


Рис. 15. Информационная панель «Справочники»

Информационная панель содержит вкладки с данными справочников Модуля УКИНС (списки классов и подклассов инцидентов, типовые сценарии реагирования, перечень видов инцидентов, угроз ИБ, правил корреляции и таблицу времени реагирования в зависимости от приоритета инцидента).

### 4.3. Рабочая область Руководства САОБ

Для перехода к рабочей области нажать на логотип в левом верхнем углу.

Рабочая область пользователя с ролью «Руководство САОБ» (Рисунок 16) предназначена для отображения основной информации о зарегистрированных событиях и инцидентах.

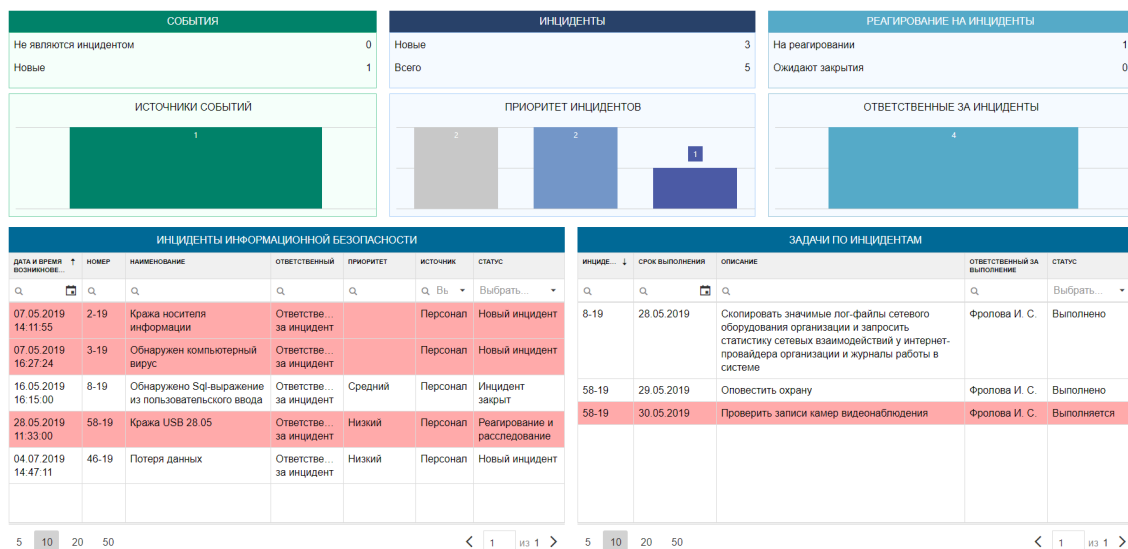


Рис. 16. Рабочая область Руководства САОВ

Рабочая область состоит из следующих виджетов:

1. Виджет «События информационной безопасности» (Рисунок 17)

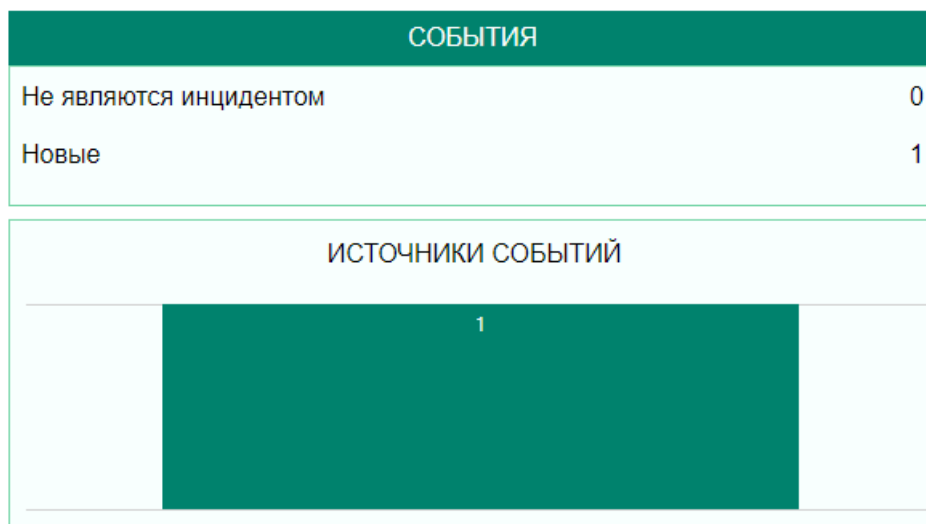


Рис. 17. Виджет «События информационной безопасности»

Виджет содержит данные о событиях ИБ. В верхней части отображается счётчик новых событий ИБ, требующих обработки, и счётчик событий ИБ, не являющихся инцидентами. Нижний график содержит информацию о распределении событий ИБ по источникам их обнаружения.

2. Виджет «Инциденты информационной безопасности» (Рисунок 18).

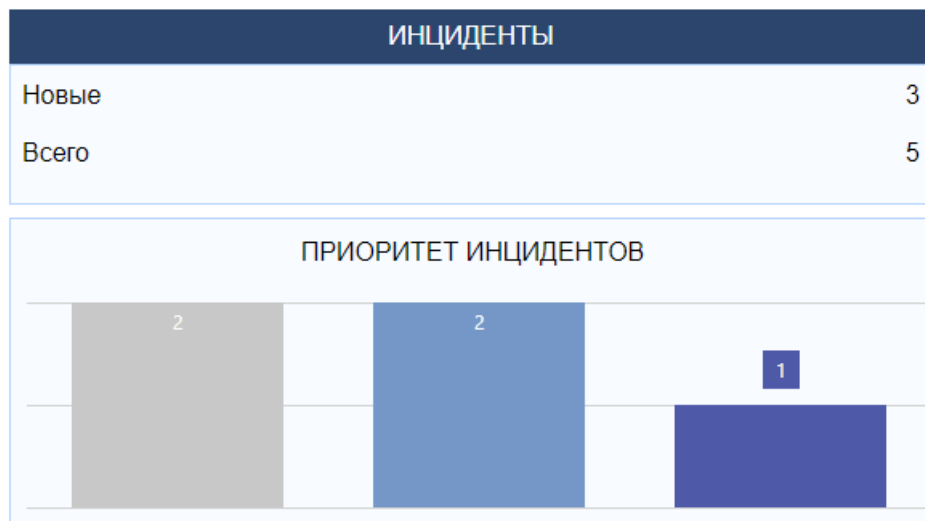


Рис. 18. Виджет «Инциденты информационной безопасности»

Виджет содержит данные об инцидентах ИБ, за которые ответственен пользователь. В верхней части отображается счётчик новых инцидентов ИБ, требующих обработки, а также общее количество инцидентов ИБ. Нижний график содержит информацию о распределении инцидентов ИБ по приоритетам реагирования.

### 3. Виджет «Реагирование на инциденты» (Рисунок 19).

Виджет содержит данные об инцидентах ИБ, находящихся в обработке. В верхней части отображается счётчик инцидентов ИБ, находящихся на реагировании, и счётчик инцидентов ИБ, ожидающих закрытия. Нижний график содержит информацию о распределении незакрытых инцидентов по ответственным пользователям.

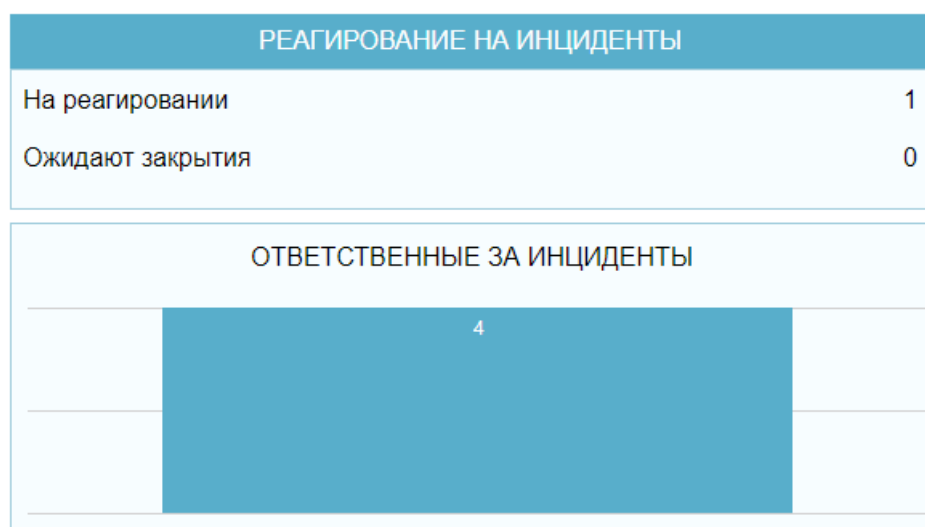


Рис. 19. Виджет «Реагирование на инциденты»

### 4. Таблица «Инциденты информационной безопасности» (Рисунок 20).

Таблица содержит общий список инцидентов ИБ. Цветом выделены незакрытые инциденты с истёкшим сроком реагирования. Двойной щелчок левой кнопкой мыши по записи инцидента открывает его карточку.

ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ						
ДАТА И ВРЕМЯ ВОЗНИКНОВЕ...	НОМЕР	НАИМЕНОВАНИЕ	ОТВЕТСТВЕННЫЙ	ПРИОРИТЕТ	ИСТОЧНИК	СТАТУС
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Выбрать...
07.05.2019 14:11:55	2-19	Кража носителя информации	Ответстве... за инцидент		Персонал	Новый инцидент
07.05.2019 16:27:24	3-19	Обнаружен компьютерный вирус	Ответстве... за инцидент		Персонал	Новый инцидент
16.05.2019 16:15:00	8-19	Обнаружено Sql-выражение из пользовательского ввода	Ответстве... за инцидент	Средний	Персонал	Инцидент закрыт
28.05.2019 11:33:00	58-19	Кража USB 28.05	Ответстве... за инцидент	Низкий	Персонал	Реагирование и расследование
04.07.2019 14:47:11	46-19	Потеря данных	Ответстве... за инцидент	Низкий	Персонал	Новый инцидент

5 10 20 50 < 1 из 1 >

Рис. 20. Таблица «Инциденты информационной безопасности»

#### 5. Таблица «Задачи по инцидентам» (Рисунок 21).

ЗАДАЧИ ПО ИНЦИДЕНТАМ				
ИНЦИДЕ...	СРОК ВЫПОЛНЕНИЯ	ОПИСАНИЕ	ОТВЕТСТВЕННЫЙ ЗА ВЫПОЛНЕНИЕ	СТАТУС
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Выбрать...
8-19	28.05.2019	Скопировать значимые лог-файлы сетевого оборудования организации и запросить статистику сетевых взаимодействий у интернет-провайдера организации и журналы работы в системе	Фролова И. С.	Выполнено
58-19	29.05.2019	Оповестить охрану	Фролова И. С.	Выполнено
58-19	30.05.2019	Проверить записи камер видеонаблюдения	Фролова И. С.	Выполняется

5 10 20 50 < 1 из 1 >

Рис. 21. Таблица «Задачи по инцидентам»

Таблица содержит список сформированных задач по расследованию и реагированию на инциденты ИБ. Цветом выделены невыполненные задачи с истёкшим сроком выполнения. Двойной щелчок левой кнопкой мыши по записи о задаче открывает её карточку. Карточка доступна только для чтения.

#### 6. Информационная панель «Реестр событий ИБ» (Рисунок 22).

Для того чтобы перейти к информационной панели, необходимо в боковом меню пользователя выбрать пункт «События ИБ».

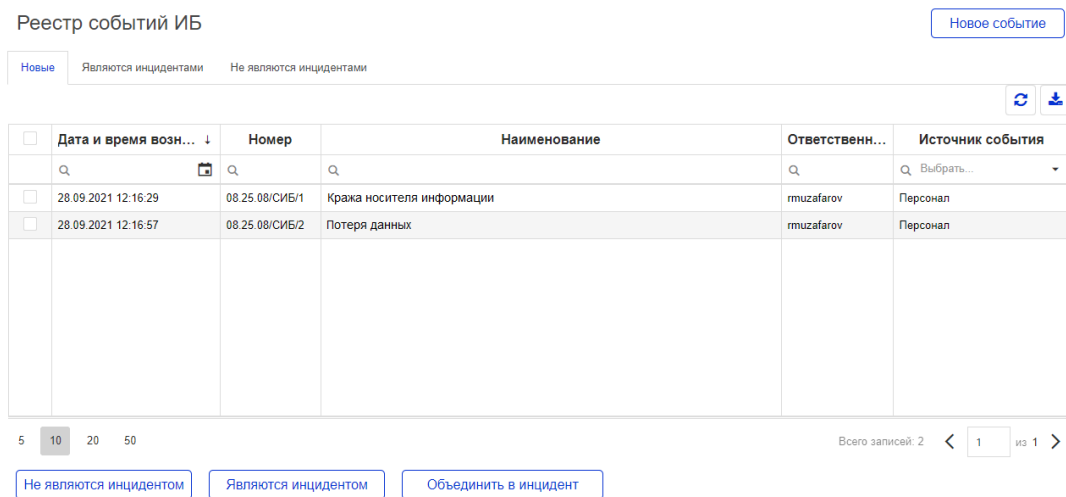


Рис. 22. Информационная панель «Реестр событий ИБ»

На соответствующих вкладках панели отображается список новых событий ИБ, список событий ИБ, являющихся и не являющихся инцидентами. В реестре событий доступно создание новых событий, перевод событий в инцидент для дальнейшей обработки и перевод в не являющиеся инцидентами. Двойной щелчок левой кнопкой мыши по записи события открывает его карточку.

#### 7. Информационная панель «Реестр инцидентов ИБ» (Рисунок 23).

Для того чтобы перейти к информационной панели, необходимо в боковом меню пользователя выбрать пункт «Инциденты ИБ».

На соответствующих вкладках панели отображается список инцидентов ИБ, разделенных по статусам: новые, в работе и обработанные (закрытые) инциденты. В реестре инцидентов ИБ доступно создание новых инцидентов и перевод в не являющиеся инцидентами. Цветом выделены инциденты с истёкшим сроком реагирования. Двойной щелчок левой кнопкой мыши по записи инцидента открывает его карточку.

Реестр инцидентов ИБ

Новый инцидент

Новые В работе Обработанные

Данные таблицы:

	Дата и время возникновения...	Номер	Наименование	Подкласс	Приоритет	Источник	Ответственный
	08.11.2021 15:54:20	08.25.08/ИИБ/4	Вирус на ПК с КТ	Компьютерный вирус	Средний	Персонал	ozib
	03.11.2021 10:25:22	08.25.08/ИИБ/2	Кража носителя данных	Кража носителя данных	Низкий	Персонал	Кудряшова К.

Всего записей: 2

Не является инцидентом

Рис. 23. Информационная панель «Реестр инцидентов ИБ»

## 8. Информационная панель «Справочники» (Рисунок 24).

Для того чтобы перейти к информационной панели, необходимо в боковом меню пользователя выбрать пункт «Справочники».

Классификация инцидентов Виды инцидента Реагирование на инциденты ИБ Время реагирования Угрозы Категории нарушений

Правила корреляции Виды нештатной ситуации Реагирование на нештатные ситуации

Подклассы инцидента

Наименование	Приоритет	Сценарий
нет значения (Продолжение на следующей странице)		
Навязчивые агрессивные действия	Низкий	✗
Сетевой червь		✗
Троянский конь		✗
Зомби-сеть, Botnet		✗
Смешанные атаки		✗
«Кража личности»		✗
GTNN Error Backup		✗
GTNN Error SEP		✗
GTNN AdminLogin WinAD 1		✗
GTNN Config ACS		✗

Всего записей: 162

Рис. 24. Информационная панель «Справочники»

Информационная панель содержит вкладки с данными справочников Модуля УКИНС.

В таблице «Реестр планов реагирования на инцидент ИБ, требующих утверждения» отображается список инцидентов ИБ, для которых необходимо утвердить план мероприятий по реагированию и расследованию. Двойной щелчок левой кнопкой мыши по записи инцидента открывает карточку плана реагирования на инцидент ИБ.

Рис. 25. Информационная панель «Реестр планов реагирования на инцидент информационной безопасности»

Для перехода к стартовой странице нажать на логотип в левом верхнем углу.

Назначенные на меня

Назначенные мной

Выполненные

Отмененные мной

Искать...

Наимено...	Дата создания	Плановая дата заверше...	Статус	Автор	Исполнит...	Дата начала работы	
Выполн... меропри... по расслед... инцидента №20-19	01.07.2019	02.07.2019	В работе	kkudryas...	ГРИБ	01.07.2019	

1

ИНЦИДЕНТЫ

Новые	32
Всего	46

МЕРОПРИЯТИЯ ПО РЕАГИРОВАНИЮ

Выполняется	2
Выполнено	5

МЕРОПРИЯТИЯ ПО РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ

ИНЦ... ↓	ОПИСАНИЕ	СТАТУС	СРОК ВЫПОЛНЕНИЯ
Q	Q	Выбрать...	Q
8-19	Скопировать значимые лог-файлы сетевого оборудования организации и запросить статистику сетевых взаимодействий у интернет-провайдера организации и журналы работы в системе	Выполнено	28.05.2019
58-19	Оповестить охрану	Выполнено	29.05.2019
58-19	Проверить записи камер видеонаблюдения	Выполняется	30.05.2019

5

10

20

50

<

1

из 1

>



МЕРОПРИЯТИЯ ПО РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ			
ИНЦ... ↓	ОПИСАНИЕ	СТАТУС	СРОК ВЫПОЛНЕНИЯ
🔍	🔍	Выбрать... ▼	🔍 📅
8-19	Скопировать значимые лог-файлы сетевого оборудования организации и запросить статистику сетевых взаимодействий у интернет-провайдера организации и журналы работы в системе	Выполнено	28.05.2019
58-19	Оповестить охрану	Выполнено	29.05.2019
58-19	Проверить записи камер видеонаблюдения	Выполняется	30.05.2019

5 10 20 50
< 1 из 1 >

Рис. 29. Виджет «Мероприятия по реагированию на инциденты»

Виджет содержит перечень мероприятий по реагированию, назначенных на пользователя. С него можно осуществить переход к карточке мероприятия.

4. Виджет с перечнем задач, назначенных на пользователя (Рисунок 30).

Назначенные на меня    Назначенные мной    Выполненные    Отмененные мной							
<div> <div>↺</div> <div>🔍 Искать...</div> </div>							
Наимено...	Дата создания	Плановая дата заверше...	Статус	Автор	Исполнит...	Дата начала работы	
Выполн... меропр... по расслед... инцидента №20-19	01.07.2019	02.07.2019	В работе	kkudryas...	ГРИИБ	01.07.2019	➡

1

Рис. 30. Виджет с перечнем задач, назначенных на пользователя

Виджет содержит перечень системных задач, назначенных на пользователя. С него можно осуществить переход к карточке задачи.

На вкладке «Назначенные на меня» отображаются незакрытые задачи. Красным цветом выделены задачи с истекшим сроком выполнения.

На вкладке «Выполненные» отображаются все задачи, выполненные пользователем.

## 4.5. Рабочая область Оператора-диспетчера

Для перехода к рабочей области нажать на логотип в левом верхнем углу.

Рабочая область пользователя с ролью «Оператор-диспетчер» ([Рисунок 31](#)) предназначена для отображения списка новых событий и инцидентов ИБ.

Реестр событий ИБ		Реестр инцидентов ИБ					
							Новое событие
Дата и время возникновения	↓	Номер	Наименование	Ответстве...	Подкласс	Источник	
🔍	📅	🔍	🔍	🔍	🔍	🔍 Выбрать. ▾	
12.12.2019 12:26:04		08.25.08/СИБ/39	Тестовое событие	Ответстве... за инцидент	Дефекты периферийного оборудования	Персонал	✖
08.12.2019 11:04:11		08.25.08/СИБ/38	Тестовое Событие	dapershin	Социальный инжиниринг	Персонал	✖
03.12.2019 12:00:18		08.25.08/СИБ/27	Тестовое событие	kkudryashova	Дефекты периферийного оборудования	Персонал	✖
02.12.2019 10:57:33		08.25.08/СИБ/20	Тестовое событие	kkudryashova	Фальсификация информации	Персонал	✖
25.11.2019 11:37:48		08.25.08/СИБ/19	Событие ИБ	Ответстве... за инцидент	Несанкционирова... модификация информации. Разрушение	Персонал	✖
5 10 20 50		Всего записей: 5 < 1 из 1 >					

Рис. 31. Рабочая область Оператора-диспетчера

## 5. Сценарии работы пользователей

В разделе приведены сценарии работы пользователей во всех ролях, предусмотренных для корректного функционирования модуля УКИНС.

### 5.1. Работа со справочниками

Для работы со справочниками пользователю необходимо в боковом меню выбрать раздел «Справочники». Откроется форма со справочниками (Рисунок 32).

Данный раздел содержит следующие вкладки:

- Справочник «Классификация инцидентов»;
- Справочник «Виды инцидента»;
- Справочник «Реагирование на инциденты ИБ»;
- Справочник «Время реагирования»;
- Справочник «Угрозы»;
- Справочник «Категории нарушений»;
- Справочник «Правила корреляции»;
- Справочник «Виды нештатной ситуации»;
- Справочник «Реагирование на нештатные ситуации».

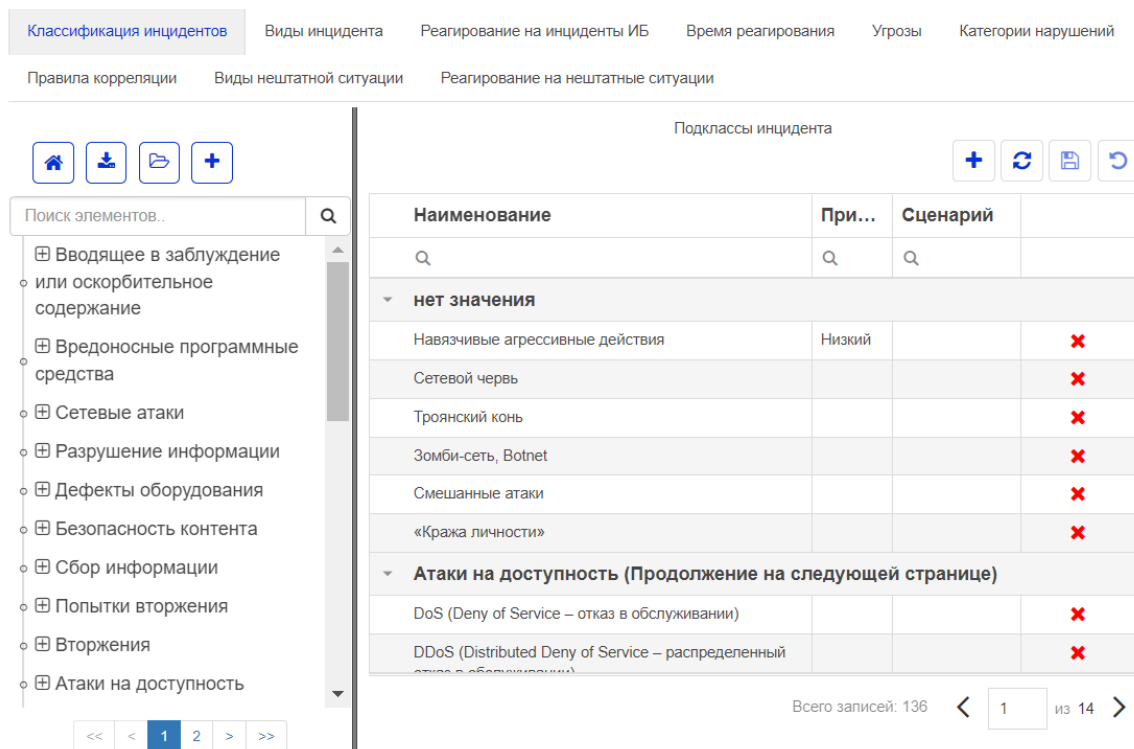


Рис. 32. Раздел меню «Справочники»

#### 5.1.1. Справочник «Классификация инцидентов»

Справочник содержит типовые классы и подклассы инцидентов (Рисунок 33).

В левой части справочника отображается дерево классов инцидентов и связанных с ним подклассов. В правой части расположена таблица со списком подклассов, сгруппированных по связанным классам.

Данные из справочника используются для классификации инцидентов и событий ИБ, а также их автоматической приоритизации.

Для возврата к главной странице справочника нажать .

Для экспорта списка классов инцидентов нажать .

Для импорта списка классов инцидентов нажать .

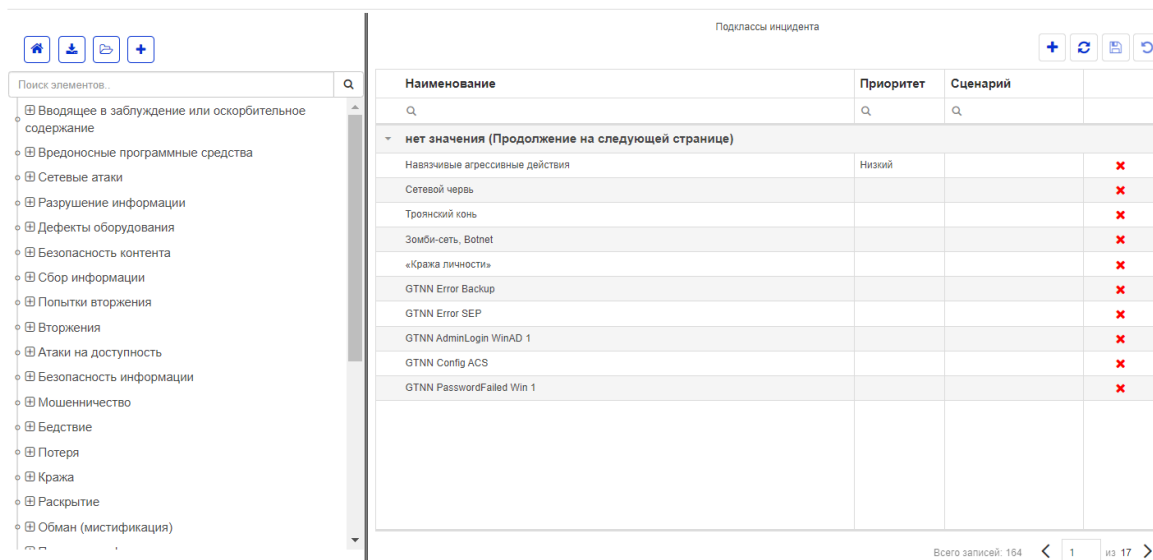



Рис. 33. Справочник «Классификация инцидентов»

#### 5.1.1.1. Создание класса инцидента

1. Над списком классов нажать кнопку .
2. В правой части экрана откроется карточка нового класса ([Рисунок 34](#)).

Класс

Наименование \*

Наименование

Подклассы

+

Наименование	Приоритет	
Q	Q	

Сохранить

Рис. 34. Карточка нового класса инцидента

3. Указать наименование класса.
4. Добавить в карточку связанные подклассы:
  - Над таблицей «Подклассы» нажать кнопку +.
  - Откроется форма выбора.
  - Выбрать необходимые записи с помощью флага ☒.
  - Нажать кнопку 

Сохранить

.
5. Для удаления связи с подклассом нажать кнопку ✖ в соответствующей строке.
6. Нажать кнопку 

Сохранить

.
7. Для удаления класса инцидента из справочника нажать кнопку Удалить.

### 5.1.1.2. Создание подкласса инцидента

1. Перейти в карточку нового подкласса ([Рисунок 35](#)) одним из следующих способов:

- над списком подклассов нажать кнопку **+** ([Рисунок 33](#));
- в карточке класса инцидента нажать кнопку **Новый подкласс** ([Рисунок 34](#)).

Подкласс:

Наименование подкласса \*

Текст

Описание

Описание подкласса

Класс инцидента \*

Вводящее в заблуждение или оскорбительное содержание x

Приоритет

Приоритет

Сохранить

Рис. 35. Карточка нового подкласса инцидента

2. В открывшейся форме заполнить доступные поля:

- Наименование подкласса;
- Приоритет;



**Внимание:**

Указанный приоритет будет автоматически назначаться всем инцидентам, отнесенным к данному подклассу.

- Класс инцидента (поле заполняется автоматически при создании подкласса из карточки класса).
- Описание.

3. Нажать кнопку **Сохранить**.

4. После сохранения станет доступно поле «Сценарий реагирования» ([Рисунок 36](#)).

5. Выберите сценарий реагирования, связанный с подклассом.

Для создания и привязки нового сценария - нажать **+** («Создать новый сценарий реагирования») - подробнее в разделе [«Создание сценария реагирования»](#).

**Внимание:**

Указанный сценарий реагирования будет автоматически формироваться при переходе к этапу реагирования на инциденты, отнесенные к данному подклассу.

6. Нажать кнопку .

7. Для удаления подкласса инцидента из справочника нажать кнопку  Удалить.

Наименование подкласса \*

Саботаж

Описание

При этом виде атаки система бомбардируется таким множеством сетевых пакетов, что операции приостанавливаются или происходит критический сбой системы. Примерами удаленной атаки «отказ в обслуживании» являются: SYS-a, перегрузка сети запросами


Класс инцидента \*

Атаки на доступность x ▾

Приоритет

Приоритет ▾

Сценарий реагирования

Сценарий ИБ ▾ 

Сохранить

Рис. 36. Карточка подкласса инцидента

### 5.1.2. Справочник «Виды инцидента»

Справочник ([Рисунок 37](#)) содержит список видов инцидентов ИБ.









Виды инцидента информационной безопасности	
<div>     </div>	
Вид инцидента ИБ	
Q	
Ошибка	✖
Намеренный	✖
Случайный	✖
Неизвестно	✖

Рис. 37. Справочник «Виды инцидента»

#### 5.1.2.1. Создание вида инцидента

1. Нажать кнопку .
2. В таблице отобразится пустая строка.
3. Ввести наименование вида инцидента.
4. Для сохранения изменений нажать кнопку .
5. Для отмены действия нажать кнопку .
6. Для удаления вида нажать кнопку  в соответствующей строке.

#### 5.1.3. Справочник «Реагирование на инциденты ИБ»

Справочник содержит типовые сценарии реагирования на инциденты ИБ и список типовых мероприятий по реагированию и расследованию ([Рисунок 38](#)).

В левой части справочника отображается дерево сценариев и связанных с ним мероприятий. В правой части расположена таблица со списком мероприятий по расследованию и реагированию.

Данные из справочника используются для формирования плана реагирования на инциденты ИБ.

Для возврата к главной странице справочника нажать .

Для экспорта списка сценариев нажать .

Для импорта списка сценариев нажать .



Перечень мероприятий по реагированию на инциденты ИБ

Описание	Тип мероприятия УИ	
Заменить изъятые, упакованные и опечатанные носители информации на новые	Реагирование	✗
Запрос материалов по событию	Расследование	✗
Копирование журналов систем контроля доступа в помещения организации, копирование видеопотока систем видеонаблюдения в офисе или офисном центре за максимально возможный промежуток времени	Реагирование	✗
Отключение или блокировка пораженных ИТ-активов	Реагирование	✗
Отключить, упаковать, опечатать, сдать на хранение соответствующие носители информации	Реагирование	✗
Подготовить документы для правоохранительных органов и работников подразделения (описание инцидента в письменной форме, договор на предоставление услуги, договор на предоставление услуги доступа в сеть Интернет, заявление о преступлении)	Расследование	✗

Всего записей: 16 < 1 из 2 >

Рис. 38. Справочник «Реагирование на инциденты ИБ»

### 5.1.3.1. Создание сценария реагирования

1. Перейти в карточку нового сценария (Рисунок 39) любым из следующих способов:
  - над списком сценариев нажать кнопку **+** (Рисунок 38);
  - из карточки подкласса инцидента (нажать кнопку **+**) (Рисунок 36).

Сценарий реагирования на инцидент ИБ:

Наименование \*

Наименование

Описание

Описание


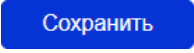





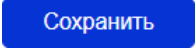

Подклассы инцидента

Подклассы

Сохранить

Рис. 39. Карточка нового сценария

2. В открывшейся форме заполнить доступные поля:
  - Наименование;
  - Описание.
3. Добавить в карточку связанные подклассы:
  - Нажать кнопку **■** возле поля «Подклассы инцидента».
  - Откроется форма выбора.

- Выбрать необходимые записи с помощью флага ☒.
  - Нажать кнопку .
4. Нажать кнопку .
  5. После сохранения станет доступна вкладка «Мероприятия» (Рисунок 40).
  6. Для добавления мероприятий в таблице «Мероприятия»:
    - Нажать кнопку .
    - В таблице отобразится пустая строка;
    - Ввести порядковый номер мероприятия.
    - Из выпадающего списка выбрать мероприятие
    - Выбрать ответственного.
    - Указать срок реагирования. При формировании плана реагирования срок выполнения задач будет вычислен исходя из указанного срока реагирования.
    - Для сохранения изменений нажать кнопку .
    - Для отмены действия нажмите кнопку .
  7. Для создания и привязки нового мероприятия - нажать  - подробнее в разделе «[Создание мероприятия](#)».
  8. Для удаления мероприятия нажать кнопку  в соответствующей строке.
  9. Для сохранения нового сценария реагирования нажать кнопку .
  10. Для удаления сценария из справочника нажать кнопку  Удалить.

Сценарий реагирования на инцидент ИБ:

Сценарий противодействия инъекциям

Общая информация

Мероприятия

Мероприятия

Создать мероприятие

+

Номер	Тип мероприятия	Мероприятие	Ответственный	Срок выполнен... (ед.изм. времени)	Срок выполнения (количество единиц)	
Q	Q Выбрать...	Q	Q	Q Выбрат	Q	

Сохранить

Удалить

Рис. 40. Карточка сценария реагирования

### 5.1.3.2. Создание мероприятия

1. Перейти в карточку нового мероприятия (Рисунок 41) любым из следующих способов:

- над списком мероприятий нажать кнопку **+** (Рисунок 38);
- из карточки сценария (нажать кнопку **Создать мероприятие**) (Рисунок 40).

Создание мероприятия ИБ

Описание \*

Тип мероприятия \*

Тип

Тип происшествия

Инцидент/Событие ИБ

Сохранить

Отмена

Рис. 41. Карточка создания нового мероприятия

2. В открывшейся форме заполнить доступные поля:

- Описание;
- Тип мероприятия.

3. Нажать кнопку **Сохранить**.




4. Для отмены действия нажмите на кнопку **Отмена**.


5. Для удаления мероприятия в перечне мероприятий (Рисунок 38) нажать кнопку **✗** в соответствующей строке.

#### 5.1.4. Справочник «Время реагирования»

Справочник содержит нормы времени реагирования на инциденты ИБ в зависимости от приоритета (Рисунок 42).

Для редактирования справочника:

1. В соответствующей строке нажать кнопку .
2. Запись станет доступной для редактирования.
3. Изменить значение времени реагирования.
4. Для сохранения изменений нажать кнопку .
5. Для отмены - нажать кнопку .






Приоритет инцидента	Время реагирования, ч	
Q	Q	
Высокий	24	
Низкий	48	
Средний	72	

Рис. 42. Справочник времени реагирования

#### 5.1.5. Справочник «Угрозы»

Справочник (Рисунок 43) содержит список типовых угроз ИБ. Дополнительно в справочник загружен перечень угроз ФСТЭК.

В левой части справочника отображается список всех угроз и признак значения по умолчанию. В правой части расположена диаграмма распределения угроз по видам инцидентов.

Данные из справочника используются для оценки инцидентов ИБ.

Для возврата к главной странице справочника нажать .

Для экспорта списка сценариев нажать .

Для импорта списка сценариев нажать .

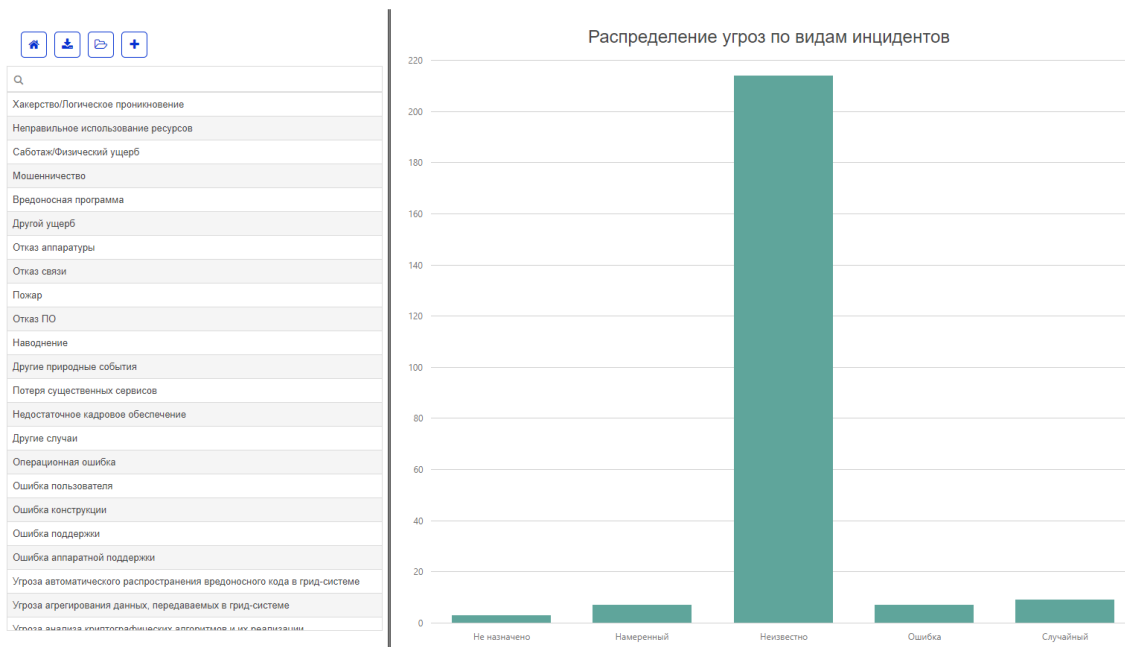


Рис. 43. Справочник «Угрозы»

### 5.1.5.1. Создание угрозы

1. Над списком угроз нажать кнопку **+**.
2. В правой части экрана откроется карточка новой угрозы (Рисунок 44).

Угроза

Основная информация

Виды инцидента

Наименование \*

Введите наименование

Описание

Введите описание

Сохранить

Рис. 44. Карточка новой угрозы ИБ

3. В открывшейся форме заполнить доступные поля:

- Наименование;
  - Описание.
- Добавить связанные виды инцидента:
    - Нажать кнопку **+** на вкладке «Виды инцидента».
    - Откроется форма выбора.
    - Выбрать необходимые записи с помощью флага ☒.
    - Нажать кнопку **Сохранить**.
  - Для удаления связи с видом инцидента нажать кнопку **✗** в соответствующей строке.
  - Для сохранения новой записи угрозы ИБ нажать кнопку **Сохранить**.

### 5.1.6. Справочник «Категории нарушений»

Справочник содержит список категорий нарушений ([Рисунок 45](#)).

Категории воздействия		
		<input type="button" value="↺"/> <input type="button" value="+"/> <input type="button" value="💾"/> <input type="button" value="↻"/>
Указатель категории	Наименование категории	
КЗЭИ	Коммерческие и экономические интересы	✗
МиБП	Информация содержащая менеджмент и бизнес-процессы	✗
НПО	Информация содержащая правовые и нормативные обязательства	✗
ФП/СБП	Финансовые потери/срыв бизнес-процессов	✗
ПДн	Информация, содержащая персональные данные	✗
ПП	Потеря престижа	✗

Рис. 45. Справочник «Категории нарушений»

#### 5.1.6.1. Создание категории нарушения

- Нажать кнопку **+**.
- В таблице отобразится пустая строка.
- Ввести наименование категории, указатель категории.
- Для сохранения изменений нажать кнопку **💾**.
- Для отмены действия нажмите кнопку **↺**.
- Для удаления категории нажать кнопку **✗** в соответствующей строке.

### 5.1.7. Справочник «Правила корреляции»

Справочник содержит список правил корреляции ([Справочник «Правила корреляции»](#)).

Перечень правил корреляции

+
↺

Описание	
Q	
Неудачный вход в операционную систему от имени одной учетной записи в течение пяти минут	✖

1 из 1

Рис. 46. Справочник «Правила корреляции»

### 5.1.7.1. Создание правила корреляции

1. Нажать кнопку +.
2. Откроется форма создания правила корреляции (Рисунок 47).
3. Ввести описание правила корреляции.

Создание правила корреляции

✖

Описание \*

Описание

Сохранить

Отмена

Рис. 47. Форма создания правила корреляции

4. Для сохранения нового правила нажать кнопку Сохранить.
5. Для отмены создания нажать кнопку Отмена.
6. После сохранения в карточке станут доступны поля:
  - Условие наступления;
  - Счетчик;
  - Глубина корреляции.
7. Заполнить упомянутые в п.6 поля (Рисунок 48).

Описание
Неудачный вход в операционную систему от имени одной учетной записи в течение пяти минут
Условие наступления
Неуспешная попытка доступа
Счетчик
5
Глубина корреляции
5 минут

Рис. 48. Карточка правила корреляции

8. Нажать .

9. Для удаления правила нажать кнопку  в соответствующей строке справочника.

### 5.1.8. Справочник «Виды нештатной ситуации»

Справочник содержит список видов нештатных ситуаций ([Рисунок 49](#)).

В левой части справочника отображается список видов нештатных ситуаций. В правой части расположена диаграмма распределения количества нештатных ситуаций по видам.

Данные из справочника используются для классификации видов нештатных ситуаций, а также их автоматической приоритизации.

Для возврата к главной странице справочника нажать .

Для экспорта списка видов нештатных ситуаций нажать .

Для импорта списка видов нештатных ситуаций нажать .



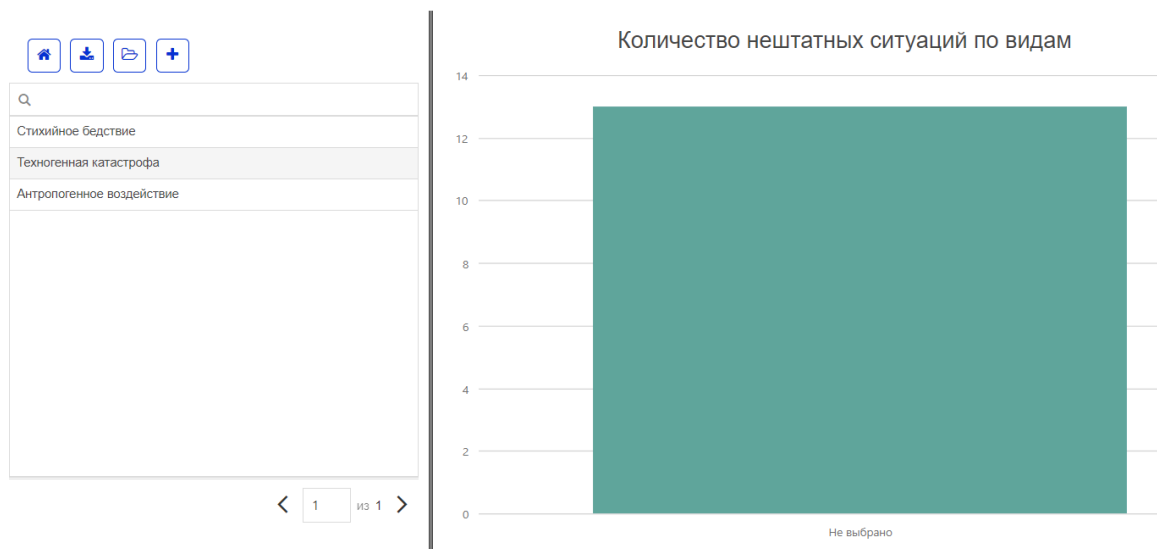


Рис. 49. Справочник «Виды нештатной ситуации»

#### 5.1.8.1. Создание вида нештатной ситуации

1. Над списком видов нажать кнопку **+**.
2. В правой части экрана откроется карточка нового вида ([Рисунок 50](#)).
3. Заполнить доступные поля:
  - Вид нештатной ситуации;
  - Описание;
  - Приоритет.



#### Внимание:

Указанный приоритет будет автоматически назначаться всем нештатным ситуациям, отнесенным к данному виду.

4. Нажать кнопку **Сохранить**.

### Вид нештатной ситуации:

Вид нештатной ситуации *	
<input type="text" value="Вид нештатной ситуации"/>	
Описание	
<input type="text" value="Описание вида нештатной ситуации"/>	
Приоритет *	<input type="text" value="Приоритет"/>

Сохранить

Рис. 50. Карточка нового вида нештатной ситуации

- После сохранения станет доступно поле «Сценарий реагирования» ([Рисунок 51](#)).
- Выберите сценарий реагирования на нештатную ситуацию, связанный с данным видом.

Для создания и привязки нового сценария - нажать **+** («Создать новый сценарий реагирования») - подробнее в разделе «[Создание сценария реагирования](#)».



#### Внимание:

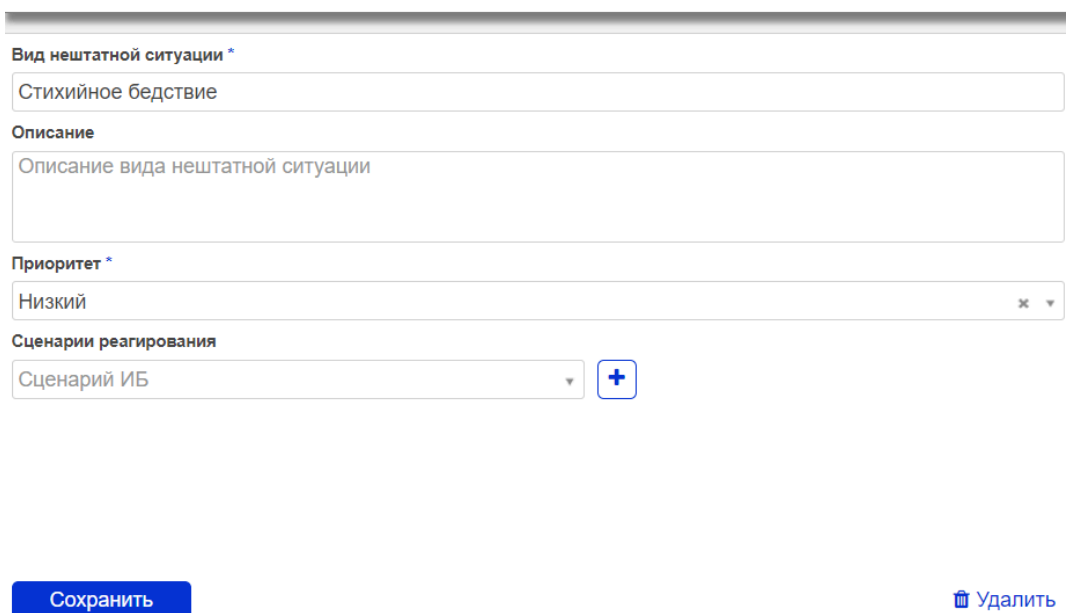
Указанный сценарий реагирования будет автоматически формироваться при переходе к этапу реагирования на нештатные ситуации, отнесенные к данному виду.

- Нажать кнопку

Сохранить

8. Для удаления вида нештатной ситуации из справочника нажать кнопку  Удалить.

Вид нештатной ситуации: Стихийное бедствие



Вид нештатной ситуации \*

Стихийное бедствие

Описание

Описание вида нештатной ситуации

Приоритет \*

Низкий

Сценарии реагирования

Сценарий ИБ

Сохранить

Удалить

Рис. 51. Карточка вида нештатной ситуации

### 5.1.9. Справочник «Реагирование на нештатные ситуации»

Справочник содержит типовые сценарии реагирования на нештатные ситуации и список типовых мероприятий по реагированию и расследованию ([Рисунок 52](#)).

В левой части справочника отображается дерево сценариев и связанных с ним мероприятий. В правой части расположена таблица со списком мероприятий по расследованию и реагированию.

Данные из справочника используются для формирования плана реагирования на нештатные ситуации.

Для возврата к главной странице справочника нажать .

Для экспорта списка сценариев нажать .

Для импорта списка сценариев нажать .

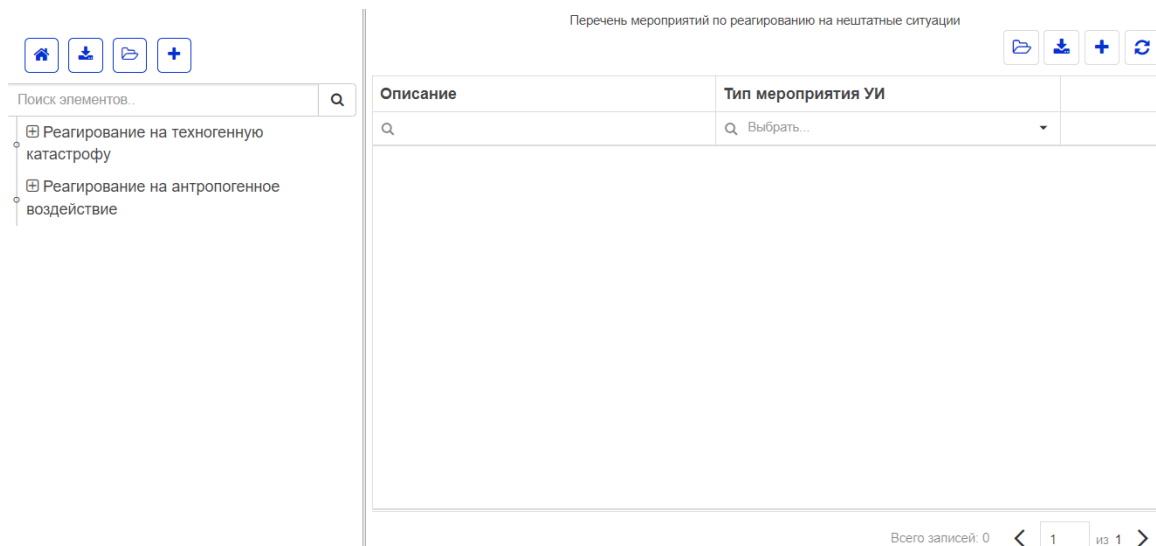


Рис. 52. Справочник «Реагирование на нештатные ситуации»

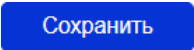





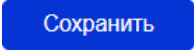

### 5.1.9.1. Создание сценария реагирования

1. Перейти в карточку нового сценария (Рисунок 39) любым из следующих способов:
  - над списком сценариев нажать кнопку **+** (Рисунок 52);
  - из карточки вида нештатной ситуации (нажать кнопку **+**) (Рисунок 51).

Сценарий реагирования на нештатную ситуацию:

Рис. 53. Карточка нового сценария

2. В открывшейся форме заполнить доступные поля:
  - Наименование;
  - Описание.
3. Добавить в карточку связанные виды нештатных ситуаций:
  - Нажать кнопку **+** возле поля «Виды нештатной ситуации».
  - Откроется форма выбора.
  - Выбрать необходимые записи с помощью флага ☒.
  - Нажать кнопку **Сохранить**.

4. Нажать кнопку .
5. После сохранения станет доступна вкладка «Мероприятия» (Рисунок 54).
6. Для добавления мероприятий в таблице «Мероприятия»:
  - Нажать кнопку .
  - В таблице отобразится пустая строка;
  - Ввести порядковый номер мероприятия.
  - Из выпадающего списка выбрать мероприятие
  - Выбрать ответственного.
  - Указать срок реагирования. При формировании плана реагирования срок выполнения задач будет вычислен исходя из указанного срока реагирования.
  - Для сохранения изменений нажать кнопку .
  - Для отмены действия нажмите кнопку .
7. Для создания и привязки нового мероприятия - нажать  - подробнее в разделе «Создание мероприятия».
8. Для удаления мероприятия нажать кнопку  в соответствующей строке.
9. Для сохранения нового сценария реагирования нажать кнопку .
10. Для удаления сценария из справочника нажать кнопку  Удалить.





Сценарий реагирования на нештатную ситуацию:









### Реагирование на техногенную катастрофу

Общая информация

Мероприятия

Мероприятия

Номер	Тип меропр...	Мероприятие	Ответстве...	Срок выпол... (ед.изм. врем...	Срок выпол... (колич... единиц)	
	 Выб↓			 В ↓		
	Реагирование		Пелевина Т.С.			
	Расследова...		Пелевина Т.С.			

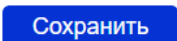






Рис. 54. Карточка сценария реагирования

## 5.2. Формирование группы реагирования на инциденты ИБ

1. В боковом меню пользователя выбрать пункт «ГРИИБ».
2. Откроется список участников ГРИИБ (Рисунок 55).
3. Нажать кнопку .
4. Откроется форма выбора работников.
5. Выбрать необходимые записи с помощью флага .

6. Нажать кнопку .

7. Для удаления работника из ГРИИБ нажать кнопку  в соответствующей строке таблицы.



Группа реагирования на инциденты ИБ и нештатные ситуации





Руководитель ГРИИБ

Выберите сотрудника

---

Работники\*

Фамилия И.О.	Должность	email	
<input type="text" value="Q"/>	<input type="text" value="Q"/>	<input type="text" value="Q"/>	
Зубова Н.А.	Администратор	zubova@email.ru	
Кудряшова К.А.	Начальник отдела	kudryashova@email.ru	
Пелевина Т.С.	Администратор	pelevina@email.ru	
Музафаров Р.Д.	Аудитор	muzafarov@email.ru	

5 10 20 50







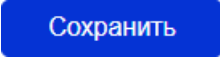
 1 из 1 

Рис. 55. Список участников ГРИИБ

### 5.2.1. Добавление участника ГРИИБ

1. В боковом меню пользователя выбрать пункт «ГРИИБ».
2. Нажать кнопку .
3. Откроется форма выбора работников.
4. Выбрать необходимые записи с помощью флага .
5. Нажать кнопку .
6. Для удаления работника из ГРИИБ нажать кнопку  в соответствующей строке таблицы.

### 5.2.2. Редактирование информации об участнике ГРИИБ

1. Дважды кликнуть левой кнопкой мыши по записи работника в списке.
2. Откроется карточка участника ГРИИБ ([Рисунок 56](#)).
3. Внести необходимые изменения в поля карточки.
4. Для сохранения изменений нажать кнопку .
5. Для отмены изменений нажать кнопку [Отменить](#).

## Карточка работника: Пелевина Т.С.

Общая информация

Фамилия	Имя	Отчество
<input type="text" value="Пелевина"/>	<input type="text" value="Татьяна"/>	<input type="text" value="Сергеевна"/>
Подразделение *	Должность	
<input style="border-bottom: 1px solid #ccc;" type="text" value="Администрация"/>	<input style="border-bottom: 1px solid #ccc;" type="text" value="Администратор"/>	
email	Телефон	
<input type="text" value="pelevina@email.ru"/>	<input type="text" value="Телефон"/>	

Сохранить

Отменить

Рис. 56. Карточка участника ГРИИБ

### 5.3. Управление событиями информационной безопасности

События ИБ могут быть обнаружены работниками Общества в ходе их трудовой деятельности, а также автоматизированными системами и средствами защиты информации (системы управления событиями ИБ, системы обнаружения вторжений, системы анализа защищенности, межсетевые экраны, операционные системы и др.), и лицами, ответственными за их администрирование и эксплуатацию, по результатам мониторинга.

Для перехода к реестру событий ИБ необходимо в боковом меню выбрать раздел «События ИБ» ([Рисунок 57](#)).

Новые

Являются инцидентами

Не являются инцидентами



<input type="checkbox"/>	Дата и время возн... ↓	Номер	Наименование	Ответственн...	Источник события
	🔍	📅 🔍	🔍	🔍	🔍 Выбрать...
<input type="checkbox"/>	28.09.2021 12:16:29	08.25.08/СИБ/1	Кража носителя информации	rmuzafarov	Персонал
<input type="checkbox"/>	28.09.2021 12:16:57	08.25.08/СИБ/2	Потеря данных	rmuzafarov	Персонал

5 10 20 50

Всего записей: 2 < 1 из 1 >

Не являются инцидентом

Являются инцидентом

Объединить в инцидент

Рис. 57. Информационная панель «Реестр событий ИБ»

### 5.3.1. Создание записи о событии информационной безопасности

1. В боковом меню пользователя выбрать пункт «События ИБ».
2. На информационной панели «Реестр событий ИБ» нажать кнопку
3. Откроется карточка нового события (Рисунок 58).

Новое событие



## Событие

Наименование события \*

Дата и время возникновения



Дата и время обнаружения



Дата и время оповещения



Класс события \*



Подкласс события \*



Оповестил работник

Ответственный за событие \*



Информация о сообщившем

Что произошло

Рис. 58. Карточка нового события ИБ

4. В открывшейся форме заполнить доступные поля.

По умолчанию поля «Дата и время возникновения», «Дата и время обнаружения», «Дата и время оповещения» заполняются текущими значениями.

В поле «Ответственный за событие» по умолчанию указывается текущий пользователь. При необходимости данные этих полей можно отредактировать



### Внимание:

Ответственный за событие может быть выбран только среди пользователей с ролью «Ответственный за инцидент ИБ».



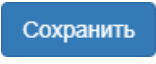

5. После заполнения формы возможны следующие действия:

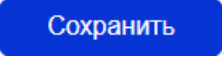
- для создания записи о событии и возврата в реестр событий ИБ необходимо нажать кнопку ;
- для создания записи о событии и перехода в карточку созданного события необходимо нажать кнопку .

### 5.3.2. Редактирование записи о событии информационной безопасности



1. Перейти в карточку события из перечня новых событий информационной панели «Реестр событий ИБ» (Рисунок 57).

Рис. 59. Карточка события ИБ

2. На вкладке «Описание» при необходимости изменить значения в редактируемых полях (Рисунок 59).
3. Для добавления связанных бизнес-процессов на вкладке «Пораженные компоненты» в таблице «Бизнес-процессы»:
  - нажать кнопку +;
  - выбрать необходимые записи с помощью флага ☒;
  - нажать кнопку .
4. Для удаления связи с бизнес-процессом на вкладке «Пораженные компоненты» нажать кнопку  в соответствующей строке.
5. Для добавления связанных объектов защиты на вкладке «Пораженные компоненты» в таблице «Информационные активы, программное обеспечение, технические средства»:
  - нажать кнопку +;
  - выбрать необходимые записи с помощью флага ☒;
  - нажать кнопку .
6. Для удаления связи с объектом защиты на вкладке «Пораженные компоненты» нажать кнопку  в соответствующей строке.

7. На вкладке «Уязвимости» при необходимости заполнить доступные поля.
8. Для применения изменения без изменения статуса события ИБ необходимо нажать кнопку .

### 5.3.3. Формирование отчетных форм о событии информационной безопасности

1. Открыть карточку события ИБ на вкладке «Описание» ([Рисунок 59](#)).
2. Нажать кнопку  рядом с полем «Отчет о событии» для формирования отчета.
3. Нажать кнопку  для скачивания сформированного отчета.



#### Внимание:


В случае изменения данных о событии ИБ необходимо обновить отчет, для этого повторно нажать кнопку .

### 5.3.4. Обработка события информационной безопасности

По результатам обработки события у пользователя есть возможность:

- перевести событие в статус «Новый инцидент» (см. [Перевод в статус «Новый инцидент»](#));
- перевести событие в статус «Не является инцидентом» (см. [Перевод в статус «Не является инцидентом»](#)).

#### 5.3.4.1. Перевод в статус «Новый инцидент»

1. Перейти в карточку нового события.
2. Нажать кнопку  (доступна только на статусе «Новое событие»).
3. Откроется форма перевода события в инцидент ([Рисунок 60](#)).

Событие 08.25.08/СИБ/3

- ☒ Является новым инцидентом  
☐ Связан с существующим инцидентом

Ответственный за инцидент \*



Отмена

Рис. 60. Форма перевода события в инцидент

4. После открытия формы перевода события в инцидент возможны следующие действия:

- Выбрать пункт «Является новым инцидентом», в появившемся поле «Ответственный за инцидент» указать ответственного. В этом случае будет зарегистрирован новый инцидент.
- Выбрать пункт «Связан с существующим инцидентом», в появившемся поле «Наименование инцидента» указать инцидент ИБ, к которому относится событие. В этом случае событие будет связано с уже существующим инцидентом.

5. Нажать кнопку

6. Статус события изменится на «Не является инцидентом». На карточке события отобразится вкладка «Инцидент» (Рисунок 61). Вкладка содержит основную информацию о связанном инциденте ИБ и ссылку на карточку инцидента и доступна только для чтения.

Описание	Пораженные компоненты	Уязвимости	Инцидент
<b>Номер инцидента</b> <input type="text" value="08.25.08/ИИБ/5"/>			<b>Наименование инцидента</b> <input type="text" value="Кража носителя информации"/>
<b>Дата и время возникновения</b> <input type="text" value="09.11.2021 11:50:55"/>			<b>Время реагирования, ч</b> <input type="text" value="72"/>
<b>Статус</b> <input type="text" value="Новый инцидент"/>			<b>Ответственный за инцидент</b> <input type="text" value="Зубова Н."/>

Рис. 61. Карточка события ИБ. Вкладка «Инцидент»

### 5.3.4.2. Перевод в статус «Не является инцидентом»

1. Перейти в карточку нового события.

2. Нажать кнопку

(доступна только на статусе «Новое событие»).



#### **Внимание:**

Данное действие доступно в случае, если текущий пользователь выбран Ответственным за событие с ролью «Ответственный за инцидент ИБ».


3. Статус события изменится на «Не является инцидентом».

### **5.3.5. Групповая обработка событий информационной безопасности**


На форме реестра событий ИБ ([Рисунок 57](#)) пользователь может осуществлять следующие действия:

- [Перевод группы событий в статус «Новый инцидент»](#);
- [Перевод группы событий в статус «Не является инцидентом»](#);
- [Объединение группы событий в один инцидент](#).

#### **5.3.5.1. Перевод группы событий в статус «Новый инцидент»**

1. Перейти в реестр событий ИБ ([Рисунок 57](#)).
2. В перечне выбрать необходимые записи с помощью флага ☒.
3. Нажать кнопку .
4. Выбранные события будут переведены в статус «Новый инцидент».

#### **5.3.5.2. Перевод группы событий в статус «Не является инцидентом»**

1. Перейти в реестр событий ИБ ([Рисунок 57](#)).
2. В перечне выбрать необходимые записи с помощью флага ☒.
3. Нажать кнопку .
4. Откроется форма перевода в ложное срабатывание ([Рисунок 62](#)).

### Событие не является инцидентом

Комментарий \*

Текст

Подтвердить

Отменить

Рис. 62. Форма перевода события в ложное срабатывание

5. Заполнить поле «Комментарий» .

6. Нажать кнопку

Подтвердить

7. Текущий статус событий изменится на «Не является инцидентом».



#### Внимание:

Карточка события на статусе «Не является инцидентом» доступна только для чтения.

8. Для отмены перевода события в ложное срабатывание необходимо закрыть форму перевода или нажать на кнопку **Отменить**.

### 5.3.5.3. Объединение группы событий в один инцидент

1. Перейти в реестр событий ИБ ([Рисунок 57](#)).

2. В перечне выбрать необходимые записи с помощью флага ☒.

3. Нажать кнопку

Объединить в инцидент

4. Выбранные события будут объединены в инцидент: самое раннее из них перейдет в статус «Новый инцидент» (в качестве ответственного автоматически будет назначен текущей пользователь), остальные события из выборки станут связаны с инцидентом.

## 5.4. Управление инцидентами информационной безопасности

Инциденты ИБ могут быть обнаружены работниками Общества, а также автоматизированными системами и средствами защиты информации.

Для перехода к реестру инцидентов ИБ необходимо в боковом меню выбрать раздел «Инциденты ИБ» ([Рисунок 63](#)).

Реестр событий ИБ

Новое событие

Новые

Являются инцидентами

Не являются инцидентами

↺

↻

<input type="checkbox"/>	Дата и время возн... ↓	Номер	Наименование	Ответственн...	Источник события
<input type="checkbox"/>	28.09.2021 12:16:29	08.25.08/СИБ/1	Кража носителя информации	rmuzafarov	Персонал
<input type="checkbox"/>	28.09.2021 12:16:57	08.25.08/СИБ/2	Потеря данных	rmuzafarov	Персонал

5 10 20 50

Всего записей: 2 < 1 из 1 >

Не являются инцидентом

Являются инцидентом

Объединить в инцидент

Рис. 63. Информационная панель «Реестр инцидентов ИБ»

### 5.4.1. Создание записи об инциденте информационной безопасности

Для того чтобы создать запись об инциденте ИБ, пользователь должен выполнить следующие действия:

1. На информационной панели «Реестр инцидентов ИБ» нажать кнопку 

Новый инцидент

.
2. Откроется карточка нового инцидента (Рисунок 64).

## Инцидент ИБ

Наименование инцидента \*

Дата и время возникновения



Дата и время обнаружения



Дата и время оповещения



Класс инцидента \*



Подкласс инцидента \*



Тип инцидента



Ответственный за инцидент \*



Что произошло

Рис. 64. Карточка нового инцидента ИБ

3. В открывшейся форме заполнить доступные поля:

- Наименование инцидента;
- Класс инцидента;
- Подкласс инцидента;
- Тип инцидента;
- Что произошло.

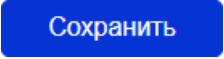
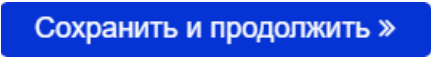
По умолчанию поля «Дата и время возникновения», «Дата и время обнаружения», «Дата и время оповещения» заполняются текущими значениями, в поле «Ответственный за инцидент» указывается текущий пользователь. При необходимости данные этих полей можно отредактировать.

**Внимание:**

Ответственный за инцидент может быть выбран только среди пользователей с ролью «Ответственный за инцидент ИБ».

4. После заполнения формы возможны следующие действия:



- для создания записи об инциденте и возврата в реестр инцидентов ИБ необходимо нажать кнопку ;
- для создания записи об инциденте и перехода в карточку этого инцидента необходимо нажать кнопку .

#### 5.4.2. Редактирование записи об инциденте информационной безопасности








Для того чтобы отредактировать карточку инцидента ИБ ([Рисунок 65](#)), пользователь должен выполнить следующие действия:

1. Перейти в карточку инцидента любым из следующих способов:
  - из перечня новых инцидентов информационной панели «Реестр инцидентов ИБ» (в боковом меню пользователя выбрать пункт «Инциденты ИБ»);
  - из таблицы «Инциденты информационной безопасности» стартовой страницы пользователя;
  - из перечня новых инцидентов ИБ на виджете «Инциденты информационной безопасности» (нажать счетчик новых инцидентов. *В данном перечне доступны только карточки со статусом «Новый инцидент»*).
2. На вкладке «Описание» при необходимости изменить значения доступных полей.



#### Внимание:

Поля карточки «Дата и время возникновения/обнаружения/оповещения», «Класс инцидента», «Подкласс инцидента», «Источник события», «Приоритет» и «Время реагирования» доступны для редактирования только на статусе «Новый инцидент».

3. Для добавления сотрудников, сообщивших об инциденте, на вкладке «Сообщившие сотрудники» в таблице «Сотрудники, сообщившие об инциденте»:
  - нажать кнопку ;
  - выбрать необходимые записи с помощью флага ;
  - нажать кнопку .
4. Для удаления связи с сообщившими сотрудниками на вкладке «Сообщившие сотрудники» нажать кнопку  в соответствующей строке.
5. Для добавления связанных объектов КИИ на вкладке «Пораженные объекты КИИ» в таблице «Пораженные объекты КИИ»:
  - нажать кнопку ;
  - выбрать необходимые записи с помощью флага ;
  - нажать кнопку .
6. Для добавления связанных бизнес-процессов на вкладке «Пораженные компоненты» в таблице «Бизнес-процессы»:

- нажать кнопку **+**;
- выбрать необходимые записи с помощью флага ☒;
- нажать кнопку **Сохранить**.

Рис. 65. Карточка инцидента ИБ

- Для удаления связи с бизнес-процессом на вкладке «Пораженные компоненты» нажать кнопку **✗** в соответствующей строке.
- Для добавления связанных объектов защиты на вкладке «Пораженные компоненты» в таблице «Информационные активы, программное обеспечение, технические средства»:
  - нажать кнопку **+**;
  - выбрать необходимые записи с помощью флага ☒;
  - нажать кнопку **Сохранить**.
- Для удаления связи с объектом защиты на вкладке «Пораженные компоненты» нажать кнопку **✗** в соответствующей строке.
- На вкладке «Пораженные компоненты» при необходимости заполнить поле «Другое».
- Для добавления связанных угроз на вкладке «Угрозы и уязвимости» в таблице «Выявленные угрозы»:
  - нажать кнопку **+**;
  - выбрать необходимые записи с помощью флага ☒;
  - нажать кнопку **Сохранить**.
- Для удаления связи с угрозой на вкладке «Угрозы и уязвимости» нажать кнопку **✗** в соответствующей строке.
- На вкладке «Угрозы и уязвимости» при необходимости заполнить поле «Выявленные уязвимости».
- Для добавления нарушителя или причастного лица на вкладке «Нарушители» (Рисунок 66):

- нажать кнопку **+**;
- выбрать тип нарушителя;
- указать мотивацию нарушителя;
- ввести описание нарушителя;
- нажать кнопку **Сохранить**;
- для отмены действия нажать **Отменить**.

Карточка нарушителя 🔍 ✕

---

### Сведения о нарушителе

Тип нарушителя \* Мотивация

Выберите тип нарушителя Укажите мотивацию

Описание нарушителя

Текст

**Сохранить** Отменить

Рис. 66. Ввод сведений о нарушителе

- Для удаления нарушителя на вкладке «Нарушители» нажать кнопку **✕** в соответствующей строке.
- Для добавления связанных событий и инцидентов ИБ на вкладке «Связанные инциденты и события»:
  - нажать кнопку **+**;
  - выбрать необходимые записи с помощью флага ☒;
  - нажать кнопку **Сохранить**.
- Для удаления связи с событием или инцидентом на вкладке «Связанные инциденты и события» нажать кнопку **✕** в соответствующей строке.
- Для добавления связанных нештатных ситуаций на вкладке «Связанные нештатные ситуации»:
  - нажать кнопку **+**;
  - выбрать необходимые записи с помощью флага ☒;
  - нажать кнопку **Сохранить**.
- Для удаления связи с нештатной ситуацией на вкладке «Связанные нештатные ситуации» нажать кнопку **✕** в соответствующей строке.
- Для добавления последствий инцидента ИБ на вкладке «Последствия» в таблице «Неблагоприятные воздействия инцидента на бизнес»:

- нажать кнопку **+**. Откроется форма добавления воздействия ([Рисунок 67](#));

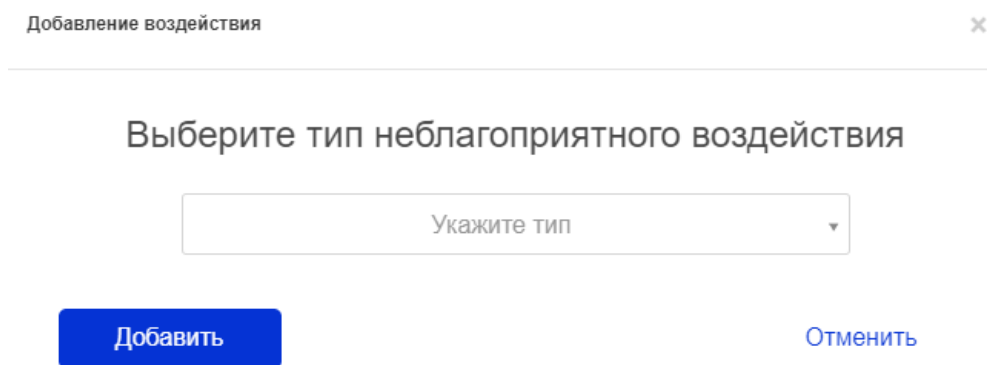




Рис. 67. Форма добавления неблагоприятного воздействия

- в выпадающем списке типов воздействия выбрать тип, нажать кнопку **Добавить**. В таблицу будет добавлена новая запись;
- в колонке «Значимость» указать уровень неблагоприятного воздействия по шкале от 1 до 10, в колонке «Категории» добавить категории воздействия, в колонку «Издержки» ввести действительные издержки;
- для сохранения изменений необходимо нажать кнопку .

21. Для добавления полных стоимостей восстановления после инцидента на вкладке «Последствия» в таблице «Полные стоимости восстановления после инцидента»:

- нажать кнопку **+**. В таблицу будет добавлена новая запись;
- в колонке «Значимость» указать общий уровень неблагоприятного воздействия по шкале от 1 до 10, в колонке «Категории» добавить категории воздействия, в колонку «Стоимость» ввести полную стоимость восстановления;
- для сохранения изменений необходимо нажать кнопку .

22. Для применения изменений без изменения статуса инцидента ИБ необходимо нажать кнопку **Сохранить**.

23. Для применения изменений и перехода к этапу формирования плана реагирования необходимо нажать кнопку **Перейти к плану мероприятий** (доступна только на статусе «Новый инцидент»). На карточке инцидента отобразится вкладка «План мероприятий» ([Рисунок 68](#)). В плане мероприятий автоматически добавятся мероприятия, входящие в сценарий, связанный с подклассом инцидента.

Общая информация
План мероприятий
История изменений

↺

+

📄

↻



№	Тип мероприятия	Описание	Ответственный за выполнение	Выполнить ↑ до
🔍	🔍 Выбрать...	🔍	🔍	🔍 📅

5
10
20
50

<
1
из 1
>


Рис. 68. Карточка инцидента ИБ. Вкладка «План мероприятий»

### 5.4.3. Формирование отчетных форм об инциденте информационной безопасности

1. Открыть карточку инцидента ИБ на вкладке «Описание» ([Рисунок 65](#)).
2. Нажать кнопку  рядом с полем «Отчет по инциденту» для формирования отчета.
3. Нажать кнопку  для скачивания сформированного отчета.



#### Внимание:

В случае изменения данных об инциденте ИБ необходимо обновить отчет, для этого повторно нажать кнопку .

### 5.4.4. Перевод инцидента в статус «Не является инцидентом»

1. Перейти в карточку нового инцидента.
2. Нажать кнопку Перевести в ложное срабатывание (доступна только на статусе «Новый инцидент»).
3. Откроется форма перевода инцидента в ложное срабатывание ([Рисунок 69](#)).



### Внимание:

Данное действие можно выполнить в случае, если текущий пользователь выбран Ответственным за событие с ролью «Ответственный за инцидент ИБ».

Комментарий при переводе в ложное из реестра. Инцидент



## Не является инцидентом

Комментарий \*

Текст

Подтвердить

Отменить

Рис. 69. Форма перевода инцидента в ложное срабатывание

4. Заполнить поле «Комментарий».

5. Нажать кнопку **Подтвердить**.

6. Текущий статус инцидента изменится с «Новый инцидент» на «Не является инцидентом».



### Внимание:

Карточка инцидента на статусе «Не является инцидентом» доступна только для чтения.

7. Для отмены перевода инцидента в ложное срабатывание необходимо закрыть форму перевода или нажать на кнопку **Отменить**.



### Прим.:

Перевод инцидентов в статус «Не является инцидентом» можно также осуществлять группами - см. [Перевод группы инцидентов в статус «Не является инцидентом»](#).

#### 5.4.4.1. Перевод группы инцидентов в статус «Не является инцидентом»

1. Перейти в реестр инцидентов ИБ ([Рисунок 63](#)).
2. В перечне выбрать необходимые записи с помощью флага ☒.
3. Нажать кнопку [Не является инцидентом](#). Откроется форма перевода в ложное срабатывание ([Рисунок 69](#)).



**Внимание:**

Данное действие можно выполнить в случае, если текущий пользователь выбран Ответственным за событие с ролью «Ответственный за инцидент ИБ».

4. Заполнить поле «Комментарий».
5. Нажать кнопку [Подтвердить](#).
6. Текущий статус инцидентов изменится с «Новый инцидент» на «Не является инцидентом».



**Внимание:**

Карточка инцидента на статусе «Не является инцидентом» доступна только для чтения.

7. Для отмены перевода инцидентов в ложное срабатывание необходимо закрыть форму перевода или нажать на кнопку [Отменить](#).

#### 5.4.5. Формирование плана реагирования на инцидент информационной безопасности

Сформировать план реагирования на инцидент ИБ можно двумя способами:

1. добавить мероприятия из [справочника](#) (см. раздел [Добавление мероприятия из справочника](#));
2. добавить новое мероприятие (см. раздел [Добавление нового мероприятия](#)).

После формирования списка мероприятий по реагированию на инцидент необходимо завершить формирование плана ([Завершение формирования плана реагирования](#)).

##### 5.4.5.1. Добавление мероприятия из справочника

1. Перейти в карточку инцидента.
2. На вкладке «План мероприятий» (доступна только на этапе формирования плана реагирования) Нажать кнопку [Выбрать из справочника](#).
3. Заполнить форму добавления мероприятия из справочника ([Рисунок 70](#)):

- указать тип мероприятия;
- выбрать нужное мероприятие из выпадающего списка;
- назначить ответственного за выполнение мероприятия.



#### Внимание:

Ответственный за выполнение мероприятия может быть выбран только среди пользователей, входящих в группу реагирования на инцидент ИБ.

4. Нажать кнопку

**Сохранить**

5. Выбранное мероприятие будет добавлено в план реагирования. Поле «Выполнить до» автоматически будет заполнено датой завершения реагирования на инцидент. При необходимости данные этих полей можно отредактировать.



#### Внимание:

После перехода к этапу реагирования и расследования добавленные мероприятия будут доступны только для чтения. Для отмены действия необходимо закрыть форму перевода или нажать на кнопку **Отменить**.

Добавление мероприятия



Тип мероприятия \*

Текст

Мероприятия ИБ

Текст

Ответственный \*

**Сохранить**

**Отменить**

Рис. 70. Форма добавления мероприятия из справочника

#### 5.4.5.2. Добавление нового мероприятия

Для добавления в план реагирования нового мероприятия пользователь должен выполнить следующие действия:





1. На вкладке «План мероприятий» нажать кнопку **+**. В таблице отобразится пустая строка.
2. Из выпадающего списка выбрать тип мероприятия, ввести его описание, указать срок и ответственного за выполнение.




**Внимание:**

Ответственный за выполнение мероприятия может быть выбран только среди пользователей, входящих в группу реагирования на инцидент ИБ.

3. Для сохранения изменений необходимо нажать кнопку . Чтобы сбросить изменения нажмите кнопку .
4. Для удаления мероприятия на вкладке «План мероприятий» нажать кнопку **×** в соответствующей строке.

#### 5.4.5.3. Завершение формирования плана реагирования

Для отправки сформированного плана на утверждение пользователь должен выполнить следующие действия:

На вкладке «План мероприятий» нажать кнопку . После завершения формирования плана реагирования возможно следующее:

1. если включена настройка согласования плана реагирования на инцидент, текущий план реагирования на инцидент ИБ будет отправлен на утверждение. Пользователям с ролью «Руководство САОБ» будет отправлено уведомление о необходимости утверждения плана. Вкладка «План мероприятий» в карточке инцидента станет недоступной для редактирования. После утверждения или возврата на корректировку плана реагирования (осуществляет пользователь с ролью «Руководство САОБ») пользователю ответственному за обработку инцидента будет отправлено соответствующее уведомление. Если при возврате плана реагирования на корректировку были указаны какие-то рекомендации, они станут доступны для чтения на вкладке «План мероприятий» в карточке инцидента по ссылке на форму просмотра комментариев ([Рисунок 71](#)).

Комментарий	Автор комментария	Дата ↓
🔍	🔍	🔍 📅
Увеличить срок выполнения мероприятий	kkudryashova	13.01.2020 15:22:05
Описать мероприятия подробнее	kkudryashova	13.01.2020 14:50:59

< 1 из 1 >

Рис. 71. Форма просмотра комментария при возврате плана реагирования на корректировку

После утверждения плана реагирования на пользователей, которые назначены ответственными за выполнения мероприятий, будут назначены задачи и отправлены уведомления. На карточке инцидента отобразится вкладка «Реагирование и расследование» (Рисунок 72) с перечнем мероприятий по реагированию и расследованию, сгруппированным по статусу. Для просмотра карточки мероприятия необходимо дважды щелкнуть левой кнопкой мыши по нужной записи (информация о мероприятии доступна только для чтения);


- если настройка согласования плана реагирования на инцидент отключена, текущий статус инцидента изменится на «Реагирование и расследование». На пользователей, которые назначены ответственными за выполнения мероприятий, будут назначены задачи и отправлены уведомления, минуя этап утверждения плана реагирования. На карточке инцидента отобразится вкладка «Реагирование и расследование» (Рисунок 72) с перечнем мероприятий по реагированию и расследованию, сгруппированным по статусу.

< 1 M3 1 >

- 67 -

4. Согласно утвержденному плану реагирования на пользователей, которые назначены ответственными за выполнения новых мероприятий, будут назначены задачи и отправлены уведомления.
5. Статус инцидента изменится с «Новый инцидент» на «Реагирование и расследование», на карточке инцидента отобразится вкладка «Реагирование и расследование» ([Рисунок 72](#)) с перечнем мероприятий по реагированию и расследованию, сгруппированным по статусу.

#### 5.4.5.6. Возврат на корректировку плана реагирования на инцидент информационной безопасности

1. В карточке плана реагирования нажать кнопку .
2. Откроется форма ввода комментария ([Рисунок 73](#)).

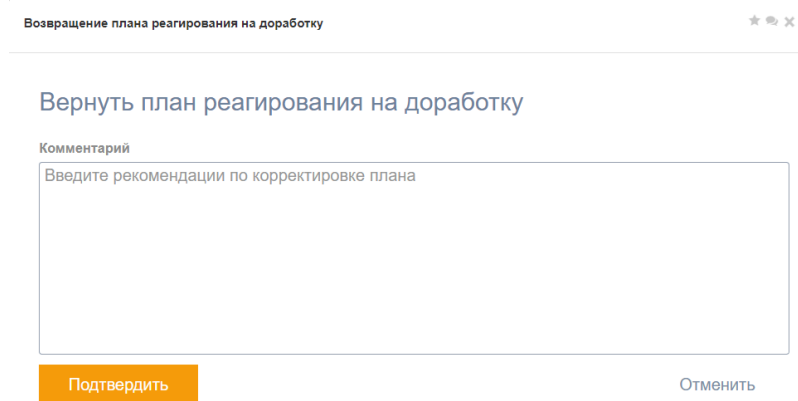
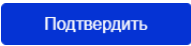





Рис. 73. Форма ввода комментария при  
возврате плана реагирования на корректировку

3. Ввести рекомендации по корректировке плана реагирования.
4. Нажать кнопку .
5. План реагирования будет возвращен на корректировку. Пользователю, ответственному за обработку инцидента, будет отправлено уведомление о необходимости корректировки плана реагирования на инцидент. В карточке инцидента план реагирования станет доступен для редактирования.
6. Для отмены возврата плана реагирования на корректировку нажать кнопку [Отменить](#).

#### 5.4.5.7. Работа с задачами по реагированию и расследованию инцидента информационной безопасности

Переход в карточку задачи осуществляется одним из следующих способов:

- на стартовой странице на виджете с перечнем задач (вкладка «Назначенные на меня») дважды нажать по строке с задачей или по кнопке ;
- перейти в системный раздел «Задачи» по кнопке  Задачи **1** на верхней панели и на вкладке «Назначенные на меня» дважды нажать по строке с задачей или по кнопке .

Содержание карточки рассматривается подробнее в разделе [Описание карточки задачи](#).

Порядок выполнения задач описан в разделе [Выполнение задачи](#).

#### 5.4.5.7.1. Описание карточки задачи

1. Карточка задачи состоит из трех разделов:

- общая информация о задаче;
- информация о мероприятии;
- информация об инциденте.

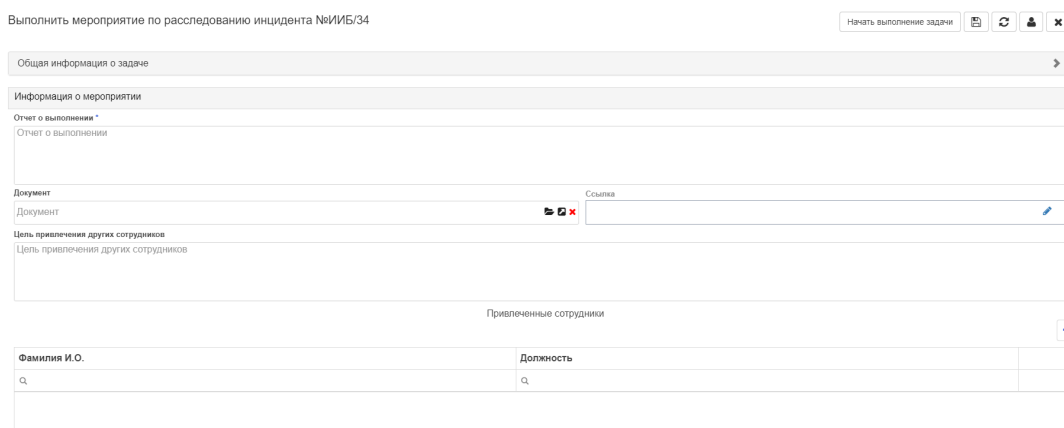


Рис. 74. Карточка задачи по реагированию на инцидент

В разделе «Общая информация» ([Рисунок 75](#)) расположена служебная информация о задаче, недоступная для редактирования.

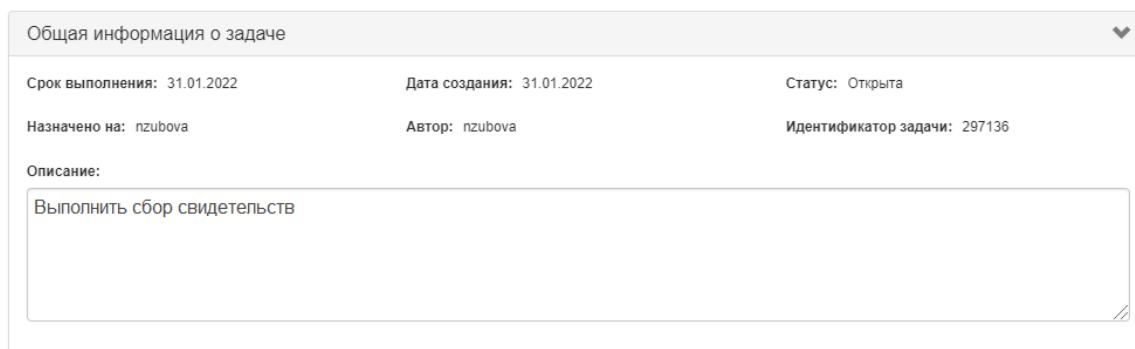


Рис. 75. Раздел «Общая информация» в карточке задачи

В разделе «Информация о мероприятии по реагированию» ([Рисунок 76](#)) расположена информация о результатах выполнения реагирования на инцидент ИБ.

Информация о мероприятии

Отчет о выполнении \*

Отчет о выполнении

Документ

Документ

Ссылка

Цель привлечения других сотрудников

Цель привлечения других сотрудников

Привлеченные сотрудники

+

Фамилия И.О.	Должность
q	q

Рис. 76. Раздел «Информация о мероприятии по реагированию» в карточке задачи

В разделе «Информация об инциденте» (Рисунок 77) расположена служебная информация о соответствующем задаче инциденте ИБ, недоступная для редактирования.

Информация об инциденте

Инцидент ИБ № ИИБ/34

Приоритет: Низкий

Срок реагирования до: 03.02.2022 10:36:40

Наименование: Инцидент для демонстрации

Описание

Дата и время

Дата и время возникновения: 31.01.2022 10:36:40

Дата и время обнаружения: 31.01.2022 10:36:40

Дата и время оповещения: 31.01.2022 10:36:40

Время реагирования, ч: 72

Подкласс инцидента: Прочие инциденты

Класс инцидента: Прочие инциденты

Источники события: Персонал

Тип инцидента: Действительный

Вид инцидента: Вид инцидента

Ответственный: nzubova

Что произошло: Текст

Как произошло: Текст

Почему произошло: Текст

Рис. 77. Раздел «Информация об инциденте» в карточке задачи

#### 5.4.5.7.2. Выполнение задачи

1. Нажать кнопку Начать выполнение задачи в верхней части карточки задачи. Задача перейдет на статус «В работе».
2. В разделе «Информация о мероприятии по реагированию» (Рисунок 76):
  - Ввести текст отчета о выполнении.
  - Загрузить отчетный материал с помощью кнопки в поле «Документ».

- Указать привлеченных к реагированию работников:
  - нажать кнопку **+**;
  - во всплывающем окне с помощью флага ☒ выбрать работников ([Рисунок 78](#));
  - нажать на кнопку **Сохранить**.

Выбор элементов

✕

<input type="checkbox"/>	Фамилия И.О.	Должность	Подразделение
<input type="checkbox"/>	Гусаров Р. С.	Главный специалист	Служба информационной безопасности
<input type="checkbox"/>	Краснова А. С.	Аналитик	Служба информационной безопасности
<input type="checkbox"/>	Панаев Ф. В.	Заместитель руководителя	Отдел маркетинга
<input type="checkbox"/>	Председатель К. К.	Руководитель проекта разработки	Департамент информационных технологий
<input checked="" type="checkbox"/>	Самойлова Е. В.	Ведущий специалист	Администрация
<input checked="" type="checkbox"/>	Федоров И. О.	Руководитель департамента	Коммерческий департамент
<input type="checkbox"/>	Эксперт О. З.	Главный эксперт	Служба информационной безопасности
<input type="checkbox"/>	Степанова Н. Д.	Специалист	Административно-хозяйственный отдел

1

2

3

4

5


...

606

Сохранить



Рис. 78. Окно для выбора привлеченных к реагированию работников

3. После корректировки информации о результатах выполнения мероприятия пользователю доступны следующие действия:



- для сохранения изменений без изменения статуса задачи необходимо нажать кнопку ;
- для сохранения изменений с закрытием задачи по реагированию на инцидент ИБ необходимо нажать на кнопку **Завершить выполнение задачи**.

Когда задача будет закрыта, статус мероприятия изменится с «Выполняется» на «Выполнено», а сама задача на стартовой странице и в системном разделе «Задачи» будет отображаться на вкладке «Выполненные».

#### 5.4.5.8. Загрузка документов

1. Откройте карточку инцидента ИБ на вкладке «Документы».
2. Нажмите кнопку **+**.
3. Введите наименование документа.
4. С помощью кнопки  загрузите файл.
5. Для сохранения нажмите . Поля «Кто загрузил» и «Дата загрузки» заполнятся автоматически.
6. Для удаления документа нажмите **✗**.

Общая информация	Выполненные мероприятия	Документы	Заключение	История изменений
------------------	-------------------------	-----------	------------	-------------------





Наименование	Файл документа	Комментарий	Кто загрузил	Дата загрузки	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
					 

Рис. 79. Карточка инцидента ИБ. Документы

#### 5.4.5.9. Завершение реагирования и расследования инцидента информационной безопасности

1. На вкладке «Реагирование и расследование» нажать кнопку **Завершить реагирование »**.



##### Прим.:






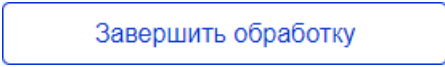
Кнопка станет доступна только после выполнения всех мероприятий из плана реагирования. О выполнении всех мероприятий ответственному за инцидент будет отправлено уведомление.

2. Текущий статус инцидента изменится с «Реагирование и расследование» на «Формирование заключения».
3. На карточке инцидента отобразится вкладка «Заключение», добавятся вкладки «Выполненные мероприятия» и «Документы».

#### 5.4.5.10. Формирование заключения по инциденту

1. Перейти в карточку инцидента любым из следующих способов:
  - из перечня инцидентов информационной панели «Реестр инцидентов ИБ», находящихся в работе (в боковом меню пользователя выбрать пункт «Инциденты ИБ», перейти на вкладку «В работе»);
  - из таблицы «Инциденты информационной безопасности» стартовой страницы пользователя.



2. На вкладке «Заключение» заполнить доступные поля.
3. Для добавления связанных документов на вкладке «Документы»:
  - нажать кнопку . В таблице отобразится пустая строка;
  - ввести наименование документа и дату публикации;
  - для загрузки файла:
    - в колонке «Документ» нажать кнопку  и загрузить необходимый файл;
    - для сохранения изменений нажать кнопку ;
    - для отмены действия нажмите кнопку .
  - для удаления документа нажать кнопку  в соответствующей строке.
4. Для завершения этапа формирования заключения и закрытия инцидента необходимо на вкладке «Заключение» нажать кнопку  (доступна только на статусе «Формирование заключения»).


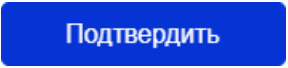

После завершения обработки возможно следующее:

- если включена настройка согласования закрытия инцидента, текущий статус инцидента изменится с «Формирование заключения» на «Ожидает закрытия». Пользователям с ролью «Руководство САОБ» будет отправлено уведомление о необходимости закрыть инцидент.

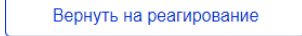
После закрытия или возврата инцидента на доработку (осуществляет пользователь с ролью «Руководство САОБ») будут отправлены соответствующие уведомления;

- если настройка согласования закрытия инцидента отключена, текущий статус инцидента изменится с «Формирование заключения» на «Инцидент закрыт». Лицам, указанным в таблице «Оповещаемые лица/субъекты внутри организации», будут отправлены уведомления о закрытии инцидента. Карточка инцидента за исключением вкладки «Документы» станет доступна только для чтения.


#### **5.4.5.10.1. Перевод инцидента в ложное срабатывание**

1. Для перевода инцидента ИБ в ложное срабатывание со статуса «Формирование заключения» необходимо на вкладке «Заключение» нажать кнопку  (доступна только на статусе «Формирование заключения»).
2. Откроется форма перевода инцидента в ложное срабатывание (Рис. 1). Заполнить поле «Комментарий» и нажать кнопку .
3. Текущий статус инцидента изменится с «Формирование заключения» на «Не является инцидентом». Карточка инцидента станет доступна только для чтения.
4. Для отмены перевода инцидентов в ложное срабатывание необходимо закрыть форму перевода или нажать на кнопку .

#### 5.4.5.10.2. Возврат инцидента на этап расследования и реагирования

1. На вкладке «Заключение» нажать кнопку  (доступна только на статусе «Формирование заключения»).
2. Текущий статус инцидента изменится с «Формирование заключения» на «Реагирование и расследование».
3. В карточке инцидента станет доступно добавление мероприятий по реагированию (см. раздел «Реагирование и расследование на инцидент информационной безопасности»). Вкладка «Заключение» станет недоступной.





#### 5.4.5.11. Закрытие инцидента ИБ

1. Перейти в карточку инцидента любым из следующих способов:
  - из перечня инцидентов информационной панели «Реестр инцидентов ИБ», находящихся в работе (в боковом меню пользователя выбрать пункт «Инциденты ИБ», перейти на вкладку «В работе»);
  - из таблицы «Инциденты информационной безопасности» стартовой страницы пользователя;
  - по ссылке из уведомления о необходимости закрытия инцидента;
  - из перечня инцидентов, ожидающих закрытия, на виджете «Реагирование на инциденты» (нажать счетчик инцидентов, ожидающих закрытия. В данном перечне доступны только карточки со статусом «Ожидает закрытия»).
2. На вкладке «Заключение» нажать кнопку  (доступна только на статусе «Ожидает закрытия»).



#### Внимание:

После закрытия инцидента карточка инцидента за исключением вкладки «Документы» станет доступна только для чтения.

3. Откроется форма выбора оповещаемых лиц ([Рисунок 80](#)). В список оповещаемых лиц будут автоматически добавлены сотрудники, проводившие расследование и реагирование на инцидент, а также руководитель ГРИИБ.
4. Для добавления оповещаемых лиц на форме «Выбор оповещаемых лиц»:
  - нажать кнопку ;
  - выбрать необходимые записи с помощью флага ;
  - нажать кнопку .
5. Для удаления сотрудника из списка оповещаемых лиц нажать кнопку  в соответствующей строке.

Выберите работников для отправки уведомления о закрытии инцидента

+
📄
↺

ФИО	Должность	Подразделение	Email
🔍	🔍	🔍	🔍

Уведомить и закрыть инцидент
Закрыть инцидент
Отменить

Рис. 80. Форма выбора оповещаемых лиц

6. После заполнения формы возможны следующие действия:

- для закрытия инцидента и отправки уведомлений выбранным сотрудникам нажать кнопку Уведомить и закрыть инцидент. Текущий статус инцидента изменится с «Формирование заключения» на «Инцидент закрыт». Указанным лицам будут отправлены оповещения о закрытии инцидента;
- для закрытия инцидента без отправки уведомлений нажать кнопку Закрыть инцидент. Текущий статус инцидента изменится с «Формирование заключения» на «Инцидент закрыт»;
- для отмены действия необходимо закрыть форму выбора оповещаемых лиц или нажать на кнопку Отменить.

#### 5.4.5.11.1. Возврат инцидента ИБ в работу

1. Для возврата инцидента в работу необходимо на вкладке «Заключение» нажать кнопку Вернуть в работу (доступна только на статусах «Инцидент закрыт» и «Не является инцидентом»).
2. Текущий статус инцидента изменится на «Формирование заключение».
3. Пользователю, ответственному за обработку инцидента, будет отправлено соответствующее уведомление.

## 5.5. Мониторинг и контроль управления инцидентами ИБ

Для мониторинга статистической информации по зарегистрированным событиям и инцидентам ИБ пользователь с ролью «Руководство САОБ» имеет доступ к просмотру формы со статистикой (Рисунок 81). Подробное описание формы приведено в разделе «Стартовая страница пользователя» роли «Эксперт УКИНС».

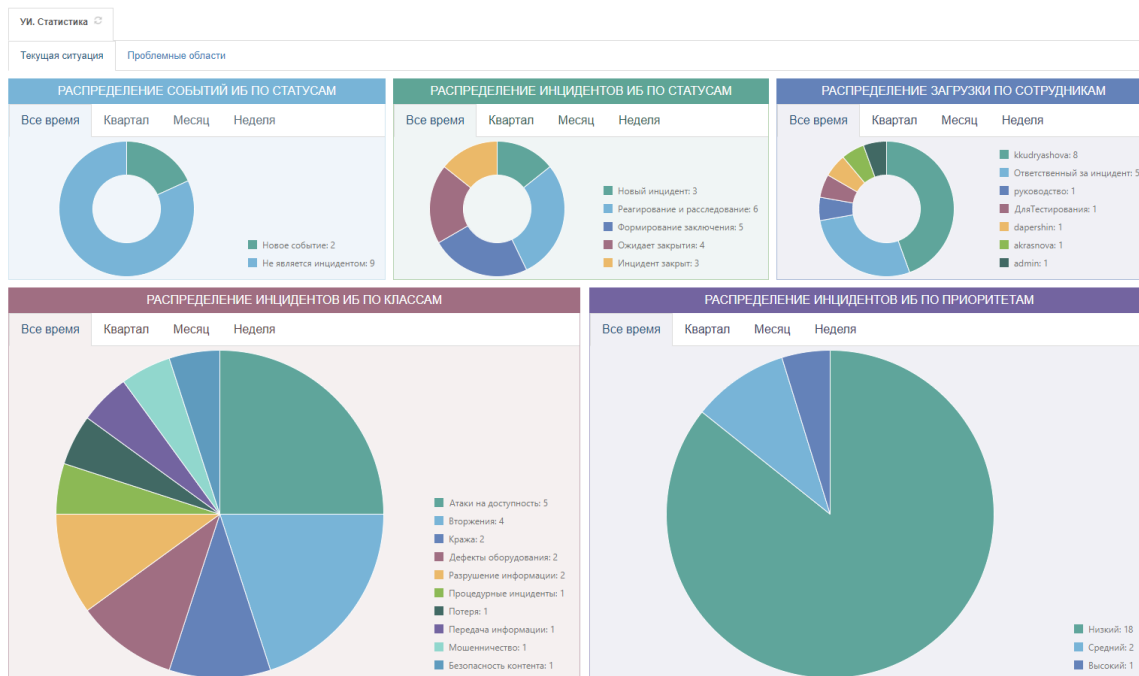


Рис. 81. Форма для просмотра статистики по зарегистрированным событиям и инцидентам

## 5.6. Управление нештатными ситуациями

Нештатные ситуации (далее - НС) регистрируются в системе работниками Общества.

### 5.6.1. Создание записи о нештатной ситуации

1. Перейти в реестр «Нештатные ситуации».
2. Для создания новой НС нажать кнопку «Добавить нештатную ситуацию».
3. В открывшейся карточке создания НС заполнить данные (Рисунок 82): наименование, вид и тип нештатной ситуации, описать суть НС в поле «Что произошло».

Даты и ответственный заполняются автоматически. При необходимости ответственного за НС можно изменить.

4. Сохранить карточку НС с помощью кнопок «Сохранить и выйти» или «Сохранить и продолжить».

## Нештатная ситуация

Наименование нештатной ситуации \*

Наименование

Дата и время возникновения

08.01.2022 09:22:39



Дата и время обнаружения

08.01.2022 09:22:39



Дата и время оповещения

08.01.2022 09:22:39



Вид нештатной ситуации \*

Вид нештатной ситуации

Тип нештатной ситуации

Действительный



Ответственный за нештатную ситуацию \*

nzubova



Что произошло

Сохранить

Сохранить и продолжить »

Рис. 82. Регистрация новой нештатной ситуации

## 5.6.2. Редактирование записи о нештатной ситуации

1. Перейти в карточку НС (Рисунок 83).

Нештатная ситуация **НС/5** приоритет Низкий срок реагирования 11.01.2022 09:33:42 [Новая нештатная ситуация](#)







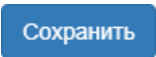







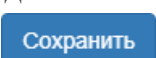




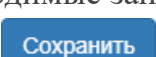

Нештатная ситуация

Общая информация	История изменений
<p><b>Описание</b></p> <p>Сообщение сотруднику</p> <p>Пораженные компоненты</p> <p>Угрозы и уязвимости</p> <p>Связанные события</p> <p>Связанные инциденты</p> <p>Последствия</p>	<p><b>Дата и время</b></p> <p>Дата и время возникновения * 08.01.2022 09:33:42</p> <p>Дата и время обнаружения * 08.01.2022 09:33:42</p> <p>Дата и время оповещения 08.01.2022 09:33:42</p> <p>Время реагирования, ч 72</p> <p><b>Характеристика нештатной ситуации</b></p> <p>Тип нештатной ситуации Действительный</p> <p>Вид нештатной ситуации * Антропогенное воздействие</p> <p><b>Ответственный</b></p> <p>Подразделение</p> <p>Ответственный за нештатную ситуацию * nzubova</p> <p>Приоритет Низкий</p> <p><b>Подробности о нештатной ситуации</b></p> <p>Что произошло</p> <p>Как произошло</p>

Сохранить [Перейти к плану мероприятия](#)

Рис. 83. Редактирование карточки НС

2. На вкладке «Описание» при необходимости изменить значения доступных полей.

3. Для добавления сотрудников, сообщивших об инциденте, на вкладке «Сообщившие сотрудники»:
  - нажать кнопку ;
  - выбрать необходимые записи с помощью флага ;
  - нажать кнопку .
4. Для удаления связи с сообщившими сотрудниками на вкладке «Сообщившие сотрудники» нажать кнопку  в соответствующей строке.
5. Для добавления связанных бизнес-процессов на вкладке «Пораженные компоненты» в таблице «Бизнес-процессы»:
  - нажать кнопку ;
  - выбрать необходимые записи с помощью флага ;
  - нажать кнопку .
6. Для удаления связи с бизнес-процессом на вкладке «Пораженные компоненты» нажать кнопку  в соответствующей строке.
7. Для добавления связанных объектов защиты на вкладке «Пораженные компоненты» в таблице «Информационные активы, программное обеспечение, технические средства»:
  - нажать кнопку ;
  - выбрать необходимые записи с помощью флага ;
  - нажать кнопку .
8. Для удаления связи с объектом защиты на вкладке «Пораженные компоненты» нажать кнопку  в соответствующей строке.
9. На вкладке «Пораженные компоненты» при необходимости заполнить поле «Другое».
10. Для добавления связанных угроз на вкладке «Угрозы и уязвимости» в таблице «Выявленные угрозы»:
  - нажать кнопку ;
  - выбрать необходимые записи с помощью флага ;
  - нажать кнопку .
11. Для удаления связи с угрозой на вкладке «Угрозы и уязвимости» нажать кнопку  в соответствующей строке.
12. На вкладке «Угрозы и уязвимости» при необходимости заполнить поле «Выявленные уязвимости». Для удаления нарушителя на вкладке «Нарушители» нажать кнопку  в соответствующей строке.
13. Для добавления связанных событий ИБ на вкладке «Связанные события»:
  - нажать кнопку ;
  - выбрать необходимые записи с помощью флага ;
  - нажать кнопку .
14. Для удаления связи с событием на вкладке «Связанные события» нажать кнопку  в соответствующей строке.
15. Для добавления связанных инцидентов ИБ на вкладке «Связанные инциденты»:

- нажать кнопку **+**;
  - выбрать необходимые записи с помощью флага ☒;
  - нажать кнопку **Сохранить**.
16. Для удаления связи с инцидентом на вкладке «Связанные события» нажать кнопку **✗** в соответствующей строке.
17. Для удаления связи с событием или инцидентом на вкладке «Связанные инциденты и события» нажать кнопку **✗** в соответствующей строке.
18. Для добавления последствий инцидента ИБ на вкладке «Последствия» в таблице «Неблагоприятные воздействия инцидента на бизнес»:
- нажать кнопку **+**;
  - в выпадающем списке типов воздействия выбрать тип, нажать кнопку **Добавить** (Рисунок 84);

Добавление воздействия ✕

---

Выберите тип неблагоприятного воздействия

Добавить
Отменить

Рис. 84. Форма добавления неблагоприятного воздействия

- в таблицу будет добавлена новая запись;
  - в колонке «Значимость» указать уровень неблагоприятного воздействия по шкале от 1 до 10;
  - в колонке «Категории» добавить категории воздействия;
  - в колонку «Издержки» ввести действительные издержки;
  - для сохранения изменений необходимо нажать кнопку **💾**.
19. Для добавления полных стоимостей восстановления после инцидента на вкладке «Последствия» в таблице «Полные стоимости восстановления после инцидента»:
- нажать кнопку **+**;
  - в колонке «Значимость» указать общий уровень неблагоприятного воздействия по шкале от 1 до 10;
  - в колонке «Категории» добавить категории воздействия;
  - в колонку «Стоимость» ввести полную стоимость восстановления;
  - для сохранения изменений необходимо нажать кнопку **💾**.
20. Для применения изменений без изменения статуса НС необходимо нажать кнопку **Сохранить**.
21. Для применения изменений и перехода к этапу формирования плана реагирования необходимо нажать кнопку **Перейти к плану мероприятий**.

### 5.6.3. Формирование плана реагирования на нештатную ситуацию

1. Перейти в карточку НС на вкладку «План мероприятий».

Способы формирования плана аналогичны работе с инцидентами ИБ - см. [Добавление мероприятия из справочника](#), [Добавление нового мероприятия](#).





2. Завершить формирование плана с помощью кнопки .






План перейдет в статус «Реагирование и расследование».

### 5.6.4. Работа с задачами по реагированию и расследованию нештатной ситуации

Выполнение задач по нештатным ситуациям осуществляется аналогично задачам по реагированию и расследованию инцидентов ИБ - см. раздел [Работа с задачами по реагированию и расследованию инцидента информационной безопасности](#).

### 5.6.5. Загрузка документов

1. Откройте карточку нештатной ситуации на вкладке «Документы».
2. Нажмите кнопку .
3. Введите наименование документа.
4. С помощью кнопки  загрузите файл.
5. Для сохранения нажмите . Поля «Кто загрузил» и «Дата загрузки» заполнятся автоматически.
6. Для удаления документа нажмите .

Общая информация					
Выполненные мероприятия					
Документы					
Заключение					
История изменений					
 					
Наименование	Файл документа	Комментарий	Кто загрузил	Дата загрузки	
🔍	🔍	🔍	🔍	🔍 📅	
					 



### 5.6.6. Завершение реагирования и расследования нештатной ситуации

1. На вкладке «Реагирование и расследование» нажать кнопку .



**Прим.:**

Кнопка станет доступна только после выполнения всех мероприятий из плана реагирования. О выполнении всех мероприятий ответственному за инцидент будет отправлено уведомление.

2. Текущий статус НС изменится с «Реагирование и расследование» на «Формирование заключения».
3. На карточке НС отобразится вкладка «Заключение», добавятся вкладки «Выполненные мероприятия» и «Документы».





### 5.6.7. Завершение обработки нештатной ситуации

1. Перейти в карточку НС в статусе «Формирование заключения».
2. На вкладке «Заключение» заполнить доступные поля.



**Прим.:**

Поля «Значимость нештатной ситуации» и «Итоги расследования нештатной» ситуации являются обязательными.

3. Для добавления лиц и субъектов, которым будут отправлены оповещения о закрытии НС:
  - нажать кнопку  над таблицей «Оповещаемые лица/субъекты внутри организации»;
  - выбрать необходимые записи с помощью флага .
  - нажать кнопку .
4. Для добавления связанных документов на вкладке «Документы»:
  - нажать кнопку .
  - ввести наименование документа и дату публикации;
  - для загрузки файла:





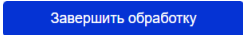
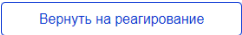
- в колонке «Документ» нажать кнопку  и загрузить необходимый файл;
  - для сохранения изменений нажать кнопку ;
  - для отмены действия нажмите кнопку .
  - для удаления документа нажать кнопку  в соответствующей строке.
5. Для завершения этапа формирования заключения и закрытия инцидента необходимо на вкладке «Заключение» нажать кнопку  (доступна только на статусе «Формирование заключения»).

Рис. 86. Карточка НС. Заключение

### 5.6.8. Возврат нештатной ситуации в работу

1. Для возврата НС в работу необходимо на вкладке «Заключение» нажать кнопку  (доступна только на статусах «Формирование заключения» и «Обработка завершена»).
2. Текущий статус НС изменится на «Реагирование и расследование».
3. Пользователю, ответственному за обработку НС, будет отправлено соответствующее уведомление.