

ООО «УЦСБ»

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Модуль ePlat4m «Управление инцидентами ИБ»

Екатеринбург
2021

Содержание

1 Введение	4
1.1 Область применения	4
1.2 Рабочие процессы	4
1.3 Структура модуля	4
2 Назначение и цели создания	5
3 Описание функциональных характеристик	6
4 Подготовка к работе	7
5 Ролевая структура модуля	8
6 Сценарии работы пользователей	9
6.1 Роль «Эксперт по управлению инцидентами ИБ»	9
6.1.1 Стартовая страница пользователя	9
6.1.2 Работа со справочниками.....	14
6.1.3 Формирование группы реагирования на инциденты ИБ	31
6.2 Роль «Ответственный за инцидент ИБ»	32
6.2.1 Стартовая страница пользователя.....	33
6.2.2 Управление событиями информационной безопасности	37
6.2.3 Управление инцидентами информационной безопасности	43
6.3 Роль «Руководство СУИБ»	60
6.3.1 Стартовая страница пользователя.....	60
6.3.2 Управление событиями и инцидентами ИБ.....	66
6.3.3 Утверждение и возврат на корректировку плана реагирования на инцидент информационной безопасности	66
6.3.4 Закрытие и возврат на доработку инцидента ИБ	70
6.3.5 Работа со справочниками.....	72
6.3.6 Мониторинг и контроль управления инцидентами ИБ	72
6.4 Роль «Участник ГРИИБ»	73
6.4.1 Стартовая страница пользователя.....	73

6.4.2 Работа с задачами по реагированию и расследованию инцидента информационной безопасности.....	75
6.5 Роль «Оператор-диспетчер»	79
6.5.1 Стартовая страница пользователя.....	80
6.5.2 Создание и удаление новой записи о событии информационной безопасности.....	80
6.5.3 Создание и удаление записи об инциденте информационной безопасности.....	81
6.6 Роль «САПУИБ»	83
6.6.1 Стартовая страница пользователя.....	83
7 Перечень сокращений.....	85

1 Введение

1.1 Область применения

Настоящий документ пользователя устанавливает порядок работы с модулем «Управление инцидентами ИБ» (далее – модуль УИИБ).

1.2 Рабочие процессы

Модуль реализует следующие рабочие процессы:

- регистрация, обработка и учет событий и инцидентов ИБ;
- выгрузка отчетных форм по событиям и инцидентам ИБ.

1.3 Структура модуля

Модуль «Управление инцидентами информационной безопасности» состоит из следующих разделов:

1. События и инциденты ИБ;
2. Планы реагирования на инциденты ИБ;
3. Справочники.

2 Назначение и цели создания

В модуле УИИБ осуществляется выполнение следующих функций:

1. Формирование группы реагирования на инциденты ИБ;
2. Регистрация и учёт событий и инцидентов ИБ;
3. Обработка событий и инцидентов ИБ, управление процессом реагирования и расследования инцидентов ИБ;
4. Выполнение задач по реагированию и расследованию инцидентов ИБ;
5. Формирование типовых сценариев по реагированию и расследованию инцидентов ИБ;
6. Анализ статистических данных.

3 Описание функциональных характеристик

1. Учет событий и инцидентов ИБ	<ul style="list-style-type: none">– ведение классификации инцидентов;– регистрация событий и инцидентов;– мониторинг статусов инцидентов.
2. Обработка событий и инцидентов	<ul style="list-style-type: none">– формирование плана мероприятий по реагированию на инцидент;– выполнение задач по реагированию и расследованию;– контроль за выполнением мероприятий.
3. Сбор данных о событиях и инцидентах	<ul style="list-style-type: none">– сбор данных о количестве событий и инцидентов;– сбор данных о статусе инцидентов;– сбор данных о текущих задачах по инцидентам.

4 Подготовка к работе

Для начала работы с модулем «Управление инцидентами ИБ» 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.

5 Ролевая структура модуля

В модуле УИИБ пользователь может иметь следующие роли:

Таблица 1 – Функциональные роли

Функциональная роль	Функция
Эксперт по управлению инцидентами ИБ	Формирование группы реагирования на инциденты ИБ
	Формирование типовых сценариев по реагированию и расследованию инцидентов ИБ
Участник ГРИИБ	Выполнение задач по реагированию и расследованию инцидентов ИБ
Ответственный за инцидент ИБ	Регистрация и учёт событий и инцидентов ИБ
	Обработка событий и инцидентов ИБ, управление процессом реагирования и расследования инцидентов ИБ
	Формирование типовых сценариев по реагированию и расследованию инцидентов ИБ
Оператор-диспетчер	Регистрация и учёт событий и инцидентов ИБ
САПУИБ (системная роль)	Анализ статистических данных
Руководство СУИБ	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
	Формирование типовых сценариев по реагированию и расследованию инцидентов ИБ
	Анализ статистических данных

Настоящая инструкция описывает порядок действий пользователей модуля УИИБ (далее – Модуль) при выполнении своих задач, которые соответствуют назначенным на пользователей ролям.

При работе с Модулем пользователи должны руководствоваться инструкциями, описанными в соответствующих разделах данного Руководства.

6 Сценарии работы пользователей

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

6.1 Роль «Эксперт по управлению инцидентами ИБ»

Задача пользователя в роли «Эксперт по управлению инцидентами ИБ» — ведение справочников Модуля (справочника классификации событий и инцидентов, списка угроз, справочника правил корреляции и т. д.), формирование типовых сценариев реагирования на инцидент и формирование группы реагирования. Пользователь имеет доступ к реестру инцидентов информационной безопасности. Также пользователь может просматривать карточки инцидентов без возможности их редактирования.

6.1.1 Стартовая страница пользователя

Для того чтобы перейти к стартовой странице Модуля необходимо нажать на логотип сайта в левом верхнем углу.

Стартовая страница пользователя с ролью «Эксперт по управлению инцидентами ИБ» (Рисунок 1) предназначена для отображения основной статистической информации о зарегистрированных событиях и инцидентах.

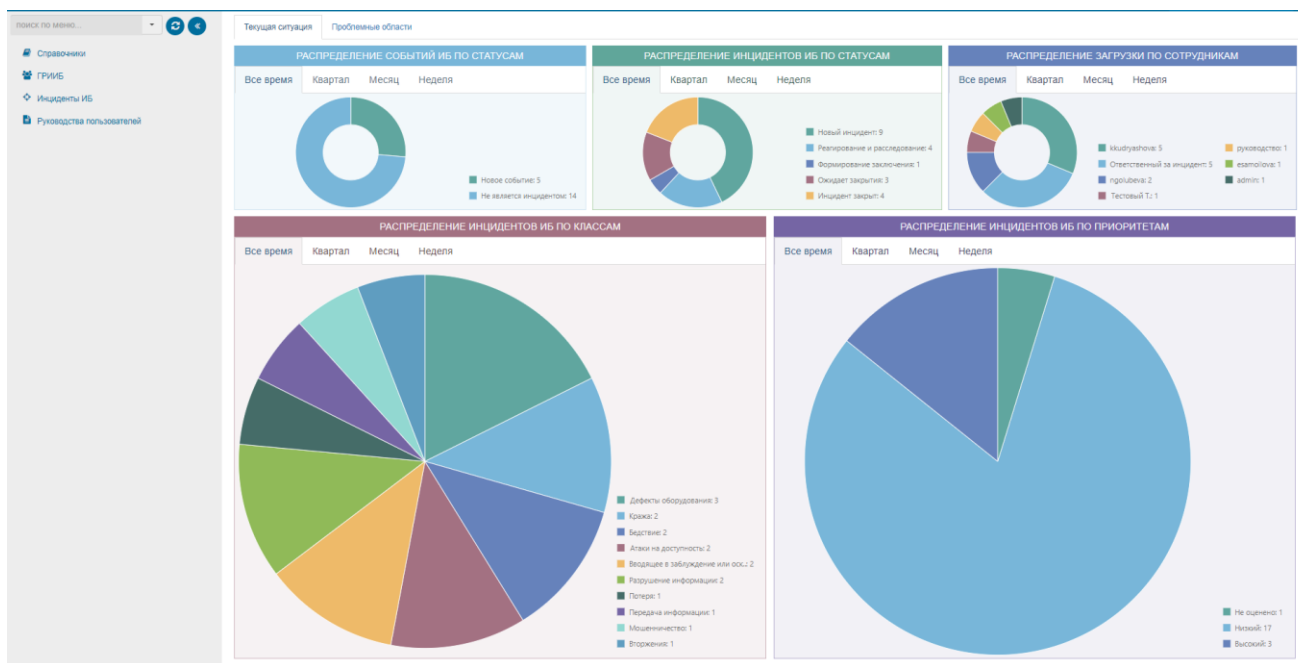


Рисунок 1 – Стартовая страница пользователя с ролью «Эксперт по управлению инцидентами ИБ»

Стартовая страница 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».

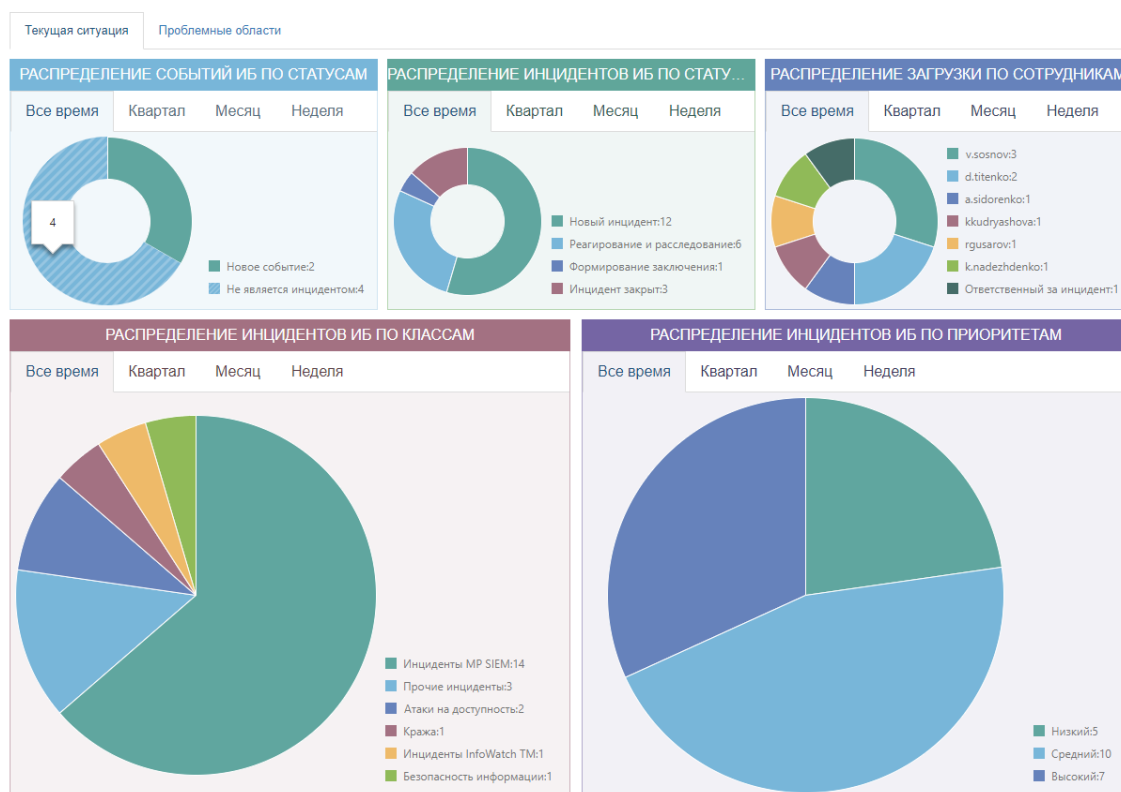


Рисунок 2 – Информационная панель «Текущая ситуация»

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».

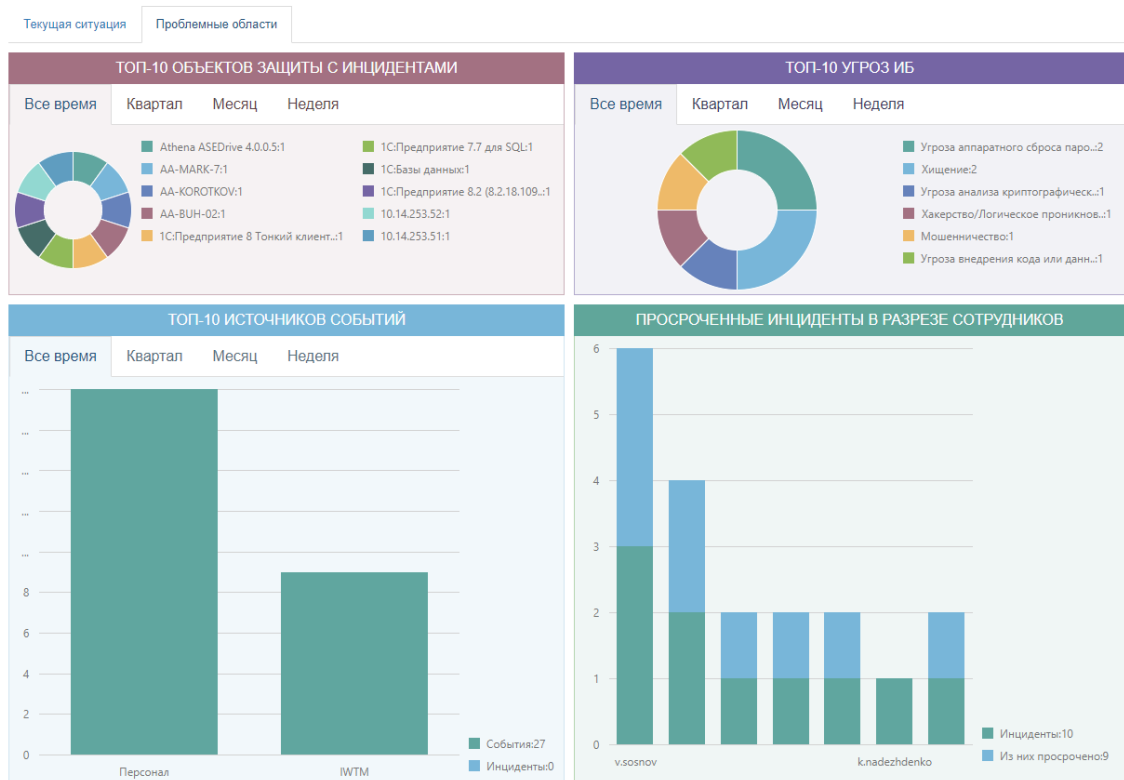


Рисунок 3 – Информационная панель «Проблемные области»

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 инцидента Категории нарушений Правила корреляции Время реагирования

Подклассы инцидента

Наименование	Приоритет	Сценарий	
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 >

Рисунок 4 – Информационная панель «Справочники»

Информационная панель содержит вкладки с данными справочников Модуля (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».

ГРИИБ

Группа реагирования на инциденты ИБ

Руководитель ГРИИБ

Гусаров Р.С., Главный специалист

Работники

Фамилия И.О.	Должность	email	
Першин Д.А.	Администратор проекта		✘
Фролова И.С.	Ведущий бухгалтер		✘
Кудряшова К.А.	Аналитик		✘

5 10 20 50 < 1 из 1 >

Рисунок 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

Новые В работе Обработанные

Дата и время ↓ возникнове...	Номер	Наименование	Подкласс	Приоритет	Источник	Ответствен...
02.12.2019 11:04:55	08.25.08/ ИИБ/16	Кража информации (тест)	Потеря носителя данных	Низкий	Персонал	Ответствен... за инцидент

5 10 20 50

Всего записей: 1 < 1 из 1 >

Рисунок 6 – Информационная панель «Реестр инцидентов ИБ»

На соответствующих вкладках панели отображается список зарегистрированных инцидентов ИБ, разделённых по статусам: новые, в работе и обработанные (закрытые) инциденты. Цветом выделены инциденты с истёкшим сроком реагирования. Двойной щелчок левой кнопкой мыши по записи инцидента открывает его карточку. Карточка доступна только для чтения. Реестр инцидентов доступен только для просмотра списка.

6. Информационная панель «Руководства пользователей» (Рисунок 7).

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

Информационная панель содержит руководства пользователей и инструкции, доступные для загрузки.

ИНСТРУКЦИИ ПО МОДУЛЯМ	
ИНСТРУКЦИЯ	ДАТА ОБНОВЛЕНИЯ
УИИБ. Руководство пользователя системы.pdf	18.10.2019

Рисунок 7 – Информационная панель «Руководства пользователей»

6.1.2 Работа со справочниками

Для работы со справочниками пользователю необходимо в боковом меню выбрать раздел «Справочники». Откроется форма со справочниками (Рисунок 8).

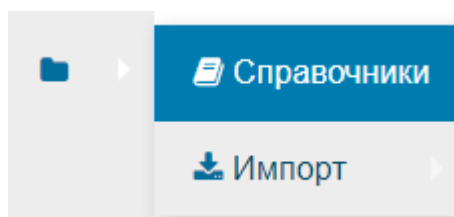


Рисунок 8 – Раздел меню «Справочники»

6.1.2.1 Справочник «Классификация инцидентов»

Справочник (Рисунок 9) содержит типовые классы и подклассы.


Наименование	Приоритет	Сценарий	
Q	Q	Q	
нет значения			
Тест Эксперт подкласс	Низкий		✘
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	Реагирование на сетевые атаки	✘
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			
Запрещенный контент	Низкий		✘
Контент панического характера	Низкий		✘
Контент злонамеренного характера	Низкий		✘

Рисунок 9 – Справочник «Классификация инцидентов»

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.

При необходимости состав справочника может быть изменен и дополнен.

Для того чтобы создать новый класс инцидента, пользователю необходимо выполнить следующие действия:

1. В боковом меню пользователя выбрать пункт «Справочники».
2. На вкладке «Классификация инцидентов» информационной панели «Справочники» нажать на кнопку . В правой части экрана откроется карточка нового класса (Рисунок 10).

Класс

Наименование *

Наименование

Подклассы







Наименование	Приор...	
q	q	

Сохранить

Удалить

Рисунок 10 – Карточка нового класса инцидента

3. В открывшейся форме ввести наименование класса.
4. Для добавления связанных подклассов в таблице «Подклассы»:
 - нажать кнопку . Откроется форма выбора;
 - выбрать необходимые записи с помощью флага ;
 - нажать кнопку .
5. Для удаления связи с подклассом нажать кнопку  в соответствующей строке.
6. Для сохранения нового класса инцидента нажать кнопку .

Для того чтобы отредактировать карточку класса инцидента, пользователь должен выполнить следующие действия:

1. В боковом меню пользователя выбрать пункт «Справочники».
2. На вкладке «Классификация инцидентов» информационной панели «Справочники в дереве классов нажать на интересующую запись. В

правой части экрана откроется карточка выбранного класса (Рисунок 11).

Класс Разрушение информации

Наименование *





Подклассы



Новый подкласс +

Наименование	Приор...	
🔍	🔍	
Подмена информации		✗
Фальсификация информации		✗
Разглашение информации		✗
Хищение информации		✗
Потеря информации		✗



Сохранить

Рисунок 11 – Карточка класса

3. В открывшейся форме при необходимости отредактировать наименование класса.
4. Для добавления связанных подклассов в таблице «Подклассы»:
 - нажать кнопку  . Откроется форма выбора;
 - выбрать необходимые записи с помощью флага ;
 - нажать кнопку  .
5. Для удаления связи с подклассом нажать на кнопку  в соответствующей строке.
6. Для сохранения изменений нажать на кнопку  .

7. Для удаления класса инцидента из справочника нажать на кнопку  .
8. Для возврата на основную страницу справочника к списку подклассов необходимо нажать на кнопку  .

Для того чтобы создать новый подкласс инцидента, пользователь должен выполнить следующие действия:

1. Перейти в карточку нового подкласса (Рисунок 12) любым из следующих способов:
 - из перечня подклассов инцидентов на информационной панели «Справочники» (на вкладке «Классификация инцидентов» в таблице подклассов нажать кнопку );
 - из карточки класса инцидента (нажать кнопку ).

Подкласс

Наименование подкласса *

Текст

Описание

Описание подкласса

Класс инцидента * Приоритет

Класс инцидента Низкий x

Сценарий реагирования

Сценарий ИБ Создать сценарий



 

Рисунок 12 – Карточка нового подкласса инцидента

2. В открывшейся форме заполнить доступные поля.
Внимание! Указанный приоритет будет автоматически назначаться всем инцидентам, отнесённым к данному подклассу. Указанный сценарий реагирования будет автоматически формироваться при переходе к этапу реагирования на инциденты, отнесённые к данному подклассу.

3. Для сохранения нового подкласса инцидента нажать кнопку




4. Для удаления класса инцидента из справочника нажать кнопку

Удалить

5. Для отмены действия нажмите на кнопку

Отмена

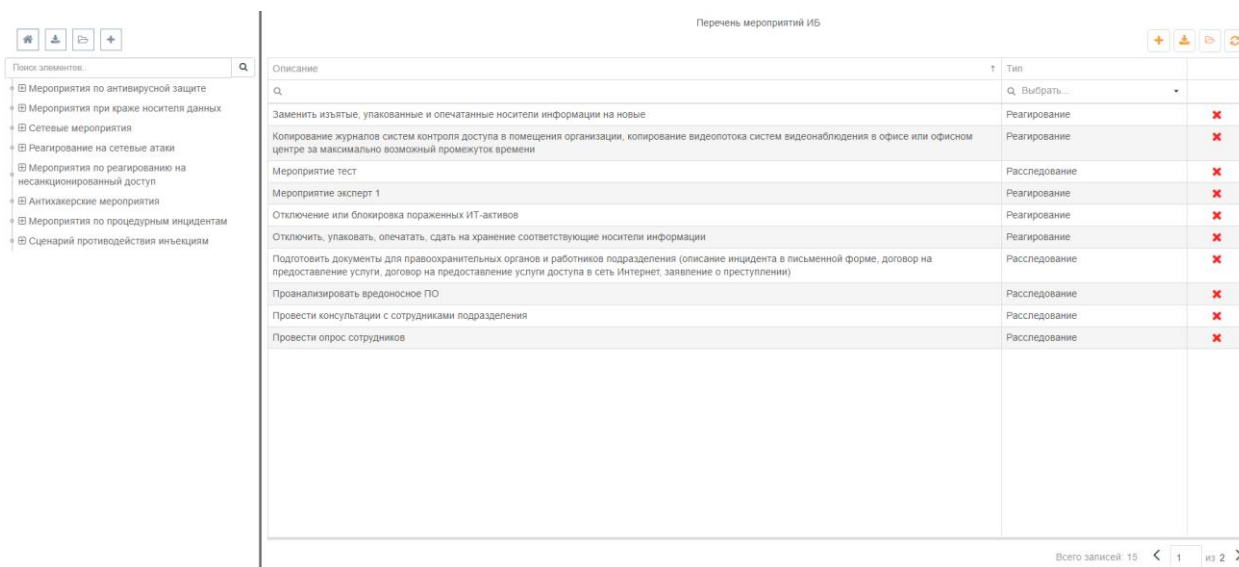
6. Для выгрузки справочника классов и подклассов в формате файла Excel

необходимо нажать кнопку , для загрузки справочника необходимо

нажать кнопку .

6.1.2.2 Справочник «Сценарии реагирования»

Справочник (Рисунок 13) содержит типовые сценарии реагирования на инциденты ИБ и список типовых мероприятий по реагированию и расследованию.



Описание	Тип	
Q	Q. Выбрать...	
Заменить изъятые, упакованные и опечатанные носители информации на новые	Реагирование	✗
Копирование журналов систем контроля доступа в помещения организации, копирование видеопотока систем видеонаблюдения в офисе или офисном центре за максимально возможный промежуток времени	Реагирование	✗
Мероприятие тест	Расследование	✗
Мероприятие эксперт 1	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	✗
Проанализировать вредоносное ПО	Расследование	✗
Провести консультации с сотрудниками подразделения	Расследование	✗
Провести опрос сотрудников	Расследование	✗

Рисунок 13 – Справочник сценариев реагирования

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.

При необходимости состав справочника может быть изменен и дополнен.

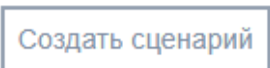
Для того чтобы создать новый сценарий реагирования, пользователь должен выполнить следующие действия:

1. Перейти в карточку нового сценария (Рисунок 14) любым из следующих способов:

– из перечня сценариев инцидентов на информационной панели «Справочники» (на вкладке «Сценарии реагирования» нажать кнопку



– из карточки подкласса инцидента (нажать кнопку



Наименование *

Описание

Подклассы инцидента

Мероприятия

+📄↺

№	↑	Мероприятие	Ответственный	Срок (количество)	Срок (ед. изм. времени)	
🔍		🔍	🔍	🔍	🔍	Выбрать... ▾

СохранитьОтменаУдалить

Рисунок 14 – Карточка нового сценария

2. В открывшейся форме заполнить доступные поля.

3. Для редактирования поля «Подклассы»:

– нажать кнопку . Откроется форма выбора связи;



– выбрать необходимые записи с помощью флага ;


– нажать кнопку .


4. Для добавления мероприятий в таблице «Мероприятия»:


– нажать кнопку . В таблице отобразится пустая строка;

– ввести порядковый номер мероприятия, из выпадающего списка выбрать мероприятие и ответственного, указать срок реагирования. При формировании плана реагирования срок выполнения задач будет вычислен исходя из указанного срока реагирования;

– для сохранения изменений необходимо нажать кнопку . Для отмены действия нажмите кнопку .

5. Для удаления мероприятия нажать на кнопку  в соответствующей строке.

6. Для сохранения нового сценария реагирования нажать кнопку .

7. Для отмены создания нажмите на кнопку .

Для того чтобы отредактировать карточку сценария реагирования, пользователь должен выполнить следующие действия:


1. В боковом меню пользователя выбрать пункт «Справочники».
2. На вкладке «Сценарии реагирования» информационной панели «Справочники» в дереве сценариев нажать на интересующую запись. В правой части экрана откроется карточка сценария реагирования (Рисунок 15).

Сценарий Сетевые мероприятия




Наименование *

Описание

Подклассы инцидента






Мероприятия





[Создать мероприятие](#)   

№ ↑	Тип мероприя...	Мероприятие	Ответственный	Срок выполн... (ед.изм. времени)	Срок выполн... (количе... единиц)	
🔍	🔍 Выбг ▾	🔍	🔍	🔍 Вг ▾	🔍	



[Сохранить](#) [Удалить](#)

Рисунок 15 – Карточка сценария реагирования

3. В открывшейся форме при необходимости отредактировать доступные поля.
4. Для редактирования поля «Подклассы»:
 - нажать кнопку  . Откроется форма выбора связи;
 - выбрать необходимые записи с помощью флага ;
 - нажать кнопку  .
5. Для добавления мероприятий в таблице «Мероприятия»:
 - нажать кнопку  . В таблице отобразится пустая строка;
 - ввести порядковый номер мероприятия, из выпадающего списка выбрать мероприятие и ответственного, указать срок реагирования. При формировании плана реагирования срок выполнения задач будет вычислен исходя из указанного срока реагирования;
 - для сохранения изменений необходимо нажать кнопку  . Для отмены действия нажмите кнопку  .

6. Для удаления мероприятия нажат кнопку  в соответствующей строке.
7. Для сохранения изменений нажать кнопку .
8. Для удаления класса инцидента из справочника нажать кнопку .
9. Для возврата на основную страницу справочника к списку подклассов нажать кнопку .

Для того чтобы создать новое мероприятие, пользователь должен выполнить следующие действия:

1. Перейти в карточку нового мероприятия (Рисунок 16) любым из следующих способов:
 - из перечня мероприятий ИБ на информационной панели «Справочники» (на вкладке «Сценарии реагирования» в таблице мероприятий нажать кнопку );
 - из карточки сценария (нажать кнопку ).

Описание

Описание

Тип мероприятия

Тип








 

Рисунок 16 – Карточка создания нового мероприятия

2. В открывшейся форме заполнить доступные поля. Указать тип мероприятия.
3. Для сохранения нового мероприятия нажать кнопку .
4. Для отмены действия нажмите на кнопку .

5. Для удаления мероприятия в перечне мероприятий на вкладке «Сценарии реагирования» нажать кнопку  в соответствующей строке.

Для выгрузки справочника сценариев в формате файла Excel необходимо

нажать кнопку , для загрузки справочника необходимо нажать кнопку .

6.1.2.3 Справочник «Угрозы»

Справочник (Рисунок 17) содержит список типовых угроз ИБ. Дополнительно в справочник загружен перечень угроз ФСТЭК.

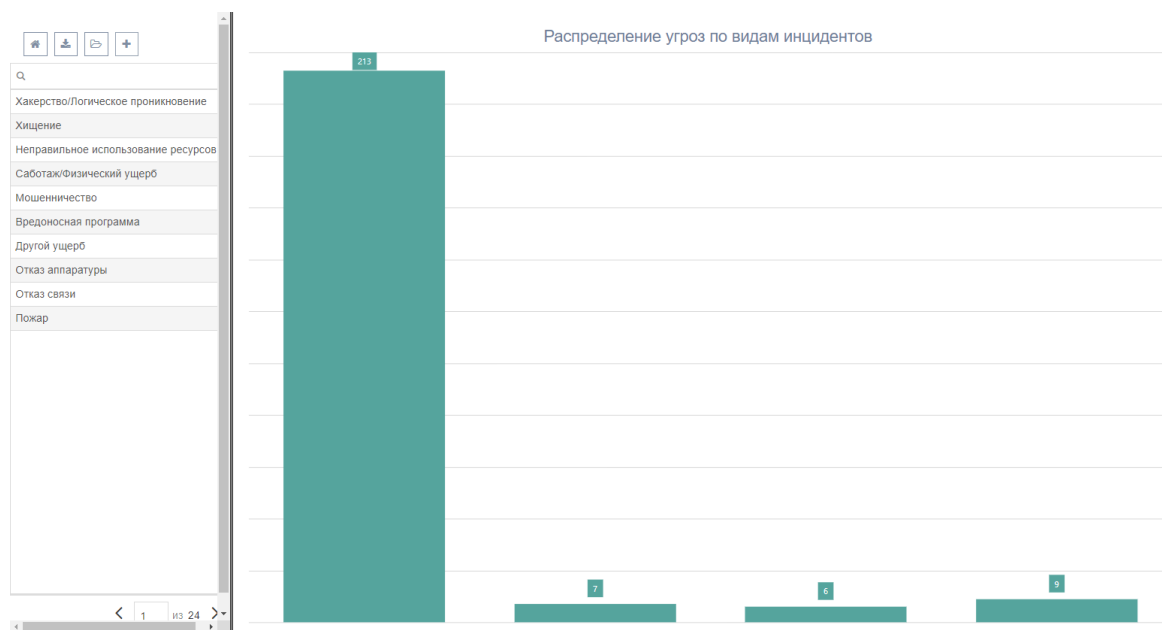



Рисунок 17 – Справочник «Угрозы»


В левой части справочника отображается список всех угроз. В правой части расположена диаграмма распределения угроз по видам инцидентов. Данные из справочника используются для оценки инцидентов ИБ.

При необходимости состав справочника может быть изменен и дополнен.

Для того чтобы создать новую запись угрозы ИБ, пользователь должен выполнить следующие действия:

1. В боковом меню пользователя выбрать пункт «Справочники».
2. На вкладке «Угрозы» информационной панели «Справочники» нажать

кнопку . В правой части экрана откроется карточка новой угрозы

(Рисунок 18). Для отмены создания нажмите на кнопку .

Угроза

Наименование

Введите наименование

Описание

Введите описание

Виды инцидента

+

✖

↺

Вид инцидента ИБ

Укажите виды инцидента



5 10 20 50

Всего записей: 0 < 1 из 1 >


Сохранить Удалить Отменить

Рисунок 18 – Карточка новой угрозы ИБ

3. В открывшейся форме заполнить доступные поля.
4. Для добавления связанных видов инцидента в таблице «Виды» инцидента:

- нажать кнопку . Откроется форма выбора;
- выбрать необходимые записи с помощью флага ;


- нажать кнопку .







5. Для удаления связи с видом инцидента нажать кнопку  в соответствующей строке.
6. Для сохранения новой записи угрозы ИБ нажать кнопку





Для того чтобы отредактировать запись угрозы ИБ, пользователь должен выполнить следующие действия:

1. В боковом меню пользователя выбрать пункт «Справочники».
2. На вкладке «Угрозы» информационной панели «Справочники» в списке угроз нажать на интересующую запись. *В правой части экрана*

откроется карточка выбранного класса. Для отмены действия нажмите на кнопку  .

3. В открывшейся форме при необходимости отредактировать доступные поля.
4. Для добавления связанных видов инцидента в таблице «Виды инцидента»:
 - нажать кнопку  . Откроется форма выбора;
 - выбрать необходимые записи с помощью флага ;
 - нажать кнопку  .
5. Для удаления связи с видом инцидента нажать кнопку  в соответствующей строке.
6. Для сохранения изменений нажать кнопку  .
7. Для удаления угрозы из справочника нажать кнопку  .
8. Для возврата на основную страницу справочника к списку подклассов нажать кнопку  .

Для выгрузки справочника сценариев в формате файла Excel необходимо нажать кнопку  , для загрузки справочника необходимо нажать кнопку  .

6.1.2.4 Справочник «Виды инцидентов»





Справочник (Рисунок 19) содержит список видов инцидентов ИБ.

Вид инцидента ИБ	
Ошибка	✘
Намеренный	✘
Случайный	✘
Неизвестно	✘

5 10 20 50 Всего записей: 4 < 1 из 1 >

Рисунок 19 – Справочник видов инцидентов

Для того чтобы создать новый вид инцидентов, пользователь должен выполнить следующие действия:

1. В боковом меню пользователя выбрать пункт «Справочники».
2. На вкладке «Виды инцидентов» информационной панели «Справочники» в таблице «Виды инцидентов информационной безопасности» нажать кнопку . В таблице отобразится пустая строка.
3. Ввести наименование вида.
4. Для сохранения изменений необходимо нажать кнопку . Для отмены действия нажмите кнопку .
5. Для удаления вида нажать кнопку  в соответствующей строке.

6.1.2.5 Справочник «Категории нарушений»

Справочник (Рисунок 20) содержит список категорий нарушений.

Справочники УИ

Классификация инцидентов Сценарии реагирования Угрозы Виды инцидента Категории нарушений Правила корреляции Время реагиро





Категории воздействия

Указатель категории	Наименование категории	
Q	Q	
КиЭИ	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	✘

5 10 20 50 Всего записей: 6 < 1 из 1 >

Рисунок 20 – Справочник «Категории нарушений»

Для того чтобы создать новую категорию нарушений, пользователь должен выполнить следующие действия:

1. В боковом меню пользователя выбрать пункт «Справочники».
2. На вкладке «Категории нарушений» информационной панели «Справочники» в таблице «Категории воздействия» нажать кнопку . В таблице отобразится пустая строка.
3. Ввести наименование категории, указатель категории.
4. Для сохранения изменений необходимо нажать кнопку . Для отмены действия нажмите кнопку .
5. Для удаления вида нажать кнопку  в соответствующей строке.

6.1.2.6 Справочник «Правила корреляции»

Справочник (Рисунок 21) содержит список правил корреляции.

Перечень правил корреляции

+
↺


Описание	
<input style="width: 95%; border: none; border-bottom: 1px solid #ccc;" type="text" value="Q"/>	
Неудачный вход в операционную систему от имени одной учетной записи в течение пяти минут	✖

<
1
из 1
>

Рисунок 21 – Справочник «Правила корреляции»

Для того чтобы создать новое правило корреляции, пользователь должен выполнить следующие действия:

1. В боковом меню пользователя выбрать пункт «Справочники».
2. На вкладке «Правила корреляции» информационной панели «Справочники» в таблице «Перечень правил корреляции» нажать

кнопку . Откроется форма создания правила корреляции (Рисунок 22).

Создание правила корреляции ★ 🗨 ✕


Описание *

Описание

Сохранить

Отмена

Рисунок 22 – Форма создания правила корреляции

3. Для сохранения нового правила нажать кнопку .

4. Для отмены создания нажать кнопку Отмена.

Для того чтобы создать новое правило корреляции, пользователь должен выполнить следующие действия:

1. В справочнике «Правила корреляции» дважды щёлкнуть левой кнопкой мыши по записи правила. *Откроется карточка правила корреляции* (Рисунок 23).

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

Рисунок 23 – Карточка правила корреляции

2. В карточке правила корреляции при необходимости изменить доступные поля.
3. Для сохранения нового правила нажать кнопку Сохранить.
4. Для удаления вида нажать кнопку ✖ в соответствующей строке таблицы.

6.1.2.7 Справочник «Время реагирования»

Для того чтобы отредактировать справочник времени реагирования на инциденты ИБ, пользователь должен выполнить следующие действия:

1. В боковом меню пользователя выбрать пункт «Справочники».
2. На вкладке «Время реагирования» (Рисунок 24) информационной панели «Справочники» в строке записи таблицы нажать кнопку . Запись станет доступной для редактирования.






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




Рисунок 24 – Справочник времени реагирования

3. При необходимости изменить время реагирования в зависимости от приоритета инцидента. Исходя из указанного времени реагирования будет вычисляться срок реагирования на все инциденты с соответствующим приоритетом.
4. Для сохранения изменений нажать кнопку .
5. Для отмены нажать кнопку .

6.1.3 Формирование группы реагирования на инциденты ИБ

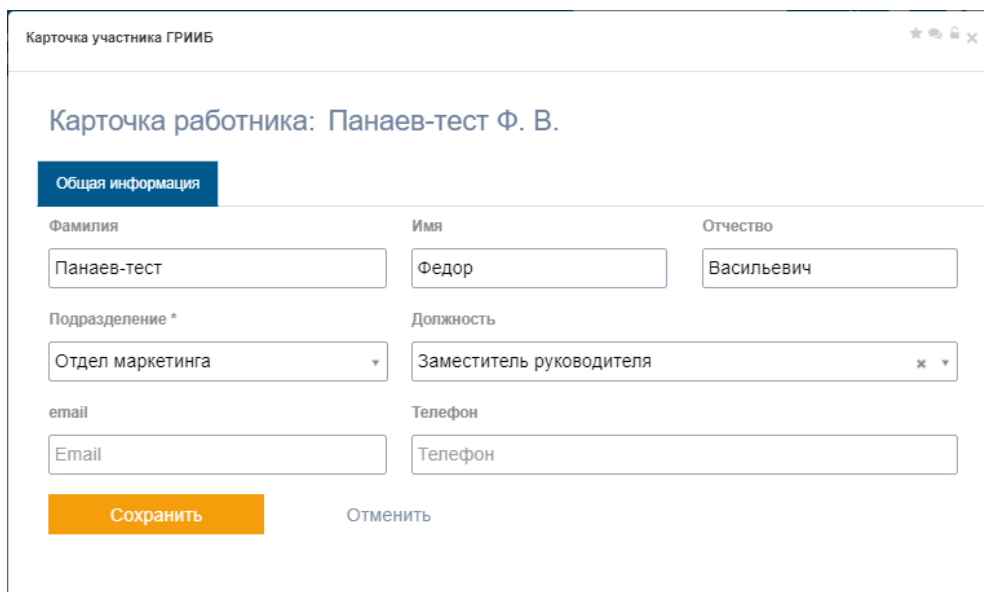
6.1.3.1 Редактирование группы реагирования на инциденты ИБ

Для того чтобы отредактировать список работников, входящих в ГРИИБ, пользователь должен выполнить следующие действия:

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

Для того чтобы отредактировать информацию об участнике ГРИИБ, пользователь должен выполнить следующие действия:

1. Дважды щёлкнуть левой кнопкой мыши по записи работника на информационной панели «ГРИИБ». Откроется карточка участника ГРИИБ (Рисунок 25).



Карточка участника ГРИИБ

Карточка работника: Панаев-тест Ф. В.

Общая информация

Фамилия	Имя	Отчество
<input type="text" value="Панаев-тест"/>	<input type="text" value="Федор"/>	<input type="text" value="Васильевич"/>
Подразделение *	Должность	
<input type="text" value="Отдел маркетинга"/>	<input type="text" value="Заместитель руководителя"/>	
email	Телефон	
<input type="text" value="Email"/>	<input type="text" value="Телефон"/>	

Рисунок 25 – Карточка участника ГРИИБ

2. При необходимости изменить доступные поля.
3. Для сохранения изменений нажать кнопку .
4. Для отмены изменений нажать кнопку .

6.2 Роль «Ответственный за инцидент ИБ»

Задача пользователя с ролью «Ответственный за инцидент ИБ» — обработка инцидента информационной безопасности (классификация и оценка инцидента, формирование плана реагирования на инцидент ИБ, контроль его выполнения, анализ и закрытие расследования, анализ и закрытие инцидента ИБ). Пользователь имеет доступ к реестру событий информационной безопасности и реестру инцидентов, ответственным за которые назначен данный пользователь. Так же пользователь может создавать новые события и инциденты, при этом не может переназначить инцидент на другого пользователя.

Также «Ответственный за инцидент ИБ» имеет доступ к редактированию справочников Модуля.

6.2.1 Стартовая страница пользователя

Для того чтобы перейти к стартовой странице Модуля необходимо нажать на логотип сайта в левом верхнем углу.

Стартовая страница пользователя с ролью «Ответственный за инцидент ИБ» (Рисунок 26) предназначена для отображения основной информации о зарегистрированных событиях и инцидентах, назначенных на данного пользователя.

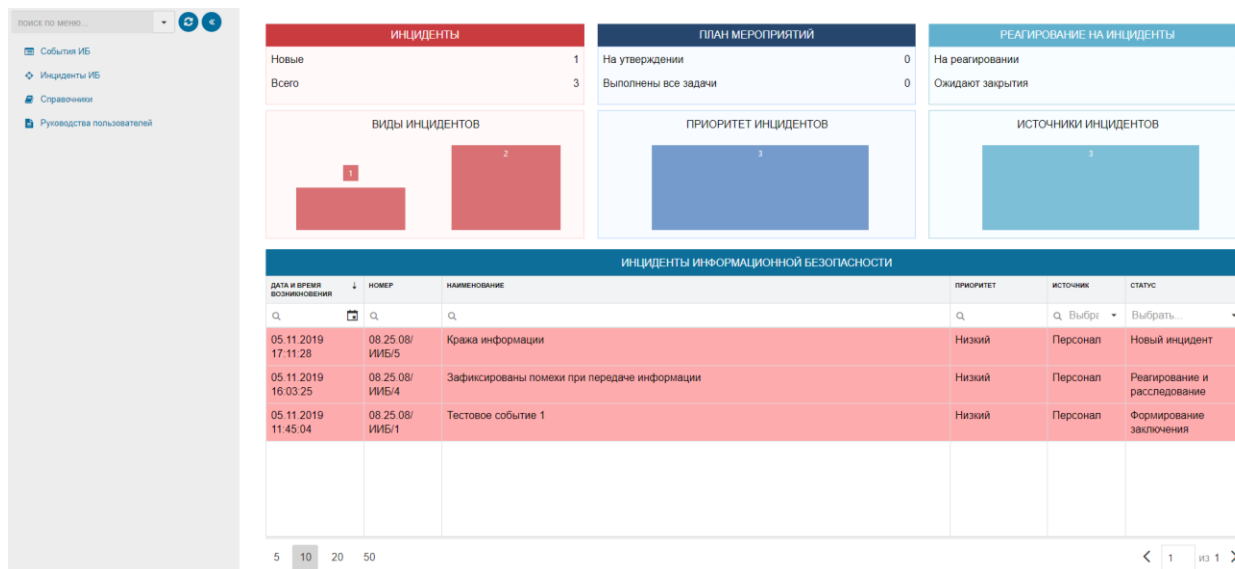


Рисунок 26 – Стартовая страница пользователя с ролью «Ответственный за инцидент ИБ»

Стартовая страница состоит из следующих виджетов:

1. Виджет «Инциденты информационной безопасности» (Рисунок 27).

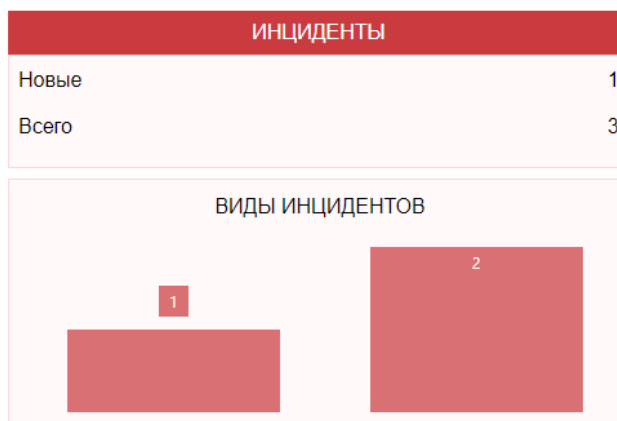


Рисунок 27 – Виджет «Инциденты информационной безопасности»

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 28).



Рисунок 28 – 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 29).

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 инцидентов ИБ по счетчикам.

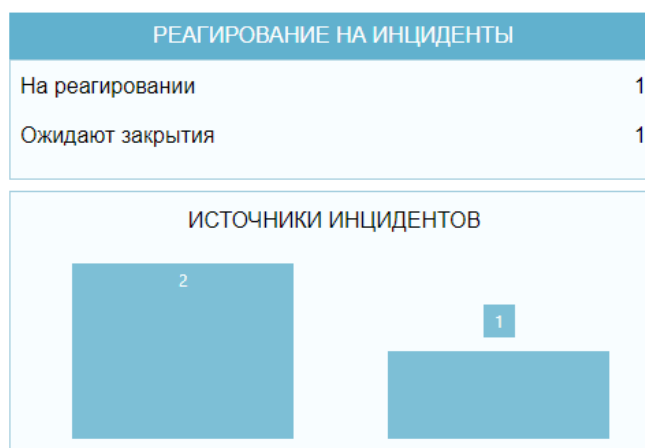


Рисунок 29 – Виджет «Реагирование на инциденты»

4. Таблица «Инциденты информационной безопасности» (Рисунок 30).

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	Тестовое событие 1	Низкий	Персонал	Формирование заключения

5 10 20 50 < 1 из 1 >

Рисунок 30 – Таблица «Инциденты информационной безопасности»

5. Информационная панель «Реестр событий ИБ» (Рисунок 31).

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

Реестр событий ИБ Новое событие

Новые Являются инцидентами Не являются инцидентами

<input type="checkbox"/>	Дата и время возни... ↓	Номер	Наименование	Ответственный	Источник события
<input type="checkbox"/>	05.07.2019 10:51:52	26	Зафиксированы помехи при передаче информации	test	Персонал
<input type="checkbox"/>	04.07.2019 15:08:51	23	Неисправность оборудывания	Ответствен...	Персонал

5 10 20 50 Всего записей: 2 < 1 из 1 >

Рисунок 31 – 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 32).

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.

<input type="checkbox"/>	Дата и время возникновения	Номер	Наименование	Подкласс	Приоритет	Источник	Ответственный
<input type="checkbox"/>	01.12.2017 08:25:52	08.25.08/ИИБ/4	Test Incident		Высокий	MaxPatrol SIEM	k.nadezhdenko
<input type="checkbox"/>	15.11.2016 07:14:00	08.25.08/ИИБ/2	Тест Инцидент Уведомление		Высокий	MaxPatrol SIEM	d.titenko
<input type="checkbox"/>		08.25.08/ИИБ/6	test		Средний	MaxPatrol SIEM	
<input type="checkbox"/>		08.25.08/ИИБ/13	test		Средний	MaxPatrol SIEM	
<input type="checkbox"/>		08.25.08/	test		Средний	MaxPatrol SIEM	

Рисунок 32 – Информационная панель «Реестр инцидентов ИБ»

7. Информационная панель «Справочники» (Рисунок 33).

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

Наименование	Приоритет	Сценарий	
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	✘

Рисунок 33 – Информационная панель «Справочники»

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

6.2.2 Управление событиями информационной безопасности

События ИБ могут быть обнаружены работниками 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.

6.2.2.1 Создание записи о событии информационной безопасности

Для того чтобы создать запись о событии ИБ, пользователь должен выполнить следующие действия:

1. В боковом меню пользователя выбрать пункт «События ИБ».
2. На информационной панели «Реестр событий ИБ» нажать кнопку

. Откроется карточка нового события (Рисунок 34).

Рисунок 34 – Карточка нового события ИБ

3. В открывшейся форме заполнить доступные поля. По умолчанию поля «Дата и время возникновения», «Дата и время обнаружения», «Дата и время оповещения» заполняются значениями текущей даты и времени, в поле «Ответственный за событие» 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».

4. После заполнения формы возможны следующие действия:
 - для создания записи о событии и возврата в реестр событий ИБ необходимо нажать кнопку **Сохранить и закрыть** ;
 - для создания записи о событии и перехода в карточку созданного события необходимо нажать кнопку **Сохранить и перейти к событию** .




6.2.2.2 Редактирование записи о событии информационной безопасности, формирование отчета










Для того чтобы отредактировать карточку события ИБ (Рисунок 35), пользователь должен выполнить следующие действия:

1. Перейти в карточку события любым из следующих способов:
 - из перечня новых событий информационной панели «Реестр событий ИБ» (в боковом меню пользователя выбрать пункт «События ИБ»);
 - из перечня новых событий ИБ на виджете «События информационной безопасности» (нажать счетчик новых событий. В данном перечне доступны только карточки со статусом «Новое событие»).

Рисунок 35 – Карточка события ИБ

2. На вкладке «Описание» при необходимости изменить доступные поля.
3. Для добавления связанных бизнес-процессов на вкладке «Пораженные компоненты» в таблице «Бизнес-процессы»:

- нажать кнопку . Откроется форма выбора;
- 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  . Откроется форма выбора;
 - 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  .
9. Для формирования отчёта о событии на вкладке «Описание» необходимо нажать кнопку  . Для того чтобы скачать сформированный отчёт необходимо нажать кнопку  . Внимание! Для обновления отчёта в случае изменения данных о событии ИБ необходимо нажать кнопку  повторно.

6.2.2.3 Обработка события информационной безопасности

Для перевода события ИБ в статус «Новый инцидент» из карточки события пользователь должен выполнить следующие действия:


1. Перейти в карточку события.
2. Нажать кнопку  (доступна только на статусе «Новое событие» и среди пользователей, выбранных *Ответственным за событие*). Откроется форма перевода события в инцидент (Рисунок 36).

Рисунок 36 – Форма перевода события в инцидент

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

- для регистрации нового инцидента ИБ необходимо выбрать пункт «Является новым инцидентом», в появившемся поле «Ответственный за инцидент» указать ответственного;
- для связи события с уже существующим инцидентом необходимо выбрать пункт «Связан с существующим инцидентом», в появившемся поле «Наименование инцидента» указать инцидент ИБ, к которому относится событие.

4. Нажать кнопку . На карточке события отобразится вкладка «Инцидент» (Рисунок 37). Вкладка содержит основную информацию о связанном инциденте ИБ и ссылку на карточку инцидента и доступна только для чтения.

Рисунок 37 – Карточка события ИБ. Вкладка «Инцидент»

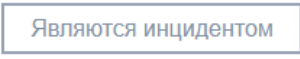
Для перевода события ИБ в статус «Не является инцидентом» из карточки события пользователь должен выполнить следующие действия:

1. Перейти в карточку события.
2. Нажать кнопку (доступна только на статусе «Новое событие»).

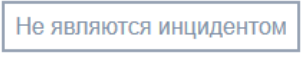
Внимание! Данное действие доступно в случае, если текущий пользователь выбран Ответственным за событие с ролью «Ответственный за инцидент ИБ».

6.2.2.4 Управление списком событий информационной безопасности

Для перевода нескольких событий ИБ в статус «Новый инцидент» из списка событий пользователь должен выполнить следующие действия:

1. Перейти в реестр событий ИБ (в боковом меню пользователя выбрать пункт «События ИБ»).
2. В перечне выбрать необходимые записи с помощью флага .
3. Нажать кнопку . *Выбранные события будут переведены на статус «Новый инцидент».*

Для перевода нескольких событий ИБ в статус «Не является инцидентом» из списка событий пользователь должен выполнить следующие действия:

1. Перейти в реестр событий ИБ (в боковом меню пользователя выбрать пункт «События ИБ»).
2. В перечне выбрать необходимые записи с помощью флага .
3. Нажать кнопку . *Откроется форма перевода в ложное срабатывание (Рисунок 38).*

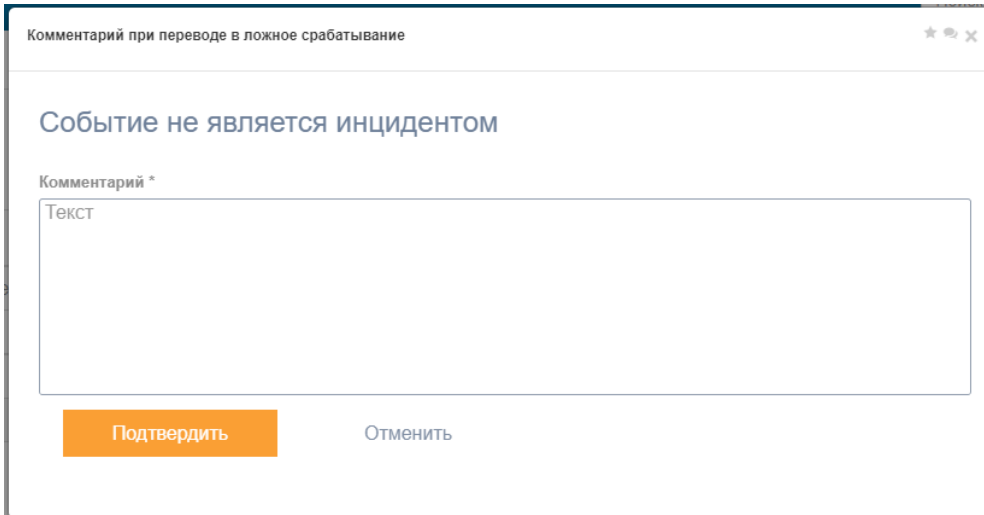






Рисунок 38 – Форма перевода события в ложное срабатывание

4. Заполнить поле «Комментарий» и нажать кнопку . *Текущий статус событий изменится с «Новое событие» на «Не*

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

5. Для отмены перевода события в ложное срабатывание необходимо закрыть форму перевода или нажать на кнопку  .

Для объединения нескольких событий в один инцидент ИБ пользователь должен выполнить следующие действия:

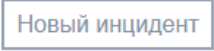
1. Перейти в реестр событий ИБ (в боковом меню пользователя выбрать пункт «События ИБ»).
2. В перечне выбрать необходимые записи с помощью флага .
3. Нажать кнопку  . *Выбранные события будут объединены в инцидент. Самое раннее из них перейдет в статус «Новый инцидент» (в качестве ответственного автоматически будет назначен текущий пользователь), остальные события из выборки станут связаны с инцидентом.*

6.2.3 Управление инцидентами информационной безопасности

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

6.2.3.1 Создание записи об инциденте информационной безопасности

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

1. В боковом меню пользователя выбрать пункт «Инциденты ИБ».
2. На информационной панели «Реестр инцидентов ИБ» нажать кнопку  . *Откроется карточка нового инцидента (Рисунок 39).*

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

Рисунок 39 – Карточка нового инцидента ИБ




3. В открывшейся форме заполнить доступные поля. По умолчанию поля «Дата и время возникновения», «Дата и время обнаружения», «Дата и время оповещения» заполняются значениями текущей даты и времени, 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 .

6.2.3.2 Редактирование записи об инциденте информационной безопасности, формирование отчёта

Для того чтобы отредактировать карточку инцидента ИБ (Рисунок 40), 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 доступные поля. 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 . Откроется форма выбора работников организации;
 - 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  . Откроется форма выбора;
- выбрать необходимые записи с помощью флага ;
- нажать кнопку  .

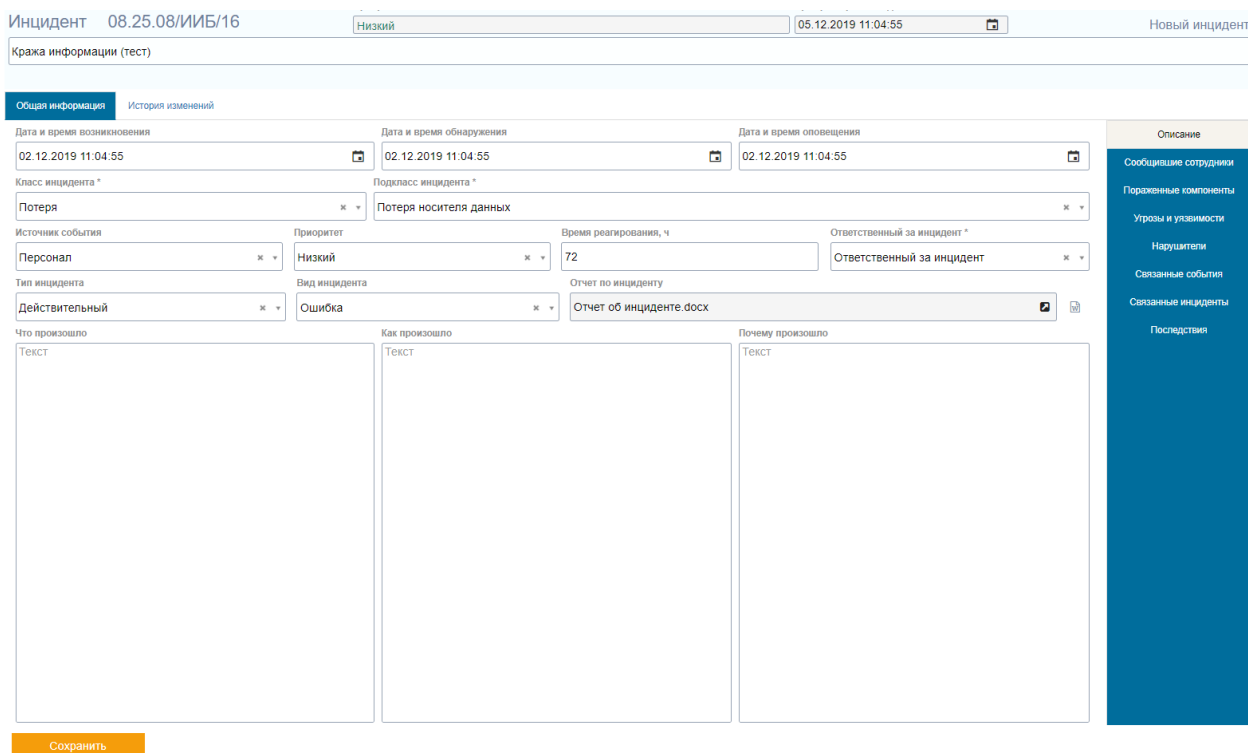





















Рисунок 40 – Карточка инцидента ИБ

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  . Откроется перечень объектов защиты, сгруппированных по типам;
- 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  . Откроется форма выбора;
 - 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».
13. Для добавления нарушителя или причастного лица на вкладке «Нарушители» необходимо нажать кнопку  . В таблице отобразится пустая строка, в которой необходимо из выпадающего списка выбрать тип нарушителя, его мотивацию и ввести известные сведения о нарушителе. Для сохранения изменений необходимо нажать кнопку  . Для отмены действия нажмите кнопку  .
14. Для удаления нарушителя на вкладке «Нарушители» нажать кнопку  в соответствующей строке.
15. Для добавления связанных событий ИБ на вкладке «Связанные события»:
 - нажать кнопку  . Откроется форма выбора;
 - выбрать необходимые записи с помощью флага ;

- нажать кнопку  .
16. Для удаления связи с событием на вкладке «Связанные события» нажать кнопку  в соответствующей строке.
17. Для добавления связанных инцидентов ИБ на вкладке «Связанные инциденты»:
- нажать кнопку  . Откроется форма выбора;
 - выбрать необходимые записи с помощью флага  ;
 - нажать кнопку  .
18. Для удаления связи с инцидентом на вкладке «Связанные события» нажать кнопку  в соответствующей строке.
19. Для добавления последствий инцидента ИБ на вкладке «Последствия» в таблице «Неблагоприятные воздействия инцидента на бизнес»:
- нажать кнопку  . Откроется форма добавления воздействия (Рисунок 41);

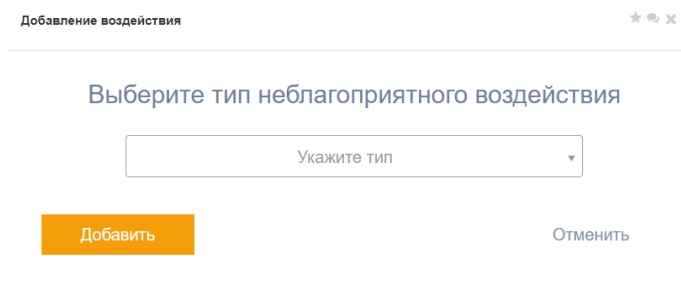











Рисунок 41 – Форма добавления неблагоприятного воздействия

- в выпадающем списке типов воздействия выбрать тип, нажать кнопку  . 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  .

20. 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 .
21. Для формирования отчета об инциденте на вкладке «Описание» необходимо нажать кнопку . Для того чтобы скачать сформированный отчет необходимо нажать кнопку . Внимание! Для обновления отчета в случае изменения данных об инциденте ИБ необходимо нажать кнопку  повторно.
22. Для применения изменений без изменения статуса инцидента ИБ необходимо нажать кнопку .
23. Для применения изменений и перехода к этапу формирования плана реагирования необходимо нажать кнопку  (доступна только на статусе «Новый инцидент»). *На карточке инцидента отобразится вкладка «План мероприятий» (Рисунок 42). В плане мероприятий автоматически добавятся мероприятия, входящие в сценарий, связанный с подклассом инцидента.*

Общая информация | **План мероприятий** | История изменений

Отправить план на утверждение

Выбрать из справочника

Тип мероприятия	Описание	Ответственный за выполнение	Выполнить до	
q. Выбрать...	q	q	q	
Расследование	Провести консультации с сотрудниками подразделения		18.11.2019	✖

5 10 20 50 < 1 из 1 >

Рисунок 42 – Карточка инцидента ИБ. Вкладка «План мероприятий»



6.2.3.3 Перевод инцидента в ложное срабатывание

Для перевода инцидента ИБ в ложное срабатывание из карточки инцидента пользователь должен выполнить следующие действия:

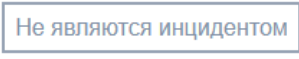
1. Перейти в карточку инцидента любым из следующих способов:
 - из перечня новых инцидентов информационной панели «Реестр инцидентов ИБ» (в боковом меню пользователя выбрать пункт «Инциденты ИБ»);
 - из таблицы «Инциденты информационной безопасности» стартовой страницы пользователя;
 - из перечня новых инцидентов ИБ на виджете «Инциденты информационной безопасности» (нажать счетчик новых инцидентов. *В данном перечне доступны только карточки со статусом «Новый инцидент»*).
2. Нажать кнопку Перевести в ложное срабатывание (доступна только на статусе «Новый инцидент»). *Откроется форма перевода инцидента в ложное срабатывание (Рисунок 43).*

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


Рисунок 43 – Форма перевода инцидента в ложное срабатывание

3. Заполнить поле «Комментарий» и нажать кнопку . Текущий статус инцидента изменится с «Новый инцидент» на «Не является инцидентом». Внимание! Карточка инцидента на статусе «Не является инцидентом» доступна только для чтения.
4. Для отмены перевода инцидента в ложное срабатывание необходимо закрыть форму перевода или нажать на кнопку .

Для перевода нескольких инцидентов ИБ в статус «Не является инцидентом» из списка инцидентов пользователь должен выполнить следующие действия:

1. Перейти в реестр инцидентов ИБ (в боковом меню пользователя выбрать пункт «Инцидент ИБ»).
2. В перечне выбрать необходимые записи с помощью флага .
3. Нажать кнопку . Откроется форма перевода в ложное срабатывание (Рисунок 38).

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

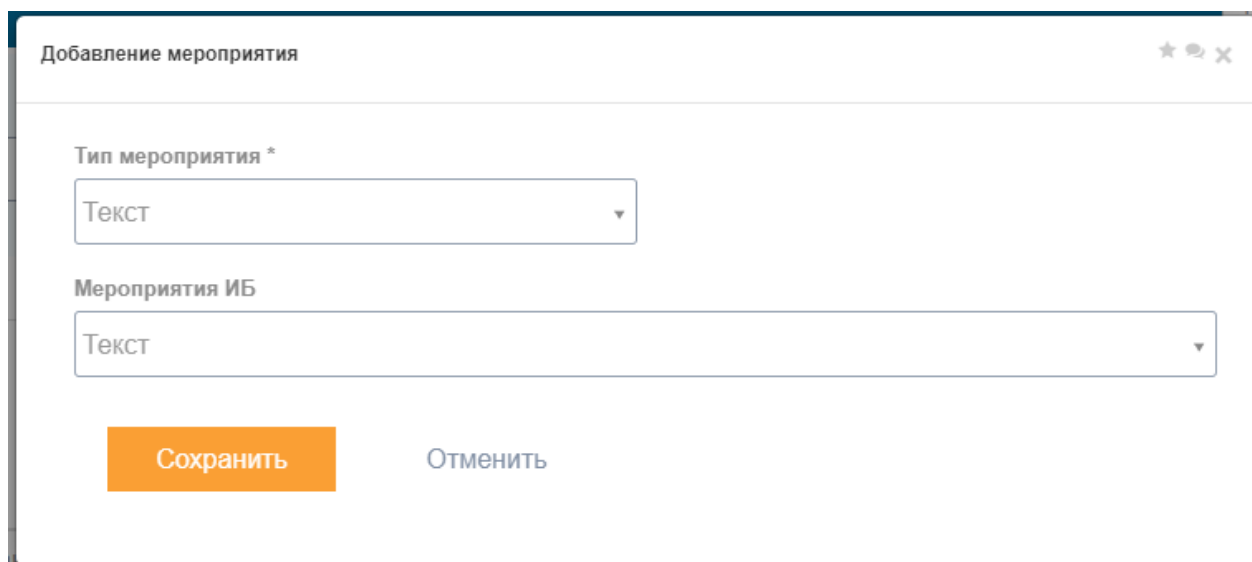
4. Заполнить поле «Комментарий» и нажать кнопку . Текущий статус инцидентов изменится с «Новый инцидент» на «Не является инцидентом». Внимание! Карточка инцидента на статусе «Не является инцидентом» доступна только для чтения.

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

6.2.3.4 Формирование плана реагирования на инцидент информационной безопасности

Для того чтобы добавить в план реагирования мероприятия из справочника мероприятий, пользователь должен выполнить следующие действия:

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;
 - из перечня инцидентов на виджете «Инциденты информационной безопасности» (нажать счетчик всех инцидентов).
2. На вкладке «План мероприятий» (доступна только на этапе формирования плана реагирования) нажать кнопку **Выбрать из справочника**. Откроется форма добавления мероприятия из справочника (Рисунок 44).



Добавление мероприятия

Тип мероприятия *

Текст



Мероприятия ИБ

Текст


Сохранить Отменить

Рисунок 44 – Форма добавления мероприятия из справочника




3. Указать тип мероприятия и выбрать нужное мероприятие из выпадающего списка.

4. Нажать кнопку . Выбранное мероприятие будет добавлено в план реагирования. В качестве ответственного за выполнение автоматически будет назначен текущий пользователь. 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 .


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 . Для отмены действия нажмите кнопку .
4. Для удаления мероприятия на вкладке «План мероприятий» нажать кнопку  в соответствующей строке.

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

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

- если включена настройка согласования плана реагирования на инцидент, текущий план реагирования на инцидент ИБ будет отправлен на утверждение. Пользователям с ролью «Руководство

СУИБ» 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 СУИБ») 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 45).

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 46) 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 46) с перечнем мероприятий по реагированию и расследованию, сгруппированным по статусу.

Комментарии при возврате плана реагирования на корректировку

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 >

Рисунок 45 – Форма просмотра комментария при возврате плана реагирования на корректировку

Общая информация Реагирование и расследование История изменений

Мероприятия по реагированию и расследованию

Добавить мероприятие

Тип меропр...	Описание	Ответств... за выполне...	Срок выполне...	Отчет о выполнении	Документ
Выб					
Выполняется					
Расследо...	Провести консультации с сотрудниками подразделения	Кудряшова К.А.	18.11.2019		

5 10 20 50 < 1 из 1 >


Рисунок 46 – Карточка инцидента ИБ. Вкладка «Расследование и реагирование»

6.2.3.5 Реагирование и расследование на инцидент информационной безопасности

Для того чтобы добавить новое мероприятие в сформированный план реагирования, пользователь должен выполнить следующие действия:

1. Перейти в карточку инцидента любым из следующих способов:

- из таблицы «Инциденты информационной безопасности» стартовой страницы пользователя;
- из перечня инцидентов, находящихся на реагировании, на виджете «Реагирование на инциденты» (нажать счетчик инцидентов на реагировании. В данном перечне доступны только карточки со статусом «Реагирование и расследование»).

2. На вкладке «Реагирование и расследование» (доступна только на статусе «Реагирование и расследование») нажать кнопку . Откроется форма добавления нового мероприятия (Рисунок 47). Поля «Выполнить до» и «Ответственный за выполнение» по умолчанию будут заполнены значением текущей даты и текущим пользователем соответственно.

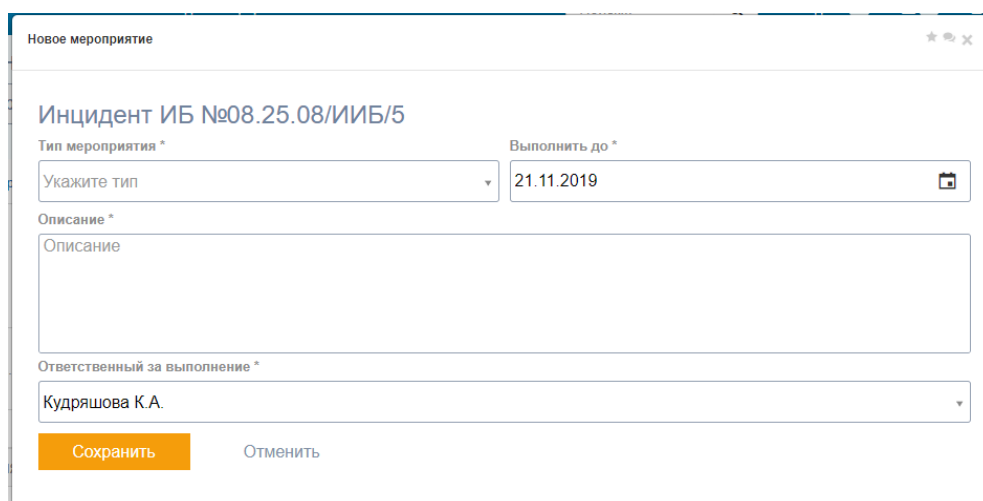
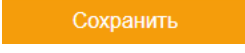


Рисунок 47 – Форма добавления нового мероприятия

3. Указать тип мероприятия и ввести его описание. При необходимости отредактировать поля «Выполнить до» и «Ответственный за выполнение».

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

4. Нажать кнопку . Мероприятие будет добавлено в план реагирования в статусе «Новое». В карточке инцидента на вкладке «реагирование и расследование» появится кнопка «Завершить формирование плана».

5. Для отмены действия необходимо закрыть форму или нажать кнопку

Отменить

6. При необходимости карточка мероприятия в статусе «Новое» может быть отредактирована. Для перехода к карточке необходимо дважды щелкнуть левой кнопкой мыши по нужной записи.

Для отправки новых мероприятий на утверждение пользователь должен выполнить следующие действия:

1. На вкладке «Реагирование и расследование» нажать кнопку

Завершить формирование плана

После завершения формирования плана реагирования возможно следующее:

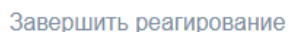
- если включена настройка согласования плана реагирования на инцидент, *текущий план реагирования с новыми мероприятиями будет отправлен на утверждение. Пользователя с ролью «руководство СУИБ» будет отправлено уведомление о необходимости утверждения плана. После утверждения или возврата на корректировку плана реагирования (осуществляет пользователь с ролью «Руководство СУИБ») 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 «Реагирование и расследование» в карточке инцидента по ссылке на форму просмотра комментариев (Рисунок 45).*

После утверждения плана реагирования на пользователей, которые назначены ответственными за выполнения мероприятий, будут назначены задачи и отправлены уведомления;

- если настройка согласования плана реагирования на инцидент отключена, *на пользователей, которые назначены ответственными за выполнения мероприятий, будут назначены задачи и отправлены уведомления, минуя этап утверждения плана реагирования.*

Для того чтобы завершить этап реагирования на инцидент, пользователь должен выполнить следующие действия:

1. На вкладке «Реагирование и расследование» нажать кнопку





 (кнопка станет доступна только после того, как


будут выполнены все мероприятия из плана реагирования. О выполнении всех мероприятий ответственному за инцидент будет отправлено уведомление). Текущий статус инцидента изменится с «Реагирование и расследование» на «Формирование заключения». На карточке инцидента отобразится вкладка «Заключение», добавятся вкладки «Выполненные мероприятия» и «Документы».


6.2.3.6 Завершение обработки инцидента, возвращение инцидента на этап расследования и реагирования


Для того чтобы завершить обработку инцидента, пользователь должен выполнить следующие действия:

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 необходимо нажать кнопку . Для отмены действия нажмите кнопку .

– для удаления документа нажать кнопку  в соответствующей строке.

4. Для возврата инцидента на этап расследования и реагирования необходимо на вкладке «Заключение» нажать кнопку  (доступна только на статусе «Формирование заключения»). Текущий статус инцидента изменится с «Формирование заключения» на «Реагирование и расследование». В карточке инцидента станет доступно добавление мероприятий по реагированию (см. раздел «Реагирование и расследование на инцидент информационной безопасности»). Вкладка «Заключение» станет недоступной.

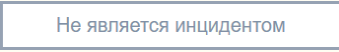
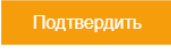

5. Для завершения этапа формирования заключения и закрытия инцидента необходимо на вкладке «Заключение» нажать кнопку  (доступна только на статусе «Формирование заключения»).

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 СУИБ» будет отправлено уведомление о необходимости закрыть инцидент.

После закрытия или возврата инцидента на доработку (осуществляет пользователь с ролью «Руководство СУИБ») 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.

6. Для перевода инцидента ИБ в ложное срабатывание со статуса «Формирование заключения» необходимо на вкладке «Заключение» нажать кнопку  (доступна только на статусе «Формирование заключения»). *Откроется форма перевода инцидента в ложное срабатывание* (Рисунок 43). Заполнить поле «Комментарий» и нажать кнопку . *Текущий статус инцидента изменится с «Формирование заключения» на «Не является инцидентом». Карточка инцидента станет доступна только для чтения.* Для отмены перевода инцидентов в ложное срабатывание необходимо закрыть форму перевода или нажать на кнопку .

6.3 Роль «Руководство СУИБ»

Задача пользователя с ролью «Руководство СУИБ» — регистрация событий и инцидентов вручную и на основе данных из смежных систем, назначение ответственных за инцидент, создание и контроль выполнения мероприятий по реагированию, закрытие и анализ инцидента ИБ. Пользователь имеет доступ к реестру событий и инцидентов информационной безопасности, ведению карточек событий и инцидентов.

Также «Руководство СУИБ» имеет доступ к редактированию справочников Модуля и группы реагирования на инциденты ИБ.

6.3.1 Стартовая страница пользователя

Для того чтобы перейти к стартовой странице Модуля необходимо нажать на логотип сайта в левом верхнем углу и перейти на вкладку «Управление инцидентами информационной безопасности».

Стартовая страница пользователя с ролью «Руководство СУИБ» (Рисунок 48) предназначена для отображения основной информации о зарегистрированных событиях и инцидентах.

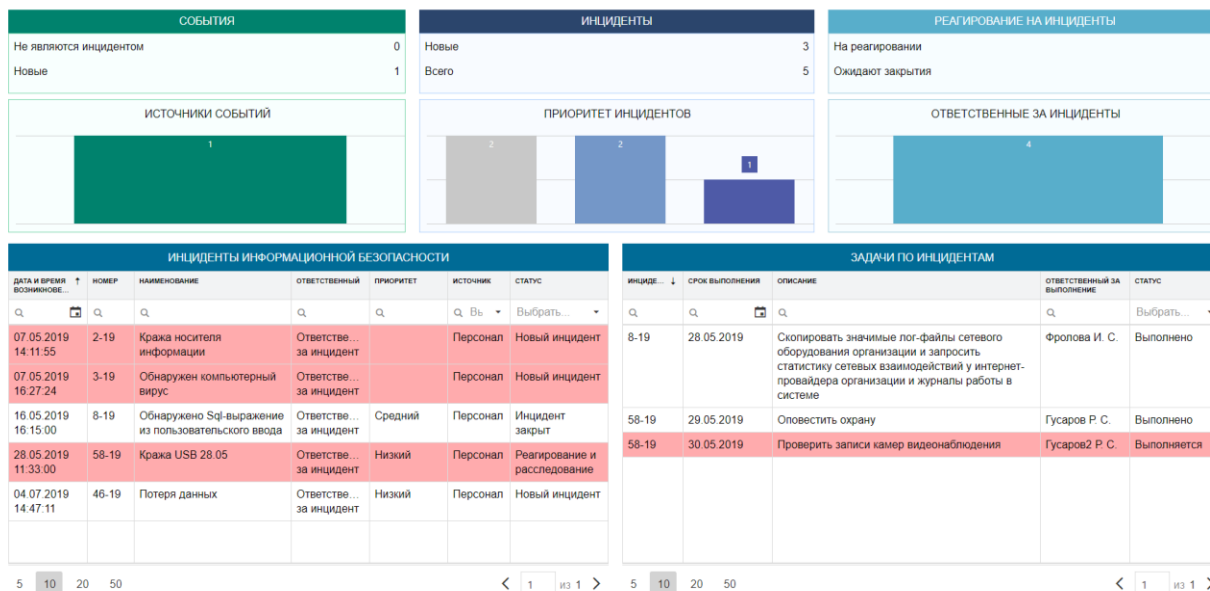


Рисунок 48 – Стартовая страница пользователя «Руководство СУИБ»
 Стартовая страница состоит из следующих виджетов:

1. Виджет «События информационной безопасности» (Рисунок 49)

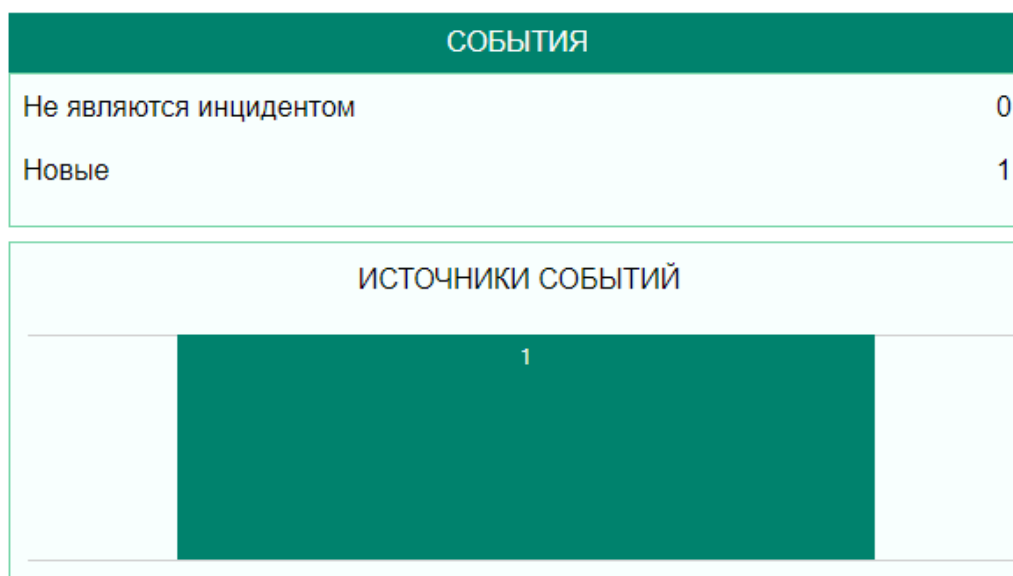


Рисунок 49 – Виджет «События информационной безопасности»

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 50).

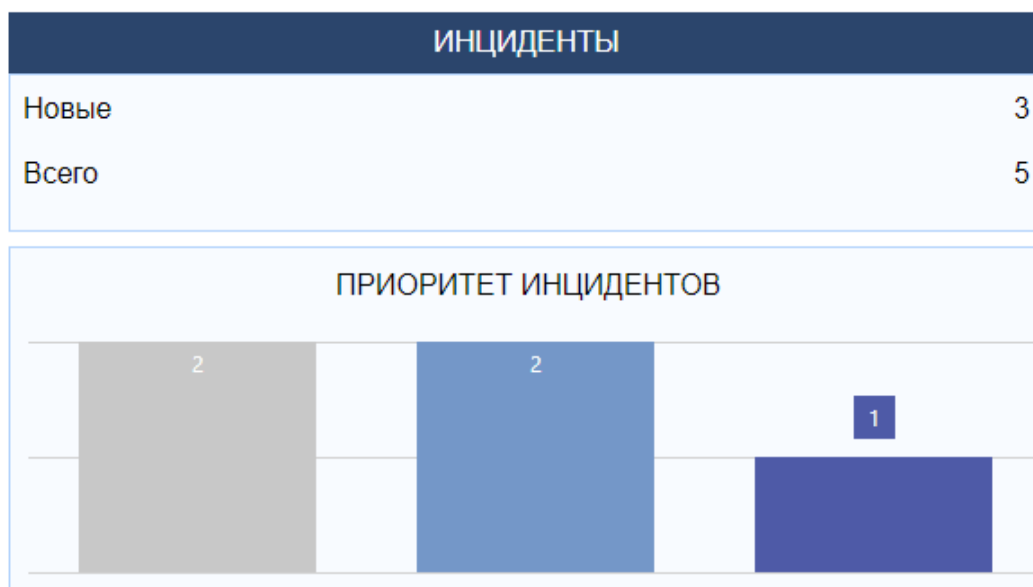


Рисунок 50 – Виджет «Инциденты информационной безопасности»

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 51).

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.

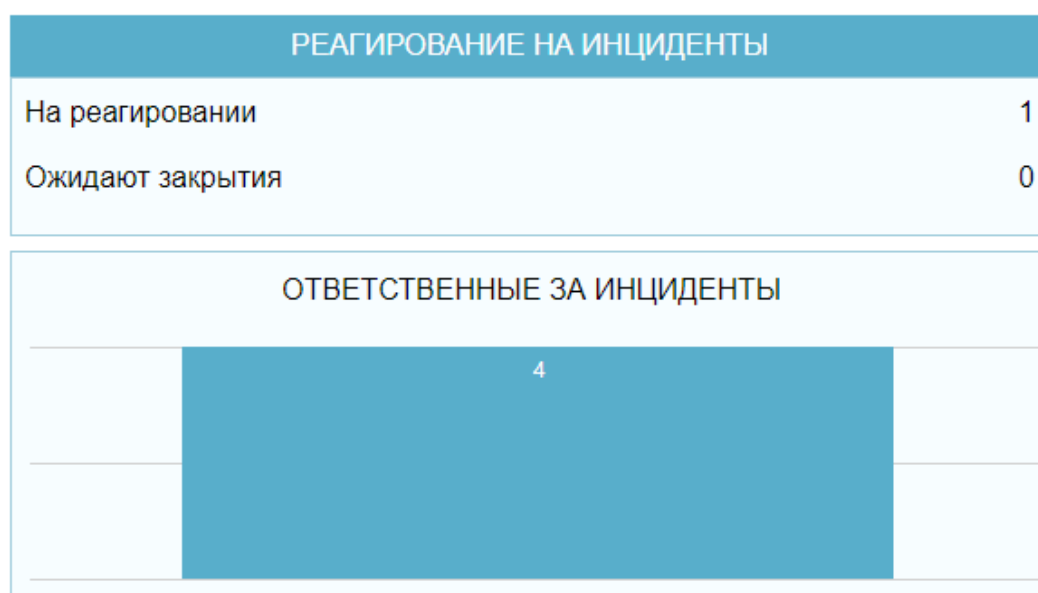


Рисунок 51 – Виджет «Реагирование на инциденты»

4. Таблица «Инциденты информационной безопасности» (Рисунок 52).

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
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 >

Рисунок 52 – Таблица «Инциденты информационной безопасности»

5. Таблица «Задачи по инцидентам» (Рисунок 53).

ЗАДАЧИ ПО ИНЦИДЕНТАМ				
ИНЦИДЕ... ↓	СРОК ВЫПОЛНЕНИЯ	ОПИСАНИЕ	ОТВЕТСТВЕННЫЙ ЗА ВЫПОЛНЕНИЕ	СТАТУС
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 >

Рисунок 53 – 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 54).

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

<input type="checkbox"/>	Дата и время возникн... ↓	Номер	Наименование	Ответственный	Источник события
<input type="checkbox"/>	05.07.2019 10:51:52	26	Зафиксированы помехи при передаче информации	test	Персонал
<input type="checkbox"/>	04.07.2019 15:08:51	23	Неисправность оборудования	Ответствен...	Персонал

Рисунок 54 – 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 55).

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

На соответствующих вкладках панели отображается список инцидентов ИБ, 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.

Реестр инцидентов ИБ Новый инцидент

Новые В работе Обработанные

<input type="checkbox"/>	Дата и время ↓ возникновения	Номер	Наименование	Подкласс	Приоритет	Источник	Ответственный
<input type="checkbox"/>	01.12.2017 08:25:52	08.25.08/ ИИБ/4	Test Incident		Высокий	MaxPatrol SIEM	k.nadezhdenko
<input type="checkbox"/>	15.11.2016 07:14:00	08.25.08/ ИИБ/2	Тест Инцидент Уведомление		Высокий	MaxPatrol SIEM	d.tifenko
<input type="checkbox"/>		08.25.08/ ИИБ/6	test		Средний	MaxPatrol SIEM	
<input type="checkbox"/>		08.25.08/ ИИБ/7	test		Средний	MaxPatrol SIEM	
<input type="checkbox"/>		08.25.08/ ИИБ/8	test		Средний	MaxPatrol SIEM	
		08.25.08/ ИИБ/8	test		Средний	MaxPatrol	

5 10 20 50 Всего записей: 9 < 1 из 1 >

Не является инцидентом

Рисунок 55 – Информационная панель «Реестр инцидентов ИБ»

8. Информационная панель «Справочники» (Рисунок 56).

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

Справочники УИ

Классификация инцидентов Сценарии реагирования Угрозы Виды инцидентов Правила корреляции Время реагирования

Подклассы инцидента

Наименование	Приоритет	Сценарий	
нет значения			
Тест Эксперт подкласс	Низкий		✘
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	Реагирование на сетевые атаки	✘
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			
Запрещенный контент	Низкий		✘
Контент панического характера	Низкий		✘
Контент злонамеренного характера	Низкий		✘

Всего записей: 132 < 1 из 14 >

Рисунок 56 – Информационная панель «Справочники»

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

9. Информационная панель «Реестр планов реагирования на инцидент информационной безопасности» (Рисунок 57).

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

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.

РЕЕСТР ПЛАНОВ РЕАГИРОВАНИЯ НА ИНЦИДЕНТ ИБ, ТРЕБУЮЩИХ УТВЕРЖДЕНИЯ				
НОМЕР ИНЦИДЕНТА	НАИМЕНОВАНИЕ ИНЦИДЕНТА	ОТВЕТСТВЕННЫЙ	ПРИОРИТЕТ	СРОК РЕАГИРОВАНИЯ
08.25.08/ИББ/5	Кража информации	kkudryashova	Высокий	08.11.2019 17:11:28

Рисунок 57 – Информационная панель «Реестр планов реагирования на инцидент информационной безопасности»

6.3.2 Управление событиями и инцидентами ИБ

Пользователь с ролью «Руководство СУИБ» имеет полный доступ к управлению событиями и инцидентами ИБ. Процедуры обработки события и инцидента подробно описаны в разделах «Создание и удаление новой записи о событии информационной безопасности» и «Создание и удаление записи об инциденте информационной безопасности».

6.3.3 Утверждение и возврат на корректировку плана реагирования на инцидент информационной безопасности

Для того чтобы просмотреть и отредактировать план реагирования на инцидент информационной безопасности, пользователь должен выполнить следующие действия:

1. Перейти в карточку плана реагирования на инцидент ИБ (Рисунок 58) любым из следующих способов:
 - из перечня планов реагирования на инцидент ИБ, требующих утверждения (в боковом меню пользователя выбрать пункт «УИИБ», «Реестр планов реагирования»);
 - по ссылке из уведомления о необходимости утверждения плана реагирования.

План реагирования на инцидент Вернуть Утвердить

План мероприятий **Информация об инциденте**

Инцидент ИБ № 08.25.08/ИИБ/5 Приоритет: **Высокий** Срок реагирования до: 08.11.2019 17:11:28

Кража информации Выбрать из справочника + + + + + Требуется утверждения

Тип мероприятия	Описание	Ответств...	Выполнить до	
Расследов...	Провести консультации с сотрудниками подразделения	Кудряшова К.А.	18.11.2019	✖

5 10 20 50 Всего записей: 1 < 1 из 1 >

Рисунок 58 – Карточка плана реагирования на инцидент ИБ

2. Для добавления в план мероприятия из справочника на вкладке «План мероприятий» подвкладке «Требуется утверждения» нажать кнопку Выбрать из справочника. Откроется форма добавления мероприятия из справочника (Рисунок 59).

Добавление мероприятия ★ 🗨 ✕

Тип мероприятия *

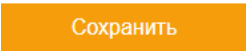


Текст

Мероприятия ИБ




Текст

Сохранить Отменить


Рисунок 59 – Форма добавления мероприятия из справочника

3. Указать тип мероприятия и выбрать нужное мероприятие из выпадающего списка.
4. Нажать кнопку . *Выбранное мероприятие будет добавлено в план реагирования.* Внимание! После утверждения плана и перехода к этапу реагирования и расследования добавленные мероприятия будут доступны только для чтения. Для отмены действия необходимо закрыть форму или нажать на кнопку .
5. Для добавления в план реагирования нового мероприятия на вкладке «План мероприятий» подвкладке «Требует утверждения» нажать кнопку . *В таблице отобразится пустая строка.*
6. 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.

7. При необходимости данные таблицы можно отредактировать. Для сохранения изменений необходимо нажать кнопку . Для отмены действия нажмите кнопку .
8. Для удаления мероприятия на вкладке «План мероприятий» нажать кнопку  в соответствующей строке.

Для того чтобы вернуть план реагирования на инцидент информационной безопасности на корректировку, пользователь должен выполнить следующие действия:

1. В карточке плана реагирования нажать кнопку . Откроется форма ввода комментария (Рисунок 60).

Вернуть план реагирования на доработку

Комментарий

Введите рекомендации по корректировке плана

Подтвердить

Отменить

Рисунок 60 – Форма ввода комментария при возврате плана реагирования на корректировку

2. При необходимости ввести рекомендации по корректировке плана реагирования. Нажать кнопку **Подтвердить**. 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.
3. Для отмены возврата плана реагирования на корректировку необходимо закрыть форму или нажать на кнопку **Отменить**.

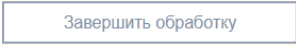
Для того чтобы утвердить план реагирования на инцидент информационной безопасности, пользователь должен выполнить следующие действия:

1. В карточке плана реагирования нажать кнопку **Утвердить**. *План реагирования будет утвержден. Пользователю, ответственному за обработку инцидента, будет отправлено соответствующее уведомление. Согласно утвержденному плану реагирования на пользователей, которые назначены ответственными за выполнения новых мероприятий, будут назначены задачи и отправлены уведомления. При первичном утверждении текущий статус инцидента изменится с «Новый инцидент» на «Реагирование и расследование», на карточке инцидента отобразится вкладка*

«Реагирование и расследование» (Рисунок 46) с перечнем мероприятий по реагированию и расследованию, сгруппированным по статусу.

6.3.4 Закрытие и возврат на доработку инцидента ИБ

Для того чтобы завершить обработку инцидента, пользователь должен выполнить следующие действия:




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 «Формирование заключения»*).
2. Для закрытия инцидента необходимо на вкладке «Заключение» нажать кнопку  (доступна только на статусе «Формирование заключения»). **Внимание!** После закрытия инцидента карточка инцидента за исключением вкладки «Документы» станет доступна только для чтения. *Откроется форма выбора оповещаемых лиц (Рисунок 61). В список оповещаемых лиц будут автоматически добавлены сотрудники, проводившие расследование и реагирование на инцидент, а также руководитель ГРИИБ.*

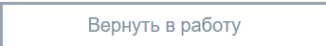
Выберите работников для отправки уведомления о закрытии инцидента

ФИО	Должность	Подразделение	Email	
q	q	q	q	

Уведомить и закрыть инцидент
Закрыть инцидент
Отменить

Рисунок 61 – Форма выбора оповещаемых лиц

3. Для добавления оповещаемых лиц на форме «Выбор оповещаемых лиц» необходимо в таблице:
 - нажать кнопку . Откроется форма выбора;
 - выбрать необходимые записи с помощью флага ;
 - нажать кнопку Сохранить.
4. Для удаления сотрудника из списка оповещаемых лиц нажать кнопку  в соответствующей строке.
5. После заполнения формы возможно следующие действия:
 - для закрытия инцидента и отправки уведомлений выбранным сотрудникам необходимо 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 необходимо 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.

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

6.3.5 Работа со справочниками

Пользователь с ролью «Руководство СУИБ» имеет полный доступ к справочникам Модуля. Процедура ведения справочников подробно описана в разделе «Работа со справочниками».

6.3.6 Мониторинг и контроль управления инцидентами ИБ

Для мониторинга статистической информации по зарегистрированным событиям и инцидентам ИБ пользователь с ролью «Руководство СУИБ» имеет доступ к просмотру формы со статистикой (Рисунок 62). Подробное описание формы приведено в разделе «Стартовая страница пользователя» роли «Эксперт по управлению инцидентами ИБ».

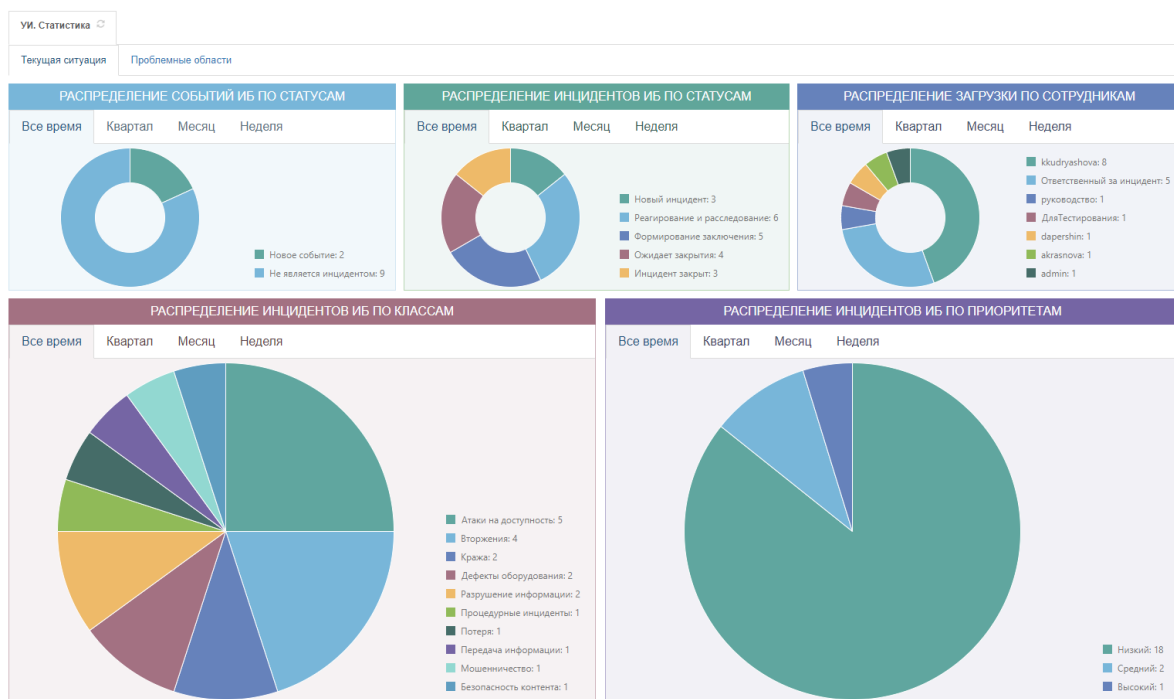


Рисунок 62 – Форма для просмотра статистики по зарегистрированным событиям и инцидентам

6.4 Роль «Участник ГРИИБ»

Задача пользователя с ролью «Участник ГРИИБ» — выполнение задач по расследованию и реагированию на инциденты ИБ и ввод результатов их выполнения. Пользователь имеет доступ к реестру мероприятий по расследованию и реагированию на инциденты, назначенных на данного пользователя.

6.4.1 Стартовая страница пользователя

Для того чтобы перейти к стартовой странице Модуля необходимо нажать на логотип сайта в левом верхнем углу.

Стартовая страница пользователя с ролью «Участник ГРИИБ» (Рисунок 63) предназначена для отображения основной информации о зарегистрированных инцидентах, о задачах и мероприятиях по реагированию, назначенных на пользователя.

The screenshot displays the user's dashboard with the following components:

- Incidents Summary:**

ИНЦИДЕНТЫ	
Новые	32
Всего	46
- Response Activities Summary:**

МЕРОПРИЯТИЯ ПО РЕАГИРОВАНИЮ	
Выполняется	2
Выполнено	5
- Main Table: Мероприятия по реагированию на инциденты**

ИНЦ...	ОПИСАНИЕ	СТАТУС	СРОК ВЫПОЛНЕНИЯ
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
20-19	Мероприятие по реагированию 1	Выполнено	01.07.2019
20-19	Мероприятие 2	Выполнено	02.07.2019
20-19	Мероприятие 3	Выполняется	02.07.2019
	Проанализировать вредоносное ПО	Выполнено	27.05.2019

Рисунок 63 – Информационная панель «Рабочая область Участника ГРИИБ»

Стартовая страница состоит из следующих виджетов:

1. Виджет «Инциденты» (Рисунок 64) содержит данные о всех зарегистрированных инцидентах ИБ.

ИНЦИДЕНТЫ	
Новые	32
Всего	46

Рисунок 64 – Виджет «Инциденты»

Виджет содержит счётчик новых инцидентов ИБ, требующих обработки, и общее количество зарегистрированных инцидентов ИБ.

2. Виджет «Мероприятия по реагированию» (Рисунок 65).

МЕРОПРИЯТИЯ ПО РЕАГИРОВАНИЮ	
Выполняется	2
Выполнено	5

Рисунок 65 – Виджет «Мероприятия по реагированию»

Виджет содержит счётчик мероприятий по реагированию, назначенных на пользователя (мероприятия на статусе «Выполняется»), и количество выполненных пользователем мероприятий (мероприятия на статусе «Выполнено»).

3. Виджет «Мероприятия по реагированию на инциденты» (Рисунок 66).

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
20-19	Мероприятие по реагированию 1	Выполнено	01.07.2019
20-19	Мероприятие 2	Выполнено	02.07.2019
20-19	Мероприятие 3	Выполняется	02.07.2019
	Проанализировать вредоносное ПО	Выполнено	27.05.2019

5 10 20 50 < 1 из 1 >

Рисунок 66 – 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 67).

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...	ГРИИБ	01.07.2019	➔

Рисунок 67 – Виджет с перечнем задач, назначенных на пользователя

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


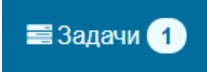

На вкладке «Назначенные на меня» отображаются незакрытые задачи. Красным цветом выделены задачи с истекшим сроком выполнения.

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

6.4.2 Работа с задачами по реагированию и расследованию инцидента информационной безопасности

Мероприятия по реагированию на инцидент создаются в карточке инцидента пользователями в роли «Ответственный за инцидент ИБ» или «Руководство СУИБ».

Соответственно каждому мероприятию создается системная задача. Для того чтобы ввести результаты выполнения задачи по реагированию на инцидент ИБ, пользователь должен выполнить следующие действия:

1. Перейти в карточку задачи 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  на верхней панели и на вкладке «Назначенные на меня» дважды нажать по строке с задачей или по кнопке .

Откроется карточка задачи по реагированию на инцидент (Рисунок 68).

Выполнить мероприятие по расследованию инцидента №28-19

Начать выполнение задачи

Общая информация о задаче

Информация о мероприятии по реагированию

Отчет о выполнении *

Отчет о выполнении

Документ

Документ

Привлечённые сотрудники

Фамилия И.О.	Должность	Подразделение
🔍	🔍	🔍

5 10 20 50

Всего записей: 0 < 1 из 1 >

Информация об инциденте

Инцидент ИБ № 28-19	Приоритет	Срок реагирова
Network_host_inaccessibility	Высокий	26.04.2019 1

Рисунок 68 – Карточка задачи по реагированию на инцидент

Карточка задачи состоит из трех разделов: общая информация о задаче, информация о мероприятии и информация об инциденте.

В разделе «Общая информация» (Рисунок 69) расположена служебная информация о задаче, недоступная для редактирования.

Общая информация о задаче

Срок выполнения: 10.07.2019 Дата создания: 10.07.2019 Статус: Открыта

Назначено на: ГРИИБ Автор: akrasnova Идентификатор задачи: 995332

Описание:

Устранить последствия инцидента

Рисунок 69 – Раздел «Общая информация» в карточке задачи


В раздел «Информация о мероприятии по реагированию» (Рисунок 70) расположена информация о результатах выполнения реагирования на инцидент ИБ.


Информация о мероприятии по реагированию

Отчет о выполнении *

Отчет о выполнении

Документ

Документ 

Привлечённые сотрудники 

Фамилия И.О.	Должность	Подразделение	
🔍	🔍	🔍	

5 10 20 50 Всего записей: 0 < 1 из 1 >

Рисунок 70 – Раздел «Информация о мероприятии по реагированию» в карточке задачи

В разделе «Информация об инциденте» (Рисунок 71) расположена служебная информация о соответствующем задаче инциденте ИБ, недоступная для редактирования.

Информация об инциденте

Инцидент ИБ № 28-19

Network_host_inaccessibility

Приоритет: Высокий

Срок реагирования до: 26.04.2019 12:30:41

Общая информация

Дата и время возникновения	Дата и время обнаружения	Дата и время оповещения	Описание
25.04.2019 12:30:29	25.04.2019 12:30:41	26.05.2019 23:14:52	
Источник события	Класс инцидента	Подкласс инцидента *	
MaxPatrol SIEM	Инциденты MP SIEM	Не определен	
Что произошло	Узел 192.168.21.122 недоступен		
Как произошло	Текст		
Почему произошло	Текст		

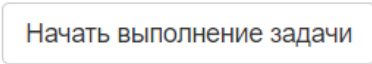



Объекты защиты

Угрозы

Связанные события

Последствия

Рисунок 71 – Раздел «Информация об инциденте» в карточке задачи

1. Нажать кнопку  вверху карточки задачи. Задача перейдет на статус «В работе».
2. В разделе «Информация о мероприятии по реагированию» необходимо:
 - ввести текст отчета о выполнении;
 - при необходимости загрузить документ по кнопке  – какой-либо отчетный материал по выполненному мероприятию;
 - при необходимости указать привлеченных к реагированию работников по кнопке  ;
 - во всплывающем окне (Рисунок 72) с помощью флага выбрать работников и нажать на кнопку  .

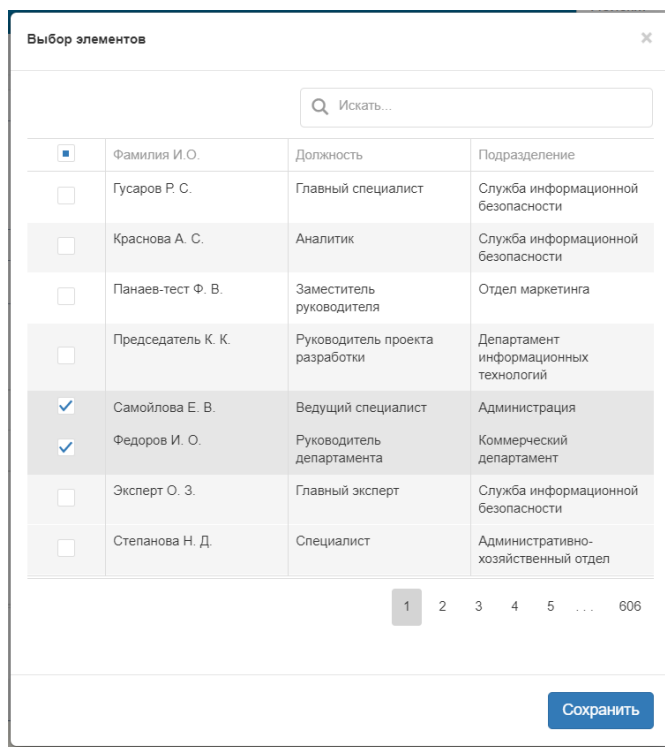


Рисунок 72 – Окно для выбора привлеченных к реагированию работников

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  .

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».

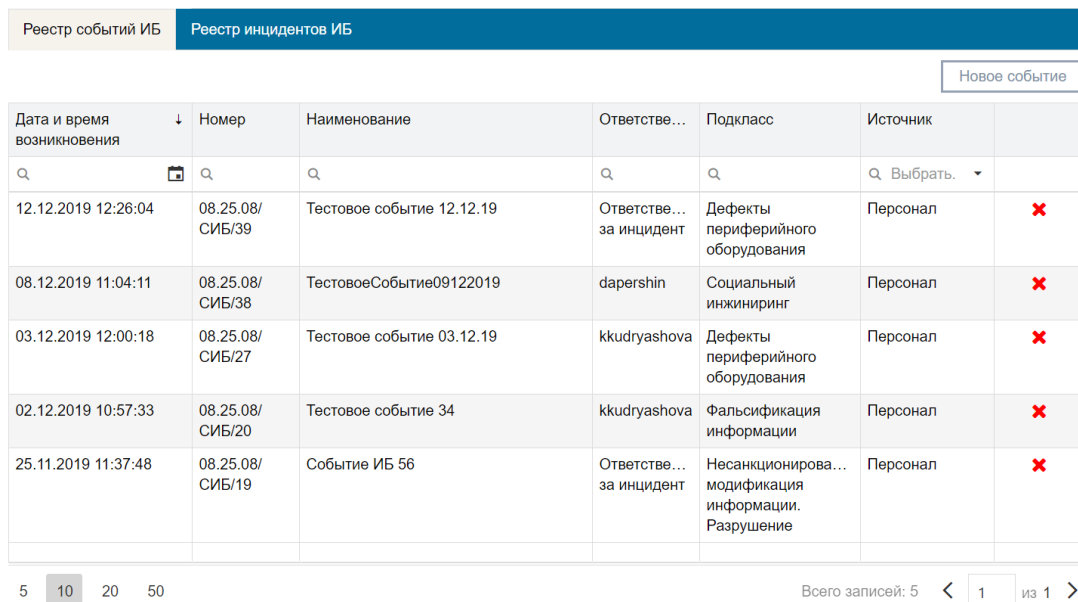
6.5 Роль «Оператор-диспетчер»

Задача пользователя с ролью «Оператор-диспетчер» — создание новых событий и инцидентов информационной безопасности и назначение пользователей, ответственных за их обработку. Пользователь имеет доступ к редактированию и удалению новых событий и инцидентов.

6.5.1 Стартовая страница пользователя

Для того чтобы перейти к стартовой странице Модуля необходимо нажать на логотип сайта в левом верхнем углу и перейти на вкладку «Управление инцидентами информационной безопасности».

Стартовая страница пользователя с ролью «Оператор-диспетчер» (Рисунок 73) предназначена для отображения списка новых событий и инцидентов ИБ.




Дата и время возникновения	Номер	Наименование	Ответстве...	Подкласс	Источник	
12.12.2019 12:26:04	08.25.08/СИБ/39	Тестовое событие 12.12.19	Ответстве... за инцидент	Дефекты периферийного оборудования	Персонал	✘
08.12.2019 11:04:11	08.25.08/СИБ/38	ТестовоеСобытие09122019	dapershin	Социальный инжиниринг	Персонал	✘
03.12.2019 12:00:18	08.25.08/СИБ/27	Тестовое событие 03.12.19	kkudryashova	Дефекты периферийного оборудования	Персонал	✘
02.12.2019 10:57:33	08.25.08/СИБ/20	Тестовое событие 34	kkudryashova	Фальсификация информации	Персонал	✘
25.11.2019 11:37:48	08.25.08/СИБ/19	Событие ИБ 56	Ответстве... за инцидент	Несанкционирова... модификация информации. Разрушение	Персонал	✘

Рисунок 73 – Стартовая страница пользователя с ролью «Оператор-диспетчер»

6.5.2 Создание и удаление новой записи о событии информационной безопасности

Для того чтобы создать запись о событии ИБ, пользователь должен выполнить следующие действия:

1. На стартовой странице пользователя перейти на вкладку «Реестр событий ИБ».
2. На информационной панели «Реестр событий ИБ» нажать кнопку . Откроется карточка нового события (Рисунок 74).
3. В открывшейся форме заполнить доступные поля. По умолчанию поля «Дата и время возникновения», «Дата и время обнаружения», «Дата и время оповещения» заполняются значениями текущей даты и времени, в поле «Ответственный за событие» 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».

Карточка нового события

Событие 35

Наименование события *

Наименование

Дата и время возникновения Дата и время обнаружения Дата и время оповещения

05.07.2019 13:12:09 05.07.2019 13:12:09 05.07.2019 13:12:09

Класс события *

Класс

Подкласс события *

Подкласс

Оповестил работник Ответственный за событие *

Ответственный за инцидент

Дополнительно

Информация о сообщившем

Что произошло

Информация о событии

Сохранить и закрыть Сохранить и перейти к событию


Рисунок 74 – Карточка нового события ИБ

4. После заполнения формы возможны следующие действия:
- для создания записи о событии и возврата в реестр событий ИБ необходимо нажать кнопку **Сохранить и закрыть**;
 - для создания записи о событии и перехода в карточку созданного события необходимо нажать кнопку **Сохранить и перейти к событию**.

Для удаления нового события в таблице «Реестр событий ИБ» нажать кнопку **✗** в соответствующей строке.

6.5.3 Создание и удаление записи об инциденте информационной безопасности

Для того чтобы создать запись о событии ИБ, пользователь должен выполнить следующие действия:




1. На стартовой странице пользователя перейти на вкладку «Реестр инцидентов ИБ».
2. На информационной панели «Реестр инцидентов ИБ» нажать на кнопку . Откроется карточка нового инцидента (Рисунок 75).

Карточка нового инцидента ×

Инцидент ИБ

Наименование инцидента *

Дата и время возникновения Дата и время обнаружения Дата и время оповещения

05.06.2020 16:40:21  05.06.2020 16:40:21  05.06.2020 16:40:21 

Класс инцидента *

+

Подкласс инцидента *

+

Тип инцидента Ответственный за инцидент *

Действительный × ▾ Ответственный за инцидент × ▾

Что произошло



Сохранить и закрыть Сохранить и перейти к инциденту


Рисунок 75 – Карточка нового инцидента ИБ

3. В открывшейся форме заполнить доступные поля. По умолчанию поля «Дата и время возникновения», «Дата и время обнаружения», «Дата и время оповещения» заполняются значениями текущей даты и времени, в поле «Ответственный за инцидент ИБ (исполнитель отчета)» (сотрудник, ответственный за обработку инцидента) указывается текущий пользователь. При необходимости данные этих полей можно отредактировать.

Внимание! Исполнитель отчета 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  .

Для удаления нового инцидента в таблице «Реестр инцидентов ИБ» нажать кнопку  в соответствующей строке.

6.6 Роль «САПУИБ»

Задача пользователя с ролью «САПУИБ» — формирование и просмотр статистических данных о зарегистрированных событиях и инцидентах.

6.6.1 Стартовая страница пользователя

Статистические данные на основе информации о зарегистрированных событиях и инцидентах формируются автоматически и отображаются в виде графиков на стартовой странице пользователя (Рисунок 76). Подробное описание формы стартовой страницы приведено в разделе «Стартовая страница пользователя» роли «Эксперт по управлению инцидентами ИБ».

Для того чтобы перейти к стартовой странице Модуля необходимо нажать на логотип сайта в левом верхнем углу и перейти на вкладку «Управление инцидентами информационной безопасности».

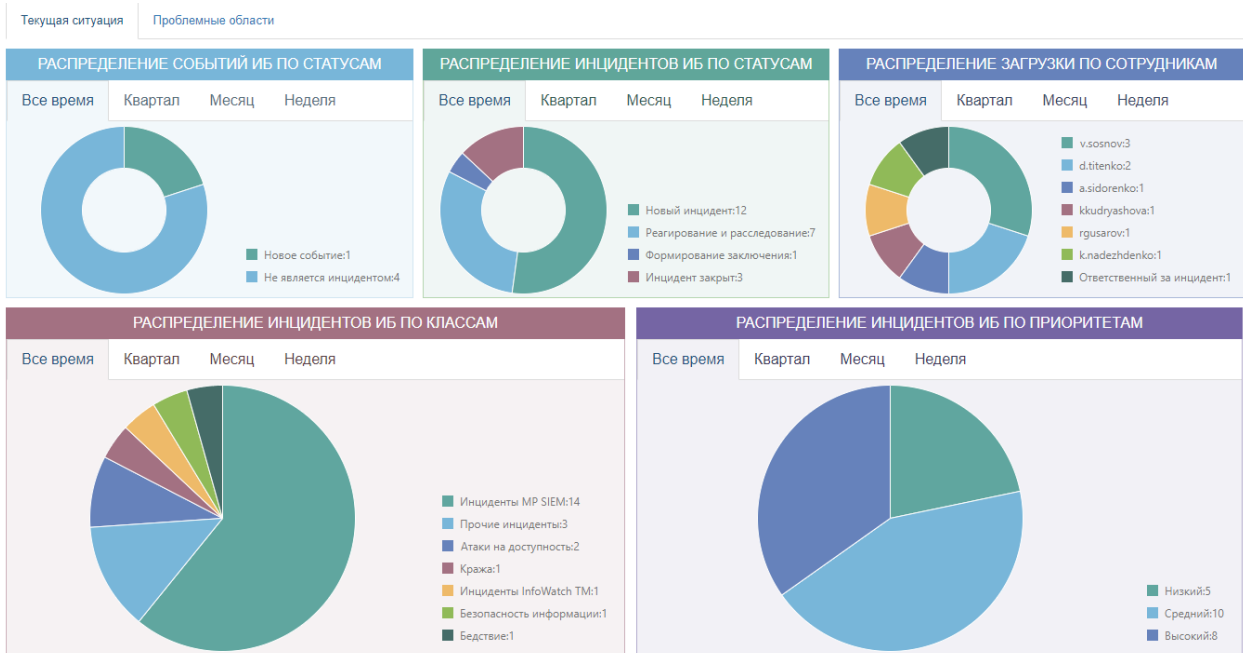


Рисунок 76 – Стартовая страница пользователя с ролью «САПУИБ»

7 Перечень сокращений

- ГРИИБ – группа реагирования на инциденты ИБ
- ИБ – информационная безопасность
- УИБ – управление информационной безопасностью