

**«СИСТЕМА АВТОМАТИЗАЦИИ
ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ»**
Взаимодействие с НКЦКИ
Руководство пользователя

Содержание

- 1. Общие положения.....3**
 - 1.1. Термины, определения, сокращения..... 3
 - 1.2. Общие сведения..... 3
 - 1.3. Назначение модуля..... 3
- 2. Описание ролевой модели..... 4**
- 3. Начало работы с модулем.....5**
- 4. Рабочая область Эксперта ГосСОПКА..... 6**
- 5. Сценарии работы пользователя..... 7**
 - 5.1. Работа с реестром инцидентов..... 7
 - 5.1.1. Карточка инцидента..... 7
 - 5.2. Обработка инцидента.....8

1. Общие положения

1.1. Термины, определения, сокращения

В настоящем руководстве использованы следующие сокращения:

ГосСОПКА - государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы.

ИБ - информационная безопасность.

КИИ - критическая информационная инфраструктура.

НКЦКИ - национальный координационный центр по компьютерным инцидентам.

ОКИИ - объект критической информационной инфраструктуры.

САОБ - система автоматизации обеспечения безопасности.

1.2. Общие сведения

Настоящее руководство пользователя устанавливает порядок работы с модулем «Взаимодействие с НКЦКИ».

1.3. Назначение модуля

Модуль используется для обработки инцидентов, связанных с субъектами или объектами критической информационной инфраструктуры (далее – КИИ) для последующей передачи информации государственному регулятору – Национальному координационному центру по компьютерным инцидентам (далее – НКЦКИ).

2. Описание ролевой модели

Для получения доступа к работе с модулем пользователь должен быть включен в роль «Эксперт ГосСОПКА» (далее – Эксперт).

Пользователь в роли Эксперта имеет доступ к реестру инцидентов ИБ, статистике инцидентов, выполняет функционал по отправке инцидентов ИБ в Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

3. Начало работы с модулем

Для начала работы с модулем выполните следующие действия:

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

4. Рабочая область Эксперта ГосСОПКА

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

Рабочая область Эксперта (Рисунок 1) содержит следующие элементы:

- 1. Диаграмма, отображающая распределение инцидентов ИБ по статусам.
- 2. Диаграмма, отображающая распределение инцидентов ИБ по статусам отправки.
- 3. Реестр инцидентов ИБ.

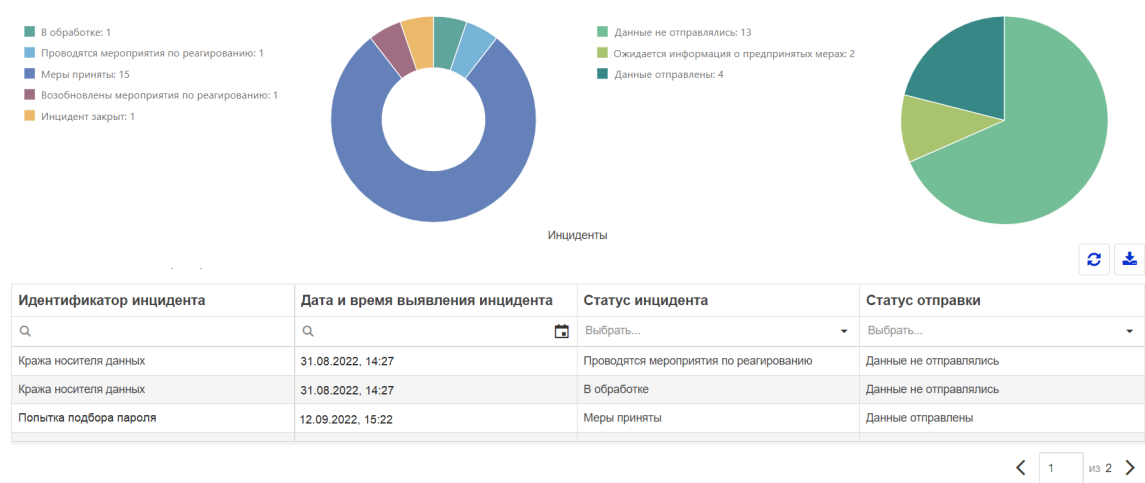


Рис. 1. Рабочая область Эксперта ГосСОПКА

Переход к реестру также возможно осуществить, открыв в боковом меню раздел «Инциденты».

5. Сценарии работы пользователя

В разделе приведены сценарии работы пользователя в роли, предусмотренной для корректного функционирования модуля.

5.1. Работа с реестром инцидентов

Для работы с инцидентами ИБ с помощью бокового меню перейдите в раздел «Инциденты». Откроется реестр, содержащий инциденты ИБ (Рисунок 2).

Инциденты могут быть созданы вручную или загружены в реестр из смежных систем. Инциденты имеют первоначальный статус «Меры приняты» и подлежат отправке в НКЦКИ.

Реестр инцидентов				
Идентификатор инцидента	Дата и время выявления инцидента	Статус инцидента	Статус отправки	Субъект КИИ
Q	Q	Выбрать...	Выбрать...	Q
Кража носителя данных	31.08.2022, 14:27	Меры приняты	Данные не отправлялись	Новая организация
Кража носителя данных	31.08.2022, 14:27	В обработке	Данные не отправлялись	Новая организация
Попытка подбора пароля	12.09.2022, 15:22	Меры приняты	Данные отправлены	Новая организация

< 1 из 3 >

Рис. 2. Реестр инцидентов

5.1.1. Карточка инцидента

Для перехода к карточке инцидента ИБ дважды кликните на соответствующую строку реестра (Рисунок 2).

Инцидент

Создан вручную

Кража носителя данных

Меры приняты

Данные не отправлялись

Заполнение
общих сведений

Подтверждение
инцидента

Реагирование
на инцидент

Завершение
обработки инцидента

Инцидент в УКИНС: Кража носителя данных

Описание

Объект атаки и влияние

Рекомендации

Меры по реагированию

Расследование

История изменений

Идентификатор уведомления *

Кража носителя данных

Ограничительный маркер *

TLP:GREEN

Субъект КИИ *

Новая организация

Сведения о средстве или способе выявления инцидента

Краткое описание события ИБ *

Кража носителя данных

Дата и время обнаружения *

31.08.2022 14:27:30

Тип уведомления *

Уведомление о компьютерном ...

Тип события ИБ *

Несанкционированное разглашен...

Объект КИИ *

АСУ ТП

Объект размещения *

Объект С-300

Содействие ГосСОПКА

Отчет по уведомлению

Сформируйте отчет

Лица, ответственные за взаимодействие с НКЦКИ по данному инциденту

Фамилия Имя Отчество

Должность

Контактный телефон

Адрес электронной почты

Рис. 3. Карточка инцидента

В верхней части карточки отображаются наименование инцидента, статусы инцидента, ссылка на соответствующий инцидент в смежной системе. Карточка инцидента ИБ содержит вкладки:

- Описание - содержит основную информацию об инциденте, заполненную на основе сведений, указанных в смежной системе.
- Объект атаки и влияние - содержит основную информацию о влиянии последствий инцидента, указанную в смежной системе.
- Рекомендации - содержит перечень рекомендаций для ликвидации последствий инцидента, указанных в смежной системе.
- Меры по реагированию - содержит меры, предпринятые для реагирования и расследования инцидента; заполняется с помощью кнопки «Получить мероприятия».
- История изменений - содержит информацию об изменениях статуса инцидента.

5.2. Обработка инцидента

1. В реестре откройте карточку инцидента.

Рис. 4. Карточка инцидента

2. На вкладке «Описание» карточки инцидента заполните обязательные поля:
 - «Объект размещения» - выберите объект размещения, привязанный к ОККИ.
 - «Краткое описание события ИБ» - введите описание инцидента.
3. На вкладке «Меры по реагированию» нажмите кнопку [Получить мероприятия](#), чтобы получить перечень мероприятий по расследованию и реагированию из смежной системы (Рисунок 5).
4. После заполнения карточки инцидента, нажмите кнопку [Отправить в НКЦКИ](#) для отправки в НКЦКИ.
5. После получения ответа от НКЦКИ Эксперт закрывает инцидент.

Дата и время восстановления штатного режима работы ИП после КИ

Дата и время восстановления

Предпринятые меры по реагированию на ...

Получить мероприятия

Дата и время фиксации в НКЦКИ	Описание предпринятых действий	Наименование субъекта, сообщившего о принятых мерах	
<div>🔍</div> <div></div>	<div>🔍</div> <div></div>	<div>🔍</div> <div></div>	
	Сбор и проверка данных	Новая организация	✖

<

1

из 1

>

Сохранить

Отправить в НКЦКИ

Рис. 5. Заполнение вкладки «Меры по реагированию».