ООО «Компания Информационных Технологий»

«СИСТЕМА АВТОМАТИЗАЦИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ»

Моделирование угроз безопасности

Руководство пользователя

Екатеринбург
2022

Содержание

1. Общие положения

1.1. Термины, определения, сокращения

В настоящем руководстве использованы следующие термины:

Объект критической информационной инфраструктуры (объект КИИ) — информационная система, автоматизированная система управления или информационно-телекоммуникационная сеть, представляющая собой совокупность объектов защиты, выполняющих критический бизнес-процесс.

Субъект критической информационной инфраструктуры (Субъект КИИ) – организация (юридическое лицо), которому на праве собственности (или ином законном основании) принадлежат объекты КИИ.

Шаблон — создаваемый и настраиваемый объект в модуле, используемый для создания сущностей с заранее заданными параметрами.

Элемент справочника — создаваемый и редактируемый в модуле объект, применяемый для ввода (выбора из списка) часто используемой информации.

Пользователь — сотрудник организации или иной организации, получивший в установленном порядке доступ к модулю.

1.2. Общие сведения

Настоящее руководство пользователя устанавливает порядок работы с модулем «Моделирование угроз безопасности».

Модуль предназначен для моделирования угроз безопасности информации, данные моделирования угроз могут быть использованы для различных процессов обеспечения информационной безопасности, в том числе для процесса категорирования объектов критической информационной инфраструктуры.

1.3. Назначение модуля

Модуль предназначен для моделирования угроз безопасности информации, а также хранения информации о разработанных моделях угроз.

Модуль позволяет пользователям выполнять следующие функции:

- создание модели угроз при выключенном ручном моделировании;
- создание модели угроз при включенном ручном моделировании.

2. Описание ролевой модели

В модуле «Моделирование угроз безопасности» предусмотрены следующие роли пользователей:

- Эксперт ИБ ОКИИ;
- Системная роль.

Пользователь в роли **Эксперт ИБ ОКИИ** отвечает за организацию работы по обеспечению безопасности. Имеет полный доступ к моделированию угроз безопасности информации и доступ на чтение всей остальной информации, необходимой для выполнения его обязанностей.

Пользователь в роли **Системная роль** имеет полные полномочия по работе в системе, может настраивать интеграцию с другими системами, добавлять пользователей и вносить другие необходимые изменения в справочники и настройки.

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. Сценарии работы пользователей

4.1. Работа с моделированием угроз

Для начала работы со списком перейдите в раздел «Список моделей угроз» с помощью бокового меню.

На начальном экране раздела представлен список моделей угроз (Рисунок 1).

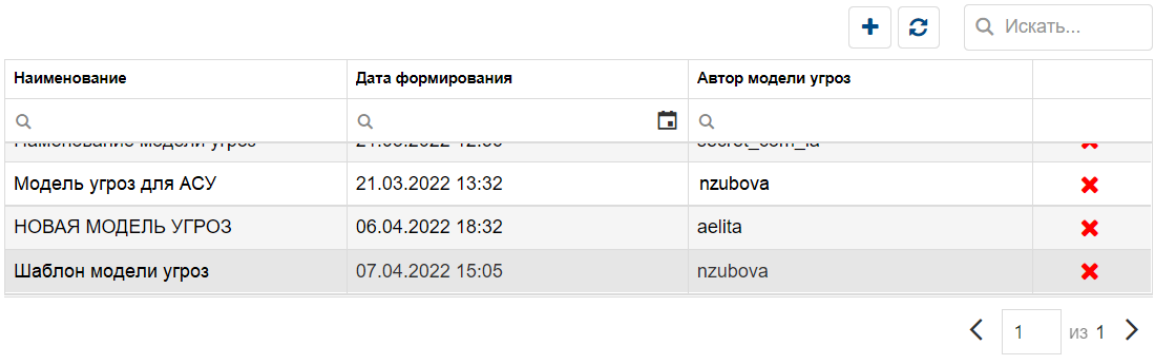

Рис. 1. Список моделей угроз

Предусмотрены следующие варианты работы со списком моделей угроз:

- создание новой модели угрозы (Создание новой модели угроз);
- просмотр карточки модели угрозы;
- редактирование карточки модели угрозы.

4.1.1. Создание новой модели угроз

Для создания новой модели угроз:

1. Нажмите кнопку ✚.
2. В всплывающем окне откроется карточка новой модели угрозы (Рисунок 2).
3. Заполните карточку:
    - введите наименование модели угроз;
    - дата формирования автоматически указана текущая;
    - выберите субъект КИИ;
    - выберите способ моделирования;

- укажите количество экспертов (если в поле «Моделирование вручную» выбран вариант «Да» количество экспертов указывать не требуется, соответствующее поле будет скрыто).

> **Прим.:**
>
> В поле «Количество экспертов» укажите количество пользователей, проводящих оценку. Если созданием модели угроз занимаются более 1 эксперта, то для формирования окончательного результата системой будет проведено сравнение оценок (система примет за окончательный вариант тот, который выбрали 50% и более экспертов).

4. Нажмите кнопку Создать, во всплывающем окне подтвердите действие.

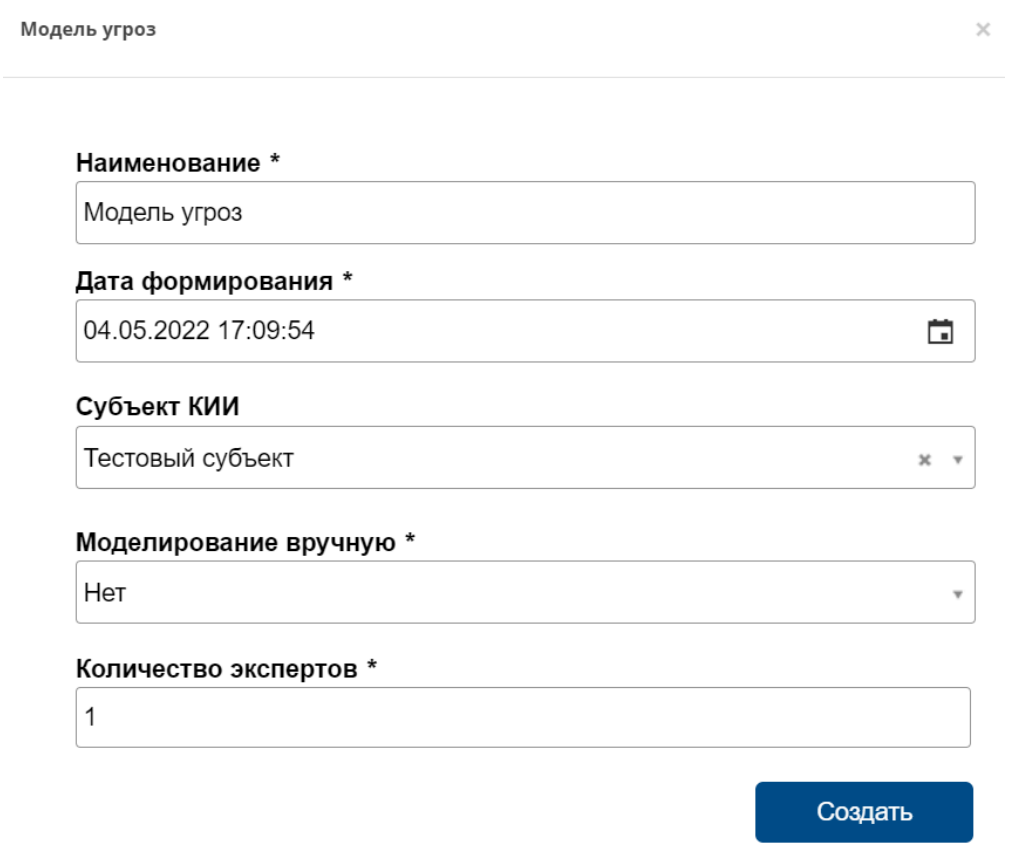

Рис. 2. Создание модели угроз

5. В списке будет добавлена новая модель угроз.
6. Для продолжения моделирования откройте карточку модели угроз и заполните в зависимости от выбранного способа моделирования:
   - Создание модели угроз при выключенном ручном моделировании;
   - Создание модели угроз при включенном ручном моделировании.

4.1.2. Создание модели угроз при выключенном ручном моделировании

Если при создании карточки модели угроз в поле «Моделирование вручную» был выбран вариант «Нет», то в карточку будут добавлены опросные листы для заполнения (Рисунок 3).

Опросные листы находятся на вкладке «Экспертная оценка».

Если экспертов несколько, опросные листы формируются для каждого эксперта. В этом случае опросные листы заполняются в два раунда.

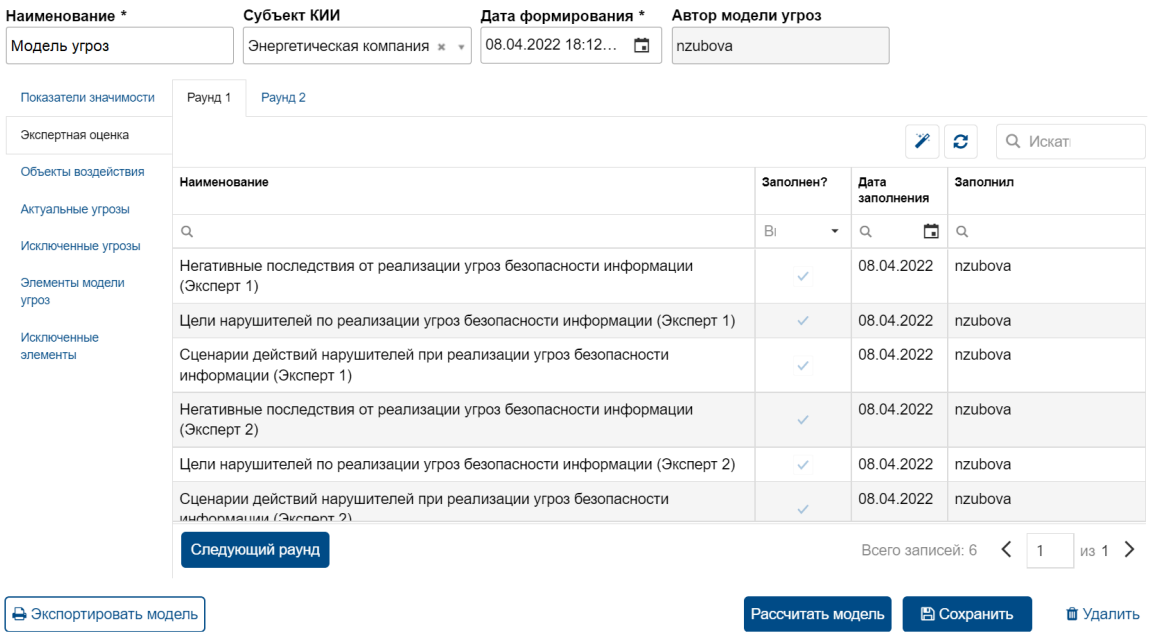

Рис. 3. Карточка модели угроз

Для заполнения опросного листа:

1. Перейдите на вкладку «Экспертная оценка».
2. Дважды кликните на название опросного листа.
3. Откроется карточка опросного листа (Рисунок 4).
4. В столбце «Ответ» выберите ответ на вопрос (по умолчанию на все вопросы выбран ответ «Нет»).

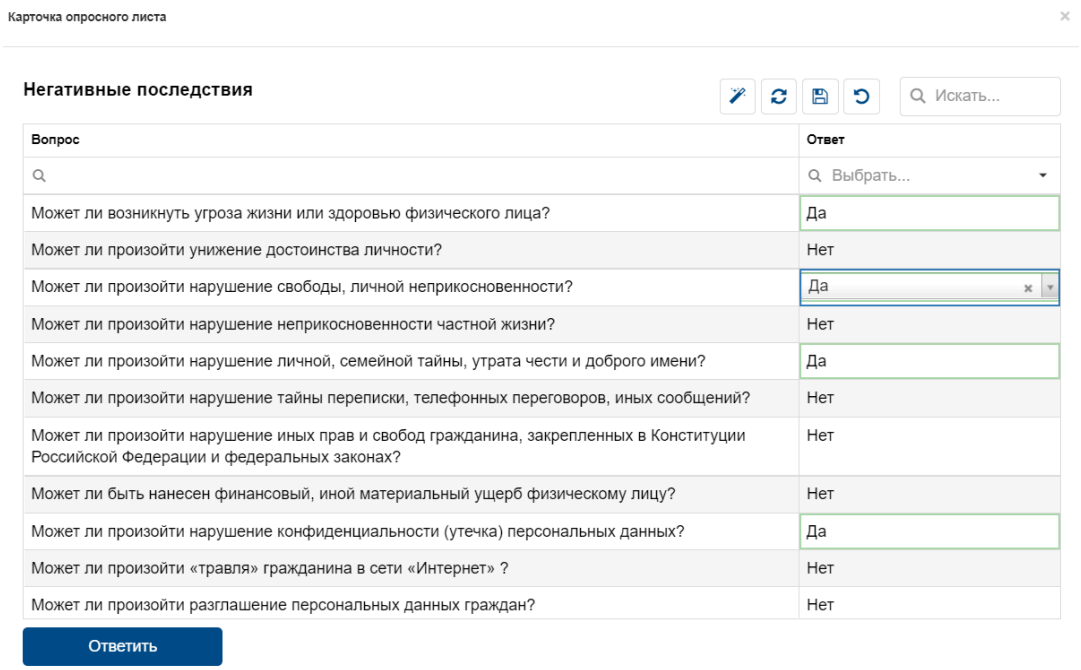

Рис. 4. Карточка опросного листа

5. После заполнения опросного листа нажмите кнопку 

.
6. Для опросного листа в карточке модели угрозы будет проставлена отметка о заполнении. Заполненные опросные листы станут недоступны для редактирования (Рисунок 5).

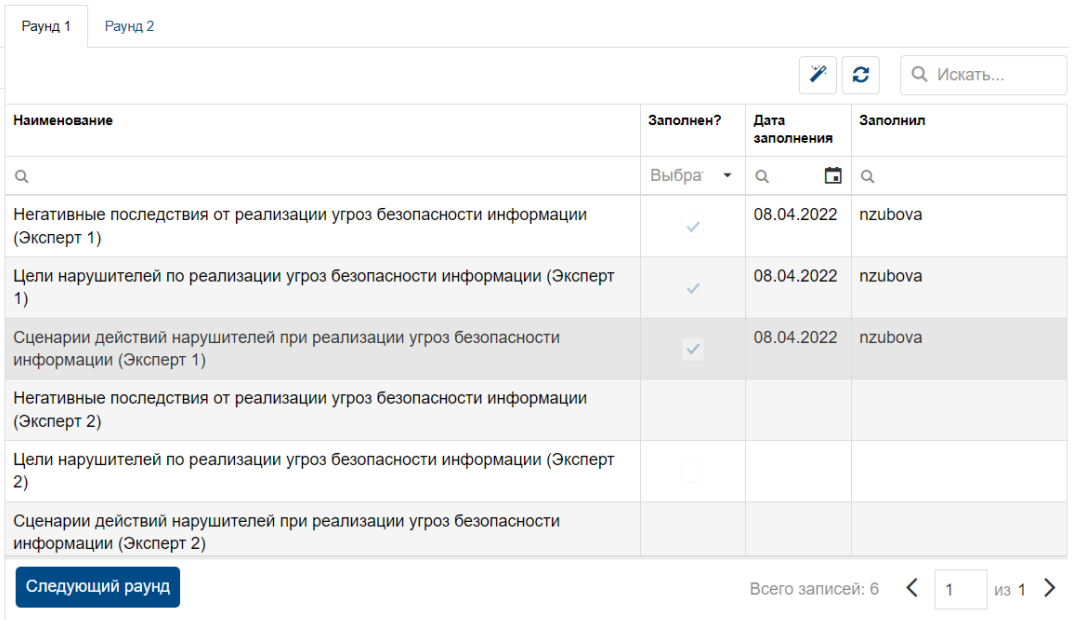

Рис. 5. Список опросных листов

7. При проведении оценки в *два раунда* нажмите кнопку 

для создания опросных листов для второго раунда. Если оценка проводится в *один раунд*, перейдите к шагу № 11.
8. Перейдите на вкладку «Раунд 2».
9. Заполните опросные листы, при необходимости исправьте оценку, опираясь на промежуточный результат в столбце «Предыдущий ответ».

Прим.:

Промежуточный результат формируется по итогам ответов всех экспертов в первом раунде, при этом выбираются ответы с наибольшей критичностью.

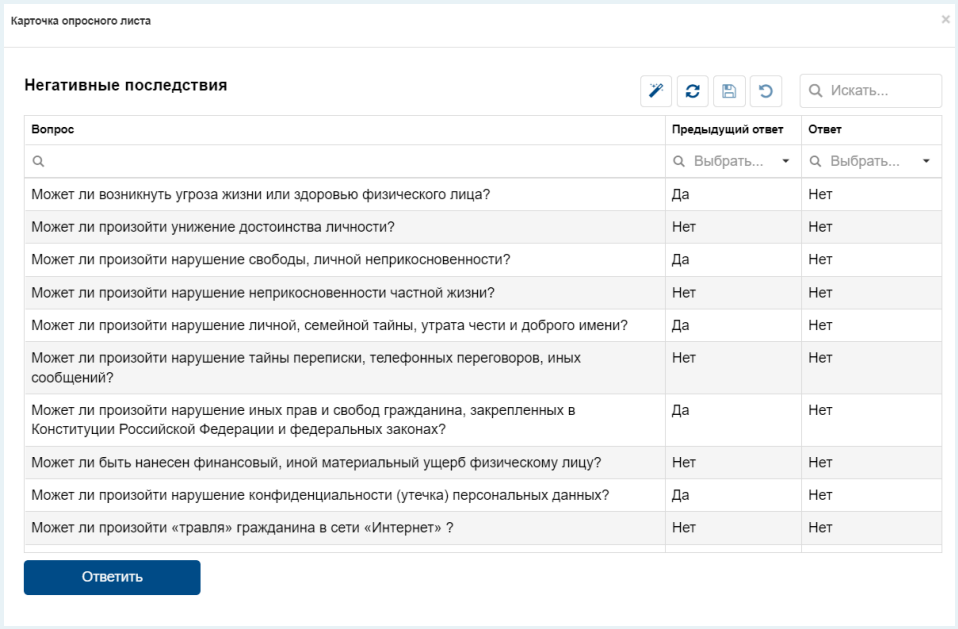

Рис. 6. Опросный лист второго раунда оценки

10. Для завершения проведения экспертной оценки нажмите кнопку Завершить
11. Для формирования модели угроз нажмите кнопку Рассчитать модель. Модель будет рассчитана автоматически на основании заполненных анкет.
12. В результате расчета модели определится актуальность всех объектов модели, итоги расчета модели будут отражены на вкладках «Объекты воздействия», «Актуальные угрозы», «Исключенные угрозы», «Элементы модели угроз», «Исключенные угрозы», «Показатели значимости».
13. Для экспорта сведений о модели угроз нажмите кнопку Экспортировать модель.
14. Для удаления модели угроз нажмите кнопку Удалить, подтвердите удаление во всплывающем окне.

4.1.3. Создание модели угроз при включенном ручном моделировании

Для ручного заполнения модели угроз:

1. Нажмите кнопку Выбрать элементы.
2. Откроется окно выбора объектов воздействия (Рисунок 7).
3. Последовательно выберите элементы модели: объекты воздействия, интерфейсы, способы реализации угроз, последствия, цели, воздействия, техники, нарушителей, возможные угрозы, актуальные угрозы:

- отметьте актуальные элементы с помощью флага ☑;
- нажмите кнопку Выбрать.
- при выборе угроз уточните формулировки исключения для невозможных и неактуальных угроз.

4. После выбора актуальных угроз нажмите Завершить.

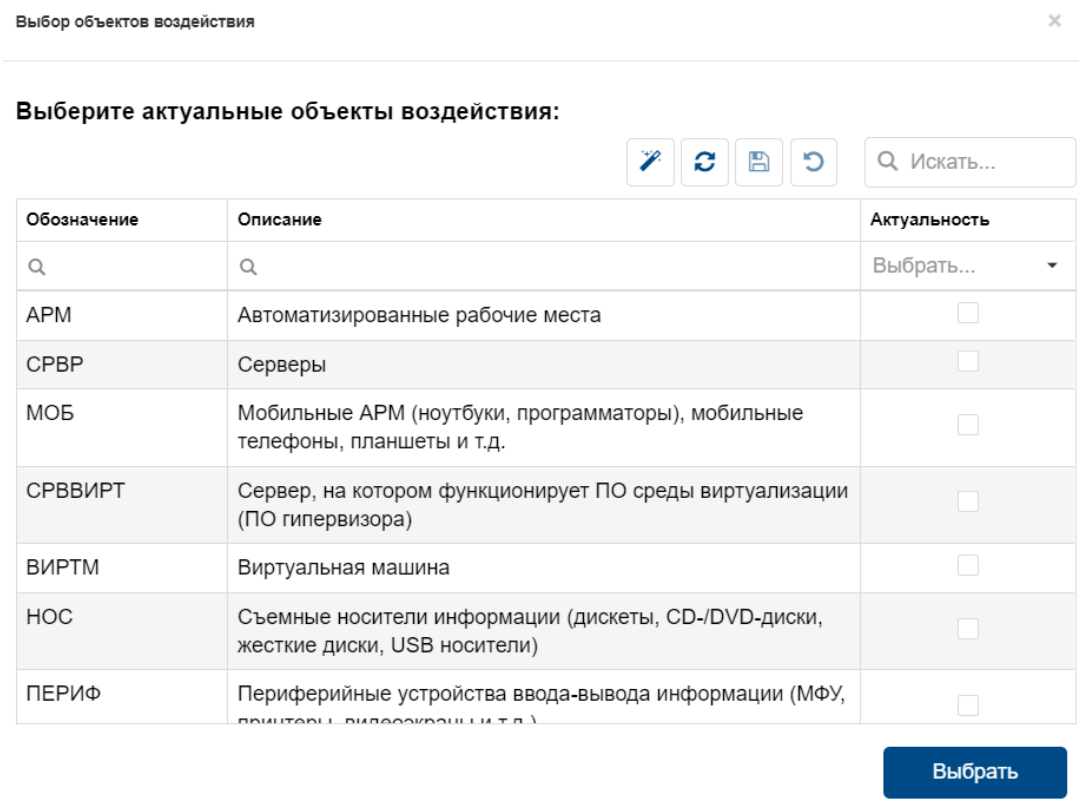

Рис. 7. Выбор элементов модели угроз

5. В результате будет определена актуальность всех объектов модели, итоги расчета модели будут отражены на вкладках «Актуальные угрозы», «Исключенные угрозы», «Элементы модели угроз», «Исключенные элементы».
6. Для экспорта сведений о модели угроз нажмите кнопку Экспортировать модель.
7. Для удаления модели угроз нажмите кнопку Удалить, подтвердите удаление во всплывающем окне.