

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Модуль ePlat4m «Категорирование объектов критической информационной
инфраструктуры»

Екатеринбург
2021

Содержание

1 Введение	4
1.1 Общие сведения.....	4
1.2 Рабочие процессы.....	5
1.3 Структура модуля.....	5
1.4 Ролевая модель	5
2 Назначение и цели создания	6
2.1 Назначение модуля	6
2.2 Цели создания	6
2.3 Функции модуля УКИИ	6
3 Описание функциональных характеристик	7
4 Подготовка к работе	8
5 Ведение реестра субъектов КИИ.....	9
5.1 Работа со списком субъектов КИИ.....	9
5.2 Создание нового субъекта КИИ	10
5.3 Просмотр и редактирование информации о субъекте КИИ	10
5.3.1 Просмотр и редактирование общей информации	11
5.3.2 Процессы	12
5.3.3 АСУ, ИС и ИТС	13
5.3.4 Комиссия.....	13
5.3.5 Проекты по категорированию	15
5.3.6 Объекты КИИ.....	17
5.3.7 Показатели.....	17
6 Ведение реестра объектов КИИ.....	19
6.1 Работа со списком объектов КИИ	19
6.2 Просмотр и редактирование информации об объекте КИИ	19
6.2.1 Сведения об объекте КИИ	20
6.2.2 Модель нарушителя.....	22

6.2.3 Модель угроз	23
6.2.4 Показатели критериев значимости	24
6.2.5 Защитные меры	25
6.2.6 Документы	26
7 Проведение проекта по категорированию.....	27
7.1 Создание нового проекта.....	27
7.2 Формирование области категорирования	28
7.3 Перечень объектов.....	33
7.4 Категорирование	35
7.5 Результаты категорирования.....	48
7.6 Защитные меры.....	48
7.7 Формирование итоговых документов	49

1 Введение

1.1 Общие сведения

В соответствии с Постановлением Правительства Российской Федерации от 08.02.2017 №127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», субъект КИИ должен сформировать перечень объектов КИИ, принадлежащих ему на праве собственности, аренды или ином законном основании, подлежащих категорированию.

Можно выделить следующие этапы категорирования:

1. Формирование комиссии по категорированию.
2. Определение управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка (критические процессы).
3. Формирование перечня объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, и подлежат категорированию (перечень объектов КИИ).
4. Оценка объектов КИИ в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ.
5. Присвоение каждому из объектов КИИ одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.

С целью автоматизации перечисленных работ разработан модуль «Управление критической информационной инфраструктурой» (далее – модуль УКИИ).

1.2 Рабочие процессы

Модуль реализует следующие рабочие процессы:

- «Жизненный цикл объекта КИИ», который предназначен для определения статуса объекта КИИ;
- «Модель угроз объекта КИИ», который предназначен для определения модели угроз для объекта КИИ;
- «Процесс категорирования», который содержит стадии категорирования объектов КИИ.

1.3 Структура модуля

Модуль «Управление КИИ» состоит из следующих разделов:

1. Субъекты КИИ;
2. Объекты КИИ;
3. Модели угроз;
4. Проекты по категорированию;
5. Справочники.

1.4 Ролевая модель

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

2 Назначение и цели создания

2.1 Назначение модуля

Модуль УКИИ предназначен для учета сведений об ОКИИ Эксплуатирующей организации, а также хранения и актуализации данных о результатах категорирования ОКИИ.

2.2 Цели создания

Целью создания модуля является автоматизация процесса управления безопасностью ОКИИ Эксплуатирующей организации.

2.3 Функции модуля УКИИ

В модуле УКИИ осуществляется выполнение следующих функций:

1. Ведение реестра субъектов КИИ;
2. Ведение реестра объектов КИИ;
3. Ведение справочников;
4. Проведение оценки соответствия выявленных объектов требованиям №187-ФЗ.

3 Описание функциональных характеристик

1. Ведение справочного материала	<ul style="list-style-type: none">– предоставление справочного материала по стадиям категорирования;– актуализация справочного материала
2. Организация работ по проведению категорирования ОКИИ	<ul style="list-style-type: none">– планирование работ по категорированию ОКИИ;– управление задачами;– мониторинг и контроль
3. Заполнение сведений о субъекте КИИ и ОКИИ	<ul style="list-style-type: none">– формирование шаблонов типовых территориальных подразделений (площадок) и ОКИИ;– сбор данных о субъекте КИИ;– сбор данных об ОКИИ;– определение перечня выполняемых защитных мер
4. Проведение категорирования ОКИИ	<ul style="list-style-type: none">– разработка модели угроз ОКИИ;– расчет показателей критериев значимости;– актуализация рассчитанных значений при повторном категорировании;– определение категории значимости ОКИИ;– хранение и учет данных о категорировании
5. Формирование и хранение отчетных документов	<ul style="list-style-type: none">– формирование документов в редактируемом формате в соответствии с требованиями законодательства:<ul style="list-style-type: none">• акт категорирования ОКИИ;• сведения о категорировании ОКИИ;• перечень ОКИИ, подлежащих категорированию;– формирование прочих документов в редактируемом формате:<ul style="list-style-type: none">• перечень критических БП;• модель угроз безопасности информации

4 Подготовка к работе

Для начала работы необходимо выполнить следующие действия:

1. Открыть браузер.
2. В адресной строке браузера указать адрес, по которому расположен экземпляр платформы.
3. На странице аутентификации ввести логин и пароль учетной записи пользователя системы.
4. Нажать кнопку «Войти». Откроется рабочая область, соответствующая роли, в которой находится пользователь.

Для корректной работы модуля необходима предварительная загрузка справочных данных.

5 Ведение реестра субъектов КИИ

Для начала работы с реестром субъектов перейдите в раздел «Субъекты КИИ» с помощью меню, расположенного на левой панели рабочей области.

На начальном экране раздела «Субъекты КИИ» представлен список субъектов.

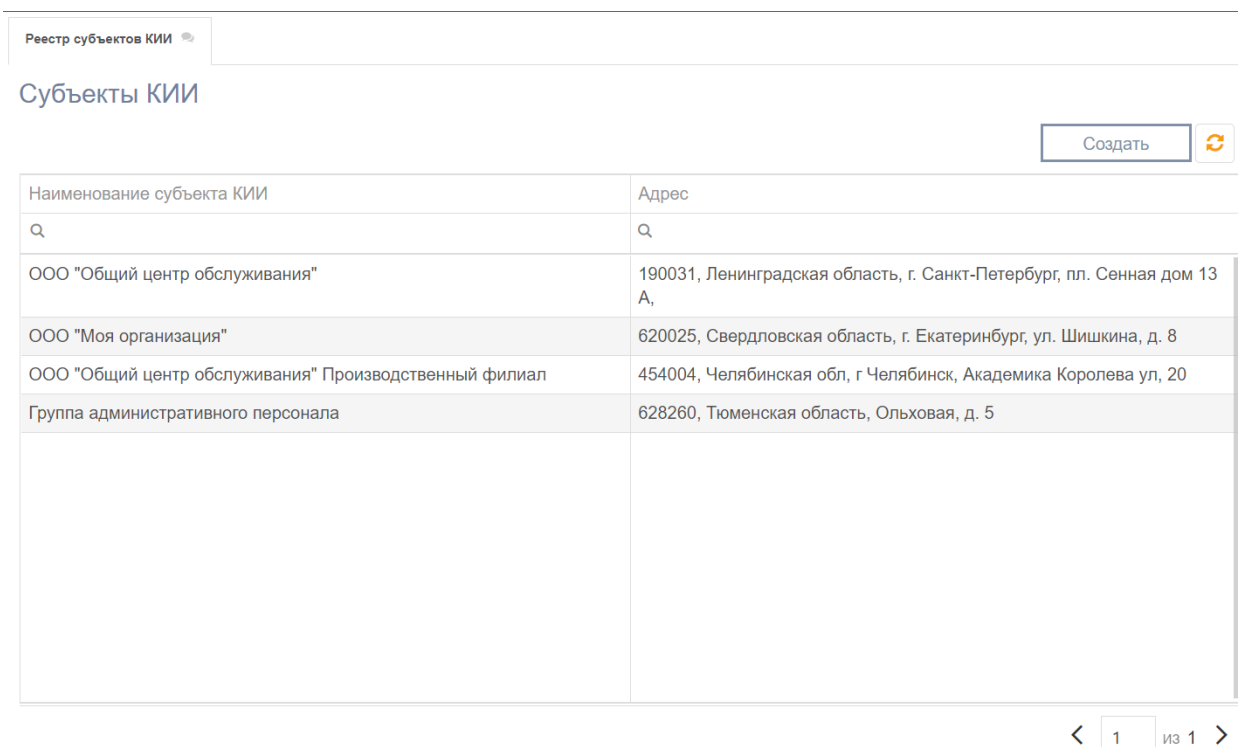



Рисунок 1 – Реестр субъектов КИИ

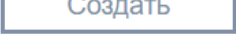
Предусмотрены следующие варианты работы с реестром субъектов КИИ:

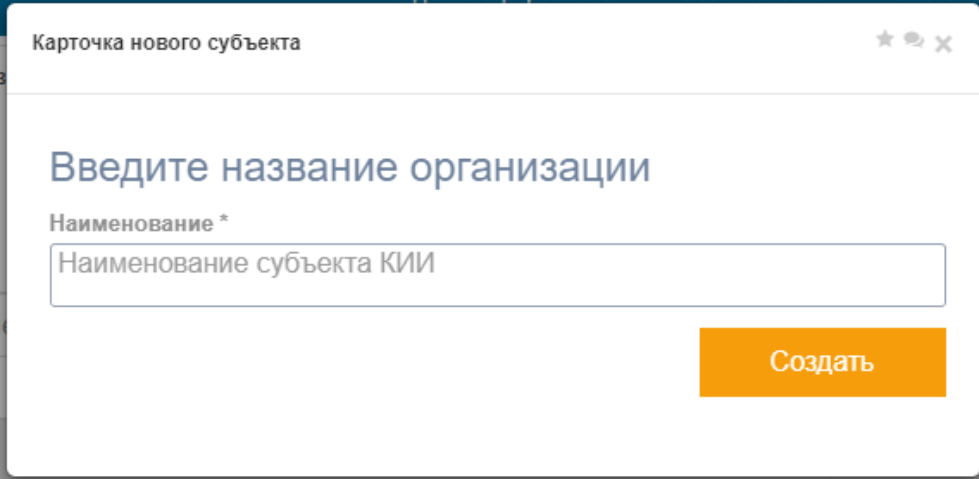
- фильтрация списка по наименованию субъекта КИИ (см. раздел Работа со списком субъектов КИИ);
- фильтрация списка по адресу субъекта КИИ (см. раздел Работа со списком субъектов КИИ);
- создание нового субъекта КИИ (см. раздел Создание нового субъекта КИИ);
- просмотр карточки субъекта КИИ;
- редактирование карточки субъекта КИИ.

5.1 Работа со списком субъектов КИИ

Для фильтрации списка субъектов по наименованию или адресу введите искомые символы в строку поиска  под заголовком таблицы.

5.2 Создание нового субъекта КИИ

Для создания нового субъекта КИИ нажмите кнопку  в правом верхнем углу экрана. В всплывающем окне откроется карточка нового субъекта (Рисунок 2).



Карточка нового субъекта

Введите название организации

Наименование *

Наименование субъекта КИИ

Создать

Рисунок 2 – Создание субъекта КИИ

Выберите наименование субъекта и нажмите кнопку «Создать». После закрытия окна созданный субъект КИИ появится в реестре субъектов КИИ.

5.3 Просмотр и редактирование информации о субъекте КИИ

Для перехода к просмотру или редактированию детальной информации о субъекте КИИ, выполните двойной щелчок левой кнопкой мыши на записи субъекта КИИ в таблице. В новой вкладке откроется карточка субъекта КИИ (Рисунок 3).

Реестр субъектов КИИ Карточка субъекта КИИ

Новый

Общая информация | Процессы | АСУ, ИС и ИТС | Комиссия | Проекты по категорированию | Объекты КИИ | Показатели

Наименование

Адрес местонахождения субъекта Сфера (область) деятельности
 Текст

Должность руководителя субъекта Фамилия Имя Отчество

Назначено должностное лицо, на которое возложены функции обеспечения безопасности значимых объектов

Структурное подразделение, ответственное за обеспечение безопасности значимых объектов

Структурное подразделение	Должность руководителя	ФИО руководителя
<input type="text" value="q"/>	<input type="text" value="q"/>	<input type="text" value="q"/>

Назначен штатный специалист, ответственный за обеспечение безопасности значимых объектов

Рисунок 3 – Карточка субъекта КИИ. Общая информация

В карточке информация о субъекте КИИ структурирована в виде отдельных вкладок, содержащих сведения определенного типа:

- Общая информация;
- Процессы;
- АСУ, ИС и ИТС;
- Комиссия по категорированию;
- Проекты по категорированию;
- Объекты КИИ;
- Показатели значимости для субъекта.

5.3.1 Просмотр и редактирование общей информации

По умолчанию карточка субъекта КИИ открыта на вкладке «Общая информация», на которой содержатся основные сведения о субъекте КИИ, такие, как: организация, руководитель, адрес, уполномоченное лицо, подразделения, отвечающее за безопасность значимых объектов КИИ и их руководители, или штатный работник, ответственный за безопасность КИИ.

Для редактирования данных введите новые значения в соответствующие поля и нажмите кнопку «Сохранить» в левом нижнем углу карточки субъекта КИИ.

Информация о руководителе субъекта заполняется в любом случае, а информация об уполномоченном лице (если такое имеется в организации) заполняется после нажатия на галочку «Назначено должностное лицо, на которое возложены функции обеспечения безопасности значимых объектов».

Флаг «Назначен штатный специалист, ответственный за обеспечение безопасности значимых объектов» заполняется в случае, если у субъекта нет отдельного подразделения, отвечающего за безопасность объектов КИИ.

5.3.2 Процессы

Для просмотра или внесения сведений о процессах субъекта КИИ перейдите на вкладку «Процессы» (Рисунок 4) карточки субъекта КИИ.

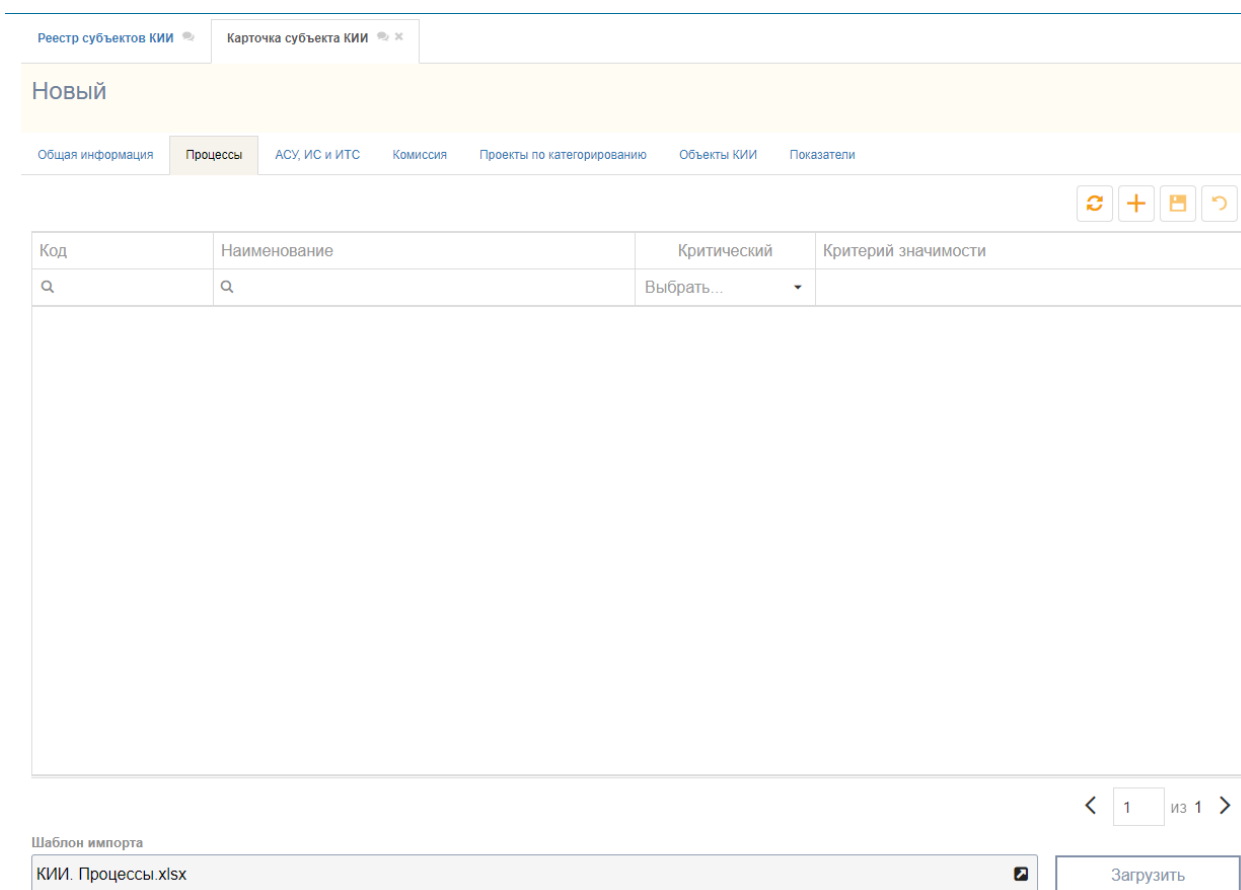



Рисунок 4 – Карточка субъекта КИИ. Процессы

Перечень процессов субъекта КИИ (далее – ПС) можно импортировать в систему из файла `xlsx`. Для этого:

1. Скачайте файл `xlsx` шаблона импорта;
2. Заполните файл, не переименовывая заголовки столбцов;

3. Нажмите кнопку «Загрузить» и укажите заполненный файл.

Сведения о ПС представлены в виде таблицы, которая содержит следующие сведения: код, наименование, критический процесс или нет и критерии значимости, по которым процесс определен как критический.

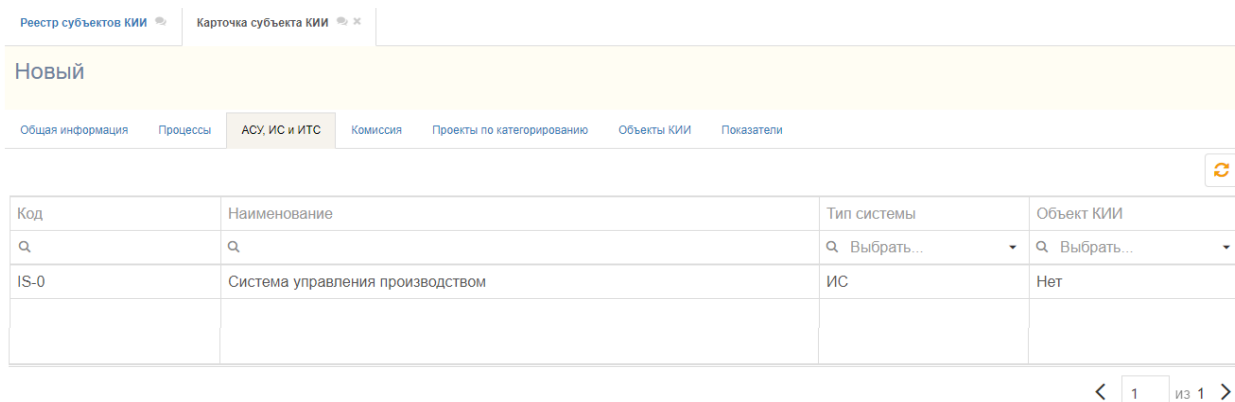
Также процессы можно добавить по кнопке  вверху таблицы, заполнив необходимые поля в появившейся строчке. После чего следует нажать кнопку сохранения над таблицей.

Для получения детальной информации о ПС выполните двойной щелчок левой кнопкой мыши на записи ПС в таблице. В новой вкладке откроется карточка ПР.

5.3.3 АСУ, ИС и ИТС

Для просмотра или внесения сведений об АСУ, ИС и ИТС субъекта КИИ перейдите на вкладку «АСУ, ИС, ИТС» (Рисунок 5) карточки субъекта КИИ.

После запуска импорта, выполненного выше, на вкладке АСУ, ИС и ИТС отобразятся системы, которые обеспечивают выполнение процессов Субъекта КИИ. Перечень систем субъекта КИИ формируется автоматически на основе данных из импортированного файла.




Код	Наименование	Тип системы	Объект КИИ
IS-0	Система управления производством	ИС	Нет

Рисунок 5 – Карточка субъекта КИИ. АСУ, ИС и ИТС

Сведения о системах представлены в виде таблицы, которая содержит следующие сведения: код, наименование, тип (возможные типы представлены в соответствии с 187-ФЗ) и является ли система объектом КИИ.

5.3.4 Комиссия

Для просмотра или создания комиссии по категорированию перейдите на вкладку «Комиссия» (Рисунок 6) карточки субъекта КИИ.

Чтобы добавить новую комиссию для субъекта КИИ нажмите  вверху таблицы и заполните наименование комиссии и дату создания комиссии. Наименование комиссии

служит для упрощения идентификации комиссии при создании проекта по категорированию и не используется при формировании документов.

Наименование комиссии	Дата создания	Члены комиссии	Архив
?	14.12.2018		Выбрать... ☐

Рисунок 6 – Карточка субъекта КИИ. Комиссия

Для сохранения комиссии нажмите кнопку сохранения вверху таблицы.

Для редактирования состава комиссии двойным кликом по записи комиссии в таблице перейдите в карточку комиссии (Рисунок 7).

Председатель	ФИО	Должность	Подразделение
Выбрать...	?	?	?

Рисунок 7 – Карточка комиссии по категорированию

В поле «Приказ о создании комиссии» загрузите документ/скан приказа о создании комиссии.

Поле «Дата создания» является обязательным для заполнения. В нём указывается дата создания комиссии в соответствии с приказом о создании комиссии.

В поле «Субъект КИИ» указывается наименование субъекта, в котором функционирует данная комиссия по категорированию. Оно недоступно для редактирования и заполняется автоматически при создании комиссии.

Состав комиссии редактируется в таблице «Члены комиссии». Чтобы добавить участника комиссии нажмите кнопку добавления вверху таблицы. В новой строке таблицы заполните ФИО участника полностью, должность с большой буквы и подразделение.

Указанные ФИО и должность будут отображаться в Акте категорирования для объектов КИИ.

Если участник комиссии является председателем, в соответствующей строке таблицы поставьте галочку «Председатель». Председатель в комиссии должен быть **один**.

! Как определяется

В соответствии с ППРФ №127 п.13 «Комиссию по категорированию возглавляет руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо».

В случае изменения вышеописанных полей нажмите на кнопку «Сохранить».

5.3.5 Проекты по категорированию

Для просмотра сведений о проектах по категорированию перейдите на вкладку «Проекты по категорированию» (Рисунок 8) карточки субъекта КИИ.

Реестр субъектов КИИ Карточка субъекта КИИ

Новый

Общая информация Процессы АСУ, ИС и ИТС Комиссия **Проекты по категорированию** Объекты КИИ Показатели

+ Создать проект ↻

Номер проекта	Наименование	Дата начала	Дата окончания	Тип проекта	Статус
🔍	🔍	📅 🔍	📅 🔍	🔍 Выбрать...	Выбрать...

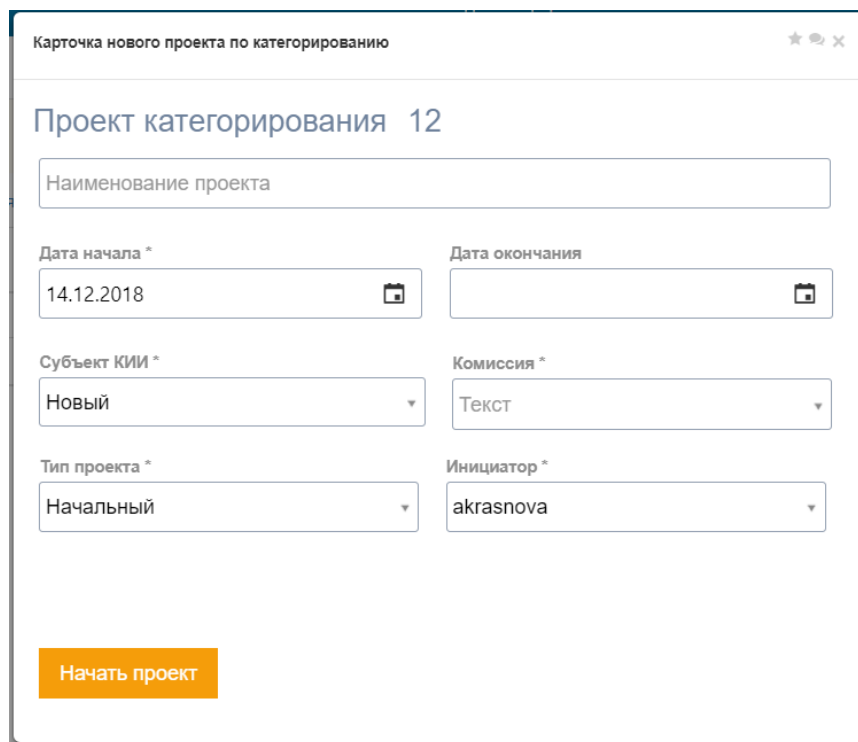
У субъекта нет проектов по категорированию

< 1 из 1 >

Рисунок 8 – Карточка субъекта КИИ. Проекты по категорированию

Сведения о проектах по категорированию объектов КИИ представлены в виде таблицы: номер проекта, наименование, дата начала, дата окончания, тип проекта, статус.

Для создания нового проекта по категорированию объектов КИИ нажмите кнопку «Создать проект», расположенную над верхним правым углом таблицы. Во всплывающем окне отразится форма «Карточка нового проекта по категорированию (Рисунок 9). Введите наименование проекта и из выпадающего списка выберите созданную выше комиссию, участники которой будут указаны в актах категорирования создаваемого проекта.



The screenshot shows a web form titled "Карточка нового проекта по категорированию" (New project card for categorization). The form is for "Проект категорирования 12" (Categorization project 12). It contains the following fields:

- Text input: "Наименование проекта" (Project name)
- Date picker: "Дата начала *" (Start date) with value "14.12.2018"
- Date picker: "Дата окончания" (End date)
- Dropdown menu: "Субъект КИИ *" (KIIO subject) with value "Новый" (New)
- Dropdown menu: "Комиссия *" (Commission) with value "Текст" (Text)
- Dropdown menu: "Тип проекта *" (Project type) with value "Начальный" (Initial)
- Dropdown menu: "Инициатор *" (Initiator) with value "akrasnova"

At the bottom left, there is an orange button labeled "Начать проект" (Start project).

Рисунок 9 – Карточка нового проекта по категорированию

Нажмите кнопку «Начать проект». В новой вкладке откроется форма «Карточка проекта категорирования».

Для просмотра детальной информации по проекту категорирования выполните двойной щелчок по записи в таблице проектов на карточке субъекта КИИ. В новой вкладке откроется форма «Карточка проекта категорирования».

На карточке проекта на вкладке «Сведения о проекте» представлена заполненная выше информация:

- порядковый номер проекта, рассчитывается автоматически;
- наименование проекта;
- дата начала проекта, по умолчанию равна текущей дате;
- дата окончания проекта;
- субъект КИИ;
- тип проекта;

- инициатор, по умолчанию текущий пользователь;
- комиссия по категорированию.

После изменения описанной выше информации нажмите кнопку сохранения.

5.3.6 Объекты КИИ

На вкладке карточки субъекта «Объекты КИИ» (Рисунок 10) представлена таблица с объектами КИИ субъекта в случае, если хотя бы в одном проекте категорирования текущего субъекта системы были явно отмечены, как объекты КИИ, т.е. был сформирован перечень объектов КИИ (подробнее о формировании перечня объектов КИИ см. раздел Формирование области категорирования).

Рисунок 10 – Перечень значимых объектов у субъекта КИИ

5.3.7 Показатели

Для просмотра или изменения сведений о показателях значимости, неприменимых для субъекта КИИ в целом (т.е. для любых его значимых объектов), перейдите на вкладку «Показатели» (Рисунок 11) карточки субъекта КИИ.

Реестр субъектов КИИ Карточка субъекта КИИ

Новый

Общая информация | Процессы | АСУ, ИС и ИТС | Комиссия | Проекты по категорированию | Объекты КИИ | **Показатели**

Применяемые показатели значимости для субъекта КИИ

Показатель значимости	Не применим	Обоснование
q	Выбрать...	q
Значимость для обеспечения обороны страны, безопасности государства и правопорядка		
Прекращение или нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра), оцениваемое в уровне (значимости) пункта управления или ситуационного центра	<input type="checkbox"/>	
Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры, оцениваемое в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции)	<input type="checkbox"/>	
Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры, оцениваемое в увеличении времени выпуска продукции (работ, услуг) с заданным объемом (процентов установленного времени выпуска продукции)	<input type="checkbox"/>	
Прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемое в максимальной	<input type="checkbox"/>	

< 1 из 3 >



Рисунок 11 – Карточка субъекта КИИ. Показатели

Перечень показателей критериев значимости объектов КИИ представлены в виде таблицы, сгруппированные по критериям значимости (в соответствии с ППРФ №127).

Категорирование осуществляется по следующим показателям:

- социальной значимости;
- политической значимости;
- экономической значимости;
- экологической значимости;
- значимости для обеспечения обороны страны, безопасности государства и правопорядка.

Для каждого показателя можно указать, что он не применим для субъекта КИИ:

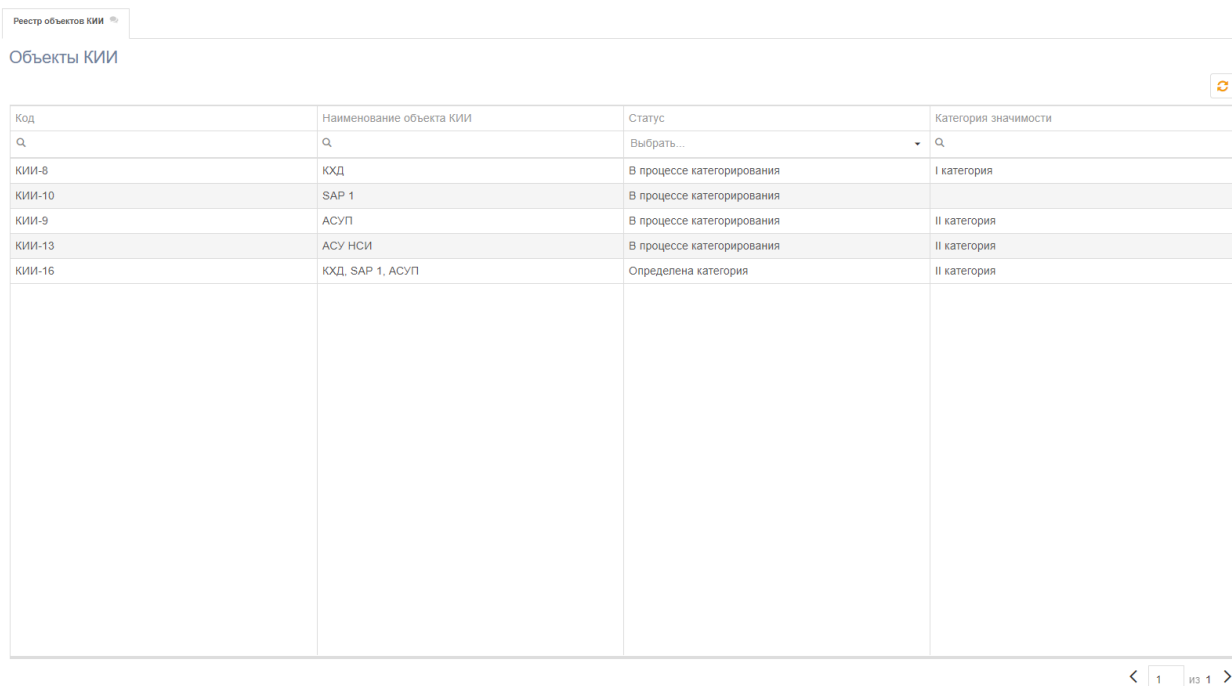
- нажмите на галочку в столбце «Не применим»;
- напишите обоснование в столбе «Обоснование»;
- нажмите значок сохранения  для подтверждения изменений или значок отмены  для сброса новых значений.

Сведения о применимости показателей передаются в проекты по категорированию на этапе формирования опросного листа показателей критериев значимости.

6 Ведение реестра объектов КИИ

Для начала работы с реестром объектов КИИ перейдите в раздел «Объекты КИИ» с помощью меню, расположенного на левой панели рабочей области.

На начальном экране раздела «Объекты КИИ» представлен список объектов.




Код	Наименование объекта КИИ	Статус	Категория значимости
Q	Q	Выбрать...	Q
КИИ-8	КХД	В процессе категорирования	I категория
КИИ-10	SAP 1	В процессе категорирования	
КИИ-9	АСУП	В процессе категорирования	II категория
КИИ-13	АСУ НСИ	В процессе категорирования	II категория
КИИ-16	КХД, SAP 1, АСУП	Определена категория	II категория

Рисунок 12 – Реестр всех объектов КИИ в системе

Предусмотрены следующие варианты работы с реестром объектов КИИ:

- фильтрация списка по наименованию субъекта КИИ (5.1);
- фильтрация списка по адресу субъекта КИИ (5.1);
- создание нового субъекта КИИ (5.2);
- просмотр карточки субъекта КИИ;
- редактирование карточки субъекта КИИ.

6.1 Работа со списком объектов КИИ

Для фильтрации списка объектов КИИ по наименованию или адресу введите искомые символы в строку поиска  под заголовком таблицы.

6.2 Просмотр и редактирование информации об объекте КИИ

Для перехода к просмотру или редактированию детальной информации об объекте КИИ, выполните двойной щелчок левой кнопкой мыши на записи объекта КИИ в таблице. В новой вкладке откроется карточка объекта КИИ (Рисунок 13).

Реестр объектов КИИ Карточка объекта КИИ

Объект КИИ **КИИ-1** Статус: Определена категория

АСУ ТП СБ

Сведения об объекте КИИ Модель нарушителя Модель угроз Показатели критериев значимости Защитные меры Документы

Сфера (область деятельности)
Сфера топливно-энергетического комплекса

Архитектура объекта
Система диспетчерского управления и контроля

Критические процессы, которые обеспечиваются объектом

Код	Наименование
Q	Q
200025	Оказание услуг
19224	Управление строительством

Всего записей: 2 < 1 из 1 >

Назначение объекта
Обеспечение технологического процесса

Адреса размещения объекта

Адрес	
Q	
Екатеринбург, ул. Ткачей, 6	✘

Всего записей: 2 < 1 из 1 >

Сохранить

Общая информация
Взаимодействие с сетями электросвязи
Эксплуатирующее лицо
Программные и технические средства
Средства защиты информации
Типы компьютерных инцидентов

Рисунок 13 – Карточка объекта КИИ. Вкладка сведений объекта КИИ

6.2.1 Сведения об объекте КИИ

Сведения об объекте КИИ представлены в виде редактируемой формы, содержимое которой утверждено Приказом ФСТЭК России №236 от 22.12.2017 г. «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из таких категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий». Форма состоит из шести разделов:

- общая информация;
- взаимодействие с сетями электросвязи;
- эксплуатирующие лица;
- программные и технические средства;
- средства защиты информации;
- типы компьютерных инцидентов.

Раздел «Общая информация» содержит следующие сведения:

- сфера (область деятельности);
- архитектура объекта;
- назначение объекта;
- адреса размещения объекта;
- критические процессы, которые обеспечиваются объектом

Раздел «Взаимодействие с сетями электросвязи» (Рисунок 14) содержит следующие сведения:

- категория сети электросвязи;
- цель взаимодействия с сетью электросвязи;
- наименование оператора связи;
- тип доступа к сети электросвязи;
- используемые технологии доступа к сети электросвязи.

Реестр объектов КИИ | Карточка объекта КИИ

Объект КИИ КИИ-1 | Статус: Определена категория

АСУ ТП СБ

Сведения об объекте КИИ | Модель нарушителя | Модель угроз | Показатели критериев значимости | Защитные меры | Документы

Категория сети электросвязи: Нет категории

Наименование оператора связи: -

Цель взаимодействия с сетью электросвязи: Иная цель

Тип доступа к сети электросвязи: Проводной

Используемые технологии доступа к сети электросвязи: Нет технологий

Сохранить

Общая информация

- Взаимодействие с сетями электросвязи
- Эксплуатирующее лицо
- Программные и технические средства
- Средства защиты информации
- Типы компьютерных инцидентов

Рисунок 14 – Карточка объекта КИИ. Сведения об объекте КИИ. Взаимодействия с сетями электросвязи

Раздел «Программные и технические средства» (Рисунок 15) содержит следующие сведения о программных и технических средствах в виде таблицы:

- наименование технического средства;
- тип ТС;
- производитель ТС;
- программное обеспечение, которое содержится на ТС.

Реестр объектов КИИ | Карточка объекта КИИ x

Объект КИИ КИИ-1 Статус: Определена категория

АСУ ТП СБ

Сведения об объекте КИИ | Модель нарушителя | Модель угроз | Показатели критериев значимости | Защитные меры | Документы

Сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ

Техническое средство	Тип ТС	Производитель	Программное обеспечение
Сервер 2	Сервер	Lenovo	MS Windows Server 2016
Сервер 1	Сервер	Lenovo	MS Windows Server 2016
АРМ 2	Автоматизированное рабочее место	HP	Adobe Reader
АРМ 2	Автоматизированное рабочее место	HP	MS Windows 2012
АРМ 1	Автоматизированное рабочее место	Lenovo	MS Office 2016
АРМ 1	Автоматизированное рабочее место	Lenovo	MS Windows 2012

< 1 из 1 >

Общая информация

Взаимодействие с сетями электросвязи

Эксплуатирующее лицо

Программные и технические средства

Средства защиты информации

Типы компьютерных инцидентов

Рисунок 15 – Карточка объекта КИИ. Сведения об объекте КИИ. Программные и технические средства

Все сведения об объекте КИИ, в том числе и сведения о программных, технических средствах и средствах защиты могут быть загружены с помощью импорта.

Шаблоны для импорта представлены в файлах «КИИ. Сведения об объектах.xlsx» и «КИИ. Программно-аппаратные средства и СрЗИ.xlsx».

6.2.2 Модель нарушителя

На вкладке Модель нарушителя (Рисунок 16) отображается таблица, содержащая сведения об актуальных нарушителях для объекта КИИ, если она была создана в проекте по категорированию данного объекта КИИ.

! Важно

*Модель нарушителя отображается корректно только, если в проекте по категорированию для текущего объекта КИИ на вкладке «Категорирование» была создана модель нарушителя. Иначе на вкладке отображается карточка **новой** модели нарушителя.*

Таблица содержит следующие сведения о нарушителях:

- категория нарушителя (внутренний или внешний с указанием потенциала нарушителя);
- вид нарушителя;
- актуальность нарушителя для объекта;

- обоснование неактуальности нарушителя (заполняется в случае, если стоит признак неактуальности).

Реестр объектов КИИ Карточка объекта КИИ

Объект КИИ КИИ-8 Статус: В процессе категорирования

Наименование
КХД

Сведения об объекте КИИ **Модель нарушителя** Модель угроз Показатели критериев значимости Защитные меры Документы

Модель нарушителя №17 Завершена

Определение возможных действий нарушителей в отношении объектов КИИ, а также иных источников информации

Наименование модели
Модель нарушителя

Объекты КИИ
КХД, SAP ERP, Типовой объект КИИ

Категория нарушителя	Виды нарушителя	Не актуальный	Обоснование невозможности реализовать УБИ
Q	Q	Выбрать...	Q
Внешний нарушитель с низким потенциалом	Внешние субъекты (физические лица), бывшие работники	<input checked="" type="checkbox"/>	Такого нарушителя нет
Внутренний нарушитель с низким потенциалом	Пользователи системы, лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру, лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных работ	<input type="checkbox"/>	
Внешний нарушитель со средним потенциалом	Террористические, экстремистские группировки, преступные группы (криминальные структуры), конкурирующие организации, разработчики, производители, поставщики программных, технических и программнотехнических средств	<input checked="" type="checkbox"/>	Такого нарушителя нет

← 1 из 1 →

[Изменить модель](#) [Удалить модель](#)

Рисунок 16 – Карточка объекта КИИ. Модель нарушителя

Если данный нарушитель не актуален для выбранного объекта КИИ, то в графе «Не актуальный» будет указан соответствующий признак, в графе «Обоснование невозможности реализовать УБИ» приведено аргументированное обоснование такому выбору.

6.2.3 Модель угроз

На вкладке Модель угроз (Рисунок 17) приведена актуальная модель угроз безопасности информации, если она была создана в проекте по категорированию текущего объекта КИИ. Модель представляет собой таблицу, содержащую следующие сведения об угрозах безопасности:

- ID угрозы (идентификатор из БДУ ФСТЭК России);
- наименование;
- нарушитель;
- уязвимости.

Реестр объектов КИИ Карточка объекта КИИ

Объект КИИ **КИИ-8** Статус: В процессе категорирования

Наименование
КХД

Сведения об объекте КИИ **Модель нарушителя** **Модель угроз** Показатели критериев значимости Защитные меры Документы

Модель угроз №2 Завершена

Анализ угроз безопасности информации и уязвимостей, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ

Наименование модели
Модель угроз в проекте №0

Объекты КИИ, для которых создается модель угроз
КХД Удалить связь с объектом

ID угрозы	Наименование	Нарушитель	Уязвимости
УБИ 004	Угроза аппаратного сброса пароля BIOS	Внутренний нарушитель с низким потенциалом	Уязвимости некоторых системных (материнских) плат – наличие механизмов аппаратного сброса паролей, установленных в BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к системному блоку компьютера
УБИ 005	Угроза внедрения вредоносного кода в BIOS	Внутренний нарушитель с высоким потенциалом	Слабости технологий контроля за обновлением программного обеспечения BIOS/UEFI и заменой чипсета BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера
УБИ 006	Угроза внедрения кода или данных	Внешний нарушитель с низким потенциалом	Уязвимости программного обеспечения; Слабости мер антивирусной защиты и разграничения доступа. Наличие открытого Telnet-порта на IoT-устройстве (только для IoT-устройств). Реализация данной угрозы возможна в режиме работы

Изменить Удалить

Рисунок 17 Карточка объекта КИИ. Модель угроз

Таблица содержит информацию обо всех актуальных для текущего объекта КИИ угрозах безопасности информации в соответствии с Банком данных угроз ФСТЭК России.

! Важно

*Модель угроз отображается корректно только, если в проекте по категорированию для текущего объекта КИИ на вкладке «Категорирование» была создана модель угроз. Иначе на вкладке отображается карточка **новой** модели угроз.*

6.2.4 Показатели критериев значимости

На данной вкладке (Рисунок 18) продемонстрирована оценка показателей критериев значимости для объекта КИИ, если она была проведена в проекте по категорированию выбранного объекта КИИ.

Форма содержит наименование опросного листа, кнопку «Удалить связь с объектом» и 5 разделов с показателями значимости по соответствующим критериям в соответствии с Постановлением Правительства Российской Федерации №127 от 8.02.2018 г. «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». Данные разделов заполняются автоматически при создании опросных листов на этапе категорирования в проекте категорирования объекта.

Реестр объектов КИИ Карточка объекта КИИ

Объект КИИ КИИ-8 Статус: В процессе категорирования

Наименование
КХД

Сведения об объекте КИИ Модель нарушителя Модель угроз Показатели критериев значимости Защитные меры Документы

Оценка показателей критериев значимости №8 I категория

Наименование опросного листа
Опросный лист

Объекты КИИ
КХД, SAP ERP, Типовой объект КИИ Удалить связь с объектом

I. Социальная значимость II. Политическая значимость III. Экономическая значимость IV. Экологическая значимость V. Значимость для обеспечения обороны страны, безопасности государства и правопорядка Результаты

Критерий	Категория
Q	Q
Социальная значимость	I категория
Экологическая значимость	III категория
Значимость для обеспечения обороны страны, безопасности государства и правопорядка	III категория
Экономическая значимость	I категория
Политическая значимость	Без категории

Изменить Удалить

Рисунок 18 – Карточка объекта КИИ. Показатели критериев значимости

6.2.5 Защитные меры

На вкладке Защитные меры (Рисунок 19) в разделе «Необходимые меры» отображается перечень требований в соответствии с Приказом ФСТЭК №239, которые должны быть выполнены для защиты любого объекта КИИ от актуальных угроз безопасности, указанных в модели угроз.

Перечень с необходимыми мерами формируется автоматически при создании объекта КИИ.

В разделе с выполненными мерами отображаются меры защиты, *уже внедренные* для защиты объекта КИИ в организации, его эксплуатирующей.

Заполнение и оценка выполнения защитных мер производится либо в карточке объекта КИИ, либо на статусе проекта «Определение мер» после этапа категорирования (более подробно см. раздел Защитные меры).

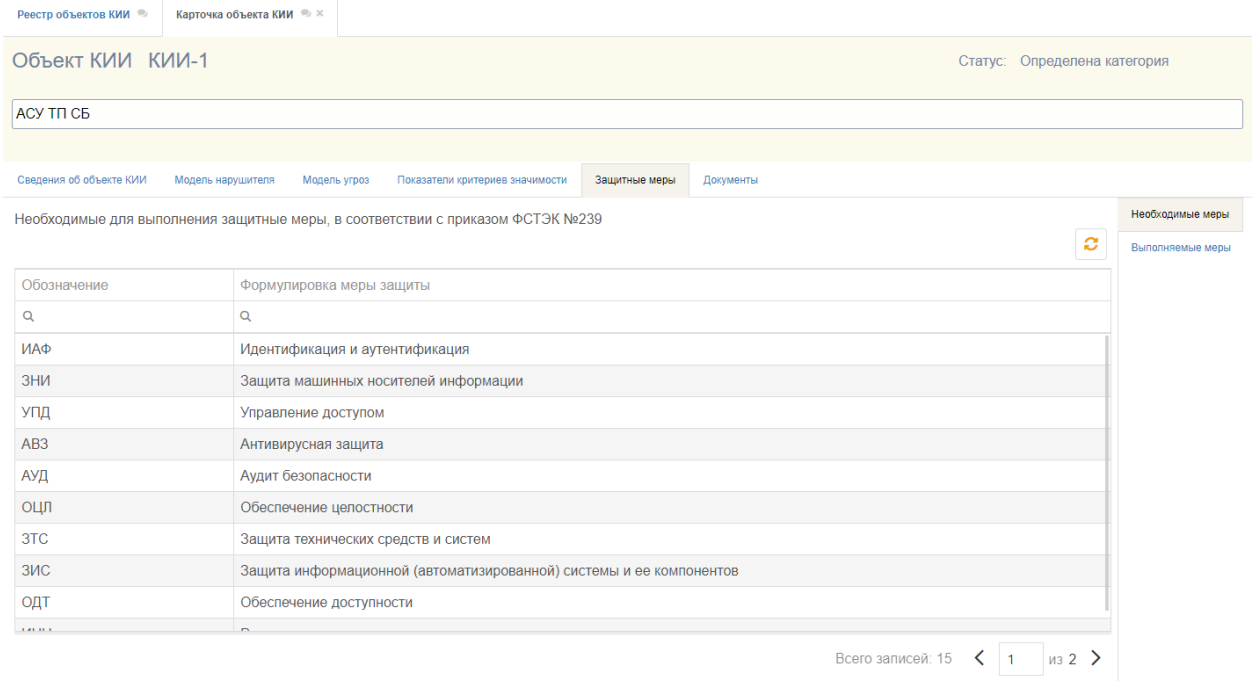



Рисунок 19 – Карточка объекта КИИ. Защитные меры

6.2.6 Документы

На данной вкладке отображаются акт категорирования и сведения об объекте КИИ по утвержденной форме ФСТЭК (Рисунок 20). Документы формируются после завершения проекта по категорированию текущего объекта КИИ (более подробно см. раздел Формирование итоговых документов).

По нажатию на иконку  в поле с документом можно скачать файл в формате .docx.

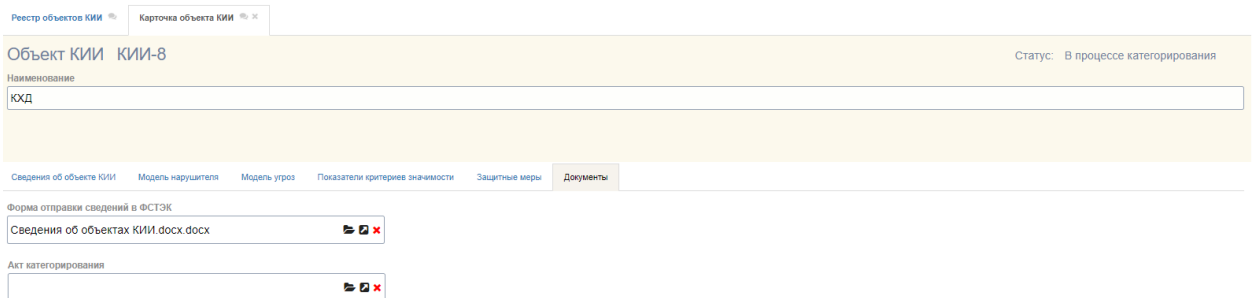


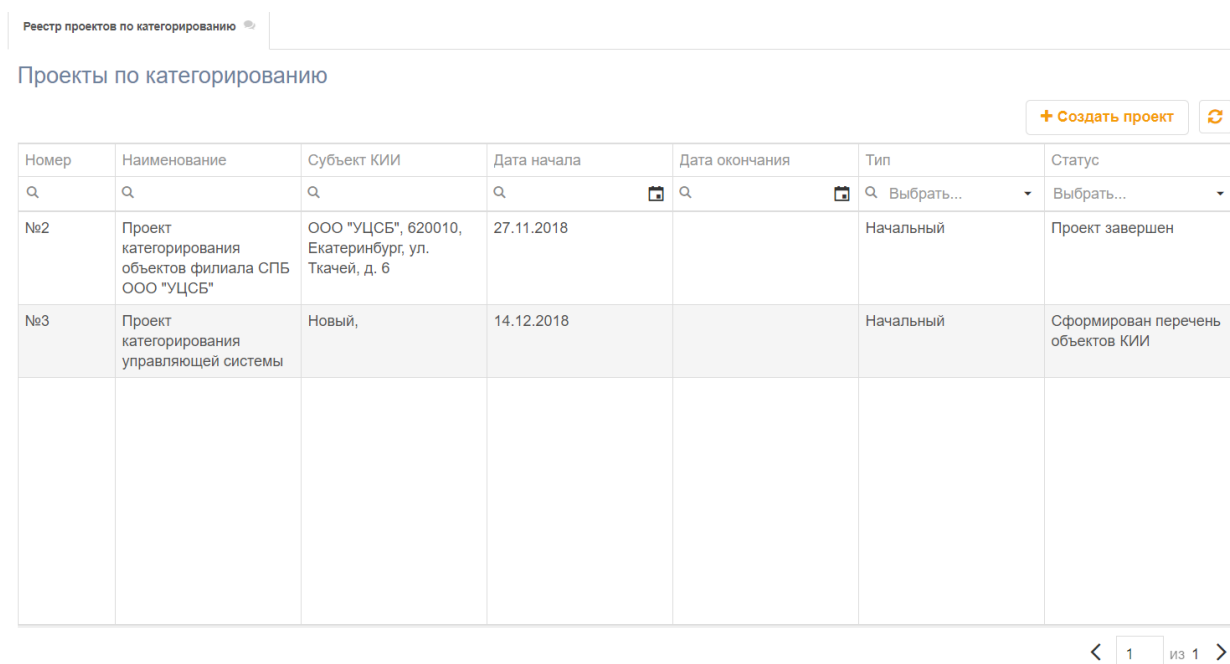
Рисунок 20 – Карточка объекта КИИ. Документы

7 Проведение проекта по категорированию

Раздел «Категорирование» предназначен для автоматизации процесса категорирования объектов КИИ.

До начала процесса категорирования необходимо убедиться, что в Реестре субъектов КИИ создан субъект, для которого проводится категорирование.

На начальном экране раздела (Рисунок 21) представлен реестр проектов по категорированию.



Реестр проектов по категорированию

Проекты по категорированию

+ Создать проект

Номер	Наименование	Субъект КИИ	Дата начала	Дата окончания	Тип	Статус
№2	Проект категорирования объектов филиала СПБ ООО "УЦСБ"	ООО "УЦСБ", 620010, Екатеринбург, ул. Ткачей, д. 6	27.11.2018		Начальный	Проект завершен
№3	Проект категорирования управляющей системы	Новый,	14.12.2018		Начальный	Сформирован перечень объектов КИИ

< 1 из 1 >

Рисунок 21 – Реестр проектов по категорированию

Чтобы перейти в карточку проекта из реестра проектов по категорированию, необходимо дважды кликнуть по соответствующей записи в таблице.

7.1 Создание нового проекта

Для создания нового проекта нажмите кнопку «Создать проект», расположенную над таблицей. Во всплывающем окне откроется карточка нового проекта по категорированию (Рисунок 22).

Создание нового проекта по категорированию

Проект категорирования 13

Наименование проекта

Дата начала * 14.12.2018

Дата окончания

Субъект КИИ * Субъект

Комиссия * Текст

Тип проекта * Начальный

Инициатор * akrasnova

Начать проект

Рисунок 22– Карточка нового проекта по категорированию

Внесите общие сведения о новом проекте в соответствующие поля карточки:

- наименование проекта;
- дата начала (по умолчанию автоматически присваивается текущая дата);
- плановая дата завершения;
- субъект КИИ;
- комиссия по категорированию;
- тип проекта;
- инициатор (по умолчанию автоматически присваивается текущий пользователь).



Нажмите кнопку «Начать проект».

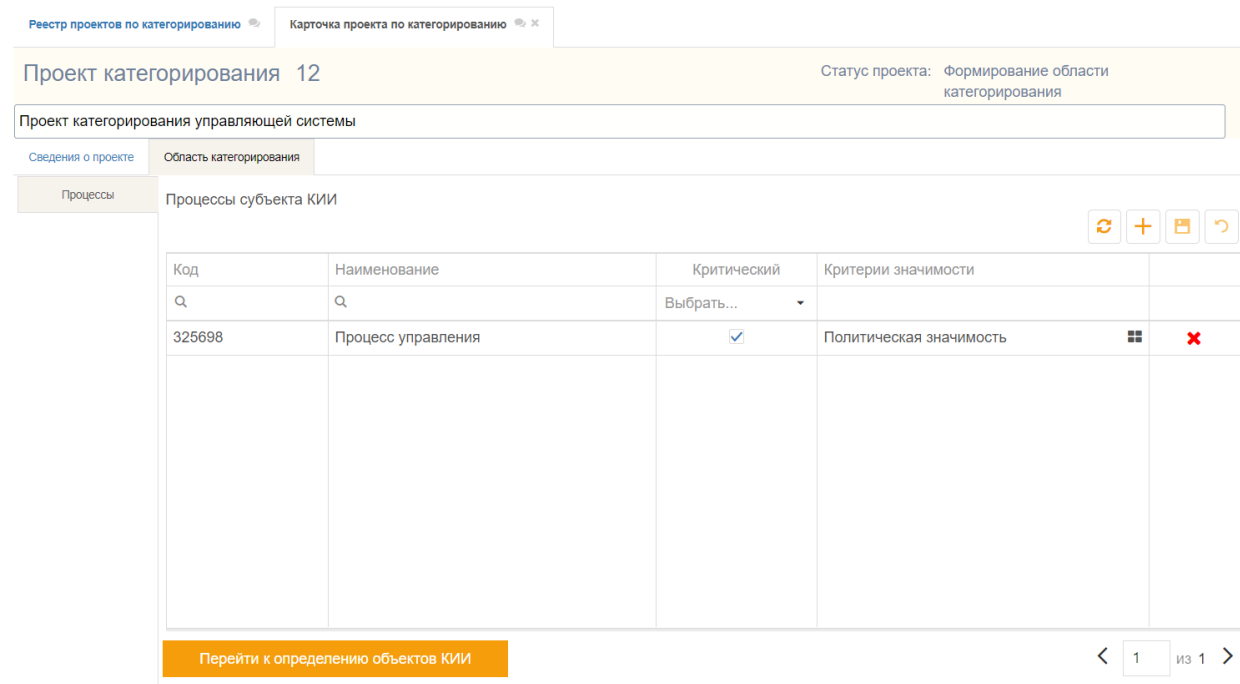
Проект перейдет в статус «Формирование области категорирования».

7.2 Формирование области категорирования

В карточке проекта на статусе формирования области открывается вкладка «Область категорирования» (Рисунок 23), в которой отражены сведения о процессах субъекта.

На первом этапе категорирования необходимо выбрать критические процессы и указать критерии значимости, по которым процесс является критическим. Для того, чтобы указать критические процессы, поставьте галочку в колонке «Критический» в

необходимых строках таблицы и нажмите кнопку . Чтобы указать критерии значимости, по которому критичен процесс, нажмите на  в соответствующей строке.





Реестр проектов по категорированию | Карточка проекта по категорированию

Проект категорирования 12 | Статус проекта: Формирование области категорирования

Проект категорирования управляющей системы

Сведения о проекте | Область категорирования

Процессы | Процессы субъекта КИИ

Код	Наименование	Критический	Критерии значимости
Q	Q	Выбрать...	
325698	Процесс управления	<input checked="" type="checkbox"/>	Политическая значимость  

Перейти к определению объектов КИИ | 1 из 1

Рисунок 23– Карточка проекта по категорированию. Определение критичных процессов

Чтобы добавить процесс в таблицу, необходимо нажать на кнопку добавления в верхнем правом углу таблицы. После этого в новой строке таблицы заполните необходимые поля и нажмите кнопку сохранения вверху таблицы.

После того, как определены бизнес-процессы, нажмите на кнопку «Перейти к определению объектов КИИ».

На форме отобразится вкладка с системами, которые обеспечивают выполнение ранее указанных критических процессов субъекта КИИ (Рисунок 24).

Реестр проектов по категорированию | Карточка проекта по категорированию

Проект категорирования 12 | Статус проекта: Формирование области категорирования

Проект категорирования управляющей системы

Сведения о проекте | Область категорирования

Процессы | Системы, обеспечивающие критические процессы

ИС, АСУ, ИТС

<input type="checkbox"/>	Код	Наименование	Тип системы	Объект КИИ
	Q	Q	Q Выбрать...	Q Выбрать...
<input type="checkbox"/>	IS-0	Система управления производством	ИС	Да

1 из 1

Являются объектами КИИ | Не являются объектами КИИ | Сформировать перечень

Рисунок 24 – Карточка проекта. Область категорирования. Системы

Для того, чтобы зафиксировать решение является ли система объектом КИИ, необходимо в таблице в первом столбце отметить нужные системы и нажать кнопку

Являются объектами КИИ

, если системы являются таковыми, или кнопку

Не являются объектами КИИ

в противном случае. После нажатия той или иной кнопки в графе «Объект КИИ» таблицы автоматически отобразится выбранный статус для систем.

После определения значимых объектов, нажмите кнопку «Сформировать перечень».

На форме отобразится вкладка «Объекты КИИ» с перечнем объектов, подлежащих категорированию (Рисунок 25).

Реестр проектов по категорированию | Карточка проекта по категорированию

Проект категорирования 12 | Статус проекта: Формирование области категорирования

Проект категорирования управляющей системы

Сведения о проекте | Область категорирования

Процессы
ИС, АСУ, ИТС

Объекты КИИ

Перечень объектов КИИ

Искать...

<input type="checkbox"/>	Наименование	Статус	Системы, входящие в объект КИИ
<input type="checkbox"/>	?	Выбрать...	
<input type="checkbox"/>	Система управления производством	В перечне объектов КИИ	☰ ✖

< 1 из 1 >

Объединить в один объект | Разгруппировать объекты | Перечень сформирован

Рисунок 25 – Карточка проекта. Область категорирования. Объекты КИИ

Для того, что сформировать группу из нескольких подобных объектов, необходимо в первом столбце отметить объединяемые объекты и нажать на кнопку «Объединить в один объект». После чего в таблице вместо записей выбранных объектов появится одна запись группы объектов, а в столбце «Системы, входящие в объект» отобразятся системы, которые были сгруппированы.

! Важно

Объединять объекты допускается в случае, если системы автоматизируют один (одни) критический(-ие) процесс(-ы).

*В случае объединения значимых объектов, обеспечивающих **разные** критические процессы, в строке таблицы с сгруппированным объектом ячейка с системами подсветится красным цветом (Рисунок 26).*

В таком случае отметьте объект в первом столбце таблицы и нажмите кнопку «Разгруппировать объекты».

Реестр проектов по категорированию | Карточка проекта по категорированию

Проект категорирования 12 | Статус проекта: Формирование области категорирования

Проект категорирования управляющей системы

Сведения о проекте | Область категорирования

Процессы
ИС, АСУ, ИТС

Объекты КИИ


Перечень объектов КИИ

Искать...

<input type="checkbox"/>	Наименование	Статус	Системы, входящие в объект КИИ	
	Q	Выбрать...		
<input type="checkbox"/>	Система управления производством, Система с другими критическими процессами	В перечне объектов КИИ	Система управления производством, Система с другими критическими процессами	✘

Объединить в один объект | Разгруппировать объекты | Перечень сформирован

Рисунок 26 – Карточка проекта. Попытка сгруппировать системы, обеспечивающие разные критические процессы

Автоматически формируется имя сгруппированного объекта: связка имён объединённых систем. Имя можно изменить в таблице, нажав на ячейку с именем объекта. После внесения изменений нажмите кнопку сохранения .

Чтобы разгруппировать объект, нажмите на соответствующую кнопку внизу формы. Вместо одной сгруппированной записи объекта КИИ отобразятся записи объектов КИИ, которые ранее были сгруппированы.

Чтобы удалить объект из списка, нужно нажать левой кнопкой мыши на красный крестик в строке объекта (Рисунок 27).

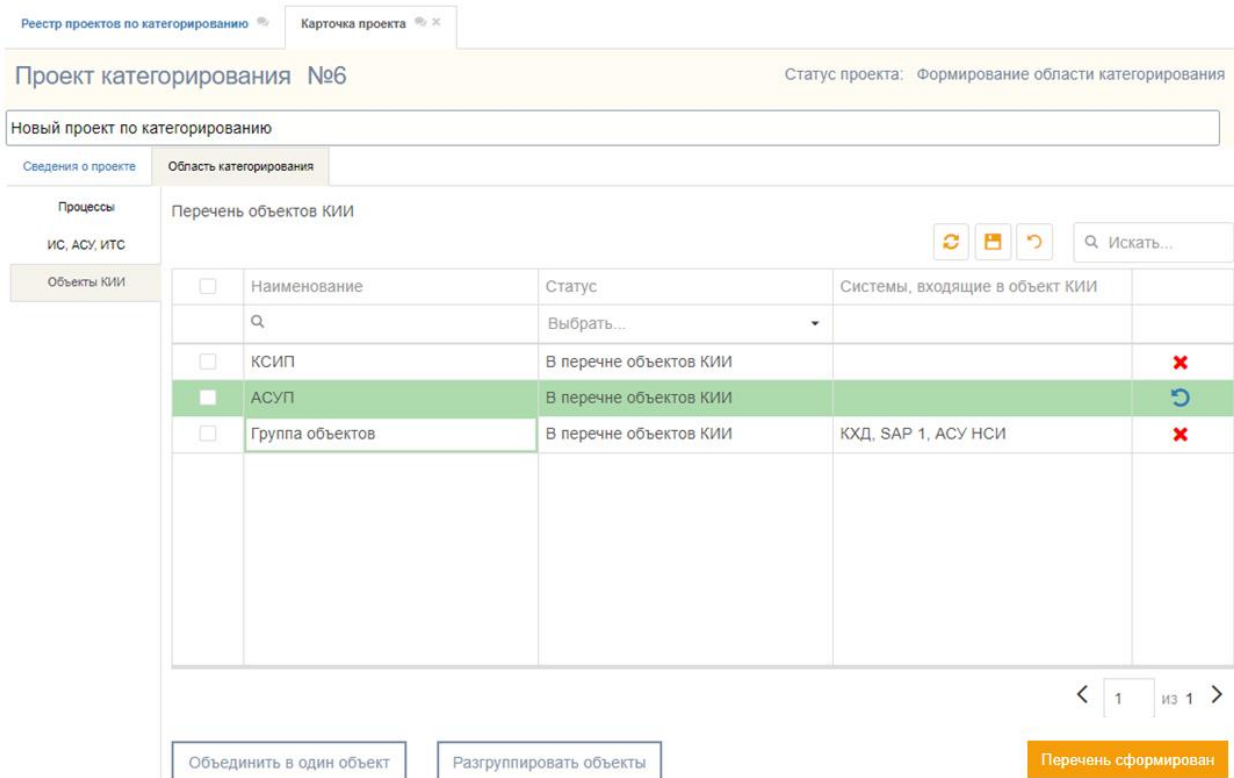


Рисунок 27 – Карточка проекта. Область категорирования. Объекты. Пример удаления систем

По двойному клику левой кнопкой мыши на запись объекта в таблице открывается редактируемая карточка категорируемого объекта (более подробно см. раздел Просмотр и редактирование информации об объекте КИИ).

После завершения формирования перечня объектов КИИ нажмите кнопку «Перечень сформирован». Проект перейдет на статус «Сформирован перечень объектов КИИ».

7.3 Перечень объектов

При переходе проекта на статус «Сформирован Перечень объектов» открывается вкладка «Перечень объектов КИИ» (Рисунок 28). На вкладке присутствует следующая информация:

- сформированный в формате Microsoft Word документ Перечень объектов КИИ, подлежащих категорированию;
- реестр объектов, подлежащих категорированию.

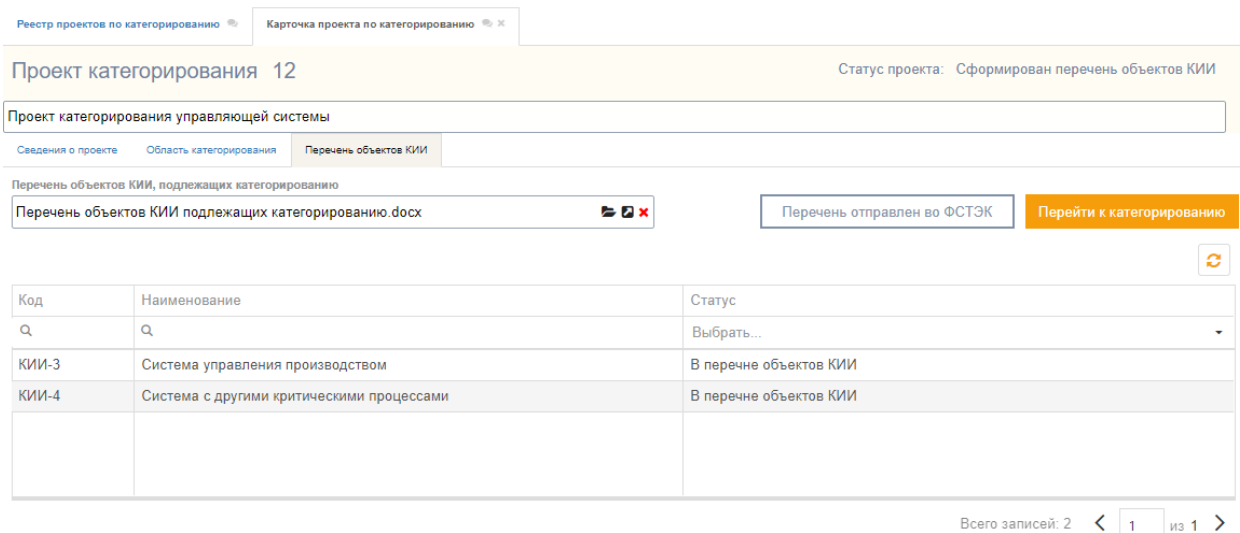


Рисунок 28 – Карточка проекта. Перечень объектов КИИ

На вкладке доступны следующие действия:

1. Перечень отправлен во ФСТЭК

Соответственно законодательству (ПП 127) перечень объектов в течение 5 рабочих дней **после утверждения** должен быть направлен во ФСТЭК.

По кнопке «Перечень отправлен во ФСТЭК» открывается всплывающее окно (Рисунок 29) для указания даты утверждения перечня руководителем субъекта КИИ или уполномоченным лицом.

При нажатии на кнопку «Сохранить» проекту будет присвоен срок категорирования, который равен одному году со дня утверждения субъектом КИИ Перечня объектов.

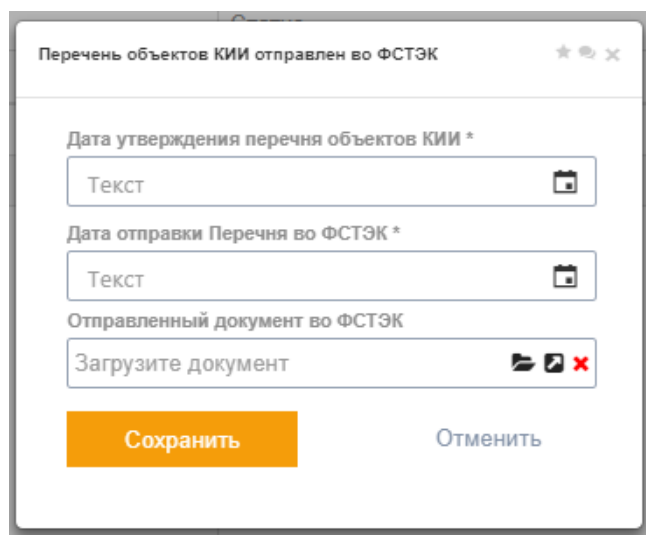


Рисунок 29 – Заполнение информации о направлении перечня объектов КИИ во ФСТЭК

2. Замечания ФСТЭК

Кнопка «Замечания от ФСТЭК» отобразится на форме после того, как будет заполнена информация о направлении перечня ФСТЭК.

Кнопку следует нажать в случае, если по отправленному перечню ФСТЭК ответил замечаниями.

В таком случае существуют два сценария (Рисунок 30):

- можно внести изменения в текущий проект – проект перейдет на статус формирования перечня.
- можно создать новый проект, если замечания серьезные.

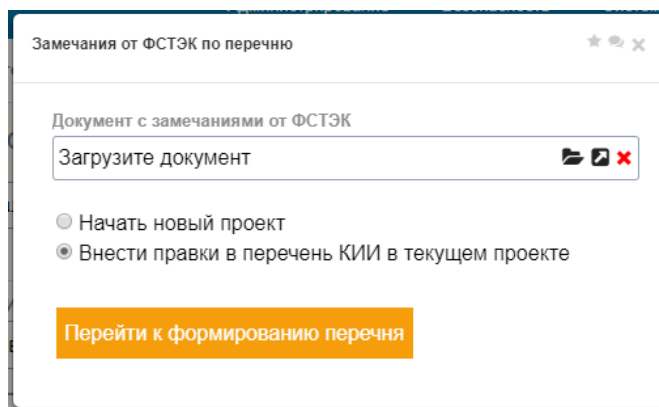


Рисунок 30 – Всплывающее окно с выбором дальнейших действий в системе после замечаний от ФСТЭК России по отправленному перечню объектов КИИ

При любом варианте все результаты категорирования, если какие-то действия уже были сделаны (например, для некоторых объектов была создана модель угроз), сохраняются.

3. Перейти к категорированию

При нажатии на кнопку «Перейти к категорированию» проект перейдет на статус «Категорирование» и откроется вкладка «Категорирование».

7.4 Категорирование

Определение категории состоит из 3 шагов.

1. Разработка модели нарушителя (анализ возможных действий нарушителей в отношении объектов КИИ, а также иных источников угроз безопасности информации).
2. Разработка модели угроз (анализ угроз безопасности информации и уязвимостей, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ)

3. Заполнение опросного листа в соответствии с перечнем показателей критериев значимости, приведенные в ППРФ №127.

Создание модели нарушителя

На вкладке «Модель нарушителей» отображена таблица с категорируемыми объектами, созданными моделями нарушителя для объектов и статусом модели нарушителя (Рисунок 31):

The screenshot shows a web interface for 'Project Categorization 12'. At the top, it displays 'Срок категорирования: 14.12.2019' and 'Статус проекта: Категорирование'. Below this is a search bar containing 'Проект категорирования управляющей системы'. A navigation menu includes 'Сведения о проекте', 'Область категорирования', 'Перечень объектов КИИ', and 'Категорирование'. The main content area is titled 'Модели нарушителя объектов КИИ' and contains a table with the following data:

<input type="checkbox"/>	Код	Наименование	Статус	Модель нарушителя	Статус модели
<input type="checkbox"/>	Q	Q	Выбрать...		
<input type="checkbox"/>	КИИ-3	Система управления производством	Анализ возможных действий нарушителей		
<input type="checkbox"/>	КИИ-4	Система с другими критическими процессами	Анализ возможных действий нарушителей		

Below the table is an orange button labeled 'Создать модель нарушителя' and a pagination control showing '< 1 из 1 >'. On the left side, there are navigation tabs for 'Модель нарушителей', 'Модель угроз', and 'Показатели критериев значимости'.

Рисунок 31 – Карточка проекта. Категорирование

Ячейки с моделью нарушителя и её статусом будут пустыми, если модель еще не была создана для соответствующего объекта КИИ.

Для создания модели нарушителя необходимо в первом столбце таблицы указать объект(-ы) и нажать кнопку «Создать модель нарушителя». Если одну модель нарушителя нужно создать для нескольких объектов, допускается множественный выбор объектов.

При нажатии на кнопку «Создать модель нарушителя» во всплывающем окне отобразится форма «Создание модели нарушителя», на которой указывается наименование модели и приводится список объектов КИИ, для которых создается модель (Рисунок 32).

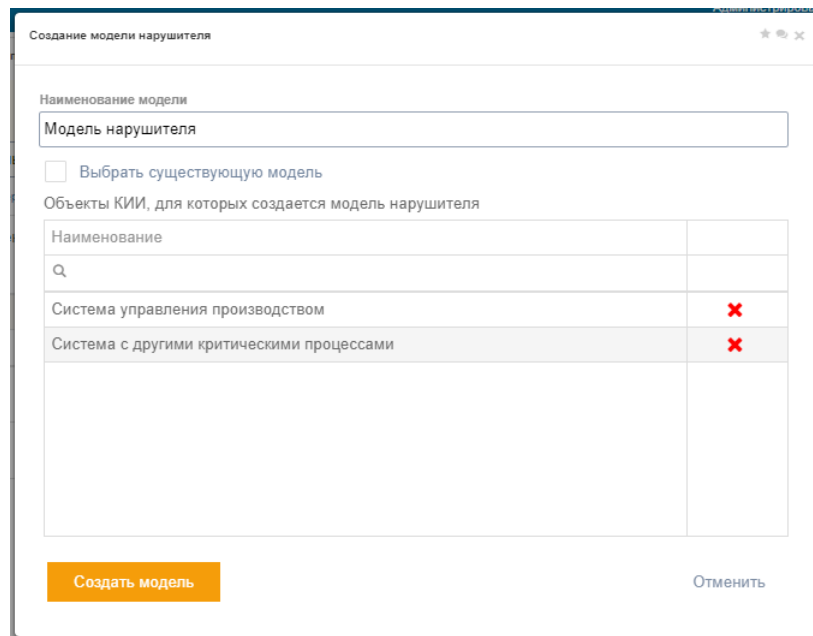


Рисунок 32 – Всплывающее окно с настройками создающейся модели нарушителя

На форме можно вместо создания новой модели нарушителя выбрать существующую модель. При выборе данной опции отобразится поле «Модель нарушителя» с выпадающим списком, в котором можно выбрать модель нарушителя, которая уже создавалась в *текущем* проекте. Если в текущем проекте модели нарушителей еще не создавались, выпадающий список будет пустым.

Для удаления связи с объектом КИИ у создаваемой модели нарушителя нажмите значок удаления **✗**, расположенный в крайней правой колонке таблицы «Объекты КИИ, для которых создается модель нарушителя».

Нажмите кнопку «Создать модель».

Всплывающее окно закроется и в таблице «Модели нарушителя объектов КИИ» (карточка проекта по категорированию, вкладка Категорирование) у указанных ранее объектов КИИ появится ссылка на карточку модели нарушителя в четвертой колонке. В последнем столбце отобразится статус модели (Редактируется).

Переход в карточку модели нарушителя осуществляется по нажатию на ссылку в столбце «Модель нарушителя». Откроется карточка модели нарушителя объекта КИИ.

На карточке модели нарушителя можно задать следующую информацию:

- Наименование модели
- Удалить связь с объектом
- Перечень актуальных нарушителей
- Чтобы завершить разработку модели нажмите кнопку «Завершить».





При завершении модель перейдет в статус «Завершена» (Рисунок 33) и все связанные объекты переходят на статус «Анализ угроз и уязвимостей» и карточка модели закрывается.

Модель нарушителя №0 Завершена

Определение возможных действий нарушителей в отношении объектов КИИ, а также иных источников информации

Наименование модели
Модель нарушителя

Объекты КИИ
Система управления производством, Система с другими критическими процессами

Категория нарушителя	Виды нарушителя	Не актуальный	Обоснование невозможности реализовать УБИ
q	q	Выбрать... ▾	q
Внешний нарушитель с низким потенциалом	Внешние субъекты (физические лица), бывшие работники	<input type="checkbox"/>	
Внутренний нарушитель с низким потенциалом	Пользователи системы, лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру, лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных работ	<input type="checkbox"/>	
Внешний нарушитель со средним потенциалом	Террористические, экстремистские группировки, преступные группы (криминальные структуры), конкурирующие организации, разработчики, производители, поставщики программных, технических и программнотехнических средств	<input type="checkbox"/>	
Внешний нарушитель с высоким потенциалом	Специальные службы иностранных государств (блоков государств)	<input type="checkbox"/>	
Внутренний нарушитель со средним потенциалом	Администраторы информационной системы и администраторы безопасности	<input type="checkbox"/>	
Внутренний нарушитель с высоким потенциалом	Специальные службы иностранных государств (блоков государств)	<input type="checkbox"/>	




 из 1 

Рисунок 33 – Завершенная модель нарушителя

Создание модели угроз

Для создания модели угроз перейдите в раздел «Модель угроз» на вкладке «Категорирование» карточки проекта.

На вкладке «Модель угроз» отображена таблица с категорируемыми объектами, для которых уже создана модель нарушителя (Рисунок 34): Объекты КИИ сгруппированы в таблице по моделям нарушителя.

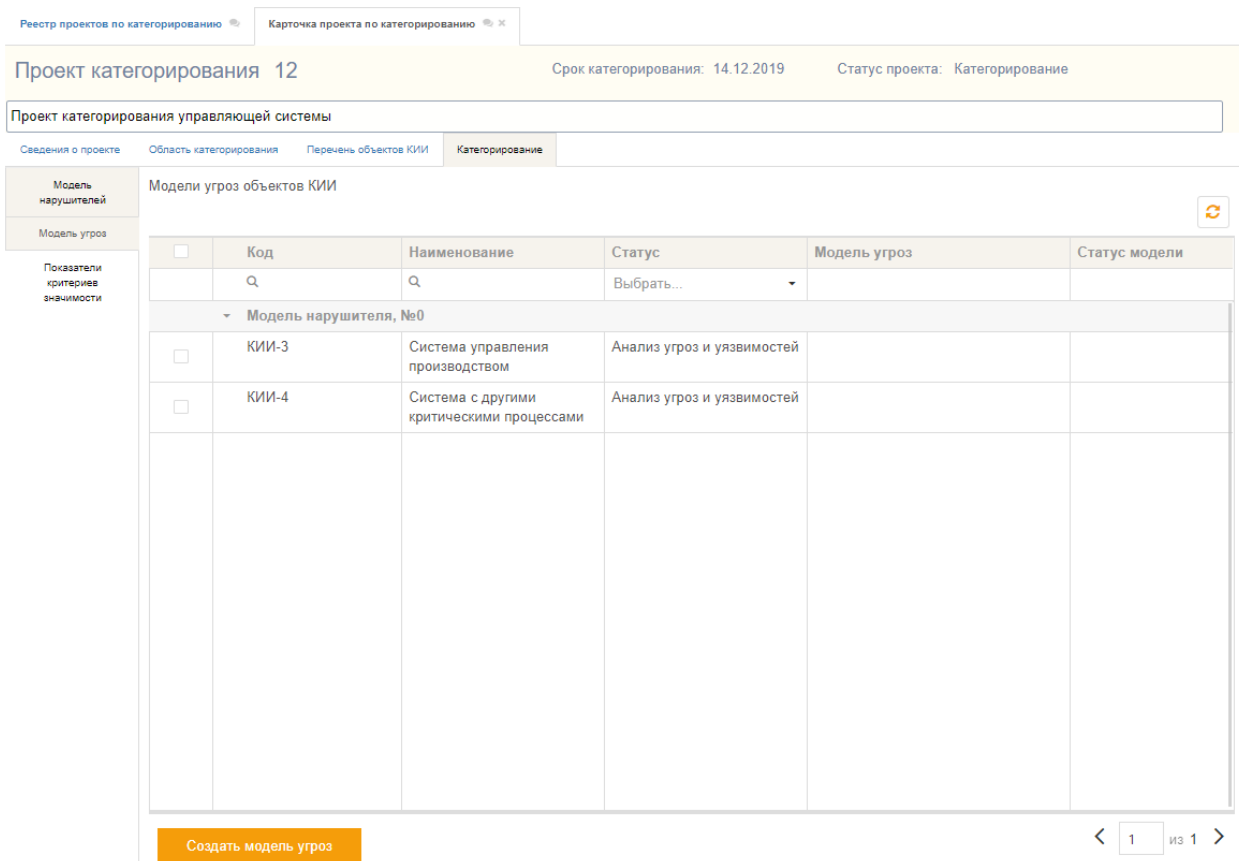


Рисунок 34 – Карточка проекта. Категорирование. Модель угроз

По аналогии с созданием моделей нарушителя для создания модели угроз необходимо в первом столбце таблицы указать объекты и нажать кнопку «Создать модель угроз». Если требуется создать одну модель угроз для нескольких объектов, допускается множественный выбор объектов.

! Для сведения

В соответствии с Приказом ФСТЭК России №239 от 25.12.2017 г. «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», модель угроз может разрабатывать для группы объектов, имеющих одинаковые цели создания и архитектуру, а также типовые угрозы безопасности.

При нажатии на кнопку «Создать модель угроз» во всплывающем окне отобразится форма «Создание модели угроз», на которой указывается наименование модели и приводится список объектов КИИ, для которых создается модель угроз (Рисунок 35).

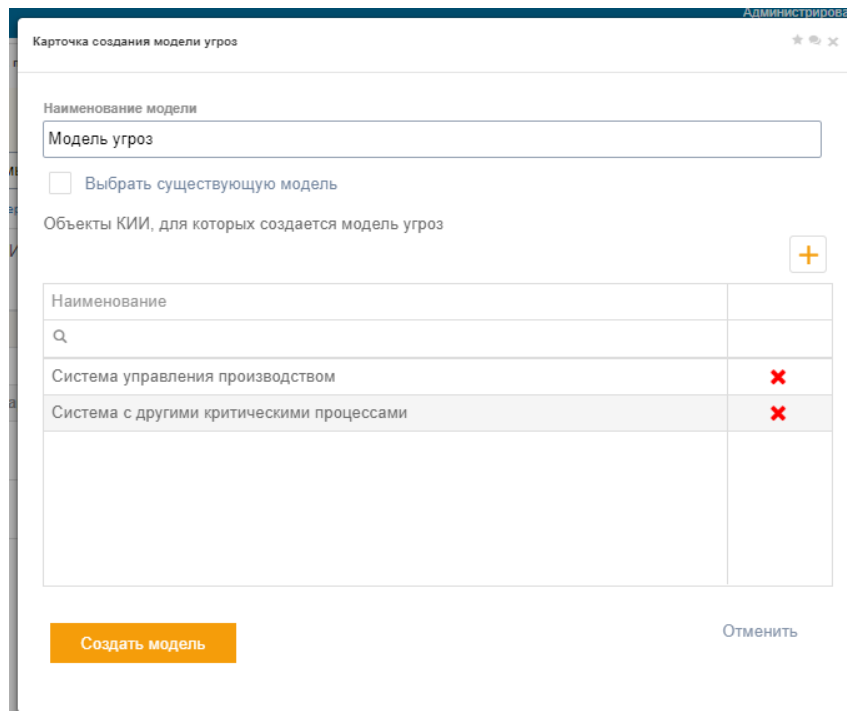


Рисунок 35 – Всплывающее окно с настройками создающейся модели угроз

На форме можно вместо создания новой модели угроз выбрать существующую модель. При выборе данной опции отобразится поле «Модель угроз» с выпадающим списком, в котором можно выбрать модель, которая уже создавалась в *текущем* проекте. Если в текущем проекте модели угроз еще не создавались, выпадающий список будет пустым.

! Важно

*Модель угроз не может быть создана для нескольких объектов КИИ, у которых **разные** модели нарушителя. Модель угроз жестко привязана к какой-то конкретной модели нарушителя, так как актуальные нарушители выступают в качестве источника угроз.*

Если попытаться создать модель угроз для нескольких объектов с разными моделями нарушителей, во всплывающем окне отобразится соответствующее предупреждение.

При нажатии на кнопку «Создать модель» во всплывающем окне отобразится форма фильтрации (Рисунок 36).

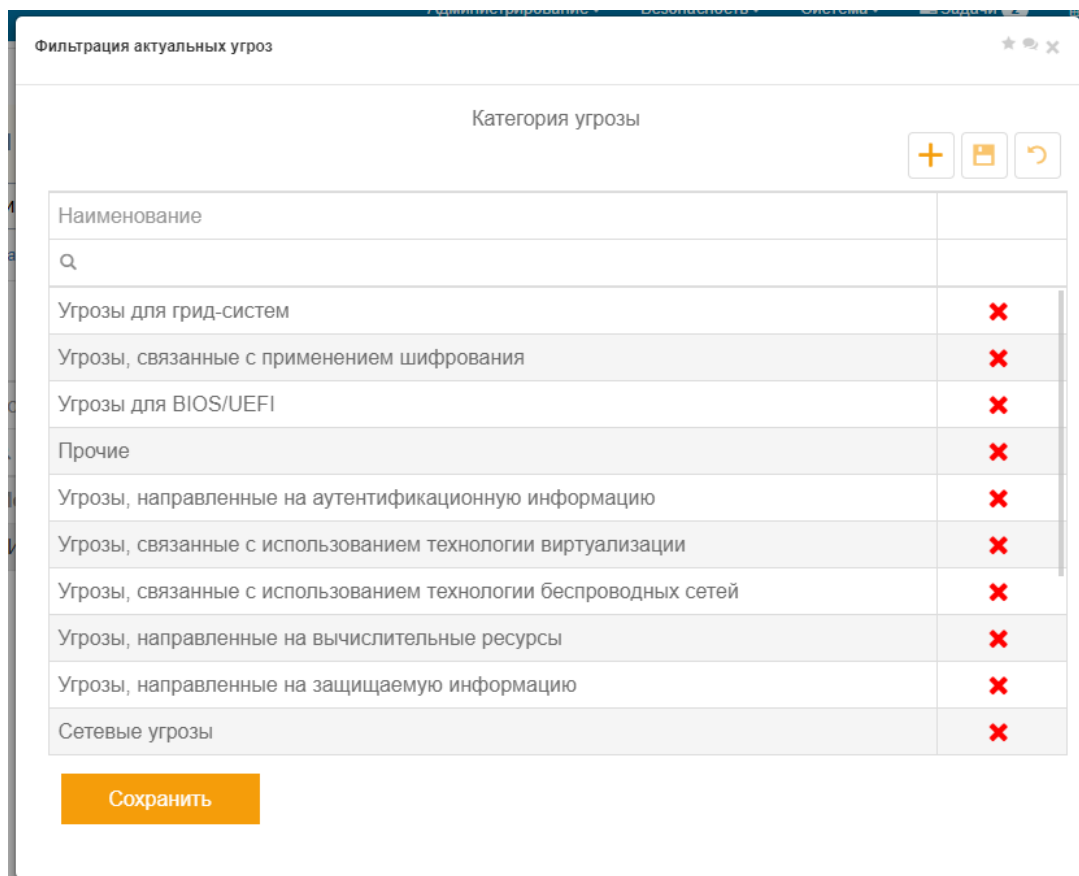


Рисунок 36 – Фильтрация угроз из БДУ ФСТЭК России по категориям угроз

В таблице представлены категории угроз из Базы данных угроз ФСТЭК России. Если в архитектуре объекта(-ов) отсутствует соответствующая технология или для объекта(-ов) не свойственны угрозы представленной категории, нажмите на значок ✘ в последнем столбце таблицы.

Угрозы оставленных категорий будут включены в создаваемую модель угроз, то есть будут считаться актуальными угрозами информационной безопасности для объекта(-ов) КИИ, для которых создается модель угроз.

Нажмите кнопку «Сохранить». Всплывающее окно закроется.

В таблице «Модели угроз объектов КИИ» (карточка проекта по категорированию, вкладка Категорирование) у указанных ранее объектов КИИ появится ссылка на карточку модели угроз в четвертой колонке (Рисунок 37). В последнем столбце отобразится статус модели (Редактируется).

Реестр проектов по категорированию | Карточка проекта по категорированию

Проект категорирования 12 | Срок категорирования: 14.12.2019 | Статус проекта: Категорирование

Проект категорирования управляющей системы

Сведения о проекте | Область категорирования | Перечень объектов КИИ | Категорирование

Модель нарушителей | Модели угроз объектов КИИ

<input type="checkbox"/>	Код	Наименование	Статус	Модель угроз	Статус модели
▼ Модель нарушителя, №0					
<input type="checkbox"/>	КИИ-3	Система управления производством	Анализ угроз и уязвимостей	Модель угроз, №0	Редактируется
<input type="checkbox"/>	КИИ-4	Система с другими критическими процессами	Анализ угроз и уязвимостей	Модель угроз, №0	Редактируется

Рисунок 37 – Вкладка Категорирование. Ссылки на созданные модели угроз для объектов КИИ

Переход в карточку модели осуществляется по нажатию на ссылку в столбце «Модель угроз».

В новой вкладке откроется форма с моделью угроз (Рисунок 38).

Реестр проектов по категорированию | Карточка проекта | Карточка модели угроз объекта КИИ

Модель угроз №0 | Редактируется

Анализ угроз безопасности информации и уязвимостей, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ


Наименование модели:

Объекты КИИ, для которых создается модель угроз:

ID угрозы	Наименование	Нарушитель	Уязвимости
УБИ 027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с высоким потенциалом	Слабости мер антивирусной защиты и контроля достоверности входных и выходных данных, а также ошибками, допущенными в ходе проведения специальных проверок аппаратных средств вычислительной техники. Реализация данной угрозы возможна при условии наличия в дискредитируемой информационной системе вредоносного программного обеспечения (например, виртуальных драйверов устройства) или аппаратных закладок
УБИ 107	Угроза отключения контрольных датчиков	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с высоким потенциалом	Слабости мер защиты информации в автоматизированных системах управления технологическими процессами, а также наличием уязвимостей в программном обеспечении, реализующим данные меры. Реализация данной угрозы возможна при условии получения доступа

1 из 1

Рисунок 38 – Карточка модели угроз

В таблице на форме представлен перечень актуальных угроз для объекта(-ов) КИИ. Для добавления угрозы в перечень актуальных угроз нажмите на  над таблицей.

Откроется всплывающее окно с перечнем всех угроз из БДУ ФСТЭК России (Рисунок 39).



Рисунок 39 – Добавление актуальной угрозы в модель угроз

В первом столбце таблицы отметьте галочками актуальные угрозы и нажмите «Сохранить».

Для завершения создания модели угроз нажмите на на форме модели угроз.

На форме над таблицей отобразится автоматически сформированный документ в формате .docx с моделью угроз (Рисунок 40).

Модель угроз №0

Завершена

Анализ угроз безопасности информации и уязвимостей, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ

Наименование модели

Модель угроз

Объекты КИИ, для которых создается модель угроз

Система управления производством, Система с другими критическими процессами

Удалить связь с объектом

Модель угроз.docx

ID угрозы	Наименование	Нарушитель	Уязвимости
	привилегиями	потенциалом, Внешний нарушитель со средним потенциалом,	и команд, а также мер по разграничению доступа. Реализация данной угрозы возможна при условиях: обладания дискредитируемой программой повышенными привилегиями в системе; осуществления дискредитируемой программой приема входных данных от других программ или от пользователя; нарушитель имеет возможность осуществлять передачу данных к дискредитируемой программе
УБИ 010	Угроза выхода процесса за пределы виртуальной машины	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Уязвимости программного обеспечения гипервизора, реализующего функцию изолированной программной среды для функционирующих в ней программ, а также слабости инструкций аппаратной поддержки виртуализации на уровне процессора. Реализация данной угрозы приводит не только к компрометации гипервизора, но и запущенных в созданной им виртуальной среде средств защиты, а, следовательно, к их неспособности

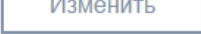
Всего записей: 58 1 из 6

Изменить

Удалить

Рисунок 40 – Завершенная модель угроз информационной безопасности для категорируемых объекта(-ов) КИИ

Чтобы выгрузить документ нажмите на иконку  в поле с документом.

Кнопка  возвращает модель на начальный статус, на котором можно внести изменения в модель угроз.

По кнопке  модель угроз удаляется.

Создание опросного листа Показателей критериев значимости

Для создания опросного листа перейдите в раздел «Показатели критериев значимости» на вкладке «Категорирование» в карточке проекта по категорированию.

На форме отображена таблица с категорируемыми объектами, созданными опросными листами для объектов КИИ и их статусами:

Ячейки с опросными листами и их статусом будут пустыми, если опросные листы еще не были созданы для соответствующих объектов КИИ.

Для создания опросного листа необходимо в первом столбце таблицы указать объекты КИИ, для которых будет создаваться опросный лист. Далее нажмите кнопку «Создать опросный лист».

Во всплывающем окне откроется форма «Карточка создания опросного листа», на которой указывается наименование опросного листа и приводится список объектов КИИ, для которых он создается (Рисунок 41).

Карточка создания опросного листа

Наименование опросного листа

Опросный лист

Выбрать существующий опросный лист

Объекты КИИ, для которых создается опросный лист

Наименование	
Система управления производством	✗
Система с другими критическими процессами	✗

Создать опросный лист

Отменить

Рисунок 41 – Всплывающее окно с настройками создающегося опросного листа

На форме можно вместо создания нового опросного листа выбрать существующий. При выборе данной опции отобразится поле «Опросный лист» с выпадающим списком, в котором можно выбрать опросный лист, который уже был создан ранее. Если этот опросный лист уже завершен, то объектам сразу же присвоится категория, которая была определена в выбранном опросном листе.

При нажатии на кнопку «Создать опросный лист» будет создан опросный лист. Всплывающее окно закроется.

Ссылка на карточку созданного опросного листа отобразится в реестре «Опросные листы Показателей критериев значимости» (Рисунок 42). Для перехода к карточке опросного листа нажмите на соответствующую ссылку.

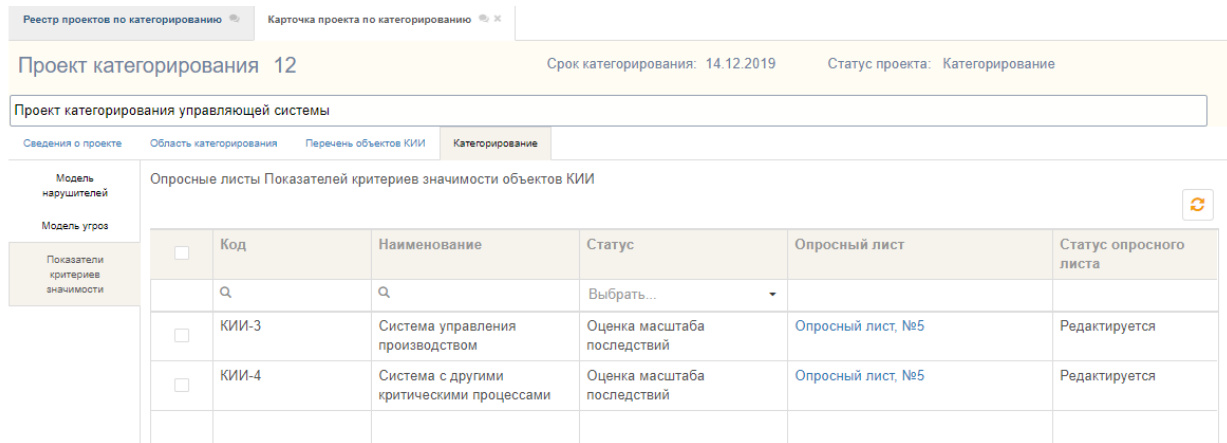


Рисунок 42 – Вкладка Категорирование. Ссылки на опросные листы

Заполнение опросного листа Показателей критериев значимости

Перейдите на карточку проекта на вкладку Категорирование в раздел Показатели критериев значимости (Рисунок 42).

Для перехода в карточку опросного листа нажмите на ссылку опросного листа в таблице «Опросные листы Показателей критериев значимости». Откроется карточка опросного листа (Рисунок 43).

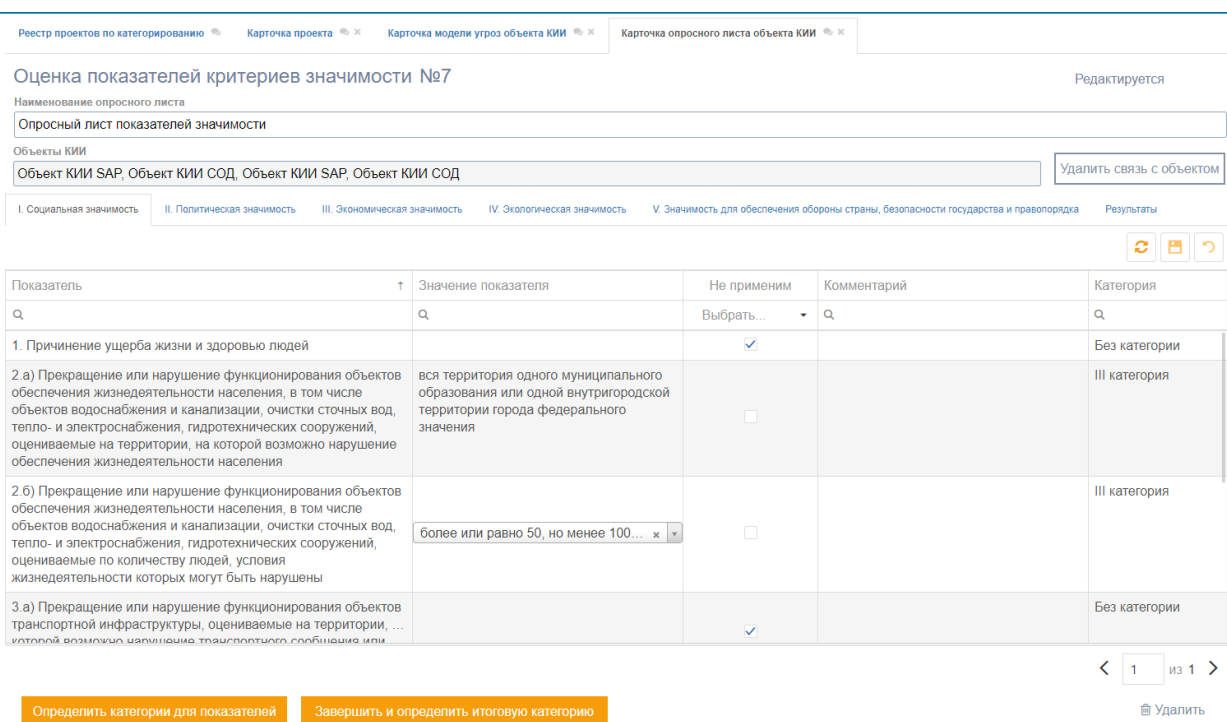


Рисунок 43 – Карточка опросного листа объекта КИИ

На карточке отображены:

- поле Наименование опросного листа;
- поле Объекты КИИ, отображается список объектов КИИ, связанных с данным опросным листом.

- Показатели критериев значимости разбиты по критериям значимости на 5 вкладок:
 - а) Социальная значимость;
 - б) Политическая значимость;
 - в) Экономическая значимость;
 - г) Экологическая значимость;
 - д) Значимость для обеспечения обороны страны, безопасности государства и правопорядка.

На каждой вкладке отображена таблица с показателями со следующими колонками:

- Показатель – наименование показателя;
- Значение показателя – выпадающий список с выбором значения показателя;
- Не применим – оценка применимости показателя;
- Комментарий – обоснование неприменимости показателя;
- Категория – определенная категория в результате расчета по кнопке «Определить категории для показателей».

Для каждого показателя необходимо выбрать значение в столбце «Значение показателя» или указать, что он не применим (поставив галочку в колонке *Не применим*) и написать обоснование в поле «Комментарий». После этого нажмите кнопку «Определить категории для показателей», в колонке *Категория* отобразится рассчитанная категория.

При определении категории всех показателей хотя бы для одного критерия значимости отобразится вкладка «Результаты», на которой представлены рассчитанные результаты по каждому критерию значимости.

! Как определяется

В соответствии с Постановлением Правительства РФ №127 объекту КИИ присваивается категория значимости с наивысшим значением. Для каждого критерия значимости определяется наивысшая категория по результатам оценки значений показателей критериев значимости.

Если определены категории по каждому критерию значимости, отображается кнопка Завершить и определить итоговую категорию, при нажатии определяется итоговая

категория для объекта КИИ. Итоговая категория для объекта(-ов) КИИ отобразится в верхнем правом углу карточки опросного листа.

Если опросный лист завершен и необходимо внести изменения, нажмите кнопку «Изменить» в нижнем правом углу. Карточка опросного листа станет доступной для редактирования.

Для удаления опросного листа нажмите кнопку «Удалить»

Закройте опросный лист и перейдите на карточку проекта по категорированию.

7.5 Результаты категорирования

Для просмотра результатов категорирования, перейдите на карточку проекта на вкладку «Результаты категорирования» (Рисунок 44).

Результаты категорирования

Код	Наименование	Категория значимости	Критерии, по которым определена категория	Сведения заполнены
КИИ-12	Объект КИИ SAP	III категория	Социальная значимость, Экономическая значимость	✓
КИИ-6	Объект КИИ СОД	III категория	Социальная значимость, Экономическая значимость	✓

Рисунок 44 – Карточка проекта. Результаты категорирования

В таблице отображаются присвоенные объектам категории на основании заполненных опросных листов.

Кнопка «Перейти к определению защитных мер» переводит проект на статус «Определение мер». На форме отображается вкладка с защитными мерами.

7.6 Защитные меры

Перечень необходимых защитных мер для объектов КИИ формируется на основании Приказа ФСТЭК России №239.

Для просмотра перечня необходимых для внедрения защитных мер перейдите на карточку проекта по категорированию. Вкладка с защитными мерами (Рисунок 45).

Реестр проектов по категорированию Карточка проекта по категорированию Карточка проекта по категорированию

Проект категорирования 12 Срок категорирования: 14.12.2019 Статус проекта: Определение мер

Проект категорирования управляющей системы

Сведения о проекте Область категорирования Перечень объектов КИИ Категорирование Результаты категорирования **Кросс-таблица ЗМ**

	Организационные меры		Технические меры													
			АВЗ, Антивирусная защита		АУД, Аудит безопасности		ДНС, Обеспечение действий в нештатных ситуациях		ЗИС, Защита информационной (автоматизированной) системы и ее компонентов		ЗНИ, Защита машинных носителей информации		ЗТС, Защита технических средств и систем		ИАФ, Идентификация и аутентификация	
	Границы реализации меры	Да/Нет	Границы реализации меры	Да/Нет	Границы реализации меры	Да/Нет	Границы реализации меры	Да/Нет	Границы реализации меры	Да/Нет	Границы реализации меры	Да/Нет	Границы реализации меры	Да/Нет	Границы реализации меры	Да/Нет
КИИ-3, . . . Система управления производством		Нет, Нет, Нет		Нет		Нет		Нет		Нет		Нет		Нет		Нет
КИИ-4, . . . Система с другими критическими процессами		Нет, Нет, Нет		Нет		Нет		Нет		Нет		Нет		Нет		Нет

Сформировать итоговые документы

Рисунок 45 – Карточка проекта. Реализованные защитные меры

На форме отображается кросс-таблица с перечнем необходимых для защиты объектов КИИ мер, которые должны быть внедрены.

В ячейке на пересечении объекта КИИ и требования из выпадающего списка выберите вариант:

- «Да», если мера реализована для значимого объекта;
- «Нет», если не реализована.

Если был указан вариант «Да», введите в соседнюю ячейку слева границы реализации меры для объекта КИИ.

7.7 Формирование итоговых документов

Для формирования актов категорирования и сведений об объектах КИИ по утвержденной форме ФСТЭК перейдите на карточку проекта по категорированию на вкладку с защитными мерами (Рисунок 45).

Нажмите «Сформировать итоговые документы». Проект перейдет на статус «Проект завершен». На форме отобразится вкладка «Заключение» (Рисунок 46).

Код	Наименование объекта КИИ	Сведения об объекте для ФСТЭК	Акт категорирования
КИИ-6	Объект КИИ СОД	Сведения об объектах КИИ.docx.docx	Акт категорирования объекта КИИ.docx
КИИ-12	Объект КИИ SAP	Сведения об объектах КИИ.docx.docx	Акт категорирования объекта КИИ.docx

Рисунок 46 – Сформированные итоговые документы по проекту

В таблице представлены заполненные формы сведений об объектах КИИ и акты категорирования объектов КИИ. Чтобы скачать документ, нажмите на название соответствующего документа в таблице, скачанные документы отобразятся в нижней строке браузера (Рисунок 47).

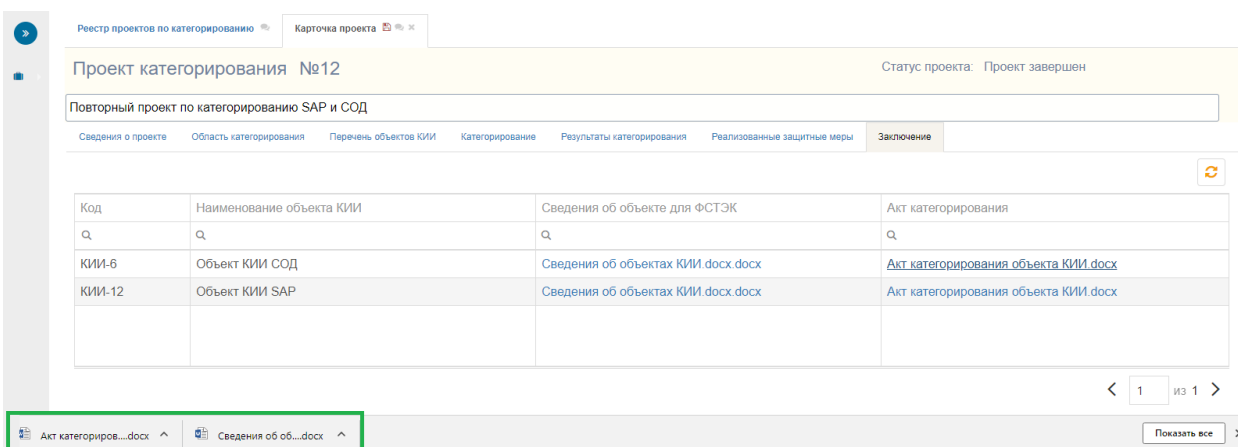


Рисунок 47 – Выгрузка документов