ООО «Компания Информационных Технологий»

«СИСТЕМА АВТОМАТИЗАЦИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ»

Управление обработкой персональных данных

Руководство пользователя

Екатеринбург
2022

Содержание

1. Общие положения

1.1. Термины, определения, сокращения

В настоящем руководстве использованы следующие сокращения:

- ИБ – Информационная безопасность.
- ИСПДн– Информационная система персональных данных.
- НДВ – Недекларированные возможности.
- ПДн – Персональные данные.
- ПО – Программное обеспечение.
- РФ – Российская федерация.
- УЗ – Уровень защищенности.
- ФСТЭК России – Федеральная служба по техническому и экспортному контролю России.

1.2. Общие сведения

Настоящее руководство пользователя устанавливает порядок работы с модулем «Управление обработкой персональных данных» (далее – модуль УОПДн).

Модуль «Управление обработкой персональных данных» предназначен для автоматизации деятельности организации по выполнению требований Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных» и его подзаконных актов.

1.3. Назначение модуля

Модуль УОПДн позволяет выполнять следующие функции:

1. Учет субъектов ПДн:
    - Учет типов ПДн для категорий субъектов;
    - Учет обращений субъектов ПДн;
2. Учет ИСПДн:
    - Ведение реестра типов, процессов обработки, носителей ПДн в составе ИСПДн, учет работников, допущенных к ИСПДн;
    - Определение уровня защищенности ИСПДн и уровня исходной защищенности ПДн;
    - Формирование модели угроз и нарушителей ИСПДн, учет нейтрализованных угроз при выполнении требований по защите;
    - Формирование перечня требований по защите ИСПДн и учет выполненных требований;
    - Учет инцидентов с ИСПДн.

3. Учет носителей ПДн.
4. Учет средств защиты информации.
5. Наполнение и актуализация справочников для ведения учета:
    - Категорий субъектов ПДн, чьи персональные данные обрабатываются в организации;
    - Типов, обрабатываемых ПДн;
    - Процессов обработки ПДн;
    - Носителей ПДн;
    - Работников, допущенных к ПДн;
    - Средств защиты информации (СрЗИ);
    - Третьих лиц и сторонних организаций, которым передаются ПДн и каналов передачи ПДн.
6. Автоматизированное формирование печатных форм и загрузка документов в систему.

2. Описание ролевой модели

Для получения доступа к работе с модулем у пользователя должна быть настроена роль «Руководство САОБ».

Пользователь в данной роли имеет полный доступ к функционалу модуля.

3. Начало работы с модулем

Для начала работы с модулем УОПДн 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 Руководства САОБ

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

В рабочей области Руководства САОБ отображаются вкладки с информацией по модулям Системы.

На рабочей области «Управление обработкой персональных данных» отображены диаграммы, в которые выведена основная информация по состоянию безопасности по каждой ИСПДн: количество угроз и количество нейтрализованных, требований и выполненных, количество инцидентов и из них – количество закрытых, результаты проверок соответствия требованиям (Рисунок 1).

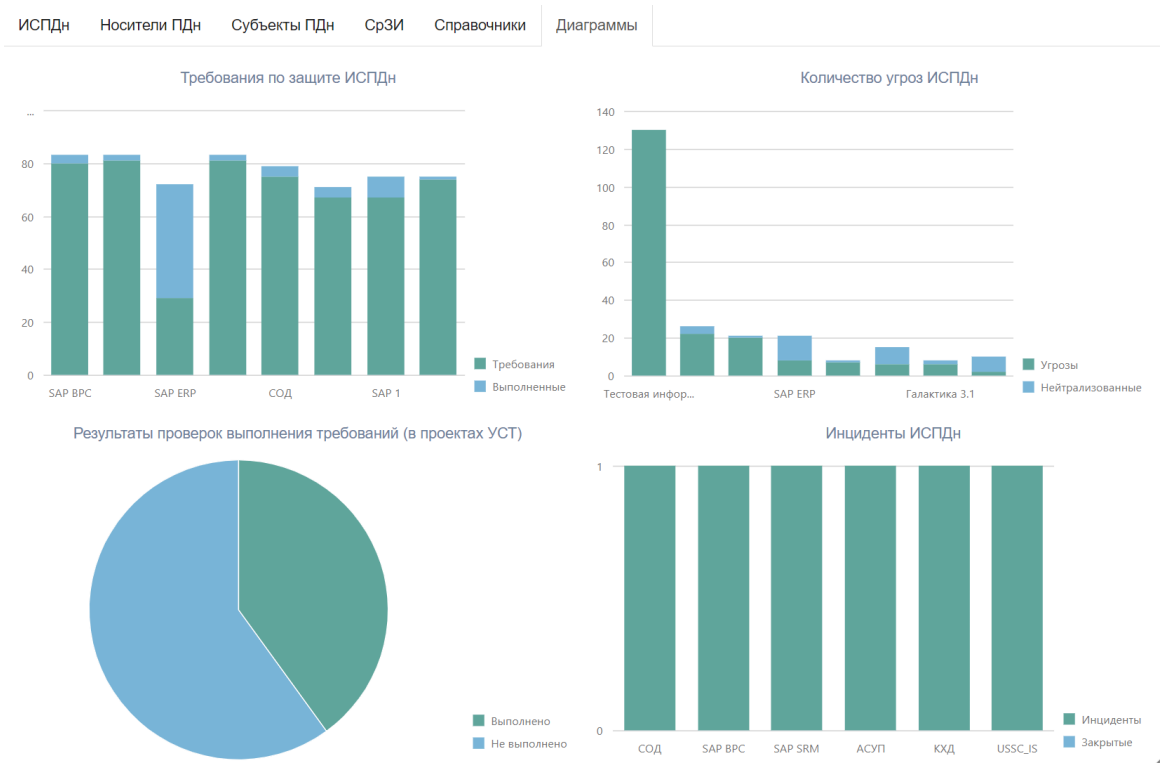

Рис. 1. Рабочая область Руководства САОБ

Переход к другим разделам модуля осуществляется с помощью вкладок в верхней части рабочей области:

- ИСПДн;
- Носители ПДн;
- Субъекты ПДн;
- СрЗИ;
- Справочники;
- Диаграммы.

5. Сценарии работы пользователя

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

5.1. Работа с субъектами ПДн

Для перехода к разделу открыть вкладку «Субъекты ПДн».

В данном разделе ведется учет типов ПДн в разрезе категорий субъектов ПДн и обращений субъектов.

Для перехода к карточке категории или обращения субъектов дважды кликнуть на соответствующую запись в списке.

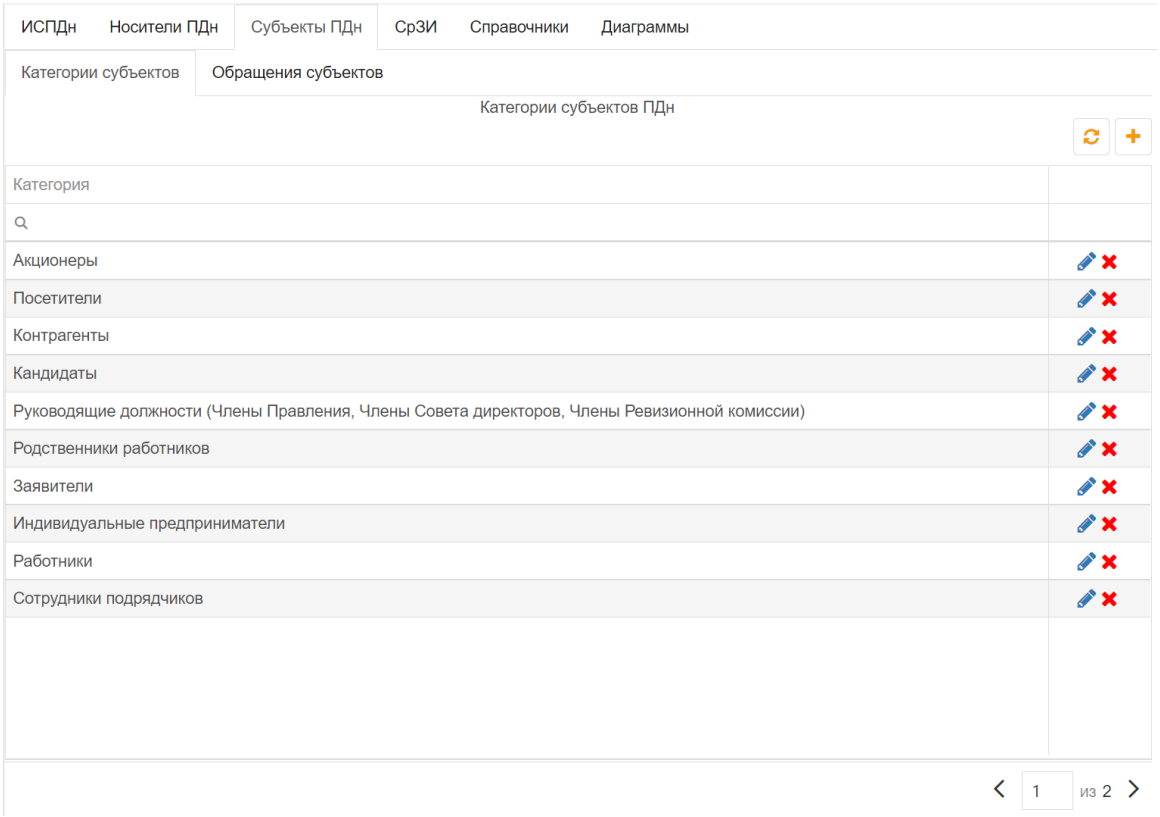

Рис. 2. Субъекты ПДн

5.1.1. Редактирование списка категорий субъектов ПДн

Для добавления категории:

1. Нажать кнопку ✚.
2. В появившейся строке ввести наименование категории.
3. Для сохранения нажать кнопку 🖫, для отмены - ↺.

Для редактирования категории:

1. В соответствующей строке нажать кнопку .
2. Отредактировать название категории.
3. Для сохранения нажать кнопку , для отмены - .

Для удаления категории:

1. В соответствующей строке нажать кнопку .
2. Для сохранения нажать кнопку , для отмены - .

5.1.2. Учет типов ПДн для категорий субъектов

1. Открыть карточку категории субъектов ПДн (Рисунок 3).

   На карточке категории субъекта ПДн отображается перечень типов ПДн, актуальный для данной категории. Для каждого типа ПДн выведено, в каких ИСПДн он обрабатывается и обрабатывается ли вручную.

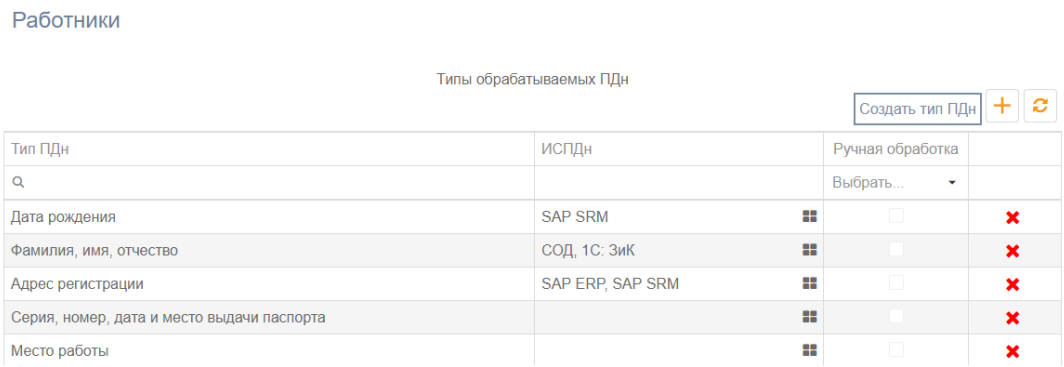

Рис. 3. Карточка категории ПДн

2. Для добавления существующего типа ПДн:
   - нажать кнопку ;
   - в открывшемся окне отметить нужные записи;

• нажать кнопку Сохранить.

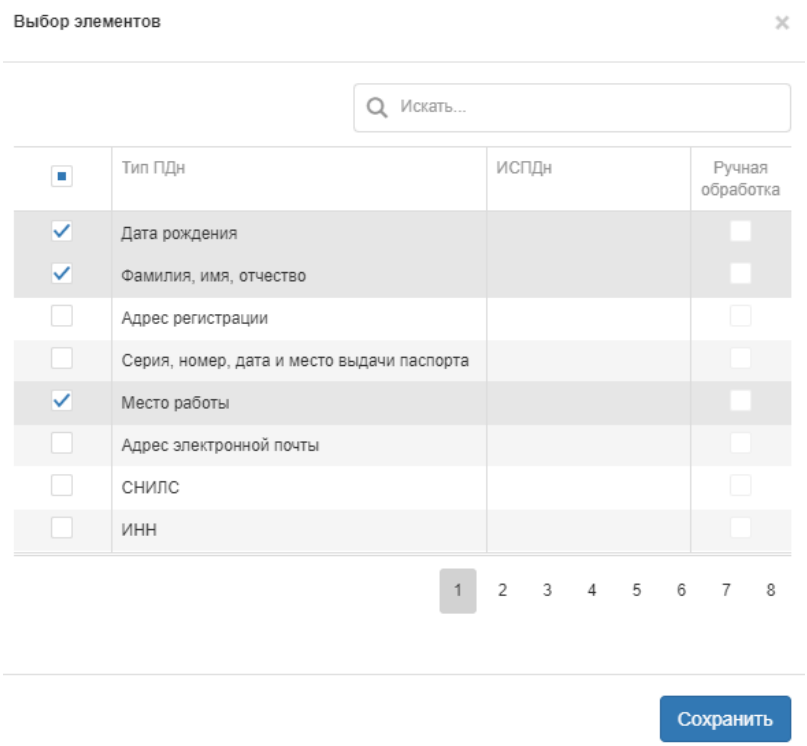

Рис. 4. Выбор типа ПДн

3. Для создания типа ПДн нажать кнопку Создать тип ПДн. Подробнее - см. Создание типа ПДн.
4. Для удаления типа ПДн в соответствующей строке нажать кнопку ✖.

5.1.2.1. Создание типа ПДн

1. Открыть карточку категории субъектов ПДн (Рисунок 3).
2. Нажать кнопку Создать тип ПДн. Откроется карточка нового типа ПДн (Рисунок 5).

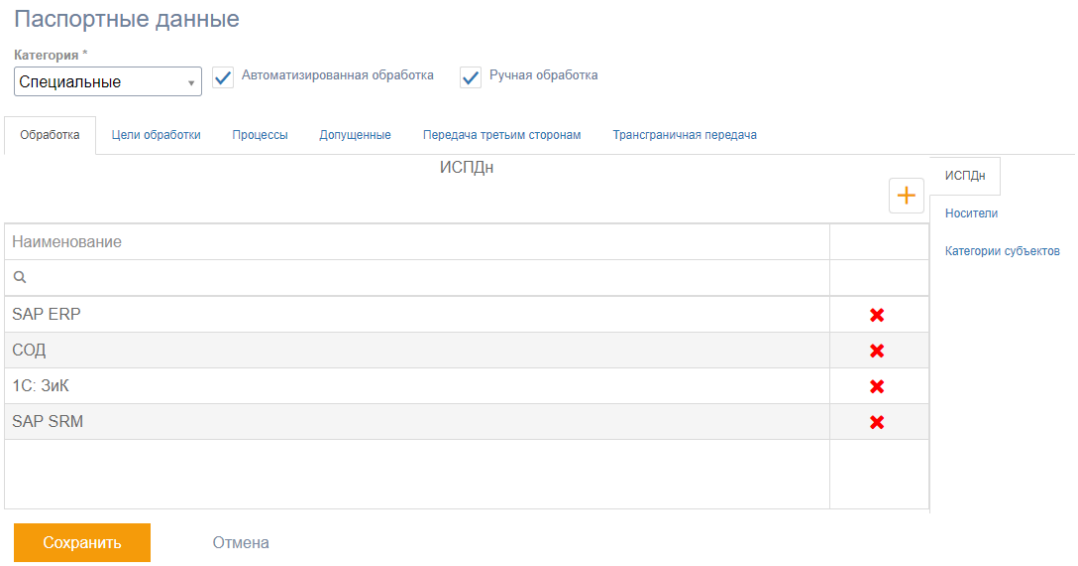

Рис. 5. Карточка типа ПДн

3. Указать категорию ПДн.

4. Выбрать типы обработки ПДн.

   По умолчанию установлен признак для автоматизированной обработки – «Да», для ручной – «Нет».
5. На вкладке «Обработка» на подвкладке «ИСПДн» добавить ИСПДн, в которых обрабатывается данный тип ПДн:
   - нажать кнопку +;
   - в открывшемся окне отметить нужные записи;
   - нажать кнопку Сохранить.

   > **Прим.:**
   >
   > Подвкладка «ИСПДн» отображается, только если для автоматизированной обработки установлен признак «Да».
6. На вкладке «Обработка» на подвкладке «Носители» добавить информационные активы и технические средства, на которых размещены ПДн данного типа:
   - нажать кнопку +;
   - в открывшемся окне отметить нужные записи;
   - нажать кнопку Сохранить.
7. На вкладке «Обработка» на подвкладке «Категории субъекта» добавить категорим субъекта ПДн, у которых обрабатывается данный тип ПДн:
   - нажать кнопку +;
   - в открывшемся окне отметить нужные записи;
   - нажать кнопку Сохранить.
8. На вкладке «Цели обработки» выбрать цели обработки данного типа ПДн:
   - нажать кнопку ▪▪ в поле «Цели обработки»;
   - в открывшемся окне отметить нужные записи;
   - нажать кнопку Сохранить.
9. На вкладке «Цели обработки» указать действия, которые осуществляются с данным типом ПДн:
   - нажать кнопку +;
   - в открывшемся окне отметить нужные записи;
   - нажать кнопку Сохранить.
10. На вкладке «Процессы» выбрать процессы обработки данного типа ПДн:
    - нажать кнопку +;
    - в открывшемся окне отметить нужные записи;
    - нажать кнопку Сохранить.
11. На вкладке «Допущенные» выбрать работников организации, допущенных к обработке данного типа ПДн.
    - нажать кнопку +;
    - в открывшемся окне отметить нужные записи;
    - нажать кнопку Сохранить.

Прим.:

Для выбора доступны только работники с допуском к ПДн.

12. На вкладке «Передача третьим сторонам» выбрать третью сторону, которой могут передаваться:
    - нажать кнопку +;
    - в новой строке выбрать из справочника третью сторону и указать канал передачи ПДн;
    - для сохранения нажать кнопку .

Прим.:

Если третья сторона отсутствует в справочнике, необходимо создать ее с помощью кнопки «Добавить третью сторону». Подробнее - см.Ведение справочников модуля.

13. На вкладке «Трансграничная передача» выбрать страны, в которые передаются ПДн данного типа.
    - нажать кнопку +;
    - в открывшемся окне отметить нужные записи;
    - нажать кнопку Сохранить.

Прим.:

Если в стране, куда передаются ПДн, не обеспечивается требуемый уровень защиты ПДн, пользователь получит соответствующее предупреждение.

14. Для сохранения карточки ПДн нажать кнопку Сохранить.

5.1.3. Учет обращений субъектов ПДн

Для перехода к разделу в списке субъектов ПДн открыть вкладку «Обращения субъектов» (Рисунок 6).

Список обращений содержит две вкладки:

- Новые - содержит обращения в статусах «Новое обращение»;
- Обработанные - содержит обращения в статусах «Выполнено» и «Отклонено».

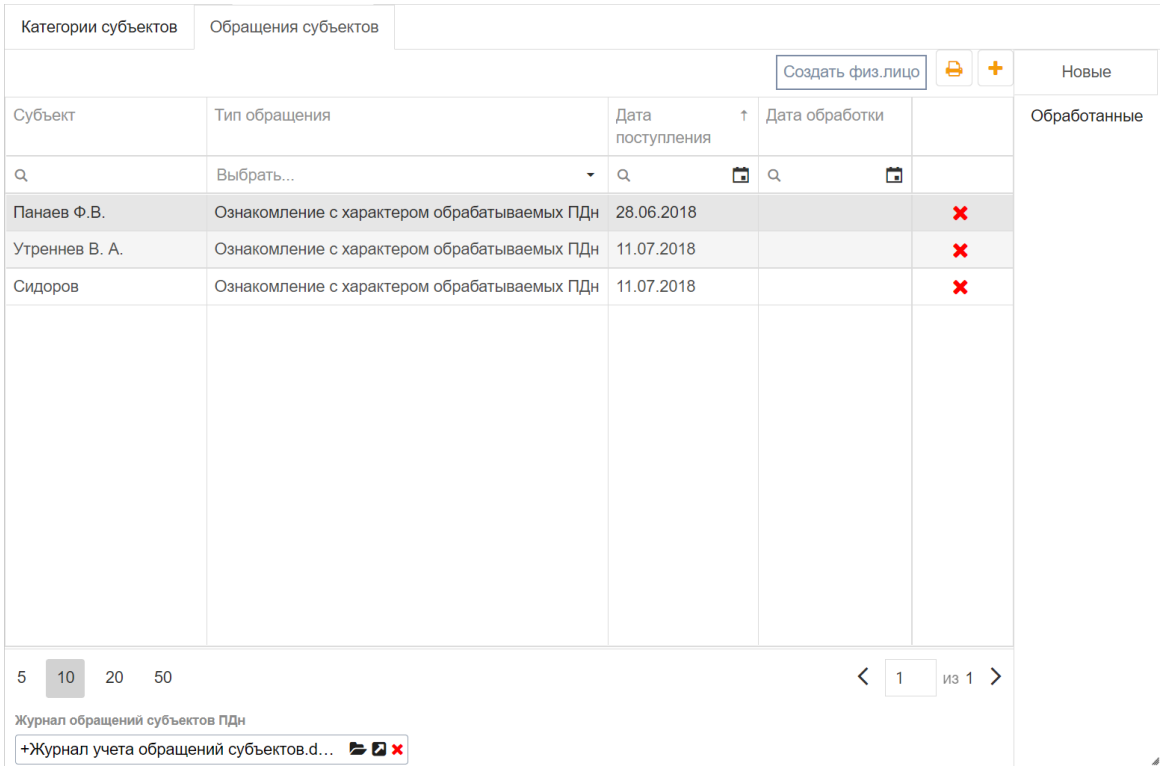

Рис. 6. Реестр обращений субъектов ПДн

5.1.3.1. Создание обращения

1. Нажать кнопку ✚ в списке обращений субъектов ПДн. Откроется карточка нового обращения.

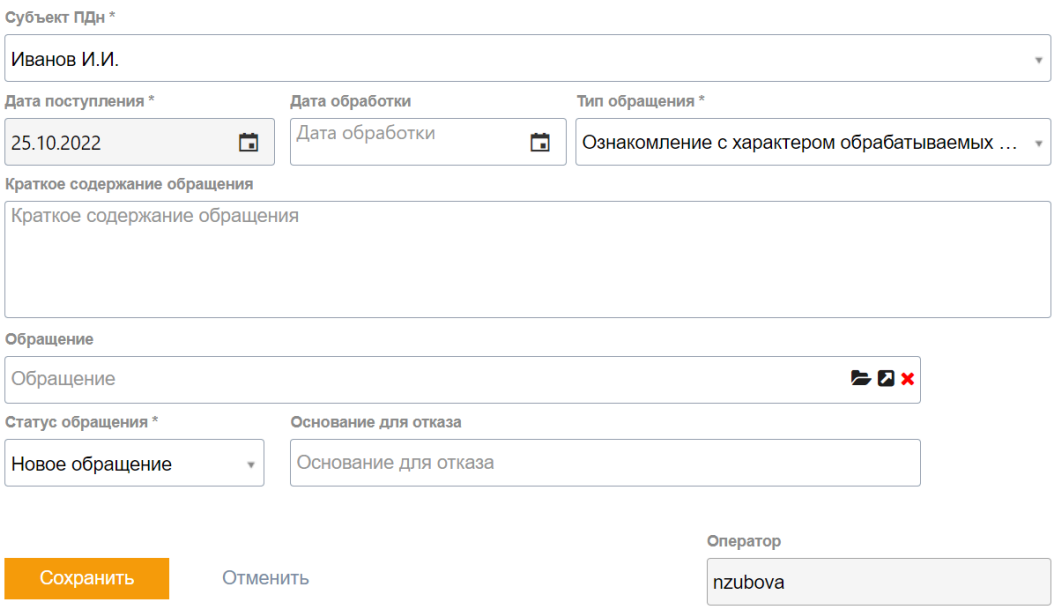

Рис. 7. Реестр обращений субъектов ПДн

2. В поле «Субъект ПДн» выбрать лицо, чье обращение обрабатывается.

Прим.:

Если субъект, чье обращение обрабатывается, не заведен в систему, необходимо его добавить - см.Создание физического лица.

3. Выбрать тип обращения.
4. Заполнить краткое содержание обращения.
5. В поле «Обращение» прикрепить вложение с помощью кнопки 🗁.
6. Поле «Дата поступления» не доступно для редактирования, по умолчанию указывается текущая дата.
7. Поле «Оператор» не доступно для редактирования, по умолчанию указывается текущий пользователь.
8. Нажать кнопку Сохранить.

5.1.3.2. Обработка обращения

1. Открыть в списке обращений субъектов ПДн нужную запись.
2. Если обращение выполнено:
   - в поле «Статус обращения» выбрать значение «Выполнено»;
   - нажать кнопку Сохранить. Карточка сохранится и автоматически закроется.
3. Если обращение отклонено:
   - в поле «Статус обращения» выбрать значение «Отклонено»;
   - заполнить поле «Основание для отказа»;
   - нажать кнопку Сохранить. Карточка сохранится и автоматически закроется.
4. После обработки обращения оно будет отображаться в реестре на вкладке «Обработанные».

5.1.3.3. Создание физического лица

1. Нажать кнопку Создать физ.лицо в списке обращений субъектов (Рисунок 6). Откроется карточка физического лица (Рисунок 8).
2. Указать ФИО физического лица.
3. Выбрать категорию субъекта;
4. На вкладке «Данные физ. лица» указать дополнительные сведения:
   - дату рождения;
   - адрес;
   - телефон;
   - электронную почту.
5. Выбрать значение в поле «Статус лица»:
   - если выбрать «Сотрудник организации», то после сохранения рядом появится ссылка на карточку работника;
   - если выбрать «Внешнее лицо» - появится ссылка на карточку третьей стороны.

6. Нажать на кнопку Согласие на обработку ПДн для формирования и скачивания печатной формы согласия на обработку ПДн.

> **Прим.:**
>
> Скан согласия в дальнейшем загрузить в поле «Согласие на обработку ПДн» с помощью кнопки 🗁.

7. Нажать кнопку Сохранить.

После сохранения поле «Статус лица» станет недоступно для редактирования.

На вкладке «Обращения» будут отображаться обращения данного субъекта.

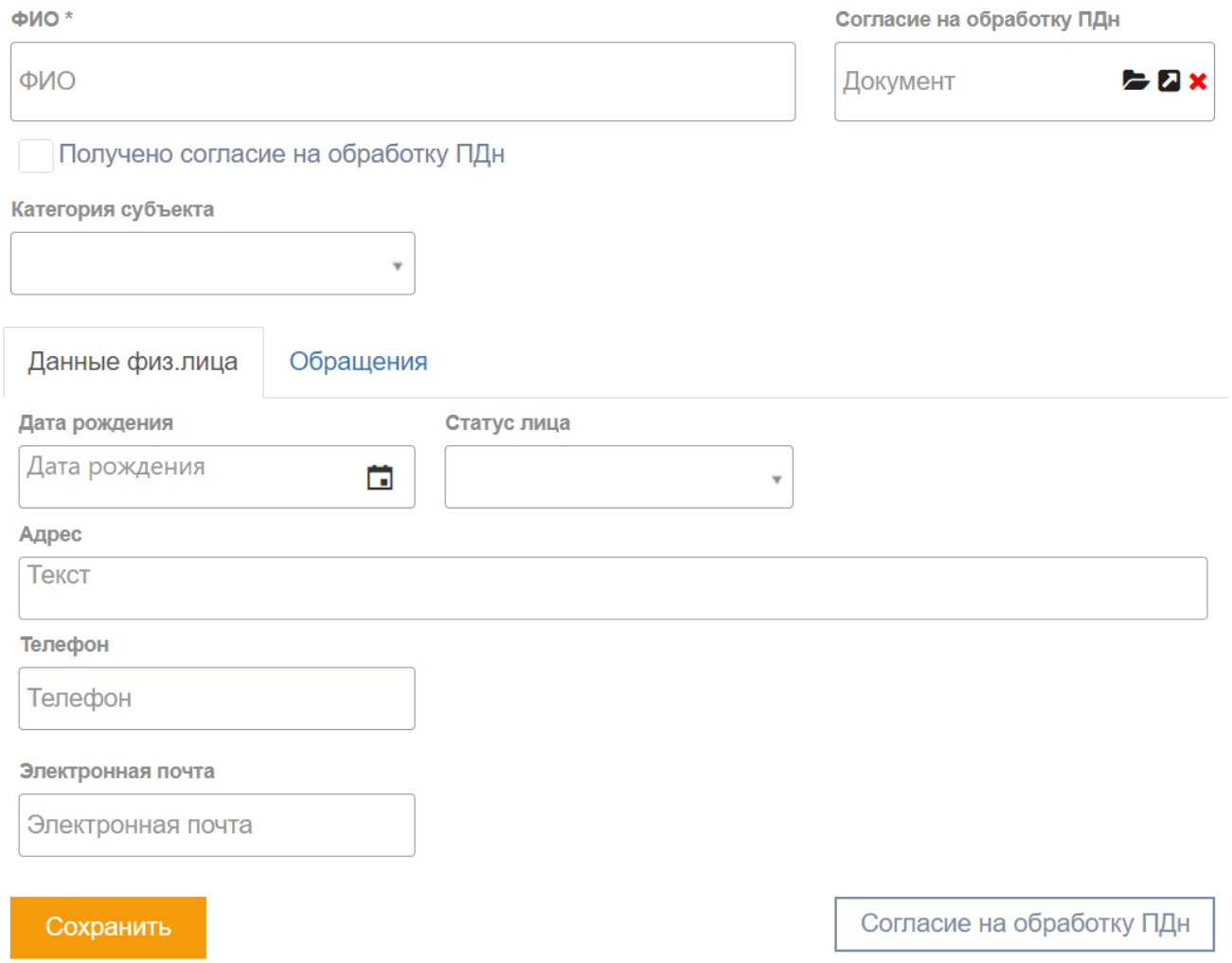

Рис. 8. Карточка физического лица

5.1.3.4. Формирование журнала учета обращений

1. Нажать кнопку () («Сформировать журнал учета обращений») над списком обращений субъектов (Рисунок 6).

   Будет сформирован документ в формате docx, ссылка на него появится в поле «Журнал обращений субъектов ПДн».
2. Для скачивания документа нажать  . Произойдет скачивание сформированного документа.

5.2. Работа с ИСПДн

Для перехода к разделу открыть вкладку «ИСПДн».

В данном разделе ведется учет ИСПДн, допущенных работников, угроз и требований по защите ИСПДн.

Список ИСПДн содержит две вкладки:

- Активные ИСПДн;
- ИСПДн в архиве.

Для перехода к карточке ИСПДн дважды кликнуть на соответствующую запись в списке.

Прим.:

Создать ИСПДн вручную нельзя, это происходит в модуле Учет и классификация объектов при утверждении ИС, являющейся ИСПДн.

Активные ИСПДн | ИСПДн в архиве

ИСПДн	Статус модели угроз	Уровень исходной защищенности	Уровень защищенности	Угрозы	Нейтрализованн...	Защитные меры	Выполненные
Тест ИСПДн	Требуется формирование	Средний	Требуется определить уровень защищенности ИСПДн	0	0	0	0
SAP BPC	Утверждена	Средний	УЗ1	30	1	82	1
SAP SRM	Утверждена	Средний	УЗ4	28	0	0	0
SAP ERP	Утверждена	Высокий	УЗ2	9	15	29	43

Рис. 9. ИСПДн

5.2.1. Просмотр и редактирование карточки ИСПДн

В верхнюю панель выведена основная информация по текущему состоянию ИСПДн. Под наименованием расположена ссылка на карточку ИС, которая является данной ИСПДн (Рисунок 10).

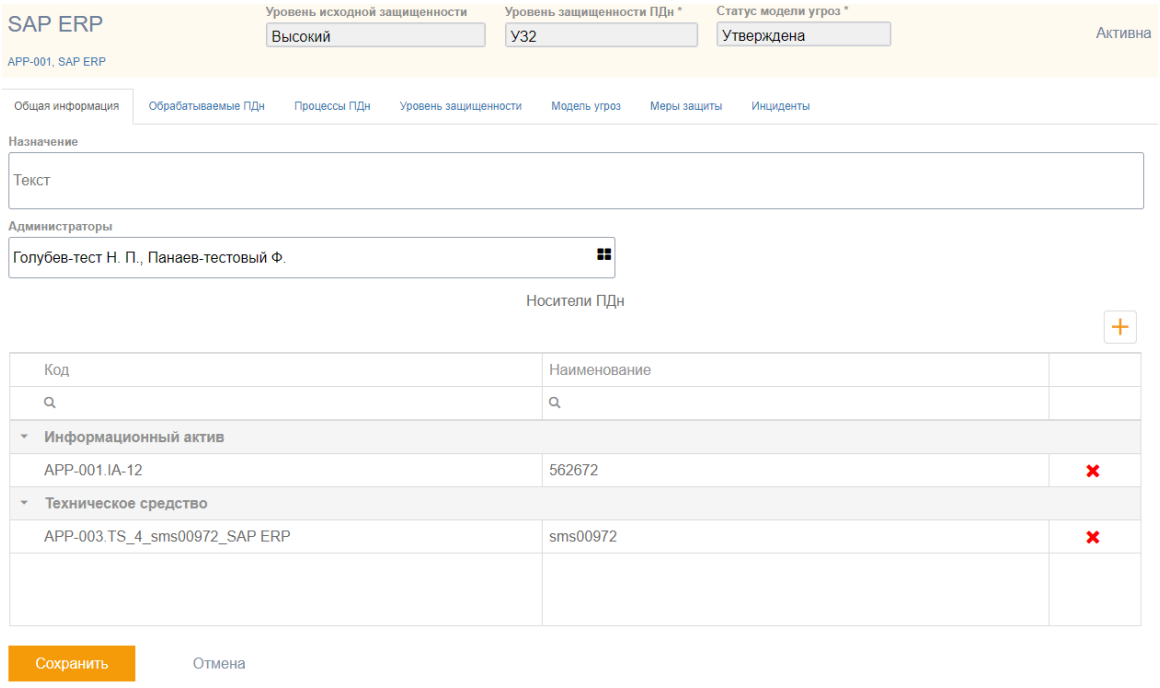

Рис. 10. Карточка ИСПДн. Общая информация

На вкладке «Общая информация» заполните назначение ИСПДн, выберите администраторов. В качестве администратора можно выбрать только работников, допущенных к обработке ПДн. Ниже расположен перечень носителей ПДн, которые учитываются в данной ИСПДн. С помощью кнопки + добавляются носители ПДн.

На вкладке «Обрабатываемые ПДн» отображается перечень типов ПДн, которые обрабатываются в данной ИСПДн. Для добавления доступны только типы ПДн с признаком «Автоматизированная обработка».

На вкладке «Процессы ПДн» отображаются процессы обработки ПДн, автоматизируемые в данной ИСПДн.

На вкладке «Инциденты» отображается перечень инцидентов, связанных с данной ИСПДн и их статус.

5.2.2. Определение уровня защищенности ПДн

Расчет уровня защищенности ПДн необходимо проводить для формирования модели угроз, актуальных для данной ИСПДн.

1. Перейдите на вкладку «Уровень защищенности», подвкладку «Уровень защищенности ПДн». (Рисунок 11)

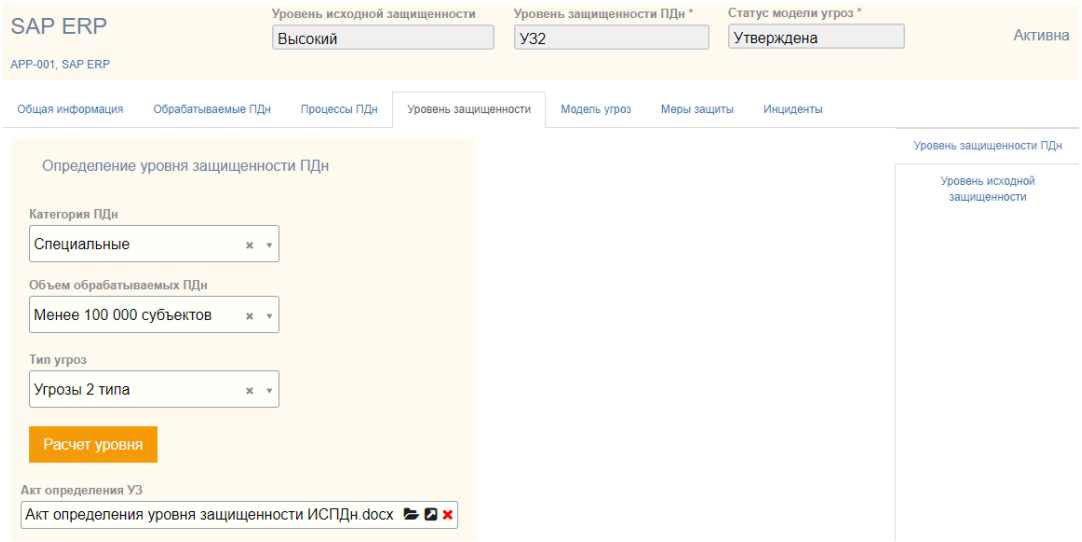

Рис. 11. Карточка ИСПДн. Определение уровня защищенности ПДн

2. Выберите категорию ПДн, которая содержится в ИСПДн.

   Выбирать необходимо категорию с максимальными требованиями по защите: самые строгие требования предъявляются, если в ИСПДн обрабатываются специальные категории ПДн, далее – биометрические, иные и наименее строгие, если обрабатываются общедоступные.
3. Выберите объем обрабатываемых ПДн (количество субъектов) и тип угроз, характерный для ИСПДн (расшифровка типов угроз приводится в приложении А).
4. Нажмите «Расчет уровня». Для данной ИСПДн будет рассчитан уровень защищенности ПДн (он будет выведен в верхнюю панель) и сформирован акт определения уровня защищенности. Акт будет автоматически загружен в поле «Акт определения УЗ». Его можно скачать с помощью значка .

5.2.3. Определение уровня исходной защищенности ИСПДн

1. Перейдите на подвкладку «Уровень исходной защищенности» (Рисунок 12).

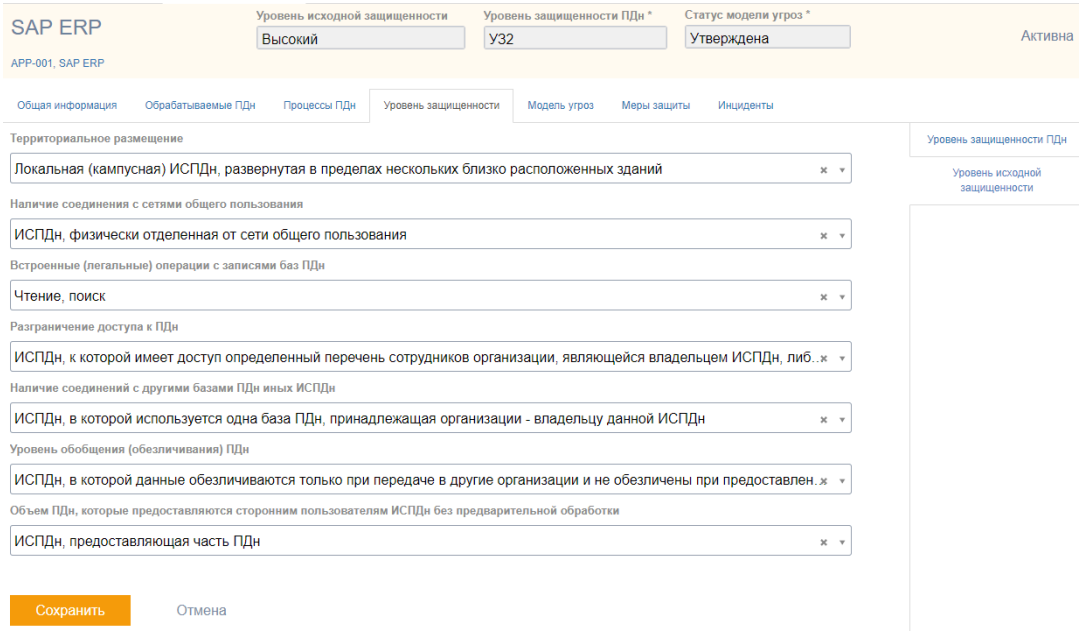

Рис. 12. Карточка ИСПДн. Определение уровня исходной защищенности ИСПДн

2. Заполните опросник и нажмите «Сохранить».

   Автоматически будет рассчитан уровень исходной защищенности (он также будет выведен в верхнюю панель) и сформирован базовый набор требований по защите ИСПДн, актуальных для данного уровня защищенности.

Если пересчитать уровень исходной защищенности, набор требований также будет изменен.

Логика расчета уровня исходной защищенности приведена в приложении Б.

5.2.4. Формирование модели угроз

1. Перейдите на вкладку «Модель угроз».
2. Нажмите кнопку «Сформировать модель».

   Сформируется перечень угроз, характерных для данной ИСПДн.

> **Важное замечание:**
>
> Для формирования модели угроз необходимо сначала определить уровень исходной защищенности ИСПДн. Если этого не сделать, кнопка «Сформировать модель» не будет отображаться, вместо нее будет выведено предупреждение о необходимости определения уровня исходной

защищенности. Когда уровень будет определен, предупреждение пропадет, а кнопка, наоборот, отобразится.

3. После формирования статус модели угроз изменится на «Оценка угроз». На этом статусе можно отредактировать перечень угроз – добавить новые или удалить неактуальные. Для удобства оценки здесь отображаются группы угроз (угрозы верхнего уровня). После утверждения модели угроз уже будут отображаться отдельные угрозы из справочника ФСТЭК.
4. Для каждой угрозы установите уровень вероятности и уровень опасности:
   - в каждой ячейке выбрать значение из выпадающего списка;
   - нажать кнопку сохранения в таблице (Рисунок 13).

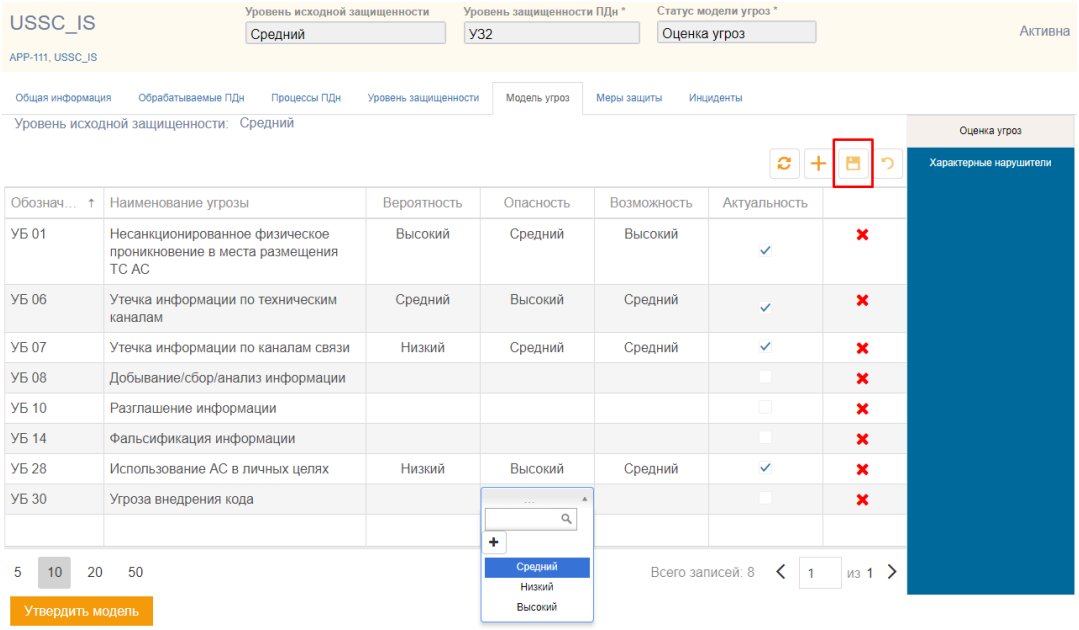

Рис. 13. Карточка ИСПДн. Модель угроз. Оценка угроз

5. После сохранения для каждой угрозы будет установлен уровень возможности реализации и признак актуальности. Логика расчета возможности реализации угрозы и актуальности представлена в приложении В.

   Кроме перечня угроз сформирован перечень характерных нарушителей, который тоже может быть отредактирован.
6. Когда все угрозы оценены, нажмите «Утвердить модель» (если остается хотя бы одна неутвержденная угроза, система выдаст ошибку). Модель угроз перейдет на статус «Утверждена».
7. На статусе «Утверждена» уже выведены угрозы из справочника ФСТЭК, для каждой угрозы выведены признаки «Актуальна» и «Нейтрализована». Угроза считается нейтрализованной при выполнении всех связанных мер защиты (см. раздел «Выполнение требований по защите»).
8. При необходимости внесения изменений в модель угроз, нажмите кнопку «Изменить модель». Модель угроз перейдет на статус «Корректировка» и перечень угроз станет доступен для редактирования. После редактирования снова нажмите «Утвердить модель».
9. Двойной щелчок по наименованию угрозы открывает карточку угрозы (Рисунок 14).

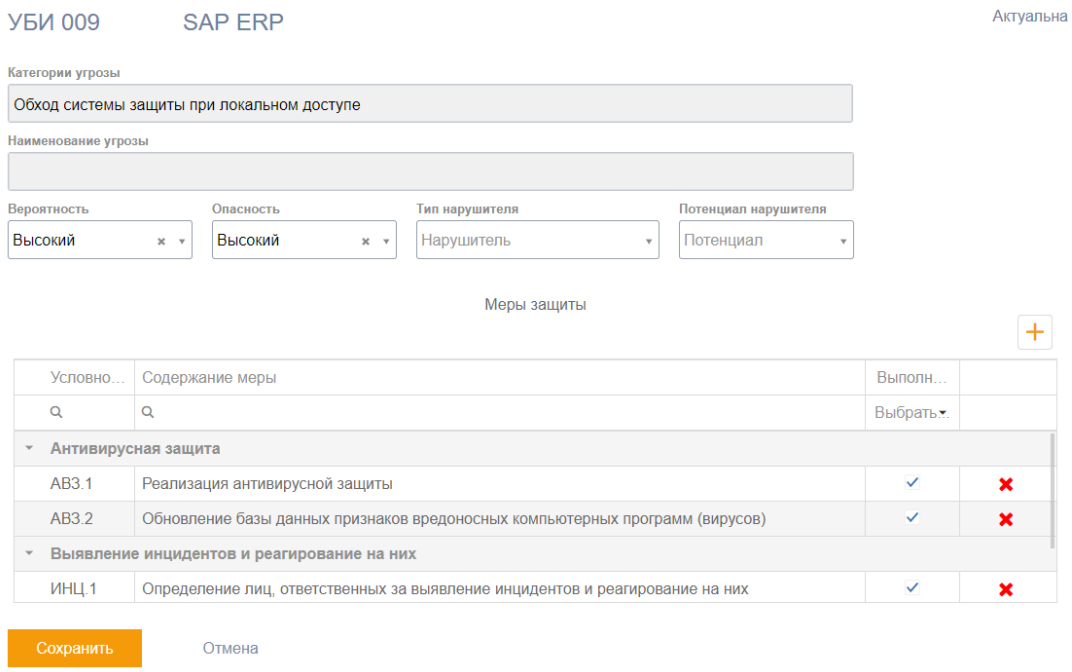

Рис. 14. Карточка угрозы

10. На карточке выберите тип и потенциал нарушителя.

    Выбрать меры защиты для нейтрализации угрозы можно только после формирования общего (уточненного) мер защиты (см. раздел «Выполнение требований по защите»). Когда после каждого сохранения карточки угрозы происходит проверка выполнения связанных защитных мер. Если у всех защитных мер стоит признак «Выполнена», угроза переходит в статус «Нейтрализована». Если хотя бы одна мера не выполнена, угроза является актуальной (статус отображается в правом верхнем углу карточки).

Двойной щелчок по наименованию защитной меры открывает ее карточку.

5.2.5. Выполнение требований по защите

1. Перейдите на вкладку «Меры защиты». На подвкладке СрЗИ отображаются все СрЗИ, связанные с данной ИСПДн (используемые во всех мерах защиты). На подвкладке «Базовый набор» - базовый набор требований, сформированный на основе уровня защищенности (см. раздел «Определение уровня защищенности ПДн»), на подвкладке «Адаптированный набор» - набор требований, сформированный на основе модели угроз. На вкладке «Общий набор требований» - объединение базового и адаптированного набора. Для формирования общего набора нажмите кнопку «Сформировать требования» (Рисунок 15).

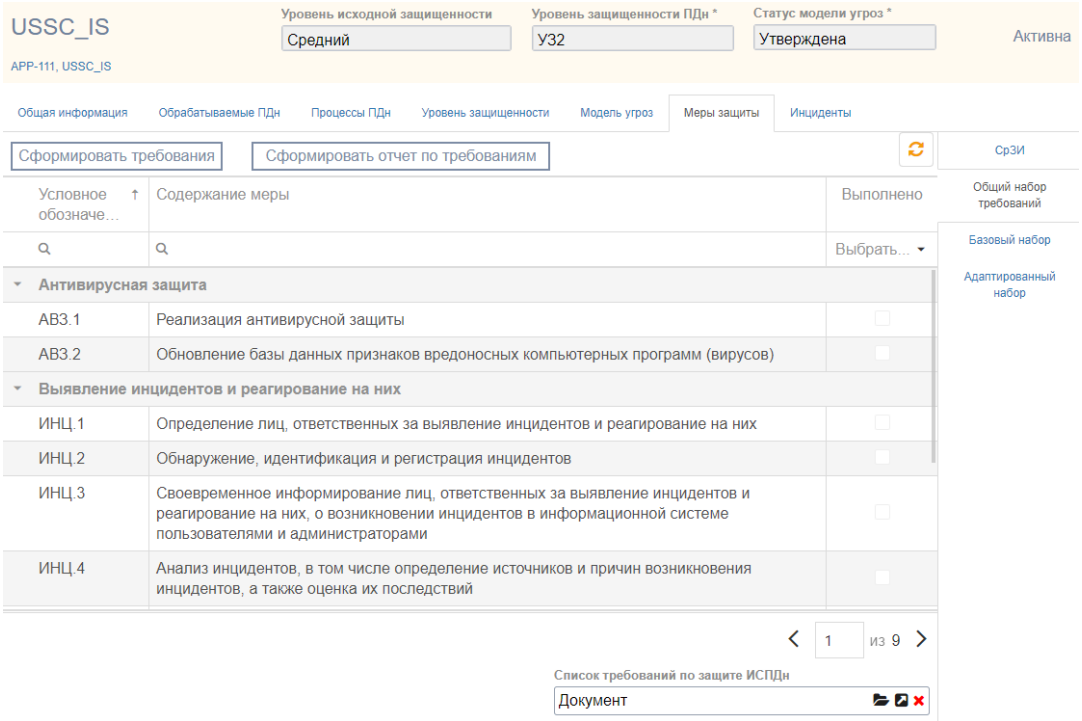

Рис. 15. Карточка ИСПДн. Меры защиты. Общий набор требований

2. Зайдите на карточку требования по защите (защитной меры) с помощью двойного щелчка левой кнопкой мыши по наименованию (Рисунок 16).

   В верхней панели отображается код защитной меры, наименование ИСПДн, к которой относится требование и комментарии по выполнению.

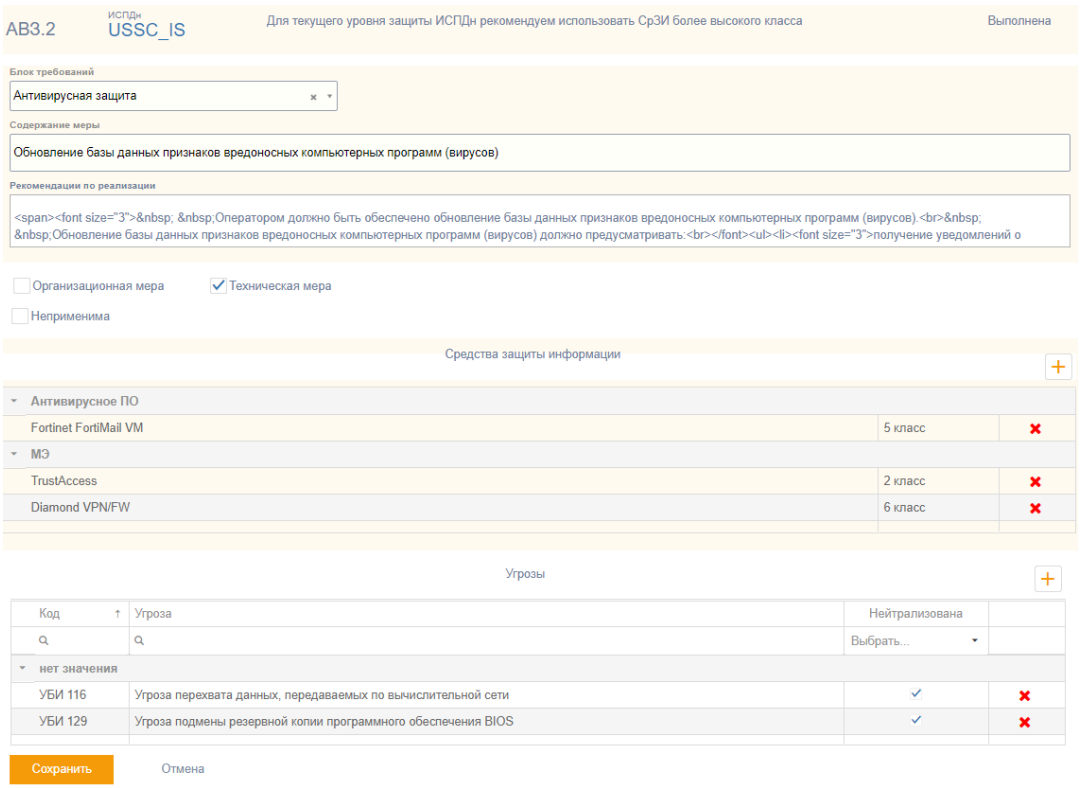

Рис. 16. Карточка требования по защите

3. Внизу карточки выберите перечень угроз, которые должна нейтрализовать текущая защитная мера.

4. Для выполнения требования необходимо определить, является защитная мера организационной или технической, а также, применима ли она в текущих условиях (возможна ли ее реализация и целесообразна ли она экономически). Признак организационной или технической меры по умолчанию уже заполнен из справочника ФСТЭК, но при необходимости эти значения можно изменить.
5. В зависимости от выбранного признака – организационная или техническая мера – отображаются соответствующие поля для заполнения. Если выбран признак «Техническая мера», необходимо выбрать СрЗИ, которые используются для защиты ИСПДн. Если «Организационная» - необходимо вручную описать действия по реализации. Если и организационная, и техническая – нужно указать хотя бы СрЗИ.
6. Если мера неприменима в текущей ситуации, необходимо выбрать признак «Неприменима». В этом случае, вне зависимости от того, организационная мера или техническая, необходимо выбрать компенсирующую меру. Компенсирующую меру можно выбрать из существующих, или сначала создать. Для этого нажмите кнопку «Создать».
7. Когда заполнены данные по выполнению защитной меры, сохраните карточку. В верхнем правом углу появится отметка «Выполнена».
8. В случае технической меры, следует учитывать класс СрЗИ. Необходимо выбирать СрЗИ класса, соответствующего требуемому уровню защищенности ПДн. Если выбрано СрЗИ недостаточно высокого класса, мера будет выполнена, но в верхней панели отобразится рекомендация использовать СрЗИ более высокого класса. Соответствие классов СрЗИ и уровней защищенности ПДн приведено в приложении Г.
9. Автоматически произойдет проверка связанных угроз: если выполнены все защитные меры (на нейтрализацию угрозы может быть направлено несколько защитных мер), угрозе присваивается признак «Нейтрализована». Если отредактировать защитную меру и она перестанет выполняться, признак «Нейтрализована» у угрозы будет снят.
10. Вернитесь в карточку ИСПДн. Над перечнем по защите ИСПДн нажмите кнопку «Сформировать отчет по требованиям». Будет сформирована печатная форма отчета, содержащего полный список всех требований по защите. Файл отчета будет сохранен в поле «Список требований по защите ИСПДн» (см. Рисунок 15). Его можно скачать, нажав на значок ↗.

5.3. Учет носителей ПДн

Для перехода к разделу открыть вкладку «ИСПДн».

В данном разделе отображается реестр носителей ПДн, сгруппированный по типам (Рисунок 17). Носителем ПДн является информационный актив с типом «Персональные данные» и технические средства, на которых размещены такие активы.

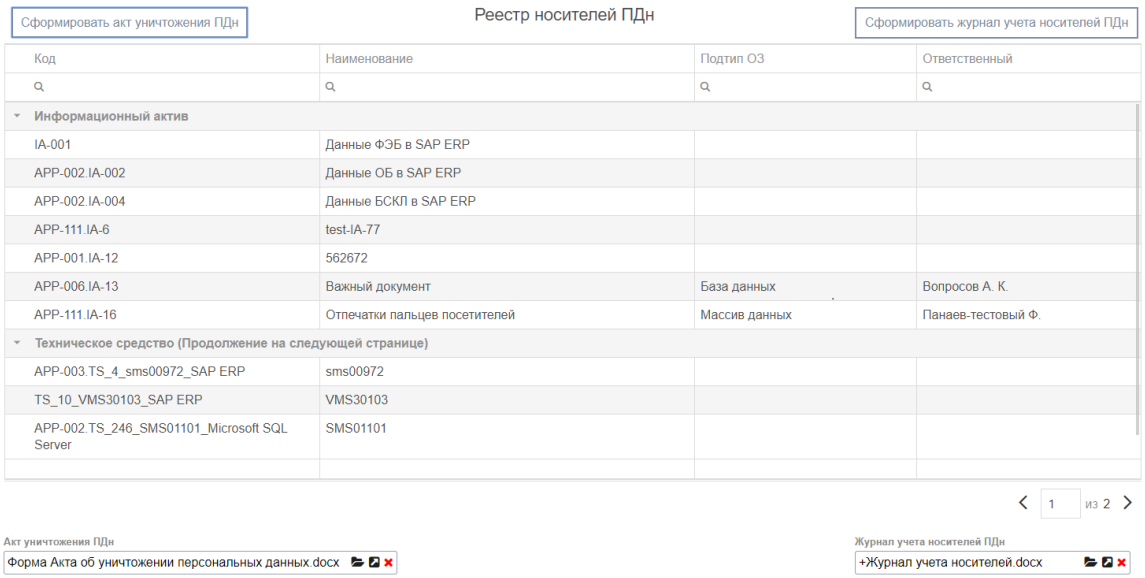

Рис. 17. Реестр носителей ПДн

Для перехода к карточке носителя ПДн дважды кликнуть на соответствующую запись в списке.

5.3.1. Просмотр и редактирование карточки носителя ПДн

В верхней панели отображается наименование носителя и его тип. Под наименованием расположена ссылка на карточку объекта защиты, который является носителем.

Если нажать на кнопку «Удалить ПДн», будет установлена текущая дата удаления ПДн с носителя и носителю будет присвоен признак «Данные удалены». Носители, на которых удалены ПДн и ИСПДн, в которых они учитываются, попадут в печатную форму акта уничтожения ПДн.

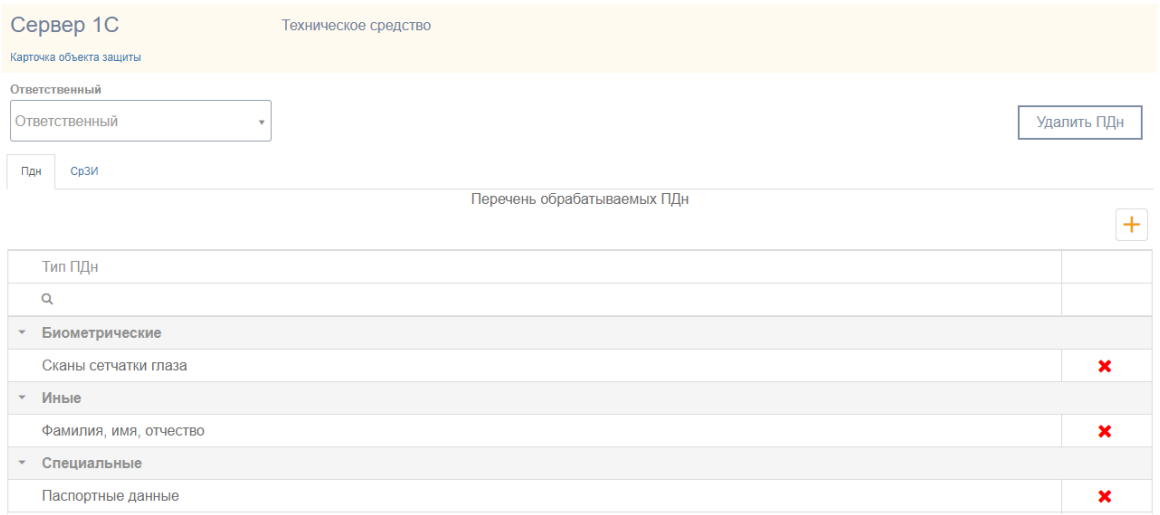

Рис. 18. Карточка носителя ПДн

На вкладке «ПДн» отображаются типы ПДн, которые хранятся на данном носителе. На вкладке «СрЗИ» - средства защиты информации, которые с ним связаны.

Для добавления типов ПДн или СрЗИ:

- нажать кнопку +;
- в открывшемся окне отметить нужные записи;
- нажать кнопку Сохранить.

5.3.2. Формирование журнала и акта

Для формирования журнала учета носителей ПДн

1. Нажмите кнопку «Сформировать журнал учета носителей ПДн» над списком носителей ПДн (Рисунок 17).

   Будет сформирован документ в формате docx, ссылка на него появится в поле «Журнал учета носителей ПДн».
2. Для скачивания документа нажать . Произойдет скачивание сформированного документа.

Для формирования акта уничтожения ПДн:

1. Нажмите кнопку «Сформировать акт уничтожения ПДн».

   Сформируется печатная форма журнала акта уничтожения ПДн на носителях и в ИСПДн. Ссылка на него появится в поле «Акт уничтожения ПДн» (см. Рисунок 17).
2. Для скачивания документа нажать . Произойдет скачивание сформированного документа.

5.4. Учет СрЗИ

Для перехода к разделу открыть вкладку «СрЗИ».

В данном разделе отображается перечень всех СрЗИ, сгруппированный по их типам. У каждого СрЗИ отображается класс и требования, которые оно закрывает.

Для перехода к карточке носителя СрЗИ дважды кликнуть на соответствующую запись в списке.

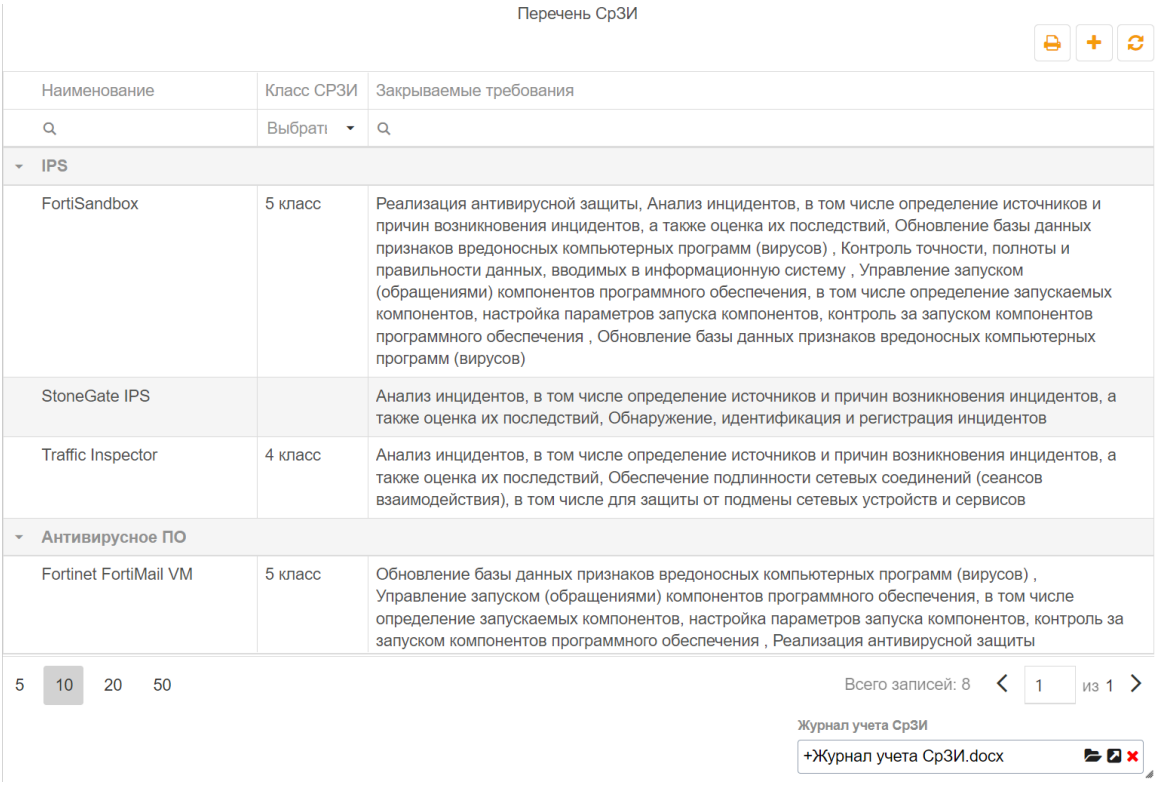

Рис. 19. Реестр СрЗИ

5.4.1. Создание СрЗИ

1. Нажмите кнопку ✚ в реестре СрЗИ (Рисунок 19). Откроется карточка создания СрЗИ (Рисунок 20).

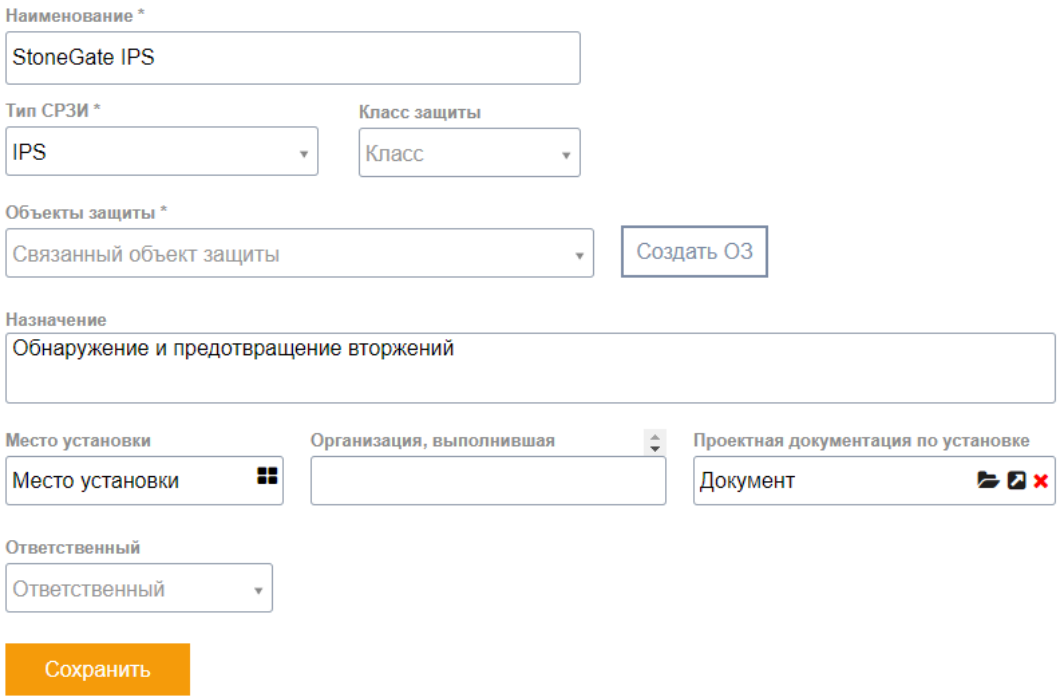

Рис. 20. Карточка создания СрЗИ

2. Укажите наименование и тип СрЗИ. Желательно указать класс защиты, который оно обеспечивает.

Выберите связанный объект защиты (техническое средство или программное обеспечение). Если нужный объект защиты еще не создан, нажмите кнопку «Создать ОЗ». Во всплывающем окне (Рисунок 21) укажите наименование и тип объекта защиты.

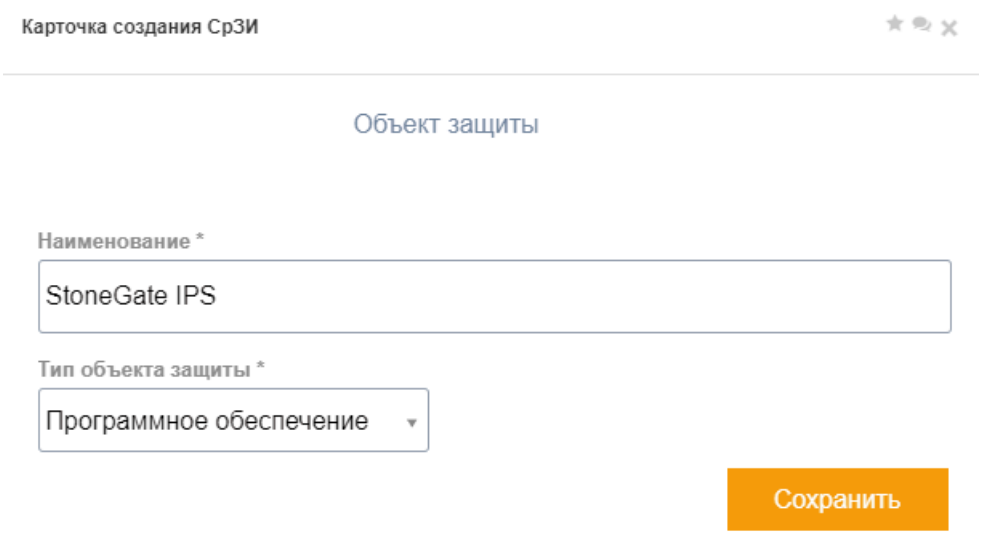

Рис. 21. Создание объекта защиты

3. Сохраните и закройте карточку объекта защиты, после этого выберите созданный объект защиты в поле «Объекты защиты».

4. Заполните остальные поля, сохраните и закройте карточку. Новое СрЗИ добавлено в реестр.

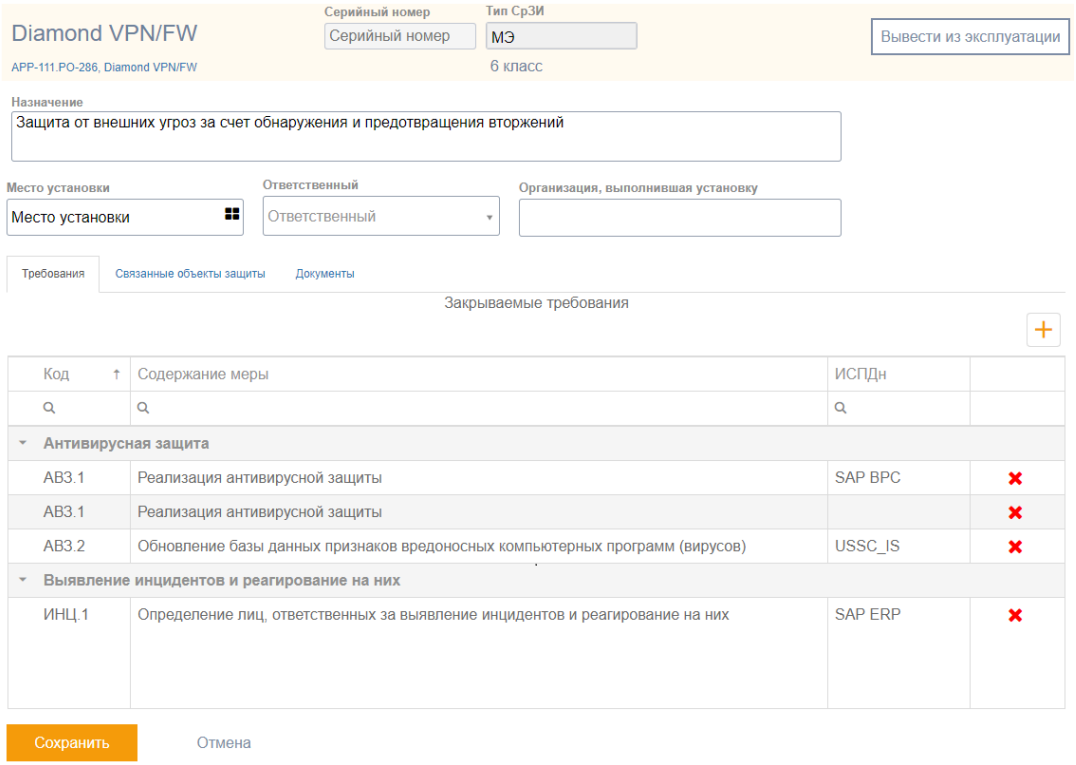

Рис. 22. Карточка СрЗИ

В верхней панели выведена основная информация по СрЗИ. Под наименованием расположена ссылка на карточку объекта защиты (ПО или ТС), которым является СрЗИ.

По кнопке «Вывести из эксплуатации» запускается процесс вывода СрЗИ из эксплуатации. Если СрЗИ используется для выполнения требований по защите, требования перестанут быть выполненными, соответственно, угрозы перестанут быть нейтрализованными. Предупреждение об этом будет выведено при нажатии на кнопку. Вернуть в эксплуатацию выведенное СрЗИ уже невозможно. В поле «Дата вывода из эксплуатации» автоматически подтянется текущая дата. Информация о выводе СрЗИ из эксплуатации попадет в журнал учета СрЗИ.

На вкладке «Требования» отображается перечень требований, для выполнения которых используется данное СрЗИ. Требования сгруппированы по типам и для каждого указано, к какой ИСПДн оно относится. Двойной щелчок по наименованию открывает карточку требования (см. Рисунок 16).

На вкладке «Связанные объекты защиты» находятся ОЗ, для защиты которых используется данное СрЗИ.

На вкладке «Документы» отображается перечень документов, связанных к СрЗИ. Для каждого документа можно приложить вложение (прямо в таблицу с помощью значка 🗁). Документы попадут в печатную форму журнала учета СрЗИ.

5.4.2. Формирование журнала учета СрЗИ

1. Нажмите кнопку «Сформировать журнал учета СрЗИ» (Рисунок 19).

   Будет сформирован документ в формате docx, ссылка на него появится в поле «Журнал учета СрЗИ».
2. Для скачивания документа нажать . Произойдет скачивание сформированного документа.

5.5. Ведение справочников модуля

Перейдите на вкладку «Справочники». В данном разделе происходит актуализация данных, которые используются в описанных выше направлениях работы: типы ПДн, процессы обработки ПДн, третьи стороны и т.д. (Рисунок 23).

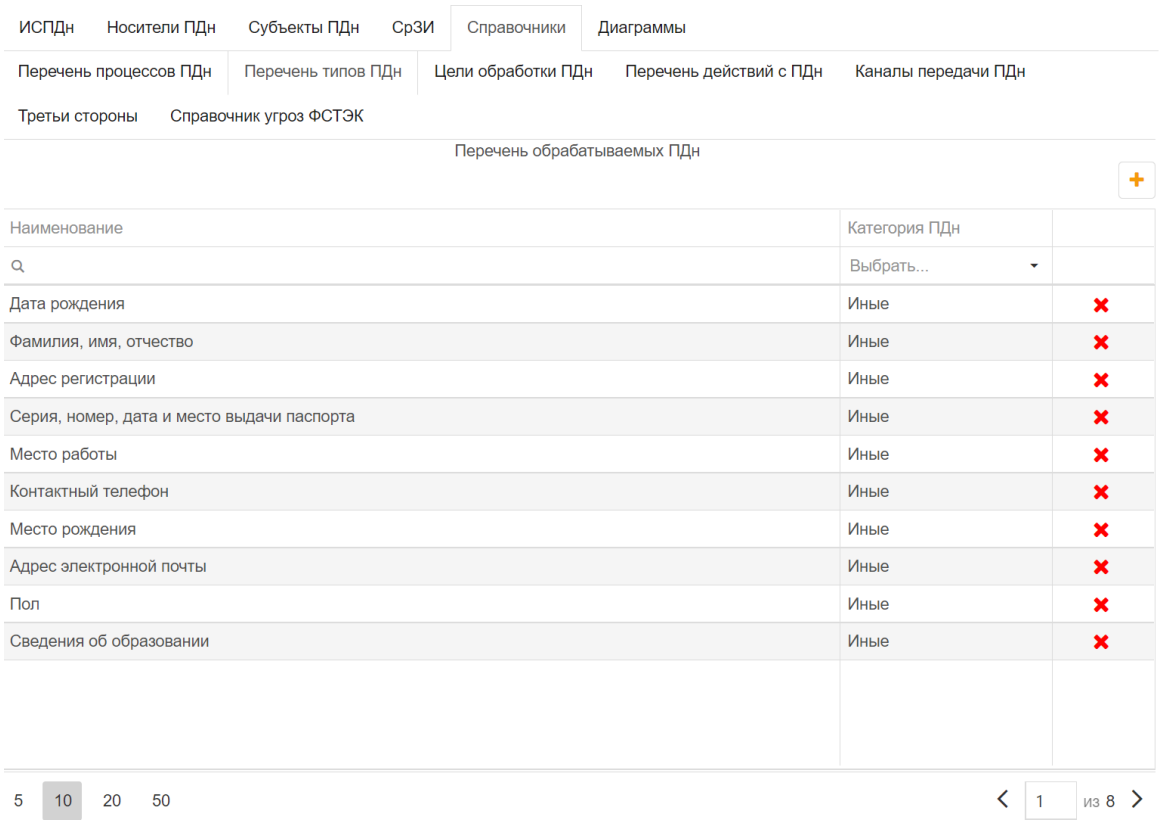

Рис. 23. Справочники

Для целей обработки ПДн, действий с ПДн, каналов передачи и угроз ФСТЭК нет карточек. Иными словами, справочник представляет собой только список, который можно редактировать.

Для процессов и типов ПДн, третьих сторон и требований по защите есть карточки, где можно редактировать данные. Открытие карточки осуществляется с помощью двойного щелчка по записи.

6. Приложения

Приложение А. Определение уровня защищенности ПДн

Согласно Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», уровень защищенности ПДн определяется на основе четырех основных характеристик ИСПДн:

- тип ИСПДн в зависимости от состава обрабатываемых ПДн (описание возможных типов ИСПДн приведено в Таблица 1);

Табл. 1. Описание типов ИСПДн в зависимости от состава обрабатываемых ПДн

Тип ИСПДн	Категория обрабатываемых ПДн	Описание категории обрабатываемых ПДн
ИСПДн-С	В ИСПДн обрабатываются специальные категории ПДн	Данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни
ИСПДн-Б	В ИСПДн обрабатываются биометрические ПДн и не обрабатываются специальные категории ПДн	Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта
ИСПДн-И	В ИСПДн обрабатываются иные категории ПДн	ПДн, не относящиеся к специальным категориям ПДн, не являющиеся биометрическими или общедоступными
ИСПДн-О	В ИСПДн обрабатываются общедоступные ПДн	ПДн, полученные только из общедоступных источников ПДн, созданных в соответствии со статьей 8 Федерального закона «О персональных данных» от 27.07.2006 N 152-ФЗ

- категория субъектов ПДн (только данные работников оператора ПДн или данные иных лиц, не являющихся работниками оператора);
- количество субъектов ПДн, данные которых обрабатываются в ИСПДн (более или менее 100 000 субъектов ПДн);
- актуальный тип угроз безопасности ПДн:
    - 1-ый тип, если для ИСПДн актуальны угрозы, связанные с наличием НДВ в **системном** ПО;
    - 2-ой тип, если для ИСПДн актуальны угрозы, связанные с наличием НДВ в **прикладном** ПО;
    - 3-ий тип, если для ИСПДн не актуальны угрозы, связанные с наличием НДВ.

Соответствие характеристик ИСПДн и уровней защищенности ПДн представлено в Таблица 2.

Табл. 2. Соответствие характеристик ИСПДн и уровней защищенности ПДн

Тип ИСПДн	Категория субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип	2 тип	3 тип
ИСПДн-С	Не работников	Более 100 000	УЗ1	УЗ1	УЗ2
		Менее 100 000	УЗ1	УЗ2	УЗ3
	Работников	Более 100 000	УЗ1	УЗ2	УЗ3
		Менее 100 000	УЗ1	УЗ2	УЗ3
ИСПДн-Б	Не работников	Более 100 000	УЗ1	УЗ2	УЗ3
		Менее 100 000	УЗ1	УЗ2	УЗ3
	Работников	Более 100 000	УЗ1	УЗ2	УЗ3
		Менее 100 000	УЗ1	УЗ2	УЗ3
ИСПДн-И	Не работников	Более 100 000	УЗ1	УЗ2	УЗ3
		Менее 100 000	УЗ1	УЗ3	УЗ4
	Работников	Более 100 000	УЗ1	УЗ3	УЗ4
		Менее 100 000	УЗ1	УЗ3	УЗ4
ИСПДн-О	Не работников	Более 100 000	УЗ2	УЗ2	УЗ4
		Менее 100 000	УЗ2	УЗ3	УЗ4
	Работников	Более 100 000	УЗ2	УЗ3	УЗ4
		Менее 100 000	УЗ2	УЗ3	УЗ4

Приложение Б. Определение исходной защищенности ИСПДн

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в Таблица 3.

Табл. 3. Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
Распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом	–	–	+

Табл. 3. Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	**Средний**	**Низкий**
Городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка)	–	–	+
Корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации	–	+	–
Локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий	–	+	–
Локальная ИСПДн, развернутая в пределах одного здания	+	–	–
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования	–	–	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования	–	+	–
ИСПДн, физически отделенная от сети общего пользования	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных			
Чтение, поиск	+	–	–
Запись, удаление, сортировка	–	+	–
Модификация, передача	–	–	+
4.По разграничению доступа к персональным данным			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	+	–
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	+
ИСПДн с открытым доступом	–	–	+
5. По наличию соединений с другими базами ПДн иных ИСПДн			
Интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн)	–	–	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	–	–
6. По уровню обобщения (обезличивания) ПДн:			

Табл. 3. Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	**Средний**	**Низкий**
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	–	–
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	–	–	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю базу данных с ПДн;	–	–	+
ИСПДн, предоставляющая часть ПДн;	–	+	–
ИСПДн, не предоставляющая никакой информации.	+	–	–