IRADD

Privacy-SPS

v.2.0.2.0

ФУНКЦИОНАЛЬНАЯ СПЕЦИФИКАЦИЯ

020314-2.0.2.0-35

2018 г.

Аннотация

Настоящий документ содержит описание функций, назначения, условий использования системы поддержки процессов обработки и защиты ПДн «Privacy-SPS» (далее СПП ПДн).

В процессе использования комплекса решаются следующие задачи:

- учет состава и структуры ИСПДн, процессов обработки и защиты ПДн;
- учет и формирование требований к процессам обработки и защиты ПДн;
- реализация (поддержка реализации) требований к процессам обработки и защиты ПДн;
- контроль соответствия процессов обработки и защиты ПДн нормативным требованиям;
- сигнализация о необходимости внесения изменений в процессы обработки и защиты ПДн.

Содержание

Перечень сокращений 2

1. Введение 3

1.1. Цели использования 3

1.2. Состав программного комплекса 3

1.3. Порядок использования 3

2. Описание комплекса 6

2.1. Функции комплекса 6

2.2. Генерируемые документы 16

2.3. Внешние интерфейсы 17

3. Нормативные документы 19

Перечень сокращений

АРМ	Автоматизированное рабочее место
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные
ПО	Программное обеспечение
СЗПДн	Система защиты персональных данных
СКЗИ	Средство криптографической защиты информации
СПП ПДн	Система поддержки процессов обработки и защиты ПДн

1. Введение

1.1. Цели использования

Целью использования программного комплекса является:

- Выполнение требований закона «О персональных данных» в части управления безопасностью процессов обработки ПДн.
- Автоматизация рутинных операций связанных с обработкой и обеспечением безопасности ПДн.
- Организация мониторинга изменений процессов обработки ПДн.

1.2. Состав программного комплекса

Программный комплекс «Privacy-SPS» является дополнительным модулем к системе «LIS-SPS».

Программный комплекс включает следующие компоненты:

- Сервер баз данных;
- Сервер приложений;
- Коннектор сервер;
- АРМ оператора.

Сервер баз данных осуществляет хранение данных используемых в СПП ПДн.

Сервер приложений представляет собой сервер IIS осуществляющий взаимодействие с пользователями.

Коннектор сервер представляет собой серверный процесс, опрашивающий внешние базы данных с заданной периодичностью, и производящий загрузку данных из этих баз в собственную базу данных «Privacy-SPS».

АРМ оператора представляет собой Web браузер, используемый на АРМ пользователей и администраторов системы.

1.3. Порядок использования

Работа в СПП ПДн осуществляется в следующем общем алгоритме:

1. Ввод данных в СПП ПДн пользователями, либо загрузка данных из внешних систем.
2. Автоматический анализ введенных данных, определение несоответствий в процессах обработки и защиты ПДн.
3. Генерация необходимых документов в автоматизированном режиме, выполнение других действий по приведению процессов в соответствие.
4. Ввод данных об изменениях в процессах, системах – повтор шагов 1-3.

Система позволяет:

- Вести работу с субъектами ПДн, генерировать необходимые уведомления, формы, разъяснения субъектам ПДн, контролировать сроки отправки документов.
- Обеспечить автоматизированный ввод данных о структуре и составе процессов обработки ПДн из разных подразделений в четко определенном формате.
- Обеспечить автоматическую загрузку и анализ данных из внешних источников – кадровых баз данных, систем учета данных по субъектам ПДн, систем инвентаризации технических средств информационных систем, CRM и IDM систем
- Обеспечить автоматизированную генерацию необходимых документов (актов, приказов, журналов учета, моделей угроз, описаний и т.п.) по введенным данным.
- Контролировать корректность введенных данных, необходимость обновления выпущенных документов, проверять необходимость уничтожения ПДн.

АРМ оператора, как правило, используется на рабочих местах ответственных:

- в пользовательских структурных подразделениях, участвующих в процессах обработки и защиты ПДн,
- в ИТ подразделениях,
- в подразделениях ответственных за защиту ПДн.

Внедрение программного комплекса предполагает разные сценарии использования. Например, возможен следующий режим работы при выполнении требований в области ПДн:

- На АРМ пользовательских подразделений, в случае изменения процессов обработки ПДн, либо в случае появления новых активов, процессов, носителей ПДн осуществляется ввод учетных данных в СПП ПДн.
- На АРМ ИТ отделов осуществляется ввод данных о составе серверов, сетевого оборудования, баз данных, архитектуре ИСПДн.
- На АРМ ИТ отделов осуществляется генерация документации по ПДн находящейся в области ответственности ИТ, например, журналов учета средств защиты, заключений о проверке эффективности и т.п.
- На АРМ отделов осуществляющих работу с субъектами ПДн, по введенным данным о процессах обработки ПДн, осуществляется генерация согласий, уведомлений, разъяснений и т.п.
- На АРМ отделов ответственных за защиту ПДн, по введенным данным, осуществляется генерация документов в области защиты ПДн – моделей угроз, актов определения уровня защищенности ИСПДн и т.п.

- На АРМ ответственного за организацию обработки ПДн осуществляется анализ введенных данных, выявление несоответствий, выдача корректирующих действий.

Система поддержки процессов защиты и обработки персональных данных «Privacy-SPS» имеет следующие основные показатели:

- включает более 200 функций по контролю процессов обработки и защиты ПДн, вводу данных и генерации документов,
- позволяет осуществить автоматизированную генерацию порядка 15 видов документов,
- позволяет произвести порядка 40 видов проверок процессов на соответствие требованиям в области ПДн.

Система позволяет эффективно организовать поддержку процессов обработки и защиты ПДн как собственными силами, так и в случае выделения некоторых функций для аутсорсинга. В последнем случае заказчик дает удаленный доступ к СПП ПДн аутсорсеру, который может осуществлять выполнения возложенных на него задач (например, генерацию модели угроз, варианта системы защиты и т.п.) удаленно.

2. Описание комплекса

2.1. Функции комплекса

СПП ПДн обеспечивает реализацию следующих основных функций:

1. **Управление процессами обработки ПДн, включая:**

1.1. учет технологических процессов обработки ПДн, включая процессы взаимодействия с контрагентами, а также иерархии процессов,

1.2. учет нормативных, договорных и других оснований для обработки ПДн, необходимости получения согласий субъектов ПДн по каждому основанию,

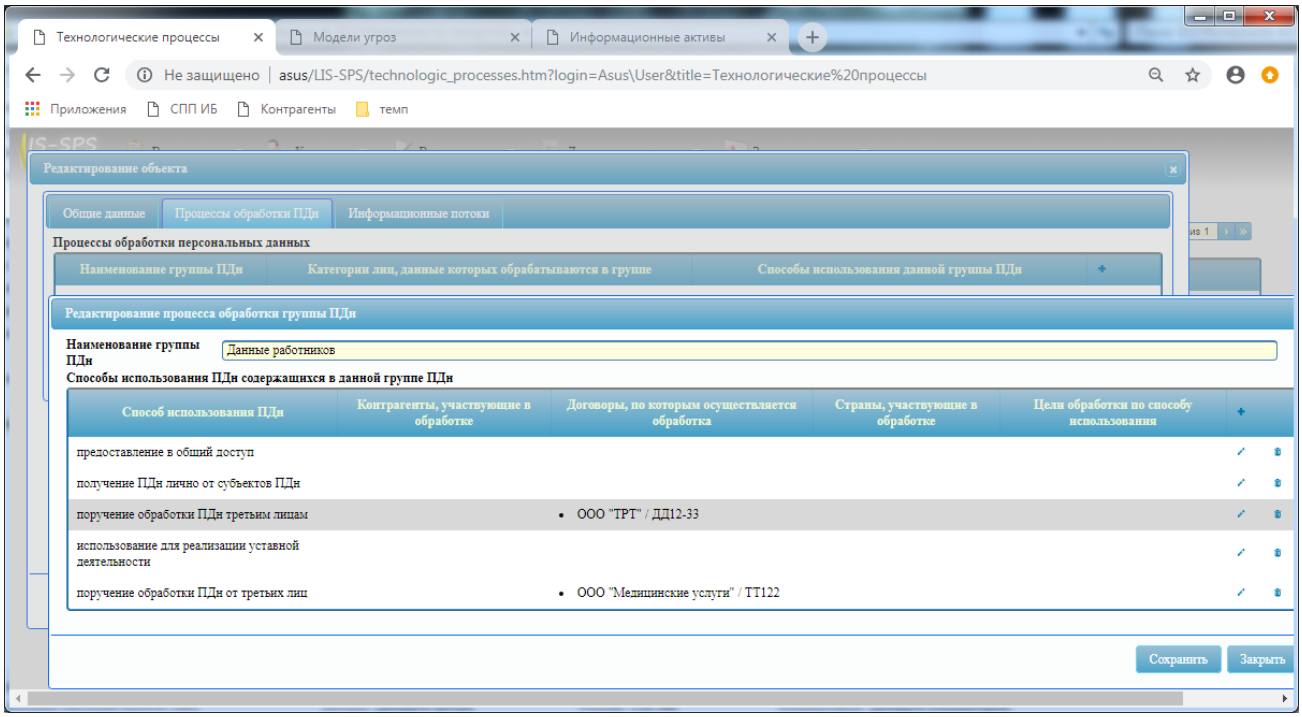

Рисунок 1 - Пример интерфейса «Технологические процессы»

1.3. учет возможности трансграничной передачи ПДн по каждому процессу с указанием стран, в которые осуществляется такая передача,

1.4. учет по каждому процессу источников получения ПДн (от субъектов ПДн лично, от третьих лиц),

1.5. учет владельцев процессов – отдельных лиц и/или структурных подразделений,

1.6. учет объема, категорий (абоненты, посетители и т.п.) лиц, данные которых обрабатываются в каждом процессе, категорий ПДн (ФИО, номер телефона, адрес и т.п.) по каждой категории лиц обрабатываемых ПДн, способов обработки ПДн (использование, передача в третьи страны, поручение на обработку и т.п.) с привязкой к целям обработки ПДн,

1.7. учет по каждому процессу информационных потоков между различными видами участников информационного процесса (субъектами ПДн, структурными подразделениями, активами, информационными активами и т.п.),

1.8. обеспечение возможности фильтрации процессов по множеству задаваемых параметров и экспорта произвольных данных по ним,

1.9. учет и нормирование (приведение к типовым) целей обработки ПДн,

1.10. автоматический контроль соответствия целей обработки ПДн, целям заранее заявленным,

1.11. обеспечение возможности согласования процесса ответственными лицами с отслеживанием версий процесса, простановкой электронной подписи.

2. Управление зданиями и помещениями, включая:

2.1. учет состава помещений, в которых производится обработка ПДн (как автоматизированная, так и неавтоматизированная),

2.2. учет помещений, в которых производится хранение съемных машинных носителей ПДн,

2.3. учет выполнения требований по защите помещений, в которых производится обработка ПДн, находятся машинные носители ПДн (наличие замков, решеток на окнах, надежных хранилищ для бумажных носителей ПДн при их неавтоматизированной обработке),

2.4. автоматический контроль необходимости обеспечения защиты помещений, в которых производится обработка ПДн посредством анализа внесенной информации о состоянии защиты помещений, наличия ПДн, характеристик расположения помещения (выход окон за пределы КЗ, возможность наличия посторонних лиц и т.п.).

3. Организация пропускного режима в помещения, включая:

3.1. учет лиц допущенных в помещения,

3.2. генерация приказа об утверждении перечня лиц имеющих доступ в помещения,

3.3. автоматический контроль актуальности перечня лиц допущенных в помещения.

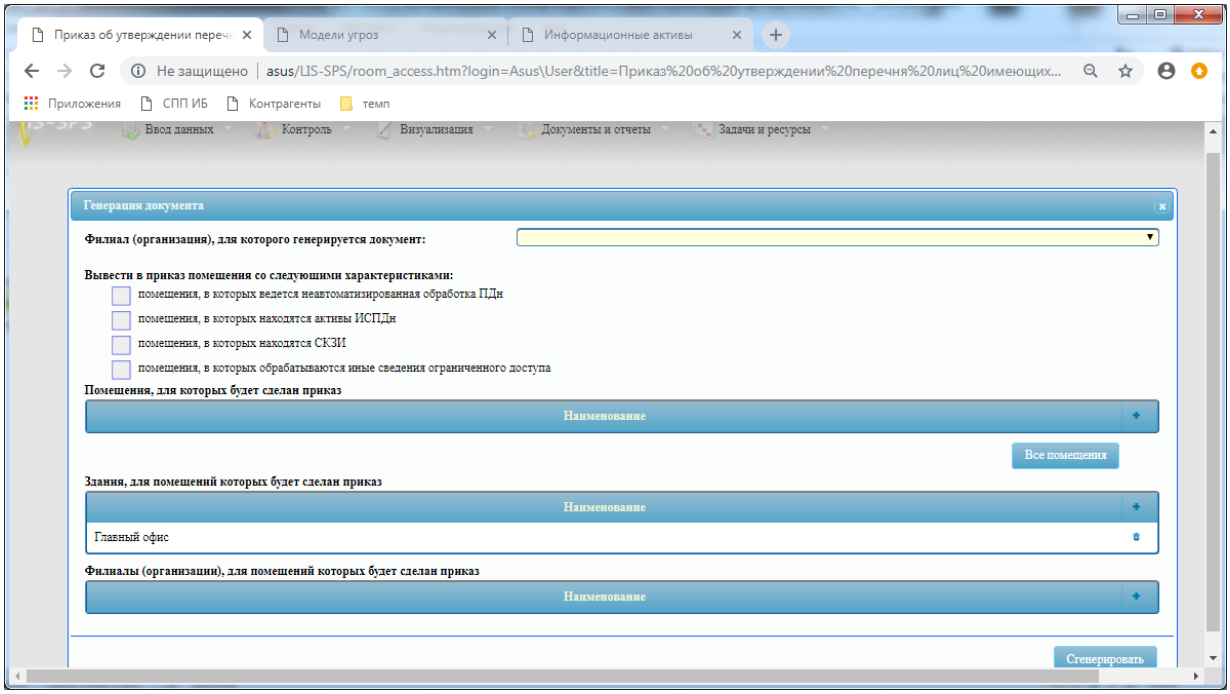

Рисунок 2 - Пример интерфейса «Генерация приказа о допуске лиц в помещения»

4. Учет информационных активов, включая:

4.1. учет информационных активов с ПДн (баз данных, файлов, бумажных документов, сервисов и т.п.), категорий лиц и состава обрабатываемых ПДн в информационных активах, характеристик режима обработки и разграничения доступа, других значимых характеристик,

4.2. автоматический расчет категорий ПДн содержащихся в активе,

4.3. обеспечение возможности ручного задания категории ПДн содержащихся в активе.

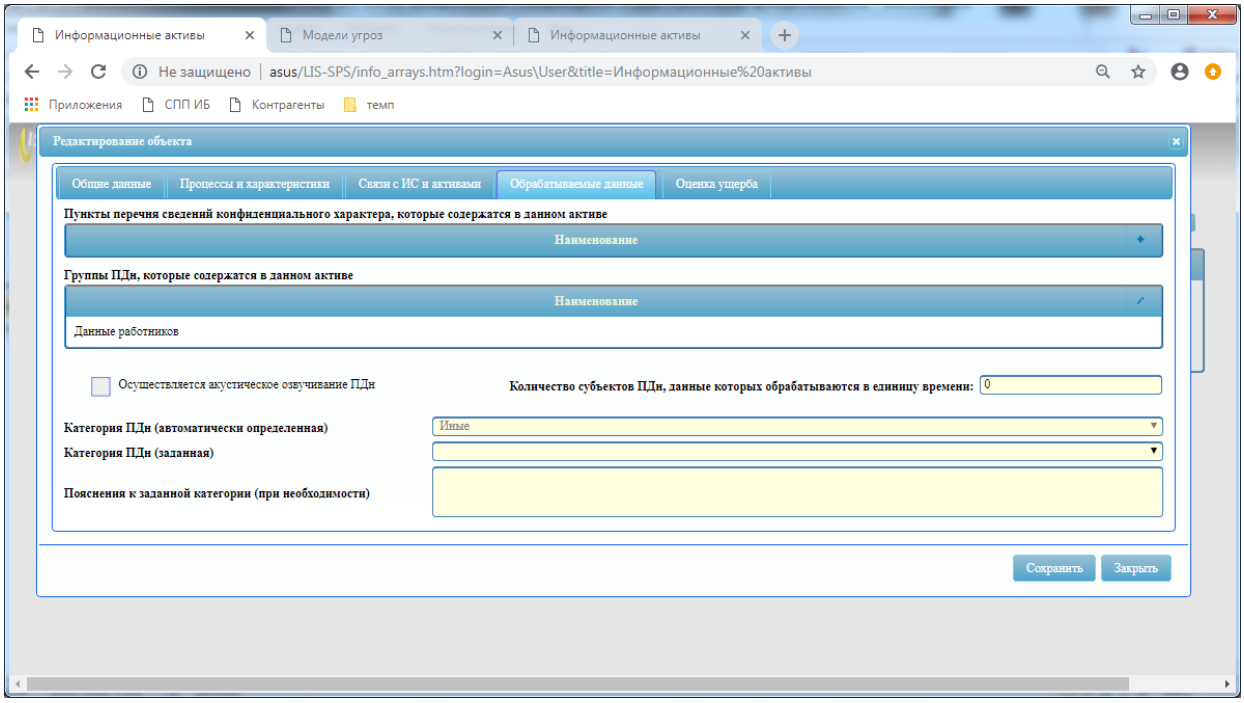

Рисунок 3 - Пример интерфейса «Информационные активы»

5. Контроль уничтожения ПДн при достижении целей обработки ПДн, включая:

5.1. ведение базы данных субъектов ПДн с заданием их ФИО, паспортных данных, принадлежности к тем или иным информационным активам,

5.2. учет произвольных характерных дат (дат, при наступлении которых начинается отсчет до конкретной даты уничтожения ПДн) по каждому субъекту ПДн позволяющих отслеживать сроки уничтожения ПДн,

5.3. автоматическое определение состава характерных дат, значимых для субъекта ПДн, посредством анализа процессов обработки ПДн, в которых участвуют ПДн данного субъекта ПДн,

5.4. задание сроков наступления характерных дат по каждому субъекту ПДн,

5.5. автоматический контроль своевременности уничтожения ПДн по каждому субъекту ПДн при окончании всех дат, которые заведены на данного субъекта ПДн.

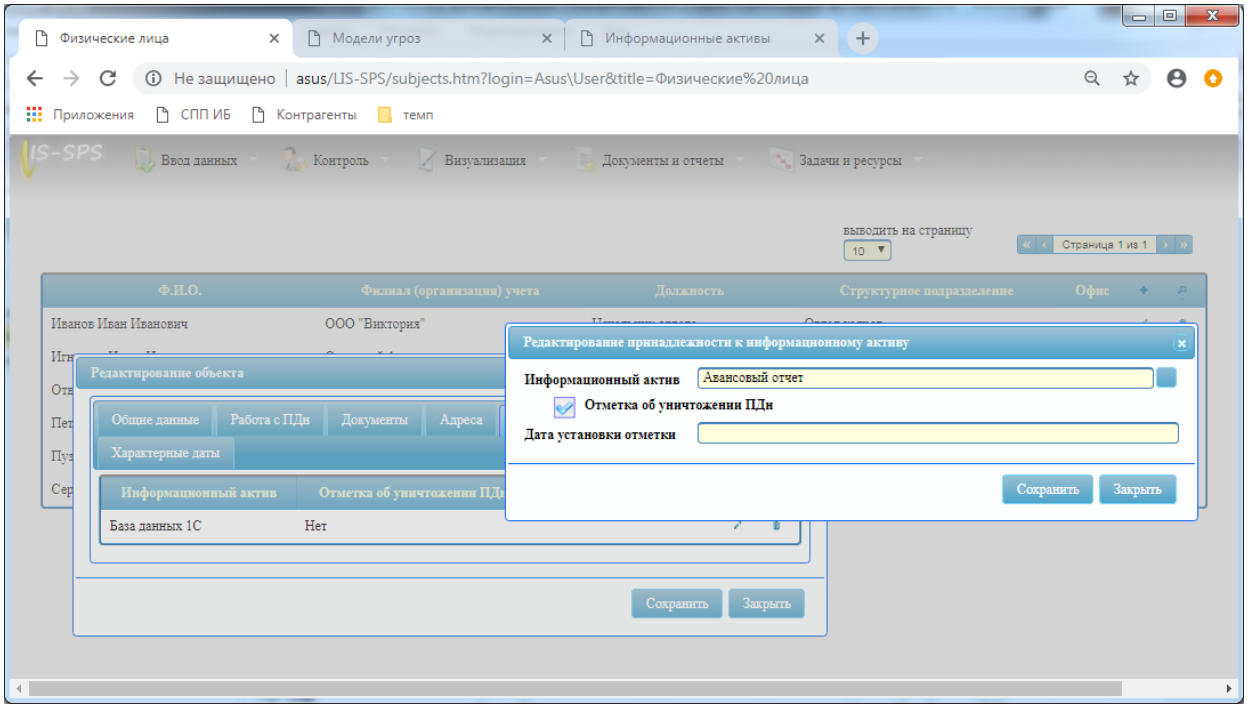

Рисунок 4 - Пример интерфейса «Физические лица»

6. Контроль наличия и генерация согласий на обработку ПДн, включая:

6.1. автоматическое определение необходимости получения согласий субъектов ПДн на обработку ПДн по участию информационных активов, в которых содержатся данные субъектов в процессах обработки ПДн требующих сбора согласий,

6.2. учет наличия согласий конкретных субъектов ПДн на обработку ПДн,

6.3. автоматический контроль необходимости получения согласий на обработку ПДн от конкретных субъектов ПДн,

6.4. генерация формы согласия на обработку ПДн с автоматическим включением в нее всех необходимых данных в зависимости от процессов обработки ПДн, в которых участвуют ПДн данного субъекта ПДн,

6.5. автоматический контроль наличия согласий на обработку ПДн от конкретных субъектов ПДн.

7. Категорирование ПДн, включая:

7.1. задание произвольных правил определения категории ПДн по категориям отдельных составов ПДн в целях автоматического определения категории ПДн обрабатываемых в информационных активах.

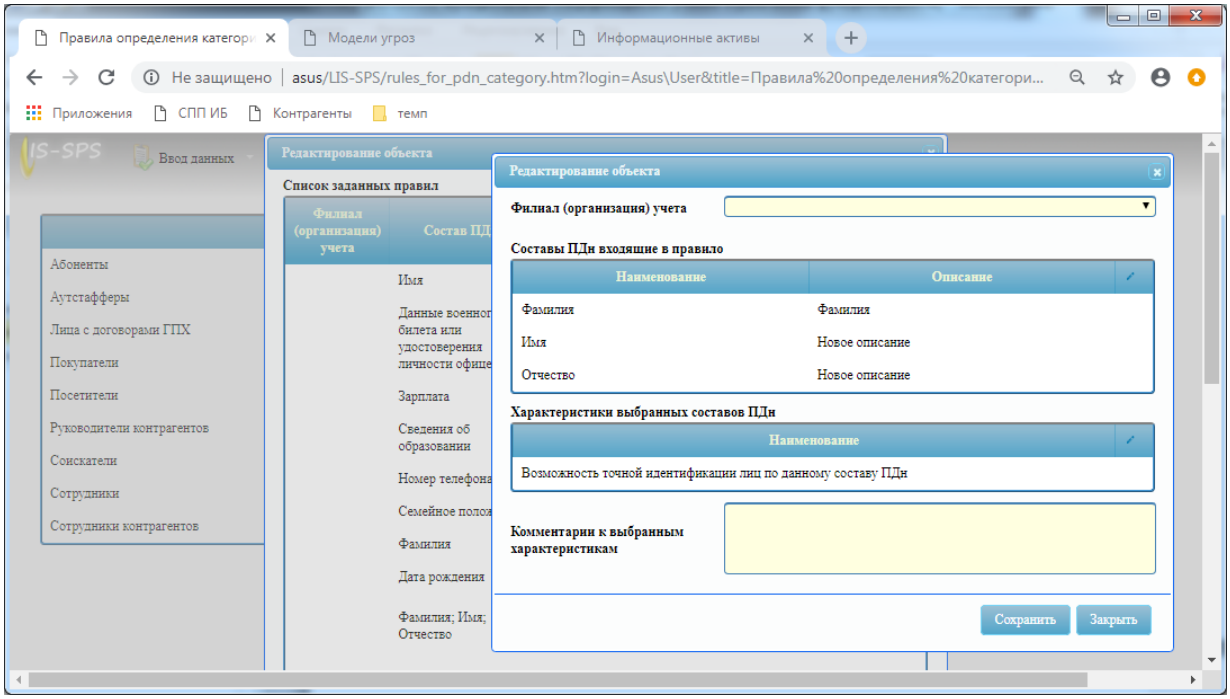

Рисунок 5 - Пример интерфейса «Правила определения категории ПДн»

8. Управление контрагентами, включая:

8.1. учет контрагентов, их адресов, ИНН, договоров контрагентов,

8.2. учет контрагентов, которым поручена обработка ПДн,

8.3. учет наличия поручений на обработку ПДн,

8.4. учет дат получения и истечения срока поручений на обработку по каждому договору контрагента,

8.5. автоматический контроль истечения срока поручения до окончания срока действия договора,

8.6. автоматический контроль наличия поручений на обработку ПДн,

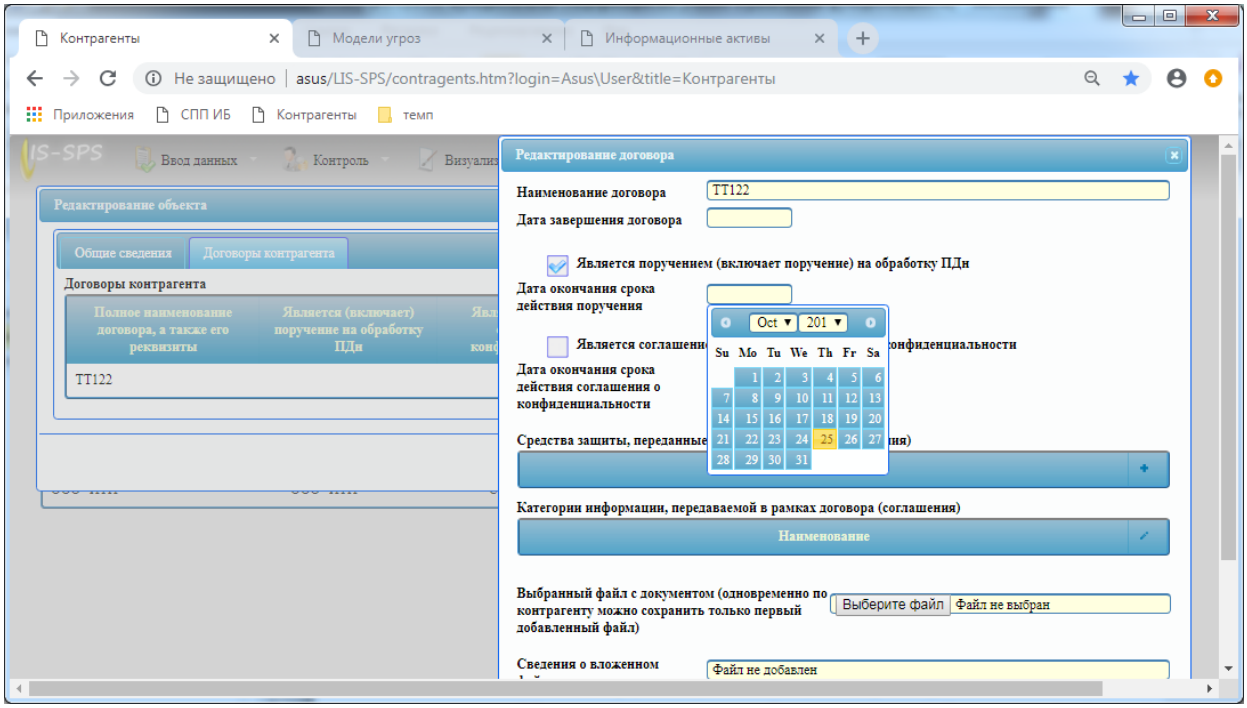

Рисунок 6 - Пример интерфейса «Контрагенты»

9. Учет доступа физических лиц к информационным активам, включая:

9.1. учет лиц и пар «должность» - «структурное подразделение», которым предоставляется доступ к ПДн по каждому заданному информационному активу (системе, базе данных, каталогу и т.п.),

9.2. учет дополнительных объектов доступа (таблиц, записей, функций, процедур и т.п.), к которым назначены права доступа в рамках информационных активов,

9.3. учет конкретных прав доступа назначенных пользователю в отношении информационных активов и/или дополнительных объектов доступа,

9.4. генерация формы матрицы доступа на допуск лиц к ПДн,

10. Учет технических активов, включая:

10.1. учет активов используемых для обработки ПДн, а также их характеристик, включая: обрабатываемые категории информации (персональные данные, коммерческая тайна и т.п.), место их размещения, содержащиеся на них информационные активы и т.п.

10.2. визуальное представление модели информационной системы.

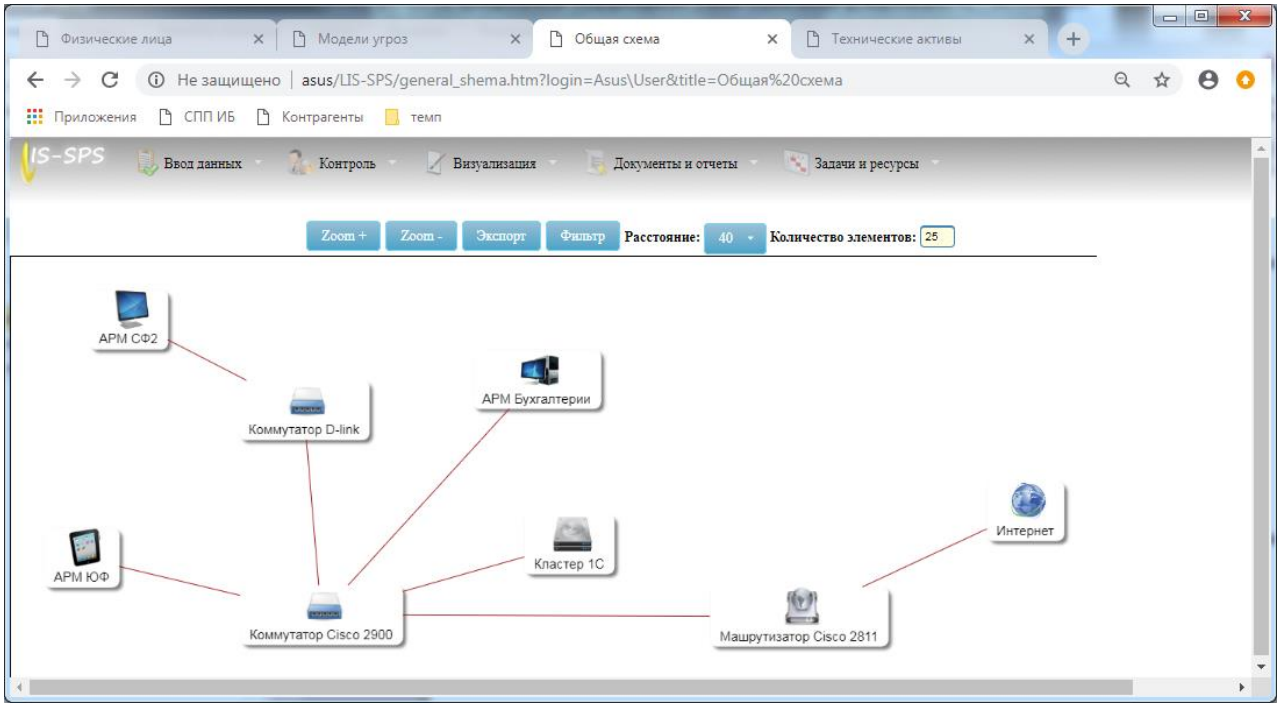

Рисунок 7 - Пример интерфейса «Общая схема»

11. Учет, контроль и генерация разъяснений порядка принятия решений при исключительно автоматизированной обработке, включая:

11.1. учет юридических последствий, которые может повлечь за собой обработка ПДн в ИСПДн в целях генерации разъяснения порядка принятия решений при исключительно автоматизированной обработке,

11.2. учет порядка защиты субъектом ПДн своих прав и законных интересов и порядка принятия решения при исключительно автоматизированной обработке в целях генерации разъяснения порядка принятия решений при исключительно автоматизированной обработке,

11.3. автоматическое определение субъектов ПДн, которым надо разъяснить порядок принятия решений при исключительно автоматизированной обработке на основании принадлежности субъекта ПДн к активам, в которых осуществляется принятие таких решений,

11.4. учет отправленных разъяснений порядка принятия решений при исключительно автоматизированной обработке,

11.5. генерация разъяснения порядка принятия решений при исключительно автоматизированной обработке и порядка защиты субъектом ПДн своих прав и законных интересов,

12. Учет, контроль и генерация Уведомлений о предполагаемой обработке ПДн, включая:

12.1. автоматическое определение состава субъектов ПДн, для которых надо генерировать Уведомление о предполагаемой обработке их ПДн,

12.2. учет отправки Уведомлений о предполагаемой обработке ПДн субъектам ПДн,

12.3. генерация формы уведомления субъекта ПДн о предполагаемой обработке его ПДн,

12.4. автоматический контроль уведомления субъекта ПДн до начала обработки его ПДн, посредством анализа наличия уже отправленного уведомления.

13. Учет ИСПДн, включая:

13.1. задание наименований ИСПДн их характеристик,

13.2. описание общих существенных для обработки ПДн характеристик ИСПДн (степень автоматизированности обработки, объем обрабатываемых ПДн, осуществляемые операции с ПДн).

14. Управление Уведомлением об обработке ПДн подаваемым в Роскомнадзор, включая:

14.1. ввод условий прекращения обработки ПДн организацией в виде даты или описания, например, ликвидация юридического лица,

14.2. учет сведений о филиальной структуре организации, адресах, ответственном за организацию обработки ПДн,

14.3. генерация формы Уведомления об обработке ПДн подаваемого в Роскомнадзор,

14.4. фиксация данных указанных в текущем Уведомлении об обработке ПДн,

14.5. автоматический контроль необходимости внесения изменений в Уведомление об обработке ПДн, посредством анализа изменений в процессах обработки и защиты ПДн, информационных активах, составе средств защиты, в сравнении с указанными в текущем Уведомлении,

14.6. автоматический контроль сроков внесения изменений в Уведомление об обработке ПДн с даты обнаружения несоответствия.

15. Управление документами в области ПДн, включая:

15.1. ввод состава утверждающих и согласующих лиц по каждому виду документов генерируемых с использованием комплекса с учетом сложного состава структурных подразделений, наличия филиалов,

15.2. обеспечения возможности согласования и утверждения документов в электронной форме с обеспечением механизмов электронной подписи,

15.3. обеспечение возможности редактирования шаблонов документов.

16. Управление актами определения уровня защищенности ИСПДн, включая:

16.1. генерация формы акта определения уровня защищенности ИСПДн посредством автоматического определений категорий ПДн, характеристик ИСПДн включаемых в акт,

16.2. фиксация данных указанных в текущем акте определения уровня защищенности ИСПДн,

16.3. автоматический контроль необходимости изменения акта определения уровня защищенности ИСПДн посредством анализа изменений в данных используемых для определения уровня и сравнении их с данными указанными в текущем акте,

16.4. автоматический контроль необходимости генерации акта определения уровня защищенности на вновь созданные ИСПДн, на которые отсутствует ранее сгенерированный акт.

17. Управление контролем защищенности ПДн, включая:

17.1. учет проведенных контролей уровня защищенности ПДн и соблюдения условий использования средств защиты,

17.2. автоматическое формирование необходимых для проверки функций защиты, средств защиты, описаний процессов обработки ПДн,

17.3. автоматический контроль необходимости проведения контроля защищенности ПДн и соблюдения условий использования средств защиты с учетом даты проведения предыдущего контроля и требуемой частоты проведения контроля,

17.4. генерация формы акта на проведение контроля защищенности ПДн и соблюдения условий использования средств защиты для конкретных активов с автоматическим указанием функций, которые должны быть проконтролированы,

17.5. генерация формы приказа на проведение контроля защищенности ПДн и соблюдения условий использования средств защиты для конкретных активов.

18. Управление моделью угроз безопасности ПДн, включая:

18.1. учет данных по категориям лиц имеющих возможность влияния на компоненты ИСПДн (пользователи, обслуживающий персонал, администраторы и т.п.)

18.2. учет всех возможных угроз безопасности ПДн, их вероятностей, условий актуальности,

18.3. генерация формы модели угроз для конкретных ИСПДн,

18.4. фиксация текущего состава каждой сгенерированной модели угроз,

18.5. автоматический контроль необходимости внесения изменений в модель угроз, посредством анализа изменений в данных, используемых для генерации модели, и их сравнения с данными указанными в текущей форме модели,

18.6. автоматический контроль необходимости генерации модели угроз на вновь созданные ИСПДн.

19. Задание проекта системы защиты ПДн, включая:

19.1. задание варианта СЗПДн (состава средств защиты для выбранного множества активов с учетом модели угроз, заданных ранее характеристик данных активов, ранее заданных характеристик средств защиты),

19.2. учет зависимостей между функциями защиты и характеристиками ИСПДн (уровнями защищённости, распределенности, наличия выхода в сети общего пользования, использовании съемных носителей и т.п.)

19.3. автоматический контроль изменений в составе системы защиты ПДн, необходимости внесения изменений в СЗПДн посредством анализа изменений в уровнях защищенности ИСПДн для защищаемых активов, актуальных угроз, режимов обработки и разграничения доступа,

19.4. автоматический контроль необходимости генерации системы защиты на вновь созданные активы, которые не входят в ранее созданный вариант СЗПДн,

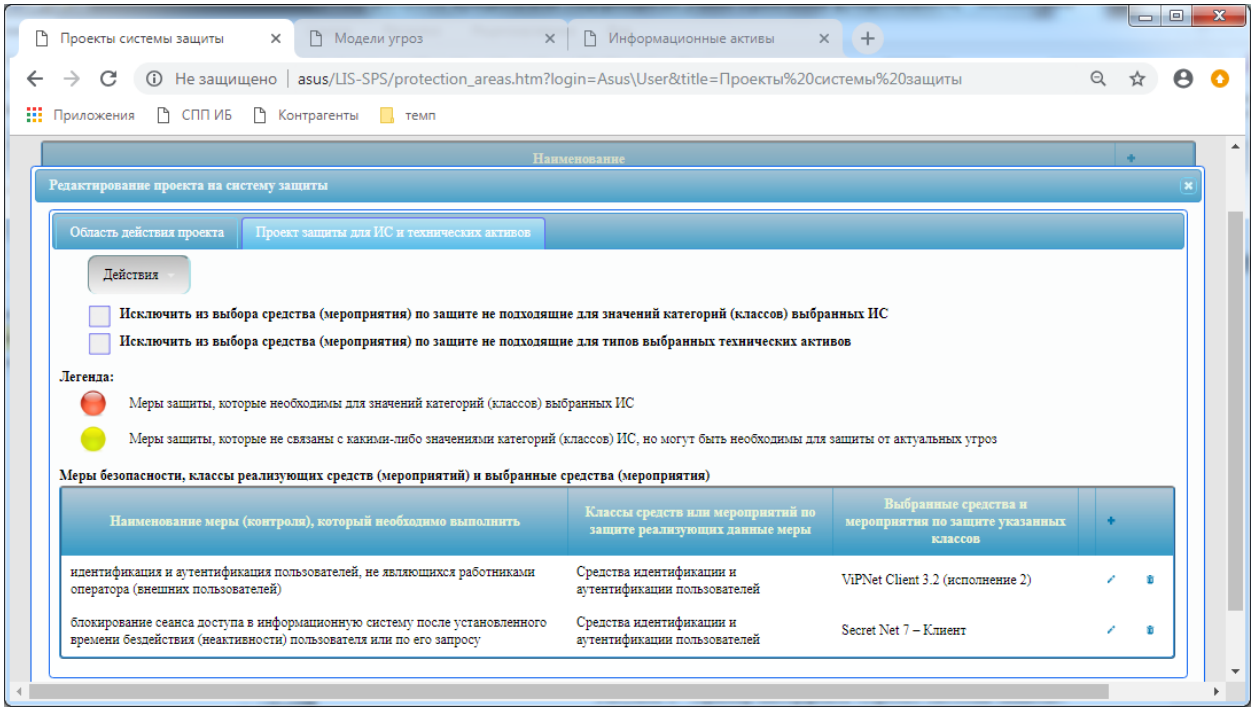

Рисунок 8 - Пример интерфейса «Проект системы защиты»

20. Учет машинных носителей ПДн, с указанием их номеров, ответственных, дат ввода в эксплуатацию.

21. Управление Перечнем ПДн, включая:

21.1. автоматическая генерация перечня персональных данных, с включением в документ данных по обрабатываемым ПДн из указанных в процессах обработки, информационных активах;

21.2. автоматический контроль необходимости актуализации перечня персональных данных по наличию изменений в составе обрабатываемых ПДн в процессах и информационных активах.

2.2. Генерируемые документы

СПП ПДн в процессе своей работы обеспечивает возможность автоматической генерации следующих документов:

1) Акта классификации ИСПДн по требованиям ЦБ РФ
2) Акт определения уровня защищенности ИСПДн
3) Акта проведения контроля защищенности
4) Журнала установки средств защиты
5) Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов
6) Матрицы доступа
7) Модели угроз
8) Перечня ПДн
9) Приказа на допуск к работе с СКЗИ
10) Приказа о проведении контроля (аудита) защищенности
11) Приказа об утверждении перечня лиц имеющих доступ в помещения
12) Приказа о предоставлении доступа к персональным данным
13) Согласия на обработку ПДн
14) Разъяснения порядка принятия решений при исключительно автоматизированной обработке и порядка защиты субъектом ПДн своих прав и законных интересов
15) Уведомления субъекта ПДн о предполагаемой обработке его ПДн
16) Уведомления об обработке ПДн предоставляемого в Роскомнадзор

2.3. Внешние интерфейсы

Внешние интерфейсы предназначены для:

- автоматизации процедур загрузки и синхронизации данных из внешних баз данных (интерфейсы импорта и синхронизации);
- автоматизации процедур подгрузки исходных данных из формализованных опросных листов (интерфейсы подгрузки).

Внешние интерфейсы импорта и синхронизации СПП ПДн осуществляют:

- загрузку данных из внешних баз данных;
- проверку необходимости обновления ранее загруженных записей;
- изменение ранее загруженных записей на актуальные (при необходимости).

СПП ПДн имеет возможность импорта и синхронизации следующих данных из внешних систем:

- списка филиалов,
- списка офисов,
- списка помещений,

- состава и структуры структурных подразделений,
- состава и структуры технологических процессов,
- состава информационных систем,
- состава информационных активов,
- состава сотрудников,
- состава технических активов,
- состава субъектов ПДн,
- состава допущенных к информационным активам лиц,
- данных о контрагентах и договорах с ними,
- состава физических лиц допущенных в помещения, структурных подразделений – владельцев помещений.

СПП ПДн имеет возможность подгрузки из опросных листов следующих данных:

- сведений о Группах ПДн,
- сведений о процессах обработки ПДн и их характеристиках,
- сведений о зданиях и помещениях,
- сведений об информационных активах,
- сведений об активах,
- сведений об информационных потоках.

Внешние интерфейсы импорта и синхронизации СПП ПДн поддерживают следующие источники данных:

- базы данных MS SQL Server 2005 Standard Edition или выше,
- базы данных Oracle 9i или выше,
- файлы формата .CSV.

3. Нормативные документы

Функции системы разработаны с учетом требований следующих нормативных документов:

- Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных»
- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»
- Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Постановление Правительства РФ от 15 сентября 2008 г N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
- Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ,утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.
- «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утверждены руководством 8 Центра ФСБ России 31 марта 2015 г. N149/7/2/6-432
- Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»
- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», введена в действие приказом от 13 июня 2001 года N 152 (ФАПСИ)

- «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», введено приказом ФСБ РФ от 9 февраля 2005 г. N 66
- РС БР ИББС-2.3-2010. Рекомендации в области стандартизации Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации»