Privacy-SPS

v.1.1.5.0

ФУНКЦИОНАЛЬНАЯ СПЕЦИФИКАЦИЯ

020314-1.1.5.0-35

2015 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

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 включает следующие компоненты:

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

Сервер баз данных осуществляет хранение данных используемых в СПП ПДн.

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

АРМ оператора представляет собой программный клиент устанавливаемый на АРМ пользователей и администраторов системы.

1.3. Краткий обзор

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 автоматизированный учет обращений субъектов 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, устанавливается 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 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 генерацию порядка 35 видов документов,
- позволяет произвести порядка 50 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 выделяет клиентское место 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,

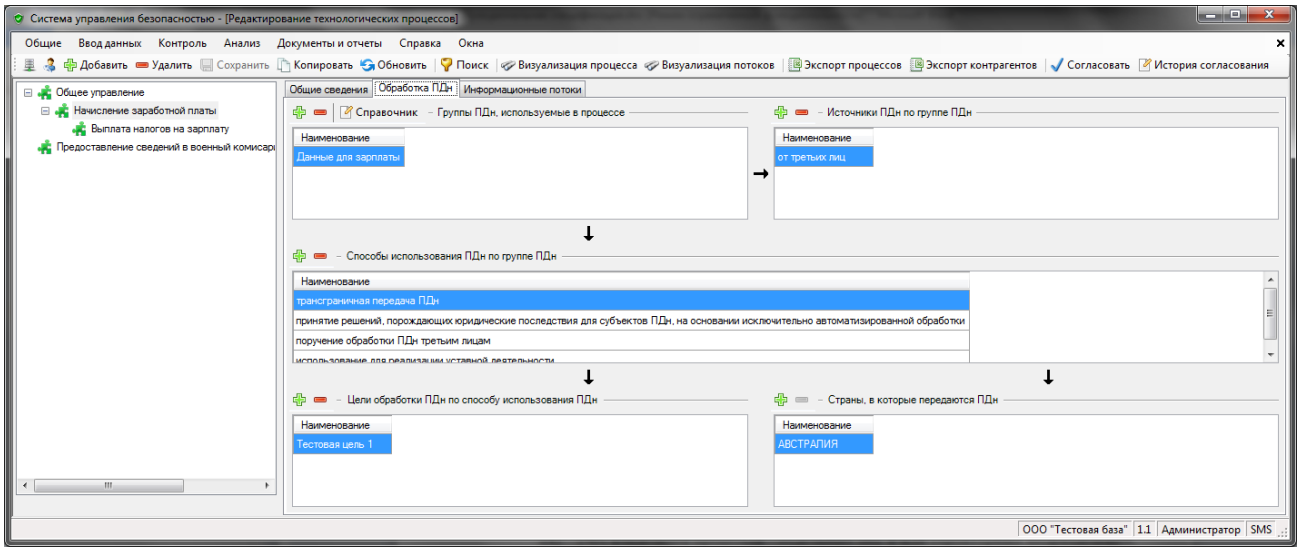

Рисунок 1 - Пример интерфейса «Технологические процессы»

1.3. учет процессов трансграничной передачи ПДн,

1.4. учет 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, состава 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 информационных потоков между различными видами участников информационного процесса (субъектами ПДн, структурными подразделениями, активами, информационными массивами и т.п.),

1.8. визуальное представление модели информационных потоков,

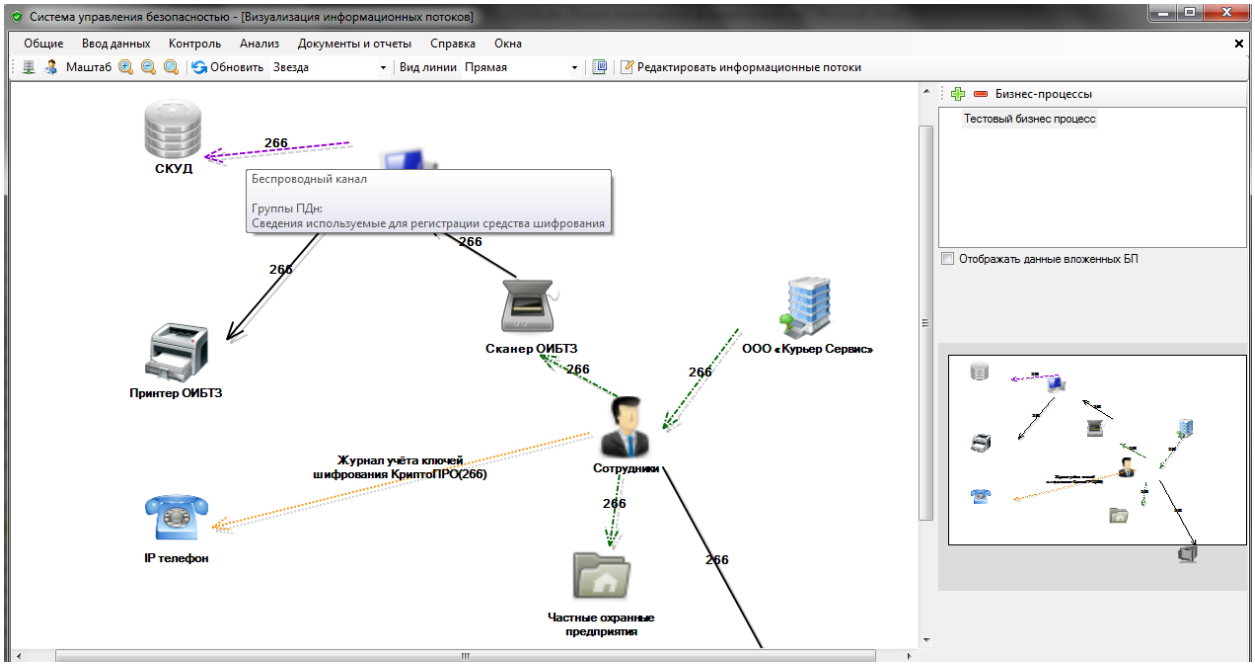

Рисунок 2 - Пример интерфейса «Визуализация информационных потоков»

1.9. ввод ограничений накладываемых целями обработки на обрабатываемые ПДн по объему ПДн, участвующим в достижении цели категориям лиц, составам ПДн, способам обработки ПДн и контроль их выполнения в информационных массивах содержащих ПДн,

1.10. редактирование модели информационных потоков в визуальной форме,

1.11. визуальное представление модели процессов обработки ПДн,

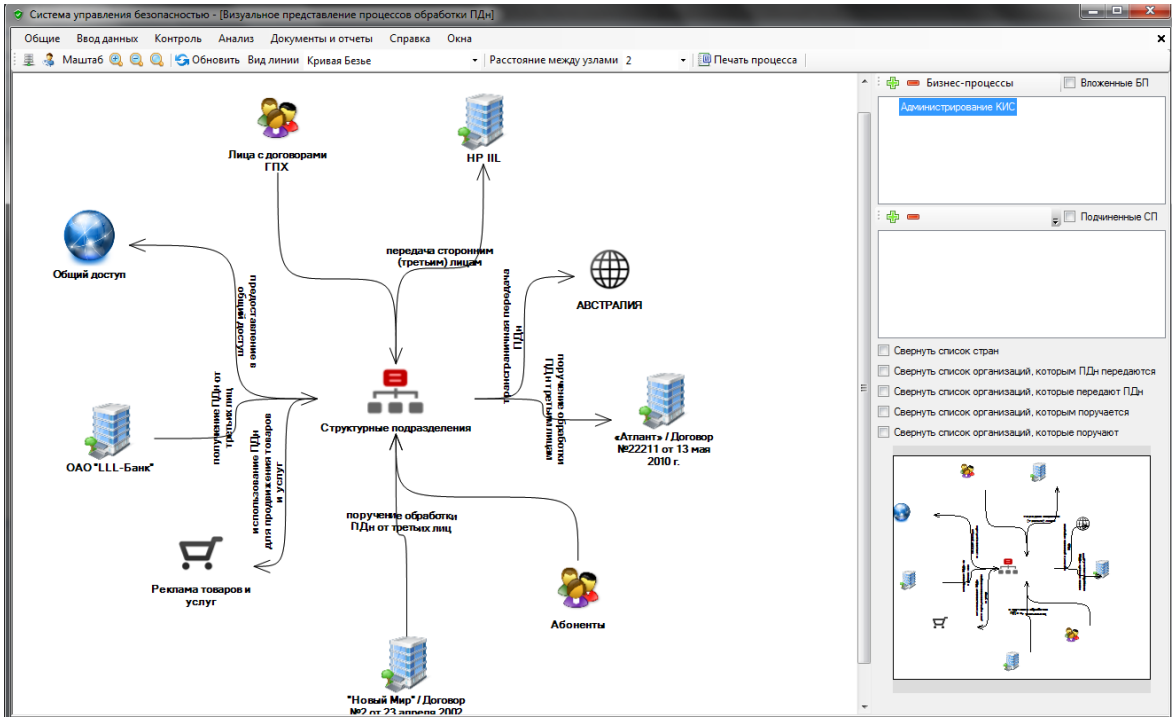

Рисунок 3 - Пример интерфейса «Визуализация процессов обработки ПДн»

1.12. ввод несовместимых целей обработки ПДн,

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

1.14. контроль соответствия целей обработки ПДн, целям заранее заявленным,

2. Управление зданиями и помещениями, включая:

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

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

2.3. 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.),

2.4. учет структурных подразделений – владельцев помещений,

3. Организация пропускного режима в помещения, включая:

3.1. учет лиц допущенных в помещения,

3.2. генерация приказа о допуске лиц в помещения,

3.3. контроль актуальности перечня лиц допущенных в помещения,

4. Учет информационных массивов, включая:

4.1. учет информационных массивов ПДн (баз данных, файлов, бумажных документов, сервисов и т.п.), категорий лиц и состава обрабатываемых ПДн в информационных массивах ПДн, состава информационных потоков между массивами, характеристик режима обработки и разграничения доступа в массиве, других значимых характеристик,

4.2. контроль информационных массивов на наличие несовместимых целей обработки,

4.3. учет общедоступных источников ПДн,

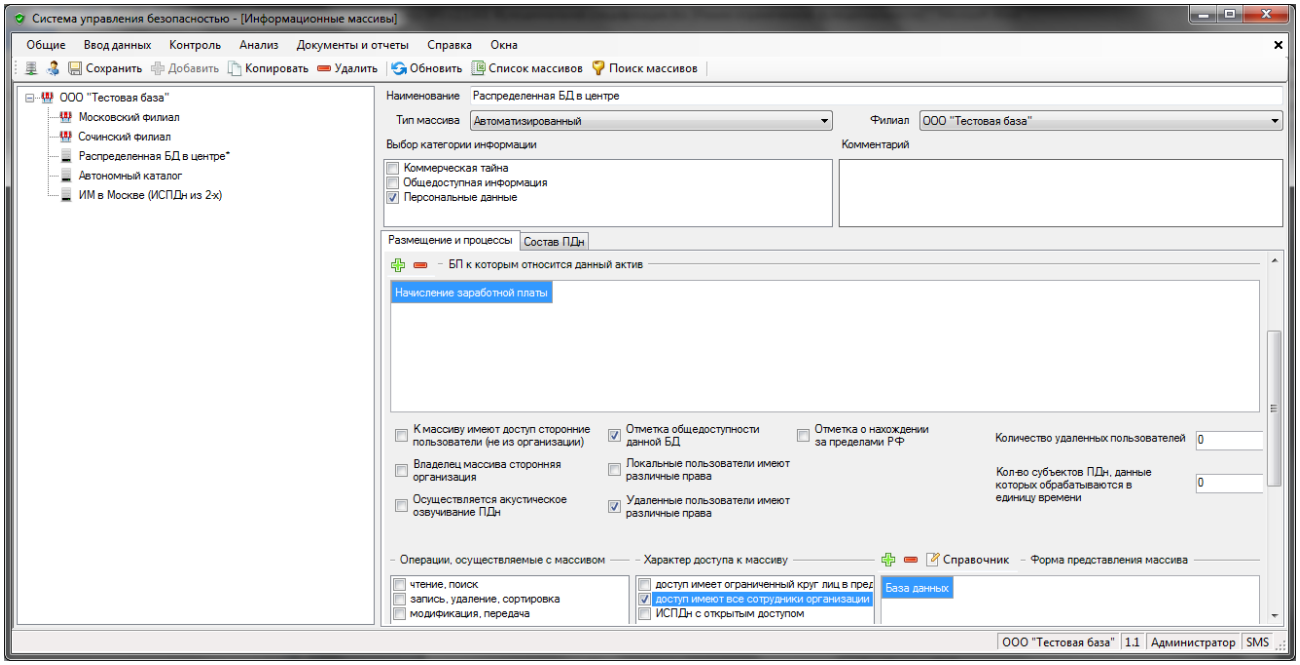

Рисунок 4 - Пример интерфейса «Информационные массивы»

5. **Контроль уничтожения ПДн при достижении целей обработки ПДн, включая:**
   - 5.1. ввод условий прекращения обработки ПДн организацией в виде даты или описания, например, ликвидация юридического лица,
   - 5.2. учет характерных дат (дат, при наступлении которых начинается отсчет до конкретной даты уничтожения ПДн) по каждой записи в информационных массивах позволяющих отслеживать сроки уничтожения ПДн,
   - 5.3. контроль своевременности уничтожения ПДн при достижении целей обработки или утраты необходимости их достижения,
6. **Контроль наличия и генерация согласий на обработку ПДн, включая:**
   - 6.1. определение необходимости получения согласий субъектов ПДн на обработку ПДн по участию информационных массивов, 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. контроль необходимости получения согласий на обработку ПДн от конкретных субъектов ПДн,
   - 6.4. генерация формы согласия на обработку ПДн,
   - 6.5. контроль наличия согласий на обработку ПДн от конкретных субъектов ПДн,
7. **Категорирование ПДн, включая:**
   - 7.1. задание правил определения категории ПДн по категориям отдельных составов ПДн в целях автоматического определения категории ПДн обрабатываемых в информационных массивах,

7.2. задание категории обрабатываемых ПДн в информационных массивах вручную, на основе собственных аналитических предположений,

8. Управление общедоступными ПДн, включая:

8.1. учет заявлений на исключение ПДн из общедоступных источников,

8.2. контроль необходимости исключения ПДн из общедоступных источников (информационных массивов, в которых содержатся общедоступные категории ПДн),

9. Управление контрагентами, включая:

9.1. учет контрагентов и договоров контрагентов,

9.2. учет лиц, которым поручена обработка ПДн,

9.3. учет наличия поручений на обработку ПДн,

9.4. учет дат получения и истечения срока поручений на обработку,

9.5. контроль истечения срока поручения до окончания срока действия договора,

9.6. контроль наличия поручений на обработку ПДн,

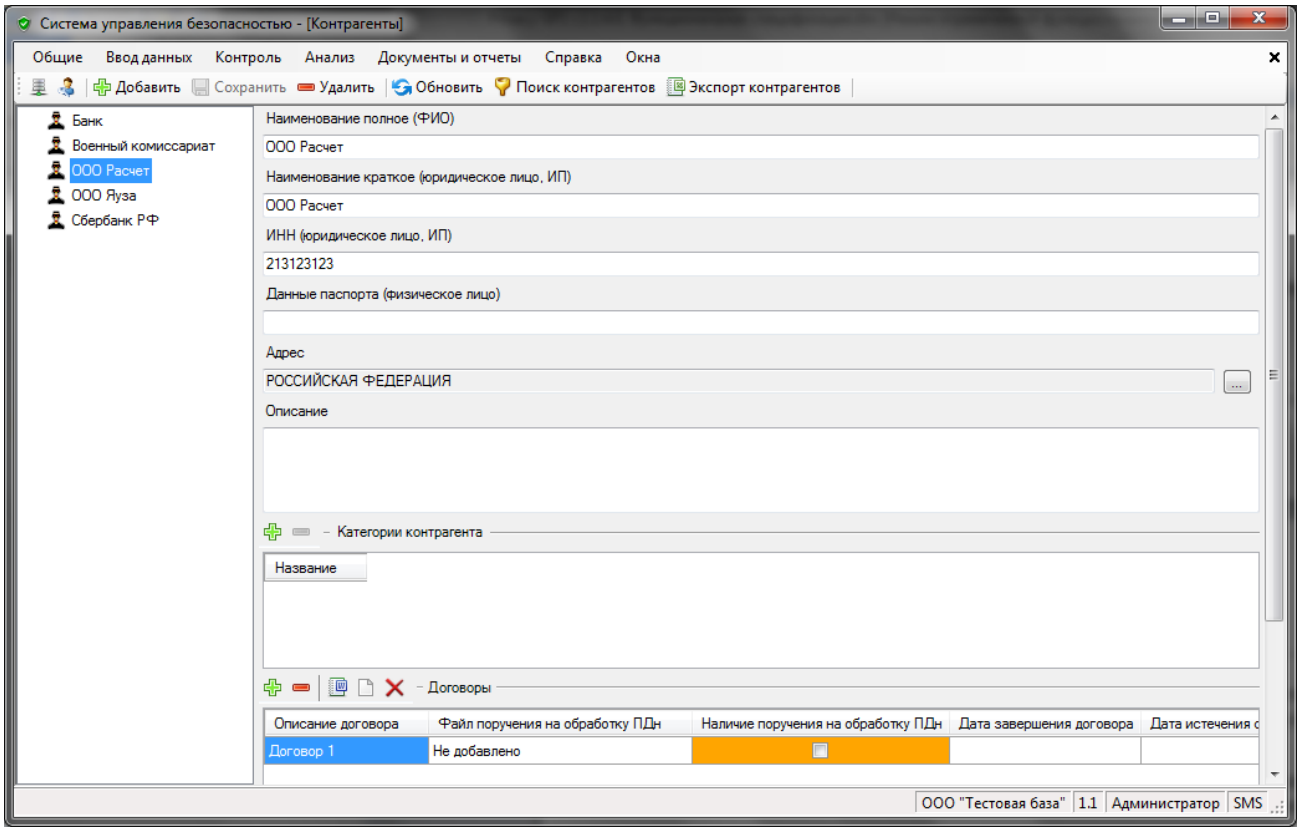

Рисунок 5 - Пример интерфейса «Контрагенты»

10. Учет доступа физических лиц к информационным массивам, включая:

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

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

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

10.4. генерация формы приказа на допуск лиц к ПДн,

10.5. генерация формы приказа на исключение допуска лиц к ПДн,

11. Учет активов, включая:

11.1. 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 массивы и массивы, к которым производится обращение, режимы обработки и т.п.

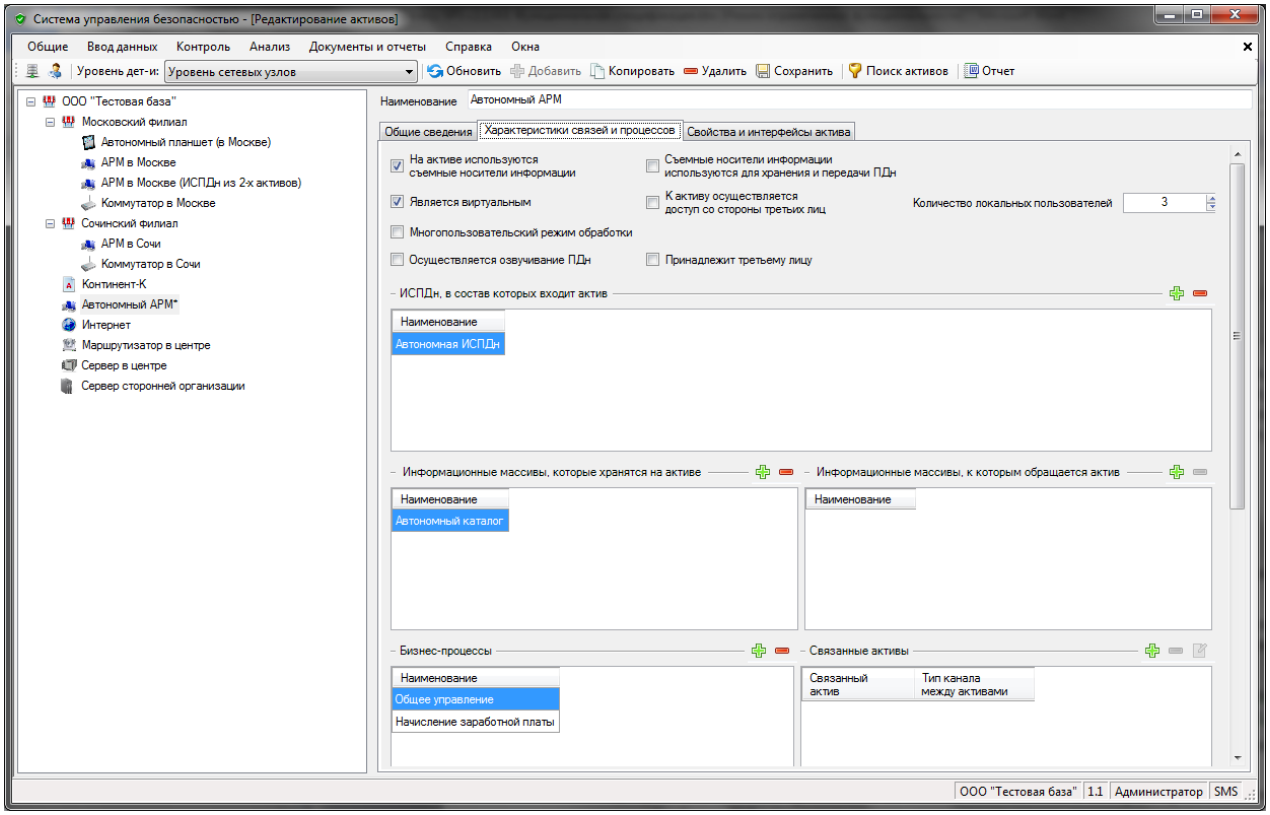

Рисунок 6 - Пример интерфейса «Активы»

11.2. визуальное представление модели информационной системы,

11.3. редактирование состава активов в визуальной форме,

12. Уведомление о характере процессов обработки ПДн, включая:

12.1. учет обращений субъектов ПДн на ознакомление с характером процессов обработки их ПДн,

12.2. контроль сроков подготовки уведомлений субъектов ПДн об обработке их ПДн,

12.3. генерация уведомления субъекта ПДн о характере процессов обработки его ПДн,

12.4. учет отправки субъектам ПДн уведомлений о характере процессов обработки их ПДн,

12.5. учет нормативных или иных оснований для отказа в предоставлении информации о характере обрабатываемых ПДн по конкретным ИСПДн в целях включения данной информации, при необходимости, в соответствующую форму уведомления субъекта ПДн,

12.6. генерация формы уведомления субъекта ПДн, содержащего мотивированный отказ на запрос о предоставлении информации о характере обрабатываемых ПДн,

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

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

13.2. 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,

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

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

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

14. Учет, контроль и генерация возражений на принятие решений, включая:

14.1. учет получения возражений на принятие решений несущих юридические последствия на основании исключительно автоматизированной обработки,

14.2. контроль сроков подготовки уведомления о результатах рассмотрения такого возражения на принятие решений несущих юридические последствия на основании исключительно автоматизированной обработки,

14.3. учет отправки Уведомлений по результатам рассмотрения возражений на принятие решений несущих юридические последствия на основании исключительно автоматизированной обработки,

14.4. генерация Уведомления субъекта ПДн о результатах рассмотрения возражения на принятие решений несущих юридические последствия на основании исключительно автоматизированной обработки,

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

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

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

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

15.4. контроль уведомления субъекта ПДн до начала обработки его ПДн, посредством анализа наличия уже отправленного уведомления;

16. Управление запросами на уточнение, изменение ПДн, неправомерные действия, включая:

16.1. учет получения запросов на уточнение, изменение и т.п. ПДн, которые являются неполными, устаревшими, недостоверными и т.п., а также о неправомерных действиях оператора с ПДн,

16.2. учет даты устранения нарушений в области обработки ПДн указанных в запросах субъектов ПДн, или уничтожения ПДн субъектов ПДн с целью контроля сроков отправки соответствующих ответов,

16.3. генерация формы уведомления об устранении нарушений в области обработки ПДн или уничтожении ПДн по результатам проверки,

16.4. ввод даты, с которой информация о неправомерных действиях с ПДн получила подтверждение с целью контроля сроков отведенных на устранение нарушений,

16.5. контроль сроков отведенных на устранение нарушений в области обработки ПДн,

16.6. учет отправки субъектам ПДн Уведомлений о внесенных изменениях в ПДн и предпринятых мерах по устранению нарушений указанных в обращениях субъектов ПДн,

16.7. контроль необходимости отправки уведомлений субъектам ПДн о внесенных изменениях в ПДн и предпринятых мерах по устранению нарушений указанных в обращениях субъектов ПДн,

17. Управление отзывами согласий на обработку ПДн, включая:

17.1. учет получения от субъектов ПДн отзывов согласий на обработку ПДн,

17.2. контроль уничтожения ПДн в срок при отзыве согласий субъектов ПДн и отсутствии других нормативных оснований для обработки ПДн,

18. Учет ИСПДн, включая:

18.1. задание наименований ИСПДн,

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

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

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

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

19.3. контроль необходимости внесения изменений в Уведомление об обработке ПДн, посредством анализа изменений в процессах обработки и защиты ПДн в сравнении с указанными в текущем Уведомлении,

19.4. контроль сроков внесения изменений в Уведомление об обработке ПДн с даты обнаружения несоответствия,

20. Управление документами в области ПДн, включая:

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

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

20.3. учет эксплуатационной и технической документации к средствам защиты с сохранением их названий, номеров, самих документов,

20.4. обеспечение возможности редактирования шаблонов документов,

21. Управление средствами защиты, включая:

21.1. учет конкретных средств защиты, условий применения средств защиты для обеспечения безопасности активов,

21.2. учет партий средств защиты, в том числе прошедших процедуру оценки соответствия, дат получения сертификатов, возможных мест их установки, условий их использования, классов и уровней защиты, режимов обработки и разграничения доступа, на которые они рассчитаны,

21.3. учет фактических мест и времени установки средств защиты (ведение журнала истории установки средств защиты на конкретных активах),

21.4. контроль сроков проведения повторной процедуры оценки соответствия средств защиты на основании введенных данных по срокам действия сертификатов на конкретные средства защиты,

22. Управление актами определения уровня защищенности ИСПДн, включая:

22.1. генерация формы акта определения уровня защищенности ИСПДн,

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

22.3. 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,

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

23. Управление резервными копиями ПДн, включая:

23.1. учет наличия резервных копий ПДн по информационным массивам,

23.2. контроль наличия резервных копий,

24. Управление контролем защищенности ПДн, включая:

24.1. учет проведенных контролей уровня защищенности ПДн и соблюдения условий использования средств защиты с указанием даты проведения контроля по каждой ИСПДн,

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

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

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

25. Управление моделью угроз безопасности ПДн, включая:

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

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

25.3. генерация формы модели угроз для конкретных ИСПДн,

25.4. фиксация текущего состава каждой сгенерированной модели угроз,

25.5. 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,

25.6. контроль необходимости генерации модели угроз на вновь созданные ИСПДн,

26. Управление моделью нарушителя, включая:

26.1. генерация формы модели нарушителя для конкретных ИСПДн,

26.2. фиксация текущего состава каждой сгенерированной модели нарушителя,

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

26.4. контроль необходимости генерации модели нарушителя на вновь созданные ИСПДн,

27. Задание системы защиты ПДн, включая:

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

27.2. 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,

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

27.4. контроль наличия активов без установленных средств защиты,

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

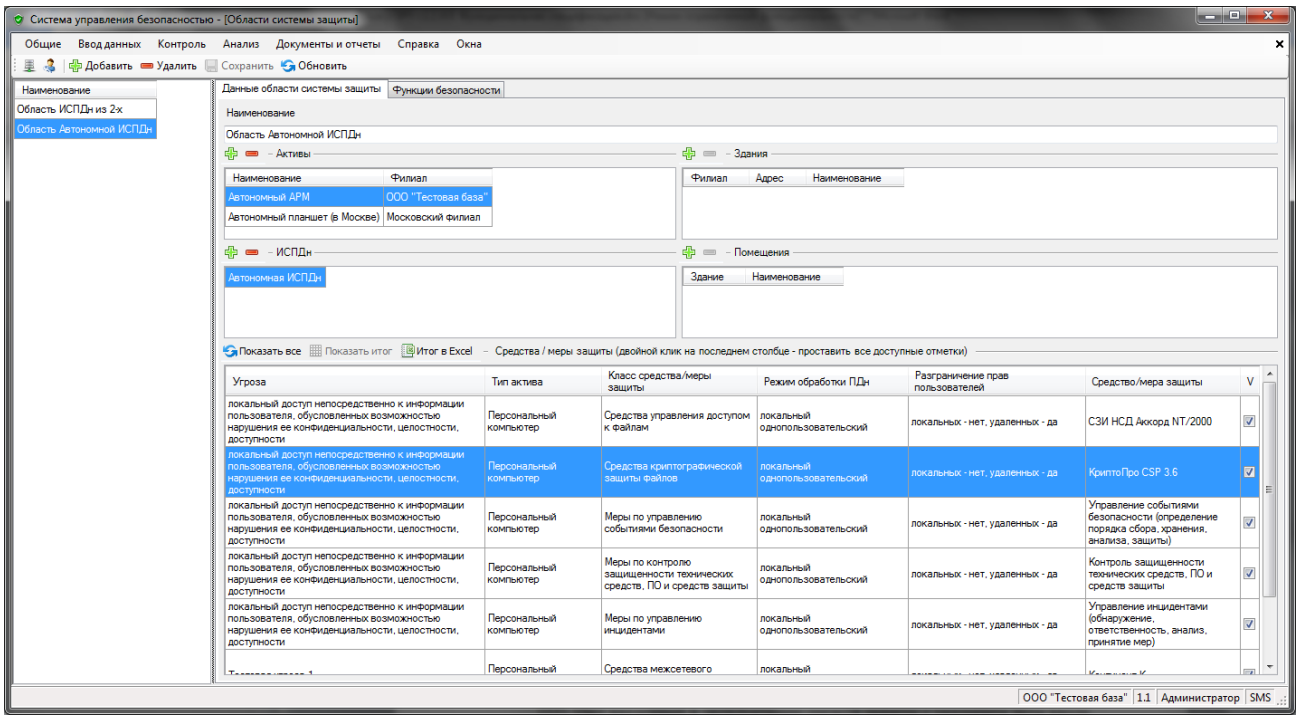

Рисунок 7 - Пример интерфейса «Область системы защиты»

28. Проверка эффективности системы защиты, включая:

28.1. учет проведенных проверок эффективности средств защиты с указанием даты проверки,

28.2. контроль необходимости проверки эффективности средств защиты, посредством анализа наличия средств защиты, для которых не указана отметка о проведенной проверке,

28.3. генерация формы акта о проверке эффективности средств защиты с указанием проверенных функций средств защиты, мест их установки,

29. Ввод средств защиты в эксплуатацию, включая:

29.1. учет введенных в эксплуатацию средств защиты с указанием даты ввода,

29.2. контроль необходимости ввода в эксплуатацию средств защиты посредством анализа наличия средств защиты не введенных в эксплуатацию,

29.3. генерация форм приказов на ввод в эксплуатацию средств защиты для средств защиты прошедших проверку эффективности,

30. Управление обучением в области ПДн, включая:

30.1. учет сотрудников, которые прошли обучение правилам обработки и защиты ПДн, а также тех, кто ознакомлен с требованиями по обработке ПДн,

30.2. контроль наличия сотрудников, которым надо пройти обучение,

30.3. учет ознакомления лиц, из числа допущенных к ПДн, с правилами обработки ПДн,

30.4. контроль ознакомления лиц, из числа допущенных к ПДн, с правилами обработки ПДн,

30.5. контроль ознакомления лиц, из числа допущенных к ПДн, с фактом обработки ими ПДн,

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

32. Учет нештатных ситуаций, включая:

32.1. учет нештатных ситуаций, описания результатов их расследования, подверженных активов, ответственных за их расследование;

32.2. учет документов связанных с нештатной ситуацией,

33. Описание системы защиты ПДн, включая:

33.1. генерация формы описания системы защиты, включающего описание состава используемых средств защиты, их функций, условий эксплуатации,

33.2. учет наличия описания системы защиты,

33.3. контроль необходимости генерации описания системы защиты на варианты системы защиты, по которым такого описания нет,

34. Управление ответственными за обеспечение безопасности ПДн, включая:

34.1. учет подразделений или конкретных лиц, которые назначены ответственными за безопасность ИСПДн,

34.2. контроль необходимости назначения ответственных за безопасность ПДн в ИСПДн, по которым ответственные не назначены,

34.3. генерация формы приказа о назначении ответственных за безопасность ПДн в ИСПДн,

35. Управление актом о пропуске на территорию посетителей, включая:

35.1. ввод данных необходимых для генерации акта оператора о пропуске на территорию посетителей и ведении журнала (ответственных за ведение журнала, порядка пропуска субъекта ПДн на территорию, на которой находится оператор, без подтверждения подлинности ПДн сообщенных субъектом ПДн),

35.2. генерация формы акта оператора о пропуске на территорию посетителей и ведении журнала,

35.3. фиксация состава данных содержащихся в текущем акте оператора о пропуске на территорию посетителей,

35.4. контроль изменений в составе данных указываемых в акте (состава ответственных, порядка пропуска субъекта ПДн на территорию, на которой находится оператор, без подтверждения подлинности ПДн, сообщенных субъектом ПДн, целей обработки ПДн),

36. Управление СКЗИ и лицами, допущенными к СКЗИ, включая:

36.1. учет лиц, которых надо допустить к работе с криптосредствами, а также лиц, которые допущены к СКЗИ,

36.2. генерация формы приказа на допуск к работе с СКЗИ,

36.3. контроль наличия лиц, которых требуется допустить к работе с СКЗИ, но приказ для которых не сгенерирован,

36.4. учет лицевых счетов пользователей СКЗИ,

36.5. учет ключевых документов к СКЗИ,

36.6. учет проведения обучения по работе с СКЗИ,

37. Учет получения предписаний регулятора в области ПДн,

38. Управление Перечнем ПДн, включая:

38.1. генерация перечня персональных данных,

38.2. контроль необходимости актуализации перечня персональных данных по наличию изменений в составе обрабатываемых ПДн,

39. Управление Перечнем процессов обработки ПДн, включая:

39.1. генерация перечня процессов обработки ПДн,

39.2. контроль необходимости актуализации перечня процессов обработки персональных данных по наличию изменений в составе процессов обработки,

40. Управление Перечнем ИСПДн, включая:

40.1. генерация приказа об утверждении перечня ИСПДн,

40.2. контроль актуальности перечня ИСПДн,

41. Генерация отчета о степени выполнения законодательных требований к процессам обработки и защиты ПДн,

42. Управление правами доступа, включая:

42.1. задание состава пользователей,

42.2. задание правил назначения и смены паролей доступа,

42.3. задание ролей пользователей, обеспечение ограничения доступа пользователей по филиалам, доступным пунктам меню,

42.4. ограничение возможностей пользователей по степени владения активами, процессами, информационными массивами.

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 на проведение контроля защищенности ПДн и соблюдения условий использования средств защиты
4) Акта о проверке эффективности средств защиты
5) Акта оператора о пропуске на территорию посетителей и ведении журнала
6) Журнала учета применяемых средств защиты ПДн
7) Журнала учета установки и снятия средств защиты
8) Журнала учета эксплуатационной и технической документации
9) Журнала учета носителей ПДн
10) Журнала учета ключевых документов к СКЗИ
11) Модели угроз
12) Модели нарушителя
13) Описания системы защиты
14) Отчета о степени соответствия требованиям к процессам обработки и защиты ПДн
15) Перечня ПДн
16) Перечня процессов обработки ПДн
17) Перечня технических средств ИСПДн
18) Приказа на допуск к работе с СКЗИ
19) Приказа на ввод в эксплуатацию средств защиты

20) Приказа на проведение контроля защищенности ПДн и соблюдения условий использования средств защиты
21) Приказа о допуске лиц в помещения
22) Приказа о назначении ответственных за безопасность ПДн
23) Приказа о предоставлении доступа к персональным данным
24) Приказа об исключении доступа к персональным данным
25) Приказа об определении мест хранения различных категорий ПДн
26) Приказа об утверждении перечня ИСПДн
27) Согласия на обработку ПДн
28) Разъяснения порядка принятия решений при исключительно автоматизированной обработке и порядка защиты субъектом ПДн своих прав и законных интересов
29) Уведомления субъекта ПДн о характере процессов обработки его ПДн
30) Уведомления субъекта ПДн об отсутствии обрабатываемых ПДн
31) Уведомления, содержащего мотивированный отказ на запрос о предоставлении информации о характере обрабатываемых ПДн
32) Уведомления субъекта ПДн о результатах рассмотрения возражения на принятие решений несущих юридические последствия на основании исключительно автоматизированной обработки
33) Уведомления субъекта ПДн о предполагаемой обработке его ПДн
34) Уведомления об устранении нарушений или уничтожении ПДн по результатам проверки
35) 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 организации,
- состава и структуры структурных подразделений,
- состава и структуры бизнес-процессов,
- списка информационных массивов,
- списка сотрудников,
- списка активов,
- списка субъектов ПДн,
- списка допущенных к информационным массивам лиц,
- данных о контрагентах и договорах с ними,
- списка 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 массивах,
- 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.

.