LIS-SPS

v.2.5.0.0

ФУНКЦИОНАЛЬНАЯ СПЕЦИФИКАЦИЯ

68470160-05-2.5.0.0-35

2025 г.

Аннотация

Настоящий документ содержит описание функций, назначения, условий использования системы поддержки процессов обеспечения информационной безопасности (далее СПП ИБ).

В процессе использования комплекса решаются следующие задачи:

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

Содержание

Перечень сокращений

АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность
ИС	Информационная система
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СПП ИБ	Система поддержки процессов обеспечения информационной безопасности
ФИО	Фамилия, имя, отчество

1. Введение

1.1. Цели использования

Целью использования программного комплекса является:

- Автоматизация рутинных операций связанных с обработкой и обеспечением безопасности критичной информации.
- Выполнение требований законодательных актов в области информационной безопасности.
- Организация мониторинга изменений процессов обработки критичной информации.

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 ИБ.

Сервер приложений представляет собой web службу обеспечивающую связь между сервером баз данных и клиентом.

АРМ оператора представляет собой тонкий клиент (web-браузер) используемый на АРМ пользователей и администраторов системы.

1.3. Краткий обзор

Работа в СПП ИБ осуществляется в следующем общем алгоритме:

1. Ввод данных в СПП ИБ пользователями, либо загрузка данных из внешних систем.
2. Формирование требований к процессам защиты критичной информации, активов, информационных систем.
3. Автоматический анализ введенных данных, определение несоответствий в процессах обработки и защиты критичной информации.
4. Генерация необходимых документов в автоматизированном режиме, выполнение других действий по приведению процессов в соответствие.
5. Ввод данных об изменениях в процессах, системах – повтор шагов 1-4.
6. Ведение различных видов учетов необходимых для поддержания процессов информационной безопасности.

Система позволяет:

- Обеспечить автоматизированный ввод данных о структуре и составе процессов обработки защищаемой информации из разных подразделений в четко определенном формате.
- Обеспечить автоматическую загрузку и анализ данных из внешних источников – кадровых баз данных, систем инвентаризации технических средств, CRM и IDM систем и т.п.
- Использовать и корректировать множество справочников связанных с вопросами ИБ – категории информации, угрозы, контроли и функции защиты, средства и меры защиты и т.п.
- 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.

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

- в пользовательских структурных подразделениях, участвующих в процессах обработки и защиты информации,
- в ИТ подразделениях,
- в подразделениях ответственных за вопросы ИБ.

Внедрение программного комплекса предполагает разные сценарии использования, например, следующий режим работы (при необходимости, функции могут быть распределены произвольно):

- на АРМ ответственных, в случае изменения процессов обработки защищаемой информации, либо в случае появления новых активов, процессов, носителей осуществляется ввод учетных данных в СПП ИБ;
- на АРМ ИТ отделов осуществляется ввод данных о составе серверов, сетевого оборудования, баз данных, архитектуре ИС, либо импорт осуществляется из внешних систем;
- на АРМ ИТ отделов осуществляется генерация документации по защите информации находящейся в области ответственности ИТ, например, журналов учета средств защиты, журналов учета технических средств и т.п.;
- на АРМ отделов ответственных за вопросы ИБ, по введенным данным, осуществляется выявление несоответствий, выработка требований к ИБ, генерация документов в области ИБ.

Система поддержки процессов обеспечения информационной безопасности «LIS-SPS» имеет следующие основные показатели:

- включает более 150 функций по контролю процессов обработки и защиты критичной информации, вводу данных и генерации документов,

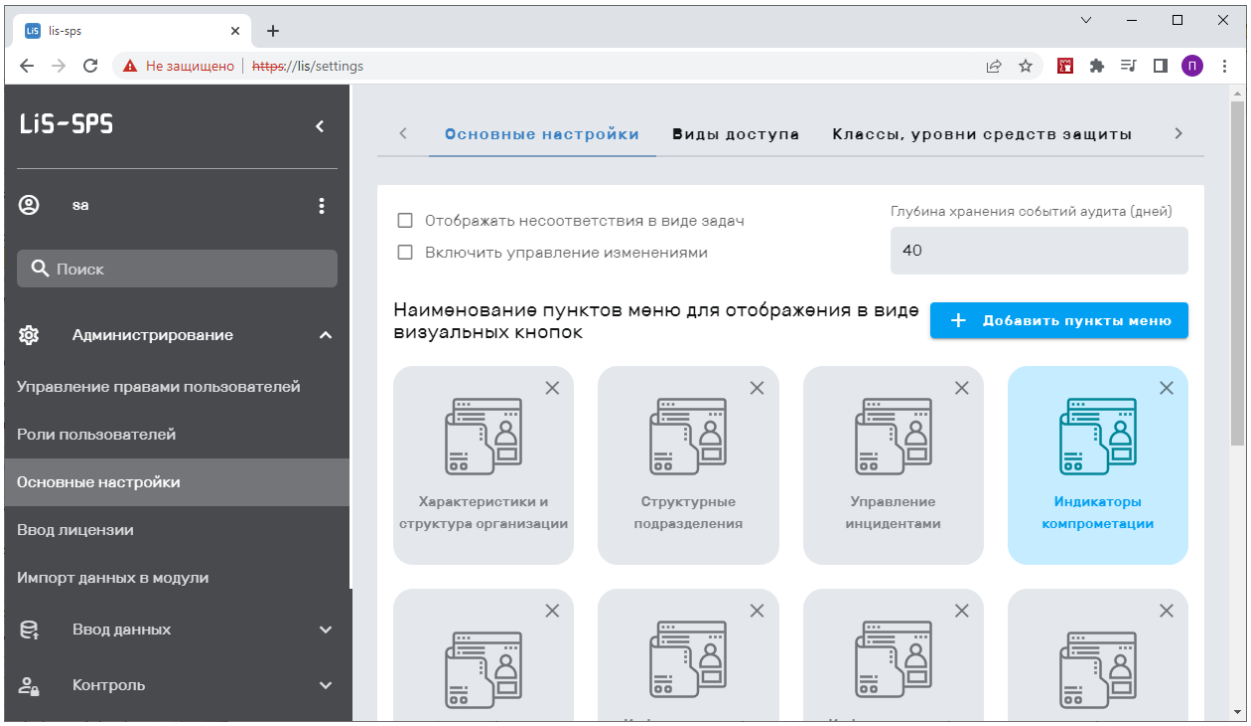
- позволяет произвести более 30 готовых видов проверок процессов на соответствие требованиям в области информационной безопасности.

Система позволяет эффективно организовать поддержку процессов обработки и защиты критичной информации, как собственными силами, так и в случае выделения некоторых функций для аутсорсинга. В последнем случае заказчик выделяет клиентское место СПП ИБ аутсорсеру, который может осуществлять выполнения возложенных на него задач (например, учет СЗИ, обработку инцидентов и т.п.) удаленно.

2. Описание комплекса

2.1. Функции комплекса

СПП ИБ обеспечивает реализацию следующих основных функций:



1. **Задание общих справочников**
   - 1.1. Учет выделенных организаций, подразделений (филиалов, представительств)
   - 1.2. Учет структурных подразделений с учетом их иерархии
   - 1.3. Учет различных категорий информации
2. **Визуализация данных**
   - 2.1. Построение графиков, схем по любым данным системы
   - 2.2. Возможность гибкой настройки состава отображаемых данных

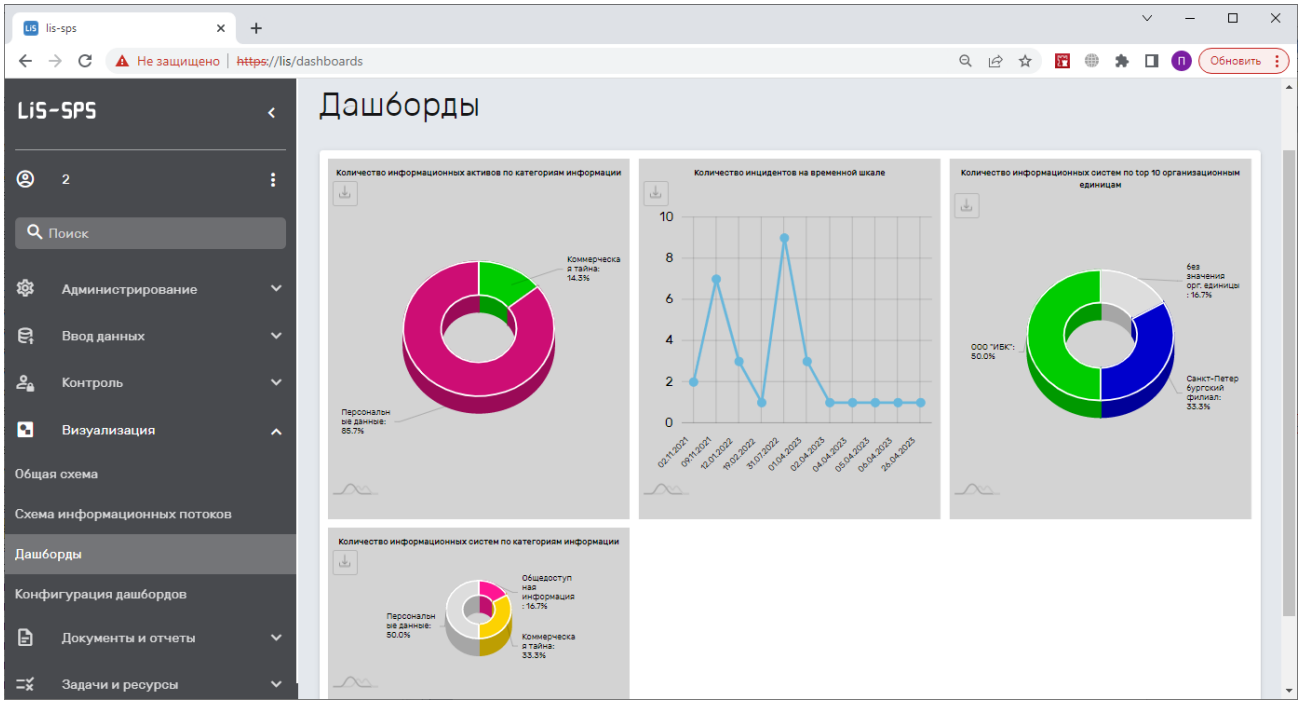


Рисунок 1 - Пример интерфейса «Дашборды»

3. Управление контрагентами, включая:

3.1. Учет контрагентов и договоров контрагентов

3.2. Учет контрагентов, с которыми заключены соглашения о конфиденциальности

3.3. Учет дат получения и истечения срока соглашений о конфиденциальности

3.4. Автоматический контроль истечения срока соглашений о конфиденциальности до окончания срока действия договора

3.5. Автоматический контроль наличия соглашений о конфиденциальности

4. Управление информационными системами

4.1. Задание произвольного справочника категорий ИС (платежные системы, системы обработки финансовой отчетности и т.п.)

4.2. Задание произвольного справочника характеристик ИС (различные статусы, классы, группы и т.п.),

4.3. Задание произвольного справочника ключевых дат связанных с ИС (даты ввода в эксплуатацию, вывода из эксплуатации, проведения испытаний и т.п.)

4.4. Учет перечня ИС с заданием их категорий, владельцев, описания, произвольных характеристик, вложенности и ключевых дат (учета, ввода в эксплуатацию, вывода и т.п.)

4.5. Учет сведений о результатах прохождения процедур подтверждения соответствия в отношении ИС (в том числе, аттестации на соответствие требованиям по информационной безопасности)

4.6. Обеспечение возможности импорта сведений об информационных системах из внешних систем

4.7. Возможность использования развитых механизмов фильтрации ИС по множеству их характеристик

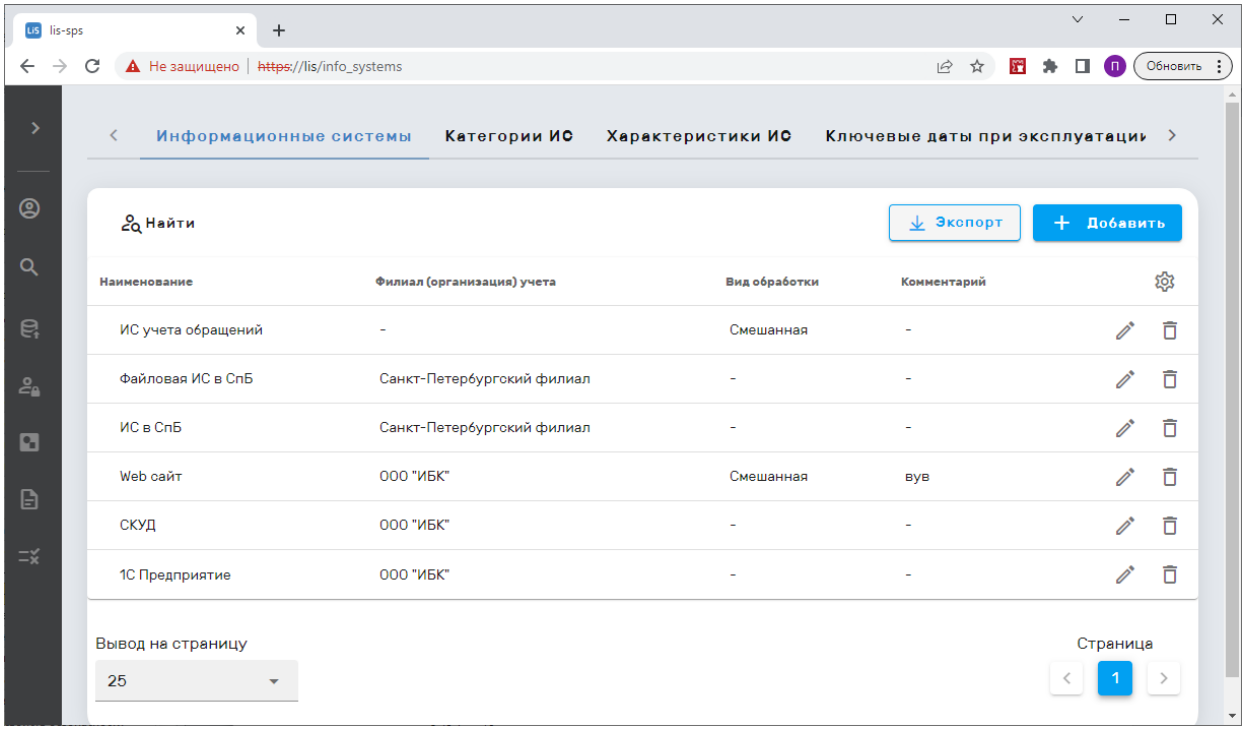


Рисунок 2 - Пример интерфейса «Информационные системы»

5. Управление процессами обработки защищаемой информации

5.1. Учет состава и иерархии процессов обработки защищаемой информации

5.2. Учет структурных подразделений участников процесса и владельцев процесса

5.3. Учет структуры и состава информационных потоков процесса посредством задания различных пар источников и получателей информационных активов, включающих контрагентов, информационные и технические активы, программное обеспечение, структурные подразделения, категории физических лиц и т.п.

5.4. Возможность визуализации информационных потоков на схеме, редактирования потоков непосредственно в визуальной форме.

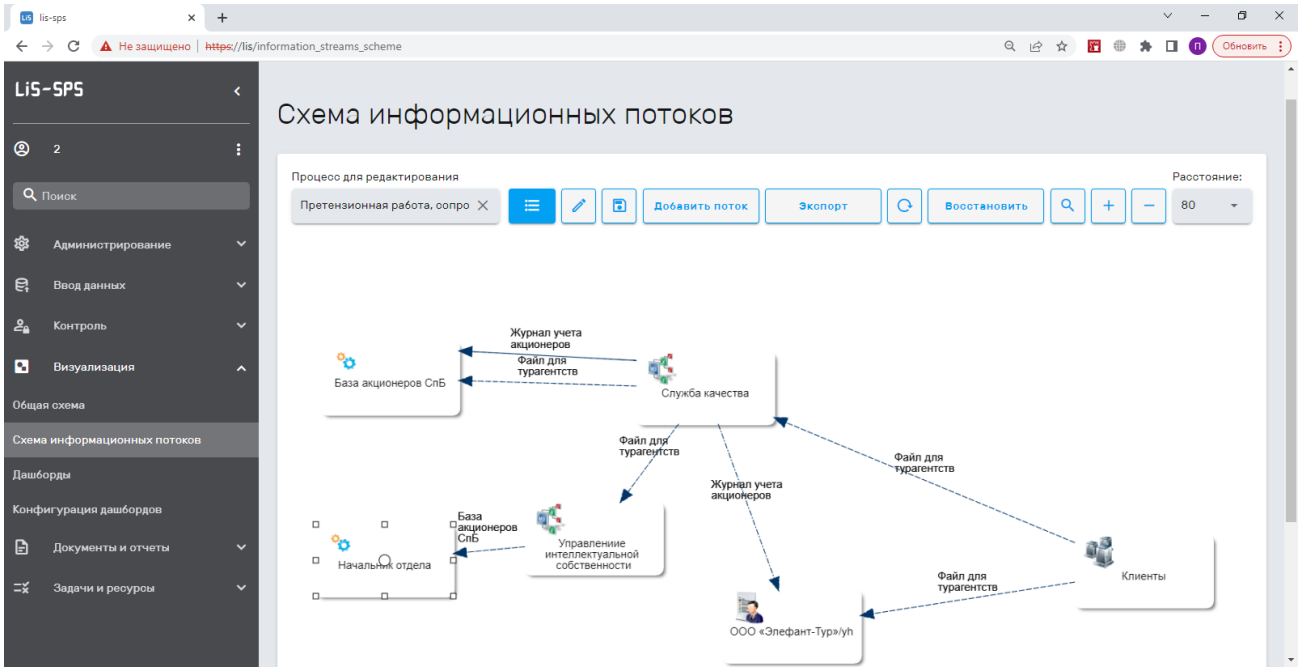


Рисунок 3 - Пример визуализации «Схема информационных потоков»

5.5. Обеспечение возможности согласования каждой версии процесса ответственными лицами с использованием механизмов электронной подписи

5.6. Возможность использования развитых механизмов фильтрации процессов по множеству их характеристик

5.7. Ведение справочника внешних нормативных документов

5.8. Ведение справочника внутренних нормативных документов

6. Управление ролями

6.1. Задание произвольных ролей

6.2. Задание структурных подразделений, которые назначены на роли

6.3. Задание конкретных физических лиц, которые назначены на данные роли

6.4. Задание ИС, в отношении которых назначены роли

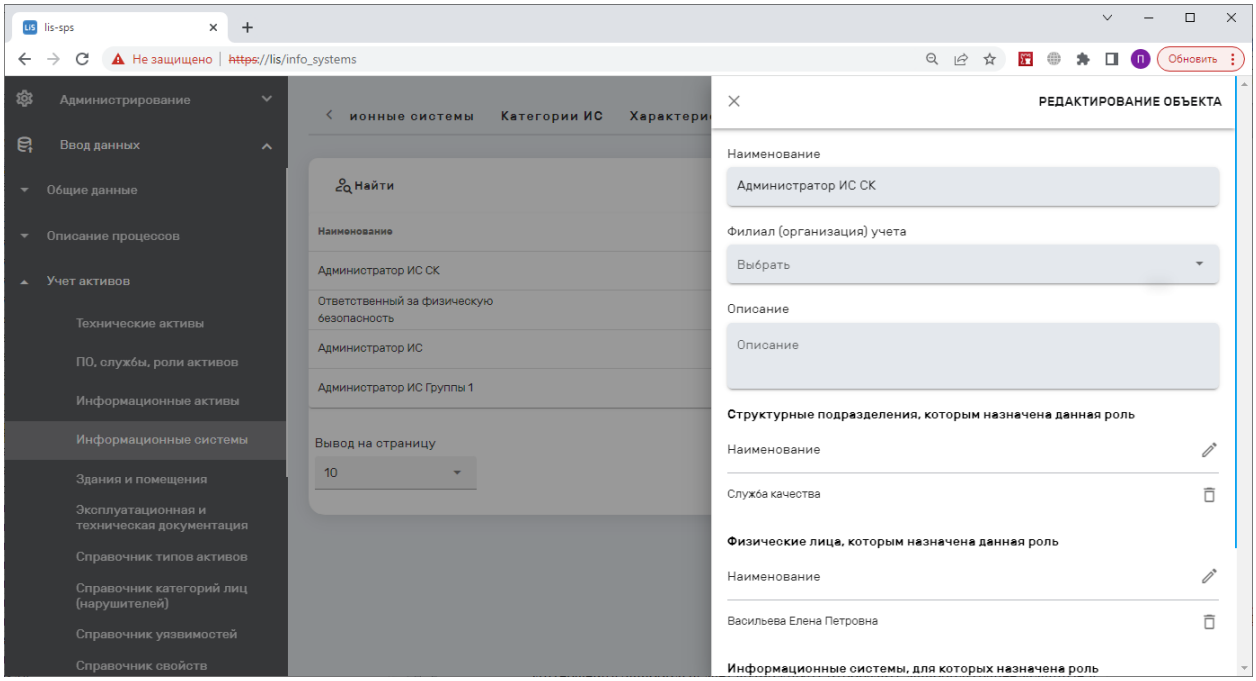


Рисунок 4 - Пример интерфейса «Роли»

7. Перечень сведений конфиденциального характера

7.1. Учет «Перечня сведения конфиденциального характера» в виде списка конфиденциальных сведений (групп сведений)

8. Управление физическими лицами, участвующими в обеспечении ИБ

8.1. Учет ФИО, паспортных данных физических лиц

8.2. Учет для сотрудников структурного подразделения, должности, офиса, где работает (при необходимости)

8.3. Возможность использования развитых механизмов поиска физических лиц по множеству критериев

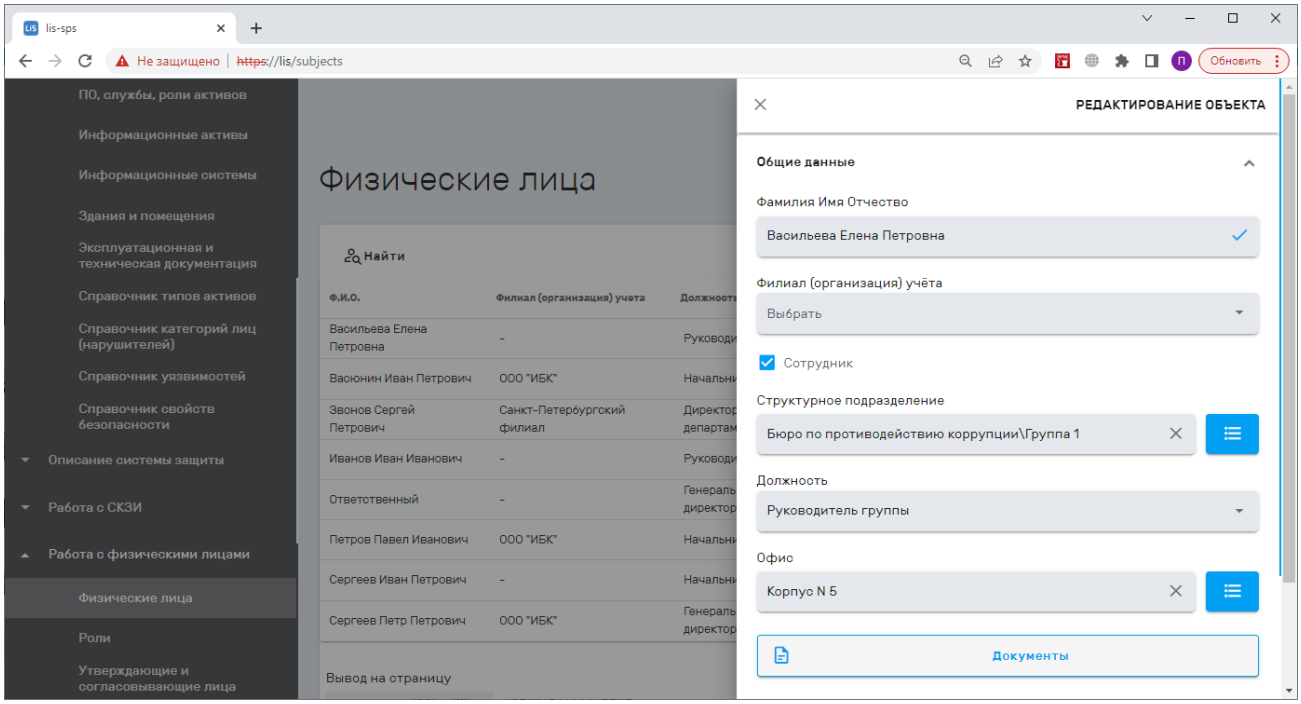


Рисунок 5 - Пример интерфейса «Физические лица»

9. Управление информационными активами

9.1. Учет информационных активов (баз данных, файлов, бумажных документов, сервисов и т.п.), категорий обрабатываемой в них информации, связанных процессов, произвольных характеристик

9.2. Учет структурных подразделений и/или физических лиц – владельцев информационных активов

9.3. Возможность использования развитых механизмов фильтрации информационных активов по множеству критериев и экспорта данных в файлы формата MS Excel

9.4. Задание различных видов ущерба, который может быть нанесен активу при нарушении свойств безопасности

10. Учет лиц допущенных к активам

10.1. Учет ролей, лиц и пар «должность» - «структурное подразделение», которым предоставляется доступ к заданным активам (информационной системе, техническому или информационному активу)

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

10.3. Учет конкретных прав доступа назначенных пользователю в отношении активов и/или дополнительных объектов доступа (чтение, запись, удаление и т.п.)

10.4. Генерация формы матрицы доступа к активам

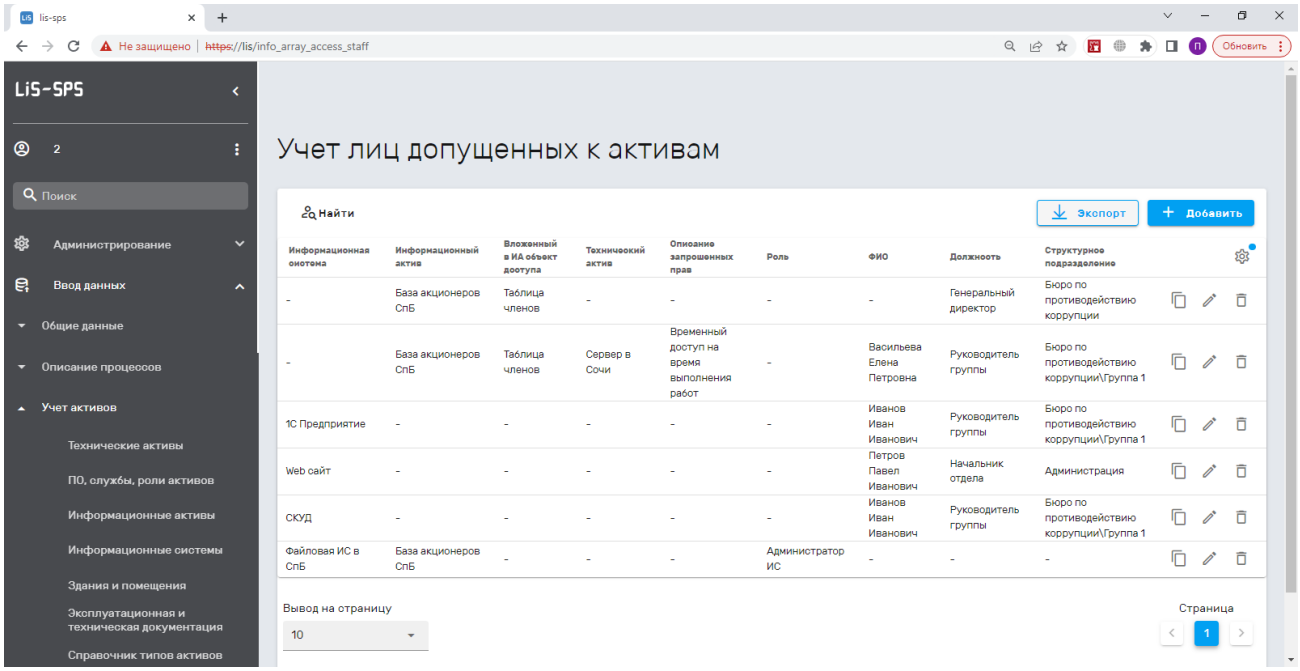


Рисунок 6 - Пример интерфейса «Учет лиц допущенных к активам»

11. Управление зданиями и помещениями

11.1. Учет состава зданий и помещений, в которых производится обработка критичной информации (как автоматизированная, так и неавтоматизированная)

11.2. Учет наличия в помещениях средств криптографической защиты информации

11.3. Учет наличия лиц допущенных в помещения

11.4. Учет структурных подразделений – владельцев данных помещений

11.5. Учет выполнения требований по защите помещений, в которых производится обработка критичной информации (наличие замков, решеток на окнах, надежных хранилищ для бумажных носителей конфиденциальной информации при их неавтоматизированной обработке)

11.6. Автоматический контроль выполнения мер защиты помещений, в которых производится обработка конфиденциальной информации посредством анализа внесенной информации о состоянии защиты помещений, наличия информационных активов, характеристик расположения помещения (выход окон за пределы контролируемой зоны, возможность наличия посторонних лиц и т.п.)

11.7. Учет выполнения требований по защите помещений, в которых находятся СКЗИ

11.8. Автоматический контроль выполнения мер защиты помещений, в которых находятся СКЗИ (наличие надежных дверей, охранной сигнализации, приспособлений для опечатывания и т.п.)

11.9. Возможность использования развитых механизмов фильтрации зданий и помещений по множеству критериев и экспорта в файлы формата MS Excel

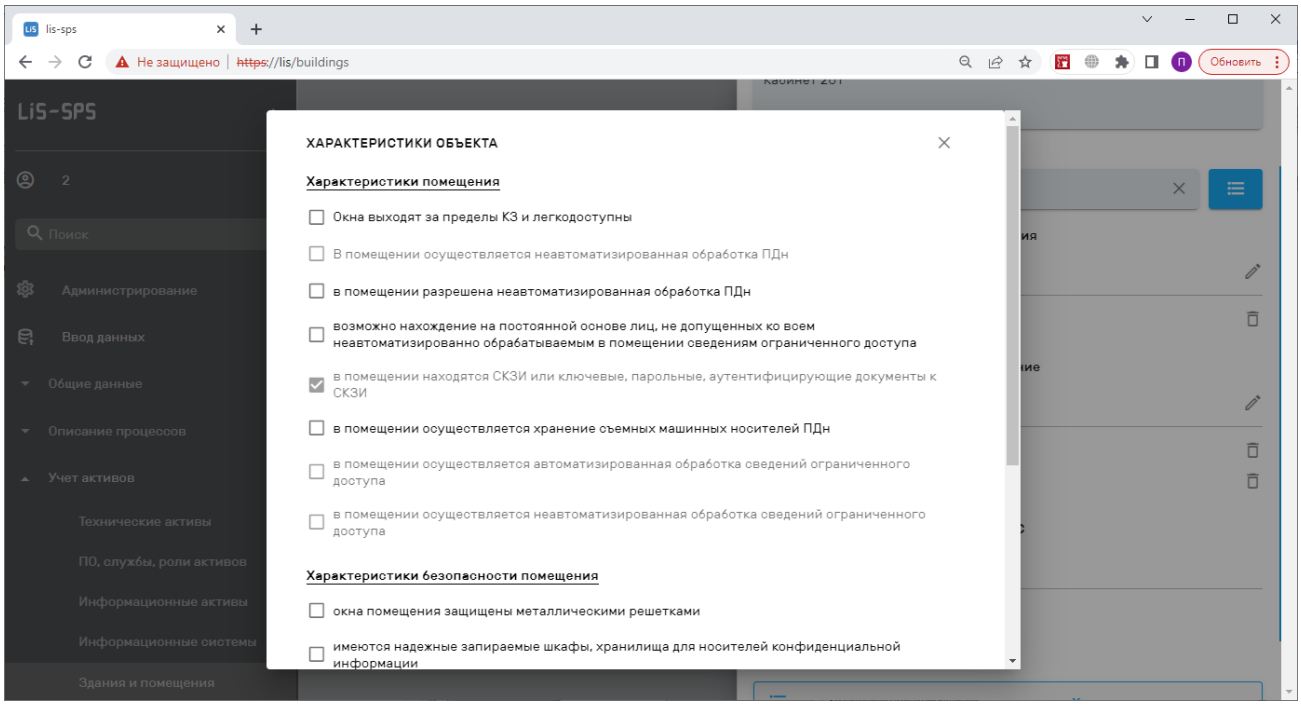


Рисунок 7 - Пример интерфейса «Здания и помещения»

12. Управление техническими активами

12.1. Учет технических активов используемых для обработки значимой информации, обрабатываемых на них категорий информации, мест их размещения, содержащихся на них информационных активов и информационных активов, к которым производится обращение, режимов обработки и т.п.

12.2. Возможность задания справочников произвольных характеристик технических активов.

12.3. Задание процессов, в которых участвует актив

12.4. Учет структурных подразделений и/или физических лиц – владельцев активов

12.5. Возможность задания программного обеспечения установленного на активах

12.6. Возможность использования развитых механизмов фильтрации активов по множеству критериев и экспорта в файлы формата MS Office

12.7. Задание различных видов возможного ущерба, который может быть нанесен активу при нарушении свойств безопасности

13. Управление моделями угроз

13.1. Задание (выбор, исключение) возможных угроз безопасности ИС, их вероятностей, условий актуальности

13.2. Автоматический контроль необходимости генерации модели угроз на вновь созданные ИС

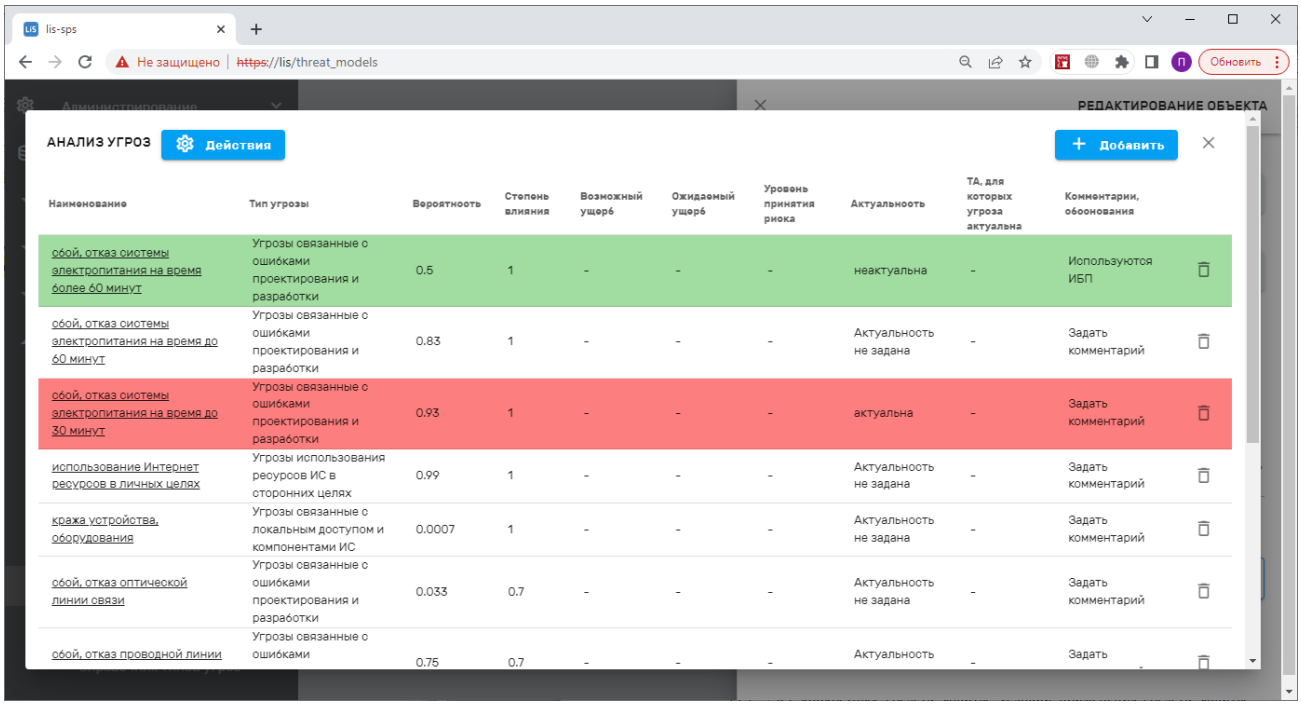


Рисунок 8 - Пример интерфейса «Модель угроз»

14. Управление средствами защиты

14.1. Учет конкретных средств защиты, условий применения средств защиты для обеспечения безопасности активов

14.2. Учет имеющихся экземпляров 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, произвольных характеристик

14.3. Учет фактических мест и времени установки средств защиты (ведение журнала истории установки средств защиты на конкретных активах) с использованием механизмов электронной подписи

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

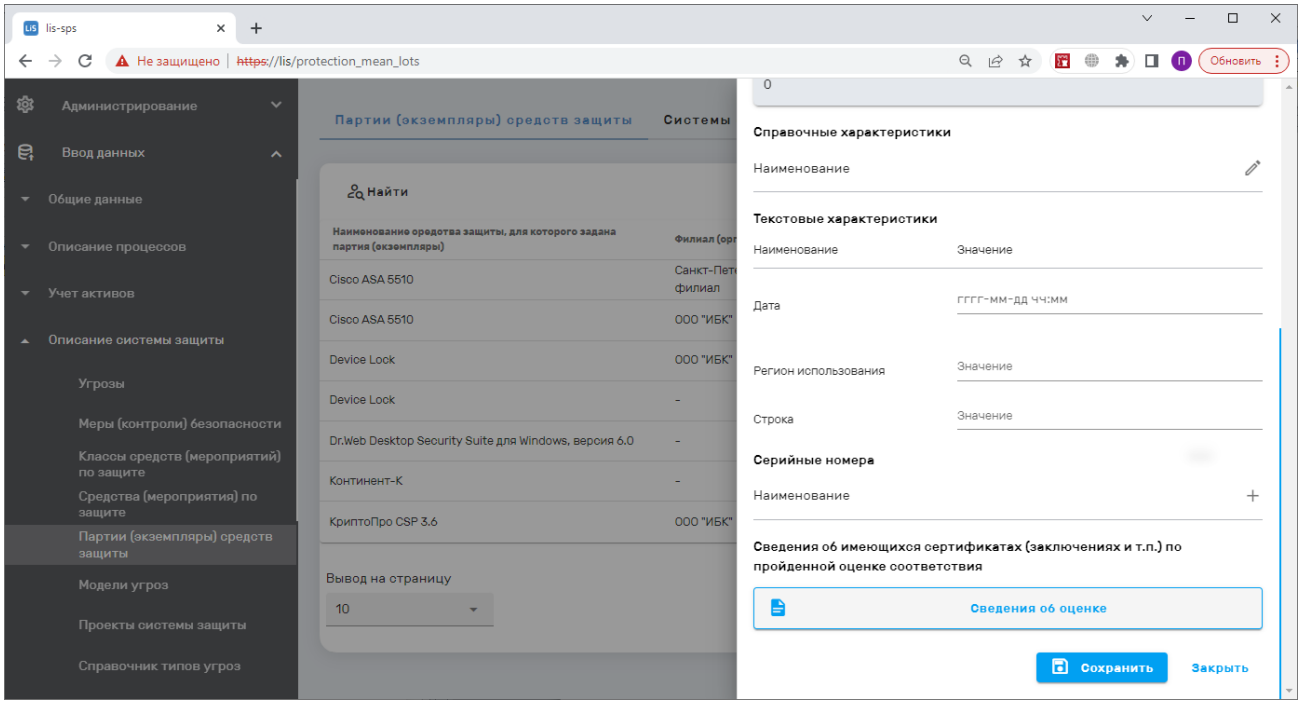


Рисунок 9 - Пример интерфейса «Партии (экземпляры) средств защиты»

15. Управление проектами на систему защиты

15.1. Ведение справочника мер (контролей), зависимости мер от категорий ИС, характеристик активов

15.2. Задание проекта системы – состава средств защиты для выбранного множества ИС и/или активов и/или процессов с учетом модели угроз, заданных ранее характеристик данных активов (ИС), характеристик средств защиты

15.3. Предоставление возможности автоматической фильтрации необходимых мер защиты в зависимости от характеристик ИС, результатов классификации ИС

15.4. Предоставление механизмов поддержки принятия решений по выбору средств и мероприятий защиты, подходящих для реализации выбранных мер защиты

16. Управление проведением контроля (аудита) защищенности

16.1. Определение активов, процессов, ИС, зданий и помещений, подразделений, для которых будет проводиться аудит (контроль) защищенности

16.2. Определение области проведения аудита – применяемые средства (мероприятия) защиты, условия эксплуатации средств защиты, реализация мер защиты, исправление уязвимостей, состоянии характеристик обработки в процессах обработки информации и т.п.

16.3. Автоматический подбор списка контролей для проведения аудита, в зависимости от выбранной области аудита, на основании данных о проекте системы защиты, характеристиках активов и т.п.

16.4. Ввод по каждому проверяемому параметру результата проверки, оценки степени выполнения, комментариев

16.5. Автоматический расчет уровня зрелости проверенных процессов

16.6. Генерация приказа на проведение аудита защищенности

16.7. Генерация акта аудита (контроля) защищенности с результирующими данными

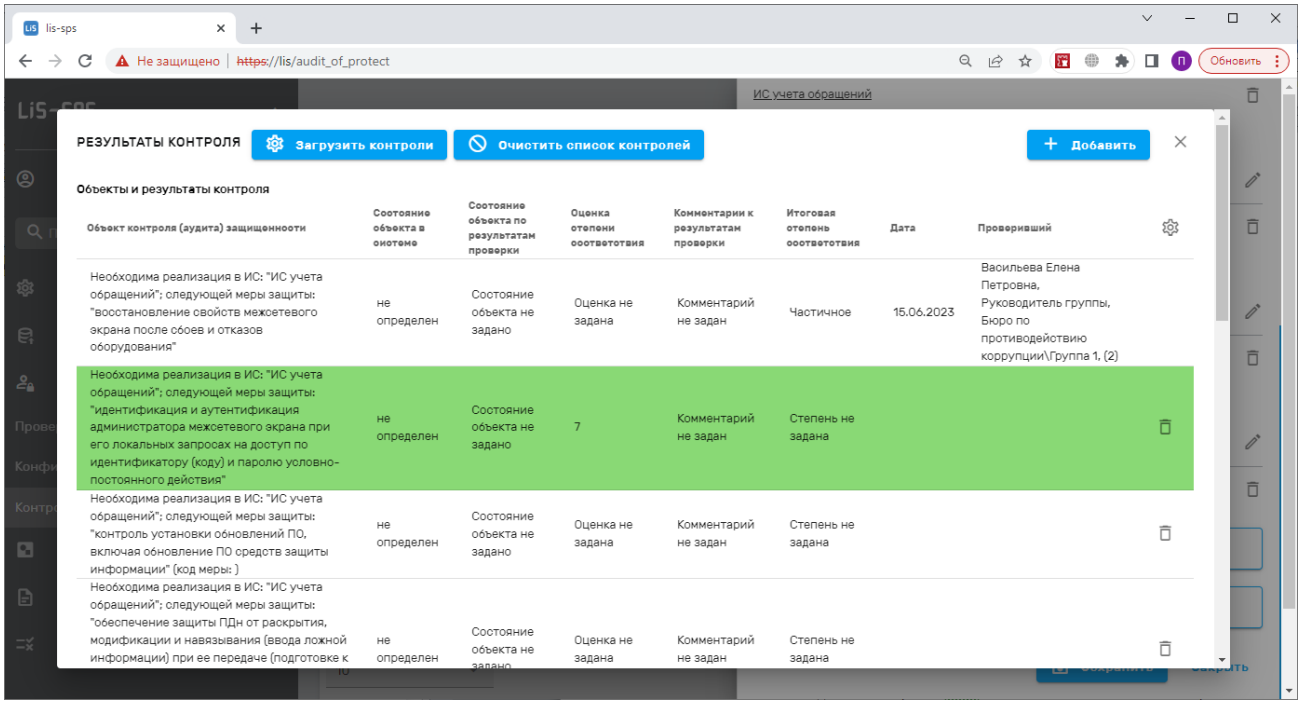


Рисунок 10 - Пример интерфейса «Контроль (аудит) защищенности»

17. Управление уязвимостями

17.1. Ведение справочника уязвимостей с произвольным набором характеристик

17.2. Возможность задания уязвимостей активов

17.3. Учет сведений об исправлении уязвимостей на конкретных активах с использованием электронной подписи

18. Управление документами

18.1. Ввод состава утверждающих и согласующих лиц по каждому виду документов, в том числе, генерируемых с использованием комплекса с учетом сложного состава структурных подразделений, наличия филиалов

18.2. Обеспечения возможности согласования и утверждения документов в электронной форме с обеспечением механизмов электронной подписи

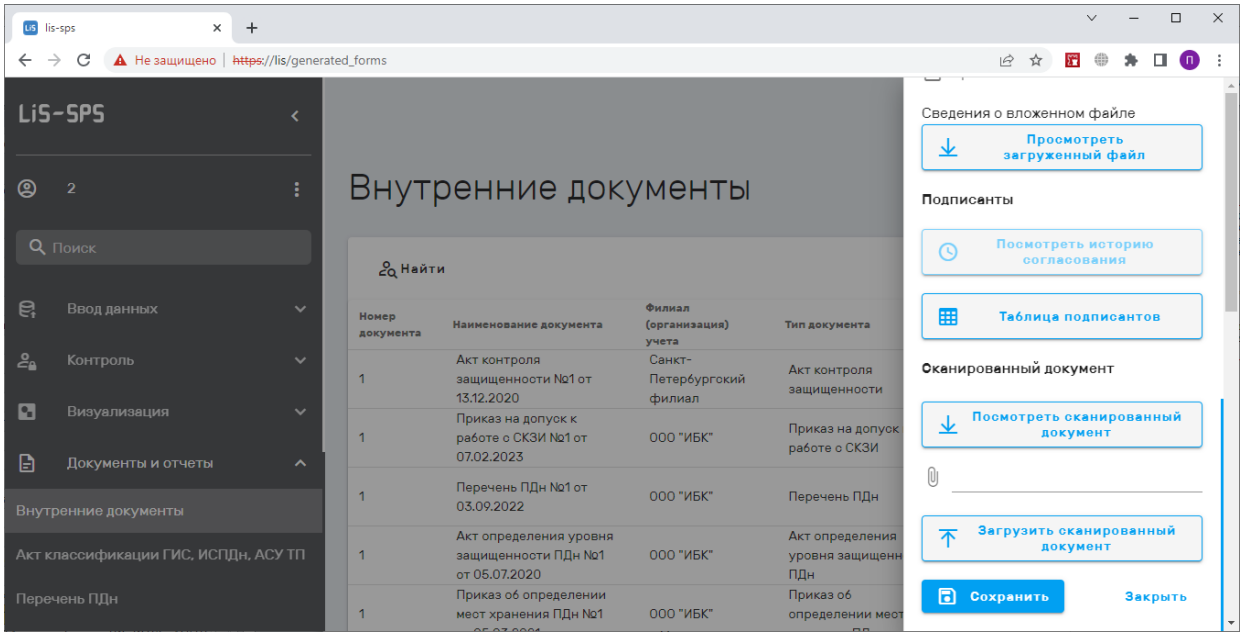


Рисунок 11 - Пример интерфейса «Внутренние документы»

18.3. Обеспечение возможности редактирования шаблонов документов во встроенном редакторе шаблонов.

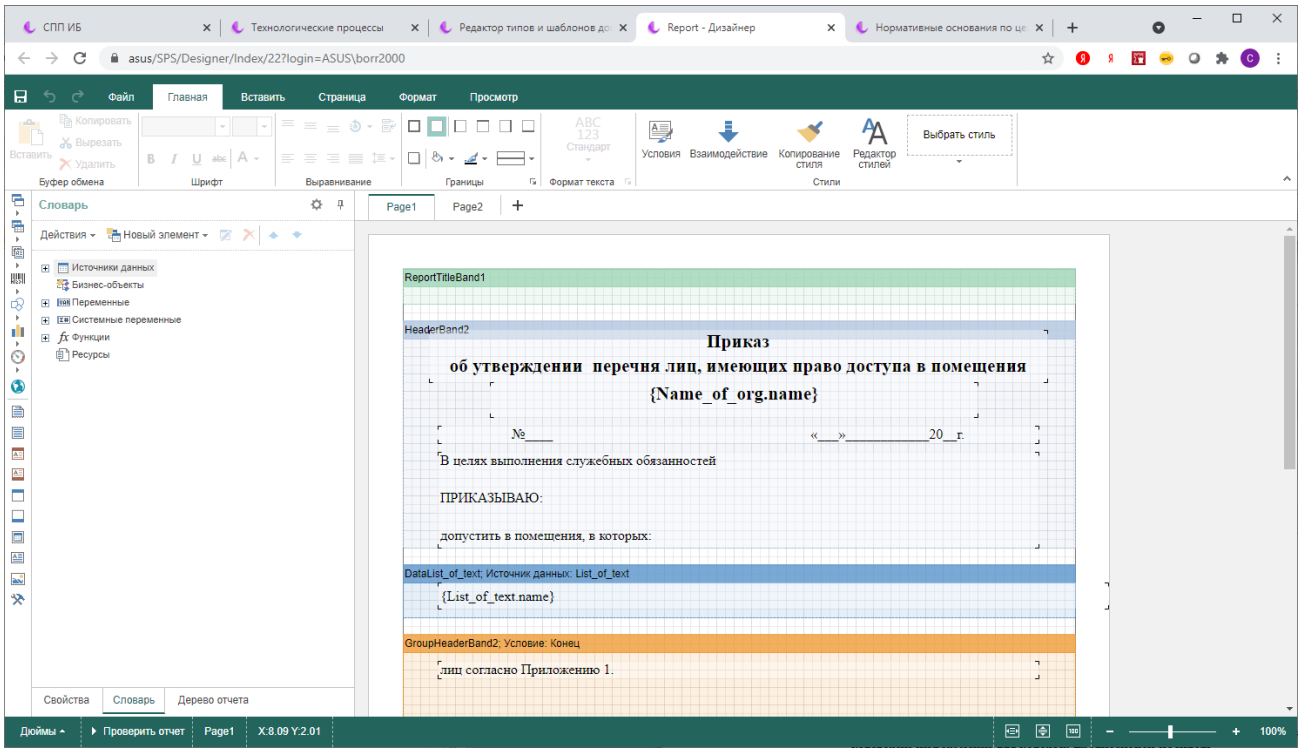


Рисунок 12 - Пример интерфейса редактора

19. Управление носителями конфиденциальной информации

19.1. Задание типов, номеров носителей

19.2. Задание физического лица – пользователя носителя, даты учета носителя, категорий информации для которых предназначен носитель

19.3. Простановка отметки, с использованием электронной подписи, о получении носителя пользователем, возвращении носителя, изъятии носителя

20. Управление инцидентами

20.1. Учет инцидентов, атак, даты происшествия, описания результатов их расследования, подверженных активов, ПО, ИС, ответственных за их расследование, связанных инцидентов

20.2. Учет документов связанных с нештатной ситуацией

20.3. Задание угроз, уязвимостей, которые привели к нештатной ситуации, связанных индикаторов компрометации

20.4. Задание шаблонов (типовых) реакций на те или иные характеристики инцидентов с предварительным заданием списка и характеристик задач, которые должны быть автоматически поставлены при срабатывании инцидента

20.5. Задание произвольных справочных и текстовых характеристик

20.6. Автоматическое создание задач по инцидентам

20.7. Получение инцидентов из внешних источников

20.8. Ведение чата по конкретным инцидентам

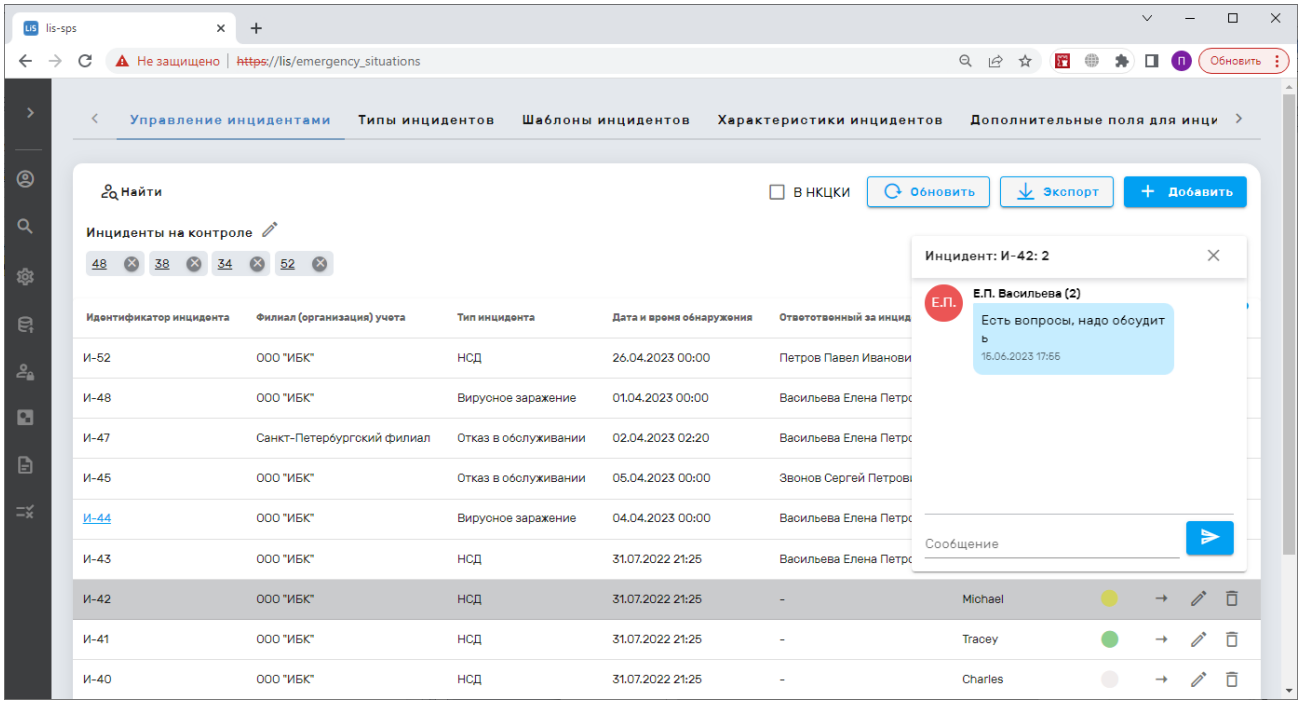


Рисунок 13 - Пример интерфейса «Управление инцидентами»

21. Организация взаимодействия с НКЦКИ

21.1. Обеспечение возможности взаимодействия как для субъекта КИИ, так и сторонних центров ГосСОПКА

21.2. Обеспечение возможности передачи данных об инцидентах, атаках, уязвимостях

21.3. Ведение чата с представителями НКЦКИ

21.4. Возможность передачи как общих, так и детальных технических данных

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

22.1. Учет лиц, которых надо допустить к работе с криптосредствами, а также лиц, которые допущены к СКЗИ

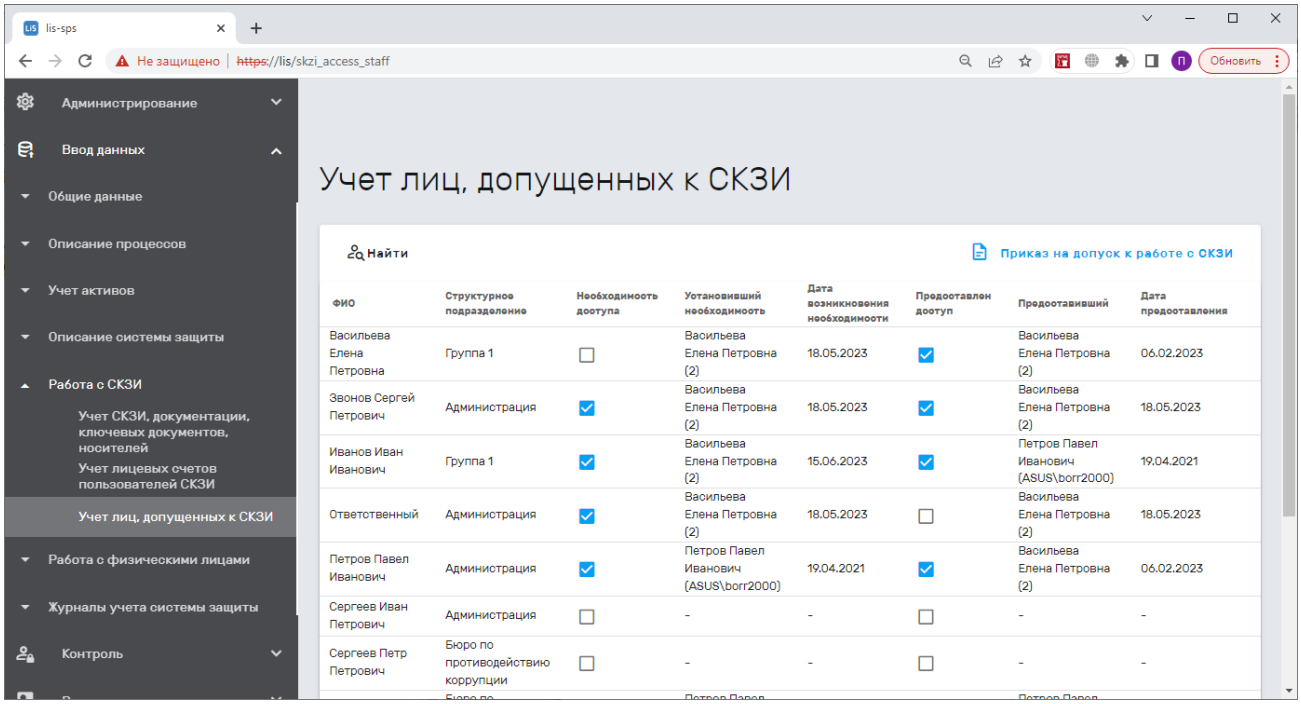


Рисунок 14 - Пример интерфейса «Учет лиц допущенных к СКЗИ»

22.2. Генерация формы приказа на допуск к работе с СКЗИ

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

22.4. Ведение лицевых счетов пользователей СКЗИ

22.5. Ведение СКЗИ, ключевых документов к СКЗИ

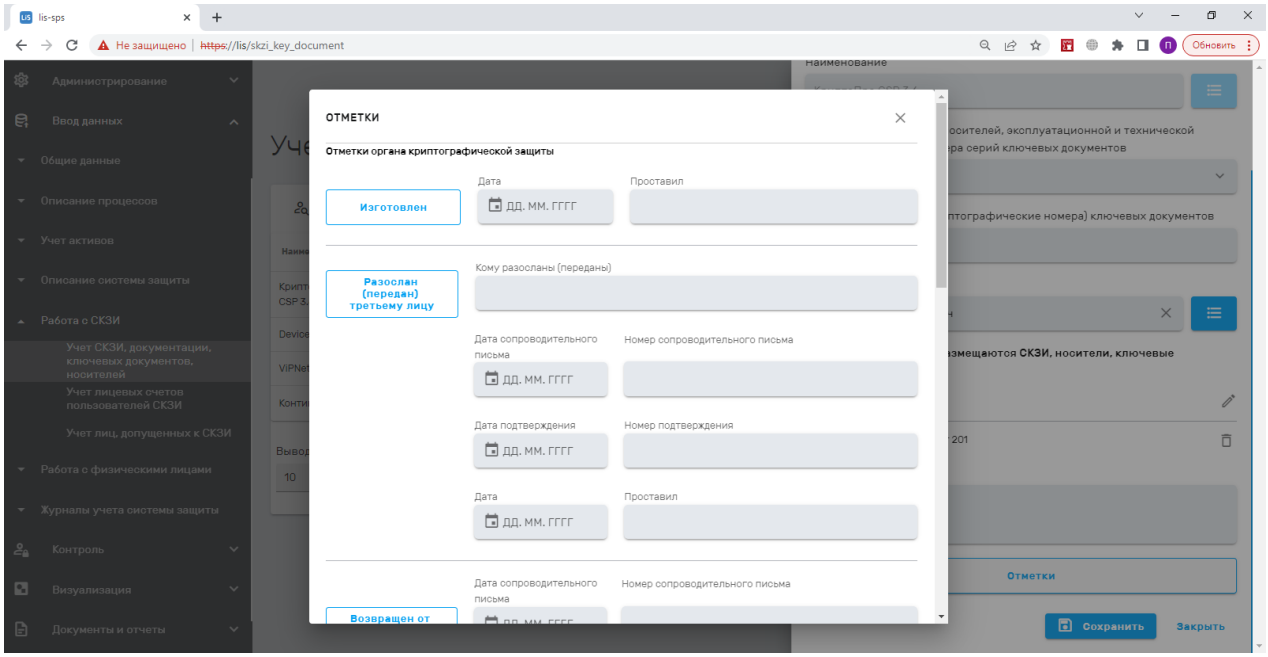


Рисунок 15 - Пример интерфейса «Учет СКЗИ, ключевых документов»

23. Управление задачами и ресурсами

23.1. Задание задач, иерархии задач, описания, дат начала и окончания, длительности, трудоемкости, статуса, вложенных файлов, приоритета, периодичности, процента готовности, ответственных за задачу физических лиц

23.2. Взаимная автоматическая коррекция длительности, сроков задачи, в том числе для вышестоящих задач

23.3. Автоматическое внесение выявленных несоответствий как отдельных задач

23.4. Поддержка механизмов оповещения пользователей об изменениях в задачах

23.5. Ведение истории изменения задачи

23.6. Фиксация каждого изменения задачи с использованием электронной подписи

23.7. Возможность использования развитых механизмов фильтрации задач по множеству критериев

23.8. Расчет нагрузки на ответственных по назначенным задачам

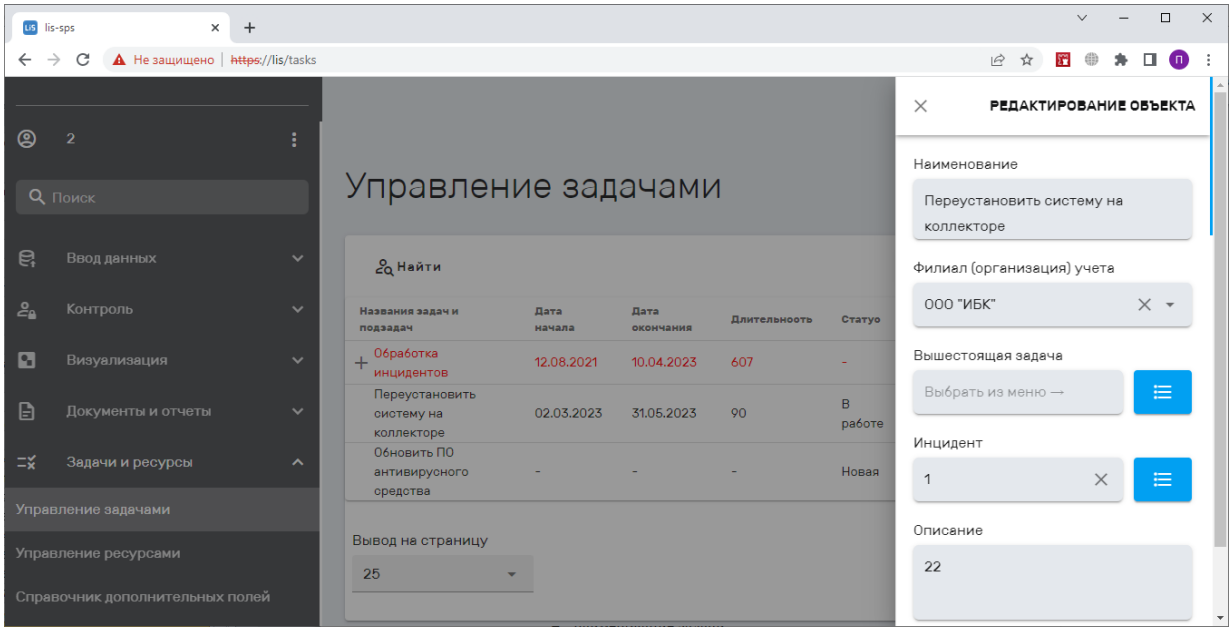


Рисунок 16 - Пример интерфейса «Управление задачами»

24. Управление запросами на изменение

24.1. Учет запросов на изменение технических средств, информационных активов, процессов

24.2. Запросы на изменение предполагают задание характеристик технических средств, информационных активов, описания процессов, которые они получат после модернизации.

24.3. Согласование запроса лицами, указанными в составе согласующих, а также владельцами актива, процесса

24.4. Фиксация сведений о запросе, согласовании, реализации, обновлении данных с использованием электронной подписи

25. Управление правами доступа

25.1. Задание состава пользователей

25.2. Задание правил назначения и смены паролей доступа

25.3. Задание ролей пользователей, обеспечение ограничения доступа пользователей по филиалам, доступным пунктам меню, выполняемым операциям (создание записи, удаление записи, редактирование записи, просмотр записей)

25.4. Ограничение возможностей пользователей по степени владения техническими средствами, процессами, информационными активами

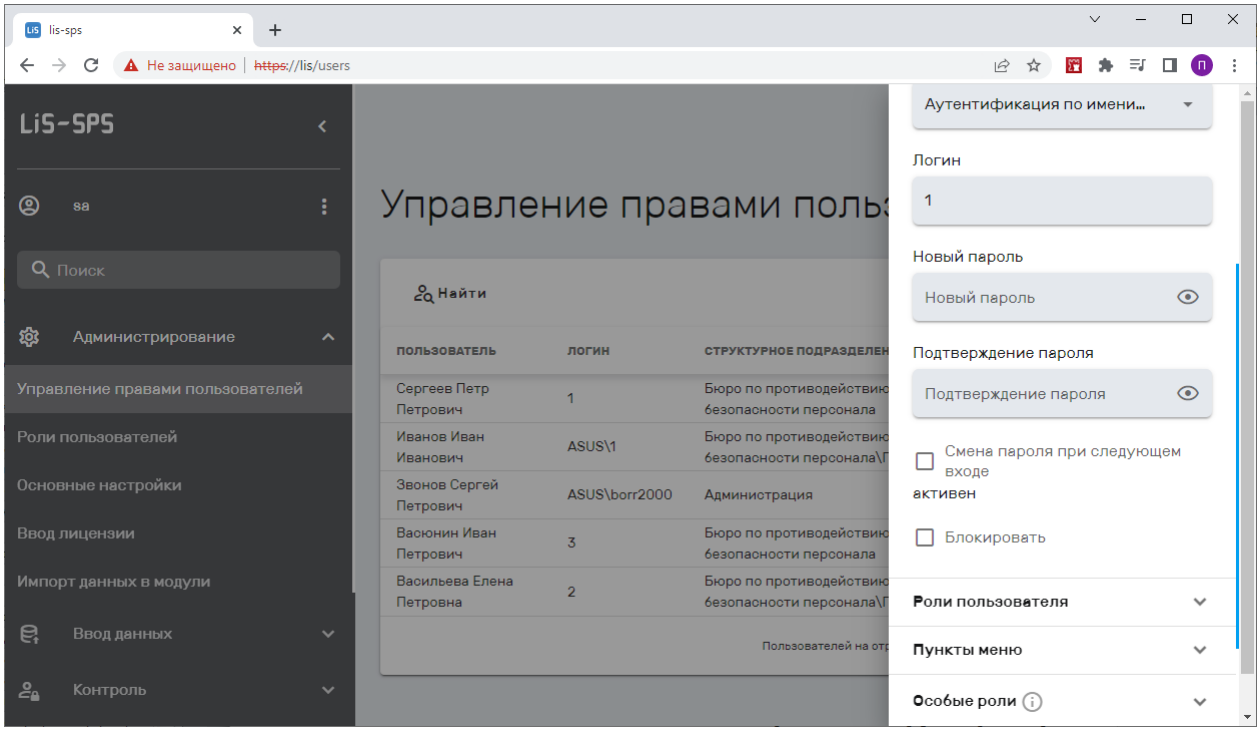


Рисунок 17 - Пример интерфейса «Управление правами доступа»

2.2. Внешние интерфейсы

Внешние интерфейсы предназначены для автоматизации процедур загрузки и синхронизации данных из внешних баз данных (интерфейсы импорта и синхронизации).

Внешние интерфейсы импорта и синхронизации СПП ИБ осуществляют:

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

Настройка внешних интерфейсов реализуется через графический интерфейс пользователем.

СПП ИБ имеет возможность импорта и синхронизации множества видов данных из внешних систем, в том числе:

- данных об инцидентах,
- индикаторов компрометации,
- филиалов и организаций,
- структурных подразделений,
- технологических процессов,
- информационных активов,

- физических лиц,
- технических активов,
- допущенных к активам лиц,
- данных о контрагентах и договорах с ними и т.п.

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

- REST API,
- базы данных MS SQL Server 2008 Standard Edition или выше,
- базы данных Oracle,
- файлы формата .CSV.

.