LIS-SPS

v.2.0.0.2

ФУНКЦИОНАЛЬНАЯ СПЕЦИФИКАЦИЯ

68470160-05-2.0.0.2-35

2016 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

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 службу MS IIS 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 следующий обобщенный режим работы (при необходимости, функции могут быть распределены произвольно) при выполнении мероприятий в области ИБ:

- на АРМ пользовательских подразделений, в случае изменения процессов обработки защищаемой информации, либо в случае появления новых активов, процессов, носителей осуществляется ввод учетных данных в СПП ИБ, простановка отметок о прохождении обучения и т.п.;
- на АРМ ИТ отделов осуществляется ввод данных о составе серверов, сетевого оборудования, баз данных, архитектуре ИС;
- 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, разработка моделей угроз, генерация документов в области ИБ – моделей угроз, актов классификации и т.п.

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,

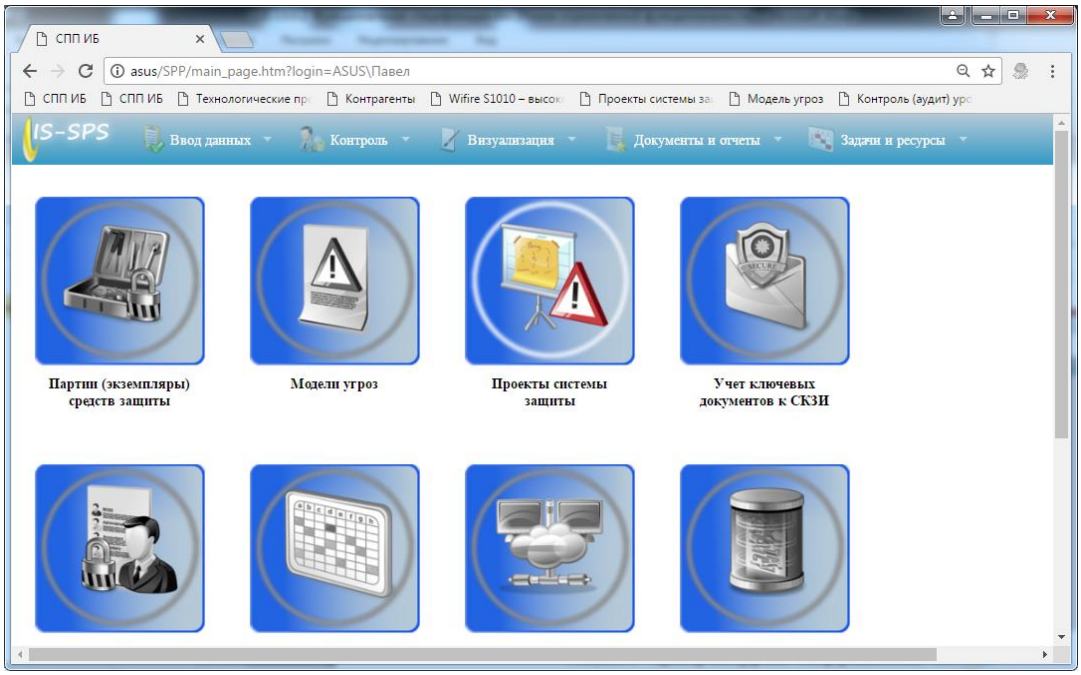
- позволяет осуществить генерацию порядка 20 видов документов,
- позволяет произвести более 30 видов проверок процессов на соответствие требованиям в области информационной безопасности.

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, генерацию модели угроз, варианта системы защиты 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 подразделений (филиалов, представительств)
   - 1.2. Учет структурных подразделений с учетом их иерархии
   - 1.3. Учет различных категорий информации
   - 1.4. Ведение справочника внешних нормативных документов
   - 1.5. Ведение справочника внутренних нормативных документов
2. **Управление контрагентами, включая:**
   - 2.1. Учет контрагентов и договоров контрагентов
   - 2.2. Учет контрагентов, с которыми заключены соглашения о конфиденциальности
   - 2.3. Учет дат получения и истечения срока соглашений о конфиденциальности
   - 2.4. Автоматический контроль истечения срока соглашений о конфиденциальности до окончания срока действия договора
   - 2.5. Автоматический контроль наличия соглашений о конфиденциальности
3. **Управление информационными системами**
   - 3.1. Задание произвольного справочника категорий ИС (платежные системы, системы обработки финансовой отчетности и т.п.)

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

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

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

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

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

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

3.8. Генерация технического паспорта ИС

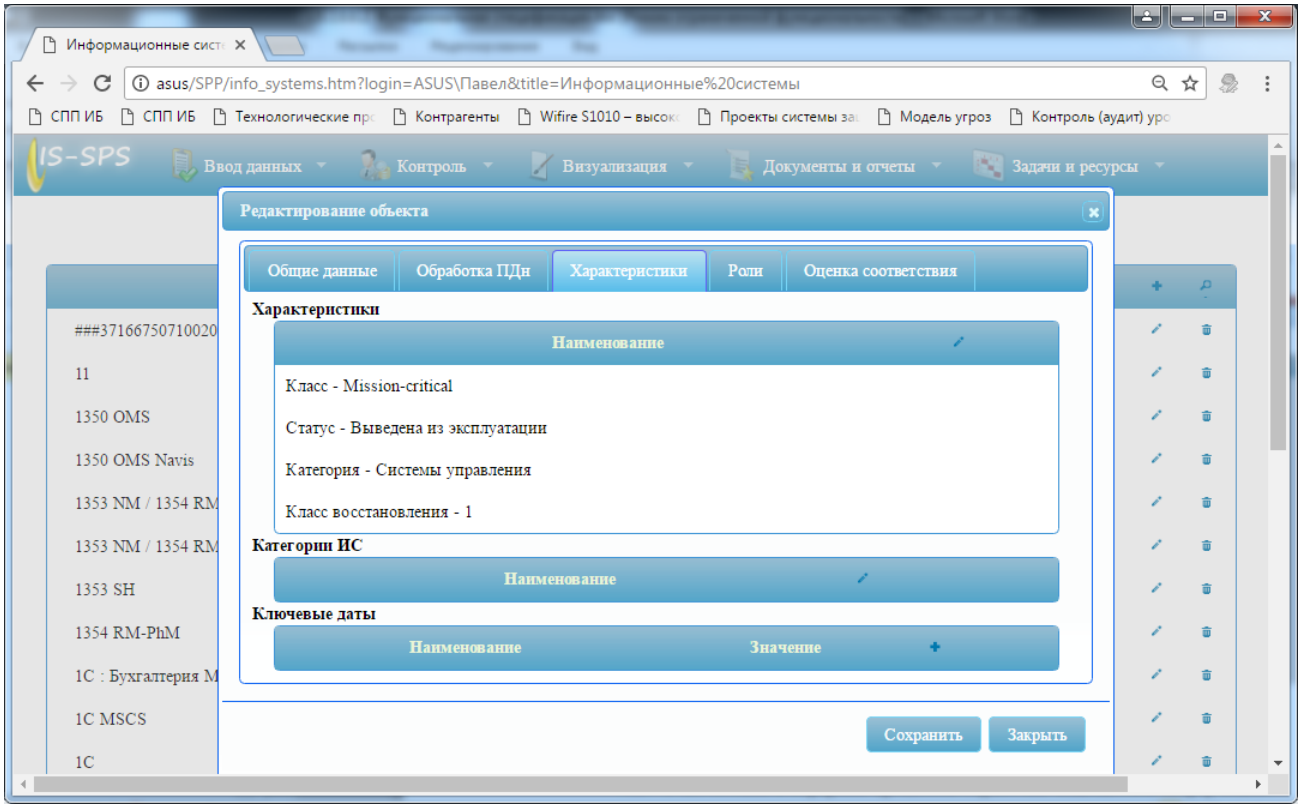


Рисунок 1 - Пример интерфейса «Информационные системы»

4. Управление процессами обработки защищаемой информации

4.1. Учет состава и иерархии процессов обработки защищаемой информации

4.2. Учет структурных подразделений участников процесса и владельцев процесса

4.3. 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.

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

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

5. Управление ролями

5.1. Задание произвольных ролей

5.2. Задание структурных подразделений, которые назначены на роли

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

5.4. Задание ИС, в отношении которых назначены роли

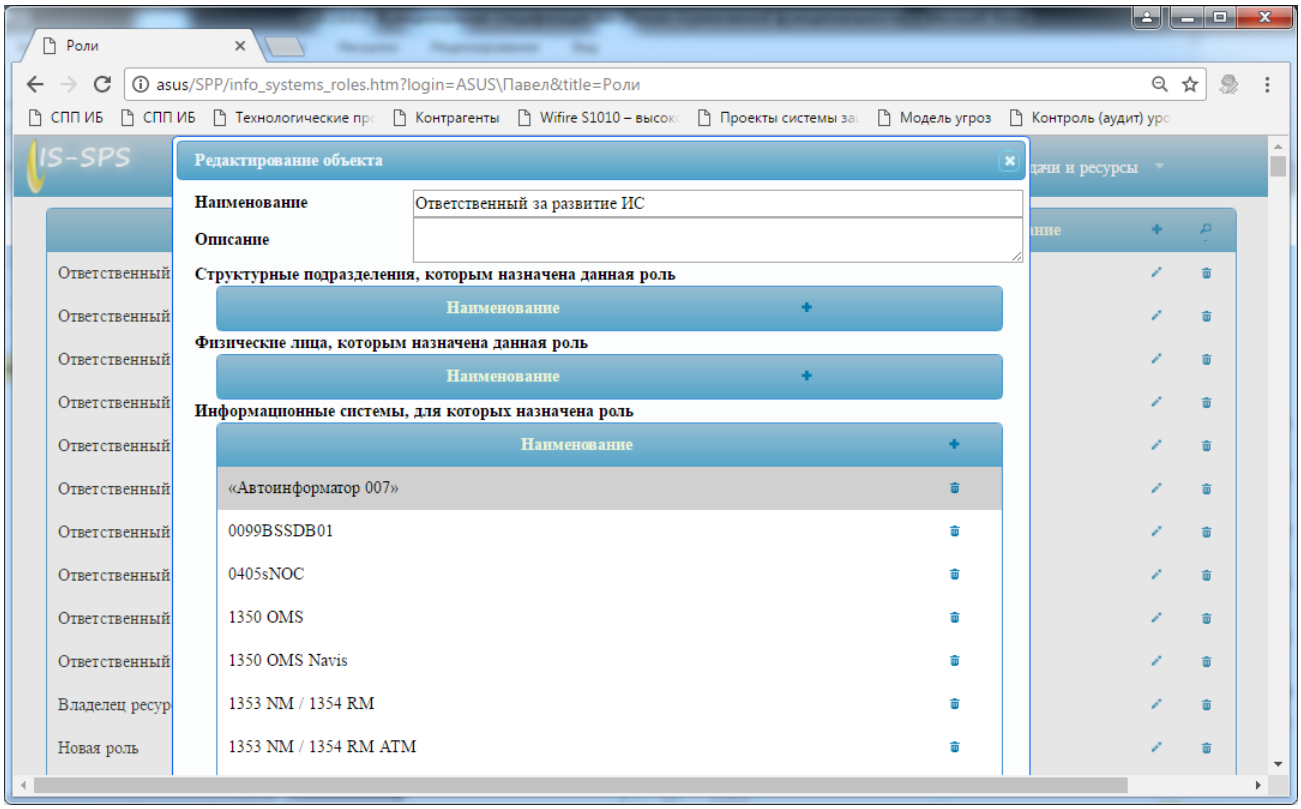


Рисунок 2 - Пример интерфейса «Роли»

6. Перечень сведений конфиденциального характера

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

6.2. Генерация «Перечня сведений конфиденциального характера» на основании учтенных данных

7. **Управление лицами, допущенными к различным категориям конфиденциальной информации**

   7.1. Выбор физических лиц, которых надо допустить к конфиденциальной информации

   7.2. Выбор категорий информации, к которым надо допустить конкретное физическое лицо

   7.3. Генерация формы приказа на допуск лиц к конфиденциальной информации

   7.4. Генерация приказа на исключение лиц из числа допущенных к конфиденциальной информации

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

   8.4. Обеспечение возможности автоматического импорта сведений о физических лицах из внешних систем

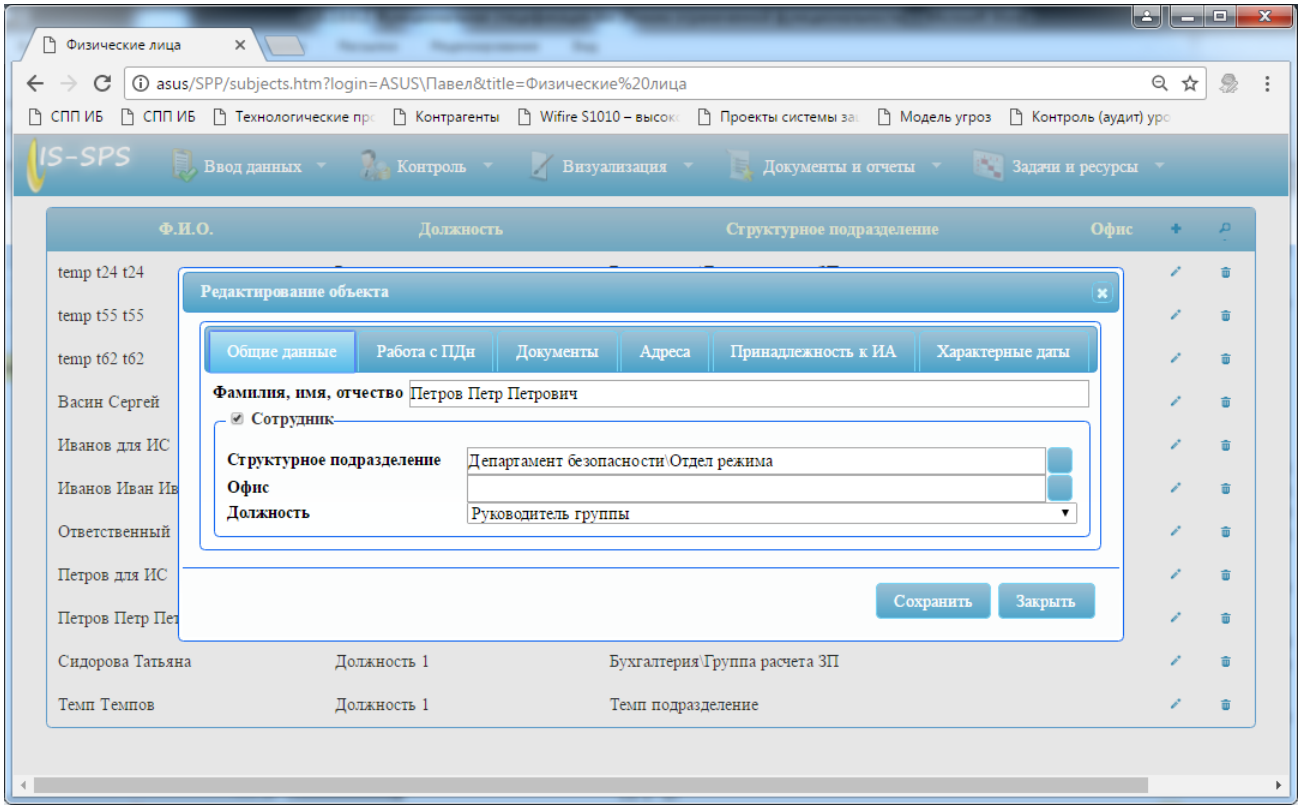


Рисунок 3 - Пример интерфейса «Физические лица»

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, характеристик режима обработки и разграничения доступа в активах, других произвольных значимых 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 доступа физических лиц к информационным активам

10.1. Учет лиц и пар «должность» - «структурное подразделение», которым предоставляется доступ к заданным информационным активам (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 активов

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

10.4. Генерация формы матрицы доступа к информационным 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

11.10. Обеспечение возможности экспорта информации по зданиям и помещениям в файл формата MS Excel

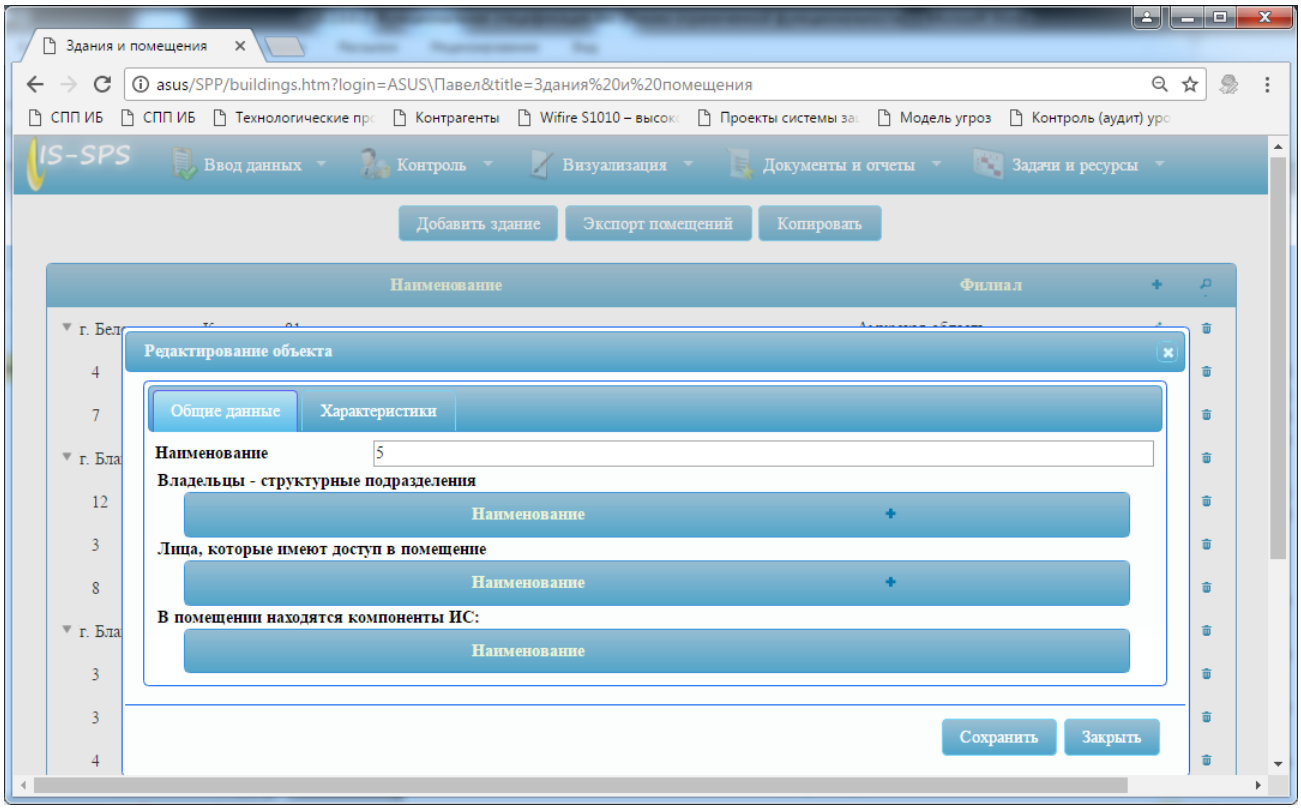


Рисунок 4 - Пример интерфейса «Здания и помещения»

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 справочника произвольных характеристик технических активов, например, операционная система, тип аппаратной части, количество процессоров и т.п.

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 Excel

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

13. Учет доступа физических лиц к техническим активам

13.1. Учет лиц и пар «должность» - «структурное подразделение», которым предоставляется доступ к заданным активам (персональным компьютерам, серверам, системам хранения и т.п.)

13.2. Генерация формы матрицы доступа к активам

14. Управление моделью угроз

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

14.2. Генерация формы модели угроз для конкретных ИС

14.3. Фиксация текущего состава каждой сгенерированной модели угроз

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

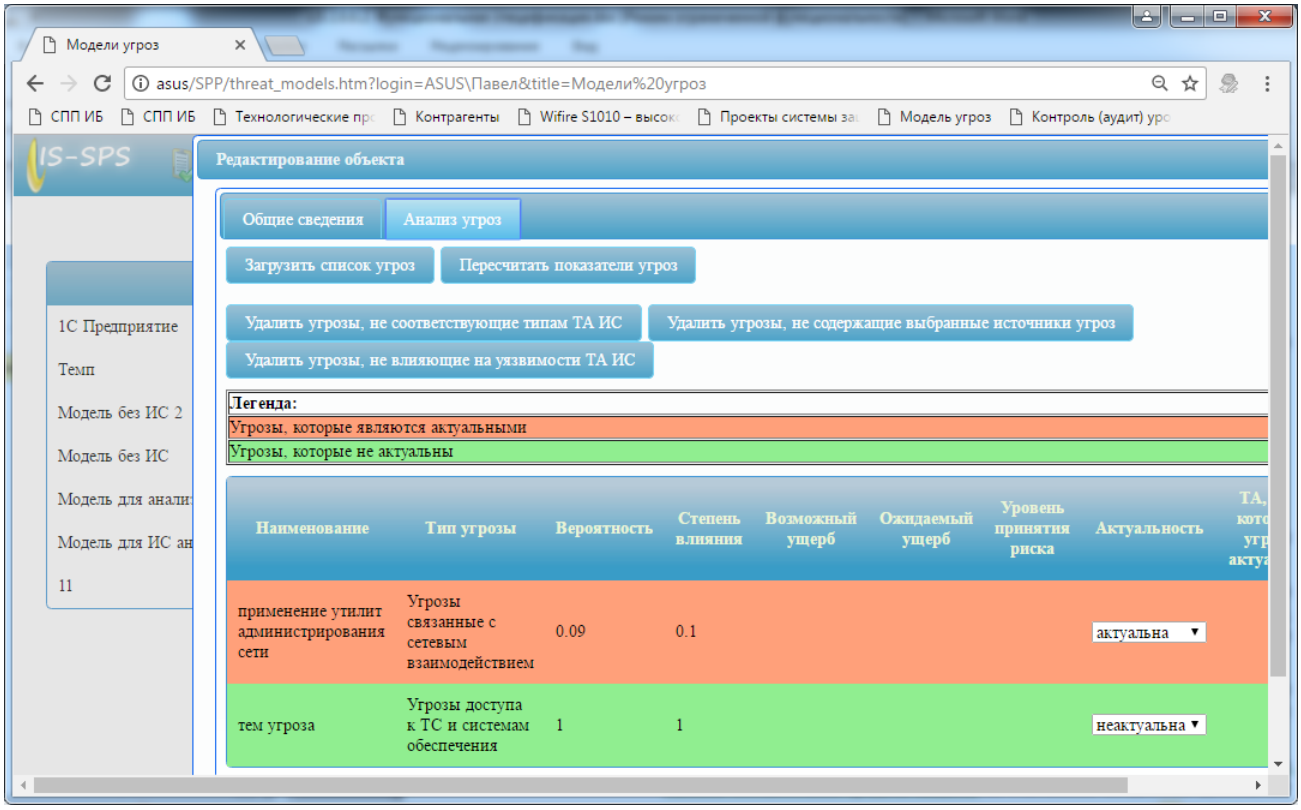


Рисунок 5 - Пример интерфейса «Модель угроз»

15. Управление средствами защиты

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

15.2. 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

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

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

16. Управление проектами на систему защиты

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

16.2. 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

16.3. Предоставление возможности автоматического импорта необходимых мер защиты в зависимости от характеристик ИС, результатов классификации ИС

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

17. Управление проведением контроля (аудита) защищенности

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

17.2. 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.

17.3. 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.

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

17.5. Автоматический расчет уровня зрелости проверенных процессов

17.6. Генерация приказа на проведение аудита защищенности

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

18. Управление уязвимостями

18.1. Ведение справочника уязвимостей с произвольным набором характеристик

18.2. Возможность задания уязвимостей активов

18.3. Учет сведений об исправлении уязвимостей с использованием электронной подписи

19. Ввод средств защиты в эксплуатацию, включая:

19.1. Учет введенных в эксплуатацию средств защиты с указанием даты ввода

19.2. Автоматический контроль необходимости ввода в эксплуатацию средств защиты посредством анализа наличия средств защиты не введенных в эксплуатацию

19.3. Генерация форм приказов на ввод в эксплуатацию средств защиты

20. Управление документами

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 системе и средствам защиты с сохранением их названий, номеров, самих документов

20.4. Обеспечение возможности редактирования шаблонов документов

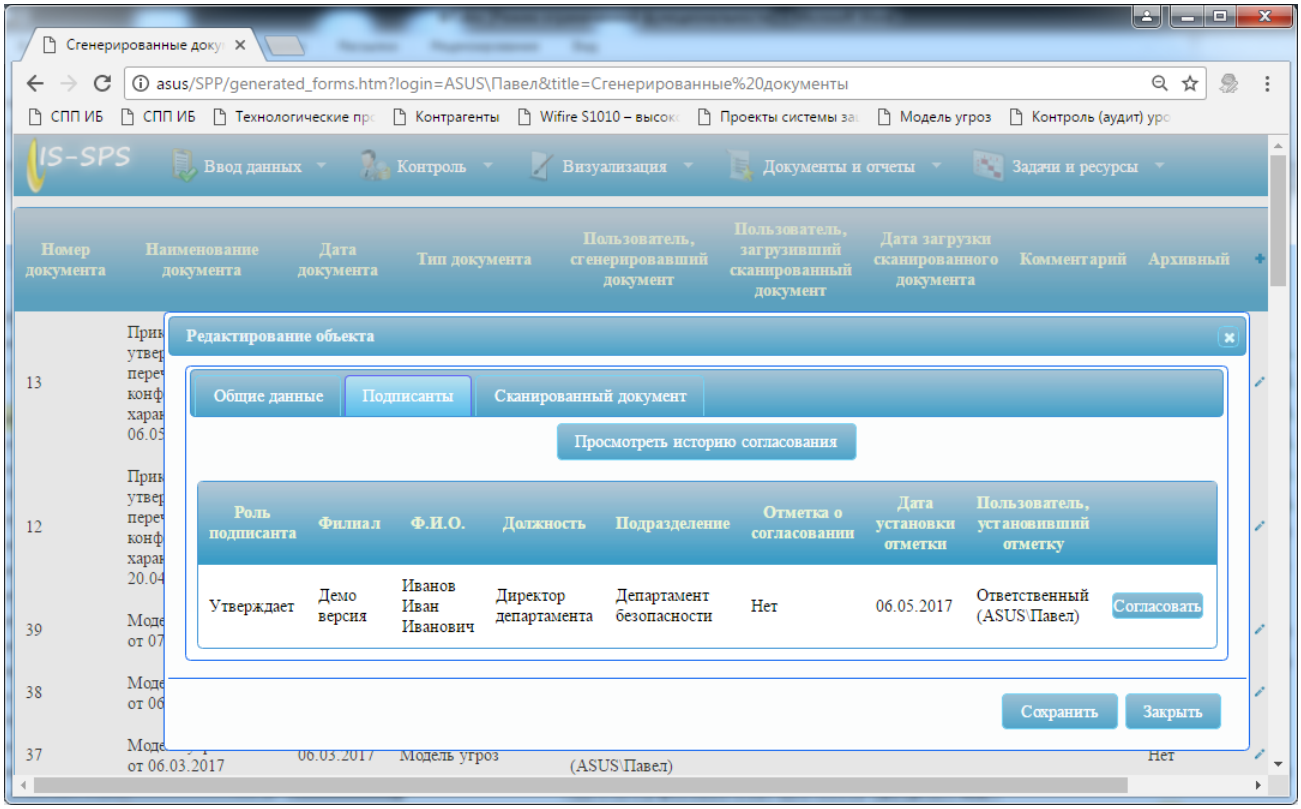


Рисунок 6 - Пример интерфейса «Сгенерированные документы»

21. Управление обучением в области ИБ

21.1. Задание произвольных программ обучения, материалов данных программ, вложенных файлов

21.2. Определение лиц, для которых заданные программы обучения являются обязательными – конкретные структурные подразделения, физические лиц, лица, допущенные к определенным ИС

21.3. Обеспечение возможности простановки пользователями системы отметок о пройденном обучении с фиксацией электронной подписи

21.4. Автоматический контроль состава лиц, которым надо пройти обучение

22. Управление носителями конфиденциальной информации

22.1. Задание типов, номеров носителей

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

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

23. Управление инцидентами

23.1. Учет нештатных ситуаций, даты происшествия, описания результатов их расследования, подверженных активов, ответственных за их расследование

23.2. Учет документов связанных с нештатной ситуацией

23.3. Задание угроз, уязвимостей, которые привели к нештатной ситуации

23.4. 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

23.5. Автоматическое создание задач по инцидентам

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

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

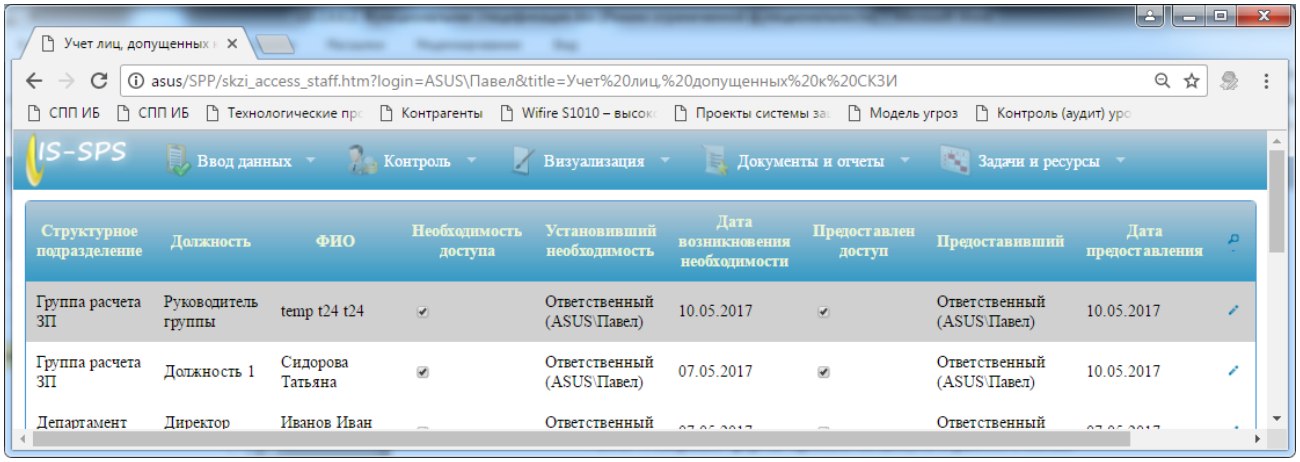


Рисунок 7 - Пример интерфейса «Учет лиц допущенных к СКЗИ»

24.2. Генерация формы приказа на допуск к работе с СКЗИ

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

24.4. Ведение лицевых счетов пользователей СКЗИ

24.5. Ведение ключевых документов к СКЗИ

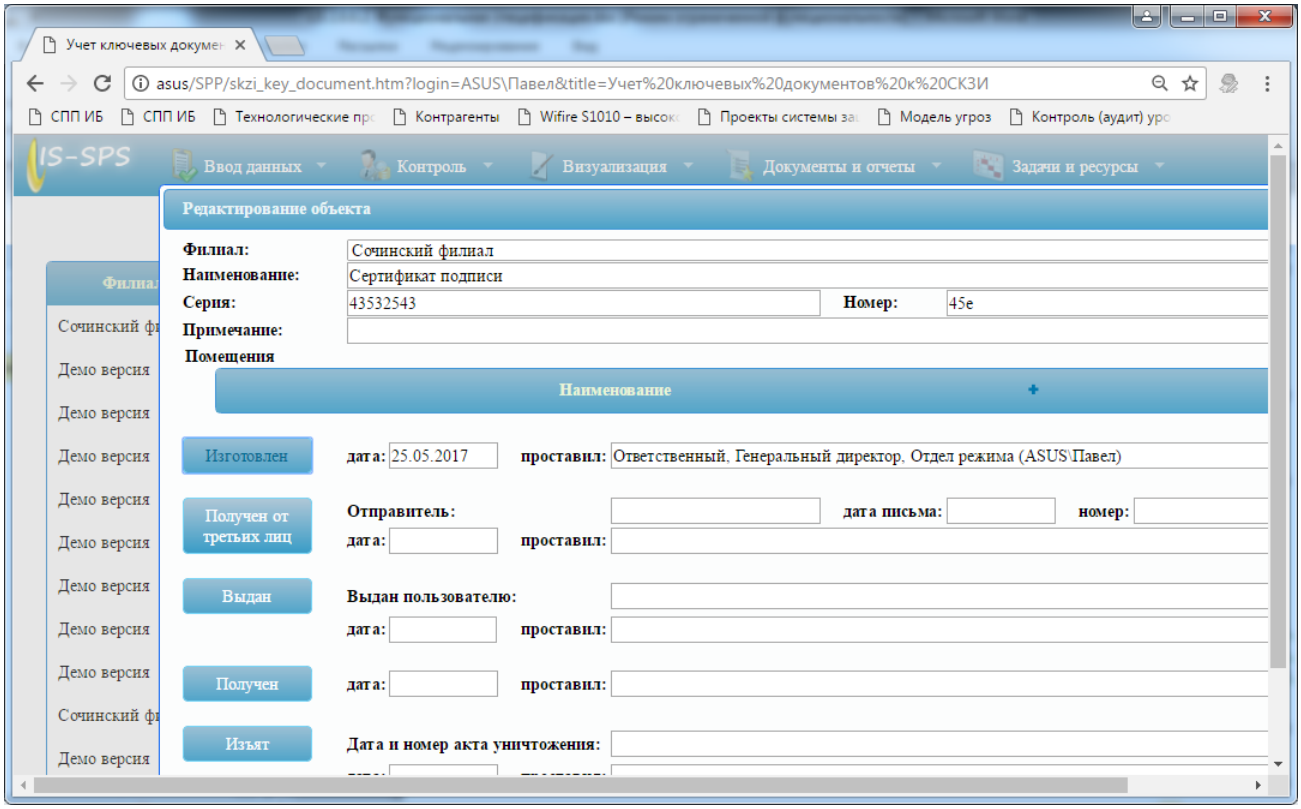


Рисунок 8 - Пример интерфейса «Учет ключевых документов»

25. Управление задачами и ресурсами

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

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

25.3. Автоматическое внесение выявленных несоответствий как отдельных задач

25.4. Поддержка механизмов оповещения пользователей об изменениях в задачах

25.5. Ведение истории изменения задачи

25.6. Фиксация каждого изменения задачи с использованием электронной подписи

25.7. Возможность использования развитых механизмов фильтрации задач по множеству критериев

25.8. Поддержка возможности ведения рабочего графика для ответственных по задаче

25.9. Расчет нагрузки на ответственных по назначенным задачам

26. Управление запросами на изменение

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

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

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

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

27. Управление правами доступа

27.1. Задание состава пользователей

27.2. Задание правил назначения и смены паролей доступа

27.3. Задание ролей пользователей, обеспечение ограничения доступа пользователей по филиалам, доступным пунктам меню

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

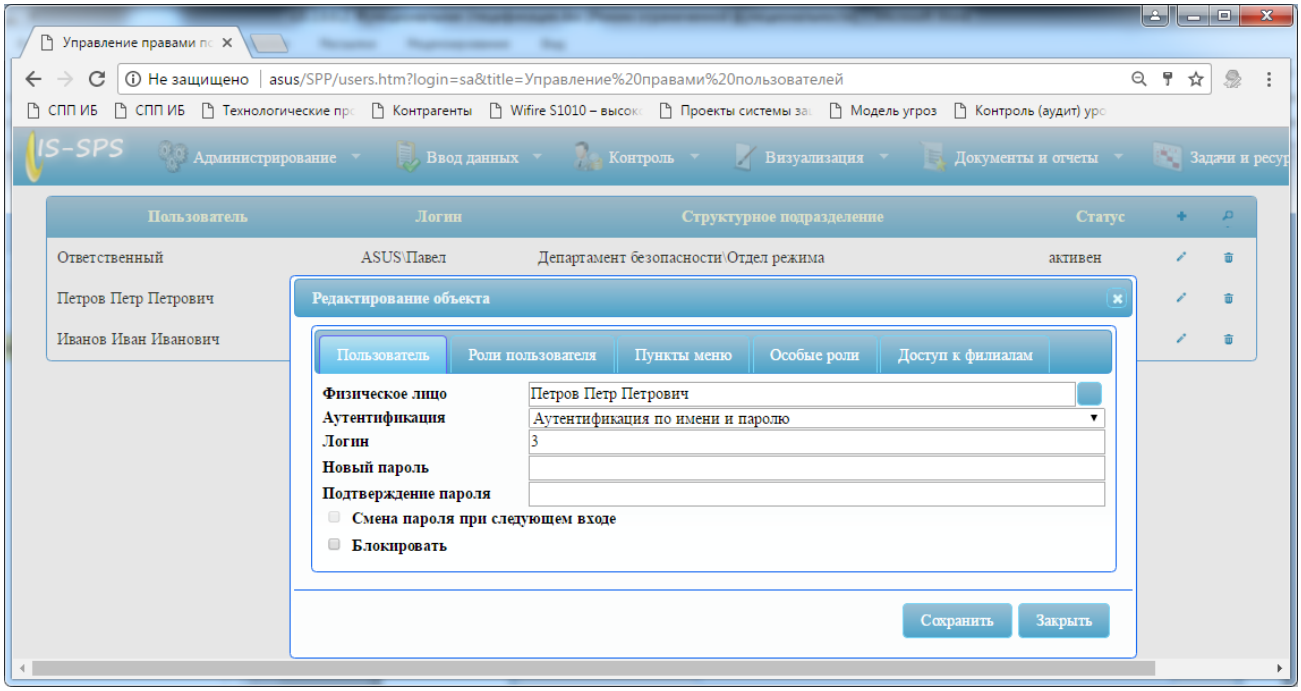


Рисунок 9 - Пример интерфейса «Управление правами доступа»

2.2. Внешние интерфейсы

Внешние интерфейсы предназначены для:

- автоматизации процедур загрузки и синхронизации данных из внешних баз данных (интерфейсы импорта и синхронизации);

- автоматизации процедур подгрузки исходных данных из формализованных опросных листов (интерфейсы подгрузки).

Внешние интерфейсы импорта и синхронизации СПП ИБ осуществляют:

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

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

- списка филиалов,
- списка офисов,
- списка помещений,
- списка лиц допущенных в помещения,
- состава и структуры структурных подразделений,
- состава и структуры технологических процессов,
- списка информационных активов,
- списка сотрудников,
- списка технических активов,
- списка физических лиц,
- списка допущенных к информационным активам лиц,
- данных о контрагентах и договорах с ними.

СПП ИБ имеет возможность подгрузки из опросных листов следующих данных:

- сведений о процессах обработки 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 ИБ поддерживают следующие источники данных:

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

.