ООО «Компания Информационных Технологий»

«СИСТЕМА АВТОМАТИЗАЦИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ»

Управление рисками

Руководство пользователя

Екатеринбург
2022

Содержание

1. Общие положения

1.1. Общие сведения

Настоящее руководство пользователя устанавливает порядок работы с модулем «Управление рисками» (далее – Модуль).

1.2. Назначение модуля

Модуль «Управление рисками ИБ» предназначен для автоматизации процедур идентификации, анализа, оценки рисков ИБ.

Для процесса оценки рисков используется полуколичественный метод анализа рисков, который обеспечивает минимально достаточную точность результатов оценки рисков ИБ. Метод использует знания экспертов и типовые перечни угроз, уязвимостей, защитных мер.

2. Описание ролевой модели

В модуле «Управление рисками ИБ» предусмотрены следующие роли:

- Руководитель;
- Аналитик ИБ;
- Эксперт по оценке.

Участие ролей пользователей в выполнении функций модуля «Управление рисками ИБ» приведено в Таблица 1

Табл. 1. Участие ролей пользователей в выполнении функций модуля

Участие в функциях	Роль		
	Руководитель	Эксперт по оценке	Аналитик ИБ
Назначение начального статуса риска после завершения проекта по оценки. Доступен просмотр карточки риска	-	+	+
Изменение атрибутов риска	-	-	+
Создание нового проекта	+	+	-
Назначение состава комиссии, определение области оценки	+	+	-
Идентификация и оценка последствий для объектов защиты. Оценка защитных мер для последствий	-	+	-
Определение и утверждение состава требований для проекта. Оценка защитных мер от эксплуатации выявленных уязвимостей	-	+	-
Проведение контрольных мероприятий и регистрация результатов проверок	-	+	-
Утверждение реестра рисков	+	+	-
Просмотр результатов оценки рисков	+	+	-

3. Начало работы с модулем

Для начала работы выполните следующие действия:

1. Откройте браузер;
2. В адресной строке браузера укажите адрес, по которому расположен экземпляр платформы;
3. На странице аутентификации введите логин и пароль учетной записи;
4. Нажмите кнопку «Войти». После успешной авторизации откроется рабочая область пользователя.

4. Сценарии работы пользователей

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

4.1. Работа с разделом «Реестр рисков и справочной информации»

С реестром рисков и справочной информации ведет работу пользователь с ролью «Аналитик ИБ».

В рабочей области пользователя отображается форма «Реестр рисков и справочной информации» (Рисунок 1).

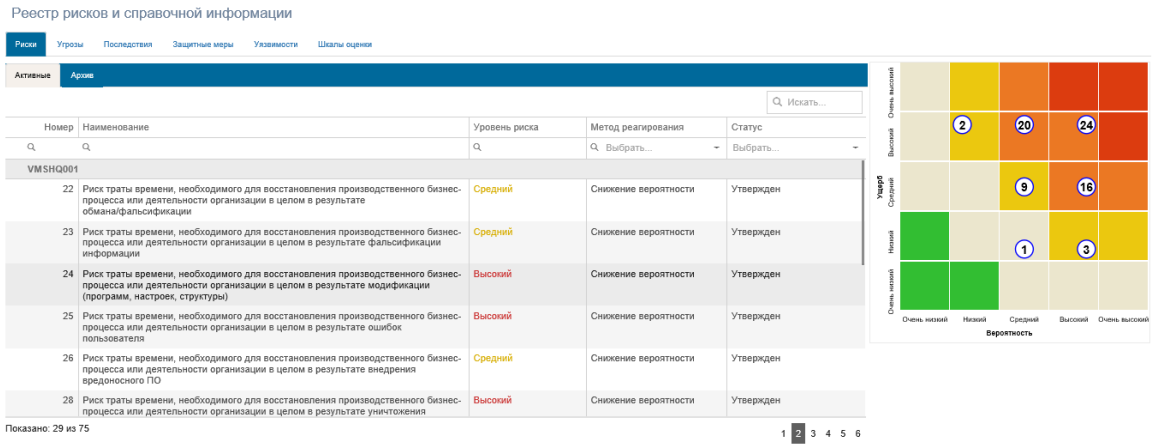

Рис. 1. Реестр рисков и справочной информации

Форма «Реестр рисков и справочной информации» используется для редактирования атрибутов рисков информационной безопасности, угроз, последствий, защитных мер и уязвимостей, шкал оценки.

Форма содержит вкладки, соответствующие задачам, связанными с управлением:

- рисками ИБ;
- угрозами;
- последствиями;
- защитными мерами;
- уязвимостями;
- шкалами оценки.

4.1.1. Управление реестром рисков ИБ

Управление реестром рисков ИБ выполняется на вкладке «Риски» формы «Реестр рисков и справочной информации» (см. Рисунок 1).

Риск информационной безопасности – неопределенность, предполагающая возможность ущерба, связанного с нарушением информационной безопасности.

В реестре отображаются риски, сформированные и утвержденные в ходе проведения проекта по оценке.

Риск ИБ обладает следующими атрибутами:

- Номер - уникальный номер риска.
- Наименование - наименование риска, описывается как вероятность реализации последствий для угрозы.
- Объект защиты - актив, для которого характерен выявленный риск.
- Угроза - угроза, связанная с риском.
- Последствие - уязвимость, связанная с риском.
- Уровень ущерба - качественный уровень по шкале Высокий-средний-низкий, полученный в ходе оценке риска.
- Уровень угрозы - качественный уровень по шкале Высокий-средний-низкий, полученный в ходе оценке риска.
- Уровень уязвимости - качественный уровень по шкале Высокий-средний-низкий, полученный в ходе оценке риска.
- Уровень риска - качественный уровень по шкале Высокий-средний-низкий, полученный в ходе оценке риска.
- Статус - статус, показывающий текущий этап жизненного цикла риска.
- Выявленные уязвимости - уязвимости, выявленные в ходе оценки рисков и характерные для выбранного риска.
- Защитные меры - перечень защитных мер, выявленных в ходе оценки, направленных на снижение уязвимостей и снижение ущерба в случае реализации риска.

4.1.1.1. Редактирование риска

Для редактирования атрибутов риска необходимо:

1. Из формы «Реестр рисков и справочной информации» перейти в карточку риска с помощью двойного клика левой клавишей мыши по соответствующей строке. В новой вкладке отобразится карточка риска (Рисунок 2).

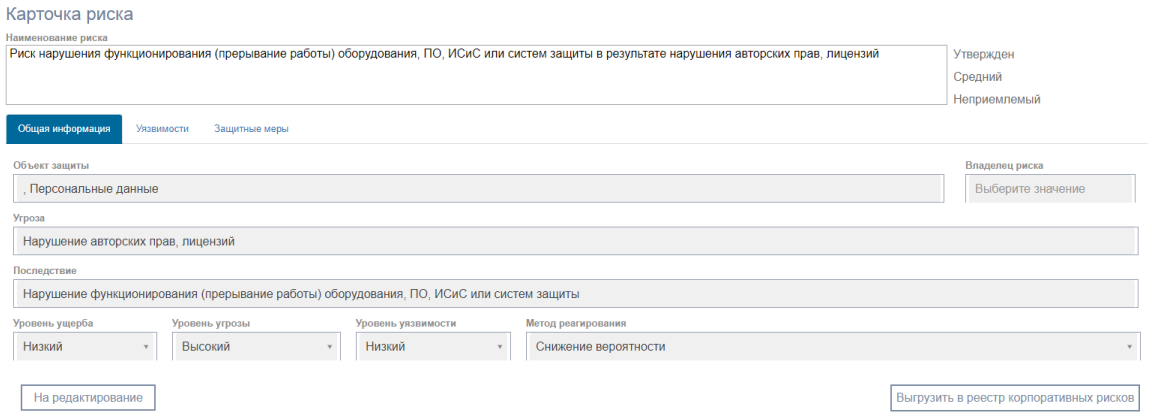

Рис. 2. Карточка просмотра и редактирования атрибутов риска

1. Нажать кнопку «На редактирование». Статус карточки риска изменится на «Требуется утверждение», и станут доступны для редактирования атрибуты уровень ущерба, уровень угрозы, уровень уязвимости и списки выявленных уязвимостей и защитных мер, а также метод реагирования.
2. После изменения атрибутов нажмите кнопку «Сохранить». Для утверждения риска нажмите кнопку «Утвердить».
3. При необходимости, выгрузите риск в реестр корпоративных рисков, для этого нажмите на кнопку «Выгрузить в реестр корпоративных рисков». После выгрузки информация о риске будет доступна для выгрузки в формате, принятом для обработки корпоративных рисков.

4.1.2. Управление угрозами

Угроза — возможная причина нежелательного инцидента, который может повредить систему или привести к ущербу для организации [ИСО/МЭК 27000:2012, пункт 2.77].

Угроза обладает следующими атрибутами:

- Обозначение - уникальное обозначение угрозы
- Название - название угрозы.
- Категория - категория угрозы, связана с нарушением свойств ИБ.
- Вероятность реализации - частота реализации угрозы в установленный период времени.
- Группы уязвимостей - типовой перечень групп уязвимостей ИБ, обуславливающий реализацию угрозы.
- Способы реализации угрозы - описание возможных способов реализации угроз.
- Источники - типовые субъекты, являющиеся причиной возникновения угрозы ИБ.
- Объекты воздействия - описание подтипов объектов защиты, для которых характерна угроза в сочетании с группой уязвимостей.

Управление угрозами выполняется на вкладке «Угрозы» формы «Реестр рисков и справочной информации».

4.1.2.1. Редактирование угрозы

Для редактирования атрибутов угрозы:

1. С формы «Реестр рисков и справочной информации» перейти в карточку угрозы с помощью двойного клика левой клавишей мыши по соответствующей строке. В новой вкладке отобразится карточка угрозы (Рисунок 3).
2. Внесите необходимые изменения и нажмите кнопку «Сохранить».

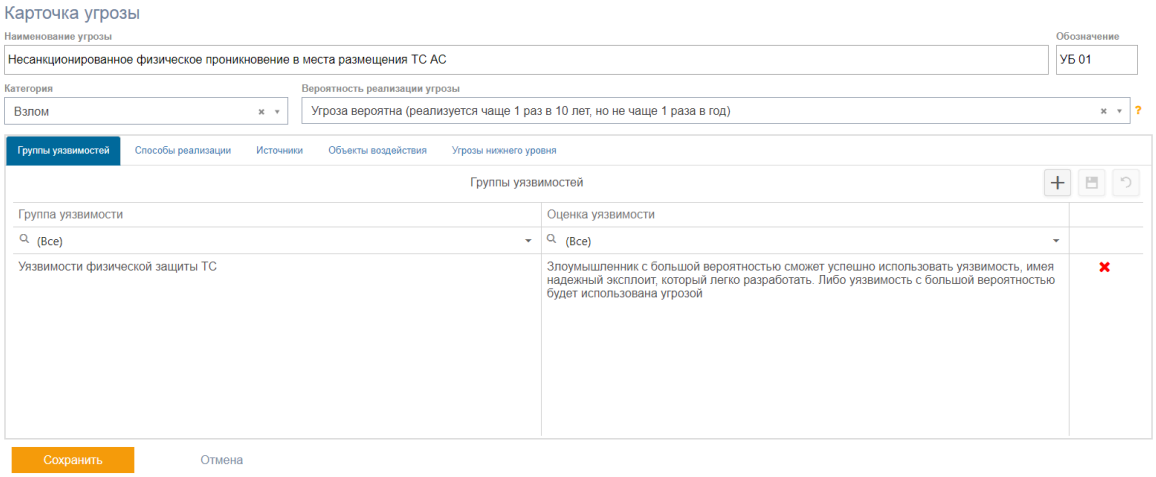

Рис. 3. Редактирование угрозы

4.1.3. Управление справочником последствий

Последствие — результат воздействия события на объект.

Последствия обладают следующими атрибутами:

- Наименование - уникальное название последствия
- Защитные меры - защитные меры, направленные на сокращение возможных последствий
- Типовые факторы оценки последствий - факторы, которые необходимо учитывать при оценке вероятности возникновения последствий

Управление последствиями выполняется на вкладке «Последствия» формы «Реестр рисков и справочной информации».

4.1.3.1. Редактирование последствия

Для редактирования атрибутов последствия:

1. С формы «Реестр рисков и справочной информации» перейти в карточку угрозы с помощью двойного клика левой клавишей мыши по соответствующей строке. В новой вкладке отобразится карточка последствия. (Рисунок 4).
2. Внесите необходимые изменения и нажмите кнопку «Сохранить».

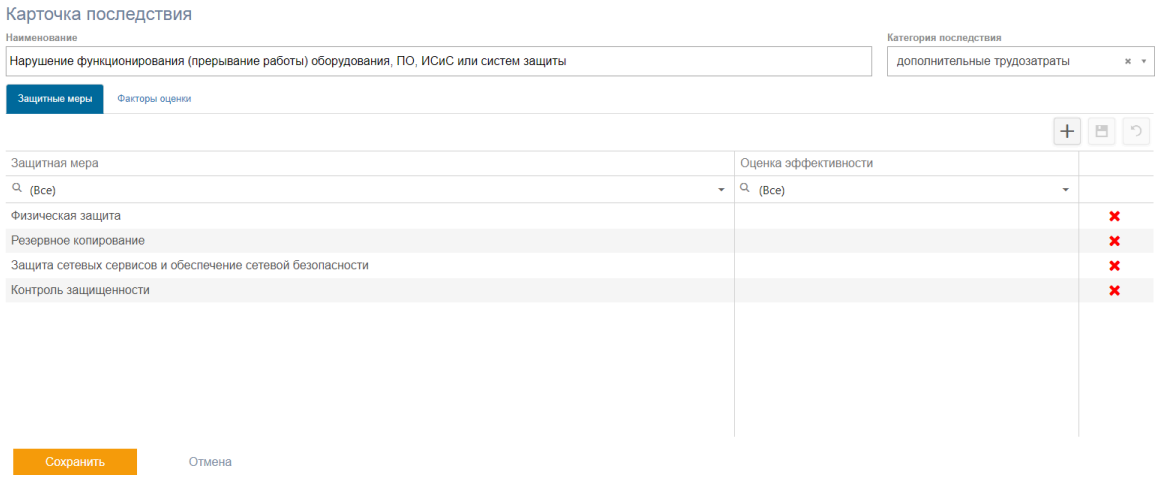

Рис. 4. Редактирование последствия

4.1.4. Управление справочником защитных мер

Защитная мера — это мера, изменяющая риск. Защитные меры включают процессы, внутренние нормативные документы, устройства, процедуры или другие действия, которые изменяют риск. Защитная мера не всегда оказывает ожидаемое или предполагаемое влияние. [Руководство ИСО 73:2009, п.3.8.1.1]

Карточка защитной меры обладает следующими атрибутами:

- Идентификатор - уникальный идентификатор защитной меры
- Наименование - название защитной меры.
- Реализована - признак, по которому оценивается реализация защитной меры.
- Снижение последствий - типовая оценка эффективности защитной меры, направленной на снижение последствий. Используется при проведении оценки последствий.
- Устранение уязвимостей - типовая оценка эффективности защитной меры, направленной на устранение уязвимостей. Используется при проведении оценки защитных мер.

Управление защитными мерами выполняется на вкладке «Защитные меры» формы «Реестр рисков и справочной информации».

4.1.4.1. Редактирование защитных мер

Для редактирования атрибутов защитных мер:

С формы «Реестр рисков и справочной информации» перейти в карточку защитной меры с помощью двойного клика левой клавишей мыши по соответствующей строке. В новой вкладке отобразится карточка защитной меры. (Рисунок 5).

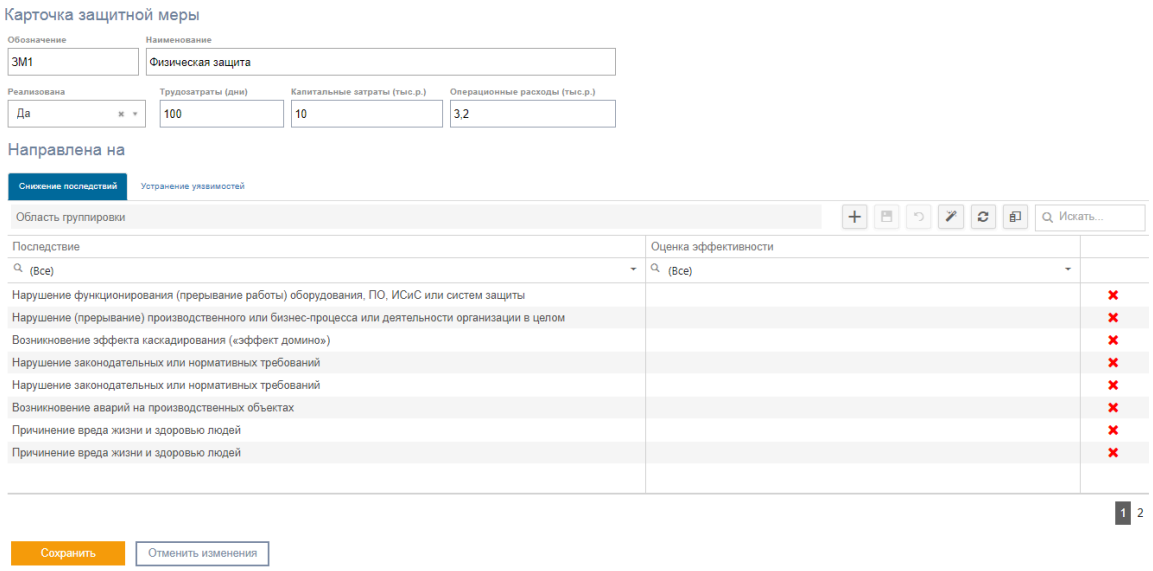

Рис. 5. Редактирование защитной меры

4.1.5. Управление справочником уязвимостей

Уязвимость — это внутренние свойства или слабые места объекта, вызывающие его чувствительность к источнику риска, что может привести к реализации события и его последствий.

Уязвимость обладают следующими атрибутами:

- Наименование - уникальное название уязвимости.
- Группа - свойство уязвимости. Для группы уязвимостей характерен определенный набор угроз.
- Защитные меры - связанные защитные меры, направленные на устранение выбранной уязвимости. Типовые оценки используется при проведении оценки защитных мер.

4.1.5.1. Редактирование уязвимости

Для редактирования атрибутов уязвимости:

1. С формы «Реестр рисков и справочной информации» перейти в карточку уязвимости с помощью двойного клика левой клавишей мыши по соответствующей строке. В новой вкладке отобразится карточка уязвимости (Рисунок 6).
2. Внесите необходимые изменения и нажмите кнопку «Сохранить».

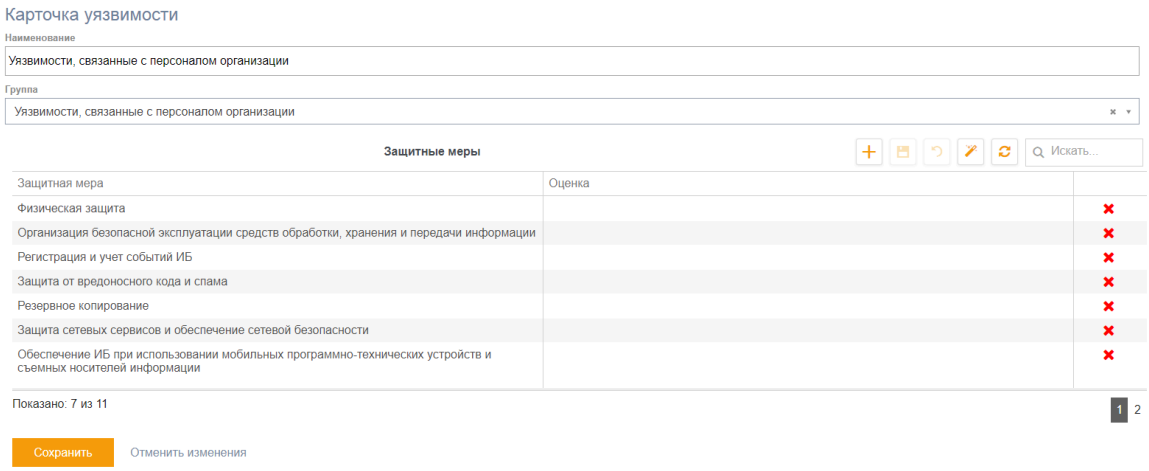

Рис. 6. Редактирование уязвимости

4.1.6. Управление шкалами оценки

Шкалы оценки используются для реализации метода анализа рисков.

Типы шкал оценки:

- Шкала оценки уязвимостей.
- Шкала оценки эффективности защитных мер от последствий.
- Шкала оценки эффективности защитных мер от уязвимостей.
- Типовые факторы оценки последствий, защитных мер, угроз.

Редактирование единиц измерения и шкалы, используемых для оценки факторов риска осуществляется на вкладке «Шкалы оценки» формы «Реестр рисков и справочной информации» (Рисунок 7).

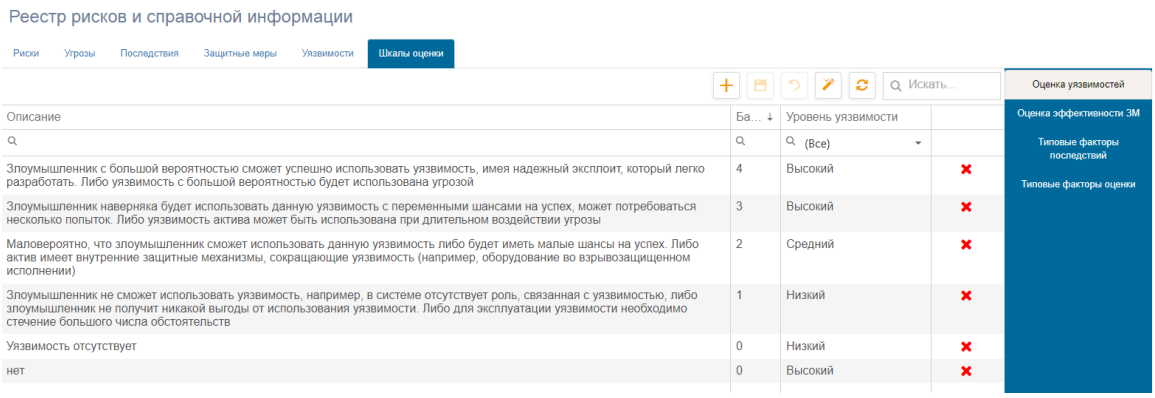

Рис. 7. Шкалы оценки

Редактирования типовых факторов оценки осуществляется из карточки типового фактора оценки. Переход в карточку осуществляется из списка типовых факторов оценки на одноименной вкладке.

4.2. Идентификация и оценка рисков ИБ

Процесс идентификации, анализа и оценки риска выполняется в разделе «Проекты по оценке».

Процесс оценки включает выполнение следующих этапов:

1. Новый проект (создание проекта)
2. Подготовка к оценке
3. Идентификация последствий
4. Идентификация угроз, уязвимостей и защитных мер
5. Оценка рисков
6. Утверждение реестра рисков
7. Завершение проекта

4.2.1. Общие сведения о проекте

Проект включает следующие основные атрибуты:

- Наименование проекта - уникальное название проекта оценки.
- Дата начала - дата начала проекта.
- Дата окончания - дата окончания проекта.
- Статус проекта - статус, показывающий текущий этап жизненного цикла проекта.

На разных этапах жизненного цикла у проекта появляются дополнительные атрибуты, в зависимости от решаемой задачи: приказ об оценке рисков на этапе реализации, определение информационных систем и объектов защиты, входящих в область оценки, и т.д.

4.2.2. Просмотр списка проектов

Просмотр списка проектов выполняется на форме «Проекты по оценке рисков» (Рисунок 8).

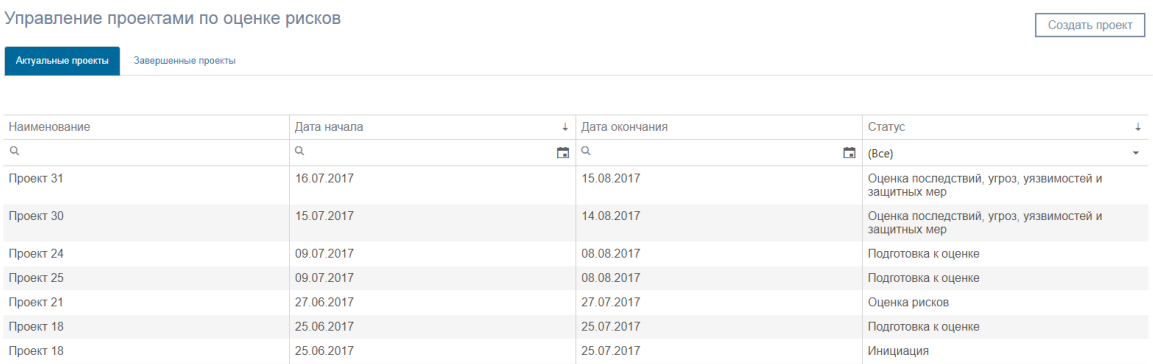

Рис. 8. Список проектов

Форма содержит две вкладки:

- Активные проекты - на вкладке отображается список активных проектов по оценке.

  В таблице отображаются параметры:

  - Наименование проекта;
  - Дата начала проекта;
  - Дата завершения проекта;
  - Статус проекта.

- Завершенные проекты - на вкладке отображается список завершенных проектов по оценке.

  В таблице отображаются параметры:

  - Код проекта;
  - Дата начала проекта;
  - Дата завершения проекта.

Переход в карточку проекта с формы осуществляется с помощью двойного клика левой клавишей мыши по строке. Карточка проекта позволяет выполнить различный набор действий в зависимости от этапа жизненного цикла проекта.

4.2.3. Новый проект

Для создания нового проекта по оценке рисков:

1. Нажмите кнопку «Новый проект» на форме «Проекты по оценке рисков». Откроется карточка нового проекта (Рисунок 9).
2. В поле «Наименование проекта» укажите уникальное название проекта оценки.
3. Для сохранения внесенных сведений нажмите кнопку «Подтвердить».

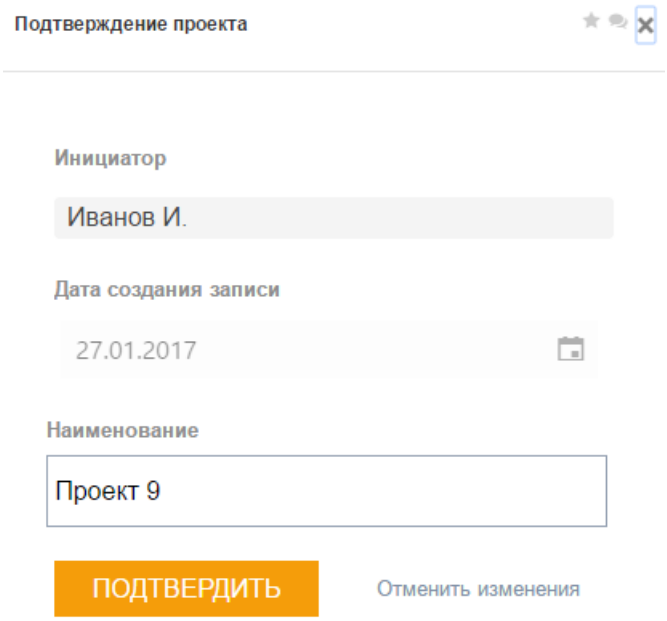

Рис. 9. Инициация нового проекта

4.2.4. Работа с новым проектом

После добавления в списке проектов по оценке добавится новая запись. Двойной щелчок мыши по записи из списка проектов вызывает карточку проекта. В карточке проекта ведется дальнейшая работа с проектом по оценке (Рисунок 10).

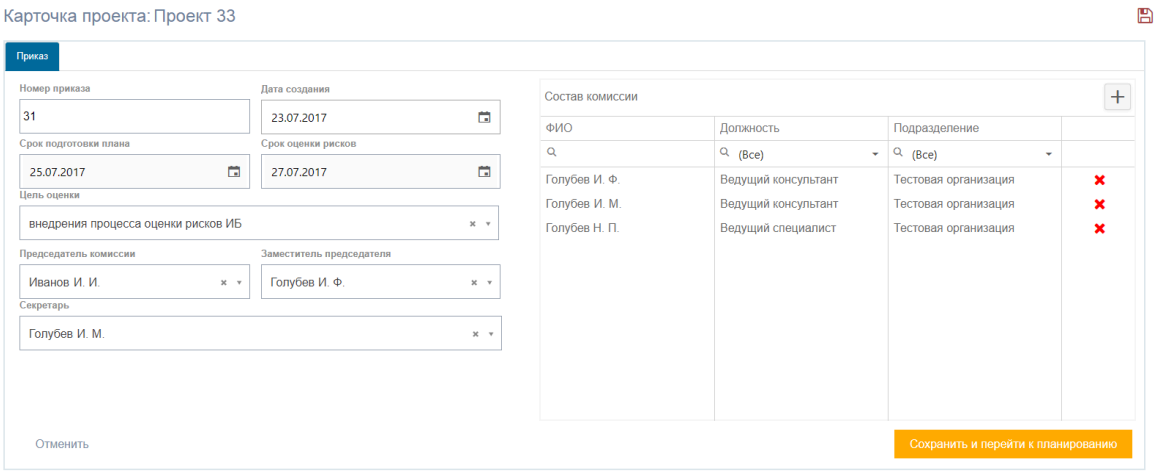

Рис. 10. Создание приказа об оценке и формирование комиссии

В зависимости от этапа жизненного цикла проекта в карточке отображаются различные атрибуты. На этапе создания проекта в карточке проекта заполняются поля для печатной формы приказа об оценке рисков и определяется состав комиссии по оценке.

Для заполнения полей приказа об оценке и определения состава комиссии руководитель СУИБ или эксперт по оценке должен заполнить поля:

1. В поле «Номер приказа» указываются реквизиты приказа, являющегося основанием для проведения оценки.
2. Поле «Дата создания» содержит дату создания приказа (по умолчанию текущая дата). При необходимости значение изменяется.

3. В поле «Срок подготовки плана» укажите конечную дату создания плана оценки. Определение плана по оценке рисков выполняется на следующем этапе жизненного цикла проекта.
4. В поле «Срок оценки рисков» укажите дату окончания проекта.
5. В поле «Цель оценки» указывается из предустановленного перечня цель оценки рисков.
6. В полях «Председатель комиссии», «Заместитель председателя», «Секретарь» указываются пользователи системы, выполняющие в проекте соответствующие полномочия.
7. Справа от полей приказа, расположена область со списком членов комиссии по оценке. Для добавления новых членов в состав комиссии и редактирования состава комиссии используется кнопка с изображением «+».
8. Для сохранения внесенных сведений без перехода на следующий этап нажмите кнопку «Сохранить».
9. Для перехода на следующий этап нажмите кнопку «Сохранить и перейти к планированию».

После определения приказа об оценке рисков и состава комиссии проект переходит на статус подготовки к оценке.

4.2.5. Подготовка к оценке

На этапе подготовки эксперт формирует план оценки. Формирование плана оценки включает в себя определение уровня оценки, информационных систем и сервисов, входящих в оценку, составление графика выполнения работ.

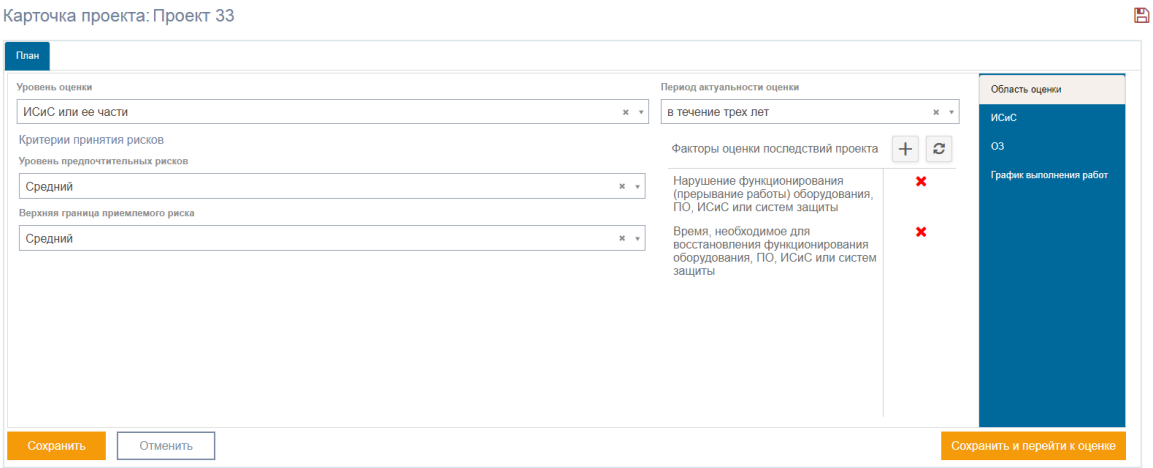

Рис. 11. Формирование плана оценки

Для определения плана оценки в карточке проекта заполняются поля:

1. В поле «Уровень оценки» указать из выпадающего списка на каком уровне будет проходить проверка.
2. Поле «Период актуальности оценки» должно содержать значения периода актуальности.

3. Блок «Критерии принятия риска» должен содержать пороговые значения для определения приемлемости риска в ходе оценки (введенные значения используются на статусе «Оценка рисков»).
4. В списке «Факторы оценки последствий проекта» укажите типовые факторы оценки последствий. Факторы оценки последствий должны быть характерны для активов, входящих в область оценки проекта. На этапе идентификации последствий из выбранного списка факторов оценки определяются последствия для каждого объекта защиты.
5. На вкладке «Информационные системы» происходит выбор информационных систем и сервисов, входящих в область оценки. Для добавления информационных систем в область оценки и редактирования используется кнопка с изображением «+».

Связанные с информационными системами активы отображаются на вкладке «Объекты защиты». Идентификация и оценка рисков проходит для всех связанных с выбранными информационными системами активами. Для корректной идентификации и оценки рисков необходимо, чтобы у активов был заполнен атрибут «Подтип».

1. На вкладке «График выполнения работ» отображается таблица, со списком планируемых работ по проекту. Добавьте в таблицу записи, содержащие основные этапы работ по оценки рисков: предоставление плана оценки, проведение оценки, составление акта, с указанием сроков предоставления и ответственных исполнителей.
2. После завершения составления плана оценки нажмите кнопку «Сохранить и перейти к оценке» для перехода на следующий этап работы с проектом. Или нажмите кнопку «Сохранить» для сохранения введенных изменений, без перехода на следующий этап.

После завершения этапа планирования, проект по оценке рисков переходит на статус «Идентификация последствий».

4.2.6. Идентификация и оценка последствий, угроз, уязвимостей и защитных мер

Форма идентификации и оценки содержит три раздела: оценка последствий, оценка угроз и уязвимостей и оценка защитных мер.

Каждый из экспертов выполняет оценку каждом из трех разделов. Для оценки используется специальный инструмент – кросс-таблица. Для оценки последствий необходимо выбрать значение оценки на пересечении последствия и объекта защиты (Рисунок 12).

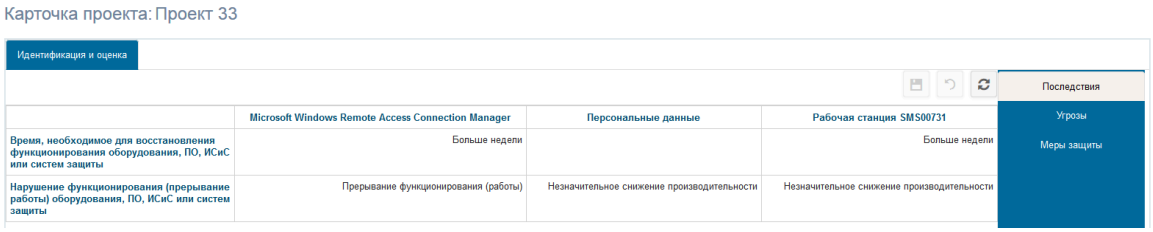

Рис. 12. Идентификация последствий для объектов защиты

Для оценки угроз и уязвимостей необходимо выбрать значения оценки на пересечении уязвимости и объекта защиты (Рисунок 13).

Рис. 13. Оценка последствий для объекта защиты

Для оценки защитных мер необходимо выбрать значения оценки на пересечении защитной меры и объекта защиты (Рисунок 14).

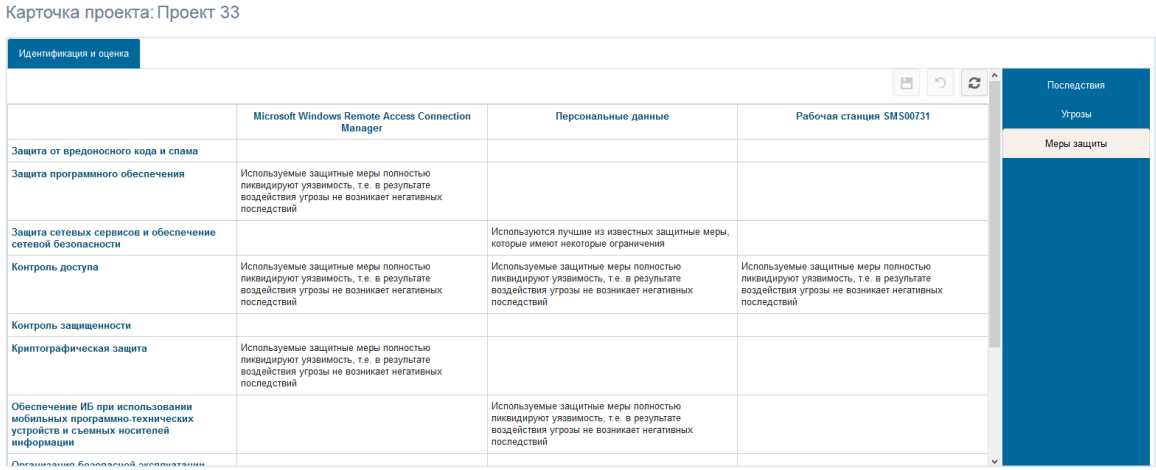

Рис. 14. Оценка эффективности защитных мер для последствий

Руководитель проекта помимо функций оценки обладает возможностью завершить оценку и просмотреть оценки других экспертов (Рисунок 15).

Рис. 15. Проверка соответствия типовых оценок уязвимостей для объекта защиты

Для просмотра результатов работы экспертов нажмите кнопку Ответы экспертов. В появившемся всплывающем окне будут отражены все оценки экспертов в данном проекте в разрезе объектов защиты (Рисунок 16).

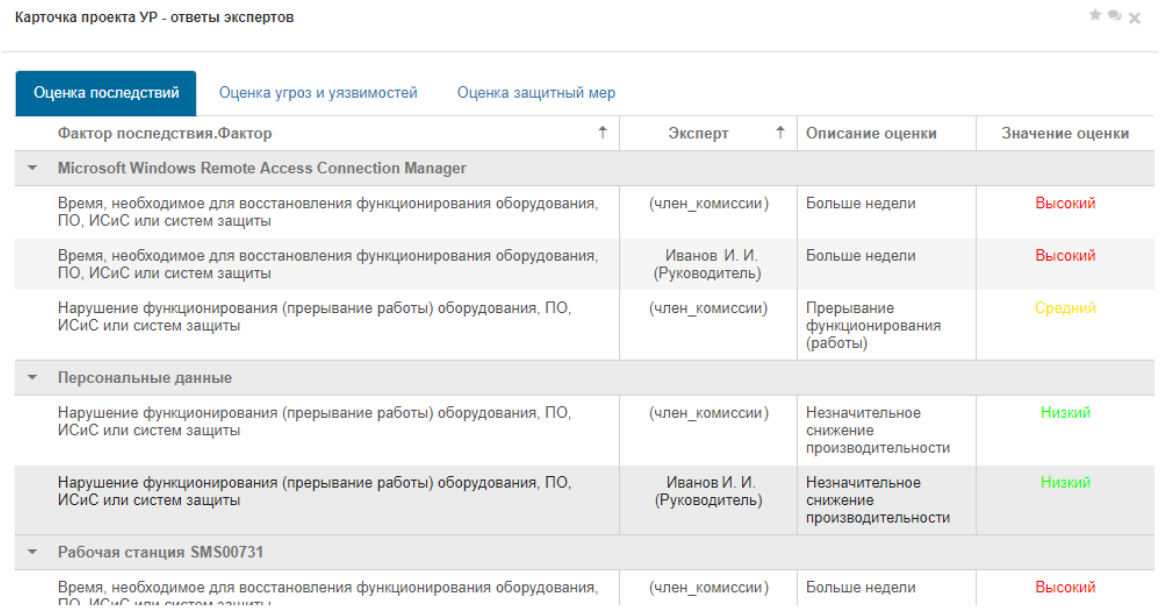

Рис. 16. Ответы экспертов

Для формирования реестра рисков нажмите кнопку «Завершить оценку». Проект переходит на статус «Оценка рисков», создается реестр рисков. Введенные ранее критерии приемлемости, оценки угроз, уязвимостей, защитных мер влияют на уровень и приемлемость формируемых рисков.

4.2.7. Оценка рисков

На этапе оценки эксперт может внести изменения в полученные оценки рисков. Оценивание риска предполагает сравнение оценочной величины риска с установленными критериями приемлемости с целью определения уровня значимости риска.

При необходимости изменения оценки в списке рисков:

1. Выберите риски, установив в первом столбце таблицы флаг.
2. В правой части окна измените значения уровней вероятности реализации угрозы, ущерба, уязвимости. Уровень и приемлемость риска рассчитаются на основании критериев приемлемости.
3. Нажмите кнопку «Сохранить оценку» (Рисунок 17).

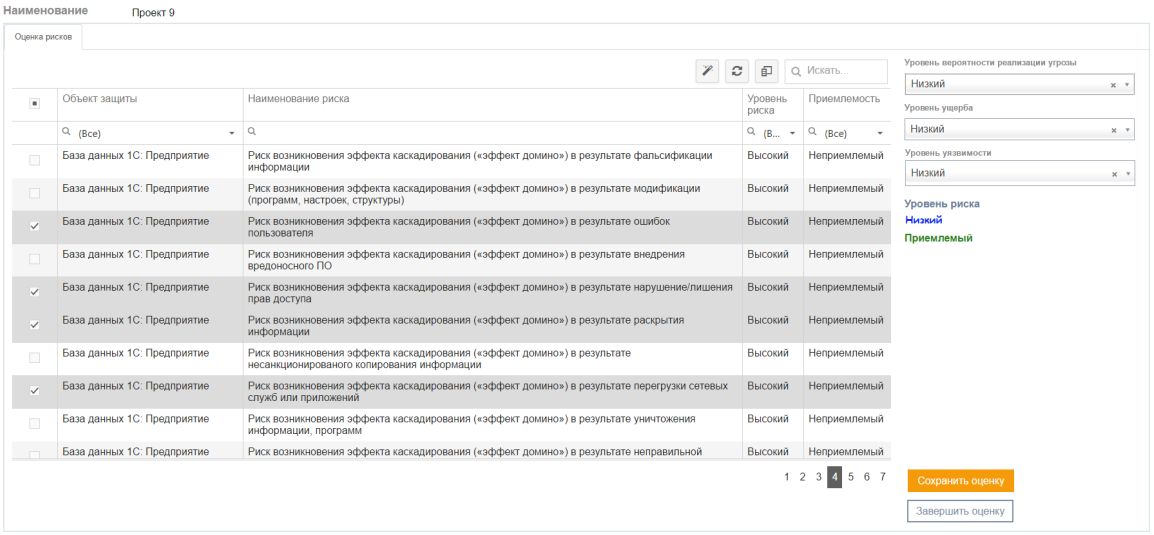

Рис. 17. Оценка рисков

Оценка для рисков обновится в соответствие с выбранными значениями.

После проверки и корректировки полученных оценок перейдите на следующий этап плана проверки, нажав кнопку «Завершить оценку». Проект перейдет на состояние утверждения рисков, и откроется вкладка «Утверждение реестра».

4.2.8. Утверждение реестра и завершение оценки

На этапе утверждения реестра рисков эксперт по оценке утверждает полученный список рисков.

Для утверждения реестра:

1. Выберите риски, установив в первом столбце таблицы флаг
2. Нажмите кнопку «Утвердить» (Рисунок 18).

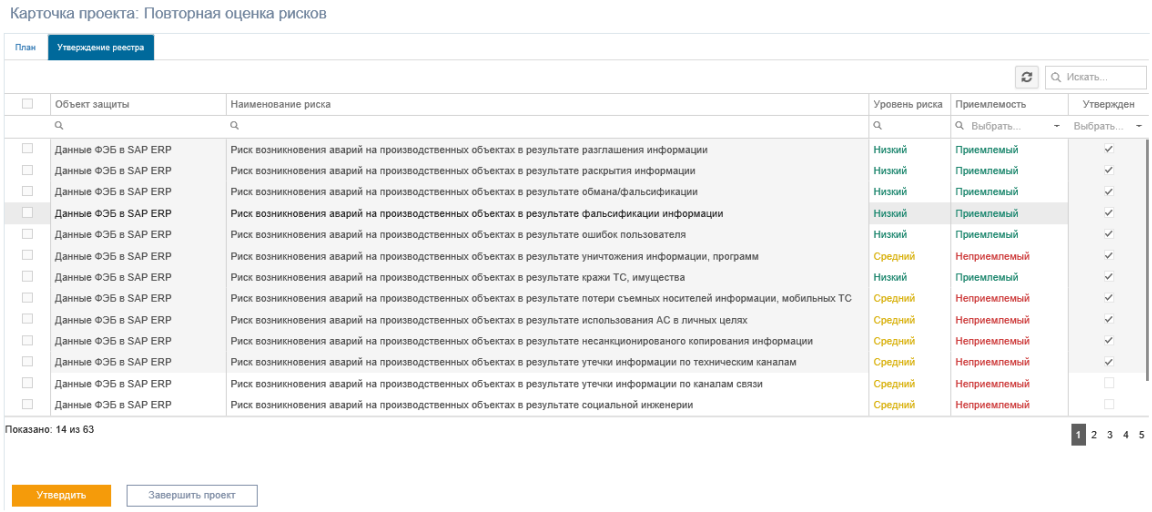

Рис. 18. Утверждение реестра рисков

Для утверждения всех рисков, полученных в рамках проекта:

1. Поставьте флаг в первом столбце заголовка таблицы.
2. Нажмите кнопку «Утвердить».

После утверждения рисков нажмите кнопку «Завершить оценку». Риски, сформированные в ходе проекта, добавятся в справочник рисков, а проект перейдет на этап завершения оценки.

На этапе завершения оценки отображается вкладка «Акт» со списком утвержденных рисков. В правой части вкладки расположена тепловая карта рисков, полученных в ходе проекта и распределение по уровню рисков. С помощью кнопки «Печать акта» распечатайте акт внутренней оценки (Рисунок 19).

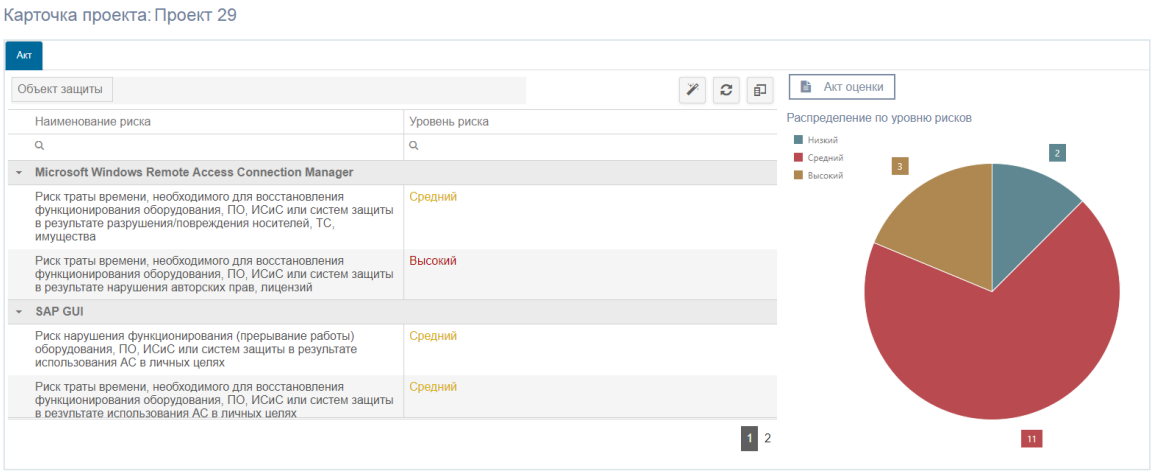

Рис. 19. Просмотр итогов проекта оценки

Из списка утвержденных рисков двойным щелком левой кнопки мыши осуществляется переход в карточку риска.

Проведение мероприятий по обработке и принятию риска зависит от принятых стандартов организации и включаются в модуль по управлению рисками ИБ после проведения обследования.

4.3. Управление мероприятиями

Для утвержденных рисков с методом реагирования «Снижение вероятности», модуль автоматически формирует реестр мероприятий. Список мероприятий создается на основе выявленных в процессе идентификации риска защитных мер.

Управление мероприятиями является бизнес-процессом, включающим следующие этапы:

- **Новое** - статус присваивается при создании мероприятия. На этом этапе пользователь в роли Руководитель СУИБ или Эксперт по рискам может вносить изменения в состав реквизитов. После завершения внесения исправлений, мероприятие передается в работу ответственному. Ответственный назначается в процессе редактирования мероприятия или назначается автоматически: для этого модуль использует данные об администраторе объекта защиты, связанного с данным риском.
- **В работе** - статус присваивается при передаче мероприятия руководителем на исполнение ответственному. На этом этапе ответственный за выполнение мероприятия должен выполнить действия, определенные в мероприятии и отчитаться о их выполнения используя средства платформы. О необходимости выполнения мероприятия ответственный информируется средствами платформы – ему назначается задача, а также по электронной почте. После завершения выполнения мероприятия ответственный должен завершить выполнение назначенной ему задачи, после чего мероприятие автоматически переводится на следующий статус.
- **Выполнено** - статус присваивается при завершении работы ответственным. На этом этапе руководитель проводит приемку выполненных работ. Если работа по мероприятию выполнена полностью, работа по мероприятию завершается: перевод в статус «**Завершено**». В случае, если руководителем установлена необходимость дополнительных действий, мероприятие может быть переведено в статус «**В работе**».
- **Отменено** - статус присваивается при невозможности выполнения мероприятия в настоящее время.
- **Завершено** - статус присваивается мероприятию, по которому работа полностью завершена.

На Рисунок 20 представлен реестр мероприятий. Мероприятия в реестре сгруппированы по их статусам (этапам), для просмотра мероприятий, находящихся на конкретном статусе, перейдите на вкладку с названием статуса.

Для передачи группы мероприятий в работу, отметьте мероприятия в левой колонке таблицы и нажмите кнопку «В работу».

Для перехода к карточке мероприятия выполните двойной клик мыши на соответствующей этому мероприятию записи в таблице.

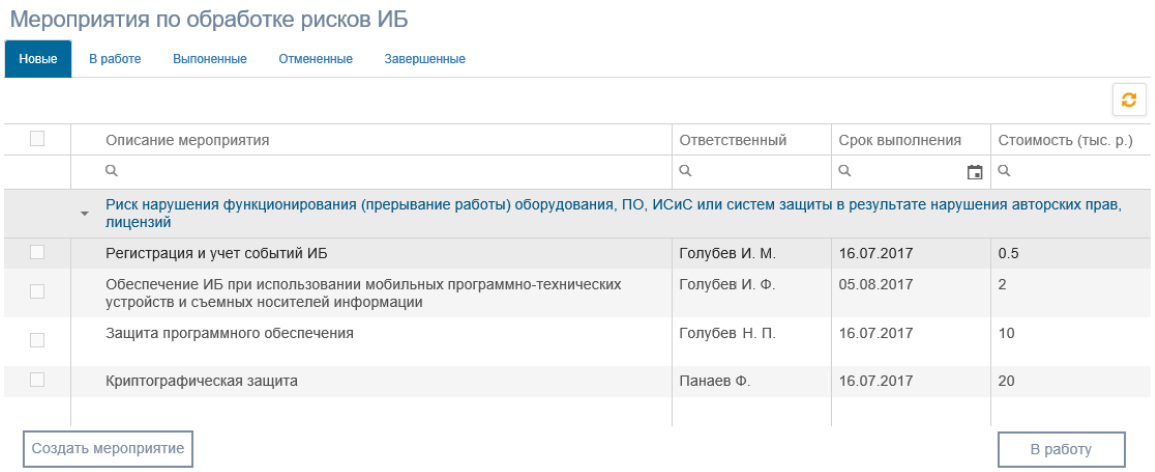

Рис. 20. Реестр мероприятий

На (Рисунок 21) представлена карточка мероприятия, которая поволяет ввести или отредактировать сведения о мероприятии на начальном этапе. Руководитель может уточнить наименование мероприятия, срок выполнения, изменить ответственного, а так же добавить подробное описание работ.

После внесения изменений руководитель может отправить мероприятие в работу: кнопка «В работу» или зафиксировать решение о невозможности выполнения мероприятия: кнопка «Выполнение мероприятия невозможно».

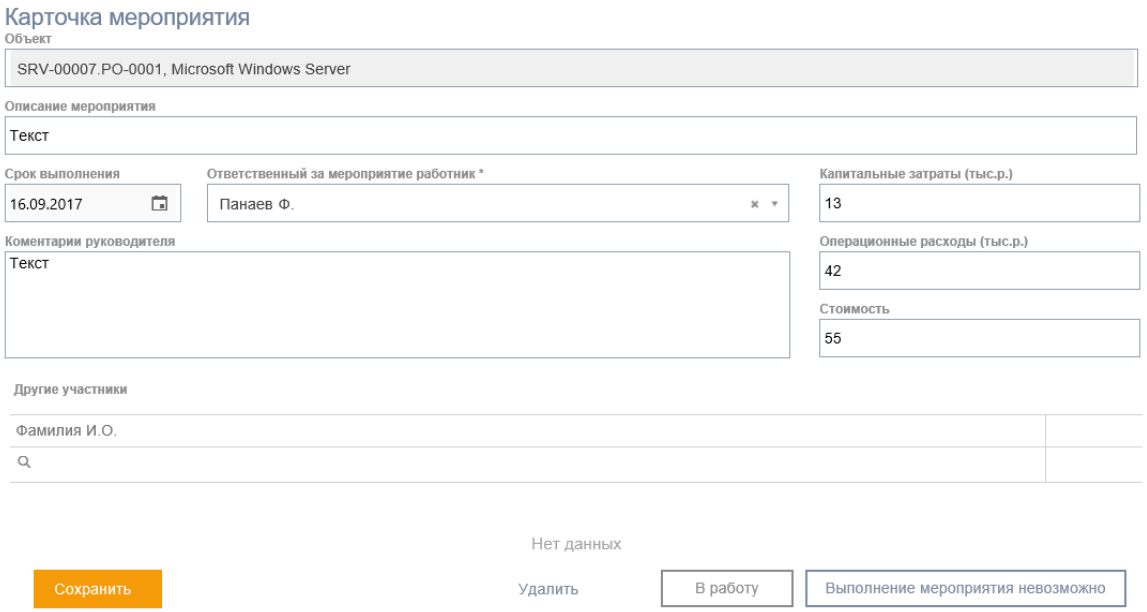

Рис. 21. Карточка мероприятия (руководитель)

На Рисунок 22 представлена стандартная форма списка задач пользователя, содержащая задачу ответственному за выполнение мероприятие. Двойным кликом мыши перейдите к выполнению задачи.

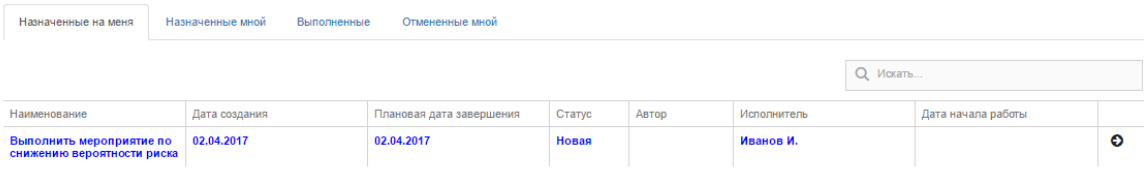

Рис. 22. Список задач ответственного

На Рисунок 23 представлена карточка ответственного за выполнение мероприятия в стандартном окружении карточки задачи.

Карточка мероприятия позволяет ответственному ввести отчет о выполнении работ, определенных в составе мероприятий.

Для начало работы с карточкой мероприятия, перейдите в задачу, нажмите на кнопку «Начать выполнение задачи». Карточка мероприятия будет разблокирована, после этого запоните отчет о выполнении и нажмите кнопку «Сохранить».

Для передачи отчета руководителю нажмите кнопку «Завершить выполнение задачи».

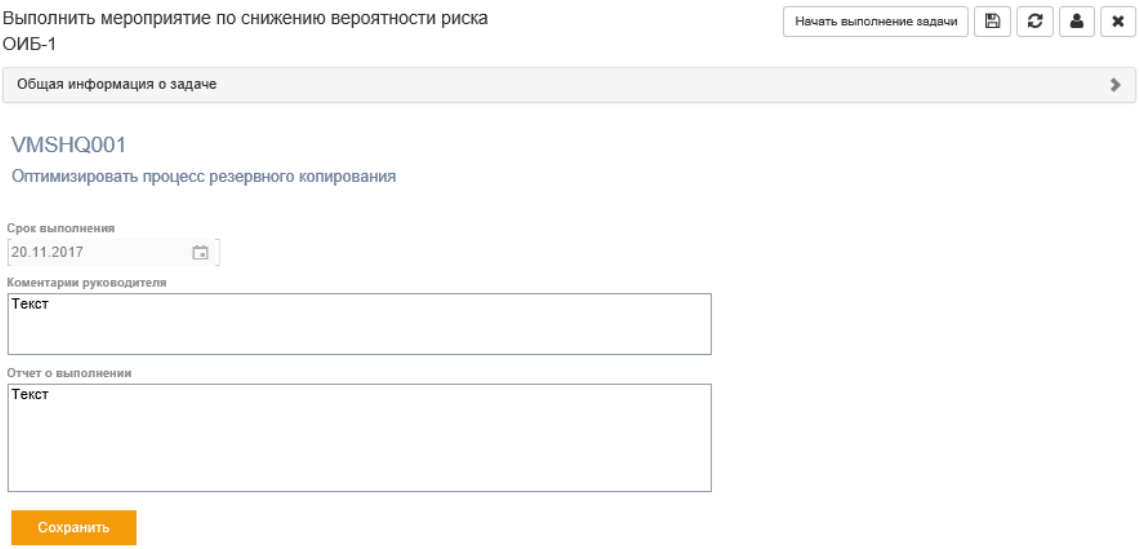

Рис. 23. Карточка мероприятия в задаче для ответственного

На Рисунок 24 представлен реестр выполненных мероприятий. Для просмотра результатов выполнения мероприятия, откройте карточку мероприятия двойным кликом мыши.

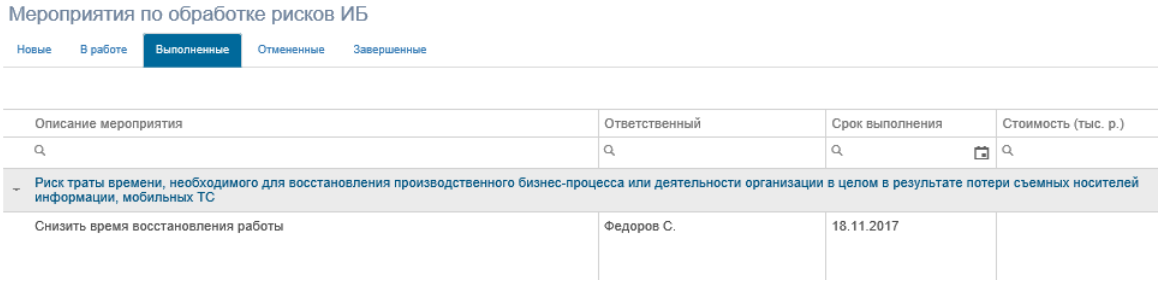

Рис. 24. Реестр выполненных мероприятий

На Рисунок 25 представлена карточка выполненного мероприятия. Используя эту карточку руководитель может ознакомиться с результатами выполнения мероприятия

(отчетом ответственного), указать затраты на выполнение мероприятия и принять решение о завершении данного мероприятия.

В случае, если все работы выполнены и мероприятие может быть завершено, нажмите на кнопку «Утвердить результаты».

Если для завершения мероприятия требуются дополнительные работы, введите при необходимости дополнительную информацию в поле «Комментарии руководителя», смените ответственного, если требуется и нажмите на кнопку «Вернуть в работу».

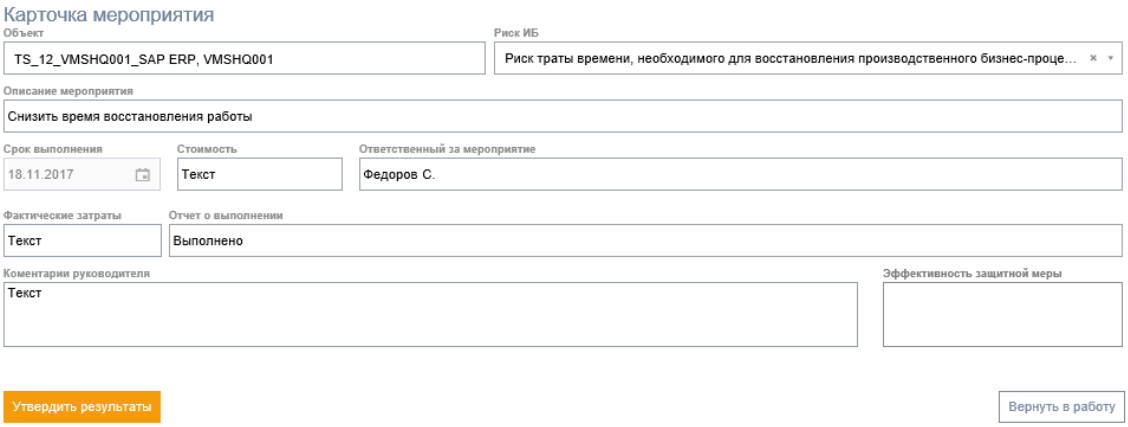

Рис. 25. Карточка выполненного мероприятия

В случае возврата задачи в работу будет назначена задача на указанного в мероприятии исполнителя, описание действий которого представлено выше (Рисунок 23).

Перед утверждением результатов выполнения мероприятия руководитель может установить новую эффективность защитной меры, связанной с этим мероприятием. При повторной оценке рисков для данного объекта защиты, эта оценка будет учитываться при оценке соответствующей защитной меры.

Статусы «Отменено» и «Завершено» являются конечными для процесса, дальнейшее выполнение работ для мероприятий в этих статусах невозможно.

4.4. Методика идентификации и оценки рисков

Раздел содержит описание этапов идентификации рисков и методики определения уровня риска на основании результатов идентификации.

Действия пользователей модуля, необходимые для выполнения процесса идентификации и оценки рисков представлены в разделах выше.

Все уровне оценки определяются по общей шкале уровней, имеющий следующие значения:

Значение уровня	Вес
Крайне высокий	0
Высокий	1
Средний	2

Низкий	3
Крайне низкий	4
Не оценивалось	-1

4.4.1. Определение области оценки

На этапе определения области оценки выполняется выбор объектов защиты, для которых будет выполняться процесс идентификации рисков.

Объекты защиты связываются с факторами последствий (см. Шкалы оценки, Типовые факторы последствий).

4.4.2. Оценка последствий

Для каждого фактора последствия, определенного для объекта защиты выполняется оценка возможного ущерба. Возможные варианты оценки для каждого фактора оценки определены в шкале оценки в разделе Типовые факторы последствий.

4.4.3. Оценка защитных мер для последствий

Производится выборка защитных мер, связанных с определенными на предыдущем этапе последствиями. Связь последствий и защитных мер должны быть определены заранее в справочном разделе «Последствия».

Связь между факторами оценки последствий и последствиями должен быть определен заранее в справочном разделе «Последствия»

Для каждой защитной меры определяется ее действительность и оценка эффективности этой меры. Оценка эффективности задана в шкале «Оценка эффективности ЗМ».

4.4.4. Определение и оценка угроз и уязвимостей

Определение угроз и уязвимостей выполняется по подтипам отобранных объектов защиты. Связь между подтипами объектов защиты, угрозами и уязвимостями определяется в справочнике «Угрозы».

Для каждой из уязвимостей определяется ее уровень, согласно шкале «Оценка уязвимости».

4.4.5. Определение и оценка защитных мер для уязвимостей

Для каждой уязвимости определяются связанные с этой уязвимостью защитные меры. Информация о связи уязвимостей и защитных мер задана в справочнике «Уязвимости».

Для каждой защитной меры определяется ее действительность и оценка эффективности этой меры. Оценка эффективности задана в шкале «Оценка эффективности ЗМ».

4.4.6. Идентификация и предварительная оценка возможных рисков

После определения для объекта защиты возможных последствий, угроз, уязвимостей и защитных мер выполняется формирование предварительного реестра возможных рисков по следующим правилам:

1. Отдельный риск формируется для каждой пары последствия и угрозы.
2. Для наименования риска используются наименования последствия и угрозы.
3. Для каждого риска сохраняются:
    - Уровень (вероятность) угрозы: значение для каждой угрозы задается в справочнике
    - Уровень уязвимости с учетом защитной меры (при наличии)
    - Уровень ущерба, вычисленный следующим образом:
        - Уровень ущерба **минимальный**, если уровень последствия минимальный или средний, а уровень защитных мер максимальный или средний.
        - Уровень ущерба **средний**, если уровень последствий максимальный, и уровень защитных мер максимальный или средний или уровень последствий средний и уровень защитных мер высокий или средний.
        - Уровень ущерба **максимальный** в остальных случаях.
4. Вычисляется уровень риска по формуле:

    Уровень угрозы + *Уровень уязвимости* + *Уровень ущерба* – *2*, уровень риска определяется следующим образом:

    - Если значение меньше 2, то уровень максимальный
    - Если значение от 2 до 5, то уровень средний
    - Если значение больше 5, то уровень минимальный.

    При этом уровни уязвимости, ущерба и защитных мер рассчитываются как максимальное среди оценок всех экспертов.

    При наличии ранее проведенных мероприятий, связанных с защитными мерами, которые оцениваются в текущем проекте, оценка эффективности защитной меры вычисляется как максимум текущей оценки и оценки установленной при проведении мероприятия.
5. Определяется приемлемость риска, на основании вычисленного значения уровня и определенных для проекта границ приемлемости риска.
6. Ручной пересчет уровня риска доступен после автоматического формирования реестра возможных рисков: для любого риска из реестра можно вручную установить значения уровне угрозы, уязвимости и ущерба, после чего уровень риска будет пересчитан по приведенной выше формуле.

4.4.7. Формирование реестра утвержденных рисков

Утверждение рисков выполняется в ручном режиме. После утверждения риск из предварительного реестра копируется в реестр утвержденных рисков.

Риск в реестре утвержденных рисков уникально идентифицируется объектом защиты, угрозой и последствием.

Если риск для объекта защиты с определенной угрозой и последствием уже существует, его параметры будут перезаписаны.

4.4.8. Вычисления на этапе формирования реестра утвержденных рисков

На этапе создания или изменения риска в реестре утвержденных рисков выполняются определение следующих его свойств:

1. **Вычисление вероятности риска.** Вероятность риска вычисляется по формуле:

   (Уровень угрозы + Уровень уязвимости) / 2

   Если вычисленное значение меньше 2, то уровень высокий, если равно двум средний, если больше двух либо один из параметров не определен, то низкий.
2. **Вычисление метода реагирования.** Метод реагирования определяется по уровню приемлемости риска, если уровень приемлемости риска «Не приемлемый» устанавливается значение «Снижение вероятности», в противном случае устанавливается значение «Принятие».
3. **Определение владельца риска.** В качестве владельца риска устанавливается должность лица, определенного как руководитель подразделения, являющего собственником объекта защиты.
4. **Создание реестра мероприятий.** Для рисков с установленным значением метода реагирования «Снижение вероятности» формируется реестр мероприятий. Реестр мероприятий формируется на основании защитных мер, определенных для данного риска. Ответственного за выполнение мероприятия лицом назначается автоматически указанный для объекта защиты администратор.