МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему «Разработка комплекта лабораторных работ по дисциплине «Управление информационной безопасностью телекоммуникационных систем»»

Исполнитель Березина Любовь Михайловна

(фамилия, имя, отчество)

Руководитель Богданов Павел Юрьевич

(фамилия, имя, отчество)

«К защите допускаю»
Заведующий кафедрой

(подпись)

Завгородний Владимир Николаевич

(фамилия, имя, отчество)

«___»_____20___г.

Санкт-Петербург

2019

РЕФЕРАТ

Дипломная работа: 130 с., 43 рис., 24 табл., 2 приложения, 20 источников литературы.

СИСТЕМА УПРАВЛЕНИЯ ИНФОРММАЦИОННОЙ БЕЗОПАСНОСТЬЮ, СТАНДАРТИЗАЦИЯ В ОБЛАСТИ СУИБ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ОБРАБОТКА РИСКОВ.

Объект исследования: учебно-образовательный процесс специальности ИБ ТКС.

Предмет исследования: учебная дисциплина УИБТКС.

Цель работы: актуализация лабораторных работ, для лучшего усвоения материала и освоения профессиональных компетенций.

В дипломной работе проводится анализ вопросов в области информационной безопасности, а также анализ существующих международных и отечественных стандартов для систем управления ИБ организации.

Разработан актуальный комплект лабораторных работ по дисциплине УИБТКС.

Разработано семь лабораторных работ с использованием различных программных средств и десять вариантов к ним, а также для проверки работоспособности разработан и сделан пробный вариант в соответствии с разработанными лабораторными работами.

Представленные в данной работе лабораторные работы предназначены для получения практических навыков при изучении дисциплины УИБТКС.

ОГЛАВЛЕНИЕ

Список сокращений

ФЗ – федеральный закон;

ИБ – информационная безопасность;

ФГОС ВО – федеральный государственный образовательный стандарт высшего образования;

УИБТКС - управление информационной безопасностью телекоммуникационных систем;

ВКР – выпускная квалификационная работа;

СМИБ – система менеджмента информационной безопасности;

ПО – программное обеспечение;

ПСК - профессионально-специализированные компетенции;

СУИБ – система управления информационной безопасностью.

ВВЕДЕНИЕ

Информация в том или ином виде окружала человечество всюду на протяжении всего его существования. Сам термин «информация» закрепился в научном сообществе с середины XX века и в соответствии Федеральным законом от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018) "Об информации, информационных технологиях и о защите информации" означает сведения (сообщения, данные) независимо от формы их представления.

В современном мире информация и такие основные информационные процессы как обработка, хранение и передача информации играют главную роль. Данная область является приоритетной в сферах внутренней и внешней безопасности страны, разведки, малого и крупного бизнеса и многих других. Во всех этих сферах остро стоит вопрос защищенности информации и каналов ее передачи[1].

Информационные технологии одни из самых динамично развивающихся отраслей современной науки. С развитием самих технологий растет и угроза информационной безопасности. А современная рыночная экономика диктует потребность поддержания ИБ на предприятии для его нормального функционирования. Для этого необходимо предотвращать возможные потери, которые могут привести к серьёзным последствиям на предприятии, связанные с уязвимостью в ИБ. Поэтому недостаточно лишь обеспечивать ИБ, также необходимо ею управлять для достижения приемлемого уровня безопасности информационных активов предприятия.

Согласно ФГОС ВО по специальности Информационная безопасность телекоммуникационных систем один из видов профессиональной деятельности выпускника, освоившего программу, это организационно-управленческая деятельность.

Данная совокупность факторов определяет актуальность настоящей ВКР, целью является «актуализация лабораторных работ, для лучшего усвоения материала и освоения профессиональных компетенций».

Для достижение сформулированной цели в ВКР поставлена и решена задача разработки методики изучения дисциплины УИБТКС в соответствии с требованиями к будущим специалистам.

Решение поставленной задачи требует её декомпозиции на пять подзадач:

1. Анализ существующих лабораторных работ по дисциплине УИБТКС;
2. Анализ существующих международных и российских стандартов и методов в области системы менеджмента ИБ;
3. Разработка актуальных лабораторных работ;
4. Разработка вариантов лабораторных работ;
5. Выполнение пробного варианта (Приложение 1).

Объектом исследования ВКР является учебно-образовательный процесс специальности ИБ ТКС. Предметом для исследования была выбрана учебная дисциплина УИБТКС.

Изначально для реализации поставленных задач нам дана учебная программа дисциплины УИБТКС и требуется актуализировать имеющиеся лабораторные работы.

В ходе выполнения ВКР возникли трудности такие как:

- Поиск необходимого современного ПО и его установка;
- Ответ на вопрос: «Каков уровень подготовки студентов?».

Затруднения связанные с поиском ПО преодолены путем обращения к разработчикам комплектов лабораторных работ и научному руководителю. В ходе исследования проблемы установки выяснилось, что для организации работы по установке ПО невозможно поставить нужные программы на виртуальные машины, а необходимо обладать правами администратора сети.

Затруднения, связанные с компетентностью студентов в вопросах УИБ решились обращению к учебному плану направления в целом.

Существующий комплект лабораторных работ устарел и не в полной мере отражает действительные навыки специалиста по ИБ.

Для решения поставленной задачи в рамках предлагаемого подхода ВКР имеет следующее содержание:

- Введение;
- 1 раздел – Анализ вопросов, рассматриваемых в курсе;
- 2 раздел – Анализ стандартов в области УИБ;
- 3 раздел – Разработка комплекта лабораторных работ;
- 4 раздел – Разработка вариантов к лабораторным работам;
- Заключение.

Введение имеет следующее содержание:

- 1 раздел посвящён рассмотрению основных тенденции социально-экономического и технико-технологического развития общества и их влияние на УИБ.

- 2 раздел посвящён постановке задачи на исследование в целом.
- 3 раздел посвящён состоянию вопроса.
- 4 раздел посвящён описанию содержания ВКР.
- 5 раздел посвящен основным положениям, выносимым на защиту.

В Заключении изложен отчет о решении поставленных задач и достижении поставленной цели.

Российские предприятия обладают проблемами в обеспечении ИБ. Некоторые из них:

- Непонимание руководством смысла в обеспечении ИБ;
- Недоработанная политика ИБ;
- Отсутствие процедуры анализа рисков;
- Недостаточность и нерегулярность аудитов и др.

В связи с этим основными положениями, выносимыми на защиту, являются:

- Решение данных проблем посредством управления ИБ ТКС;
- Для обучения будущих специалистов предлагается следующий список лабораторных работ:

1. Матричный подход к анализу рисков ИБ;
2. Разработка Политики ИБ организации;
3. Анализ рисков на основе ПО «РискДетектор»;
4. Анализ и управление рисками ИС на основе ПО «ГРИФ» пакета Digital Security Office;
5. Анализ рисков на основе моделей угроз и уязвимостей с помощью «ГРИФ» пакета DigitalSecurityOffice;
6. Анализ рисков на основе DigitalSecurity.КОНДОР;
7. Анализ рисков по методике CRAMM.

1 Анализ вопросов, рассматриваемых в курсе дисциплины «Управление информационной безопасностью ТКС

1.1 Проблемы обучения ИБ

1.1.1 Специальность «Информационная безопасность ТКС»

Специальность «Информационная безопасность телекоммуникационных систем» регламентирует Федеральный государственный образовательный стандарт и в соответствии с ним специальность имеет код 10.05.02.

Обучение проводится по уровню специалитета в очной форме обучения и должно составлять 330 зачетных единиц. Срок получения образования в очной форме обучения составляет 5,5 лет. Этот срок может меняться. Если обучение проводится в федеральных государственных организациях, ведущих подготовку кадров в интересах обороны и безопасности государства, обеспечение законности и правопорядка, указанных в части 1 статьи 81 Федерального закона от 29 декабря 2012 г. N 273-ФЗ "Об образовании в Российской Федерации", срок обучения должен быть не менее 5 лет. При обучении по индивидуальному учебному плану для лиц с ограниченными возможностями срок может быть увеличен по желанию не более чем на 1 год[2].

В РФ обучением по данной специальности занимается 21 Высшее учебное заведение. Среди них ЮФУ – Южный федеральный университет, ТУСУР – Томский государственный университет систем управления и радиоэлектроники, МГТУ ГА – Московский государственный технический университет гражданской авиации и РГГМУ – Российский государственный

гидрометеорологический университет. Первое место среди всех университетов по подготовке специалистов занимает ЮФУ, а РГГМУ находится на 12 строчке[3], но при поступлении в ЮФУ помимо ЕГЭ по русскому языку, математике и физика необходимо сдать физическую подготовку, хотя стоимость обучения несколько ниже.

Сама специальность занимает в рейтинге специальностей 98 место из 264[4].

1.1.2 Подходы к обучению

Существует 12 специализаций, по которым готовятся выпускники данной специальности:

- "Мониторинг в телекоммуникационных системах";
- "Системы представительской связи";
- "Сети специальной связи";
- "Специальный аудит информационной безопасности телекоммуникационных систем и объектов информатизации";
- "Системы специальной связи и информации для органов государственной власти";
- "Информационная безопасность космических телекоммуникационных систем";
- "Разработка защищенных телекоммуникационных систем";
- "Системы подвижной цифровой защищенной связи";
- "Защита информации в радиосвязи и телерадиовещании";
- "Защита информации в системах связи и управления";

- "Информационная безопасность мультисервисных телекоммуникационных сетей и систем на транспорте";

- "Безопасность телекоммуникационных систем информационного взаимодействия".

В соответствии с ФГОС по специальности одной из задач которые, выпускник, освоивший программу, должен уметь решать, является определение требований по защите информации, анализ защищенности телекоммуникационных систем и оценка рисков нарушения их информационной безопасности.

Структура учебной программы включает в себя обязательную (базовую) и вариативную части.

В связи с этим в учебном плане РГГМУ присутствует дисциплина: Управление информационной безопасностью телекоммуникационных систем. Она относится к базовой части учебного плана и включает в себя лекции и лабораторные занятия для освоения профессионально-специализированных компетенций, необходимых ему, в отличие от учебной программы МИРЭА - Российский технологический университет, в который включены только лекционные и практические занятия. А именно:

- способностью участвовать в разработке систем управления информационной безопасностью телекоммуникационных систем (ПСК-7.4);

- способностью обеспечивать защиту программных средств защищенных телекоммуникационных систем (ПСК-7.5).

1.2 Анализ вопросов обучения

1.2.1 Терминология в области управления ИБ

СУИБ – это система управления информационной безопасностью.

Система – это объединение объектов любой природы действующих друг на друга для достижения единой цели и обладающих такими системными свойствами как целостность, синергетичность, иерархичность, целенаправленность и многими другими.

Управление можно определить, как направленную на достижение цели, осмысленную деятельность человека, с помощью которой он организует и подчиняет своим интересам элементы живой и неживой природы.

Система управления такая система, которая исполняет функции управления. В её состав входят управляющая система и система связи. Главные вопросы, на которые она отвечает это чем и как управлять[5].

Информационная безопасность достигается за счет обеспечения конфиденциальности, целостности, доступности, достоверности и надежности информации. ИБ организации можно определить, как состояние защищенности интересов организации в условиях угроз информационной безопасности в информационной сфере[6].

Выделяют два вида подхода к обеспечению управления информационной безопасности.

1.2.1.1 Подходы

Системный подход – это методологическое направление изучения объекта как системы с разных сторон, комплексно, в совокупности отношений и связей между его элементами.

В управлении организации системный подход можно определить, как обнаружение, понимание и административное управление системой взаимосвязанных процессов с целью достижения стратегической цели.

Процессный подход – это систематическая идентификация и менеджмент применяемых организацией бизнес-процессов и особенно взаимодействия таких процессов[7].

Как видно из определения данный подход рассматривает организацию как сочетание основных бизнес-процессов, а не функциональных подразделений. Поэтому у процессного подхода есть преимущество в виде того что управление процессами происходит в рамках функциональной иерархии.

1.2.1.2 Циклическая модель PDCA

Так как при работе над УИБ мы имеем дело с системой для работы с ней используется циклическая модель PDCA. Её концепция впервые была описана в 1939 году У. Шухартом, а затем Э. Деминг ввел модификацию этого цикла (PDSA, S – study, т.е. изучать). Поэтому данный цикл носит название цикл Шухарта-Деминга.

Эта модель была разработана для описания цикла жизни любой системы и непрерывного улучшения процессов в

системе. Все процедуры должны последовательно проходить этапы данного цикла[8]:

- P – plan, т.е. планирование;
- D– do, т.е. делай;
- C – check, т.е. проверяй;
- A – act, т.е. воздействуй.

Планирование.

В процессе планирования должны быть установлены цели и пути достижения этих целей исходя из наличия ресурсов, которыми располагает предприятие. На данном этапе формируются задачи и устанавливается курс деятельности предприятия на определённый отрезок времени.

Планирование находится в постоянной переработке пока предприятие функционирует. Планирование рассматривается с точки зрения процессов необходимых для достижения поставленных целей. Поэтому необходимо советоваться с владельцами этих процессов и знать их текущее состояние и состояние, к которому нужно стремиться.

Планирование зависит от внешних факторов, таких как время, окружающая среда и др.

Выполнение.

Выполнение - осуществление запланированных мероприятий.

На данном этапе происходит создание некоторой структуры для выполнения назначенных задач и достижения поставленных целей. Но любой стандарт не идеален, поэтому всегда нужно полагаться на опыт квалифицированных сотрудников.

На каждом этапе цикла возникает проблема нехватки кадров, поэтому необходимо внедрять систему обучения кадров.

Проверка.

Проверка – сбор информации и контроль результата; выявление и анализ отклонений.

Данный этап необходим для достижения целей путем постоянного контроля и мониторинга процессов, описанных на прошлом этапе. Также нужно сообщать о полученных результатах, сравнивая их с ожидаемыми, для совершенствования системы. Если процессы идут в соответствии с планом, то корректировки не требуется, если обнаруживаются ошибки и отклонения от плана, то вмешательство руководства становится необходимым.

Воздействие.

Воздействие - принятие мер по устранению причин отклонений от запланированного результата; изменения в планировании и распределении ресурсов.

Если после этого этапа задачи не выполняются, то цикл следует повторить. Если после повторения цикла также не достигается поставленная цель, то следует пересмотреть цели, сделав их более реалистичными и достижимыми.

1.2.2 Актуальные вопросы управления ИБ

Оценка рисков является важнейшей подсистемой ИБ. В небольших организациях риск-менеджментом может заниматься один из руководителей, данная деятельность будет включена в его функциональные обязанности. Но с ростом

предприятия возникает потребность в отдельной кадровой единице для обеспечения требуемого уровня защищенности и своевременного реагирования на инциденты ИБ, а иногда и целой комиссии.

Риск-менеджер становится наиболее необходимым и популярным видом профессиональной деятельности[9].

Британский стандарт BS 7799-3 определяет требования, которым должен удовлетворять Риск-менеджер организации:

- Систематичные и организованные в своем подходе к мониторингу известных рисков и предложении соответствующих действий.

- Бизнес-ориентированные и осведомленные о текущем состоянии бизнеса и его приоритетах.

- Настойчивые и с независимым мышлением, но способные воспринимать противоположные точки зрения и идти им навстречу в случае, если это наилучшим образом помогает бизнесу.

- Способные убедительно представлять аргументацию (например, обоснование расходов на уменьшение высокого риска).

- Способные общаться на всех уровнях в организации.

- Обладающие хорошим пониманием риска, а также технологий и мер безопасности.

На основе рассмотренных международных стандартов, общих требований к специалисту по информационной безопасности и со спецификой работы (СУИР) в изучении дисциплины УИБТКС должны присутствовать разделы о политике информационной безопасности, о российских и

международных стандартах в области ИБ и об актуальных средствах оценки и обработки рисков предприятия.

1.2.2.1 Политика ИБ

Политика ИБ отражает принципы, практические методы и процедуры, а также совокупность правил в области ИБ, которыми руководствуется предприятие в рамках своей деятельности. Состав и содержание политики регламентирует отечественный стандарт ГОСТ Р ИСО/МЭК 17799-2005. В соответствии с ним политика ИБ должна включать в себя, как минимум[10]:

- определение информационной безопасности, её общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации;

- изложение целей и принципов информационной безопасности, сформулированных руководством;

- краткое изложение наиболее существенных для организации политик безопасности, принципов, правил и требований, например, таких как:

а)соответствие законодательным требованиям и договорным обязательствам;

б)требования в отношении обучения вопросам безопасности;

в)предотвращение появления и обнаружение вирусов и другого вредоносного программного обеспечения;

г)управление непрерывностью бизнеса;

д)ответственность за нарушения политики безопасности.

- определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности;

- ссылки на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры для конкретных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Чтобы реализовать предписания политики безопасности и тем самым противостоять угрозам безопасности должна достигаться цель выявления попыток нарушения политики безопасности, установка реакции на подобные попытки.

Поэтому компетентный специалист по ИБ, а в частности и риск-менеджер, должен иметь представление о назначении и значимом месте политики ИБ организации, а также обращаться к ней в ходе своей работы.

Выводы по первой главе:

Данная глава была посвящена введению терминологии и исследованию тематических источников и материалов. При это был проанализирован подход к обучению по специальности «Информационная безопасность телекоммуникационных систем», а в частности по специализации «Разработка защищенных телекоммуникационных систем», на которую обучает РГГМУ.

Наличие противоречий в учебных программах разных университетов, занимающихся подготовкой специалистов по данной специализации, еще больше обуславливает актуальность выбранной темы.

Также в главе была отражена значимость дисциплины УИБТКС в курсе подготовки и необходимость риск-менеджмента, в соответствии с международными и отечественными стандартами и временем, в котором мы живем, где информационные технологии играют одну из главных ролей в жизни каждого человека.

В следствии с обнаруженными фактами можно сделать вывод, что для получения практических навыков в изучении дисциплины УИБТКС требуются лабораторные занятия, для закрепления навыков и освоения профессиональных компетенций.

2 Анализ существующих международных и российских стандартов и методов в области системы менеджмента ИБ

2.1 Анализ международных и отечественных стандартов в области СМИБ

Так как информационная безопасность непосредственно связана с безопасностью интересов государства в области информатизации, существует государственное регулирование в данной области, представленное в виде стандартов.

2.1.1 BS 7799

Британский стандарт BS 7799 является основоположником международной стандартизации в области управления ИБ[11].

Его первая часть BS 7799-1 была разработана по заказу правительства Великобритании в 1995 году. В русском переводе название стандарта будет «Управление информационной безопасностью. Практические правила» (Code of Practice for Information Security Management).

Этот документ содержит 10 областей и 127 механизмов контроля, что в достаточной мере позволяет распланировать, обеспечить и поддерживать УИБ практически для всех организаций независимо от их размера, структуры или сферы деятельности. Он служит справочным материалом для руководителей и рядовых сотрудников.

В 2000 году данная версия стандарта была взята за основу международного стандарта ISO/IEC 17799:2000.

Вторая часть стандарта BS 7799-2 «Системы управления информационной безопасностью. Спецификация и руководство

по применению.» была разработана в мае 1999 года также Британским институтом стандартов и представляла собой кардинально пересмотренную первую часть. Данная часть также после пересмотра, который проводился в 2002 году, в 2005 году была утверждена в качестве международного стандарта ISO/IEC 27001:2005.

В 2006 году появилась третья часть стандарта BS 7799-3 «Системы управления информационной безопасностью. Руководство по управлению рисками информационной безопасности». Этот стандарт также применим к предприятиям любого размера и может быть использован руководителями и сотрудниками. В отличие от его предшественников, он не является международной версией стандарта ISO/IEC 27005:2008. Эти два стандарта взаимно перекликаются и дополняют друг друга.

2.1.2 Серия международных стандартов серии ISO/IEC 27000

Для оценки рисков ИБ стандарты семейства ISO/IEC 27000 служат фундаментом[12].

Их развитие включает в себя появление новых стандартов, которые более подробно углубляется в требования к отдельным процессам УИБ. Имея основу, в качестве стандарта ISO/IEC 27001:2005, они представляют собой руководства по управлению ИБ для различных сфер деятельности. Например, финансовой, страховой, здравоохранения и др.

На данный момент существует 46 стандартов данной серии, среди них:

- ISO/IEC 27000:2009 "Information technology. Security techniques. Information security management systems. Overview and vocabulary". Краткий обзор и словарь основных понятий.

- ISO/IEC 27001:2005 (BS 7799-2:2005) "Information technology. Security techniques. Information security management systems. Requirements". Основной стандарт по СУИБ содержащий в себе требования к СУИБ. На данный момент имеется новая версия стандарта 2013 года.

- ISO/IEC 27003:2010 "Information Technology. Security Techniques. Information Security Management Systems Implementation Guidance". Руководство по внедрению СУИБ, описывающее каждый этап более подробно и не затрагивающий функционирования, т.е. он содержит только рекомендации и никаких требований.

- ISO/IEC 27005:2011 "Information technology. Security techniques. Information security risk management". С помощью этого стандарта на предприятии можно произвести оценку рисков и их последующую обработку. Но несмотря на это сам стандарт носит описательный характер и не дает четких указаний и требований к управлению рисками в организации.

- ISO/IEC 27031:2012 "Information technology. Security techniques. Guidelines for information and communications technology readiness for business continuity". Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса.

- И др.

Также в области управления рисками имеет место быть американский стандарт NIST 800-300, положения которого

также учитывались при подготовке стандарта ISO/IEC 27005:2011.

2.1.3 ГОСТ Р ИСО/МЭК 27000

Для реализации СУИБ в РФ принята серия стандартов (на основе международных стандартов), которая регламентирует правила и требования построения таких систем, а также даёт определения основным понятиям в данной области.

Семейство отечественных стандартов ГОСТ Р ИСО/МЭК 27000 включает в себя стандарты[13]:

а)ГОСТ Р ИСО/МЭК 27004-2011 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмента ИБ. Измерения».

Стандарт взаимосвязан с международным стандартом ISO/ IEC 27004:2009.

Данный стандарт предлагает общие рекомендации и руководство действия при измерениях, их сборе для оценки рентабельности и производительности, внедрённой СУИБ на предприятия.

В приложениях стандарта содержатся типовые формы для заполнения при измерениях и приведены несколько примеров.

б)ГОСТ Р ИСО/МЭК 27006-2008 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента ИБ».

Стандарт взаимосвязан с международным стандартом ISO/ IEC 27006:2007.

Цель ГОСТа определить общие требования к сертификации или регистрации СУИБ предприятия, чтобы быть признанными достаточными и надежными для обеспечения заявленных функций СУИБ, а также содействовать при проведении аккредитации органов сертификации.

Международный стандарт есть в новой редакции 2011 года, который устанавливает новые требования для аудита и к квалификации аудиторов.

Стандарт состоит из нескольких разделов и информационных приложений.

в)ГОСТ Р ИСО/МЭК 27007-2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности».

Стандарт взаимосвязан с международным стандартом ISO/IEC 27007:2011.

Данный стандарт представляет собой дополнение к указаниям, содержащимся в ИСО 19011.

Требуется для понимания и проведения внутренних и внешних аудитов в организациях, которые нуждаются в его проведении.

г)ГОСТ Р ИСО/МЭК 27011-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002».

Стандарт взаимосвязан с международным стандартом ISO/IEC 27011:2008.

Данный стандарт представляется как дополнение к стандарту ИСО/МЭК 27002 и дает дополнительные рекомендации по организации СМИБ на предприятии.

Стандарт играет важную роль с точки зрения определения понятий «доступность», «целостность» и «конфиденциальность» информации, которые являются главными аспектами ИБ.

Под доступностью понимается то, что при необходимости должен обеспечиваться только санкционированный доступ к телекоммуникационной информации, оборудованию и среде, которые используются для предоставления услуг связи, обеспечиваемых с помощью проводной связи, радиосвязи или любыми другими способами.

Целостность подразумевает то, что установка и использование телекоммуникационных средств должны находиться под контролем, обеспечивающим уверенность в подлинности, точности и полноте информации, переданной, отправленной или полученной с помощью проводной связи, радиосвязи или любыми другими способами.

А конфиденциальность – это защищенность информации, имеющей отношение к телекоммуникационным организациям, от несанкционированного раскрытия.

2.1.4 СТО БР ИББС

Также помимо общих стандартов для обеспечения и управления ИБ существую отраслевые стандарты. Примером таких стандартов являются стандарты банковской сферы РФ.

Так как организации банковской сферы регулярно сталкиваются с инцидентами ИБ из-за постоянного внимания злоумышленников, задача ОИБ, а, следовательно, и УИБ, является важнейшим требованием бизнеса.

В настоящее время применяются 5 стандартов данной серии, а также 8 рекомендаций в области стандартизации.

Один из примеров стандарта данной серии является:

СТО БР ИББС-2.5-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности».

Данный документ дает рекомендации к реализации организацией БС РФ процесса обнаружения и реагирования на инциденты ИБ[14].

Взаимосвязан с требованиями данными в СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации/ Общие положения».

Инцидент ИБ определяется как событие ИБ или их комбинация, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ.

Менеджмент инцидентов ИБ - деятельность по своевременному обнаружению инцидентов ИБ, адекватному и оперативному реагированию на них, направленная на минимизацию и (или) ликвидацию негативных последствий от инцидентов ИБ для организации БС РФ и (или) ее клиентов.

2.2 Средства оценки и обработки рисков предприятия

Уязвимость – это недостаток программного (программно-технического) средства или ИС в целом, который может быть использован для реализации угроз безопасности информации[15].

Угроза (безопасности информации) - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Риск определяется как возможность воспользоваться уязвимостью, что впоследствии может привести к ущербу предприятия.

Для удобной, а главное действенной работы с рисками ИБ требуется ПО, которое будет удовлетворять требованиям[16]:

а)Интуитивный понятный интерфейс - для более легкого ориентирования в программе;

б)Поддержка русского языка – также для оптимизации работы с ПО;

в)Наличие предустановленных перечней угроз и активов – сокращение времени работы;

г)Многопользовательская работа и Web-доступ – для командной работы над проектом;

д)Добавление новых параметров – для более точной оценки риска, а не использование стандартной формулы риск = вероятность * ущерб;

ж) Подключение внешних источников данных – так как после оценки рисков параметры могут поменяться в

зависимости от произошедших событий и нам потребуется пересмотреть наши расчеты;

и) Инвентаризация защищаемых активов – для того чтобы программа самостоятельно вела учет активов предприятия;

к) Отображение процессов – для того чтобы видеть взаимосвязь с другими бизнес-процессами организации;

л) Визуализация рисков и инцидентов, оповещение – для наглядного мониторинга информационной системы;

м) И некоторые другие.

Это наиболее важные требования, возлагаемые на ПО, для обеспечения СМИБ на предприятии.

Мною были выбраны следующие программы и методики.

2.2.1 ГРИФ

Отечественный продукт для оценки рисков, использующий метод информационных потоков. Был разработан российской компанией «Digital Security». Его главным достоинством является отсутствие необходимости в специализированных знаниях. Однако данный продукт не имеет привязки к бизнес-процессам и возможности сравнения отчетов на разных этапах внедрения комплекса мер по обеспечению защищенности, что является минусом[17].

2.2.2 РискДетектор

Отечественный инструмент, разработанный Институтом системного анализа РАН. Позволяет решать такие проблемы как[18]:

- контроль и информированность о выполнении требований по безопасности.
- Полная картина состояния безопасности.
- Быстрое усвоение исполнителями требований по безопасности.
- Преодоление тенденций к оптимизации за счет невыполнения требований по безопасности.
- Повышение дисциплины выполнения требований во всех подразделениях.
- Усиление самоконтроля за выполнением требований, в том числе, за счет наличия полных и исчерпывающих списков требований на каждом рабочем месте и осуществления периодического контроля их выполнения.
- Быстрое реагирование на появление новых угроз путем оперативного доведения требований до исполнителей.
- Готовность к любым внешним проверкам по безопасности.
- Получение инструмента выбора и обоснования комплексов мер в области обеспечения безопасности.
- Повышение качества инспекционного контроля и сокращение затрат на инспекционный контроль.
- Обеспечение полноты требований. Устранение избыточности и противоречивости требований.

2.2.3 Матричный подход

Данный метод анализа объединяет активы, уязвимости, угрозы и средства управления и определяет важность различных средств управления, соответствующим активам организации[19]. Активы организации определяются как существенные с точки зрения защиты объекты, они могут быть как материальными, так и нематериальными.

Матричная методология использует три отдельных матрицы: матрицу уязвимостей, матрицу угроз и матрицу контроля, чтобы собрать необходимые данные для анализа рисков. Используется следующая система оценок: низкая, средняя и высокая.

При первоначальном анализе рисков формируются списки активов, уязвимостей, угроз и средств управления.

Данный подход может использоваться любым предприятием, независимо от его размера и сферы деятельности. Методология обеспечивает удобство, так как использующиеся шаблоны могут легко изменяться и дополнятся со временем и появлением новых обстоятельств. Также с помощью матриц предприятие способно само оценить риски.

2.2.4 КОНДОР

Программное обеспечение «КОНДОР» также, как и «ГРИФ» является разработкой отечественной компании «DigitalSecurity».

Данный программный комплекс предназначен для проверки ИС организации на соответствие международному стандарту ИБ ISO 17799. Для этого программа предлагает ответить на вопросы, которых более двухсот, в результате чего пользователь получает подробный отчёт о состоянии своей ИС на текущий момент. В отчёте отражаются как все требования, которым ИС соответствует, так и которым нет. Для несоответствующих требований программа даёт комментарии и советы экспертов.

2.2.5 CRAMM

Методика CRAMM является одной из первых методик для анализа рисков ИБ. Она была разработана службой безопасности Великобритании в середине 80-х гг. по заказу правительства[20].

Данный метод реализует комплексный подход к оценке рисков, т.е. сочетает в себе количественный и качественный анализ. Он подходит для предприятий любой формы (коммерческой/правительственной) и размера (крупных/малых). Также существует специальное ПО, осуществляющее анализ по данной методике.

При оценке рисков по данной методике проводятся интервью по заранее составленным подробным опросным листам.

В результате расчета рисков ИБ методика дает экономическое обоснование необходимых затрат на ИБ предприятия, позволяя избежать лишних.

Выводы по второй главе:

При СМИБ требуется полагаться на множество международных и отечественных стандартов по ИБ, которые обобщают многолетний опыт экспертов в данной области. Все стандарты так или иначе непрерывно связаны, дополняя друг друга или основываясь друг на друге.

Для управления ИБ требуется оценивать риски ИБ информационной системы предприятия. Для этих целей существует множество методик и соответствующих программных комплексов. В данной главе среди множества были выбраны методики, удовлетворяющие международным и российским стандартам в данной области, а также удовлетворяющие ряду требований, среди которых понятность, мобильность при изменении параметров ИС, возможность применения для организаций разных размеров и форм, а также для программ возможность поддержки русского языка и др.

Для ознакомления с разными возможными средствами и методиками при оценке уровня риска на следующем этапе будут составлены лабораторные работы, удовлетворяющие всем требованиям.

3 Разработка комплекта лабораторных работ

3.1 Матричный подход к анализу рисков ИБ

Лабораторная работа № 1

«Матричный подход к анализу рисков ИБ»

Цель работы: изучить основные понятия СМИБ.

Задание выполнение работы:

1. Выявить активы, уязвимости, угрозы (не менее 5 шт.) и средства управления в соответствии с вариантом задания;
2. Разработать соответствующие матрицы.

Теоретические сведения.

При оценке риска рекомендуется обращаться к международному стандарту ISO/IEC 27005 «Информационная технология - Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности», который обеспечивает рекомендации для менеджмента риском информационной безопасности в организации, в особенности поддерживая требования СМИБ согласно ISO/IEC 27001.

Матричная методология использует три отдельных матрицы: матрицу уязвимостей (Таблица 3.1.1), матрицу угроз (Таблица 3.1.2) и матрицу контроля (Таблица 3.1.3), чтобы собрать необходимые данные для анализа рисков.

Матрица уязвимостей содержит связь между активами и уязвимостями в организации, матрица угроз содержит в себе отношения между уязвимостями и угрозами, а матрица контроля содержит связи между угрозами и средствами управления. Значение в каждой ячейке матрицы показывает ценность отношения между элементом строки и столбца. Используется следующая система оценок: низкая, средняя и

высокая. При первоначальном анализе рисков формируются списки активов, уязвимостей, угроз и средств управления. Матрицы заполняются путем добавления данных о связи элемента столбца матрицы с элементом строки. Наконец, данные из матрицы уязвимостей преобразуются и заносятся в матрицу угроз. Таким же образом данные из матрицы угроз переносятся в матрицу контроля, которая содержит относительную важность средств управления.

Таблица 3.1.1 Пример матрицы активов

Шкала: **0 – нет воздействия** **1 – слабое воздействие** **2 – умеренное воздействие** **9 – сильное воздействие**	**Активы и затраты**	Торговые секреты	Конфиденциальная информация	Репутация	Потерянный доход	Затраты на восстановление	Информация	Аппаратные средства	Программное обеспечение	Обслуживание	Коммуникация
Уязвимость											
Веб-сервер											
Брандмауэр											
Маршрутизатор											

Совокупное воздействие уязвимости v на активы организации вычисляются по формуле:

$$V_i = \sum_{j=1}^{n} a_{ij} * C_j$$

Где:

C – это воздействие уязвимости v на активы.

a_i – это относительная стоимость актива.

Таблица 3.1.2 Пример матрицы угроз

Шкала: **0 – нет воздействия** **1 – слабое воздействие** **2 – умеренное воздействие** **9 – сильное воздействие**	**Угрозы**	Отказ в обслуживании	Вредоносный код	Ошибки пользователя	Внутренняя атака	Спам	Физическое повреждение аппаратных средств
Уязвимость							
Веб-сервер							
Брандмауэр							
Маршрутизатор							

Совокупное воздействие угрозы T_k определяется по формуле:

$$T_k = \sum_{j=1}^{n} d_{ij} * V_j$$

Где:

V – это воздействие уязвимости на активы.

d_i – это потенциальное воздействие угрозы уязвимости V.

Таблица 3.1.3 Пример матрицы контроля

Шкала: **0 – нет воздействия** **1 – слабое воздействие**	**Угрозы**	Отказ в	Вредоносн	Ошибки	Внутренняя	Спам	Физическое

2 – умеренное воздействие **9 – сильное воздействие** **Средства контроля**		обслуживании	ый код	пользователя	атака		повреждение аппаратных средств
Политика безопасности							
Брандмауэр							
Обучение персонала							

Относительное совокупное воздействие средств контроя Z_o определяется по формуле:

$$Z_o = \sum_{j=1}^{n} e_{ij} * T_j$$

Где:

T – это воздействие угрозы.

e_i – это воздействие средств контроля на угрозу.

Ход работы:

1.Выявить информационные активы (материальные и нематериальные), уязвимости, угрозы и средства контроля на предприятии, провести их оценку.

2.В соответствии с заданием составить матрицу уязвимостей, матрицу угроз и матрицу контроля.

3.Рассчитать совокупное воздействие уязвимости на активы, угрозы на уязвимости и средства контроля на угрозы.

Варианты заданий:

Варианты заданий представлены в файле var.pdf.

Контрольные вопросы.

1.Как определяется понятие Риск?

2. Что такое Уязвимость?

3. Что такое Угроза?

4. Что такое Актив?

5. Объясните, чем занимается СМИБ?

3.2 Разработка Политики ИБ организации

Лабораторная работа №2

«Разработка Политики ИБ организации»

Цель работы: изучить основные аспекты, включаемые в политику ИБ.

Задание выполнение работы:

1. Изучить политику ИБ «Газпромбанк»;

2. Разработать политику ИБ организации в соответствии с вариантом.

Теоретические сведения.

В соответствии с ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» определяются следующие нормы, касающиеся политики ИБ организации.

Мера и средство контроля и управления:

Политика информационной безопасности должна быть утверждена руководством, издана и доведена до сведения всех сотрудников организации и соответствующих сторонних организаций.

Рекомендация по реализации:

Политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к менеджменту информационной безопасности, Документ, в котором излагается политика, должен содержать положения относительно:

а)определения информационной безопасности, ее общих целей и сферы действия, а также упоминания значения безопасности как инструмента, обеспечивающего возможность совместного использования;

б)изложения намерений руководства, поддерживающих цели и принципы информационной безопасности в соответствии со стратегией и целями бизнеса;

в)подхода к установлению мер и средств контроля и управления, и целей их применения, включая структуру оценки риска и менеджмента риска;

г)краткого разъяснения наиболее существенных для организации политик безопасности, принципов, стандартов и требований соответствия, например:

- соответствие законодательным требованиям и договорным обязательствам;

- требования по обеспечению осведомленности, обучения и тренинга в отношении безопасности;

- менеджмент непрерывности бизнеса;

- ответственность за нарушения политики информационной безопасности;

д)определения общих и конкретных обязанностей сотрудников в рамках менеджмента информационной безопасности, включая информирование об инцидентах безопасности;

ж) ссылок на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры безопасности для определенных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Данная политика информационной безопасности должна быть доведена до сведения пользователей в рамках всей организации в актуальной, доступной и понятной форме.

Дополнительная информация:

Политика информационной безопасности может составлять часть документа по общей политике. Если политика информационной безопасности распространяется за пределами организации, следует принимать меры в отношении неразглашения чувствительной информации. Дополнительную информацию можно найти в ИСО/МЭК 13335-1.

Пересмотр политики информационной безопасности:

Мера и средство контроля и управления:

Политика информационной безопасности должна пересматриваться либо через запланированные интервалы времени, либо, если произошли значительные изменения, с целью обеспечения уверенности в ее актуальности, адекватности и эффективности.

Рекомендация по реализации:

Политика информационной безопасности должна иметь владельца, который утвержден руководством в качестве ответственного за разработку, пересмотр и оценку политики безопасности. Пересмотр заключается в оценке возможностей по улучшению политики информационной безопасности организации и подхода к менеджменту информационной

безопасности в ответ на изменения организационной среды, обстоятельств бизнеса, правовых условий или технической среды.

При пересмотре политики информационной безопасности следует учитывать результаты пересмотров методов управления. Должны существовать определенные процедуры пересмотра методов управления, в том числе график или период пересмотра.

Входные данные для пересмотра методов управления должны включать информацию об (о):

а)ответной реакции заинтересованных сторон;

б)результатах независимых пересмотров;

в)состоянии предотвращающих и корректирующих;

г)результатах предыдущих пересмотров методов управления;

д)выполнении процесса и соответствии политике информационной безопасности;

ж) изменениях, которые могли бы повлиять на подход организации к методам управления информационной безопасностью, включая изменения, касающиеся организационной среды, обстоятельств бизнеса, доступности ресурсов, контрактных, регулирующих и правовых условий или технической среды;

и) тенденциях в отношении угроз и уязвимостей;

к) доведенных до сведения инцидентах информационной безопасности;

л) рекомендациях, данных соответствующими органами.

Выходные данные пересмотра методов управления должны включать любые решения и действия относительно:

а)улучшения подхода организации к менеджменту информационной безопасности и ее процессов;

б)улучшения мер и средств контроля и управления и целей их применения;

в)улучшения распределения ресурсов и(или) обязанностей.

Пересмотр методов управления следует документировать.

Пересмотренная политика должна быть утверждена руководством.

Ход работы:

1.Изучить политику ИБ «Газпромбанк» и заполнить таблицу (Таблица 3.2.1).

2.По примеру изученной политики ИБ разработать Политику ИБ для своей организации по варианту.

Таблица 3.2.1 Основные аспекты политики ИБ

Основные объекты защиты системы ИБ.	
Цели в области информационной безопасности.	
Задачи обеспечения информационной безопасности.	
Принципы обеспечения информационной безопасности.	
Распределение ролей и ответственности.	
Ответственность за нарушение Политики информационной безопасности.	

Варианты заданий:

Варианты заданий представлены в файле var.pdf.

Контрольные вопросы.

1.Что такое Политика Информационной безопасности предприятия?

2.На основе какого (каких) нормативного (ых) документа (ов) строится Политика ИБ?

3.Что должна включать в себя Политика ИБ?

4.Когда или при каких обстоятельствах должна быть пересмотрена Политика ИБ?

5.Кем утверждается Политика ИБ предприятия?

3.3 Анализ рисков на основе ПО «РискДетектор»

Лабораторная работа № 3

«Анализ рисков на основе ПО «РискДетектор»

Цель работы: знакомство и работа с автоматизированной системой управления рисками РискДетектор.

Задание выполнение работы:

1.Выполнить пробный вариант;

2.В соответствии с описанием системы внести данные в программный комплекс.

Теоретические сведения.

Автоматизированная система РискДетектор является отечественной разработкой Института системного анализа РАН.

РискДетектор позволяет осуществлять аудит, управление рисками, мониторинг, контроль фундаментальной

безопасности, обеспечить качество критериев и нормативной базы.

Проблемы, которые позволяет решать система РискДетектор[21]:

- Контроль и информированность о выполнении требований по безопасности. Полная картина состояния безопасности.

- Быстрое усвоение исполнителями требований по безопасности.

- Преодоление тенденций к оптимизации за счет невыполнения требований по безопасности.

- Повышение дисциплины выполнения требований во всех подразделениях.

- Усиление самоконтроля за выполнением требований, в том числе, за счет наличия полных и исчерпывающих списков требований на каждом рабочем месте и осуществления периодического контроля их выполнения.

- Быстрое реагирование на появление новых угроз путем оперативного доведения требований до исполнителей.

- Готовность к любым внешним проверкам по безопасности.

- Получение инструмента выбора и обоснования комплексов мер в области обеспечения безопасности.

- Повышение качества инспекционного контроля и сокращение затрат на инспекционный контроль.

- Обеспечение полноты требований. Устранение избыточности и противоречивости требований.

Ход работы:

1.Изучить работу системы, выполнив пробный вариант из описания лабораторной работы

1.1 Создание модели

Перед началом работы необходимо авторизоваться в системе. Для этого используйте пару Имя пользователя-Пароль: system-system.

Во-первых, необходимо создать Модель. Для этого, нажав правой кнопкой мыши (ПКМ), выбираем *Создать-Модель* и называем её «ОрганизацияПример».

Аналогично в созданной модели создать Регион, назвав его «В целом по организации».

Следующим шагом для созданного региона требуется создать Локальную среду. ПКМ нажимаем на наш Регион и создаем две Локальные среды под названием «В целом по организации» и «ИС» соответственно.

Для Локальной среды «В целом по организации» создать Подсистемы «Организация в целом» и «ОУД1 Требования и профили защиты по ГОСТ Р 15408 - 2002», а для «ИС» Подсистемы: «ИВЦ», «Экономический отдел», «Бухгалтерия».

В созданных Подсистемах ПКМ создаем объекты. Для каждого нового объекта по требуется выбрать класс (Таблица 3.3.1).

Таблица 3.3.1 Объекты

Подсистема	Название объекта	Класс объекта
Организация в целом	Автоматизированная система организации	Автоматизированная система
	Идентификация и аутентификация	БСБ Требования ГОСТ Р ИСО/МЭК 15408-2002, применимые к

		большинству базовых сервисов безопасности
	Информационные ресурсы организации	Ресурсы АИС
	Критически важные сервисы/приложения организации	Критически важные сервисы/приложения организации
	Организация с АИС	Типовая организация с АИС
ОУД1 Требования и профили защиты по ГОСТ Р 15408 - 2002	ОУД1	ОУД1
	Профиль защиты ОС	Профиль защиты ОС
	Профиль защиты СУБД	Профиль защиты СУБД
	Требования ГОСТ Р ИСО/МЭК 15408 - 2002	Требования ГОСТ Р ИСО/МЭК 15408 – 2002
ИВЦ	Программное обеспечение	Программное обеспечение

Продолжение Таблицы 3.3.1

Экономический отдел	АРМ	АРМ
	Программное обеспечение	Программное обеспечение
	Информация о з/п	Ресурсы АИС
Бухгалтерия	АРМ	АРМ
	Программное обеспечение	Программное обеспечение
	Бухгалтерская информация	Ресурсы АИС

Для каждого созданного объекта требуется определить выполняемые требования по мерам защиты. Для этого необходимо перейти во вкладку Выполнение мер и требований по объекту. Условие выполнения требования можно изменить с

помощью двойного щелчка. Требования со значением «Нет» представлены в Таблицах 3.3.2-3.3.10.

Таблица 3.3.2 Перечень мер - Автоматизированная система организации

Меры защиты	Требования по мере
М.06.01. Обеспечить безопасное выполнение операционных процедур и обязанностей	1,4,5
М.06.02. Планирование развития АИС и приемки новых систем с целью сведения рисков отказов к минимуму	1-4
М.07.01. Производственные требования к управлению доступам к системам	1
М.06.03. Защита от вредоносного программного обеспечения	1
М.06.04. Обслуживание систем	1-4

Продолжение Таблицы 3.3.2

М.06.05. Сетевое администрирование	1
М.06.06. Оперирование носителями информации и их защита	1-4
М.07.02. Управление доступом пользователей	1,3,4
М.07.05. Управление доступом к компьютерам	1-3,5-7
М.07.07. Слежение за доступом к системам и их использованием	1-3
М.08.01. Выполнение требований к безопасности систем	1

Таблица 3.3.3 Перечень мер – Идентификация и аутентификация

Меры защиты	Требования по мере

Аудит безопасности работы пользователей	3,5
Криптографическая поддержка	3,5
Защита данных пользователя	3
Идентификация и аутентификация пользователей при доступе к сервисам безопасности	2,5,8
Управление сервисом безопасности	4,6,8
Защита КСБ	10,12,13,15
Обеспечение безопасности доступа к сервису безопасности	2,4

Таблица 3.3.4 Перечень мер – Информационные ресурсы организации

Меры защиты	Требования по мере
М.03.01. Обеспечение ответственности за информационные ресурсы	1

Продолжение Таблицы 3.3.4

М.03.01. Обеспечение ответственности за информационные ресурсы	1
М.08.02. Безопасность в прикладных системах	1-4
М.08.03. Защита файлов прикладных систем	1

Таблица 3.3.5 Перечень мер – Критически важные сервисы/приложения организации

Меры защиты	Требования по мере
М.05.01. Безопасное размещение частей ИС, поддерживающих критически важные или уязвимые сервисы организации	1,5,6

Таблица 3.3.6 Перечень мер – Организация с АИС

Меры защиты	Требования по мере
М.02.01. Создание инфраструктуры управления информационной безопасностью	1-7
М.09. Планирование бесперебойной работы организации	1-4
М.10.01. Выполнение правовых требований	1-4
М.10.02. Проверка безопасности информационных систем	1,2
М.10.03. Аудит систем	1,2

Таблица 3.3.7 Перечень мер – Профиль защиты ОС

Меры защиты	Требования по мере
Требования доверия к безопасности ACM. Управление конфигурацией	2, 9-14, 17-26
Требования доверия к безопасности ADV. Разработка	1-17
Класс FDP. Защита данных пользователя	1-6
Класс FMT. Управление безопасностью	7-13

Таблица 3.3.8 Перечень мер – АРМ

Меры защиты	Требования по мере
Подбор и инструктирование персонала	1,3
Обеспечение реагирования на события, несущие угрозу безопасности	2,4

Таблица 3.3.9 Перечень мер – Программное обеспечение

Меры защиты	Требования по мере
Безопасность в среде разработки и рабочей среде	1,3

Таблица 3.3.10 Перечень мер – Информация

Меры защиты	Требования по мере
М.03.02. Классификация информации по уровням конфиденциальности	1,2
М.06.06. Оперирование носителями информации и их защита	1-4

Продолжение Таблицы 3.3.10

М.08.02. Безопасность в прикладных системах	3
М.08.03. Защита файлов прикладных систем	2

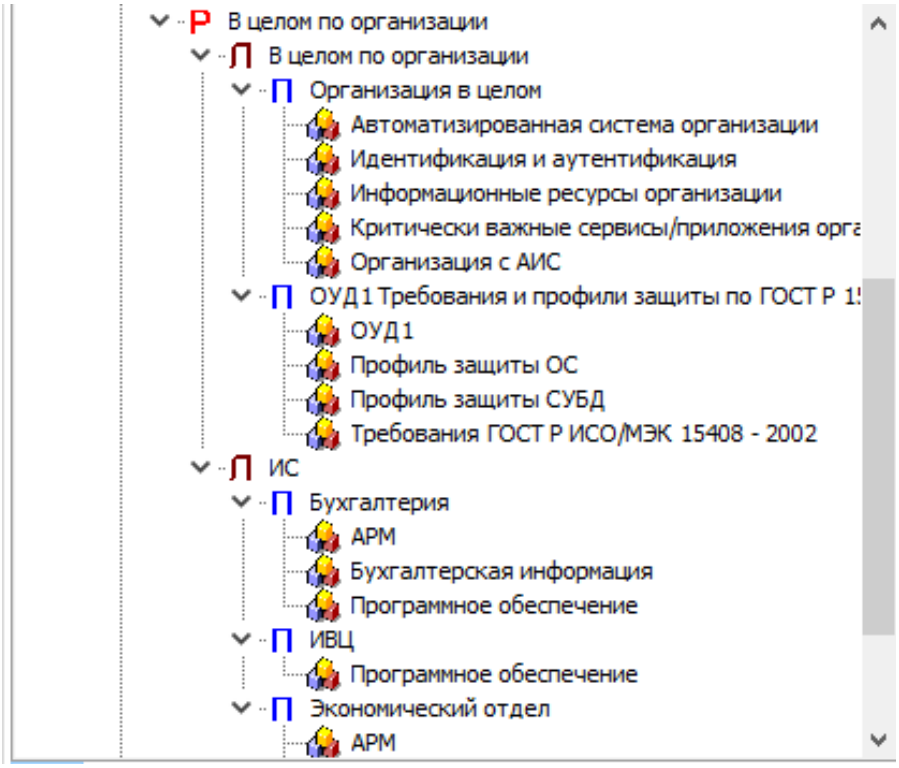

Рисунок 3.3.1 - Структура организации

После всех манипуляция структура должна выглядеть как на Рисунке 3.3.1.

1.2 Формирование отчета

Далее с помощью специальной кнопки рассчитаем риски как показано на Рисунке 3.3.2

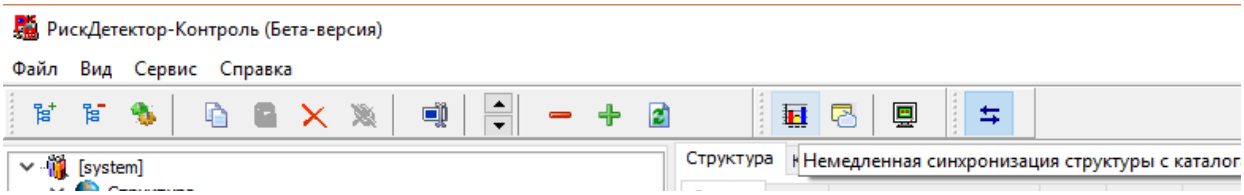

Рисунок 3.3.2 - Расчет рисков

Далее сохраняем отчет. Для этого ПКМ нажимаем на нашу модель и выбираем *Отчёты-Структурное описание оцениваемой системы* как показано на Рисунке 3.3.3

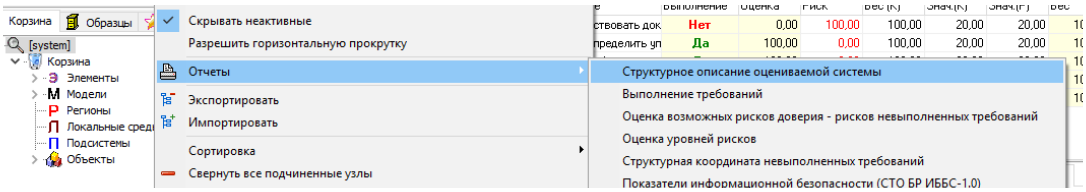

Рисунок 3.3.3 - Сохранение отчета

2. В соответствии с вариантом внести данные в систему и подготовить отчет

- Подсчитать количество рабочих станций
- Меры и требования защиты выбрать исходя из логических соображений (в реальной ситуации будет необходимо узнать об их наличие/отсутствие на организации).

В выводе отразить значения риска в целом, риска конфиденциальности, целостности и доступности.

Варианты заданий:

Варианты заданий представлены в файле var.pdf.

Контрольные вопросы.

1. Что представляет собой система РискДетектор и для каких целей она предназначена?
2. Кто разработал РискДетектор?
3. Как выглядит срез структуры?
4. Какие виды отчетов можно получить для среза структуры?
5. Приведите примеры мер защиты для Ресурсов АИС?
6. Перечислите требования к мере защиты: Классификация информации по уровням конфиденциальности.

3.4 Анализ и управление рисками ИС на основе ПО «ГРИФ» пакета DigitalSecurityOffice

Лабораторная работа № 4

«Анализ и управление рисками ИС на основе ПО «ГРИФ» пакета DigitalSecurityOffice»

Цель работы: знакомство и работа с системой анализа и управления информационными рисками ГРИФ.

Задание выполнение работы:

1. В соответствии с описанием системы составить таблицу, содержащую отделы и перечень ресурсов.
2. Составить матрицу доступа.
3. В соответствии с описанием системы по варианту внести данные в программный комплекс и составить отчёт.

Теоретические сведения.

Система «ГРИФ 2006» разработана для комплексного управления информационной безопасностью российской компанией DigitalSecurity, которая является одной из ведущих

российских консалтинговых компаний в области информационной безопасности.

Она позволяет проводить оценку риска двумя методами: «Анализ модели информационных потоков» и «Анализ модели угроз и уязвимостей». Выбор подхода зависит от сведений, которыми располагает пользователь или от того, что он хочет получить в отчёте. В данной работе воспользуемся первым методом.

При работе с моделью информационных потоков в систему вносится вся информация обо всех ресурсах с ценной информацией, пользователях, имеющих доступ к этим ресурсам, видах и правах доступа. Заносятся данные обо всех средствах защиты каждого ресурса, сетевые взаимосвязи ресурсов, а также характеристики политики безопасности компании. В результате получается полная модель информационной системы с точки зрения информационной безопасности с учетом реального выполнения требований комплексной политики безопасности, что позволяет перейти к программному анализу введенных данных для получения комплексной оценки рисков и формирования итогового отчета.

Основные понятия:

Ресурс – физический ресурс, на котором располагается ценная информация (сервер, рабочая станция, мобильный компьютер и т.д.).

Информация – ценная информация, хранящаяся и обрабатываемая в ИС. То есть объект, к которому осуществляется доступ.

Средства защиты – средства защиты ресурса, на котором расположена (или обрабатывается) информация и средства

защиты самой информации, т.е. применяемые к конкретному виду информации, а не ко всему ресурсу.

Контрмера – действие, которое необходимо выполнить для закрытия уязвимости.

Риск – вероятный ущерб, который понесет организация при реализации угроз информационной безопасности, зависящий от защищенности системы.

Ход работы:

1. Перечень отделов и ресурсов организации.

Для начала работы с комплексом необходимо иметь понятие об информационной системе (ИС) организации. Для этого составим таблицу отражающую перечень всех отделов, сетевых групп, сетевых устройств, видов информации, групп пользователей, бизнес-процессов и ресурсов на предприятии (Таблица 3.4.1).

Таблица 3.4.1 Отделы и ресурсы предприятия

Объекты	
Отделы	
Сетевая группа	
Ресурсы	
Сетевое устройство	
Вид информации	
Группа пользователей	
Бизнес-процесс	

Для примера разберем предприятие, состоящее из одного отдела – Бухгалтерия. Имеются сервер и рабочая станция, которые физически связаны между собой. На сервере хранятся два вида информации: бухгалтерский отчет и база клиентов; на рабочей станции база данных наименований товаров с описанием. В компании есть три сотрудника: финансовый директор, главный бухгалтер, бухгалтер. К бухгалтерскому

учету на сервере локальный доступ имеет главный бухгалтер, к базе клиентов удаленный доступ имеют бухгалтер (с рабочей станции через коммутатор) и финансовый директор. Причем финансовый директор имеет удаленный доступ через Интернет. К базе данных наименований товаров с описанием на рабочей станции локальный доступ имеет бухгалтер.

2. Матрица доступа

Матрица доступа будет иметь следующий вид:

Таблица 3.4.2 Матрица доступа

	Бухгалтерский отчёт	База клиентов	База данных товаров
Главный бухгалтер	WRE, Л	-	-
Бухгалтер	-	R, У, V	WRE, Л
Финансовый директор	-	WR, У, V	-
Примечания	W-запись R-чтение E-изменение V-наличие VPN – соединения - - нет прав доступа Л/У – локальный/удаленный вид доступа		

3. Использование программного комплекса

3.1 Модель информационных потоков

Перед началом работы необходимо авторизоваться в системе. Для этого запустите ярлык «ГРИФ» на рабочем столе

и используйте пару Имя пользователя-Пароль: student-password.

В начале работы программа попросит выбрать алгоритм анализа рисков. Необходимо выбрать пункт «Анализ модели информационных потоков» и создать новый проект как представлено на Рисунке 3.4.1. Название проекта задать в соответствии с названием предприятия по варианту.

Данный алгоритм предполагает три шага.

Шаг 1: Пользователю необходимо внести все объекты системы ИС, к которым относятся отделы, ресурсы (специальными объектами являются сетевые группы, сетевые устройства, виды информации, группы пользователей, бизнес-процессы).

Шаг 2: На этом шаге пользователь должен определить к каким отделам и сетевым группам относятся ресурсы, какая информация хранится на ресурсе и какие группы пользователей имеют к ней доступ, таким образом, проставляются связи. Также на данном шаге указываются средства защиты информации и ресурсов.

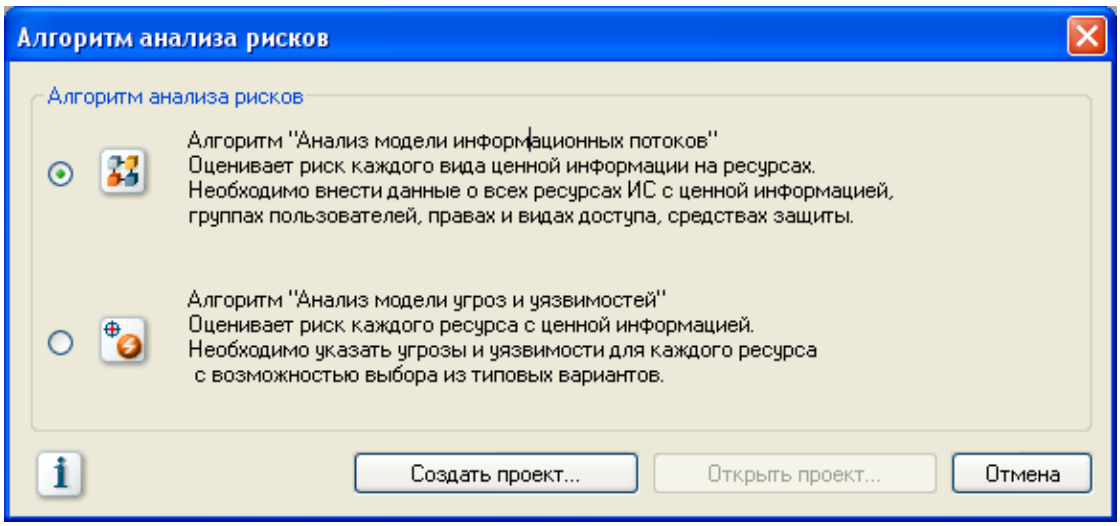

Рисунок 3.4.1 - Алгоритм анализа рисков

Шаг 3: Этот шаг предполагает ответы на список вопросов по политике безопасности, реализованный в системе, что позволяет оценить реальную степень защищенности системы и детализировать оценки рисков ИБ.

3.2 Модель ИС

Пример:

Так как у нас имеется лишь один отдел, значит и сетевая группа будет единственная. Добавим отдел и сетевую группу под названием «Бухгалтерия». Для этого нажмем кнопку «*Добавить*» в соответствующем разделе как на Рисунке 3.4.2 и Рисунке 3.4.3.

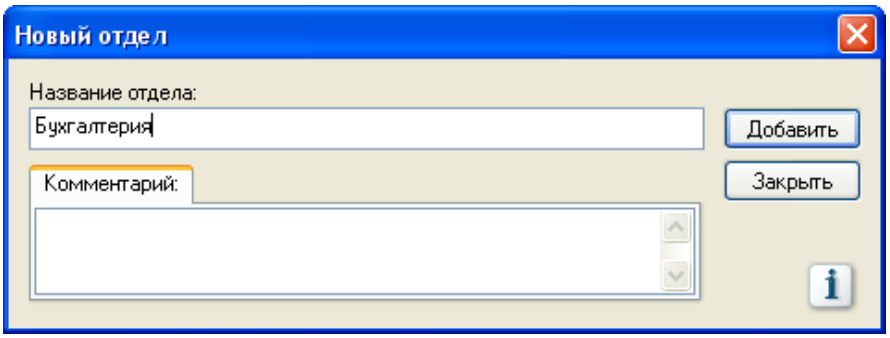

Рисунок 3.4.2 - Добавление нового отдела

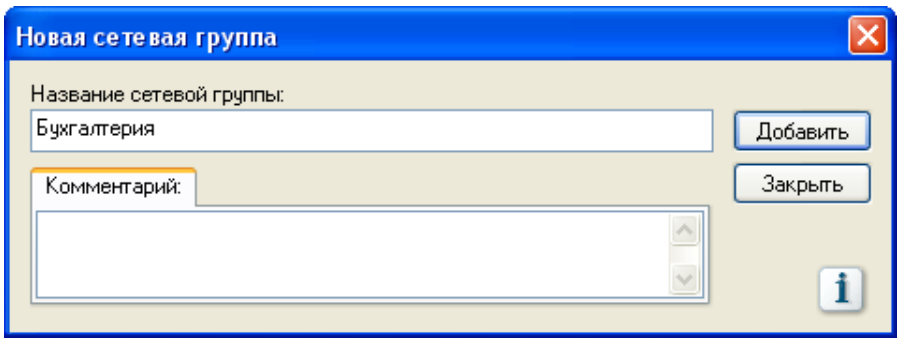

Рисунок 3.4.3 - Добавление новой сетевой группы

Из описания ИС мы видим, что у нас имеется два вида ресурсов. Это сервер и рабочая станция, которые связаны

между собой, т.е. находятся в одной сетевой группе. Добавление ресурса происходит аналогично добавлению отделов и сетевых групп как на Рисунке 3.4.4. Не забудьте указать сетевую группу и отдел.

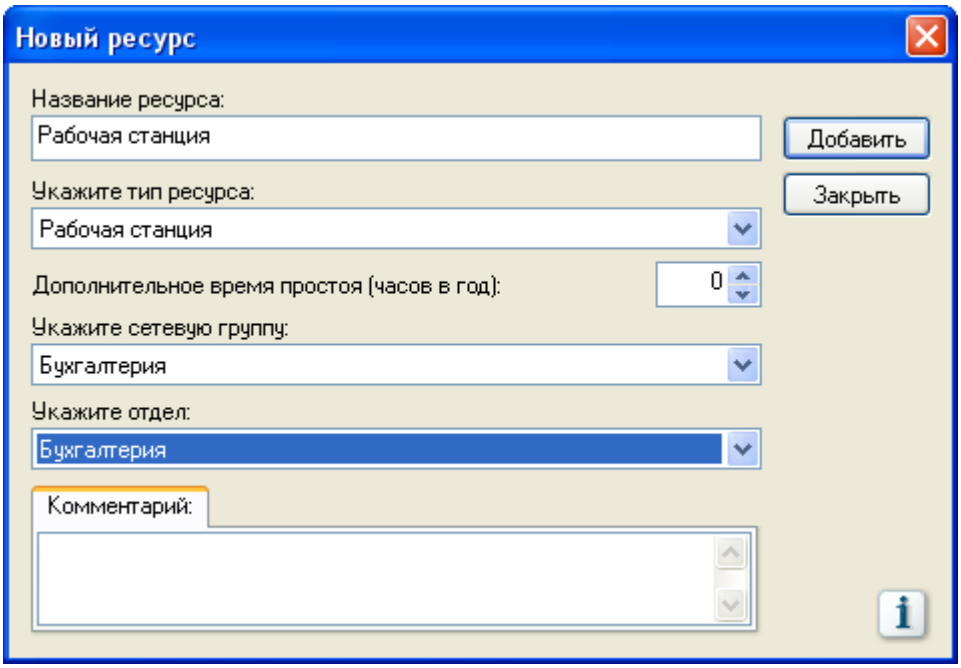

Рисунок 3.4.4 - Добавление нового ресурса

Далее необходимо добавить виды информация, имеющиеся у нас в системе. Бухгалтерский отчет, база клиентов и база данных наименований товаров с описанием. Добавим их в соответствии с описанием системы как показано на Рисунке 3.4.5.

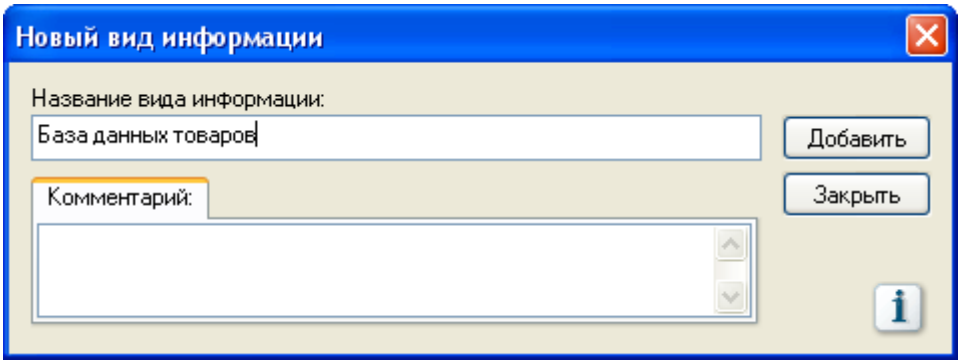

Рисунок 3.4.5 - Добавление Вида информации

Создадим три группы пользователей: главный бухгалтер, бухгалтер и финансовый директор, указав класс как на Рисунке 3.4.6.

В зависимости от выбора класса будут предложены средства защиты рабочего места группы пользователей. Средства защиты клиентского места групп авторизованных интернет-пользователей (здесь – финансовый директор) оценить невозможно, т.к. неизвестно, откуда будут осуществлять доступ пользователи этой группы.

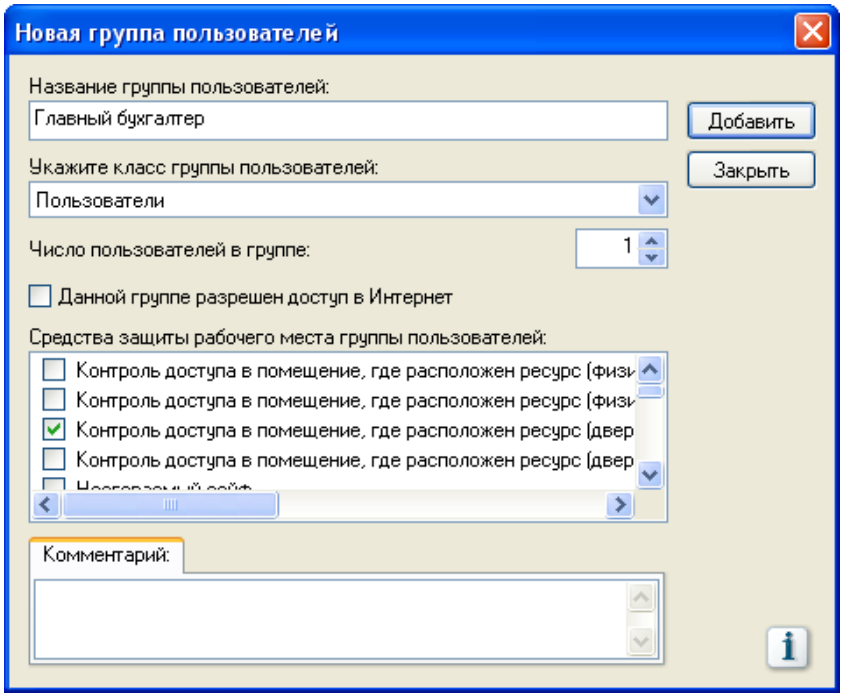

Рисунок 3.4.6 - Создание групп пользователей

Для того чтобы группы пользователей имели доступ к информации необходимо добавить сетевое устройство – Коммутатор представленное на Рисунке 3.4.7.

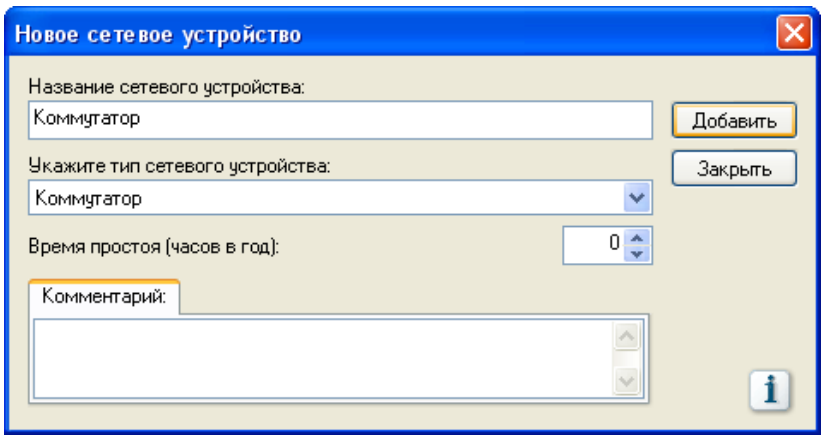

Рисунок 3.4.7 - Добавление сетевого устройства

3.3 Связи

При расстановке связей происходит определение, к каким отделам и сетевым группам относятся ресурсы, какая информация хранится на ресурсе и какие группы пользователей имеют к ней доступ, а также указываются средства защиты ресурса и информации.

В левом нижнем углу необходимо выбрать пункт *Связи*.

Нам требуется добавить виды информации «Бухгалтерский отчет» и «База клиентов» к ресурсу «Сервер». Для этого необходимо нажать кнопку «Добавить» во вкладке «Виды информации» и выбрать требуемые пункты. Потребуется установить ущерб по угрозе как изображено на Рисунке 3.4.8.

Для изменения единиц измерения требуется нажать Проект - Свойства проекта, вкладка «Единицы измерения».

Для ресурса «Рабочая станция» добавить вид информации «База данных товаров» аналогично.

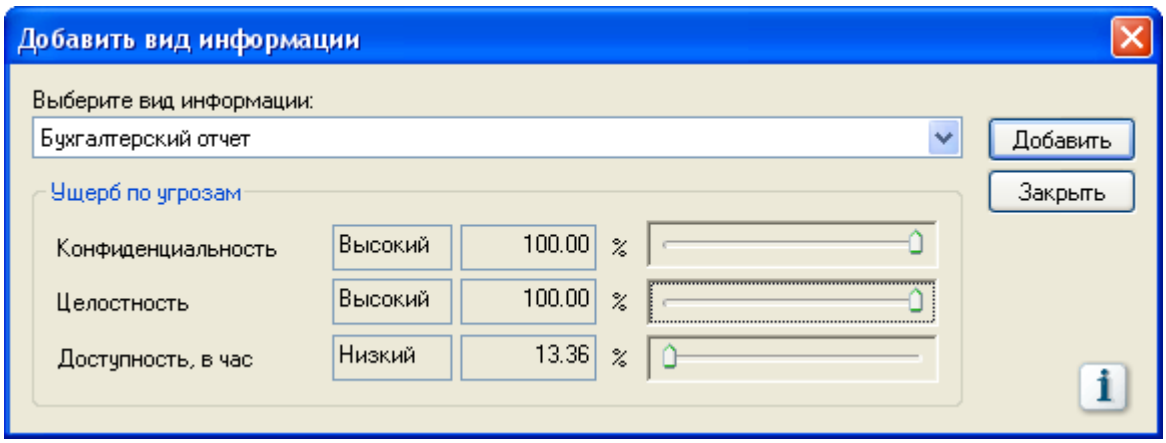

Рисунок 3.4.8 - Установка ущербов по угрозе

Во вкладке «Группы пользователей» требуется указать группы пользователей и их права на конкретный ресурс как на Рисунке 3.4.9.

Права доступа представлены в Таблице 3.4.2.

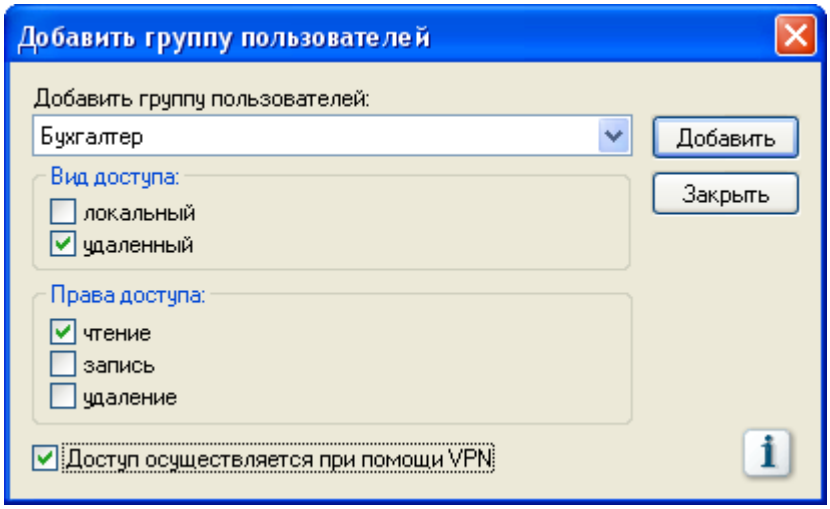

Рисунок 3.4.9 - Определение прав доступа к ресурсу

После определения всех прав доступа необходимо перейти во вкладку «Каналы связи» ресурса «Сервер» и указать, что группа пользователей «Бухгалтер» имеет доступ через сетевое устройство «Коммутатор». Для этого нажмите кнопку «*Изменить*», скриншот изображен на Рисунке 3.4.10.

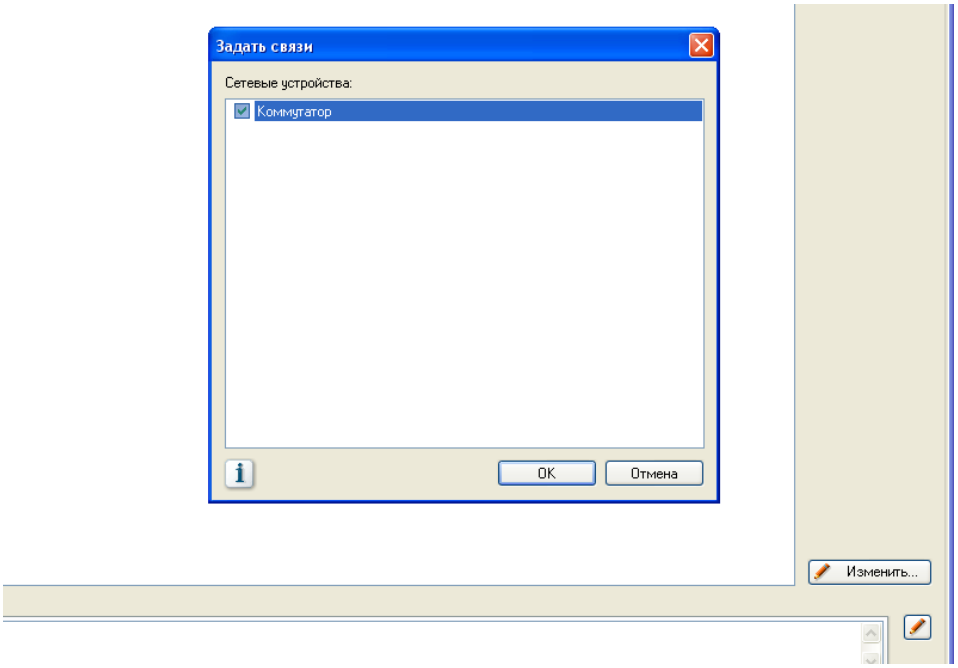

Рисунок 3.4.10 - Добавление сетевого устройства

Указание средств защиты возможно двумя способами.

Способ 1: перейдите на вкладку «Средства защиты», нажмите кнопку «*Изменить*» как показано на Рисунке 3.4.11 и укажите для ресурса «Сервер» следующие пункты: контроль доступа в помещение, где расположен ресурс (физическая охрана, дверь с замком, специальный пропускной режим в помещение); отсутствие возможности подключения внешних носителей; межсетевой экран; обманная система; система антивирусной защиты на сервере; аппаратная система контроля целостности.

Способ 2: Чтобы указать средства защиты ресурса для ресурса «Рабочая станция» задайте средства защиты из шаблона. Выбрать группу пользователей «Бухгалтер» как на Рисунке 3.4.12. Средства выберутся автоматически.

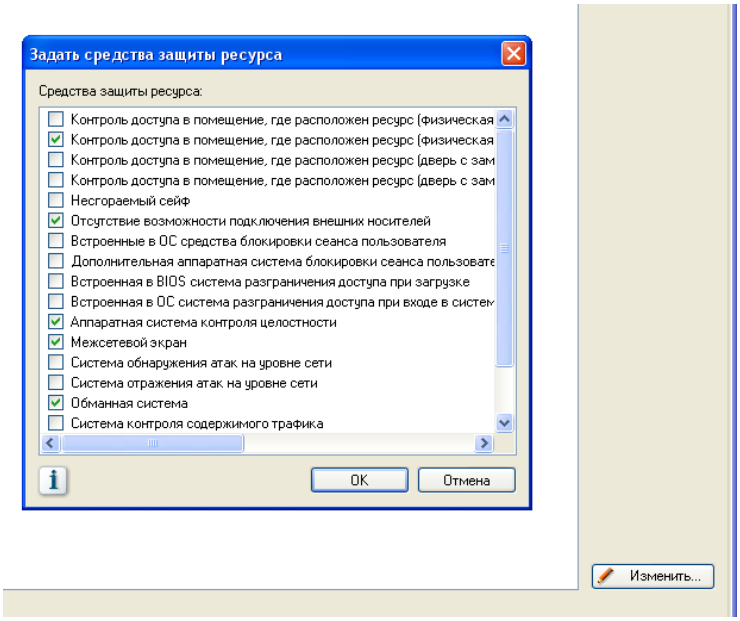

Рисунок 3.4.11 - Средства защиты для ресурса «Сервер»

Последним шагом требуется указать средства защиты для каждого вида информации как на Рисунке 3.4.13. Для вида информации «Бухгалтерский отчет» отметьте все средства защиты, кроме «Дополнительная программно-аппаратная система контроля доступа». Для вида информации «База клиентов» средств защиты информации нет. Для вида информации «База данных наименований товаров» укажите пункты «Резервное копирование» и «программная система контроля целостности».

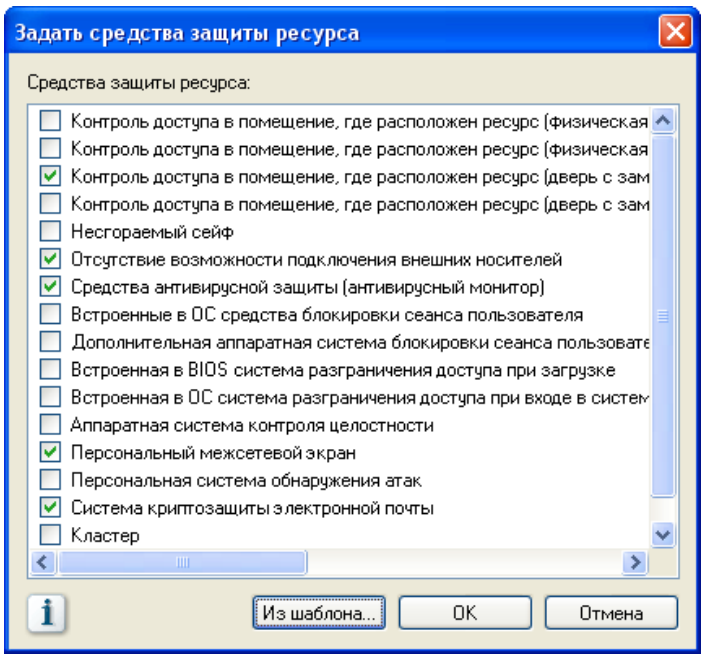

Рисунок 3.4.12 - Средства защиты для ресурса «Рабочая станция»

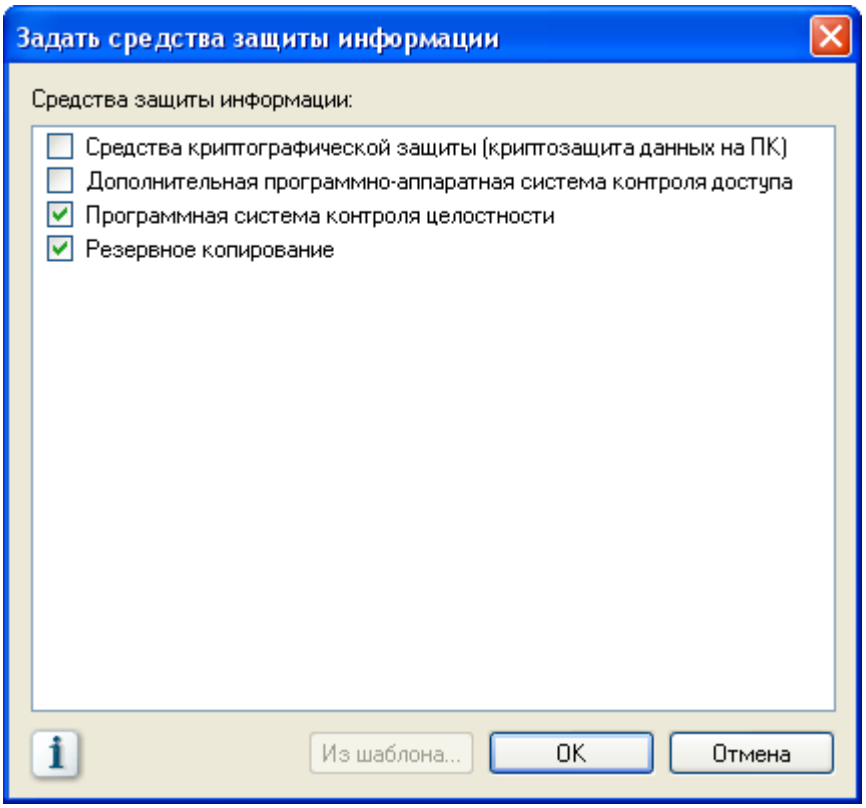

Рисунок 3.4.13 - Выбор средства защиты информации

Последним шагом требуется указать средства защиты для каждого вида информации как на Рисунке 3.4.13. Для вида информации «Бухгалтерский отчет» отметьте все средства защиты, кроме «Дополнительная программно-аппаратная система контроля доступа». Для вида информации «База клиентов» средств защиты информации нет. Для вида информации «База данных наименований товаров» укажите пункты «Резервное копирование» и «программная система контроля целостности».

3.4 Политика безопасности

Так как в модели «Информационных потоков» не учитывается поведение сотрудников организации, существует раздел «Политика безопасности» представленный на Рисунке 3.4.14.

В данном разделе требуется ответить на ряд вопросов, ответы на которые повлияют на веса средств защиты и изменение риска реализации информационной безопасности. Для ответа на вопрос дважды щелкните по нему, затем нажмите кнопку «Изменить». При ответе на вопрос не забудьте нажать «Применить».

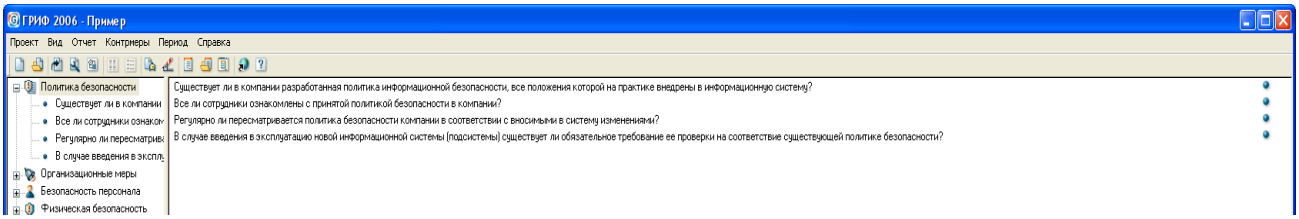

Рисунок 3.4.14 - Вопросы по Политике безопасности

3.5 Контрмеры

Теперь мы получили полную сформированную модель информационной системы нашего предприятия с точки зрения

ИБ, что позволяет перейти к программному анализу введенных данных для комплексной оценки рисков, а также внедрению контрмер.

В главном меню выберете «Контрмеры - Управление рисками» как на Рисунке 3.4.15.

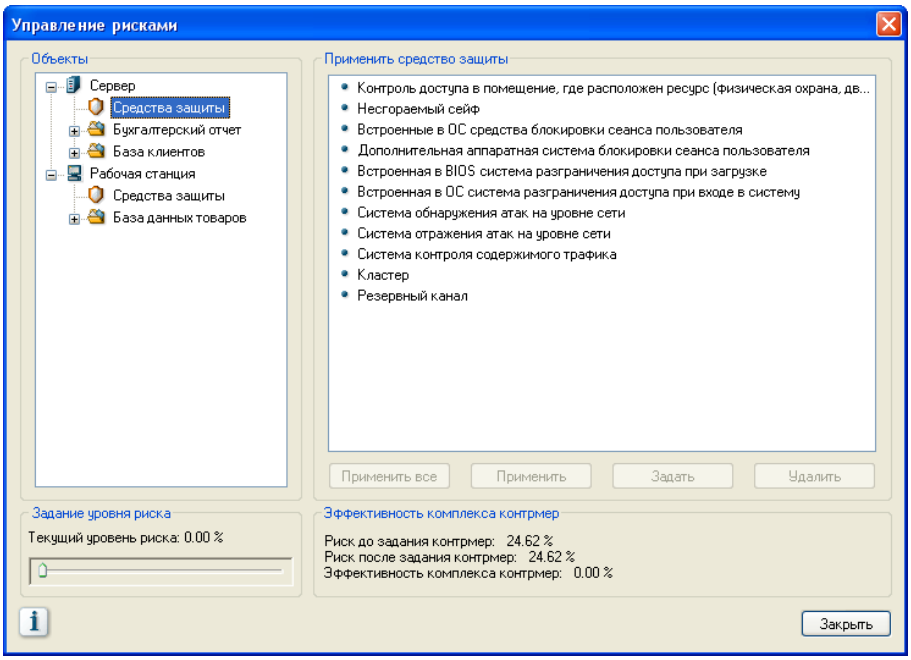

Рисунок 3.4.15 - Управление рисками

В нижней части окна расположены регулятор уровня риска «Задание уровня риска» (по умолчанию он установлен в 0) и информация об эффективности контрмер для всей системы.

Регулятор уровня риска позволяет отфильтровать объекты системы по значимости, будут показаны все объекты, уровень риска которых превышает данный порог.

Передвинув регулятор вправо, определите какой уровень риска не превышает ресурс «Рабочая станция».

В поле «Эффективность комплекса контрмер» показан суммарный риск всей системы.

Для внедрения контрмер выберите интересующий вас ресурс, в рамках ресурса будет показано, какие средства защиты не используются для защиты ресурса, какой вид информации использует данный ресурс и какие средства защиты еще не применены к данному виду информации, а также какая группа пользователей работает с данной информацией.

Выберите одно из предложенных средств защиты, нажмите кнопку «Задать», откроется окно «Новая контрмера» как на Рисунке 3.4.16.

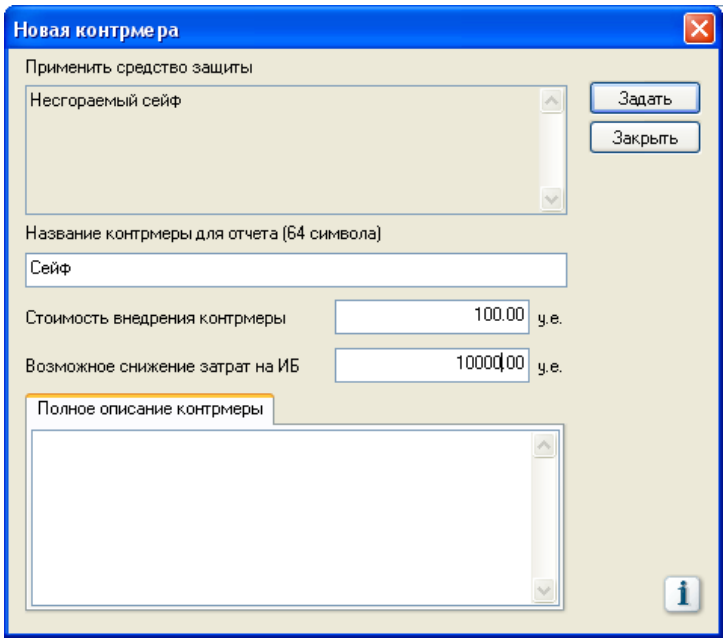

Рисунок 3.4.16 - Задание контрмеры

Заполните необходимы поля и нажмите «Задать», контрмера будет учитываться при расчете риска в окне «Эффективность комплекса контрмер». Примите еще несколько контрмер.

Внедрение контрмеры, напрямую снижает уровень риска реализации угроз, чем больше будет применено контрмер к системе, тем ниже будет показатель риска.

Заданные контрмеры подсвечиваются оранжевым кругом, после применения контрмеры, она пропадет из списка, а риск информационной системы обновится.

Вы можете принять все контрмеры, или только некоторые, исходя из необходимости и возможности их внедрения в рассматриваемую вами конкретную систему.

3.6 Отчёт

Результатом работы является Отчёт, содержащий расчёты затрат компании на ИБ, на контрмеры, вероятности реализации рисков в общем и подотделам и другую информацию, которые представлены в виде диаграмм, графиков и таблиц.

Для создания отчёта нажмите «Отчёт - Создать отчёт». Потребуется определить, какие данные вы хотите видеть в отчёте. Оставьте по умолчанию как изображено на Рисунке 3.4.17.

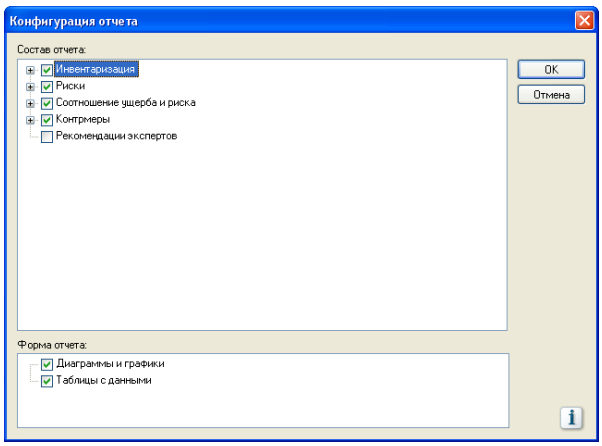

Рисунок 3.4.17 - Конфигурация отчёта

Созданный отчёт можно будет сохранить, нажав соответствующую кнопку в главном меню. Сохраните отчёт под именем «Отчет_*Название предприятия(Л4)*».

Варианты заданий:

Варианты заданий представлены в файле var.pdf.

Контрольные вопросы.

1. Что такое Риск?

2. Что такое Ресурс?

3. Что такое контрмера?

4. Какие виды анализа рисков существуют в ПО «ГРИФ»?

5. Опишите пошагово работу с моделью информационных потоков?

6. Какие виды объектов вводятся в программу при описании ИС?

3.5 Анализ рисков на основе моделей угроз и уязвимостей с помощью «ГРИФ» пакета DigitalSecurityOffice

Лабораторная работа № 5

«Анализ рисков на основе моделей угроз и уязвимостей с помощью «ГРИФ» пакета DigitalSecurityOffice»

Цель работы: знакомство и работа с системой анализа и управления информационными рисками ГРИФ; изучение алгоритма «Анализ модели угроз и уязвимостей».

Задание выполнение работы:

1. В соответствии с описанием системы внести данные в программный комплекс, также используя данные о ресурсах и

отделах из Л.р.№4 и данные об угрозах и уязвимостях из Л.р. №1.

2. Подготовить отчёт сделать соответствующие выводы.

Теоретические сведения.

Вторым методом оценки риска предприятия, который предлагает программа «ГРИФ» пакета DigitalSecurityOffice, является «Анализ модели угроз и уязвимостей».

Данный метод предполагает оценку каждого ресурса с ценной информацией, определяя его уязвимости и угрозы, которые могут быть реализованы с помощью данной уязвимости.

Понятия, применяемые в данной модели:

Ресурс – любой контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (сервер, рабочая станция, переносной компьютер). Свойствами ресурса являются: перечень угроз, воздействующих на него, и критичность ресурса.

Угроза – действие, которое потенциально может привести к нарушению безопасности. Свойством угрозы является перечень уязвимостей, при помощи которых может быть реализована угроза.

Уязвимость – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы. Свойствами уязвимости являются: вероятность (простота)реализации угрозы через данную уязвимость и критичность реализации угрозы через данную уязвимость.

Ход работы:

1. Перечень отделов и ресурсов организации.

Из Л.р. №4 возьмем таблицу с данными, содержащими ресурсы, отделы предприятия. Остальную информацию удалим.

2. Идентификация угроз и уязвимостей.

Из Л.р. №1 возьмем перечень угроз и уязвимостей и для каждой угрозы запишем вероятность её реализации и применяемые к ней контрмеры. Для каждой контрмеры запишем стоимость её внедрения и уменьшение потерь в случае её внедрения.

3. Использование программного комплекса

3.1 Модель угроз и уязвимостей

Перед началом работы необходимо авторизоваться в системе. Для этого запустите ярлык «ГРИФ» на рабочем столе и используйте пару Имя пользователя-Пароль: student-password.

Пример ввода информации об ИС предприятия:

В начале работы программа попросит выбрать алгоритм анализа рисков. Необходимо выбрать пункт «Анализ модели угроз и уязвимостей» и создать новый проект как показано на Рисунке 3.5.1. Название проекта задать - номер варианта (Например: Вариант0).

Также, как и алгоритм метода информационных потоков, данный алгоритм разбивается на шаги.

Шаг 1: Пользователю необходимо внести все объекты системы ИС, к которым относятся отделы, ресурсы (специальными объектами являются угрозы информационной системы, уязвимости, через которые реализуются угрозы).

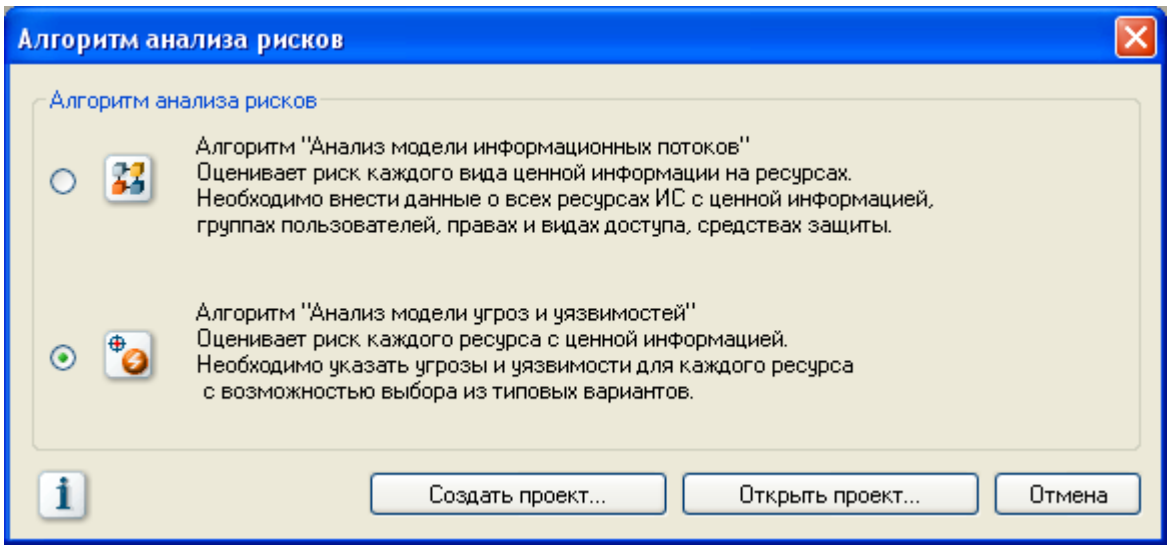

Рисунок 3.5.1 - Алгоритм анализа рисков

Шаг 2: На этом шаге пользователь должен определить, к каким отделам относятся ресурсы, какие угрозы действуют на ресурс и через какие уязвимости они реализуются, таким образом, проставляются связи.

3.2 Добавление объектов

Добавление объектов происходит аналогичным образом, что и в «Модели информационных потоков». Для этого нажимаем кнопку «*Добавить*» в соответствующем разделе как показано на Рисунке 3.5.2.

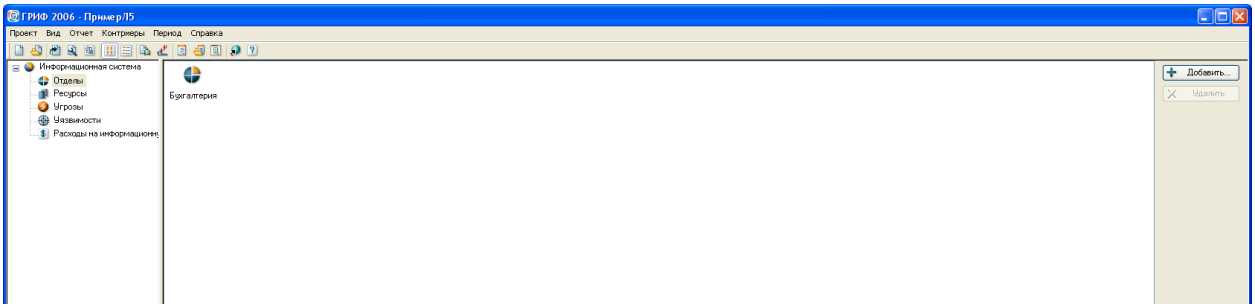

Рисунок 3.5.2 - Добавление нового отдела

Добавление ресурса происходит тоже аналогично добавлению, но в дополнение к названию ресурса, его типу и

отделу, к которому относится ресурс, требуется указать критичность ресурса, т.е. как сильно реализация угрозы повлияет на ресурс как на Рисунке 3.5.3.

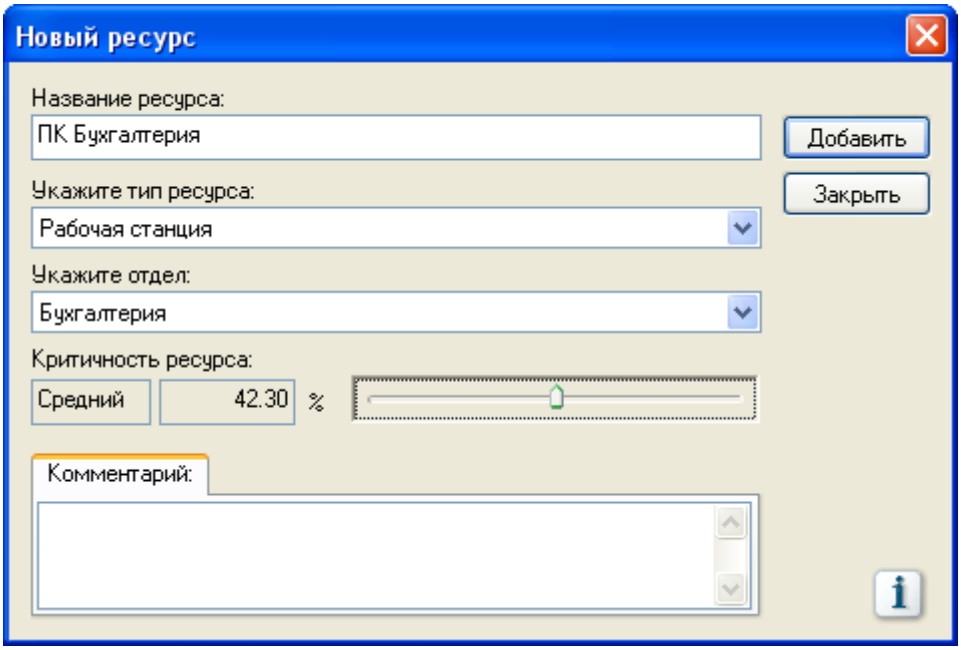

Рисунок 3.5.3 - Добавление нового ресурса

Следующим шагом необходимо добавить все возможные угрозы, имеющиеся у нас в системе.

Система «ГРИФ» делит угрозы на шесть категорий:

- физические угрозы человека (потенциального нарушителя);

- физические угрозы (вызванные форс-мажорными обстоятельствами);

- локальные программные угрозы, направленные на ресурс (без использования каналов связи);

- удаленные программные угрозы, направленные на ресурс (с использованием каналов связи);

- программные угрозы, направленные на канал связи (кабельная система, коммуникационное оборудование, ПО);

- угрозы персонала (вызванные действиями сотрудников компании).

Добавление угроз возможно двумя способами.

Первый способ: выбрать угрозу из предложенного списка и нажать кнопку «*Выбрать ...*», затем нажать «*ОК*» как изображено на Рисунке 3.5.4.

После потребуется ввести название угрозы, а её описание будет уже дано.

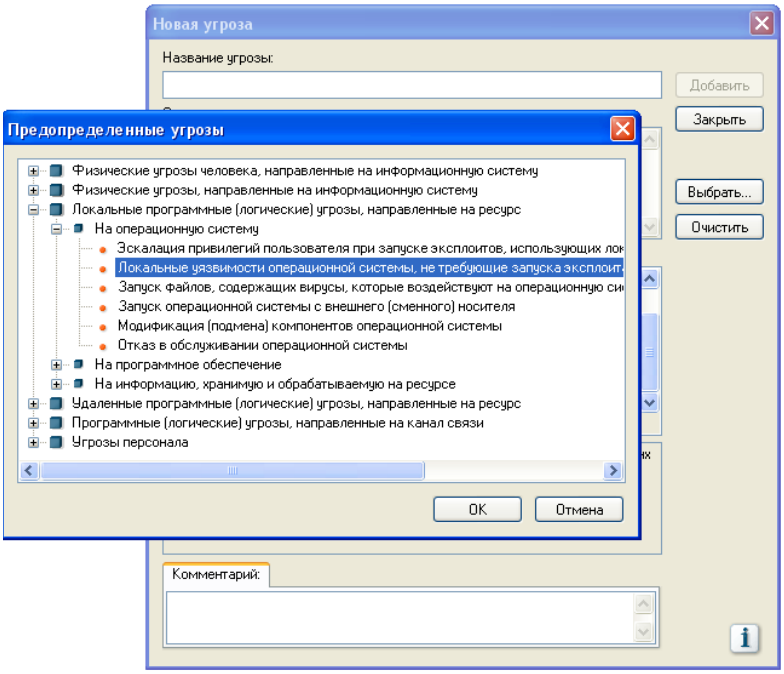

Рисунок 3.5.4 - Добавление угрозы из списка

Второй способ: Задать нужные угрозы самостоятельно. Для этого потребуется ввести название и описание угрозы, и обязательно выбрать к какой категории относится данная угроза как на Рисунке 3.5.5.

После ввода всех угроз можно приступать к добавлению уязвимостей.

Каждую уязвимость необходимо связывать с угрозой, поставив в соответствующем месте галочку, не забыть нажать на кнопку «Добавить» как показано на Рисунке 3.5.6.

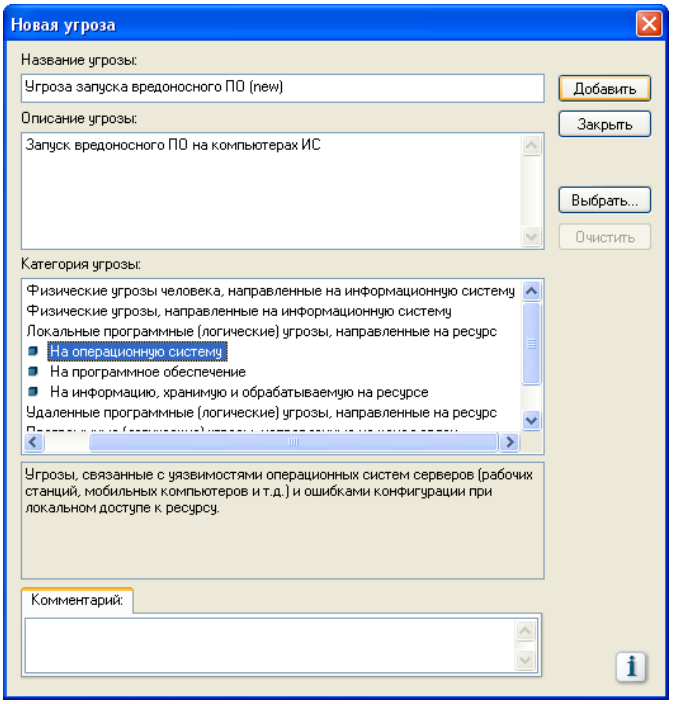

Рисунок 3.5.5 - Добавление угрозы самостоятельно

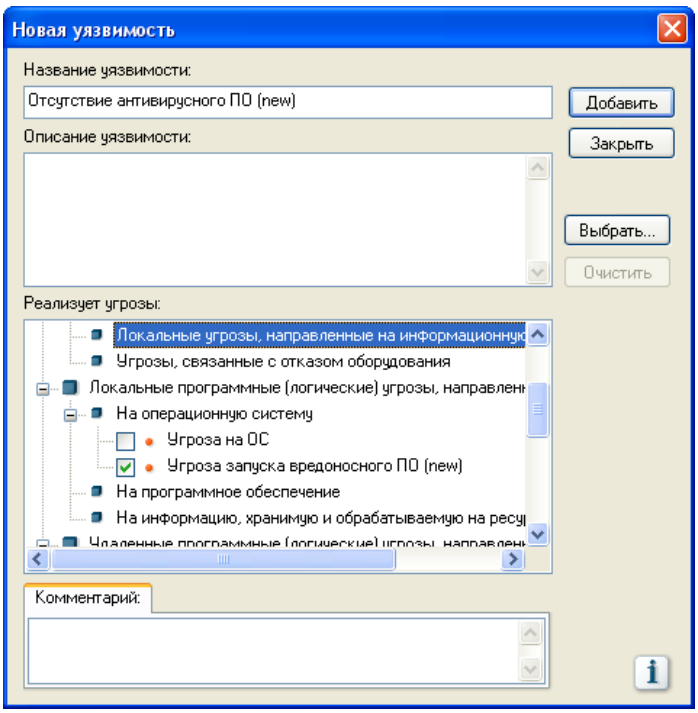

Рисунок 3.5.6 - Добавление уязвимостей

3.3 Связи

В левом нижнем углу необходимо выбрать пункт *Связи*.

Для добавления связи ресурс-угроза, нажмите кнопку «*Добавить…*» в правой части окна. Появится окно угроз, где будут отображаться все добавленные вами ранее угрозы. После потребуется указать уязвимость, вытекающую из этой угрозы и задать два параметра:

- «Вероятность угрозы через данную уязвимость в течение года»;

- «Критичность реализации угрозы» изображены на Рисунке 3.5.7 и Рисунке 3.5.8.

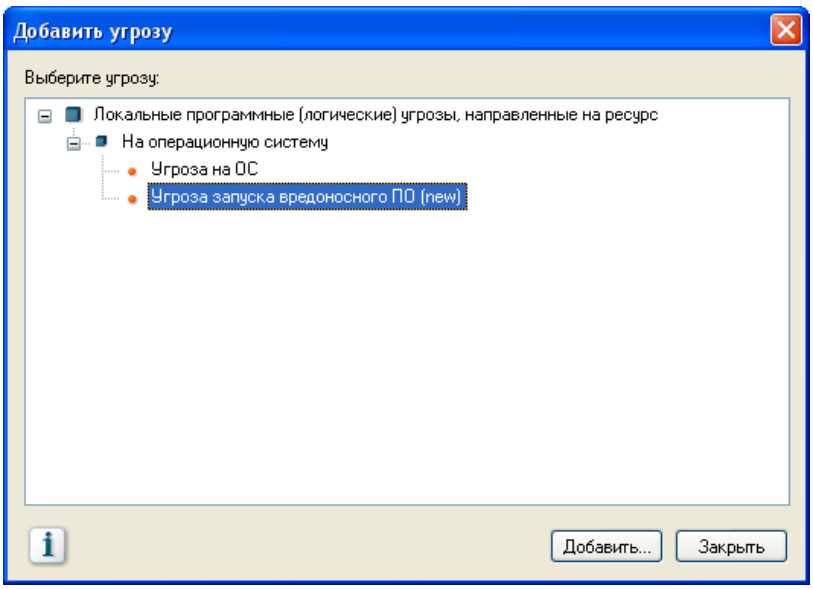

Рисунок 3.5.7 - Добавление связи ресурс-угроза

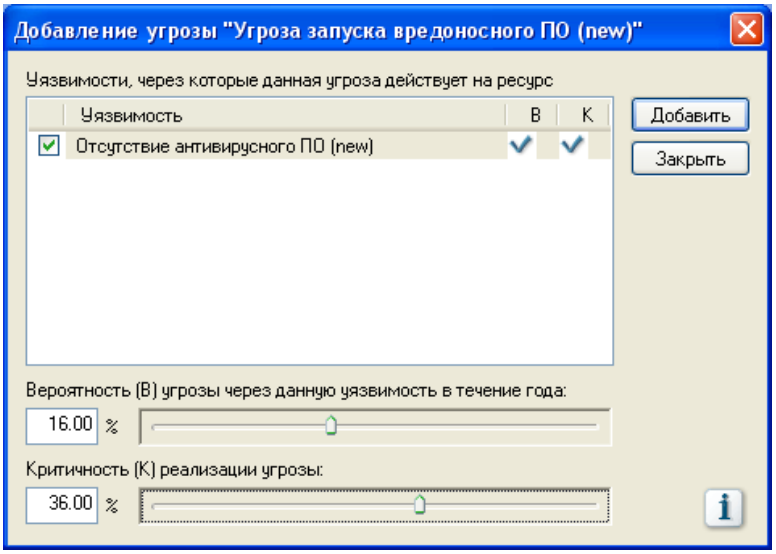

Рисунок 3.5.8 - Выбор параметров

Важно отметить, что для угроз, созданных пользователем, вероятность в течение года и критичность реализации по умолчанию равны 0%, для предопределенных угроз это значение устанавливает система «ГРИФ» (отличное от 0), при надобности пользователь может его изменить.

3.4 Управление рисками и контрмеры

После того как мы задали всю информацию о нашей ИС, можно переходить к управлению рисками и применению контрмер. Для этого в главном меню требуется выбрать пункт «*Контрмеры*» и нажать «*Управление рисками*». Появится окно управления рисками. В нем будет отражена иерархическая структура ИС, на верхней иерархии изображены ресурсы и все угрозы, относящиеся к ним, а также эффективность комплекса контрмер, риск до внедрения контрмер и после внедрения и есть регулятор текущего уровня риска, изображенного на Рисунке 3.5.9.

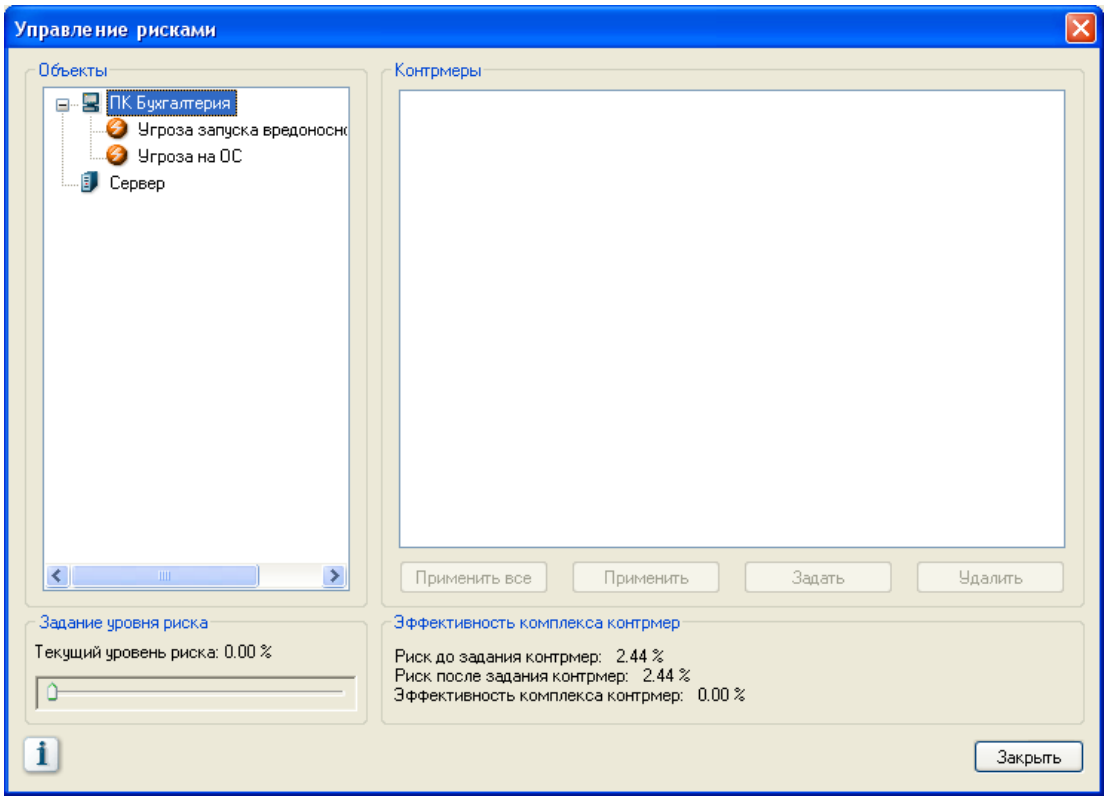

Рисунок 3.5.9 - Окно «Управление рисками»

При выделении в списке угрозы в правой части окна появится список уязвимостей, которые требуется устранить. Для этого нужно выбрать любую уязвимость из списка и

нажать кнопку «*Задать*». Скриншот представлен на Рисунке 3.5.10.

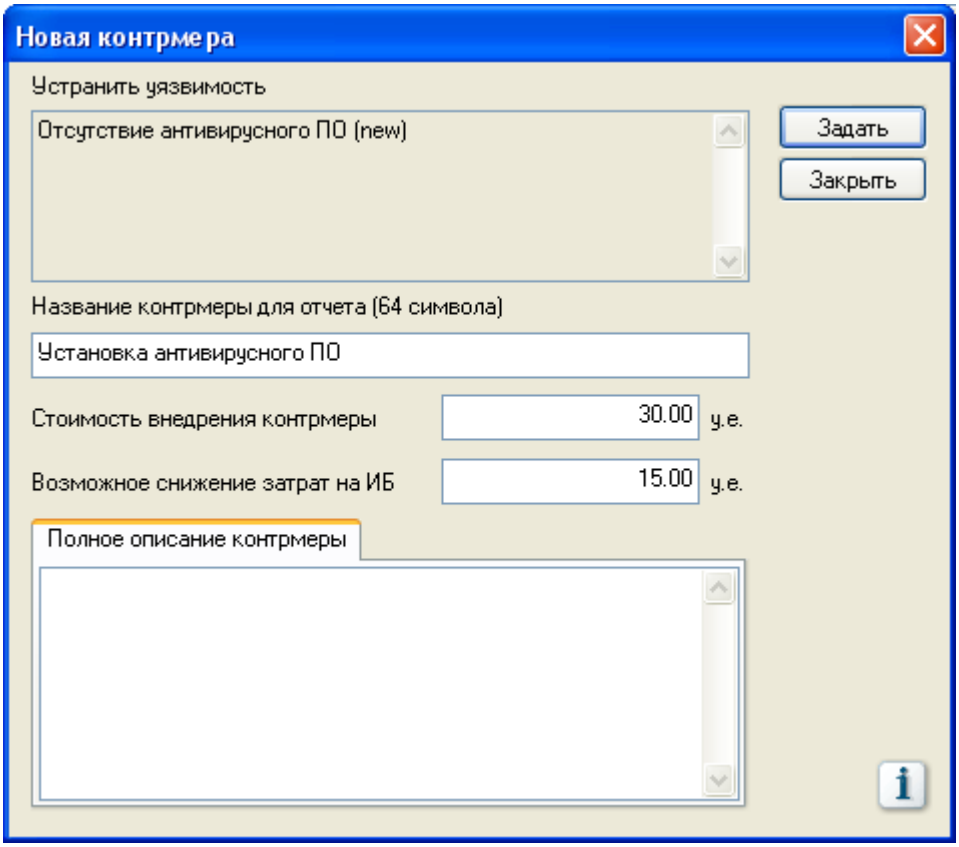

Рисунок 3.5.10 - Применение контрмеры

После того как пользователь задал контрмеру, риск на информационную систему снизится, величина снижения риска зависит от вероятности угрозы через данную уязвимость в течение года и от критичности реализации угрозы.

Таким образом, пользователь может задавать различные контрмеры для различных уязвимостей, тем самым снижая риск реализации угрозы.

3.5 Отчёт

Для создания отчета, в главном меню нажмите на пункт «*Отчет*» и в выпадающем списке выберите «*Создать отчет*» как показано на Рисунке 3.5.11.

Выберите необходимые пункты, поставив галочку напротив, инажмите кнопку «ОК».

Отчет разбит на четыре раздела:

- инвентаризация;
- информационные риски;
- соотношение ущерба и риска;
- контрмеры.

Раздел «Инвентаризация» содержит в себе информацию, о стоимости ресурса, описания угроз, описания уязвимостей. То есть общую информацию о системе.

Раздел «Информационные риски» показывает риск ресурсов, по угрозам и уязвимостям, а также суммарные риски ресурсов по отделам.

В разделе «Соотношение ущерба и риска» находится информация о соотношении ущерба и риска отделов, ресурсов и всей информационной системе в целом.

Последний раздел «Контрмеры» содержит информацию об эффективности контрмер.

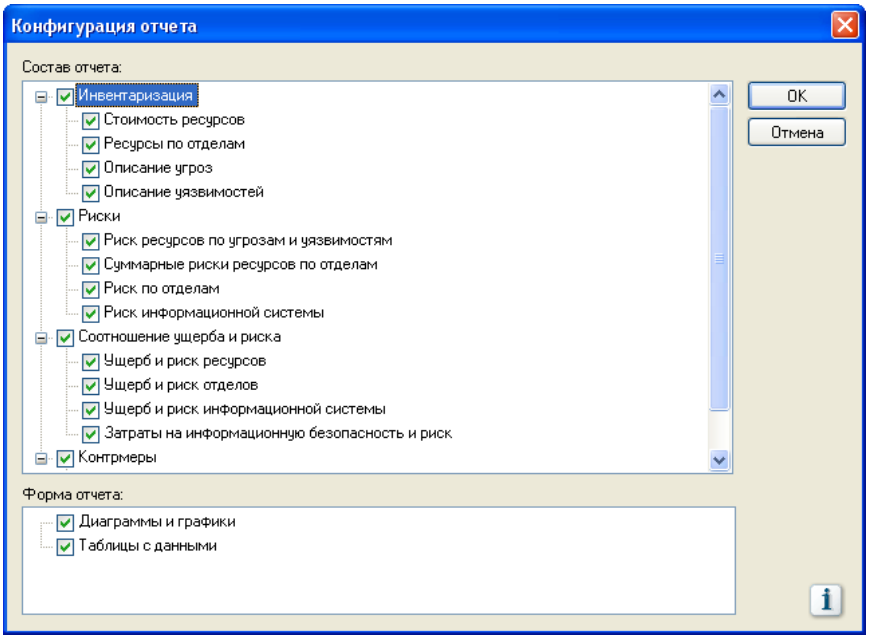

Рисунок 3.5.11 - Конфигурация отчёта

После создания отчета его можно сохранить, нажав на соответствующую кнопку в главном меню.

Варианты заданий:

Варианты заданий представлены в файле var.pdf.

Контрольные вопросы.

1.Опишите пошагово работу с моделью анализа угроз и уязвимостей?

2.Какие виды объектов вводятся в программу при описании ИС?

3.Что такое угроза?

4.Что такое уязвимость?

5.На какие категории система «ГРИФ» делит угрозы?

6.Какие виды разделов содержит отчет? Дайте краткое описание каждому разделу.

3.6 Анализ рисков на основе DigitalSecurity.КОНДОР

Лабораторная работа № 6

«Анализ рисков на основе DigitalSecurity.КОНДОР»

Цель работы: знакомство и работа с системой DigitalSecurity.КОНДОР.

Задание выполнение работы:

1. В соответствии с описанием системы и разработанной политикой ИБ в Л.р. № 2 ответить на вопросы в программном комплексе.
2. Задать контрмеры для снижения риска и подготовить отчёт, сделать соответствующие выводы.

Теоретические сведения.

«КОНДОР» является еще одной разработкой российской компании DigitalSecurity. Служит для разработки и управления политики ИБ предприятия в соответствии с международным стандартом ISO 17799 «Управление информационной безопасностью. Практические правила». Требования данного стандарта обеспечивают комплексный подход к обеспечению ИБ за счёт проверки соответствия требованиям.

Ход работы:

1. Использование программного комплекса

1.1 Создание нового проекта аудита

Перед началом работы необходимо авторизоваться в системе. Для этого запустите ярлык «КОНДОР» на рабочем столе и используйте пару Имя пользователя-Пароль: student-password.

Пример ввода информации об ИС предприятия:

В начале работы потребуется создать проект. Название проекта задать – Название_предприятия(Л6) (Например: ЧистыйМир(Л6)) как показано на Рисунке 3.6.1.

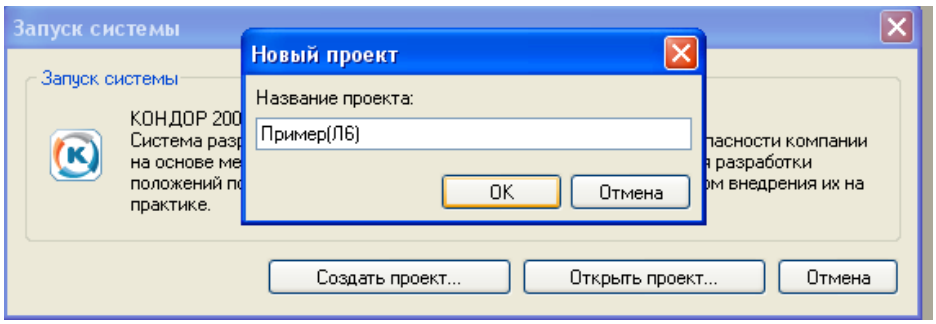

Рисунок 3.6.1 - Создание проекта

Рабочее окно, показанное на Рисунке 3.6.2, разбито на 4 части:

1. *Окно навигации.* Отображает периоды проведения аудита.

2. *Окно разделов с вопросами.* При выборе раздела отображается список вопросов данного раздела. Напротив вопроса находится иконка. Она может быть разного цвета. Если иконка синяя, то ответ на вопрос не дан; если она жёлтая – ответ дан, серая иконка отражает то, что данный вопрос неприменим к ИС.

3. *Окно рабочего поля.* Нужно для работы с вопросами.

4. *Окно подсказки.* Отображает справочную информацию по выбранному разделу.

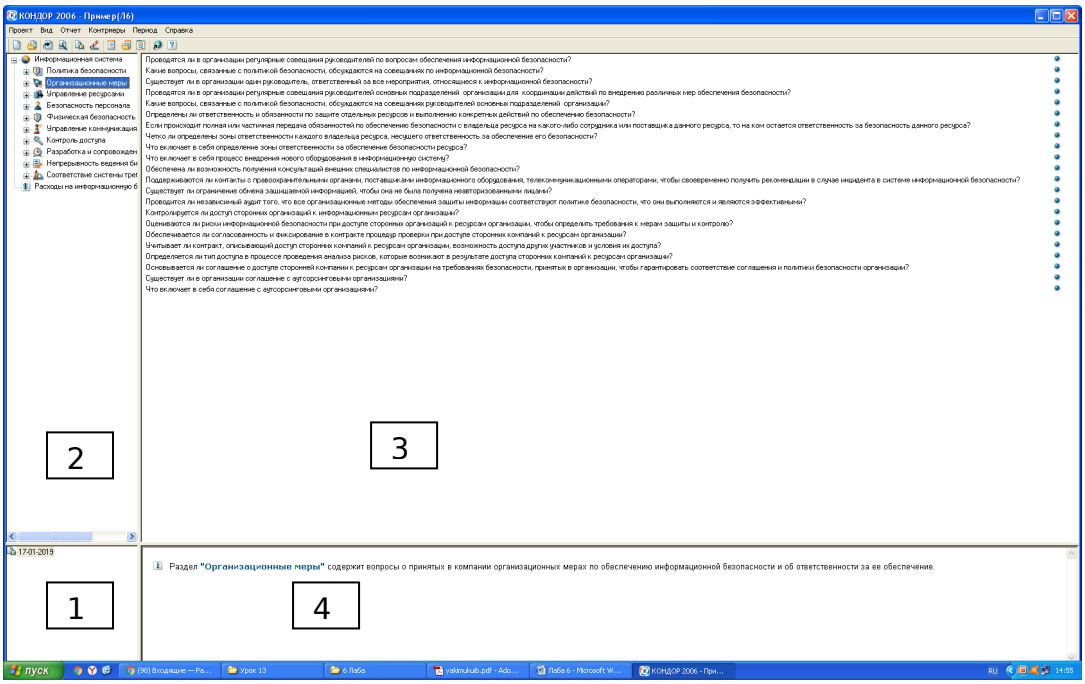

Рисунок 3.6.2 - Рабочее окно

1.2 Анализ ИС на соответствие требованиям стандарта ISO 17799

Система «КОНДОР» состоит положений стандарта ISO 17799, сформулированных в виде вопросов, ответив на которые,

мы получим представление о том какие положения выполняются в нашей ИС, а какие нет. Каждый раздел соответствует разделу стандарта. Для получения наиболее верных результатов аудита необходимо ответить на все вопросы, указав вопросы, неприменимые к ИС.

Для того чтобы работать с вопросами, выбранного раздела, необходимо дважды щелкнуть по нему. Откроется окно, в котором можно переключаться между вопросами с помощью специальных кнопок. Для того чтобы ответить на вопрос надо нажать на кнопку «*Изменить*». Скриншот представлен на Рисунке 3.6.3.

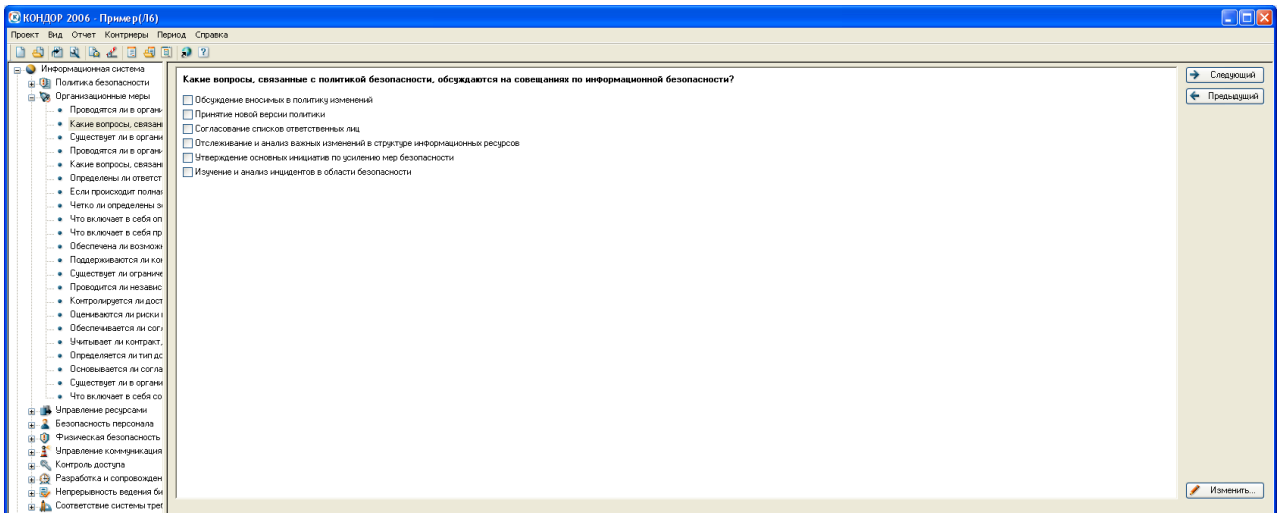

Рисунок 3.6.3 - Работа с вопросами

1.3 Расходы на информационную безопасность

Расходы на информационную безопасность – затраты организации на обеспечение информационной безопасности, включающие затраты на приобретение систем защиты информации и управление ими, стоимость обучения персонала.

Для изменения значений расходов на ИБ требуется выбрать соответствующий раздел во втором окне рабочего поля, изображенного на Рисунке 3.6.4.

- *Разовые затраты на приобретение систем защиты информации.*

В данном пункте имеются в виду затраты на лицензию ПО. Также тут учитываются затраты на аппаратное обеспечение, на котором установлены компоненты систем защиты. Кроме этого необходимо учитывать и затраты на дополнительное техническое и программное оснащение для систем защиты (тройники, БД, системы резервирования и т.д.).

Для крупных компаний, которые имеют распределенную корпоративную сеть, не стоит забывать о *затратах на внедрение систем защиты информации* (включая этап предварительного аудита).

- *Ежегодные затраты на поддержку и обучение* (если она не включена в стоимость системы защиты).

Также в эти расходы включается настройка удаленных компонентов и расходы на поездки IT-специалистов.

- *Ежегодные затраты на управление средствами защиты информации*.

Зарплаты администраторов и персонала, связанных с деятельностью по обнаружению атак, а также затраты на модернизацию программно-аппаратного обеспечения.

- *Прочие ежегодные затраты на обеспечение информационной безопасности.*

- *Изменение затрат после внедрения контрмер.*

Это значение равно разности стоимости внедрения контрмеры и возможного снижения затрат на ИБ. Поле

заполняется автоматически после установления стоимости внедрения контрмер и возможного снижения затрат на ИБ.

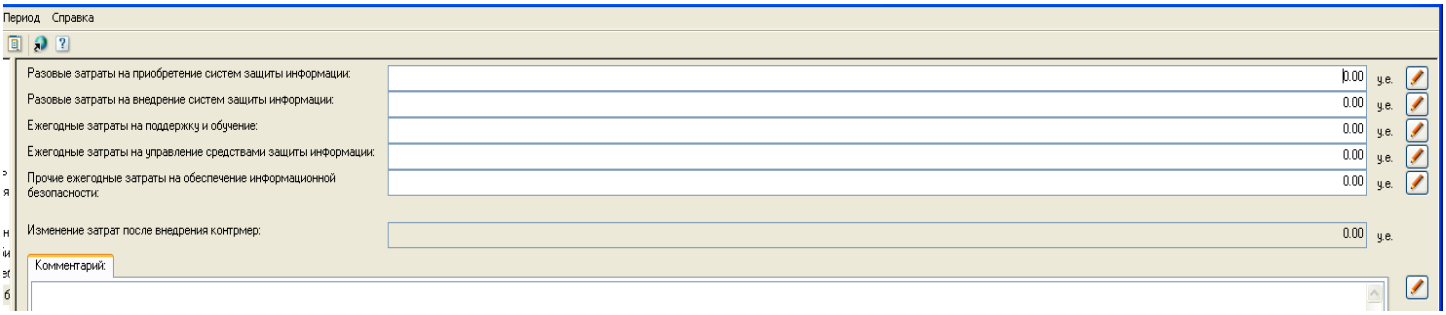

Рисунок 3.6.4 - Расходы на ИБ

1.4 Свойства проекта

Для изменения данных о нашем проекте необходимо нажать «*Проект-Свойства проекта*».

Во вкладке «Идентификация», показанной на Рисунке 3.6.5, ввести данные о проекте.

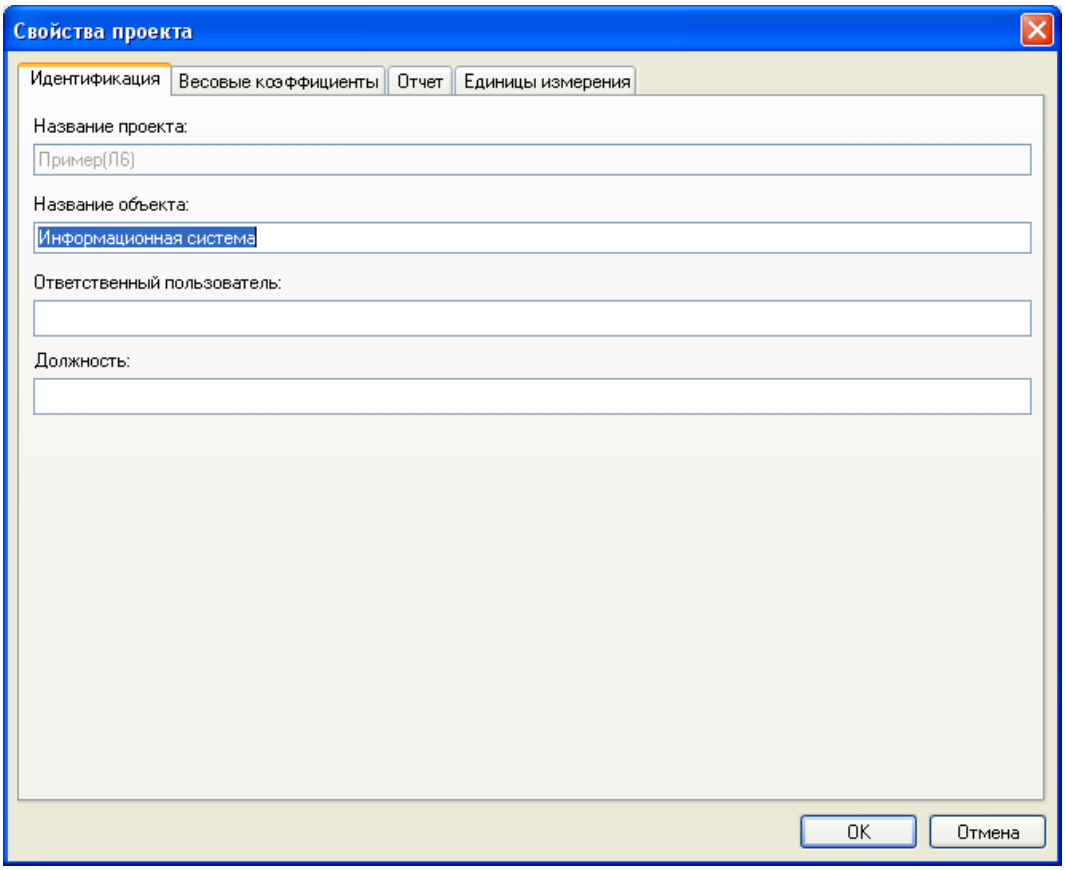

Рисунок 3.6.5 - Вкладка «Идентификация» окна «Свойства проекта»

Вкладка «Весовые коэффициенты» позволяет нам изменить веса, заданные программой, в соответствии с особенностями нашей компании. Каждое требование стандарта имеет определенное весовое значение, которое характеризует степень критичности данного положения для поддержания необходимого уровня защищенности. Требования разделены по разделам, рядом с каждым требованием стоит номер раздела стандарта ISO 17799 как показано Рисунке 3.6.6. Состояние каждого требования отражено в списке. Если маркер рядом с требованием синий, то коэффициент не изменен, если желтого – да.

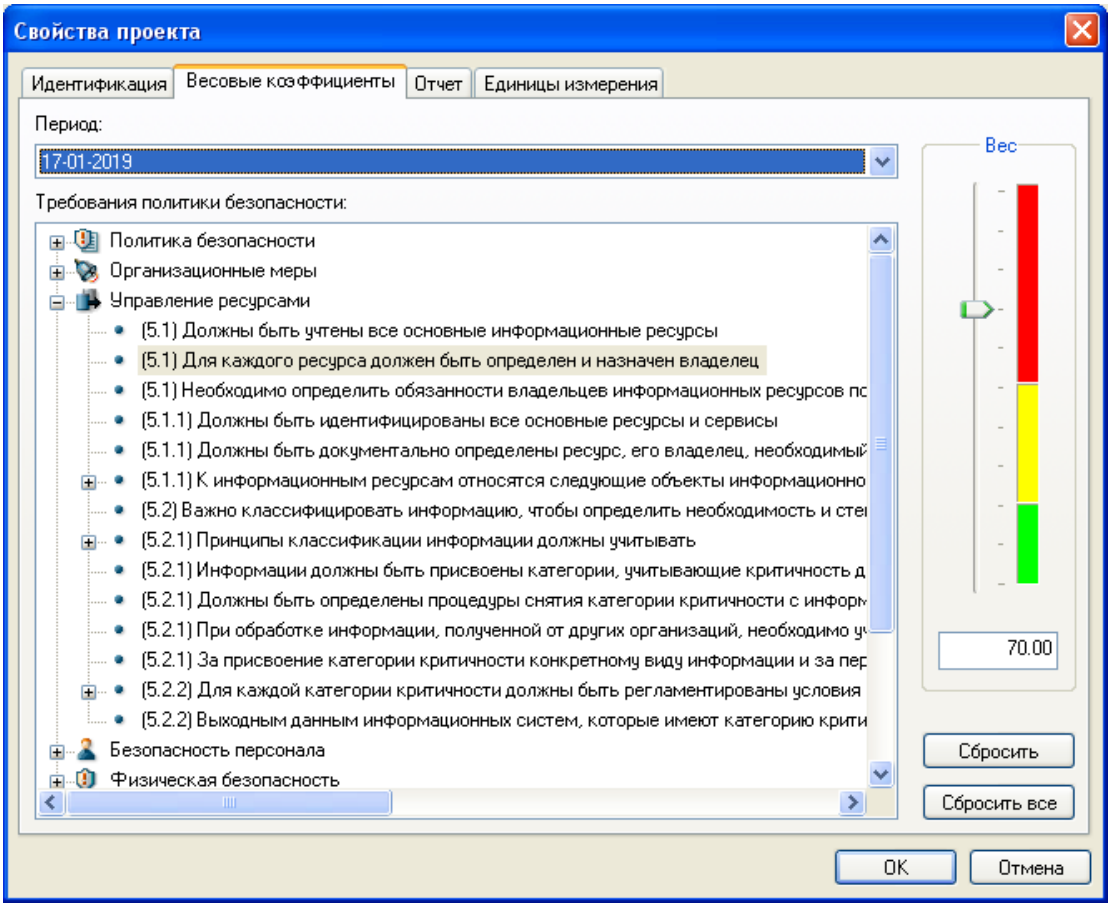

Рисунок 3.6.6 - Вкладка «Весовые коэффициенты» окна «Свойства проекта»

Вкладка «Отчёт» отражает информацию о том, какие данные (Выполненные меры, Невыполненные меры, Контрмеры, Рекомендации экспертов), и в каком виде (Диаграммы и графики или без них) будут представлены в нашем отчете. Скриншот представлен на Рисунке 3.6.7.

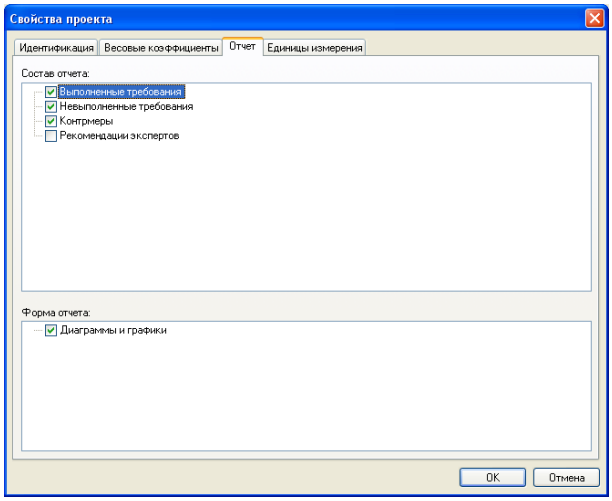

Рисунок 7 - Вкладка «Отчёт» окна «Свойства проекта»

Вкладка «Единицы измерения», показанная на Рисунке 3.6.8, позволяет задать значения единиц измерения.

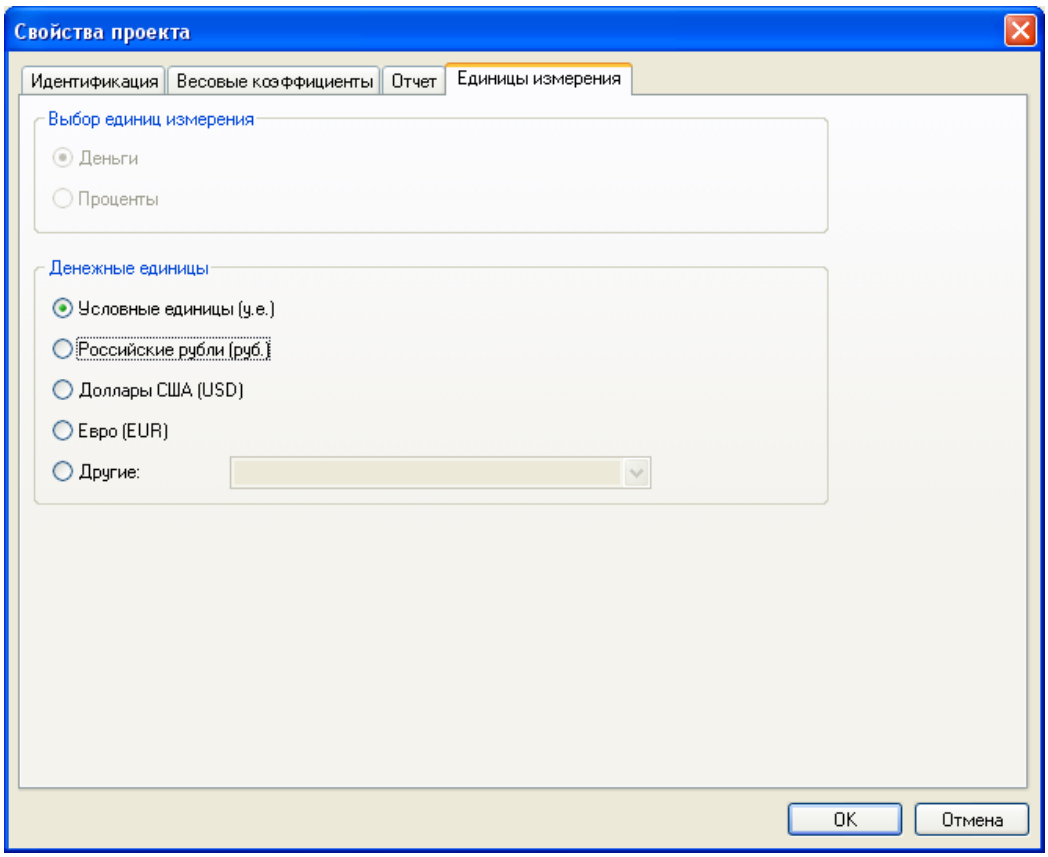

Рисунок 3.6.8 - Вкладка «Единицы измерения» окна «Свойства проекта».

1.5 Управление рисками

После ответа на все вопросы система «КОНДОР» предлагает оценить риски с помощью встроенного модуля (*Контрмеры – Управление рисками*), в котором отражаются все невыполненные требования Политики ИБ.

Причем можно самостоятельно задать пороговое значение весов, при этом будут отражаться, только те положения, которые не выполнены и критичны для пользователя как на Рисунке 3.6.9.

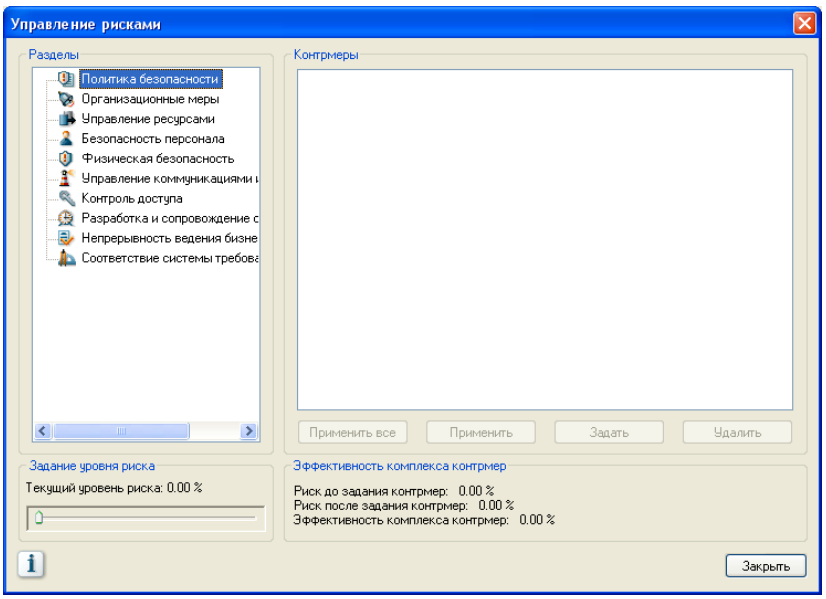

Рисунок 3.6.9 - Управление рисками

Если необходимо задать контрмеру для выбранного раздела требуется нажать кнопку «*Задать*». Откроется окно «Новая контрмера», в котором потребуется ввести нужные данные как изображено на Рисунке 3.6.10.

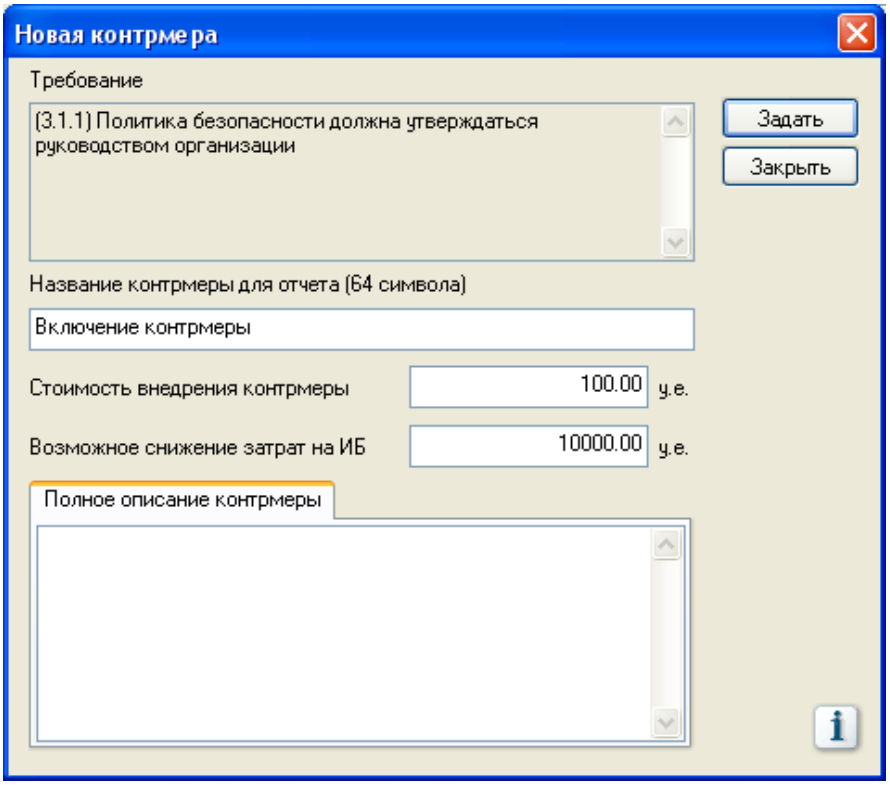

Рисунок 3.6.10 - Задание контрмеры.

После задания контрмеры внизу окна «Управление рисками» можно увидеть, на сколько меньше стало значение риска и насколько эффективна введенная контрмера.

Таким образом, система «КОНДОР» позволяется оценить эффективность как уже существующей политики ИБ организации, так и политики, находящейся в разработке.

1.6 Управление периодами

По прохождению времени степень выполнения требований может измениться, поэтому необходимо проводит аудит предприятия регулярно в определенные сроки, установленные руководством.

Для создания нового периода надо нажать правой кнопкой мыши по окну № 1 и выбрать «Управление периодами». В открывшемся окне, показанном на Рисунке 3.6.11, можно выбрать период для редактирования, изменить или создать новый.

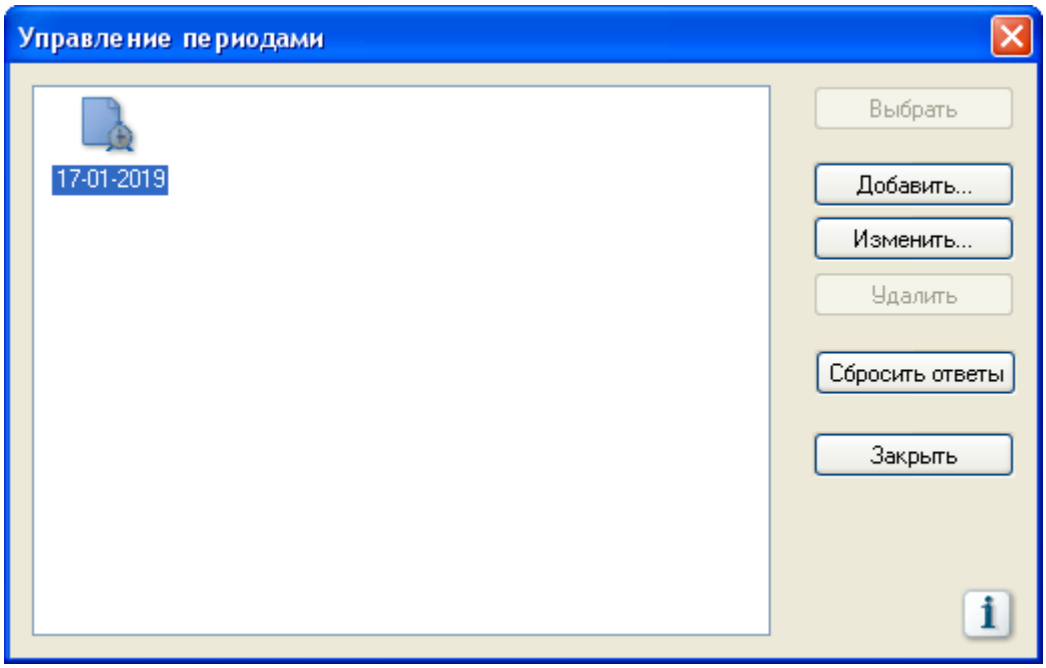

Рисунок 3.6.11 - Окно «Управление периодами»

1.7 Создание отчёта

Для создания отчета, в главном меню нажмите на пункт «*Отчет*» и в выпадающем списке выберите «*Создать отчет*» как показано на Рисунке 3.6.12.

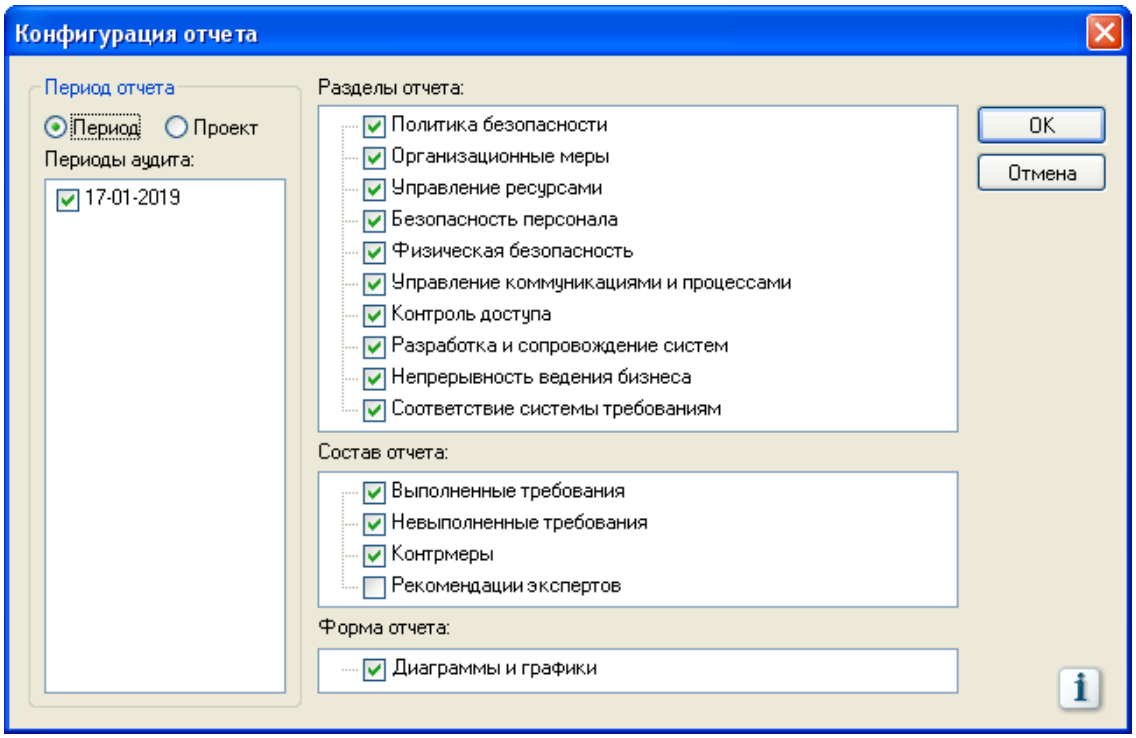

Рисунок 3.6.12 - Создание отчёта

В системе «КОНДОР» можно создать два вида отчёта:

- отчёт по проекту;
- отчёт по периоду.

Отчёт по *проекту* содержит:

- изменения количества выполненных требований в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита;

- изменения уровня риска в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита;

- изменения затрат на контрмеры в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита.

Отчёт по *периоду* содержит:

- количество выполненных и невыполненных требований в целом по системе для выбранного периода аудита;

- уровень риска невыполнения требований стандарта в целом по системе для выбранного периода аудита;

- затраты на контрмеры в целом по системе для выбранного периода аудита;

- количество выполненных и невыполненных требований по каждому разделу стандарта;

- текст выполненных требований по каждому разделу;

- текст невыполненных требований по каждому разделу, отсортированных по уровню риска;

- введенные контрмеры для каждого невыполненного требования стандарта;

- комментарии эксперта по невыполненным требованиям.

Варианты заданий:

Варианты заданий представлены в файле var.pdf.

Контрольные вопросы.

1. Какой подход к обеспечению ИБ предприятия применяет «КОНДОР»?

2. Как стандарт ISO 17799 определяет термины конфиденциальность, целостность и доступность информации?

3. Какова цель политики ИБ организации?

4.Какие данные вносятся в раздел «Расходы на ИБ»?

3.7 Анализ рисков по методике CRAMM

Лабораторная работа № 7

«Анализ рисков по методике CRAMM»

Цель работы: освоение и применение методики оценки рисков CRAMM.

Задание выполнение работы:

1. Провести оценку ресурсов, угроз и уязвимостей для ИС из Л.р.№1.

2. Рассчитать значения риска и предложить контрмеры, для значения риска в границах от 5 до 7.

Теоретические сведения.

Методика CRAMM является одной из первых методик для анализа рисков ИБ. Для сбора информации применяются специальные подробные опросные листы, на основе которых составляется идентификация ресурсов, угроз и уязвимостей.

Оценивание делится на три стадии:

1.Идентификация ресурсов ИС.

Во-первых, собираются сведения о конфигурации системы и о том, кто отвечает за физические и программные ресурсы, кто входит в число пользователей системы, как они ее применяют или будут применять.

Каждый ресурс, входящий в границы исследуемой ИС, необходимо отнести к одному из классов (физический, программный или информационный).

Ценность физических ресурсов в CRAMM определяется стоимостью их восстановления в случае разрушения.

Ценность данных и программного обеспечения определяется в соответствующими параметрами и дается оценка по шкале от 1 до 10 (Таблица 3.7.1):

- ущерб репутации организации;
- нарушение действующего законодательства;
- ущерб для здоровья персонала;
- ущерб, связанный с разглашением персональных данных отдельных лиц;
- финансовые потери от разглашения информации;
- финансовые потери, связанные с восстановлением ресурсов;
- потери, связанные с невозможностью выполнения обязательств;
- дезорганизация деятельности.

Таблица 3.7.1 Шкала оценки, связанная с потерями при восстановлении ресурсов

2 балла	Менее 1000 у.е.
6 баллов	от 1000 у.е. до 10 000 у.е.
8 баллов	от 10 000 у.е. до 100 000 у.е.
10 баллов	свыше 100 000 у.е.

При низкой оценке по всем используемым критериям (3 балла и ниже) считается, что рассматриваемая система требует базового уровня защиты (для этого уровня не требуется подробной оценки угроз ИБ) и вторая стадия исследования пропускается.

2. Идентификация угроз и уязвимостей ИС и расчёт рисков.

На этом шаге производится оценка существующих угроз и уязвимостей, вычисляются уровни рисков и анализируются результаты.

На основе имеющейся информации рассчитываются уровни рисков по шкале от 1 до 7.

Методика CRAMM объединяет угрозы и уязвимости в матрице риска. Для её составления необходимо рассмотреть:

- уровень угрозы (Таблица 3.7.2);
- уровень уязвимости (Таблица 3.7.3);
- размер ожидаемых финансовых потерь.

Таблица 3.7.2 Шкала оценки уровня угрозы

Описание	**Значение**
Инцидент происходит в среднем, не чаще, чем каждые 10 лет	Очень низкий (P=0.1)
Инцидент происходит в среднем один раз в 3 года	Низкий (P=0.34)
Инцидент происходит в среднем один раз в год	Средний (P=1)
Инцидент происходит в среднем один раз в 4 месяца	Высокий (P=3.33)
Инцидент происходит в среднем один раз в месяц	Очень высокий (P=10)

Таблица 3.7.3 Шкала оценки уровня уязвимости

Описание	**Значение**
В случае возникновения инцидента, вероятность развития событий по наихудшему сценарию меньше 0,33	Низкий (P=0.1)
В случае возникновения инцидента, вероятность развития событий по наихудшему сценарию от 0,33 до 0,66	Средний (P=0.5)
В случае возникновения инцидента, вероятность	Высокий

развития событий по наихудшему сценарию выше 0,66	(P=1)

После проведения оценки составляется матрица, вычисляющая ожидаемые годовые потери. В ней второй столбец слева содержит значения стоимости ресурса, верхняя строка заголовка таблицы - оценку частоты возникновения угрозы в течение года (уровня угрозы), нижняя строка заголовка - оценку вероятности успеха реализации угрозы (уровня уязвимости).

Затем значения переводятся CRAMM в баллы, показывающие уровень риска, по шкале (Таблица 3.7.4) и выводится матрица риска.

Таблица 3.7.4 Шкала оценки риска

Балл CRAMM	**Значение ожидаемых годовых потерь**
1	<1000 у.е.
2	<10000 у.е.
3	<100000 у.е.
4	<1000000 у.е.
5	<10000000 у.е.
6	<100000000 у.е.
7	<1000000000 у.е.

3. Контрмеры.

На этой стадии выбираются несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням.

Таким образом, CRAMM - пример методики расчета, при которой первоначальные оценки даются на качественном уровне, и потом производится переход к количественной оценке (в баллах).

Ход работы:

1. Идентификация ресурсов.

Из Л.р. №1 возьмем перечень ресурсов и оценим их с точки зрения потерь при их восстановлении. Заполним таблицу (Таблица 3.7.5).

Таблица 3.7.5 Ресурсы ИС

Ресурс	**Потери**
Ресурс 1	
…	
Ресурс N	

2. Идентификация угроз.

Из Л.р. №1 возьмем перечень угроз и их вероятность возникновения из Л.р. №5 и для каждой угрозы запишем её значение в баллах в соответствии с Таблицей 3.7.6 и Таблицей 3.7.7.

Таблица 3.7.6 Сопоставление вероятности значения

Вероятность в процентах	**Вероятность в баллах**
0-20 %	0.1
20-40%	0.33
40-60%	1
60-80%	3.33
80-100%	10

Таблица 3.7.7 Угрозы ИС

Угроза	**Значение**
Угроза 1	
Угроза 2	
Угроза 3	
Угроза 4	
Угроза 5	

3. Идентификация уязвимостей

Для уязвимостей из Л.р. №1 проведём оценку в соответствии со шкалой CRAMM и занесём данные в таблицу (Таблица 3.7.8).

Таблица 3.7.8 Уязвимости ИС

Уязвимость	**Значение**
Уязвимость 1	
Уязвимость 2	
Уязвимость 3	
Уязвимость 4	
Уязвимость 5	

4. Применение методики

Скопировать файл *CRAMM.xlsx* в личную папку под названием CRAMMВариантN и запустить его оттуда. Занести данные из таблиц в файл и получить значения рисков для каждого актива.

Для активов со значением риска в границах от 5 до 7 баллов предложить контрмеры.

Сделать выводы и сформировать отчёт.

Варианты заданий:

Варианты заданий представлены в файле var.pdf.

Контрольные вопросы.

1.Какая методика расчета рисков (количественная, качественная или комплексная) применяется CRAMM?

2. Опишите стадии оценки риска методикой CRAMM.

3. Назовите преимущества методики CRAMM?

4. Назовите недостатки метода CRAMM?

5. По какой формуле рассчитывался уровень риска в данной лабораторной работе?

6. Что такое аудит ИБ организации?

Выводы по третьей главе:

На основании проведенного анализа в прошлых главах ВКР были разработаны темы лабораторных работ и сами работы, соответствующие им, а именно:

- Матричный подход к анализу рисков ИБ;
- Разработка Политики ИБ организации;
- Анализ рисков на основе ПО «РискДетектор»;
- Анализ и управление рисками ИС на основе ПО «ГРИФ» пакета Digital Security Office;
- Анализ рисков на основе моделей угроз и уязвимостей с помощью «ГРИФ» пакета DigitalSecurityOffice;
- Анализ рисков на основе DigitalSecurity.КОНДОР;
- Анализ рисков по методике CRAMM.

4 Разработка вариантов к лабораторным работам

После окончания обучения выпускники специальности «Информационная безопасность ТКС» могут пойти работать в различные организации независимо от их характера деятельности, формы собственности и размера. Поэтому целесообразно разработать несколько вариантов лабораторных работ, описывающих разные предприятия.

План-схемы помещений указаны в Приложении 2.

1 Вариант

ООО «МамаИталия»

Род деятельности: Заведение общественного питания

Список сотрудников:

Директор	Долматова Д.С.
Коммерческий директор	Харитонова Е.Н.
Менеджер по закупкам	Сидоров Е.А.
Администратор (x2)	Жирова Н.С.
Бухгалтер	Буракова В.М.
Официант (x10)	
Повар	Страхов Г.С.
Водитель	Ухов Д.П.
Уборщица	Крапивина В.В.
Бармен (x2)	

Структура предприятия представлена на Рисунке 4.1:

Рисунок 4.1 – Структура предприятия

2 Вариант

ООО «Окно в Европу»

Род деятельности: Турфирма

Список сотрудников (главный офис):

Генеральный директор	Норильский Д.А.
Заместитель директора	Антонов Е.О.
Менеджер по работе с клиентами	Смирнова О.А.
Менеджер по работе с клиентами	Попова С.Г.
Бухгалтер	Третьяков С.С.
Секретарь	Миколайчук А.А.
Приходящий системный администратор	Иванов И.И.
Уборщица	Любинина З.С.
Начальник сектора ЗИ	Корунов А.П

Структура предприятия представлена на Рисунке 4.2:

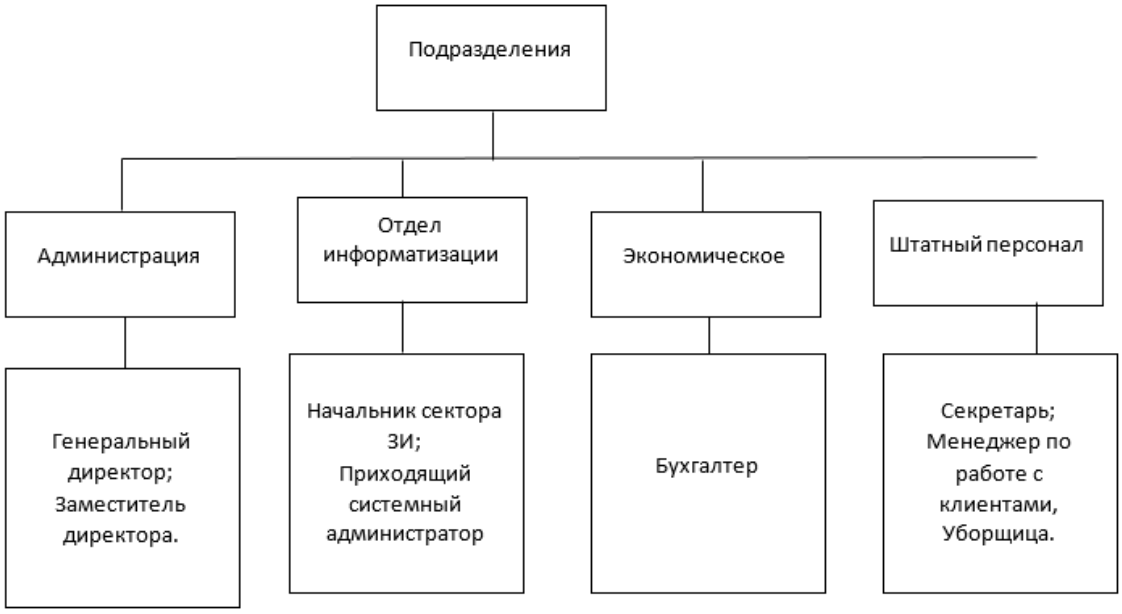

Рисунок 4.2 – Структура предприятия

3 Вариант

ООО «Такси Санкт-Петербург»

Род деятельности: Пассажирские автоперевозки

Список сотрудников (офис):

Генеральный директор		Глушков П.М.
Заместитель директора		Смирнова Е.М.
Управляющий		Березуцкий М.Н.
Менеджер		Горшкова Н.В.
Бухгалтер		Мошникова Е.А.
Секретарь		Михалкова С.В.
Приходящий администратор	системный	Петров Н.В.
Уборщица		Лосева А.И.
Техник		Мягков Н.В.
Диспетчер (х20)		

Структура предприятия представлена на Рисунке 4.3:

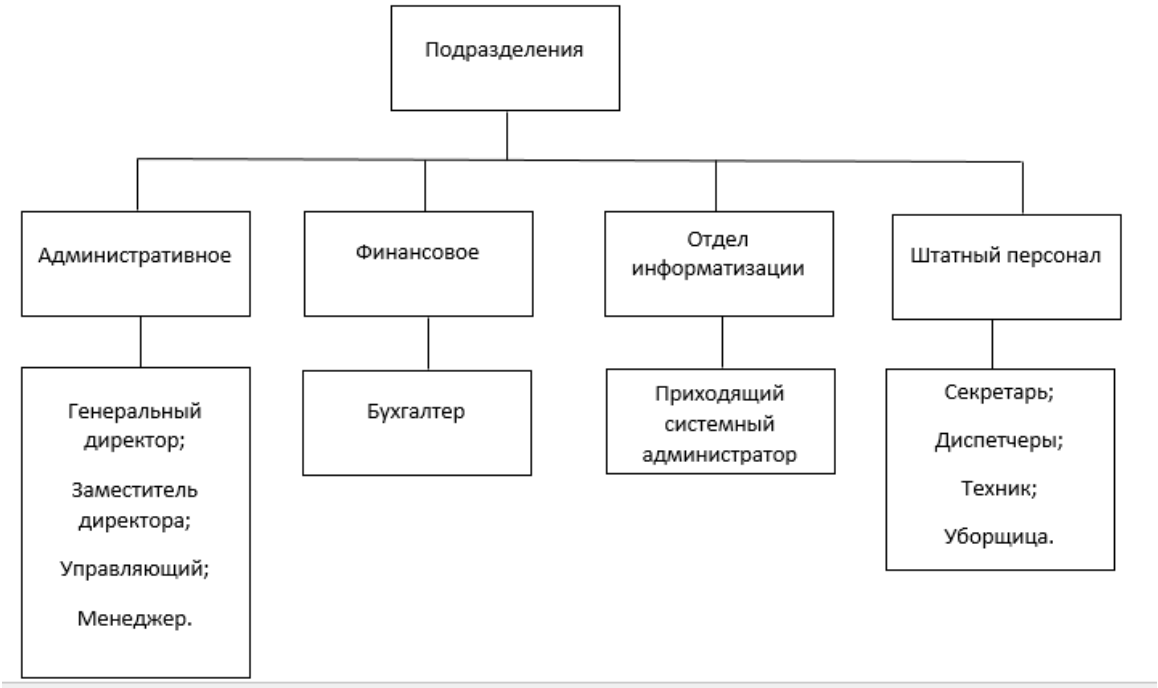

Рисунок 4.3 – Структура предприятия

4 Вариант

ООО «КнигоМир»

Род деятельности: Издательский дом

Список сотрудников (офис):

Генеральный директор	Яковлев В.С.
Заместитель директора	Третьяков М.В.
Редактор	Спиваков С.А.
Помощник редактора	Сливова Е.К.
Специалист по маркетингу	Дроздов А.В.
Специалист по производству	Теплов С.С.
Художник	Иванов И.И.
Бухгалтер	Вотинова Н.Г.
Секретарь	Лобова О.В.
Системный администратор	Красин О.О.
Специалист по кадрам	Михалкова О.Г.
Юрист	Оверчук О.О.
Уборщица	Лебедева Е.С.

Структура предприятия представлена на Рисунке 4.4:

Рисунок 4.4 – Структура предприятия

5 Вариант

Воинская часть

Род деятельности: Государственная организация

Список сотрудников (штаб):

Начальник штаба воинской части	Краснов К.А.
Заместитель начальника штаба	Времин С.С.
Начальник разведки	Смирнов Г.О.
Начальник топографической службы	Кабалин К.И.
Главный бухгалтер	Терешков С.К.

Бухгалтер	Козьмина М.А.
Врач	Смолов С.А.
Штабный писарь	Павлюков М.Н.
Штабный писарь	Сергеенко В.В.
Рядовой	Смирнов И.И.
Уборщица	Старостина Е.С.

Структура предприятия представлена на Рисунке 4.5:

Рисунок 4.5 – Структура предприятия

6 Вариант

ООО “НАНО”

Род деятельности: Ремонтные работы ПК

Список сотрудников:

Генеральный директор	Катюшина Н.С.
Управляющий	Власов А.К.
Бухгалтер	Малышева Е.А.
Оператор	Третьяков С.Н.
Техник	Ермолов С.С.
Техник	Крапивкин А.А.
Техник	Сухомлин И.Е.
Приходящий системный администратор	Петров Н.В.

Структура предприятия представлена на Рисунке 4.6:

Рисунок 4.6 – Структура предприятия

7 Вариант

ООО “Находка”

Род деятельности: Интернет-магазин одежды

Список сотрудников:

Директор	Мухачев Ю.Д.
Менеджер	Короблева В.С.
Бухгалтер	Мошникова О.А.
Приходящий системный администратор	Марин А.А.
Уборщица	Рашева В.С.
Оператор	Комков И.В.
Оператор	Азотова Л.С.
Оператор	Малышкина Н.О.

Структура предприятия представлена на Рисунке 4.7:

Рисунок 4.7 – Структура предприятия

8 Вариант

ООО “Звонок”

Род деятельности: Колл-центр

Список сотрудников (офис):

Генеральный директор		Татаров Г.В.
Управляющий		Самохина Л.В.
Бухгалтер		Березуцкая В.С.
Оператор		x8
Приходящий	системный	Смирнов Ю.Н.
администратор		

Структура предприятия представлена на Рисунке 4.8:

Рисунок 4.8 – Структура предприятия

9 Вариант

ООО “Форсаж”

Род деятельности: Автошкола

Список сотрудников:

Директор		Вотинов А.Д.
Секретарь		Туреева И.Н.
Бухгалтер		Сергиенко В.В.
Преподаватель		Яковлева В.С.
Преподаватель		Герчиков И.И.
Инструктор		Паринов С.А.
Инструктор		Брындин И.Н.
Приходящий	системный	Петров Н.В.
администратор		

Структура предприятия представлена на Рисунке 4.9:

Рисунок 4.9 – Структура предприятия

10 Вариант

ИП Солнцев Г.В.

Род деятельности: Стоматологическая клиника

Список сотрудников:

Директор	Солнцев Г.В.
Приходящий бухгалтер	Зеленин И.А.
Регистратор	Козьмина М.А.
Стоматолог-хирург	Лосев А.И.
Стоматолог-ортопед	Гриценко М.Е.
Медсестра	Вотинова Н.Г.
Медсестра	Старостина Л.Ф.
Санитар	Мошникова Н.Д.
Приходящий системный администратор	Петров Н.В.

Структура предприятия представлена на Рисунке 4.10:

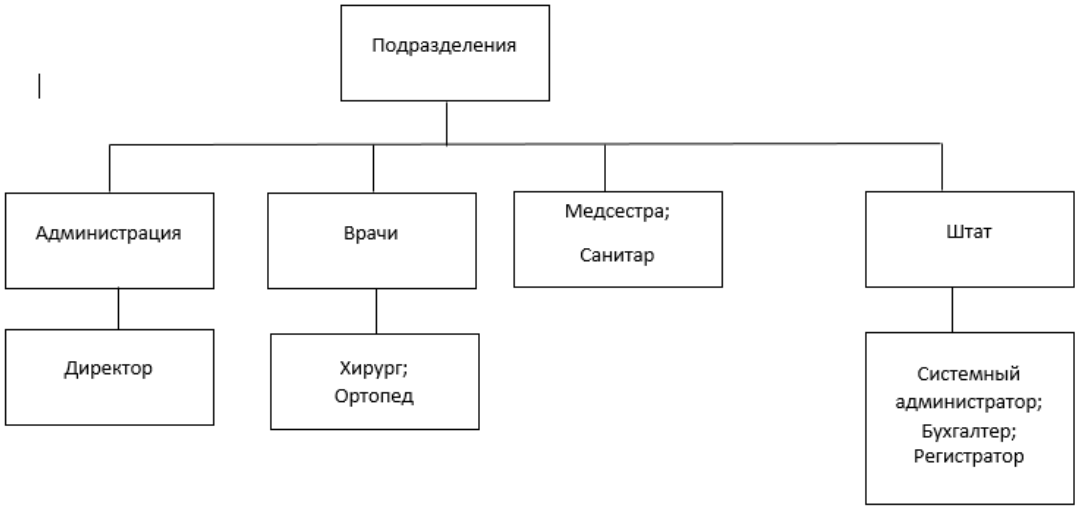

Рисунок 4.10 – Структура предприятия

Выводы по четвертой главе: После окончания обучения выпускники специальности «Информационная безопасность ТКС» могут пойти работать в различные организации независимо от их характера деятельности, формы собственности и размера. Поэтому целесообразно разработать несколько вариантов лабораторных работ, описывающих разные предприятия.

ЗАКЛЮЧЕНИЕ

Готовность будущего выпускника к профессиональной деятельности формируется в ходе получения не столько теоретических, сколько практических навыков работы. С этой целью в рабочую программу включены лабораторные занятия.

Было выявлено, что данная область динамично развивается, но проанализировав мировой опыт в управлении ИБ на предприятиях различного типа, а также изучив стандарты в данной области были разработаны семь лабораторных работ.

Разработанный комплект работ необходимо внедрить в учебный процесс дисциплины УИБТКС для качественной оценки и дальнейшего усовершенствования.

В качестве предложения по улучшению работ можно представить использование зарубежных разработок, но для этого студент должен обладать достаточными навыками в английском языке.

В ходе работы над ВКР были решены поставленные задачи тем самым была достигнута поставленная цель.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Специальность «Информационная безопасность телекоммуникационных систем». Код специальности: 10.05.02. [Электронный ресурс]. Режим доступа: https://abiturient.tusur.ru/ru/napravleniya-podgotovki/ochnaya-forma-obucheniya/2019-10-05-02-informatsionnaya-bezopasnost-telekommunikatsionnyh-sistem-fulltime (дата обращения: 25.11.18).
2. ФГОС специальности 10.05.02 «Информационная безопасность телекоммуникационных систем» Утвержден приказом Министерства образования и науки Российской Федерации от 16 ноября 2016 г. № 1426.
3. Вузы России со специальностью информационная безопасность телекоммуникационных систем – 10.05.02 [Электронный ресурс]. Режим доступа: http://vuzoteka.ru/вузы/Информационная-безопасность-телекоммуникационных-систем-10-05-02 (дата обращения: 6.01.19).
4. Рейтинг специальностей вузов [Электронный ресурс]. Режим доступа: https://moeobrazovanie.ru/specialities_rating_vuz/ (дата обращения: 6.01.19).
5. Сущность управления и менеджмента [Электронный ресурс]. Режим доступа: https://port-u.ru/managementorganizacii/sushnostupravleniya (дата обращения: 8.01.19).
6. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности организации. Основные термины и определения. – Введ. 2008-12-18. — М.: Изд-во стандартов, 2008. — 20 с.

7. Процессное управление организацией [Электронный ресурс]. Режим доступа: https://studfiles.net/preview/4002634/page:3/ (дата обращения: 6.01.19).
8. Применение цикла Шухарта-Деминга к процессу автоматизации обработки геопространственной информации. Пустынный Я. Н., Шошина К. В. Применение цикла Шухарта-Деминга к процессу автоматизации обработки геопространственной информации // Молодой ученый. — 2016. — №15. — С. 194-198. [Электронный ресурс]. Режим доступа: https://moluch.ru/archive/119/33069/ (дата обращения: 10.01.2019).
9. Астахов, А. Искусство управления информационными рисками / А. Астахов. — М.: ДМК Пресс, 2010. — 312
10. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. – Введ. 2005-12-29. — М.: Изд-во стандартов, 2006. — 62 с
11. История создания BS 7799 [Электронный ресурс]. Режим доступа: http://www.iso27000.ru/chitalnyi-zai/standarty-informacionnoi-bezopasnosti/bsi-i-bs-7799-2013-videnie-razrabotchikov (дата обращения: 14.01.2019).
12. Менеджмент информационной безопасности Лекция 1 Стандарт ISO 27001[Электронный ресурс]. Режим доступа: http://present5.com/menedzhment-informacionnoj-bezopasnosti-lekciya-1-standart-iso-27001/ (дата обращения: 14.01.2019).
13. Основы управления информационной безопасностью / Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. — 2-е изд., М.: Горячая линия - Телеком, 2014. — 244 с

14. СТО БР ИББС-2.5-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности. Введ. 2014-06-01. — Москва.: 2014. — 29 с.
15. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. – Введ. 2015-08-19. — М.: Изд-во стандартов, 20015. — 12 с
16. Программные средства для управления ИБ и анализа рисков [Электронный ресурс]. Режим доступа: http://itsec.ru/articles2/control/programmnye-sredstva-dlya-upravleniya-ib-i-analiza-riskov (дата обращения: 16.01.2019).
17. Digital Security ГРИФ и КОНДОР для "Energbak". [Электронный ресурс]. Режим доступа: http://deeplace.md/project/digital-security-grif-i-kondor-dlya-energbak (дата обращения: 16.09.2018).
18. РискДетектор [Электронный ресурс]. Режим доступа: http://www.srisks.ru (дата обращения: 17.09.2018).
19. Матричный подход к анализу рисков информационной безопасности [Электронный ресурс]. Режим доступа: https://studref.com/312208/informatika/matrichnyy_podhod_analizu_riskov_informatsionnoy_bezopasnosti (дата обращения: 18.09.2018).
20. Методика CRAMM [Электронный ресурс]. Режим доступа: https://www.intuit.ru/studies/courses/531/387/lecture/8996 (дата обращения: 18.01.2018).
21. Управление информационной безопасностью. / А.А. Конев, Е.М. Давыдова, А.А. Шелупанов — Т.: В-Спектр, 2017. — 122 с

ПРИЛОЖЕНИЕ 1

Решение пробного варианта

Лабораторная работа №1

«Матричный подход к анализу рисков ИБ»

Цель работы: изучить основные понятия СМИБ.

Задание выполнение работы:

1. Выявить активы, уязвимости, угрозы и средства управления в соответствии с вариантом задания;

2. Разработать соответствующие матрицы и рассчитать соответствующие им формулы.

Ход работы:

Вариант 0.

1. Определение ценности активов:

Шкала: от 0 до 3.

0- актив не ценен

1- Актив средней ценности

2-Ценный актив

3- Очень ценный актив

Идентификация активов

Первичные:

- Информация о поставщиках (ценность а=3)
- Информация о сбыте готового продукта (а=3)
- Метод переработки мусора (а=3)

Активы поддержки:

- Стационарная аппаратура: компьютеры, сервер (а=2)
- Периферийное обрабатывающее оборудование: факс, принтер. (а=1)
- Электронные носители данных: USB-накопители (а=1)
- Другие носители данных: документация (а=2)

- Программное обеспечение: 1:С. Предприятие 8, UniSender, Microsoft Access (a=1)

- Операционная система: Windows 8 (a=1)

- Персонал (a=2)

- Зона: Офис (a=2)

- Коммуникации: источники электропитания с низким напряжением (a=1)

Идентификация уязвимости:

1. Восприимчивость к пыли сервера.
2. Погодные условия.
3. Перепады напряжения.
4. Новое ПО.
5. Подкуп менеджера.

Идентификация угроз:

1. Загрязнение сервера и последующий выход его из строя.
2. Невыход на работу штатного персонала.
3. Поломка компьютеров.
4. Программный сбой.
5. Кража данных для аутентификации и идентификации бухгалтера и изменение данных о поставщиках.

Идентификация средств контроля:

1. Антивирус KasperskyTotalSecurity – на каждом АРМ.
2. Средство защиты от несанкционированного доступа «Страж NT» - на сервере и каждом АРМ.
3. СКУД «Castle» - для входной двери.
4. Камеры видеонаблюдения (2 шт.) – в офисе.

2. Разработка матриц:

Таблица 1 Матрица активов

Шкала: **0 – нет воздействия** **1 – слабое воздействие** **2 – умеренное воздействие** **9 – сильное воздействие** **Уязвимость**	**Активы и затраты**	Информация о поставщиках	Информация о сбыте готового продукта	Метод переработки мусора	Стационарная аппаратура	Периферийное обрабатывающее оборудование	Электронные носители данных	Документация	Программное обеспечение	Персонал	Коммуникация	Офис
Восприимчивость к пыли сервера		2	2	2	9	9	0	0	2	0	0	0
Погодные условия		0	0	0	0	0	0	0	0	9	2	1
Перепады напряжения		2	2	2	9	9	0	0	0	1	1	1
Новое ПО		1	1	1	2	0	0	0	9	2	0	0
Подкуп менеджера		9	9	9	0	0	9	9	0	1	0	0

Таблица 2 Воздействие уязвимости на активы

$V_{ij}=C_i*a_j$	C_1	C_2	C_3	C_4	C_5
a_1=3	6	0	6	3	27
a_2=3	6	0	6	3	27
a_3=3	6	0	6	3	27
a_4=2	18	0	18	4	0
a_5=1	9	0	9	0	0
a_6=1	0	0	0	0	9
a_7=2	0	0	0	0	18
a_8=1	2	0	0	9	0
a_9=2	0	18	2	4	2
a_{10}=2	0	4	2	0	0
a_{11}=1	0	1	1	0	0

Совокупное воздействие:

V_1=47

V_2=23

V_3=50

V_4=26

V_5=110

Таблица 3 Матрица угроз

Шкала: **0 – нет воздействия** **1 – слабое воздействие** **2 – умеренное воздействие** **9 – сильное воздействие** **Уязвимость**	**Угрозы**	Загрязнение сервера и последующий выход его из строя	Невыход на работу штатного персонала	Поломка компьютеров	Программный сбой	Кража данных для аутентификации и идентификации бухгалтера и изменение данных о поставщиках
Восприимчивость к пыли сервера		9	0	2	0	0
Погодные условия		1	9	1	1	0
Перепады напряжения		0	0	9	0	0
Новое ПО		0	0	2	9	0
Подкуп менеджера		0	0	1	0	9

Таблица 4 Воздействие угрозы уязвимости

$T_{ij}=d_i*V_j$	d_1	d_2	d_3	d_4	d_5
V_1	423	0	94	0	0
V_2	23	207	23	23	0
V_3	0	0	450	0	0
V_4	0	0	52	234	0
V_5	0	0	110	0	990

Совокупное воздействие:

T_1=446

T_2=207

T_3=729

T_4=257

T_5=990

Таблица 5 Матрица контроля

Шкала: **0 – нет воздействия** **1 – слабое воздействие** **2 – умеренное воздействие** **9 – сильное воздействие** **Средства контроля**	**Угрозы**	Загрязнение сервера и последующий выход его из строя	Невыход на работу штатного персонала	Поломка компьютеров	Программный сбой	Кража данных для аутентификации и идентификации бухгалтера и изменение данных о поставщиках
Антивирус KasperskyTotalSecurity		0	0	1	9	2
Средство защиты от несанкционированного доступа «Страж NT»		0	0	2	0	9
СКУД «Castle»		0	1	1	0	9
Камеры видеонаблюдения		0	2	2	0	9

Таблица 6 Воздействие средств контроля

$Z_{ij}=e_i*T_j$	e_1	e_2	e_3	e_4
T_1	0	0	0	0
T_2	0	0	207	414
T_3	729	1458	729	1458
T_4	2313	0	0	0
T_5	1980	8910	8910	8910

Совокупное воздействие:

V_1=5022

V_2=10368

V_3=9846

V_4=10782

Вывод: Анализ уязвимостей и угроз показал, что на предприятии нет средства контроля для угрозы загрязнения оборудования, а лучше всего справляются с задачей контроля камеры видеонаблюдения и средства защиты от несанкционированного доступа.

Контрольные вопросы.

1. Как определяется понятие Риск?

Риск – это потенциальная возможность того, что установленная угроза воспользуется уязвимостью актива или группой активов и тем самым нанесёт ущерб организации.

2. Что такое Уязвимость?

Уязвимость - недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации.

3. Что такое Угроза?

Угроза – совокупность условий или факторов, создающих потенциальную или реально существующую опасность нарушение безопасности информации.

4. Что такое Актив?

Актив - все, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении.

5. Объясните, чем занимается СМИБ?

Система менеджмента информационной безопасности (СМИБ) — часть общей системы менеджмента, которая основана на подходе бизнес-рисков при создании, внедрении, функционировании, мониторинге, анализе, поддержке и улучшении информационной безопасности.

Лабораторная работа №2

«Разработка Политики ИБ организации»

Цель работы: изучить основные аспекты, включаемые в политику ИБ.

Задание выполнение работы:

1. Изучить политику ИБ «Газпромбанк»;
2. Разработать политику ИБ организации в соответствии с вариантом.

Ход работы:

Вариант 0.

1. Изучить политику ИБ «Газпромбанк» и заполнить таблицу (Таблица 1).

Таблица 1 Основные аспекты политики ИБ

Основные объекты защиты системы ИБ.	• информационные ресурсы, содержащие коммерческую тайну, банковскую тайну, персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы Банка, независимо от формы и вида ее представления; • информационные ресурсы, содержащие конфиденциальную информацию, включая персональные данные

	физических лиц, а также открыто распространяемая информация, необходимая для работы Банка, независимо от формы и вида ее представления; • сотрудники Банка, являющиеся разработчиками и пользователями информационных систем Банка; • информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Продолжение Таблицы 1

Цели в области информационной безопасности.	Снижение угроз информационной безопасности до приемлемого для Банка уровня.
Задачи обеспечения информационной безопасности.	• выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты; • предотвращение инцидентов информационной безопасности; • исключение либо минимизация выявленных угроз.
Принципы обеспечения	Изложены в пункте 7 данной

информационной безопасности.	Политики.
Распределение ролей и ответственности.	• Общее руководство обеспечением информационной безопасности Банка и контроль осуществляет Куратор. • Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности Банка и контроль лежит на руководстве Ответственного подразделения.
Ответственность за нарушение Политики информационной безопасности.	определяется соответствующими положениями, включаемыми в договоры с работниками Банка, а также положениями внутренних нормативных документов Банка.

2. По примеру изученной политики ИБ разработать Политику ИБ для своей организации по варианту.

Контрольные вопросы.

1. Что такое Политика Информационной безопасности предприятия?

Политика информационной безопасности – это совокупность правил, процедур, практических методов и руководящих принципов в области ИБ, используемых организацией в своей деятельности.

2. На основе какого (каких) нормативного (ых) документа (ов) строится Политика ИБ?

СТО БР ИББС-1.0–2006, ISO/IEC 27001-2005, ISO/IEC 17799-2005, ISO/IEC 13335, ГОСТ Р ИСО/МЭК 15408, стандарты BS и ГОСТ Р.

3. Что должна включать в себя Политика ИБ?

- определение информационной безопасности, её общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации;

- изложение целей и принципов информационной безопасности, сформулированных руководством;

- краткое изложение наиболее существенных для организации политик безопасности, принципов, правил и требований;

- определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности;

- ссылки на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры для конкретных информационных систем, а также правила безопасности, которым должны следовать пользователи.

4. Когда или при каких обстоятельствах должна быть пересмотрена Политика ИБ?

Политика информационной безопасности должна пересматриваться либо через запланированные интервалы

времени, либо, если произошли значительные изменения, с целью обеспечения уверенности в ее актуальности, адекватности и эффективности.

5. Кем утверждается Политика ИБ предприятия?

Руководством организации.

Лабораторная работа №3

«Анализ рисков на основе ПО «РискДетектор»

Цель работы: знакомство и работа с автоматизированной системой управления рисками РискДетектор.

Задание выполнение работы:

1. Выполнить пробный вариант;

2. В соответствии с описанием системы внести данные в программный комплекс.

Ход работы:

Вариант 0.

1. Изучить работу системы, выполнив пробный вариант из описания лабораторной работы.

Сохраненный отчет по пробному варианту находится в файле primer.rtf.

2. В соответствии с вариантом внести данные в систему и подготовить отчет.

Сохраненный отчет по варианту 0 находится в файле var0.rtf.

Вывод: Оценка риска с помощью программного комплекса РискДетектор показала значение риска 16,01.

Риск доступности – 4,3; рикс конфиденциальности – 5,34; риск целостности – 3,89.

Контрольные вопросы.

1. Что представляет собой система РискДетектор и для каких целей она предназначена?

РискДетектор – это система автоматизации управления рисками, аудита, мониторинга, контроля фундаментальности безопасности, обеспечения качества критериев и нормативной базы.

- Контроль и информированность о выполнении требований по безопасности. Полная картина состояния безопасности.

- Быстрое усвоение исполнителями требований по безопасности.

- Преодоление тенденций к оптимизации за счет невыполнения требований по безопасности.

- Повышение дисциплины выполнения требований во всех подразделениях.

- Усиление самоконтроля за выполнением требований, в том числе, за счет наличия полных и исчерпывающих списков требований на каждом рабочем месте и осуществления периодического контроля их выполнения.

- Быстрое реагирование на появление новых угроз путем оперативного доведения требований до исполнителей.

- Готовность к любым внешним проверкам по безопасности.

- Получение инструмента выбора и обоснования комплексов мер в области обеспечения безопасности.

- Повышение качества инспекционного контроля и сокращение затрат на инспекционный контроль.

- Обеспечение полноты требований. Устранение избыточности и противоречивости требований.

2. Кто разработал РискДетектор?

Институт системного анализа РАН

3. Как выглядит срез структуры?

Срез структуры состоит из элементов: Модели, Регионы, Локальные среды, Подсистемы, Объекты.

4. Какие виды отчетов можно получить для среза структуры?

- Структурное описание оцениваемой системы;
- Выполнение требований;
- Оценка возможных рисков доверия – рисков невыполненных требований;
- Оценка уровней рисков;
- Структурная координата невыполненных требований;
- Показатели ИБ;
- Категорирование объекта.

5. Приведите примеры мер защиты для Ресурсов АИС?

- Обеспечение ответственности за ИР;
- Классификация информации по уровням конфиденциальности;
- Оперирование носителями информации и их защита;
- Безопасность в прикладных системах;
- Защита файлов прикладных систем.

6. Перечислите требования к мере защиты: Классификация информации по уровням конфиденциальности.

- Выполнение рекомендаций по классификации;
- Присваивание грифов секретности.

Лабораторная работа № 4

«Анализ и управление рисками ИС на основе ПО «ГРИФ» пакета DigitalSecurityOffice»

Цель работы: знакомство и работа с системой анализа и управления информационными рисками ГРИФ.

Задание выполнение работы:

1.В соответствии с описанием системы составить таблицу, содержащую отделы и перечень ресурсов.

2.Составить матрицу доступа.

3.В соответствии с описанием системы по варианту внести данные в программный комплекс и составить отчёт.

Ход работы:

Вариант 0.

1. Составление таблицы, содержащей отделы и перечень ресурсов.

Таблица 1 Отделы и ресурсы предприятия

Объекты	
Отделы	Администрация, Экономический, Безопасности, Штат
Сетевая группа	Офис
Ресурсы	Сервер, 9 рабочих станций
Сетевое	Маршрутизатор

устройство	
Вид информации	БД клиентов, Отчеты, личные карточки, контракты, штатное расписание, кадровые операции, аттестация, приказы, табельный учет
Группа пользователей	Руководство, Менеджер, Специалист по работе с персоналом, Системный администратор, Бухгалтерия, Секретарь ресепшен, Секретарь, Начальник ОБ, Уборщица
Бизнес-процесс	Метод переработки

2. Матрица доступа.

Таблица 2 Отделы и ресурсы предприятия

	БД клиентов	Отчеты	точкиЛичные	Контракты	аниеШтатное	цииКадровые	Аттестация	Приказы	нетТабельный
Руководство	WR E, V, У	WR E, V, У	-	WR E, V, У	WR E, V, У	-	WR E, Л	WR E, V, У	R, V, У
Менеджер	WR, V, У	WR, V, У	-	WR, V, У	R, V, У	-	-	WR, V, У	-
Специалист по работе с персоналом	-	WR, V, У	WR E, Л	R, V, У	WR E, V, У	WR E, Л	-	WR, V, У	WR E, V, У

Продолжение Таблицы 2

Бухгалтерия	R, V, У	WR, V, У	-	R, V, У	R, V, У	-	-	WR, V, У	R, V, У
Секретарь на ресепшен	-	-	-	-	R, V, У	-	-	R, V, У	WR, V, У
Секретарь	-	WR, V, У	-	-	R, V, У	-	-	R, V, У	R, V, У
Системный администратор	-	-	-	-	R, V, У	-	-	R, V, У	-
Уборщица	-	-	-	-	R, V, У	-	-	R, V, У	-
Начальник отдела безопасности	-	R, V, У	-	R, V, У	R, V, У	-	-	WR, V, У	R, V, У

W-запись
R-чтение
E-изменение
V-наличие VPN – соединения
- - нет прав доступа
Л/У – локальный/удаленный вид доступа

3. В соответствии с вариантом внести данные в систему и подготовить отчет.

Сохраненный отчет по варианту 0 находится в файле Отчёт_ЧистыйМир(Л4).dsrep, который можно открыть с помощью программы «ГРИФ». Для этого нужно запустить саму программу, нажать «Отчёт-Загрузить отчёт».

Вывод: Оценка риска с помощью программного комплекса «ГРИФ» показала, что значение риска по показателям доступности, конфиденциальности и целостности высокое, следовательно, требуются существенные контрмеры и пересмотр Политики безопасности предприятия.

Контрольные вопросы.

1. Какие виды анализа рисков существуют в ПО «ГРИФ»?

«Анализ модели информационных потоков» и «Анализ модели угроз и уязвимостей».

2. Опишите пошагово работу с моделью информационных потоков?

Шаг 1: Пользователю необходимо внести все объекты системы ИС.

Шаг 2: На этом шаге пользователь должен определить к каким отделам и сетевым группам относятся ресурсы, какая информация хранится на ресурсе и какие группы пользователей имеют к ней доступ, таким образом, проставляются связи. Также на данном шаге указываются средства защиты информации и ресурсов.

Шаг 3: Этот шаг предполагает ответы на список вопросов по политике безопасности, реализованный в системе.

3. Какие виды объектов вводятся в программу при описании ИС?

Отделы, ресурсы (специальными объектами являются сетевые группы, сетевые устройства, виды информации, группы пользователей, бизнес-процессы).

4. Что такое Риск?

Риск – вероятный ущерб, который понесет организация при реализации угроз информационной безопасности, зависящий от защищенности системы.

5. Что такое Ресурс?

Ресурс – физический ресурс, на котором располагается ценная информация (сервер, рабочая станция, мобильный компьютер и т.д.).

6. Что такое контрмера?

Контрмера – действие, которое необходимо выполнить для закрытия уязвимости.

Лабораторная работа № 5

«Анализ рисков на основе моделей угроз и уязвимостей с помощью «ГРИФ» пакета DigitalSecurityOffice»

Цель работы: знакомство и работа с системой анализа и управления информационными рисками ГРИФ; изучение алгоритма «Анализ модели угроз и уязвимостей».

Задание выполнение работы:

1. В соответствии с описанием системы внести данные в программный комплекс, также используя данные о ресурсах и отделах из Л.р.№4 и данные об угрозах и уязвимостях из Л.р. №1.

2. Подготовить отчёт сделать соответствующие выводы.

Ход работы:

Вариант 0.

1. Перечень отделов и ресурсов организации.

Таблица 1 Отделы и ресурсы предприятия

Объекты	
Отделы	Администрация, Экономический, Безопасности, Штат
Ресурсы	3 сервера, 9 рабочих станций

2. Идентификация угроз и уязвимостей.

Идентификация уязвимости:

1. Восприимчивость к пыли сервера.
2. Погодные условия.
3. Перепады напряжения.
4. Новое ПО.
5. Подкуп менеджера.

Идентификация угроз:

1. Загрязнение сервера и последующий выход его из строя. (P=13.6%)
2. Невыход на работу штатного персонала. (P=8.4%)

3.Поломка компьютеров. (P=16.8%)

4.Программный сбой. (P=31.2%)

5.Кража данных для аутентификации и идентификации бухгалтера и изменение данных о поставщиках. (P=2.8%)

Таблица 2 Контрмеры

Название контрмеры	Стоимость внедрения, у.е.	Снижение затрат на ИБ, у.е.
Более частая уборка	100000	228000
Оплата такси	10000	19000

Продолжение Таблицы 2

Работа специалиста, по настройке системы архивирования и резервного копирования	2000	3800
Резервное АРМ	50000	95000
Новое ПО с улучшенной системой разграничения прав доступа	30000	57000

Сохраненный отчет по варианту 0 находится в файле Вариант0.dsrep, который можно открыть с помощью программы «ГРИФ». Для этого нужно запустить саму программу, нажать «Отчёт-Загрузить отчёт».

Вывод: Оценка риска методом анализа угроз и уязвимостей показала риск равный 21,05%. После внедрения контрмер риск снизился до 0, т.е. эффективность контрмер составляет 100%.

Контрольные вопросы.

1. Опишите пошагово работу с моделью анализа угроз и уязвимостей?

Шаг 1: Пользователю необходимо внести все объекты системы ИС.

Шаг 2: На этом шаге пользователь должен определить, к каким отделам относятся ресурсы, какие угрозы действуют на ресурс и через какие уязвимости они реализуются, таким образом, проставляются связи.

2. Какие виды объектов вводятся в программу при описании ИС?

Отделы, ресурсы, угрозы информационной системы, уязвимости, через которые реализуются угрозы.

3. Что такое угроза?

Угроза – действие, которое потенциально может привести к нарушению безопасности. Свойством угрозы является перечень уязвимостей, при помощи которых может быть реализована угроза.

4. Что такое уязвимость?

Уязвимость – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы. Свойствами уязвимости являются: вероятность (простота)реализации угрозы через данную уязвимость и критичность реализации угрозы через данную уязвимость.

5. На какие категории система «ГРИФ» делит угрозы?

Система «ГРИФ» делит угрозы на шесть категорий:

- физические угрозы человека (потенциального нарушителя);

- физические угрозы (вызванные форс-мажорными обстоятельствами);

- локальные программные угрозы, направленные на ресурс (без использования каналов связи);

- удаленные программные угрозы, направленные на ресурс (с использованием каналов связи);

- программные угрозы, направленные на канал связи (кабельная система, коммуникационное оборудование, ПО);

- угрозы персонала (вызванные действиями сотрудников компании).

6. Какие виды разделов содержит отчет? Дайте краткое описание каждому разделу.

Отчет разбит на четыре раздела:

- инвентаризация;
- информационные риски;
- соотношение ущерба и риска;
- контрмеры.

Раздел «*Инвентаризация*» содержит информацию о системе, включая информацию о стоимости ресурса, угрозах и уязвимостей, по которым эти угрозы ревизуются.

Раздел «*Информационные риски*» отражает риск всех ресурсов по угрозам и уязвимостям, а также суммарные риски по отделам.

В разделе «*Соотношение ущерба и риска*» находится информация о соотношении ущерба и риска отделов, ресурсов и всей информационной системе в целом.

Последний раздел «*Контрмеры*» содержит информацию об контрмерах и их эффективности.

Лабораторная работа № 6

«Анализ рисков на основе DigitalSecurity.КОНДОР»

Цель работы: знакомство и работа с системой DigitalSecurity.КОНДОР.

Задание выполнение работы:

1. В соответствии с описанием системы и разработанной политикой ИБ в Л.р. № 2 ответить на вопросы в программном комплексе.

2. Задать контрмеры для снижения риска и подготовить отчёт, сделать соответствующие выводы.

Ход работы:

Вариант 0.

Отчёт находится в файле Отчёт_Л6.dsrep.

Вывод: Оценка организации на соответствие требованиям стандарта ISO 17799 с помощью «КОНДОР» показала риск равный 36,06%. После внедрения контрмер риск снизился до 34,64, т.е. эффективность контрмер составляет 1,42%.

Контрольные вопросы.

1. Какой подход к обеспечению ИБ предприятия применяет «КОНДОР»?

Комплексный подход.

2. Как стандарт ISO 17799 определяет термины конфиденциальность, целостность и доступность информации?

Конфиденциальность – обеспечение доступа к информации только авторизованным пользователям.

Целостность – обеспечение достоверности и полноты информации и методов её обработки.

Доступность - обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

3. Какова цель политики ИБ организации?

Обеспечить управление и поддержку высшим руководством ИБ в соответствии с требованиями бизнеса и соответствующими законами, и нормами.

4. Какие данные вносятся в раздел «Расходы на ИБ»?

- Разовые затраты на приобретение систем защиты информации.
- Ежегодные затраты на поддержку и обучение (если она не
- Ежегодные затраты на управление средствами защиты информации.
- Прочие ежегодные затраты на обеспечение информационной безопасности.
- Изменение затрат после внедрения контрмер.

Лабораторная работа № 7

«Анализ рисков по методике CRAMM»

Цель работы: освоение и применение методики оценки рисков CRAMM.

Задание выполнение работы:

1. Провести оценку ресурсов, угроз и уязвимостей для ИС из Л.р.№1.

2. Рассчитать значения риска и предложить контрмеры, для значения риска в границах от 5 до 7.

Ход работы:

Вариант 0.

1. Идентификация ресурсов.

Таблица 1 Ресурсы ИС

Ресурс	**Потери**
1. Информация о поставщиках	200 000 у.е.
2. Информация о сбыте готового продукта	300 000 у.е.
3. Метод переработки мусора	5 000 000 у.е.
4. Стационарная аппаратура: компьютеры, сервер	80 000 у.е.
5. Периферийное обрабатывающее оборудование: факс, принтер	20 000 у.е.
6. Электронные носители данных: USB-накопители	1 000 у.е.
7. Другие носители данных: документация	30 000 у.е.
8. Программное обеспечение: 1:С. Предприятие 8, UniSender, Microsoft Access	50 000 у.е.
9. Операционная система: Windows 8	20 000 у.е.
10. Персонал	40 000 у.е.
11. Зона: Офис	50 000 у.е.

12. Коммуникации: источники электропитания с низким напряжением	20 000 у.е.

2. Идентификация угроз.

Таблица 2 Угрозы ИС

Угроза	Значение
Загрязнение сервера и последующий выход его из строя	0,1
Невыход на работу штатного персонала	0,1
Поломка компьютеров	0,1
Программный сбой.	0,33
Кража данных для аутентификации и идентификации бухгалтера и изменение данных о поставщиках	0,1

3. Идентификация уязвимости.

Таблица 3 Уязвимости ИС

Уязвимость	Значение
Восприимчивость к пыли сервера	0,33
Погодные условия	0,1
Перепады напряжения	0,1
Новое ПО	1
Подкуп менеджера	1

4. Контрмеры

Так как при оценке риска угроза программного сбоя показала наибольший балл (6), для снижения риска предложим контрмеру.

Таблица 4 Контрмеры

Название	Стоимость

контрмеры	внедрения, у.е.
Резервное АРМ	50000

Вывод: Оценка риска методом CRAMM показала, что существует высокий риск при реализации уязвимости – Новое ПО. Были предложены контрмеры для снижения показателя уровня риска.

Контрольные вопросы.

1. Какая методика расчета рисков (количественная, качественная или комплексная) применяется CRAMM?

В методе CRAMM применяется комплексная методика расчёта рисков.

Первоначальные оценки даются на качественном уровне, и потом производится переход к количественной оценке (в баллах).

2. Опишите стадии оценки риска методикой CRAMM.

1) Идентификация ресурсов;
2) Идентификация угроз и уязвимостей и расчёт рисков;
3) Применение контрмер.

3. Назовите преимущества методики CRAMM?

- Комплексный подход;

- Экономическое обоснование расходов предприятия на ОИБ при грамотном использовании метода, что позволяет избежать лишних расходов.

4. Назовите недостатки метода CRAMM?

- Использование метода CRAMM требует специальной подготовки и высокой квалификации аудитора;

- CRAMM в гораздо большей степени подходит для аудита уже существующих ИС, находящихся на стадии эксплуатации, нежели чем для ИС, находящихся на стадии разработки;

- Аудит по методу CRAMM – процесс достаточно трудоемкий и может потребовать месяцев непрерывной работы аудитора;

- Программный инструментарий CRAMM генерирует большое количество бумажной документации, которая не всегда оказывается полезной на практике;

- CRAMM не позволяет создавать собственные шаблоны отчетов или модифицировать имеющиеся;

- ПО CRAMM существует только на английском языке

5. По какой формуле рассчитывался уровень риска в данной лабораторной работе?

*Величина риска = Оценка частоты возникновения угрозы * Оценка частоты возникновения уязвимости * Значение стоимости ресурса.*

6. Что такое аудит ИБ организации?

Аудит – это систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению информационной безопасности и установлению степени выполнения в организации критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности организации.

ПРИЛОЖЕНИЕ 2
Графическое представление организаций

1 Вариант:

Рисунок 1 – ООО «МамаИталия»

2 Вариант:

Рисунок 2 – ООО «Окно в Европу»

3 Вариант:

Рисунок 3 - ООО Такси «Санкт-Петербург»

4 Вариант:

Рисунок 4 – ООО «КнигоМир»

5 Вариант:

Рисунок 5 – Воинская часть

6 Вариант:

Рисунок 6 – ООО «Нано»

7 Вариант:

Рисунок 7 – ООО «Находка»

8 Вариант:

Рисунок 8 – ООО «Звонок»

9 Вариант:

Рисунок 9 – ООО «Форсаж»

10 Вариант:

Рисунок 10 – ИП Солнцев ГВ