МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г.Локтионова
«4» 04 2022 г

АНАЛИЗ И УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ В ПРОГРАММЕ “ГРИФ”

Методические рекомендации для практических занятий и самостоятельной работы для студентов специальностей и направлений подготовки 10.00.00 10.03.01, 38.05.01, 09.03.02, 09.03.03, 45.03.03, 09.03.04, 40.03.01, 38.03.03, 12.03.04, 11.03.02

Курск 2022

2

УДК 004.056(076.5)

Составитель: А.Л. Марухленко

Рецензент

Кандидат технических наук, доцент М.О.Таныгин

Анализ и управление информационными рисками в программе "Гриф": методические указания по выполнению лабораторных работ и практических занятий/ Юго-Зап. гос. ун-т; сост.: А.Л.Марухленко. – Курск, 2022. – 31 с.: ил. 6, табл. 3. – Библиогр.: с. 31.

Содержат краткие теоретические положения о методике анализа информационных рисков, оценки ущерба и принятия контрмер в целях обеспечения информационной безопасности системы.

Методические указания соответствуют требованиям программы по направлению подготовки : информационная безопасность и специалистов: экономическая безопасность. Предназначены для студентов специальностей и направлений подготовки 10.00.00 10.03.01, 38.05.01, 09.03.02, 09.03.03, 45.03.03, 09.03.04, 40.03.01, 38.03.03, 12.03.04, 11.03.02.

Текст печатается в авторской редакции

Подписано в печать Формат 60x84 1/16
Усл.печ. л. Уч. –изд. л. Тираж 100 экз. Заказ 1259 Бесплатно
Юго-Западный Государственный Университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Введение

Построение любой ИС должно начинаться с анализа рисков. Этот анализ включает мероприятия по обследованию безопасности ИС с целью определения того, какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите. В ходе анализа определяются наборы адекватных контрмер для управления рисками. Применительно к ИС риск определяется вероятностью причинения ущерба и величиной ущерба, наносимого ресурсам ИС в случае осуществления угрозы безопасности.

Для решения задачи оценки информационных рисков используются следующие методики: логарифмическая шкала, оценка по верхним и нижним значениям, оценка на основе выявления слабого звена, оценка риска на основе рассмотрения этапов вторжения.

Рассмотрим данные модели оценки рисков. В частности, рассмотрим модель, используемую фирмой IBM. В качестве показателя частоты возникновения интересующего события принята величина S, значения которой приведены в таблице 1.

Таблица1. Частота проявления угрозы

Частота проявления угрозы	S	Частота проявления угрозы	S
Никогда	0	Раз в год	4
Раз в 1000 лет	1	10 раз в год	5
Раз в 100 лет	2	100 раз в год	6
Раз в 10 лет	3	1000 раз в год	7

Ожидаемый ущерб (R) от i-й угрозы (причины) предложено вычислять по формуле: $Ri = 10(S+V-4)$. Общий ущерб рассчитывается как сумма ущерба от всех угроз.

Некоторые специалисты предлагают оценивать ожидаемый ущерб по верхним и нижним взвешенным значениям. Такой подход предполагает, что известны вероятности появления угроз, а также минимальное и максимальное значение ущерба при появлении угрозы. Оценки ущерба, представленные в таблице 2, получаются путем умножения вероятности появления угрозы на минимальное и максимальное значение возможного ущерба.

Таблица 2. Величина ущерба

Величина ущерба V в зависимости от абсолютного значения потерь принимает следующие значения.			
Потери, долл.	V	Потери, долл.	V
1 долл.	0	10 тыс. долл.	4
10 долл.	1	150 тыс. долл.	5
100 долл.	2	1 млн. долл.	6
1000 долл.	3	10 млн. долл.	7

Если, например, пожар в течение года может возникнуть с вероятностью 0,5%, а ущерб от пожара может вызвать потери от 100 тыс. руб. до 100 млн. руб., то нижней взвешенной оценкой будет 500 руб., а верхней – 500 тыс. руб.

В методике оценки на основе выявления слабого звена уровень защиты любой ИС определяется самым слабым ее звеном. При использовании данной методики необходимо рассматривать возможность случайного или намеренного вывода из строя каждого элемента ИС. Для полной оценки эффективности и надежности СЗИ необходимо произвести анализ местоположения не только ИС, но и всех периферийных устройств, а также предусмотреть все угрозы, связанные с физической защитой оборудования.

Следующая методика оценки рисков нарушения защиты, которая устанавливается межсетевым экраном от угроз со стороны Интернет. Эта методика основывается на восьмиэтапной модели оценки риска и представляет собой рассмотрение в виде цепочек множества возможных атак на систему. Перечислим основные этапы модели оценки риска: препятствие атаке, атака, обнаружение атаки, противодействие атаке, взлом, обнаружение взлома, противодействие взлому, результирующий ущерб.

Среди программных систем, используемых для анализа и управления рисками можно указать следующие [1]: британский CRAMM (компания Insight Consulting), американский Risk Watch (компания Risk Watch) и российский ГРИФ (компания Digital Security).

Метод CRAMM

CRAMM (the UK Government Risk Analysisand Management

Method) — метод, разработанный Службой Безопасности Великобритании и является государственным стандартом Великобритании. Получил широкое распространение в мире. Данный стандарт используется как в коммерческих, так и в государственных организациях Великобритании с 1985 года. Метод CRAMM был изобретён фирмой Insight Consulting Limited. Базируясь на комплексном подходе к оценке рисков, метод CRAMM сочетает количественные и качественные методы анализа рисков и может быть применен как в крупных, так и небольших организациях. Имеются различные версии CRAMM для разных типов организаций, они отличаются базами знаний (профилями): существует коммерческий профиль и правительственный профиль.

Грамотное использование метода CRAMM позволяет получать очень хорошие результаты, наиболее важным из которых является возможность экономического обоснования расходов организации на обеспечение информационной безопасности и непрерывности бизнеса. Экономически обоснованная стратегия управления рисками позволяет экономить средства, избегая неоправданных расходов.

CRAMM предполагает разделение всей процедуры на три последовательных этапа. На первом этапе необходимо определить достаточно ли для защиты системы применения средств базового уровня, реализующих традиционные функции безопасности, или же необходимо проведение более детального анализа. На втором этапе производится идентификация рисков и оценивается их величина. На третьем этапе решается вопрос о выборе адекватных контрмер.

Методика CRAMM для каждого этапа определяет набор исходных данных, последовательность мероприятий, анкеты для проведения интервью, списки проверки и набор отчетных документов.

На первой стадии исследования производится идентификация и определение ценности защищаемых ресурсов. Оценка производится по десятибалльной шкале, причем критериев оценки может быть несколько - финансовые потери, потери репутации и т.д.

Если по результатам проведения первого этапа, установлено, что уровень критичности ресурсов является очень низким и существующие риски заведомо не превысят некоторого базового уровня, то к системе предъявляется минимальный набор требований безопасности. В этом случае большая часть мероприятий второго этапа не выполняется, а осуществляется переход к третьему этапу, на котором генерируется стандартный

список контрмер для обеспечения соответствия базовому набору требований безопасности.

На втором этапе производится анализ угроз безопасности и уязвимостей. Исходные данные для оценки угроз и уязвимостей аудитор получает от уполномоченных представителей организации в ходе соответствующих интервью. Для проведения интервью используются специализированные опросники.

На третьем этапе решается задача управления рисками, состоящая в выборе адекватных контрмер. Решение о внедрении в систему новых механизмов безопасности и модификации старых принимает руководство организации, учитывая связанные с этим расходы, их приемлемость и конечную выгоду для бизнеса. Задачей аудитора является обоснование рекомендуемых контрмер для руководства организации.

Концептуальная схема проведения обследования по методу CRAMM показана на рисунке 1.

Рис.1-Концептуальная схема проведения обследования по методу CRAMM

К недостаткам метода CRAMM можно отнести следующее: · 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.

· Возможность внесения дополнений в базу знаний CRAMM недоступна пользователям, что вызывает определенные трудности при адаптации этого метода к потребностям конкретной организации.

· ПО CRAMM существует только на английском языке. ·

Высокая стоимость лицензии.

Risk Watch

Разработанный американской компанией Risk WatchInc., одноименный программный продукт служит мощным инструментом анализа и управления рисками. Данное семейство продуктов используется для различных видов аудитов безопасности и содержит следующие средства:

· Risc Watch for Physical Security — инструмент для физических методов защиты информационных систем; · Risc Watch for Information Systems — инструмент, применяемый к информационным рискам;

· HIPPAA-WATCH forHealthcareIndustry — инструмент для оценки соответствия стандарта HIPAA;

· Risk Watch RW17799 for ISO17799 — для оценки требованиям стандарта ISO17799.

Критериями для оценки и управления рисками в методе RiskWatch служит «предсказание годовых потерь» (ALE — Annual Loss Expectancy) и оценка подсчёта ROI (Returnon Investment) — «возврата от инвестиций».

Используемая в программе методика включает в себя 4 фазы. Первая фаза — определение предмета исследования. На данном этапе описываются общие параметры организации — тип организации, состав исследуемой системы, базовые требования в области безопасности. Описание формализуется в ряде подпунктов, которые можно выбрать для более подробного описания или пропустить.

Далее каждый из выбранных пунктов описывается подробно. Для облегчения работы аналитика в шаблонах даются списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты. Из них нужно выбрать те, что реально присутствуют в организации.

Вторая фаза — ввод данных, описывающих конкретные

характеристики системы. Данные могут вводиться вручную или импортироваться из отчетов, созданных инструментальными средствами исследования уязвимости компьютерных сетей. На этом этапе подробно описываются ресурсы, потери и классы инцидентов.

Классы инцидентов получаются путем сопоставления категории потерь и категории ресурсов. Для выявления возможных уязвимостей используется опросник, база которого содержит более 600 вопросов, связанных с категориями ресурсов. Допускается корректировка вопросов, исключение или добавление новых. Задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов. Все это используется в дальнейшем для расчета эффективности внедрения средств защиты.

Третья фаза — оценка рисков. Сначала устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих этапах. Для рисков рассчитываются математические ожидания потерь за год по формуле: $m=p * v$, где p — частота возникновения угрозы в течение года, v — стоимость ресурса, который подвергается угрозе.

Четвертая фаза — генерация отчетов. Типы отчетов: краткие итоги; полные и краткие отчеты об элементах, описанных на стадиях 1 и 2; отчет о стоимости защищаемых ресурсов и ожидаемых потерь от реализации угроз; отчет об угрозах и мерах противодействия; отчет о результатах аудита безопасности.

Таким образом, рассматриваемое средство позволяет оценить не только те риски, которые сейчас существуют у предприятия, но и ту выгоду, которую может принести внедрение физических, технических, программных и прочих средств и механизмов защиты. Подготовленные отчеты и графики дают материал, достаточный для принятия решений об изменении системы обеспечения безопасности предприятия.

Для отечественных пользователей проблема заключается в том, что получить используемые в RiskWatch оценки для наших условий достаточно проблематично. Хотя сама методология может с успехом применяться и у нас.

Подводя итог, можно отметить, что конкретную методику проведения анализа рисков на предприятии и инструментальные средства, поддерживающие ее, нужно выбирать, учитывая следующие факторы:

- Наличие экспертов, способных дать достоверные оценки объема потерь от угроз информационной безопасности;
- Наличие на

предприятии достоверной статистки по инцидентам в сфере информационной безопасности; ▪ Нужна ли точная количественная оценка последствий реализации угроз или достаточно оценки на качественном уровне. К недостаткам RiskWatch можно отнести:

· Такой метод подходит, если требуется провести анализ рисков на программно-техническом уровне защиты, без учета организационных и административных факторов. Полученные оценки рисков (математическое ожидание потерь) далеко не исчерпывают понимание риска с системных позиций — метод не учитывает комплексный подход к информационной безопасности.

· ПО RiskWatch существует только на английском языке. · Высокая стоимость лицензии — от $15 000 за одно рабочее место для небольшой компании и от $125 000 за корпоративную лицензию.

ГРИФ

В отличие от западных систем анализа рисков, достаточно громоздких и не предполагающих самостоятельное применение IT менеджерами и системными администраторами, система ГРИФ располагает интуитивно-понятным интерфейсом. Но при всей простоте, в системе ГРИФ реализованы огромное количество алгоритмов анализа рисков, учитывающие более ста параметров, и система способна предоставить максимально точную оценку рисков, которые имеют место в информационной системе. Важная особенность ГРИФ — в предоставлении возможности самостоятельной, без привлечения экспертов, оценки рисков в информационной системе, оценка текущего состояния, и расчёта инвестиций в целях обеспечения защищённости информации.

Основная задача системы ГРИФ — дать возможность IT менеджеру самостоятельно (без привлечения сторонних экспертов) оценить уровень рисков в информационной системе и эффективность существующей практики по обеспечению безопасности компании, а также предоставить возможность доказательно (в цифрах) убедить руководство компании в необходимости инвестиций в сферу ее информационной безопасности.

На первом этапе метода ГРИФ проводится опрос IT менеджера с целью определения полного списка информационных ресурсов, представляющих ценность для компании.

На втором этапе проводится опрос IT-менеджера с целью ввода

в систему ГРИФ всех видов информации, представляющей ценность для компании. Введенные группы ценной информации должны быть размещены пользователем на указанных на предыдущем этапе объектах хранения информации (серверах, рабочих станциях и т. д.). Заключительная фаза — указание ущерба по каждой группе ценной информации, расположенной на соответствующих ресурсах, по всем видам угроз.

На третьем этапе проходит определение всех видов пользовательских групп с указанием числа пользователей в каждой группе. Затем фиксируется, к каким группам информации на ресурсах имеет доступ каждая из групп пользователей. В заключение определяются виды (локальный и/или удаленный) и права (чтение, запись, удаление) доступа пользователей ко всем ресурсам, содержащим ценную информацию.

На четвертом этапе проводится опрос IT-менеджера для определения средств защиты ценной информации на ресурсах. Кроме того, в систему вводится информация о разовых затратах на приобретение всех применяющихся средств защиты информации и ежегодные затраты на их техническую поддержку, а также ежегодные затраты на сопровождение системы информационной безопасности компании.

На завершающем этапе необходимо ответить на вопросы по политике безопасности, реализованной в системе, что позволит оценить реальный уровень защищенности системы и детализировать оценки рисков.

Наличие средств информационной защиты, отмеченных на первом этапе, само по себе еще не делает систему защищенной в случае их неадекватного использования и отсутствия комплексной политики безопасности, учитывающей все аспекты защиты информации, включая вопросы организации защиты, физической безопасности, безопасности персонала, непрерывности ведения бизнеса и т. д.

В результате выполнения всех действий по данным этапам, на выходе будет сформирована полная модель информационной системы с точки зрения информационной безопасности с учетом реального выполнения требований комплексной политики безопасности, что позволит перейти к программному анализу введенных данных для получения комплексной оценки рисков и формирования итогового отчета.

К недостаткам ГРИФ можно отнести:

- Отсутствие привязки к бизнес-процессам.

· Отсутствие возможности сравнения отчетов на разных этапах внедрения комплекса мер по обеспечению защищенности. · Отсутствие возможности добавления специфичных для данной компании требований политики безопасности. Таким образом, анализ рисков — достаточно трудоемкая процедура. В процессе анализа рисков должны применяться методические материалы и инструментальные средства. Однако для успешного внедрения повторяемого процесса этого недостаточно; еще одна важная его составляющая — регламент управления рисками. Он может быть самодостаточным и затрагивать только риски ИБ, а может быть интегрирован с общим процессом управления рисками в организации.

В процессе анализа рисков задействованы многие структурные подразделения организации: подразделения, ведущие основные направления ее деятельности, подразделение управления информационной инфраструктурой, подразделение управления ИБ. Кроме того, для успешного проведения анализа рисков и эффективного использования его результатов необходимо привлечь высший менеджмент организации, обеспечив тем самым взаимодействие между структурными подразделениями.

Лабораторная работа

«Анализ и управление информационными рисками в программе ГРИФ».

Цель работы: ознакомиться с программой ГРИФ, построить модель информационной системы организации, на основе которой проанализировать риск и защищенность ресурсов.

Методические указания для алгоритма «Анализ модели информационных потоков»

1. Запустить программу ГРИФ. На экране появится окно, в которое необходимо ввести имя пользователя и пароль. **2.** В появившемся окне согласно варианту выбрать алгоритм и нажать «Создать проект». Ввести его название, если Вы работаете с программой впервые. Если же Вам необходимо открыть существующий проект, выберите «Открыть проект». **3.** Для построения модели информационной системы организации, на основе которой будут анализироваться риск и защищенность ресурсов, необходимо сначала занести данные о системе. Для этого

необходимо в рабочем меню выбрать: Проект→Свойства проекта и в закладке «Идентификация» ввести данные о системе. Пример показан на рисунке 2.

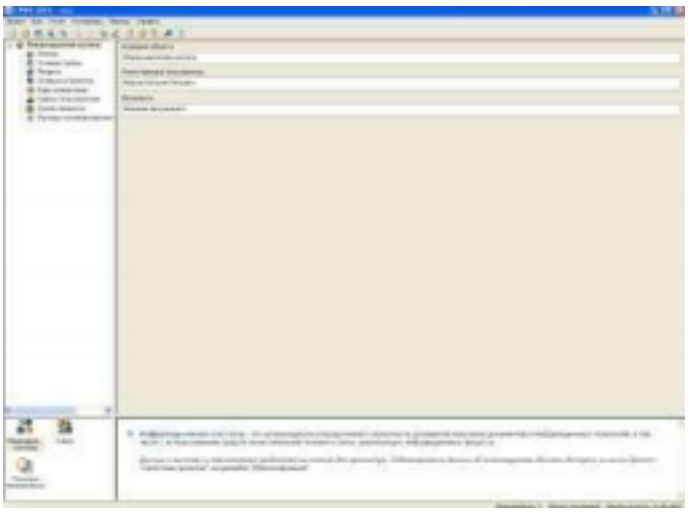

Рисунок 2 – Регистрация в системе

4. В раздел «Моделирование системы» занести данные обо всех объектах существующей информационной системы (отделы, сетевые группы, ресурсы, сетевые устройства, виды информации, группы пользователей, бизнес-процессы).

4.1 Открыть элемент информационной системы «Отделы» и согласно вашему варианту ввести название отдела. Для создания нового отдела выполните следующие шаги: 1) Нажать кнопку «Добавить».

2) Ввести название нового отдела.

3) При необходимости ввести комментарий.

4) Нажать кнопку «Добавить» или клавишу {Enter}. Созданный отдел появится на рабочем поле.

5) Для закрытия окна нажать кнопку «Закрыть» или клавишу {Esc}.

4.2 Сетевые группы записываются аналогично пункту 4.1.

4.3 Для создания нового ресурса выполните следующие шаги:

1) Нажать кнопку «Добавить».

2) Ввести название нового ресурса.

3) Указать тип ресурса.

4) Укажите параметр "Дополнительное время простоя". 5) В раскрывающемся списке "Укажите сетевую группу" выберите ту сетевую группу, к которой принадлежит добавляемый ресурс. Данный раскрывающийся список - перечень сетевых групп,

добавленных в информационную систему. Ресурс может не принадлежать ни к одной сетевой группе.

6) В раскрывающемся списке "Укажите отдел" выберите тот отдел, к которому принадлежит добавляемый ресурс. Данный раскрывающийся список - перечень отделов, добавленных в информационную систему. Ресурс может не принадлежать ни к одному отделу.

7) При необходимости введите комментарий.

8) Нажмите кнопку «Добавить» или клавишу {Enter}. Созданный ресурс появится на рабочем поле.

9) Для закрытия окна нажмите кнопку «Закрыть» или клавишу {Esc}.

4.4 Для создания нового сетевого устройства выполнить следующие шаги:

1) Нажать кнопку «Добавить».

2) Ввести название сетевого устройства.

3) Указать тип сетевого устройства:

4) Указать параметр "Время простоя".

5) При необходимости ввести комментарий.

6) Нажать кнопку «Добавить» или клавишу {Enter}. Созданное сетевое устройство появится на рабочем поле. 7) Для закрытия окна нажать кнопку «Закрыть» или клавишу {Esc}.

4.5 Для создания нового вида информации выполнить следующие шаги:

1) Нажать кнопку «Добавить».

2) Ввести название нового вида информации.

3) При необходимости ввести комментарий.

4) Нажать кнопку «Добавить» или клавишу {Enter}. Созданный вид информации появится на рабочем поле. 5) Для закрытия окна нажмите кнопку «Закрыть» или клавишу {Esc}.

4.6 Для создания новой группы пользователей выполнить следующие шаги:

1) Нажать кнопку «Добавить».

2) Ввести название группы пользователей.

3) Указать класс группы пользователей.

4) Указать параметр "Число пользователей в группе", произвольно.

5) Указать параметр "Данной группе разрешен доступ в Интернет".

6) Параметр "Данной группе разрешен доступ в Интернет" означает, что группа пользователей имеет доступ к ресурсам,

расположенным в сети Интернет, однако, доступ к ресурсам организации данная группа пользователей получает напрямую, не используя сеть Интернет.

7) Указать, какие средства используются для защиты рабочего места пользователя, по усмотрению.

8) При необходимости ввести комментарий.

9) Нажать кнопку «Добавить» или клавишу {Enter}. Созданная группа пользователей появится на рабочем поле. 10) Для закрытия окна нажмите кнопку «Закрыть» или клавишу {Esc}.

4.7 Для создания нового бизнес-процесса выполнить следующие шаги:

1) Нажать кнопку «Добавить».

2) Ввести название нового бизнес-процесса.

3) При необходимости ввести комментарий.

4) Нажать кнопку «Добавить» или клавишу {Enter}. Созданный бизнес-процесс появится на рабочем поле. 5) Для закрытия окна нажать кнопку «Закрыть» или клавишу {Esc}.

4.8 Для того, что бы задать расходы необходимо: 1) Открыть элемент информационной системы «Расходы на информационную безопасность».

2) Нажать на кнопку  . В появившемся окне задать расходы.

3) Ввести значение расходов, по своему усмотрению. 4) Нажать кнопку OK или клавишу {Enter}.

5) Для закрытия окна нажать кнопку Отмена или клавишу {Esc}.

5. В разделе «Связи» определяются связи между объектами, занесенными в разделе "Моделирование системы".

5.1 Для добавления вида информации выполнить следующие шаги:

1) Нажать кнопку «Добавить».

2) В раскрывающемся списке выбрать вид информации. 3) Указать ущерб по угрозам.

4) Нажать кнопку «Добавить» или клавишу {Enter}. Выбранный вид информации появится на рабочем поле. 5) Для закрытия окна нажать кнопку «Закрыть» или клавишу {Esc}.

5.2 Для добавления группы пользователей выполнить следующие шаги:

1) Нажать кнопку «Добавить».

2) В раскрывающемся списке выбрать группу пользователей.

3) Указать параметр "Вид доступа".

4) Указать параметр "Права доступа".

5) Для удаленного доступа к ресурсу "Сервер" указать параметр "Доступ осуществляется при помощи VPN". 6) Нажать кнопку «Добавить» или клавишу {Enter}. Выбранная группа пользователей появится на рабочем поле. 7) Для закрытия окна нажать кнопку «Закрыть» или клавишу {Esc}.

5.3 Для выбора сетевых устройств, через которые группа пользователей осуществляет доступ к ресурсу "Сервер", выполнить следующие шаги:

1) Отметить используемые сетевые устройства. Данный список - перечень сетевых устройств, добавленных в разделе "Моделирование системы".

2) Нажать кнопку OK или клавишу {Enter}.

3) Для закрытия окна без сохранения изменений нажать 4) кнопку «Отмена» или клавишу {Esc}.

5.4 Следующая закладка «Бизнес-процессы» позволяет выбрать бизнес-процессы, в которых хранится и обрабатывается ценная информация.

1) Отметить те бизнес-процессы, которые используются для данного вида информации.

2) Нажать кнопку OK или клавишу {Enter}.

3) Для закрытия окна без сохранения изменений нажать кнопку Отмена или клавишу {Esc}.

5.5 Для выбора средств защиты ресурса выполнить следующие шаги:

1) Отметить используемые средства защиты.

2) Нажать кнопку OK или клавишу {Enter}.

3) Для закрытия окна нажать кнопку Отмена или клавишу {Esc}.

5.6 Для выбора средств защиты указанного вида информации выполнить следующие шаги:

1) Отметить используемые средства защиты.

2) Нажать кнопку OK или клавишу {Enter}.

3) Для закрытия окна нажать кнопку Отмена или клавишу {Esc}.

6. Политика безопасности - раздел, в котором приведены вопросы, учитывающие организационные меры обеспечения информационной безопасности. В правой части окна находится рабочее поле. Сначала необходимо выбрать раздел, тогда на рабочем поле отобразится перечень вопросов по данному разделу. Далее необходимо выбрать вопрос и нажать кнопку «Изменить». Для ответа

на вопрос выполнить следующие шаги:

1) Отметить ответ на данный вопрос.

2) Нажать на кнопку «Принять».

3) После принятия ответа программа перейдет к следующему неотвеченному вопросу.

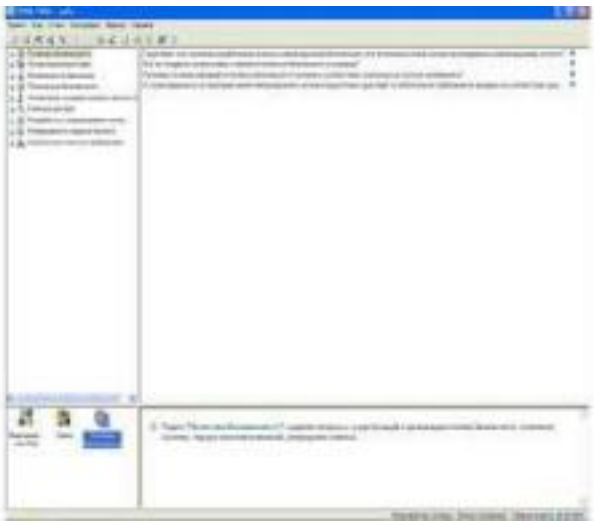

Рисунок 3 – Ввод ответа на вопрос

7. Далее необходимо ввести контрмеры. Для этого необходимо выбрать пункт меню Контрмеры→ Управление рисками и для каждого объекта задать контрмеры. Пример показан на рисунке 4.

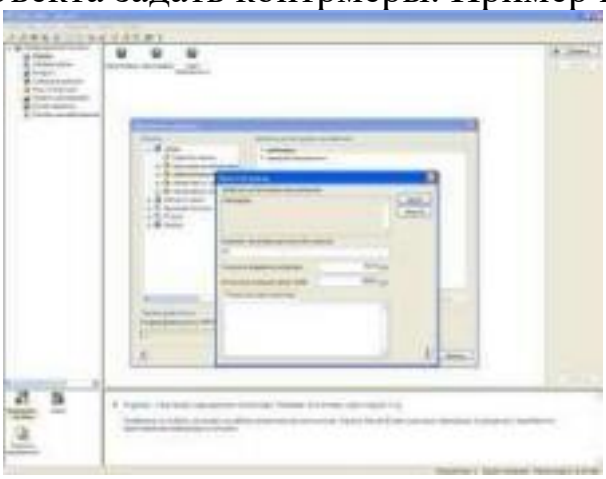

Рисунок 4 – Пример задания контрмер

8. После задания контрмер нужно создать отчет. Для настройки параметров и создания отчета выполнить следующие шаги:

1) Выбрать пункт меню Отчет→ Создать отчет

2) Выбрать состав отчета.

3) Выбрать форму отчета.

4) Нажать кнопку ОК или клавишу {Enter}.

9. Далее необходимо применить все контрмеры и повторить действия пункта 8. Должно получиться 2 отчета. Необходимо их сравнить.

Методические указания для модели «Анализ модели угроз и уязвимостей»:

1. Запустить программу ГРИФ. На экране появится окно, в которое необходимо ввести имя пользователя и пароль. **2.** В появившемся окне согласно варианту выбрать алгоритм и нажать «Создать проект». Ввести его название, если Вы работаете с программой впервые. Если же Вам необходимо открыть существующий проект, выберите «Открыть проект». **3.** Для построения модели информационной системы организации, на основе которой будут анализироваться риск и защищенность ресурсов, необходимо сначала занести данные о системе. Для этого необходимо в рабочем меню выбрать: Проект→Свойства проекта и в закладке «Идентификация» ввести данные о системе.

4. В раздел «Моделирование системы» занести данные обо всех объектах существующей информационной системы (отделы, сетевые группы, ресурсы, сетевые устройства, виды информации, группы пользователей, бизнес-процессы).

4.1 Открыть элемент информационной системы «Отделы» и согласно вашему варианту ввести название отдела. Для создания нового отдела выполните следующие шаги: 1) Нажать кнопку «Добавить».

2) Ввести название нового отдела.

3) При необходимости ввести комментарий.

4) Нажать кнопку «Добавить» или клавишу {Enter}. Созданный отдел появится на рабочем поле.

5) Для закрытия окна нажать кнопку «Закрыть» или клавишу {Esc}.

4.2 Для создания нового ресурса выполнить следующие шаги:

1) Нажать кнопку «Добавить».

2) Ввести название нового ресурса.

3) Указать тип ресурса.

4) Указать параметр "Дополнительное время простоя". 5) Указать параметр "Критичность ресурса".

6) В раскрывающемся списке "Укажите отдел" выбрать тот отдел, к которому принадлежит добавляемый ресурс. Данный раскрывающийся список - перечень отделов, добавленных в информационную систему. Ресурс может не принадлежать ни к одному отделу.

6) При необходимости ввести комментарий.

7) Нажать кнопку «Добавить» или клавишу {Enter}. Созданный ресурс появится на рабочем поле.

8) Для закрытия окна нажать кнопку «Закрыть» или клавишу {Esc}.

4.3 Для добавления новой предопределенной угрозы выполнить следующие шаги:

1) Нажать кнопку «Выбрать»...

2) В окне «Предопределенные угрозы» выбрать необходимую угрозу.

3) Нажать кнопку «ОК» или клавишу {Enter}.

4) В окне «Новая угроза» ввести название новой угрозы. 5) При необходимости ввести комментарий..

6) Нажать кнопку «Добавить». Созданная угроза появится на рабочем поле.

7) Для закрытия окна нажать кнопку «Закрыть» или клавишу {Esc}.

Для создания новой угрозы выполнить следующие шаги:

1) Ввести название новой угрозы.

2) Ввести описание угрозы.

3) Выберите категорию угрозы.

4) При необходимости ввести комментарий.

5) Нажать кнопку «Добавить» или клавишу {Enter}. Созданная угроза появится на рабочем поле. 6) Для закрытия окна нажать кнопку «Закрыть» или клавишу {Esc}.

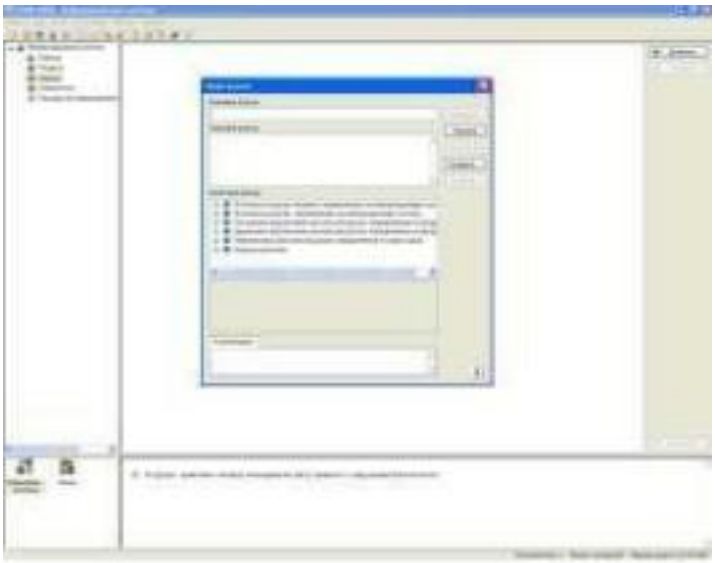

Рисунок 5 – Создание угрозы

4.4 Для создания новой уязвимости выполнить следующие шаги:

1) Ввести название новой уязвимости.

2) Ввести описание уязвимости.

3) Выбрать угрозы, которые реализует добавляемая уязвимость, по своему усмотрению.

4) При необходимости ввести комментарий.

5) Нажать кнопку «Добавить» или клавишу {Enter}. Созданная угроза появится на рабочем поле.

6) Для закрытия окна нажать кнопку «Закрыть» или клавишу {Esc}.

Для добавления новой предопределенной уязвимости выполнить следующие шаги:

1) Нажать кнопку «Выбрать»...

2) В окне "Предопределенные уязвимости" выбрать необходимую уязвимость.

3) Нажать кнопку «ОК» или клавишу {Enter}.

4) В окне "Новая уязвимость" ввести название новой уязвимости.

5) Выбрать угрозы, которые реализует добавляемая уязвимость.

6) Нажать кнопку «Добавить». Созданная угроза появится на рабочем поле.

7) Для закрытия окна нажать кнопку «Закрыть».

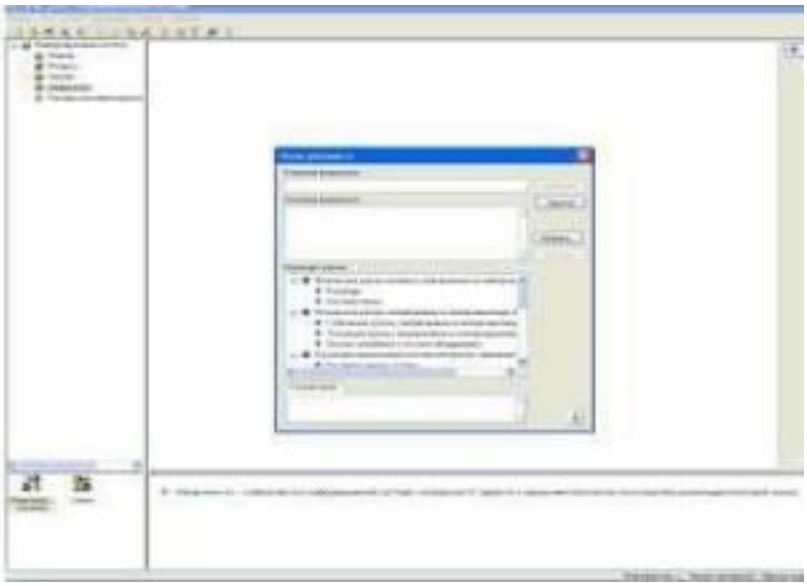

Рисунок 6 – Создание новой уязвимости

4.5 Для задания новых расходов нужно выполнить следующие шаги:

1) Ввести значение расходов.

2) Нажать кнопку «OK» или клавишу {Enter}.

3) Для закрытия окна нажать кнопку «Отмена» или клавишу {Esc}.

5. Раздел «Связи». В этом разделе определяются связи между объектами, занесѐнными в разделе «Моделирование системы».

Вид рабочего поля зависит от выбранного элемента информационной системы:

При выборе отдела рабочее поле отображает все ресурсы, принадлежащие данному отделу. Пользователь может просмотреть свойства ресурсов и при необходимости отредактировать их.

При выборе ресурса рабочее поле отображает закладки для определения связей между данным ресурсом, угрозами и уязвимостями.

5.1 Для добавления угрозы выполнить следующие шаги: 1) Выбрать угрозу, действующую на данный ресурс. 2) Нажать кнопку «Добавить» или клавишу {Enter}. 3) В появившемся окне "Добавление угрозы":

– отметить те уязвимости, через которые выбранная угроза действует на данный ресурс.

– указать параметр "Вероятность угрозы через данную уязвимость в течение года" - вероятность реализации данной угрозы. Указывается в процентах.

– указать параметр "Критичность реализации угрозы" - степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса. Задается в процентах.

– в зависимости от указанного значения параметра иконка напротив выбранной уязвимости может принять вид: 4) Нажмите кнопку «Добавить» или клавишу {Enter}.

Выбранная угроза появится на рабочем поле.

5) Для закрытия окна "Добавить угрозу" нажмите кнопку «Закрыть» или клавишу {Esc}.

5.2 Для добавления уязвимости выполнить следующие шаги:

1) Выбрать уязвимость, реализующую угрозу на данном ресурсе.

2) Нажать кнопку «Добавить» или клавишу {Enter}. 3) В появившемся окне "Добавление уязвимости": - Отметить те угрозы, которые действуют на ресурс через выбранную уязвимость.

- Указать параметр "Вероятность угрозы через данную уязвимость в течение года" - вероятность реализации данной угрозы. Указывается в процентах.

- Указать параметр "Критичность реализации угрозы" - степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса. Задается в процентах.

4) Нажать кнопу «Добавить» или клавишу {Enter}. Выбранная уязвимость появится на рабочем поле.

5) для закрытия окна "Добавить уязвимость" нажать кнопку «Закрыть» или клавишу {Esc}.

6. Далее необходимо ввести контрмеры. Для этого необходимо выбрать пункт меню Контрмеры→ Управление рисками и для каждого объекта задать контрмеры.

7. После задания контрмер нужно создать отчет. Для настройки параметров и создания отчета выполнить следующие шаги:

1. Выбрать пункт меню Отчет → Создать отчет
2. Выбрать состав отчета.
3. Выбрать форму отчета.
4. Нажать кнопку ОК или клавишу {Enter}.

8. Далее необходимо применить все контрмеры и повторить действия пункта 7. Должно получиться 2 отчета. Необходимо их сравнить.

Краткая теория

ГРИФ – комплексная система анализа и управления рисками информационной системы компании. ГРИФ 2006 дает Вам полную

картину защищенности информационных ресурсов в Вашей системе и позволяет выбрать оптимальную стратегию защиты информации Вашей компании.

Система ГРИФ:

-Анализирует уровень защищенности всех ценных ресурсов компании.

- Оценивает возможный ущерб, который понесет компания в результате реализации угроз информационной безопасности

Позволяет эффективно управлять рисками при по мощи выбора контрмер, наиболее оптимальных по соотношению цена/качество.

Как работает система ГРИФ:

Система ГРИФ 2006 предоставляет возможность проводить анализ рисков Вашей информационной системы при помощи анализа модели информационных потоков или модели угроз и уязвимостей в зависимости от того, какие исходные данные есть в Вашем распоряжении, а также от того, какие данные Вас интересуют на выходе.

При работе с моделью информационных потоков, в систему вносится полная информация обо всех ресурсах с ценной информацией, о пользователях, имеющих доступ к этим ресурсам, о 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.

Работа с моделью анализа угроз и уязвимостей подразумевает определение уязвимостей каждого ресурса с ценной информацией и подключение соответствующих угроз, которые могут быть реализованы через данные уязвимости. В результате получается полная картина того, какие слабые места есть в Вашей информационной системе и тот ущерб, который может быть нанесен.

Основные понятия и допущения модели:

Бизнес-процессы – это производственные процессы, в которых обрабатывается ценная информация.

Веб-сервер - ресурс, не содержащий ценную информацию, к которому возможен неконтролируемый доступ анонимных пользователей из Интернет.

Группа пользователей – это группа пользователей, имеющая одинаковый класс и средства защиты. Субъект, осуществляющий

доступ к информации.

Время простоя сетевого устройства - время, в течение которого доступ, осуществляемый с помощью сетевого устройства, к информации ресурса невозможен из-за отказа в обслуживании сетевого устройства.

Дополнительное время простоя ресурса - дополнительное к базовому время простоя, в течение которого доступ к информации ресурса невозможен. Обусловлено неадекватной работой программного или аппаратного обеспечения ресурса. Указывается в часах в год.

Доступ осуществляется при помощи VPN – доступ к информации осуществляется с помощью защищенного криптографическими средствами соединения.

Информационная система – это упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Информация – ценная информация, хранящаяся и обрабатываемая в информационной системе. Т.е. объект, к которому осуществляется доступ. Исходя из допущений данной модели, вся информация является ценной, т.к. оценить риск неценной информации не представляется возможным.

Класс группы пользователей – это особая характеристика группы, показывающая, как осуществляется доступ к информации.

Основные классы групп пользователей:

- Авторизованные пользователи из Интернет - пользователи, осуществляющие авторизованный доступ к ресурсам организации из Интернет.
- Анонимные пользователи из Интернет - пользователи, осуществляющие неавторизованный доступ к открытым ресурсам организации из Интернет.
- Менеджеры - руководители среднего звена, имеющие удаленный и/или локальный доступ к ресурсам из офиса организации.
- Мобильные пользователи - сотрудники организации, осуществляющие авторизованный доступ к ресурсам организации по телекоммуникационным каналам (например, находясь в командировке).
- Офицеры безопасности - пользователи, имеющие исключительные привилегии при доступе к ресурсам организации и

администрировании информационной системы организации (специалисты, отвечающие за обеспечение информационной безопасности системы).

-Пользователи - обычные сотрудники, имеющие удаленный и/или локальный доступ к ресурсам из офиса организации. - Системные администраторы - пользователи, имеющие исключительные привилегии при доступе к ресурсам организации и администрировании информационной системы организации (специалисты, отвечающие за конфигурирование и настройку информационной системы).

- Сотрудники, осуществляющие доступ через Интернет - сотрудники организации, осуществляющие доступ к ресурсам компании через Интернет из офиса (филиала) организации.

- Сотрудники, осуществляющие доступ через модем - сотрудники организации, осуществляющие доступ к ресурсам компании по модемному соединению из офиса организации.

- Топ-менеджеры - руководители высшего звена, имеющие удаленный и/или локальный доступ к ресурсам из офиса организации.

-*Коммутатор* - концентратор, который может одновременно устанавливать соединения между несколькими парами портов и реализует виртуальные соединения между сетевыми сегментами.

-*Контрмера* – это действие, которое необходимо выполнить для закрытия уязвимости

-*Концентратор* - многопортовое устройство, используемое для усиления сигналов при передаче данных.

-*Коэффициент локальной защищенности информации на ресурсе* – рассчитывается, если к информации осуществляется только локальный доступ. В этом случае клиентское место группы пользователей и ресурс, на котором хранится информация, совпадают, поэтому защищенность группы пользователей отдельно оценивать не нужно.

-*Коэффициент локальной защищенности рабочего места группы пользователей* - рассчитывается, когда группа пользователей осуществляет удаленный доступ к информации; это сумма значений эффективности средств защиты субъекта или клиентского места группы пользователей. Данный коэффициент невозможно определить для групп анонимных и авторизованных Интернет-пользователей.

-*Коэффициент удаленной защищенности информации на ресурсе* - рассчитывается, когда к информации осуществляется

удаленный доступ; это сумма значений эффективности средств защиты объекта.

-*Критичность ресурса – степень* значимости ресурса для информационной системы, т.е. как сильно реализация угроз информационной безопасности на ресурс повлияет на работу информационной системы.

-*Локальный доступ* – доступ к ресурсу, который осуществляется без использования каналов связи. Примечание: к ресурсам "Рабочая станция", "Мобильный компьютер" и "Твердая копия" возможен только локальный доступ.

-*Маршрутизатор* - устройство, обеспечивающее трафик между локальными сетями, имеющими разные сетевые адреса. -*Мобильный компьютер* - ресурс, содержащий ценную информацию, к которому возможен только локальный доступ. Пользователь имеет возможность выносить мобильный компьютер за пределы офиса организации.

-*Моделирование системы* - раздел, в котором заносятся данные обо всех объектах существующей информационной системы (отделы, сетевые группы, ресурсы, сетевые устройства, виды информации, группы пользователей, бизнес-процессы).

-*Модем* - внешнее или внутреннее устройство, подключаемое к компьютеру для передачи и приема сигналов по телекоммуникационным линиям.

-*Отдел* – это структурное подразделение организации. -*Политика безопасности* - раздел, в котором приведены вопросы, учитывающие организационные меры обеспечения информационной безопасности, т.е. аспекты, которые невозможно отобразить при построении модели информационной системы. -*Права доступа* – права пользователей при доступе к информации. чтение – право на чтение. запись – право на запись (модификацию). удаление – право на удаление.

- *Рабочая станция* - ресурс, содержащий ценную информацию, к которому возможен только локальный доступ. - *Расходы на информационную безопасность* – это затраты организации на обеспечение информационной безопасности, включающие затраты на приобретение систем защиты информации и управление ими, стоимость обучения персонала.

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

-*Риск* – это вероятный ущерб, который понесет организация при

реализации угроз информационной безопасности, зависящий от защищенности системы.

-*Риск после задания контрмер* – это значение риска, пересчитанного с учетом задания контрмер (закрытия уязвимостей).

- *Связи* - раздел, в котором определяются связи между объектами, занесенными в разделе "Моделирование системы". - *Сервер* - ресурс, содержащий ценную информацию, к которому возможен удаленный доступ.

- *Сетевая группа* – это группа, в которую входят физически взаимосвязанные ресурсы.

-*Твердая копия* - носитель, содержащий ценную информацию (CD, дискета, кассета, жесткий диск, бумажные документы и т.д.) - *Точка доступа* - коммутатор беспроводной связи.

-*Угроза* - действие, которое потенциально может привести к нарушению безопасности.

-*Удаленный доступ* – доступ к ресурсу, который осуществляется с использованием каналов связи (локальная сеть организации, телекоммуникационные сети и т.д.).

-*Ущерб по угрозе Доступность* - ущерб, который понесет организация при блокировании доступа к ценной информации (за один час).

-*Ущерб по угрозе Конфиденциальность* - ущерб, который понесет организация в случае несанкционированного раскрытия или перехвата ценной информации.

-*Ущерб по угрозе Целостность* - ущерб, который понесет организация при уничтожении или изменении ценной информации. - *Уязвимость* - слабое место в информационной системе, наличие которого может привести к нарушению безопасности путем реализации некоторой угрозы (отсутствие средства защиты ресурса, информации или рабочего места группы пользователей, а также доступ группы пользователей к информации).

-*Эффективность комплекса контрмер* – это оценка, насколько снизился уровень риска после задания комплекса контрмер по отношению к первоначальному уровню риска.

Варианты для алгоритма «Анализ модели информационных потоков» представлены в таблице 3.

Таблица 3. Варианты для алгоритма «Анализ модели информационных потоков»

	n=1	n=2

Отделы	ИВЦ Экономический отдел Бухгалтерия	Абонентский отдел Отдел связи
Сетевые группы	1 сервер и 15 компьютеров	1 сервер и 10 компьютеров
Ресурсы	Сервер, компьютеры	Сервер, компьютеры, CD-диск
Сетевые устройства	Коммутатор D-Link, концентратор	Маршрутизатор, коммутатор Creative
Виды информации	предложениях для клиентов; - информация о з/п; - бухгалтерская информация;	ия о ценовых - база данных абонентов; - данные об услугах; - информация по эксплуатации и ремонту оборудования;
Группы пользователей	- системный администратор; - экономисты; - бухгалтера;	- секретари; - инженер; - техник;
Бизнес процессы	- внедрение изменений; - подготовка и подписание договоров; - начисление з/п;	- обслуживание клиентов; - предоставление услуг абонентам; - контроль над оборудованием;
Вид доступа	- удаленный; - локальный; - локальный;	- локальный; - удаленный; - локальный;

Права - чтение, запись, - чтение; доступа удаление; - чтение, удаление; - чтение; - чтение;

n=3	n=4	n=5

Отдел продаж Бухгалтерия Отдел по приему товара	Конструкторский отдел Отдел кадров НИО	Отдел снабжения Отдел рекламы Профсоюз
1 сервер и 6 компьютеров	1 сервер, 15 компьютеров	1 сервер и 10 компьютеров
Сервер, компьютеры	Сервер, компьютеры	Сервер, компьютеры
Коммутатор, модем Nokia	Концентратор, коммутатор	Маршрутизатор, модем
- себестоимость продукции; - бухгалтерская информация; - информация о ценовых предложениях;	- информация о новых проектах; - штатное расписание; - информация о новых информационных технологиях;	- информация о заявках; - данные о продукции; - информация о работниках;
- менеджеры; - бухгалтер; - секретарь;	- инженера - конструкторы; - начальник ОК; - программисты;	- менеджеры; - администратор; - начальник профсоюза;
- обслуживание клиентов; - начисление з/п; - закупка товара;	- разработка конструкций; - прием новых сотрудников; - создание новых технологий;	- закупка товара; - создание рекламных лозунгов; - работа с сотрудниками;
- локальный; - удаленный; - локальный;	- удаленный; - локальный; - локальный;	- локальный; - локальный; - локальный;

~~- чтение, запись; - чтение, запись, - чтение, запись;~~
- чтение, запись, удаление; - чтение, запись; удаление; - чтение, запись; - чтение, - чтение; - чтение, запись; удаление.

	n=6	n=7
Отделы	ИВЦ Экономический отдел Бухгалтерия	Абонентский отдел Отдел связи
Сетевые группы	1 сервер и 15 компьютеров	1 сервер и 10 компьютеров
Ресурсы	Сервер, компьютеры	Сервер, компьютеры, CD-диск
Угрозы	-Вывод конфиденциальной информации на ресурс, доступный всем группам пользователей; -Не проведение части документов в назначенный срок; -Неверный ввод данных по причине невнимательности сотрудника;	-Утеря важных договоров, оставленных на подпись; -Несвоевременное оказание помощи абоненту при обрыве связи; -Допуск неконтролируемой работы системы в течение продолжительного времени;

~~Уязвимости -Несанкционированный -Затягивание процесса~~ доступ к заключения договора с конфиденциальной выгодной компанией информации; поставщиком;
-Накопление -Жалобы от абонентов непроверенных документов на плохую работу всей и риск неоплаченных компании;
ежемесячных счетов; -Возможный сбой и
-Ошибка в заполнении вероятность простоя документа и появление системы;
ошибок в ежемесячном

отчете;

n=8	n=9	n=0
Отдел продаж Бухгалтерия Отдел по приему товара	Конструкторский отдел снабженияОтдел кадро НИО	Отдел рекламы Профсоюз
1 сервер и 6 компьютеров	1 сервер, 15 компьютеров	1 сервер и 10 компьютеров
Сервер, компьютеры	Сервер, компьютеры	Сервер, компьютеры
-Невнимательное обслуживание клиентов; -Неверное начисление премии при расчете з/п; -Закупка не того вида товара, который был назначен на текущий период по плану;	-Допущение ряда неточностей при разработке конструкций; -Прием новых сотрудников недостаточно высокой квалификации; -Создание сопровождающей программы, не подходящей к данному виду технологического процесса;	- Закупка не того вида товара, который был назначен на текущий период по плану; -Создание рекламных лозунгов, охватывающих не все виды деятельности предприятия;

~~-Недовольство -Негативное влияние - Недостаток~~ клиентов и нежелание допустимых требуемого по обращения клиентов к неточностей на плану товара и данной компании; разработанную сбой в отлаженном -Перерасчет з/п и конструкцию; процессе задержание срока -Сотрудник не производства; выдачи денежных выполняет -Не точное средств; поставленную перед представление о
-Недостаток ним задачу; предприятии. требуемого по плану -
Задержание срока
товара и сбой в запуска тех-го
процессе производства; процесса;

n – номер последней цифры зачетки или номер бригады.

Список контрольных вопросов

1) Что представляет собой система ГРИФ и для чего она предназначена?

2) Как работает система ГРИФ?

3) Для чего нужен модуль управления рисками, который содержит система ГРИФ?

4) Дайте определение понятия «класс группы пользователей» и перечислите семь основных классов групп пользователей;

5) Что такое риск? Для чего нужно выявлять риски? 6) Какое действие необходимо выполнить для закрытия уязвимости?

7) Перечислите виды защищѐнности информации на ресурсе и дайте понятие каждого из них;

8) Кратко опишите алгоритм расчета рисков по угрозам конфиденциальность и целостность;

9) Кратко опишите алгоритм расчета рисков по угрозе доступность;

10) Кратко опишите алгоритм задания контрмер.

Список литературы

1. Тихонов В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты [текст]: учебное пособие / В. А. Тихонов, В. В. Райх. – М.: Гелиос АРВ, 2006. - 528 с.

2. Игнатьев В. А. Защита информации в корпоративных информационно-вычислительных сетях [Текст]: монография. - Старый Оскол: ТНТ, 2005. – 552 с.

3. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов / В.И. Аверченков. - 2-е изд., стереотип. - М.: ФЛИНТА, 2011. - 269 с. // Режим доступа – http://biblioclub.ru/index.php?page=book&id=93245

4. Зырянова Т. Ю. Управление информационными рисками: монография / Т. Ю.Зырянова, А. А. Захаров, Ю. И. Ялышев– Тюмень: Издательство Тюменского государственного университета, 2008. - 192 с.

5.