II. ИЗУЧЕНИЕ СИСТЕМЫ АНАЛИЗА РИСКОВ И ПРОВЕРКИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Основные определения

Безопасность (защищенность) информации в компьютерных системах (КС) - это такое состояние всех компонент КС, при котором обеспечивается защита информации от возможных угроз на требуемом уровне. Компьютерные системы, в которых обеспечивается безопасность информации, называются защищенными [1].

Информационная безопасность достигается проведением руководством соответствующего уровня *политики информационной безопасности***.** Основным документом, на основе которого проводится политика информационной безопасности, является *программа информационной безопасности***.** Этот документ разрабатывается и принимается как официальный руководящий документ высшими органами управления организацией. В документе приводятся цели политики информационной безопасности и основные направления решения задач защиты информации в КС. В программах информационной безопасности содержатся также общие требования и принципы построения систем защиты информации в КС.

Под *системой защиты информации в КС* понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности.

Угроза безопасности - потенциально возможное происшествие, которое может оказать воздействие на информацию в системе.

Уязвимость - некая неудачная характеристика системы, которая делает возможным возникновение угрозы.

Атака - действие по использованию уязвимости КС; атака - это реализация угрозы.

Угроза конфиденциальности - угроза раскрытия информации.

Угроза целостности - угроза изменения информации.

Угроза доступности - угроза нарушения работоспособности системы при доступе к информации.

Ущерб - стоимость потерь, которые понесет компания в случае реализации угроз конфиденциальности, целостности, доступности по каждому виду ценной информации. Ущерб зависит только от стоимости информации, которая обрабатывается в автоматизированной системе. Ущерб является характеристикой информационной системы и не зависит от ее защищенности.

Риск - вероятный ущерб, который зависит от защищенности системы. По определению риск всегда измеряется в деньгах.

В сущности, для коммерческой организации задача безопасного функционирования информационной системы сводится к выработке правил и выбору защитных средств. Комбинация двух этих составляющих позволит обеспечить необходимый уровень безопасности, как для ценных ресурсов организации, так и для всей информационной системы обработки этих ресурсов. Другими словами задача защиты – это разработка эффективной политики безопасности (или правил безопасности).

Чтобы меры политики безопасности по защите отвечали реальному состоянию дел необходимо знать - что, от кого и в какой степени нужно защищать. На сегодня существует только один процесс, способный в какой то мере дать ответы на поставленные вопросы, речь идет об анализе рисков.

1. Обзор программных продуктов в области анализа рисков и проверки организационных мер обеспечения информационной безопасности

В настоящее время имеется большое разнообразие как методов анализа и управления рисками, так и реализующих их программных средств. Приведем примеры некоторых отечественных продуктов.

1.1 Программный комплекс анализа и контроля рисков информационных систем компании – ГРИФ

Для проведения полного анализа информационных рисков прежде всего необходимо построить полную модель информационной системы с точки зрения ИБ. Для решения этой задачи ГРИФ, в отличие от представленных на рынке западных систем анализа рисков, которые громоздки, сложны в использовании и часто не предполагают самостоятельного применения ИТ-менеджерами и системными администраторами, ответственными за обеспечение безопасности информационных систем компаний, обладает простым и интуитивно понятным для пользователя интерфейсом. Однако за внешней простотой скрывается сложнейший алгоритм анализа рисков, учитывающий более ста параметров, который позволяет на выходе дать максимально точную оценку существующих в информационной системе рисков, основанную на глубоком анализе особенностей практической реализации информационной системы. Основная задача системы ГРИФ – дать возможность ИТ-менеджеру самостоятельно (без привлечения сторонних экспертов) оценить уровень рисков в информационной системе, оценить эффективность существующей практики по обеспечению безопасности компании и иметь возможность доказательно (в цифрах) убедить топ-менеджмент компании в необходимости инвестиций в сферу информационной безопасности компании [2].

1.1. На первом этапе система ГРИФ проводит опрос ИТ-менеджера с целью определения полного списка информационных ресурсов, представляющих ценность для компании.

1.2. На втором этапе проводится опрос ИТ-менеджера с целью ввода в систему ГРИФ всех видов информации, представляющей ценность для компании. Введенные группы ценной информации должны быть размещены пользователем на ранее указанных на предыдущем этапе объектах хранения информации (серверах, рабочих станциях и так далее). Заключительная фаза – указание ущерба по каждой группе ценной информации, расположенной на соответствующих ресурсах, по всем видам угроз.

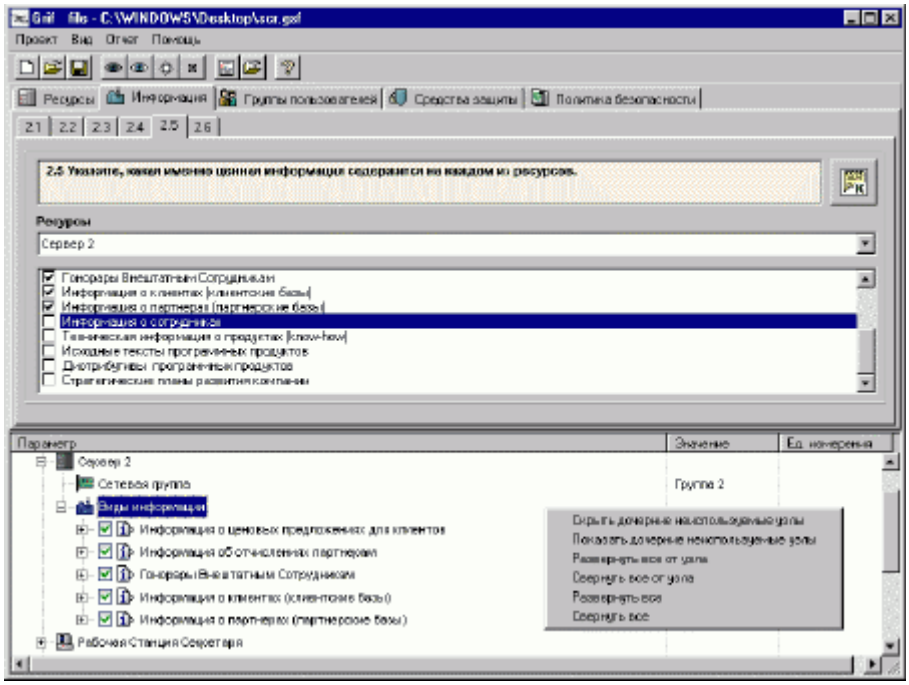

Рисунок.1.1. Интерфейс программного комплекса Гриф. Вкладка “Информация”.

1.3. На третьем этапе вначале проходит определение всех видов пользовательских групп (и число пользователей в каждой группе). Затем определяется, 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.
1.4. На четвертом этапе проводится опрос ИТ-менеджера для определения средств защиты информации, которыми защищена ценная информация 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.

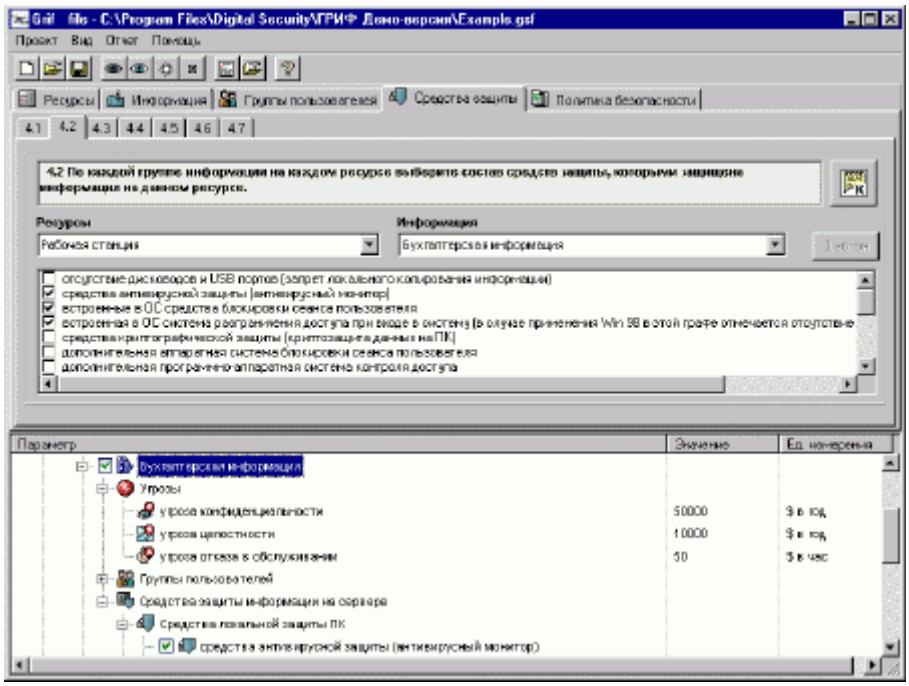

Рисунок.1.2. Интерфейс программного комплекса Гриф. Вкладка “Средства защиты”.

1.5. На завершающем этапе пользователь должен ответить на список вопросов по политике безопасности, реализованной в системе, что позволяет 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 так далее.

В результате выполнения всех действий по данным этапам на выходе сформирована 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.

1.6. Отчет по системе представляет собой подробный, дающий полную картину возможного ущерба от инцидентов документ, готовый для представления руководству компании.

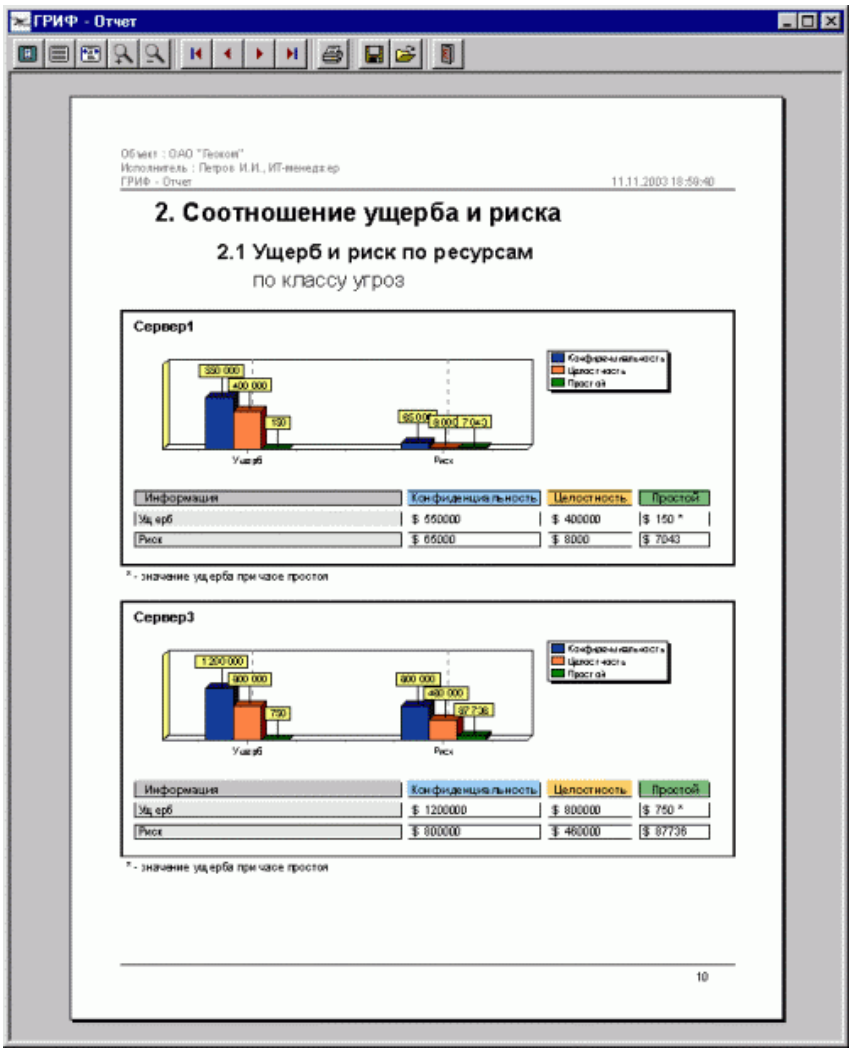

Рисунок.1.3. Интерфейс программного комплекса Гриф. Реализация отчета.

1.7. К недостаткам ГРИФ можно отнести следующее:

- отсутствует привязка к бизнес процессам (запланировано в следующей версии);
- нет возможности сравнения отчетов на разных этапах внедрения комплекса мер по обеспечению защищенности (запланировано в следующей версии);
- отсутствует возможность добавить специфичные для данной компании требования политики безопасности.

1.2. Программный комплекс управления политикой информационной безопасности компании - КОНДОР+

Российская компания Digital Security разработала программный продукт КОНДОР+, позволяющий специалистам (ИТ-менеджерам, офицерам безопасности) проверить политику информационной безопасности компании на соответствие требованиям международного стандарта безопасности ISO 17799.

Разработанный программный комплекс КОНДОР+ включает в себя более двухсот вопросов, ответив на которые, специалист получает подробный отчет о состоянии существующей политики безопасности, а так же модуль оценки уровня рисков соответствия требованиям ISO 17799 [3].

После регистрации пользователь получает возможность, выбрать соответствующий раздел стандарта ISO 17799 и ответить на вопросы.

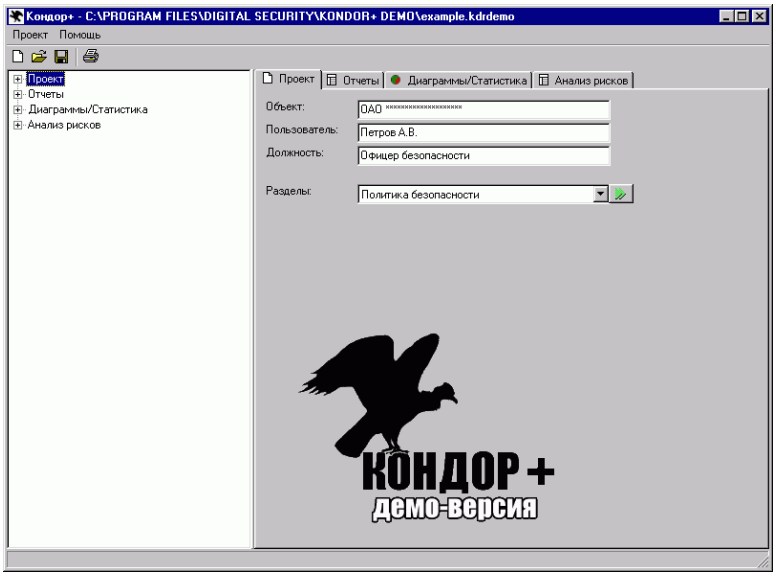

Рисунок.1.4. Интерфейс программного комплекса Кондор. Вкладка проект.

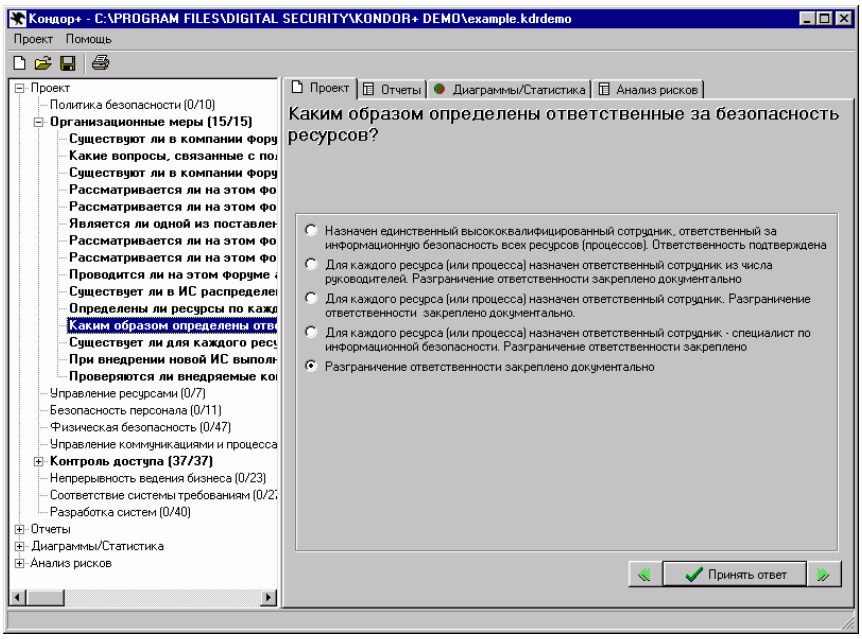

Рисунок.1.5. Интерфейс программного комплекса Кондор. Выбор раздела стандарта.

В отчете отражаются все положения политики безопасности, которые соответствуют стандарту и все, которые не соответствуют.

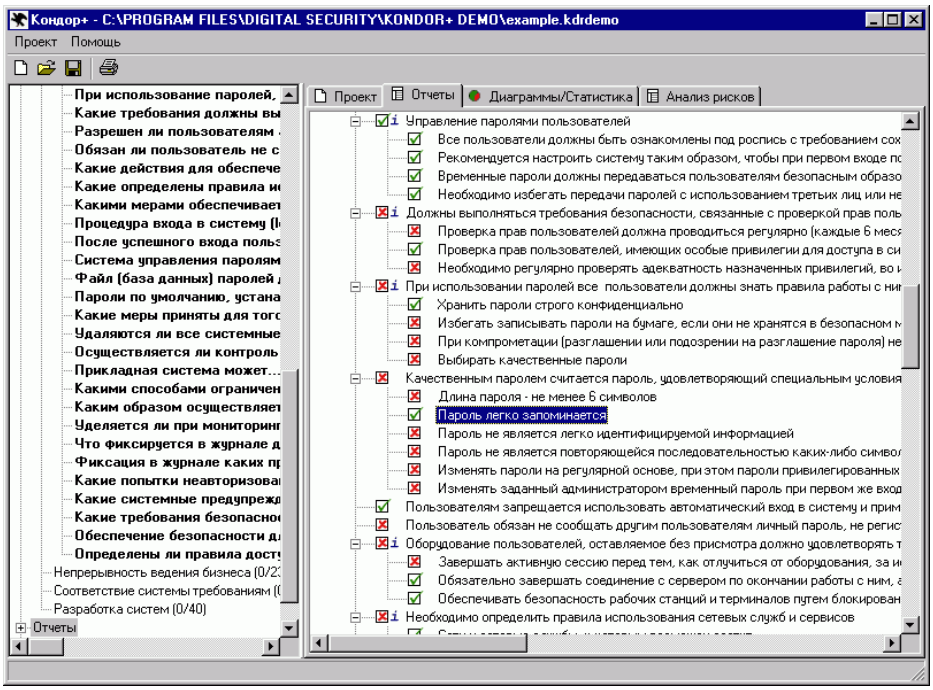

Рисунок.1.6. Интерфейс программного комплекса Кондор. Реализация отчета.

К наиболее важным элементам политики безопасности даются комментарии и рекомендации экспертов.

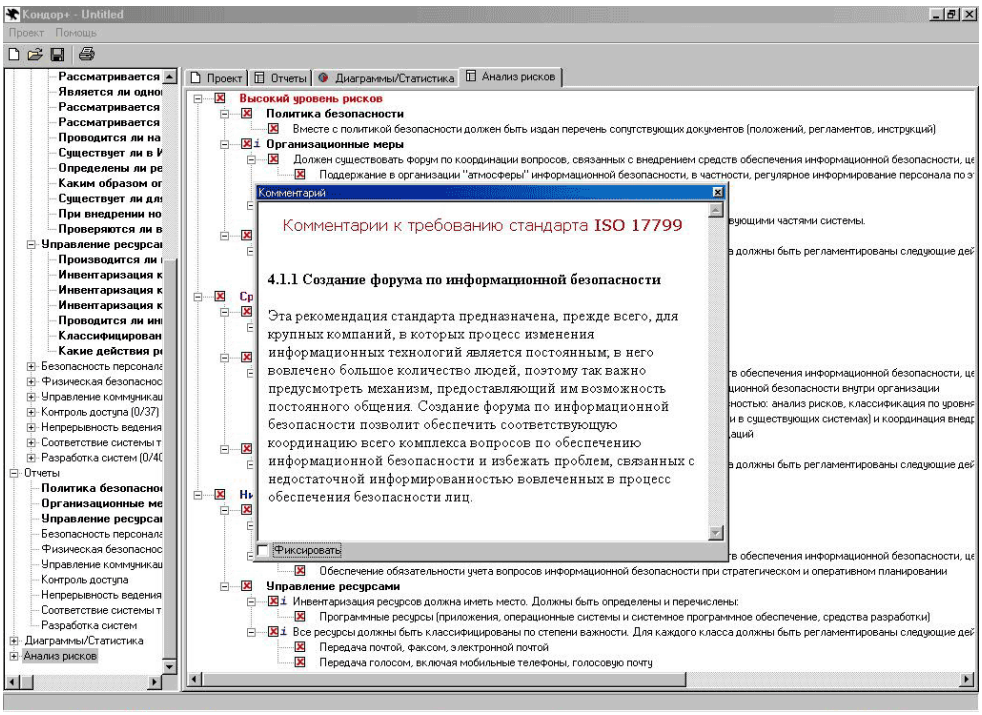

Рисунок.1.8. Интерфейс программного комплекса Кондор. Комментарии.

По желанию специалиста, работающего с программой, может быть выбрана генерация отчета, например, по какому-то одному или нескольким разделам стандарта ISO 17799, общий подробный отчет с комментариями, общий отчет о состоянии политики безопасности без комментариев для представления руководству и другие. Все варианты отчетов для большей наглядности сопровождаются диаграммами.

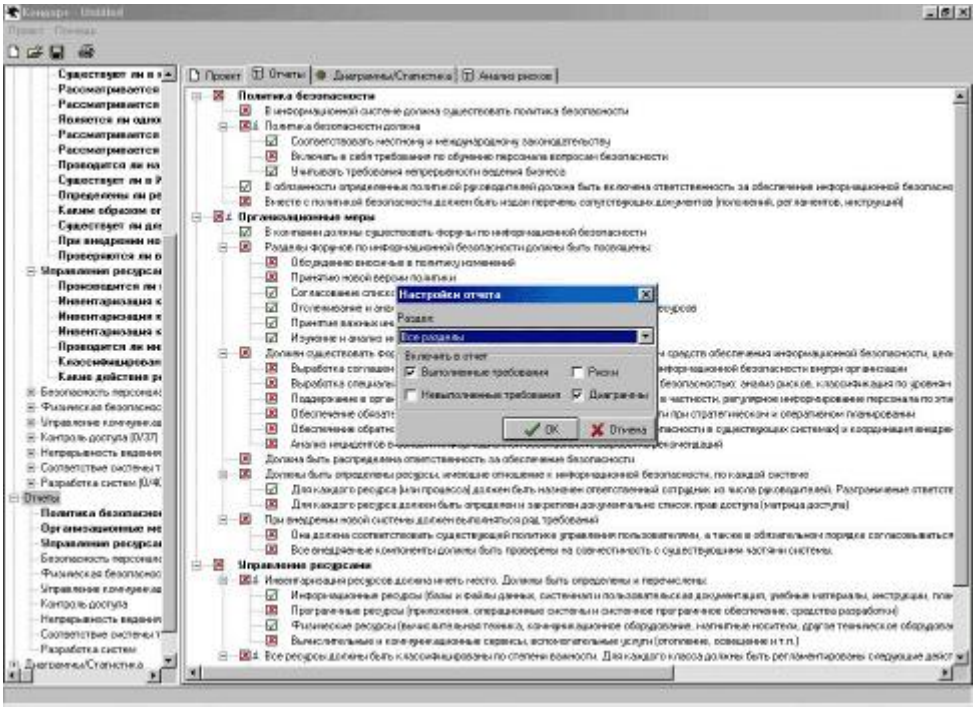

Рисунок.1.9. Интерфейс программного комплекса Кондор. Настройка отчета.

Кроме того, КОНДОР+ дает возможность специалисту отслеживать вносимые на основе выданных рекомендаций изменения в политику безопасности, постепенно приводя

ее в полное соответствие с требованиями стандарта, а также иметь возможность представлять отчеты руководству, свидетельствующие о целесообразности и обоснованности инвестиций в обеспечение безопасности информационной системы компании.

Стоимость продукта составляет 225 долл. (КОНДОР) и 345 долл. (КОНДОР+ с модулем анализа рисков базового уровня).

К недостаткам КОНДОР+ можно отнести:

- отсутствие возможности установки пользователем веса на каждое требование (запланировано в следующих версиях)
- отсутствие возможности внесения пользователем комментариев (запланировано в следующих версиях)

2. Описание системы (программного комплекса)

При разработке системы преследовались многие цели, одна из них заключалась в том, чтобы создать программный продукт, который будет способен ввести пользователя в «курс дела» не утаивая от него ни одного этапа анализа рисков.

Необходимо было разработать максимально простое в использовании программное решение, основная задача которого - дать возможность ИТ-менеджеру самостоятельно (без привлечения сторонних экспертов) оценить уровень рисков в информационной системе, оценить эффективность существующей практики по обеспечению безопасности компании и оптимизировать расходы и сформировать адекватный бюджет на информационную безопасность.

Система представляет интеграцию двух идей реализованных в системах Кондор и Гриф. В программном комплексе анализ рисков и политики безопасности информационной системы объединены в одном продукте. То есть данные, которые заносятся для анализа организационных мер, определяющих существующую политику безопасности компании, полностью используется при анализе рисков. Это означает что две составляющие управления информационной безопасностью - политика безопасности и анализ рисков - находятся в одном интегрированном решении. Кроме того, данный продукт может использоваться и в учебных целях как возможность изучить на практике методы и средства анализа рисков и проверки организационных мер обеспечивающих информационную безопасность. Благодаря значительно расширенной базе использованных положений стандарта ISO 17799 по сравнению с Кондором и Грифом в данной системе возможен более полный анализ организационных мер определяющих политику безопасности.

Известно, что существуют два подхода к анализу рисков - анализ рисков базового и полного уровня. В данной системе использованы сильные стороны разных методов, опирающихся на анализ рисков и на требования стандартов.

Но каким бы ни был подход, главная цель — формирование конкретных и применимых требований по безопасности к исследуемой информационной системе

В системе использован наиболее распространенный в настоящее время подход, основанный на учете различных факторов влияющих на уровни угроз и уязвимостей. Такой подход позволяет абстрагироваться от малосущественных технических деталей, учесть не только программно-технические, но и иные аспекты.

При работе система проводит анализ существующей политики безопасности на наличие так называемых дыр. Если их не устранять, то рано или поздно их обнаружат «плохие парни» и воспользуются для достижения своих, не всегда достойных целей.

В особенности отметим, что данная система позволяет также определить и экономическую эффективность системы информационной защиты.

Данный продукт окажет не заменимую помощь организациям, которые планируют получить сертификат на соответствие международному стандарту безопасности ISO 17799, так как при не выполнении каких либо требований, даются пояснения - как и что предпринять.

Ни для кого не секрет, что анализ информационных рисков является на сегодняшний день актуальной задачей для современного бизнеса - последние годы на каждой конференции по информационной безопасности в России можно услышать серьезные доклады на данную тему.

Анализ информационных рисков - это процесс комплексной оценки защищенности информационной системы с переходом к количественным или качественным показателям рисков. При этом риск - это вероятный ущерб, который зависит от защищенности системы. Под управлением рисками понимается процесс идентификации и уменьшения рисков, которые могут воздействовать на информационную систему. Результаты анализа используются при выборе средств защиты, оценке эффективности существующих и проектируемых систем защиты информации [3].

Итак, из определения следует, что на выходе алгоритма анализа риска можно получить либо количественную оценку рисков (риск измеряется в деньгах), либо - качественную (уровни риска; обычно: высокий, средний, низкий).

Кроме того, анализ рисков также отличается по используемому подходу; обычно условно выделяется анализ рисков базового и полного уровня. Для анализа рисков базового уровня достаточно проверить риск невыполнения требований общепринятого стандарта безопасности (обычно ISO 17799) с получением на выходе качественной оценки уровня рисков (высокий, средний, низкий).

Основное отличие полного анализа рисков от базового состоит в необходимости построения полной модели анализируемой информационной системы. Модель должна включать: виды ценной информации, объекты ее хранения; группы пользователей и виды доступа к информации; средства защиты (включая политику безопасности), виды угроз.

Далее после моделирования необходимо перейти к этапу анализа защищенности построенной полной модели информационной системы. И здесь мы попадаем в целый пласт теоретических и практических проблем, с которыми сталкиваются разработчики алгоритмов анализа риска полного уровня. Прежде всего, как алгоритмически (без эксперта) оценить защищенность информационной системы (заметим, что речь не идет о сканировании конкретных уязвимостей в конкретном применяемом программном обеспечении)? Следующая проблема - как алгоритмически определить все классы уязвимостей в системе защиты анализируемой системы? Как оценить ущерб от всех существующих в системе угроз безопасности и как добиться адекватной оценки совокупного ущерба по всем классам угроз (необходимо избежать избыточного суммирования ущербов)? И самая сложная проблема: риск категория вероятностная - как оценить вероятность реализации множества угроз информационной системы?

Весь вышеуказанный комплекс проблем необходимо решить при создании алгоритма.

Конечно, можно предложить пользователю самостоятельно ввести вероятность реализации угроз или оценить ее уровень, как в алгоритме RiskWatch. Но тогда мы сведем на нет весь процесс анализа.

При подсчете вероятности реализации тех или иных угроз можно опереться на некоторые статистические данные [5].

Таблица 2.1 Угрозы информационной безопасности

Угрозы	Вероятность проявления
Небрежность	0,188
Пиратство	0,166
Нарушение целостности	0,159
Утечка данных	0,159
"Шутки" над коллегами	0,150
Наблюдение за излучением	0,133
Умышленные повреждения данных и программ	0,129
Нарушение аутентификации	0,129
Перегрузка	0,119
Неправильная маршрутизация	0,106
Аппаратные сбои	0,090
Искажение	0,080
Сетевые анализаторы	0,074
Мошенничество	0,058
Пожары и другие стихийные бедствия	0,043
Подлог	0,033
"Логические бомбы"	0,032
Кража	0,032
Блокирование информации	0,016
"Потайные ходы и лазейки"	0,010

Но так как риск - это вероятный ущерб, который зависит от защищенности системы, то полученные данные будут не точными.

Из-за того что на оценку защищенности информационной системы существенным образом влияют организационные аспекты, то при анализе существующей защиты будем опираться на вопросник.

Так как на один и тот же вид информации может быть направлено сразу несколько угроз, то необходимо будет учесть так же и суммарный ущерб.

Необходимо смоделировать доступы всех групп пользователей ко всем видам информации и в зависимости от вида доступа и вида ресурса рассматривать конечное множество очевидных элементарных ситуаций, где начальную вероятность реализации угрозы можно определить достаточно просто и точно.

Далее анализируется множество опять же элементарных факторов (идет анализ комплексной защищенности объекта из вопросника) - которые так или иначе влияют на защищенность, а затем делается вывод об итоговых рисках.

2. 1. Определение источника угроз.

В любой методике управления рисками необходимо идентифицировать риски, как вариант – их составляющие (угрозы и уязвимости).

Целью создания любой КС является удовлетворение потребностей пользователей в своевременном получении достоверной информации и сохранении ее конфиденциальности (при необходимости). Информация является конечным «продуктом потребления» в КС и выступает в виде центральной компоненты системы. Безопасность информации на уровне КС обеспечивают такие компоненты системы как технические, программные средства, обслуживающий персонал и пользователи. Причем эта задача должна решаться путем защиты от внешних и внутренних неразрешенных (несанкционированных) воздействий. Особенности взаимодействия компонент заключаются в

следующем. Внешние воздействия чаше всего оказывают несанкционированное влияние на информацию путем воздействия на другие компоненты системы. Следующей особенностью является возможность несанкционированных действий, вызываемых внутренними причинами, в отношении информации со стороны технических, программных средств, обслуживающего, персонала и пользователей. В этом заключается основное противоречие взаимодействия этих компонент с информацией. Причем, обслуживающий персонал и пользователи могут сознательно осуществлять попытки несанкционированного воздействия на информацию. Таким образом, обеспечение безопасности информации в КС должно предусматривать защиту всех компонент от внешних и внутренних воздействий (угроз) [4].

Под **угрозой безопасности информации** понимается потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации.

Все множество потенциальных угроз безопасности информации в КС может быть разделено на два класса (рис 2.1).

Рисунок. 2.1. Угрозы безопасности информации в компьютерных системах

Случайные угрозы

Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называют *случайными* или *непреднамеренными***.**

Реализация угроз этого класса приводит к наибольшим потерям информации (по статистическим данным - до 80% от ущерба, наносимого информационным ресурсам КС любыми угрозами). При этом могут происходить уничтожение, нарушение целостности и доступности информации. Реже нарушается конфиденциальность информации, однако при этом создаются предпосылки для злоумышленного воздействия на информацию.

Стихийные бедствия и аварии чреваты наиболее разрушительными последствиями для КС, т.к. последние подвергаются физическому разрушению, информация утрачивается или доступ к ней становится невозможен.

Сбои и отказы сложных систем неизбежны. В результате сбоев и отказов нарушается работоспособность технических средств, уничтожаются и искажаются данные и программы, нарушается алгоритм работы устройств. Нарушения алгоритмов работы от дельных узлов и устройств могут также привести к нарушению конфиденциальности информации. Например, сбои и отказы средств выдачи информации могут привести к несанкционированному доступу к информации путем несанкционированной ее выдачи в канал связи, на печатающее устройство и т. п.

Ошибки при разработке КС, алгоритмические и программные ошибки приводят к последствиям, аналогичным последствиям сбоев и отказов технических средств. Кроме того, такие ошибки могут быть использованы злоумышленниками для воздействия на ресурсы КС. Особую опасность представляют ошибки в операционных системах (ОС) и в программных средствах защиты информации.

Согласно данным Национального Института Стандартов и Технологий США (NIST) 65% случаев нарушения безопасности информации происходит в результате *ошибок пользователей и обслуживающего персонала.* Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками приводят к уничтожению, нарушению целостности и конфиденциальности информации, а также компрометации механизмов защиты.

Характеризуя угрозы информации в КС, не связанные с преднамеренными действиями, в целом, следует отметить, что механизм их реализации изучен достаточно хорошо, накоплен значительный опыт противодействия этим угрозам. Современная технология разработки технических и программных средств, эффективная система эксплуатации КС, включающая обязательное резервирование информации, позволяют значительно снизить потери от реализации угроз этого класса.

Преднамеренные угрозы

Второй класс угроз безопасности информации в КС составляют преднамеренно создаваемые угрозы.

Данный класс угроз изучен недостаточно, очень динамичен и постоянно пополняется новыми угрозами. Угрозы этого класса в соответствии с их физической сущностью и механизмами реализации могут быть распределены по пяти группам:

- традиционный или универсальный шпионаж и диверсии;
- несанкционированный доступ к информации;
- электромагнитные излучения и наводки;
- модификация структур КС;
- вредительские программы.

Традиционный шпионаж и диверсии

В качестве источников нежелательного воздействия на информационные ресурсы по-прежнему актуальны методы и средства шпионажа и диверсий**,** которые использовались и используются для добывания или уничтожения информации на объектах, не имеющих КС. Эти методы также действенны и эффективны в условиях применения компьютерных систем. Чаще всего они используются для получения сведений о системе защиты с целью проникновения в КС, а также для хищения и уничтожения информационных ресурсов.

К методам шпионажа и диверсий относятся:

- подслушивание;
- визуальное наблюдение;
- хищение документов и машинных носителей информации;
- хищение программ и атрибутов системы защиты;

- подкуп и шантаж сотрудников;
- сбор и анализ отходов машинных носителей информации;
- поджоги;
- взрывы.

Для *подслушивания* злоумышленнику не обязательно проникать на объект. Современные средства позволяют подслушивать разговоры с расстояния нескольких сотен метров. Так прошла испытания система подслушивания, позволяющая с расстояния 1 км фиксировать разговор в помещении с закрытыми окнами. В городских условиях дальность действия устройства сокращается до сотен и десятков метров в зависимости от уровня фонового шума. Принцип действия таких устройств основан на анализе отраженного луча лазера от стекла окна помещения, которое колеблется от звуковых волн. Колебания оконных стекол от акустических волн в помещении могут сниматься и передаваться на расстояния с помощью специальных устройств, укрепленных на оконном стекле. Такие устройства преобразуют механические колебания стекол в электрический сигнал с последующей передачей его по радиоканалу. Вне помещений подслушивание ведется с помощью сверхчувствительных направленных микрофонов. Реальное расстояние подслушивания с помощью направленных микрофонов составляет 50-100 метров.

Разговоры в соседних помещениях, за стенами зданий могут контролироваться с помощью стетоскопных микрофонов. Стетоскопы преобразуют акустические колебания в электрические. Такие микрофоны позволяют прослушивать разговоры при толщине стен до 50-100 см. Съем информации может осуществляться также и со стекол, металлоконструкций зданий, труб водоснабжения и отопления.

Аудиоинформация может быть получена также путем высокочастотного навязывания. Суть этого метода заключается в воздействии высокочастотным электромагнитным полем или электрическими сигналами на элементы, способные модулировать эти поля, или сигналы электрическими или акустическими сигналами с речевой информацией. В качестве таких элементов могут использоваться различные полости с электропроводной поверхностью, представляющей собой высокочастотный контур с распределенными параметрами, которые меняются под действием акустических волн. При совпадении частоты такого контура с частотой высокочастотного навязывания и при наличии воздействия акустических волн на поверхность полости контур переизлучает и модулирует внешнее поле (высокочастотный электрический сигнал). Чаще всего этот метод прослушивания реализуется с помощью телефонной линии. При этом в качестве модулирующего элемента используется телефонный аппарат, на который по телефонным проводам подается высокочастотный электрический сигнал. Нелинейные элементы телефонного аппарата под воздействием речевого сигнала модулируют высокочастотный сигнал. Модулированный высокочастотный сигнал может быть демодулирован в приемнике злоумышленника.

Одним из возможных каналов утечки звуковой информации может быть прослушивание переговоров, ведущихся с помощью средств связи. Контролироваться могут как проводные каналы связи, так и радиоканалы. Прослушивание переговоров по проводным и радиоканалам не требует дорогостоящего оборудования и высокой квалификации злоумышленника.

Дистанционная видеоразведка для получения информации в КС малопригодна и носит, как правило, вспомогательный характер.

Видеоразведка организуется в основном для выявления режимов работы и расположения механизмов защиты информации. Из КС информация реально может быть получена при использовании на объекте экранов, табло, плакатов, если имеются прозрачные окна и перечисленные выше средства размещены без учета необходимости противодействовать такой угрозе.

Видеоразведка может вестись с использованием технических средств, таких как оптические приборы, фото-, кино- и телеаппаратура. Многие из этих средств допускают консервацию (запоминание) видеоинформации, а также передачу ее на определенные расстояния.

В прессе появились сообщения о создании в США мобильного микроробота для ведения дистанционной разведки. Пьезокерамический робот размером около 7 см и массой 60 г способен самостоятельно передвигаться со скоростью 30 см/с в течение 45 мин. За это время «микроразведчик» способен преодолеть расстояние в 810 метров, осуществляя транспортировку 28 г полезного груза (для сравнения - коммерческая микровидеокамера весит 15 г).

Для вербовки сотрудников и физического уничтожения объектов КС также не обязательно иметь непосредственный доступ на объект. Злоумышленник, имеющий доступ на объект КС, может использовать любой из методов традиционного шпионажа.

Злоумышленниками, имеющими доступ на объект, могут использоваться миниатюрные средства фотографирования, видео - и аудиозаписи. Для аудио- и видеоконтроля помещений и при отсутствии в них злоумышленника могут использоваться закладные устройства или «жучки». Для объектов КС наиболее вероятными являются закладные устройства, обеспечивающие прослушивание помещений. Закладные устройства делятся на проводные и излучающие. Проводные закладные устройства требуют значительного времени на установку и имеют существенный демаскирующий признак - провода. Излучающие «закладки» («радиозакладки») быстро устанавливаются, но также имеют демаскирующий при знак - излучение в радио или оптическом диапазоне. «Радиозакладки» могут использовать в качестве источника электрические сигналы или акустические сигналы. Примером использования электрических сигналов в качестве источника является применение сигналов внутренней телефонной, громкоговорящей связи. Наибольшее распространение получили акустические «радиозакладки». Они воспринимают акустический сигнал, преобразуют его в электрический и передают в виде радиосигнала на дальность до 8 км. Из применяемых на практике «радиозакладок» подавляющее большинство (около 90%) рассчитаны на работу в диапазоне расстояний 50 - 800 метров.

Для некоторых объектов КС существует *угроза вооруженного нападения террористических или диверсионных групп.* При этом могут быть применены средства огневого поражения.

Несанкционированный доступ к информации

Термин «несанкционированный доступ к информации» (НСДИ) определен как доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств вычислительной техники или автоматизированных систем.

Под правилами разграничения доступа понимается совокупность положений, регламентирующих права доступа лиц или процессов (субъектов доступа) к единицам информации (объектам доступа).

Право доступа к ресурсам КС определяется руководством для каждого сотрудника в соответствии с его функциональными обязанностями. Процессы инициируются в КС в интересах определенных лиц, поэтому и на них накладываются ограничения по доступу к ресурсам.

Выполнение установленных правил разграничения доступа в КС реализуется за счет создания системы разграничения доступа (СРД).

Несанкционированный доступ к информации возможен только с использованием штатных аппаратных и программных средств в следующих случаях:

- отсутствует система разграничения доступа;
- сбой или отказ в КС;

- ошибочные действия пользователей или обслуживающего персонала компьютерных систем;
- ошибки в СРД;
- фальсификация полномочий.

Если СРД отсутствует, то злоумышленник, имеющий навыки работы в КС, может получить без ограничений доступ к любой информации. В результате сбоев или отказов средств КС, а также ошибочных действий обслуживающего персонала и пользователей возможны состояния системы, при которых упрощается НСДИ. Злоумышленник может выявить ошибки в СРД и использовать их для НСДИ. Фальсификация полномочий является одним из наиболее вероятных путей (каналов) НСДИ.

Электромагнитные излучения и наводки

Процесс обработки и передачи информации техническими средствами КС сопровождается электромагнитными излучениями в окружающее пространство и наведением электрических сигналов в линиях связи, сигнализации, заземлении и других проводниках. Они получили названия *побочных электромагнитных излучений и наводок (ПЭМИН).* С помощью специального оборудования сигналы принимаются, выделяются, усиливаются и могут либо просматриваться, либо записываться в запоминающих устройствах. Наибольший уровень электромагнитного излучения в КС присущ работающим устройствам отображения информации на электронно-лучевых трубках. Содержание экрана такого устройства может просматриваться с помощью обычного телевизионного приемника, дополненного несложной схемой, основной функцией которой является синхронизация сигналов. Дальность удовлетворительного приема таких сигналов при использовании дипольной антенны составляет 50 метров. Использование направленной антенны приемника позволяет увеличить зону уверенного приема сигналов до 1 км. Восстановление данных возможно также путем анализа сигналов излучения неэкранированного электрического кабеля на расстоянии до 300 метров.

Наведенные в проводниках электрические сигналы могут выделяться и фиксироваться с помощью оборудования, подключаемого к этим проводникам на расстоянии в сотни метров от источника сигналов. Для добывания информации злоумышленник может использовать также «просачивание» информационных сигналов в цепи электропитания технических средств КС.

«Просачивание» информационных сигналов в цепи электропитания возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором выпрямительного устройства. «Просачивание» также возможно за счет падения напряжения на внутреннем сопротивлении источника питания при прохождении токов усиливаемых информационных сигналов. Если затухание в фильтре выпрямительного устройства недостаточно, то информационные сигналы могут быть обнаружены в цепи питания. Информационный сигнал может быть выделен в цепи питания за счет зависимости значений потребляемого тока в оконечных каскадах усилителей (информационные сигналы) и значений токов в выпрямителях, а значит и в выходных цепях.

Электромагнитные излучения используются злоумышленниками не только для получения информации, но и для ее уничтожения. Электромагнитные импульсы способны уничтожить информацию на магнитных носителях. Мощные электромагнитные и сверхвысокочастотные излучения могут вывести из строя электронные блоки КС. Причем для уничтожения информации на магнитных носителях с расстояния нескольких десятков метров может быть использовано устройство, помещающееся в портфель.

Несанкционированная модификация структур

Большую угрозу безопасности информации в КС представляет *несанкционированная модификация алгоритмической, программной и технической структур системы***.** Несанкционированная модификация структур может осуществляться на любом жизненном цикле КС. Несанкционированное изменение структуры КС на этапах разработки и модернизации получило название «закладка». В процессе разработки КС «закладки» внедряются, как правило, в специализированные системы, предназначенные для эксплуатации в какой-либо фирме или государственных учреждениях. В универсальные КС «закладки» внедряются реже, в основном для дискредитации таких систем конкурентом или на государственном уровне, если предполагаются поставки КС во враждебное государство. «Закладки», внедренные на этапе разработки, сложно выявить ввиду высокой квалификации их авторов и сложности современных КС.

Алгоритмические, программные и аппаратные «закладки» используются либо для непосредственного вредительского воздействия на КС, либо для обеспечения неконтролируемого входа в систему. Вредительские воздействия «закладок» на КС осуществляются при получении соответствующей команды извне (в основном характерно для аппаратных «закладок») и при наступлении определенных событий в системе. Такими событиями могут быть: переход на определенный режим работы (например, боевой режим системы управления оружием или режим устранения аварийной ситуации на атомной электростанции т. п.), наступление установленной даты, достижение определенной наработки и т. д.

Программные и аппаратные «закладки» для осуществления неконтролируемого входа в программы, использование привилегированных режимов работы (например, режимов операционной системы), обхода средств защиты информации получили название «люки».

Вредительские программы

Одним из основных источников угроз безопасности информации в КС является использование специальных программ, получивших общее название «вредительские программы».

В зависимости от механизма действия вредительские программы делятся на четыре класса:

- «логические бомбы»;
- «черви»;
- «троянские кони»;
- «компьютерные вирусы».

«Логические бомбы» - это программы или их части, постоянно находящиеся в ЭВМ или вычислительных системах (ВС) и выполняемые только при соблюдении определенных условий. Примерами таких условий могут быть: наступление заданной даты, переход КС в определенный режим работы, наступление некоторых событий установленное число раз и т.п.

«Червями» называются программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в ВС или сети и самовоспроизводить копии. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и, в конечном итоге, к блокировке системы.

«Троянские кони» - это программы, полученные путем явного изменения или добавления команд в пользовательские программы. При последующем выполнении пользовательских программ наряду с заданными функциями выполняются несанкционированные, измененные или какие-то новые функции.

«Компьютерные вирусы» - это небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путем создания своих копий, а при выполнении определенных условий оказывают негативное воздействие на КС.

Поскольку вирусам присущи свойства всех классов вредительских программ, то в последнее время любые вредительские программы часто называют вирусами.

Классификация злоумышленников

Возможности осуществления вредительских воздействий в большой степени зависят от статуса злоумышленника по отношению к КС. Злоумышленником может быть:

- разработчик КС;
- сотрудник из числа обслуживающего персонала;
- пользователь;
- постороннее лицо.

Разработчик владеет наиболее полной информацией о программных и аппаратных средствах КС и имеет возможность внедрения "закладок" на этапах создания и модернизации систем. Но он, как правило, не получает непосредственного доступа на эксплуатируемые объекты КС. Пользователь имеет общее представление о структурах КС, о работе механизмов защиты информации. Он может осуществлять сбор данных о системе защиты информации методами традиционного шпионажа, а также предпринимать попытки несанкционированного доступа к информации. Возможности внедрения закладок пользователями очень ограничены. Постороннее лицо, не имеющее отношения к КС, находится в наименее выгодном положении по отношению к другим злоумышленникам. Если предположить, что он не имеет доступ на объект КС, то в его распоряжении имеются дистанционные методы традиционного шпионажа и возможность диверсионной деятельности. Он может осуществлять вредительские воздействия с использованием электромагнитных излучений и наводок, а также каналов связи, если КС является распределенной.

Большие возможности оказания вредительских воздействий на информацию КС имеют специалисты, обслуживающие эти системы. Причем, специалисты разных подразделений обладают различными потенциальными возможностями злоумышленных действий. Наибольший вред могут нанести работники службы безопасности информации. Далее идут системные программисты, прикладные программисты и инженерно-технический персонал.

На практике опасность злоумышленника зависит также от финансовых, материально-технических возможностей и квалификации злоумышленника.

2.2.Примеры методик анализа рисков

Концепции анализа рисков, управления рисками на всех стадиях жизненного цикла информационной технологии были предложены многими крупными организациями, занимающимися проблемами информационной безопасности. Отечественные аналитики начали использовать различные методики на практике. Несколькими российскими организациями были разработаны собственные методики анализа и управления рисками, разработано собственное программное обеспечение, которое, наряду с зарубежным, имеется на отечественном рынке [3].

Оценка рисков

Для измерения какого-либо свойства необходимо выбрать шкалу. Шкалы могут быть разной «силы», выбор той или иной шкалы зависит как от свойств измеряемой величины, так и от имеющихся в наличии измерительных инструментов.

В качестве примера рассмотрим варианты выбора шкалы для измерения характеристического свойства «ценность информационного ресурса». Она может измеряться опосредованно в шкалах отношений, таких как стоимость восстановления ресурса, время восстановления ресурса и других. Другой вариант — определить ранговую шкалу для получения экспертной оценки, имеющую, например, три возможных значения лингвистической переменной:

1) Малоценный информационный ресурс - от него не зависят критически важные задачи, и он может быть восстановлен с небольшими затратами времени и денег;

2) Ресурс средней ценности - от него зависит ряд важных задач, но в случае его утраты он может быть восстановлен за время менее, чем критически допустимое, стоимость восстановления высокая;

3) Ценный ресурс: от него зависят критически важные задачи, в случае утраты время восстановления превышает критически допустимое, либо стоимость чрезвычайно высока.

Для измерения рисков не существует абсолютной шкалы. Риски можно оценивать по объективным либо субъективным критериям. Примером объективного критерия является вероятность выхода из строя какого-либо оборудования, например ПК за определенный промежуток времени. Примером субъективного критерия является оценка администратора информационного ресурса риска выхода из строя ПК. Для этого обычно разрабатывается ранговая шкала с несколькими градациями, например: низкий, средний, высокий уровни.

Существует ряд подходов к измерению рисков. Рассмотрим наиболее распространенные: оценка по двум факторам и оценка по трем факторам.

Оценка рисков по двум факторам.

В простейшем случае используется оценка двух факторов: вероятность происшествия и тяжесть возможных последствий. Обычно считается, что риск тем больше, чем больше вероятность происшествия и тяжесть последствий. Общая идея может быть выражена формулой:

$$\text{РИСК} = P_{\text{происшествия}} \times \text{ЦЕНА ПОТЕРИ} \qquad (2.1.)$$

Если переменные являются количественными величинами, риск — это оценка математического ожидания потерь.

Если переменные являются качественными величинами - то операция умножения не определена. Таким образом, в явном виде эта формула использоваться не должна.
Рассмотрим вариант использования качественных величин (наиболее часто встречающаяся ситуация).

Сначала должны быть определены значения лингвистической переменной вероятности событий, например такой шкалы:

- A - событие практически никогда не происходит;
- B - событие случается редко;
- C - вероятность события за рассматриваемый промежуток времени — около 0,5;
- B - скорее всего, событие произойдет;
- E - событие почти обязательно произойдет.

Кроме того, определяется лингвистическая переменная; серьезности происшествий, например:

N (Negligible) — воздействием можно пренебречь.

Mi (Minor) — незначительное происшествие - последствия легко устранимы, затраты на ликвидацию последствий невелики, воздействие на информационную технологию незначительно;

Mo (Moderate) — происшествие с умеренными результатами - ликвидация последствий не связана с крупными затратами, воздействие на информационную технологию невелико и не затрагивает критически важные задачи;

S (Serious) — происшествие с серьезными последствиями: ликвидация последствий связана со значительными затратами, воздействие на информационные технологии ощутимо, воздействует на выполнение критически важных задач;

C (Critical) — происшествие приводит к невозможности решения критически важных задач.

Для оценки рисков определяется переменная из трех значений: низкий риск, средний риск, высокий риск.

Риск, связанный с определенным событием, зависит от двух факторов и может быть определен как показано в таблице 2.2.

Шкалы факторов риска и сама таблица могут быть определены иначе, иметь другое число градаций.

Таблица.2.2. Определение риска в зависимости от двух факторов

	Negligible	Minor	Moderate	Serious	Critical
A	Низкий риск	Низкий риск	Низкий риск	Средний риск	Средний риск
B	Низкий риск	Низкий риск	Средний риск	Средний риск	Высокий риск
C	Низкий риск	Средний риск	Средний риск	Средний риск	Высокий риск
D	Средний риск	Средний риск	Средний риск	Средний риск	Высокий риск
E	Средний риск	Высокий риск	Высокий риск	Высокий риск	Высокий риск

Подобный подход к оценке рисков достаточно распространен. При разработке (использовании) методик оценки рисков необходимо учитывать следующие особенности:

- значения шкал должны быть четко определены (словесное описание) и пониматься одинаково всеми участниками процедуры экспертной оценки;
- требуются обоснования выбранной таблицы. Необходимо убедиться, что разные инциденты, характеризующиеся одинаковыми сочетаниями факторов риска, имеют с точки зрения экспертов одинаковый уровень рисков.

Подобные методики широко применяются при проведении анализа рисков базового уровня.

Оценка рисков по трем факторам.

В большинстве методик, рассчитанных на более высокие требования, чем базовый уровень, используется модель оценки риска с тремя факторами: угроза, уязвимость, цена потери. Угроза и уязвимость определяются следующим образом.

Угроза — совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации.

Уязвимость — слабость в системе защиты, которая делает возможным реализацию угрозы.

Цена потери — это качественная или количественная оценка степени серьезности происшествия.

Вероятность происшествия, которая в данном подходе может быть объективной либо субъективной величиной, зависит от уровней (вероятностей) угроз и уязвимостей:

$$P_{\text{происшествия}} = P_{\text{угрозы}} \times P_{\text{уязвимости}} \qquad (2.2.)$$

Соответственно, риск определяется следующим образом:

$$\text{РИСК} = P_{\text{угрозы}} \times P_{\text{уязвимости}} \times \text{ЦЕНА ПОТЕРИ} \qquad (2.3.)$$

Данное выражение можно рассматривать как математическую формулу, если используются количественные шкалы, либо как формулировку общей идеи, если хотя бы одна из шкал - качественная. В последнем случае используются различного рода табличные методы для определения риска в зависимости от трех факторов.

Например, показатель риска измеряется в шкале от 0 до 8 со следующими определениями уровней риска:

1) Риск практически отсутствует. Теоретически возможны ситуации, при которых событие наступает, но на практике это случается редко, а потенциальный ущерб сравнительно невелик:

2) Риск очень мал. События подобного рода случались достаточно редко, кроме того, негативные последствия сравнительно невелики;

. . .

8) Риск очень велик. Событие, скорее всего, наступит, и последствия будут чрезвычайно тяжелыми.

Матрица может быть определена следующим образом (табл.2.3). В данной таблице уровни уязвимости Н, С, В означают соответственно низкий, средний и высокий уровни.

Подобные таблицы используются как в «бумажных» вариантах методик оценки рисков, так и в различного рода инструментальных средствах анализа рисков.

Таблица.2.3. Определение риска в зависимости от трех факторов

Степень серьезности происшествия (цена потери)	Уровень угрозы								
	Низкий			Средний			Высокий		
	Уровни уязвимостей			Уровни уязвимостей			Уровни уязвимостей		
	Н	С	В	Н	С	В	Н	С	В
Незначительная	0	1	2	1	2	3	2	3	4
Несущественная	1	2	3	2	3	4	3	4	5
Умеренная	2	3	4	3	4	5	4	5	6
Серьезная	3	4	5	4	5	6	5	6	7
Критическая	4	5	6	5	6	7	6	7	8

Практические сложности в реализации этого подхода следующие.

Во-первых, должен быть собран весьма обширный материал о происшествиях в этой области.

Во-вторых, применение этого подхода оправдано далеко не всегда. Если информационная система достаточно крупная (содержит много элементов, расположена на обширной территории), имеет давнюю историю, то подобный подход, скорее всего, применим. Если система сравнительно невелика, использует новейшие элементы технологии (для которых пока нет достоверной статистики), оценки угроз и уязвимостей могут оказаться недостоверными.

2.3. Выбор методики анализа рисков

Как уже упоминалась выше для оценки угроз и уязвимостей используются различные методы, в основе которых могут лежать [6]:

- Экспертные оценки.
- Статистические данные.
- Учет факторов, влияющих на уровни угроз и уязвимостей.

Мы же, выбрали наиболее распространенный в настоящее время подход, основанный на учете различных факторов, влияющих на уровни угроз и уязвимостей. Такой подход позволяет абстрагироваться от малосущественных технических деталей, учесть не только программно-технические, но и иные аспекты.

Нам необходимо оценит следующие вероятности:

вероятность уровня(степени) угрозы и вероятность уровня уязвимости .

Для оценки угроз выберем следующие косвенные факторы:

- Статистика по зарегистрированным инцидентам.
- Тенденции в статистке по подобным нарушениям.
- Наличие в системе информации, представляющей интерес для потенциальных внутренних или внешних нарушителей.
- Моральные качества персонала.
- Возможность извлечь выгоду из изменения обрабатываемой в системе информации.
- Наличие альтернативных способов доступа к информации.

Для оценки уязвимостей выберем следующие косвенные факторы:

- Количество рабочих мест (пользователей) в системе.
- Размер рабочих групп.
- Осведомленность руководства о действиях сотрудников (разные аспекты).
- Характер используемого на рабочих местах оборудования и ПО.
- Полномочия пользователей.

Далее мы берем подготовленный список вопросов, составленный при изучении разделов стандарта ISO 17799, и делим его на две части, влияющих на уровень угроз и влияющих на уровень уязвимости. Напротив фиксированных вариантов ответов поставим определенное количество баллов, определяющих уровень критичности.

Для определения факторов влияющих на уровень угроз, приведем следующий вопрос с вариантами ответов:

Может ли сокрытие информации принести прямую финансовую или иную выгоду сотрудникам?

Варианты ответов:

а) Да 15

б) Нет 0

Для определения факторов влияющих на уровень уязвимости, приведем следующий вопрос с вариантами ответов:

Есть ли у сотрудников возможность осуществить несанкционированный доступ к информации (например, когда их непосредственно не контролируют, по вечерам и т.п.)?

а) Да 20

б) Нет 0

Итоговая оценка угрозы и уязвимости данного класса будет определяться суммированием баллов. Программный код сам оценит степень угрозы и уязвимости по количеству накопленных балов.

Таблица 2.4.Степень угрозы при количестве баллов.

До 60	Очень низкая
От 60 до 150	Низкая
От 150 до 250	Средняя
От 250 до 400	Высокая
400 и более	Очень высокая

Таблица 2.5. Степень уязвимости при количестве баллов.

До 100	Низкая
От 100 до 300	Средняя
300 и более	Высокая

Эта методика проста и дает владельцу информационных ресурсов ясное представление, каким образом получается итоговая оценка и что надо изменить, чтобы улучшить показатели.

Далее используя метод оценка рисков по трем факторам произведем расчет по формуле 2.3.

В результате проделанной работы по оценки рисков мы получим качественные показатели. А при использовании оценки ущерба в случае реализации угроз конфиденциальности, целостности и доступности– мы сможем получить и некоторые количественные результаты.

2.4. Методика проверки организационных мер на соответствие положениям международного стандарта безопасности ISO 17799.

Политика информационной безопасности компании является важнейшим нормативным документом, определяющим комплекс мер и требований по обеспечению информационной безопасности бизнеса. Политика безопасности должна описывать реальное положение дел в информационной системе компании и являться обязательным руководством к действию для всего персонала компании. На сегодняшний день общепризнанным стандартом при создании комплексной политики безопасности компании является международный стандарт управления информационной безопасностью ISO 17799, созданный в 2000 году Международной организацией по стандартизации и Международной электротехнической комиссией на основе разработок Британского института стандартов [7].

Ниже приведены основные разделы стандарта ISO 17799:

1. *Политика безопасности*
2. *Организационные меры по обеспечению безопасности*
   - Управление форумами по информационной безопасности
   - Координация вопросов, связанных с информационной безопасностью
   - Распределение ответственности за обеспечение безопасности
3. *Классификация и управление ресурсами*
   - Инвентаризация ресурсов
   - Классификация ресурсов
4. *Безопасность персонала*
   - Безопасность при выборе и работе с персоналом

- Тренинги персонала по вопросам безопасности
- Реагирование на секьюрити инциденты и неисправности

5. *Физическая безопасность*
6. *Управление коммуникациями и процессами*
    - Рабочие процедуры и ответственность
    - Системное планирование
    - Защита от злонамеренного программного обеспечения (вирусов, троянских коней)
    - Управление внутренними ресурсами
    - Управление сетями
    - Безопасность носителей данных
    - Передача информации и программного обеспечения
7. *Контроль доступа*
    - Бизнес требования для контроля доступа
    - Управление доступом пользователя
    - Ответственность пользователей
    - Контроль и управление удаленного (сетевого) доступа
    - Контроль доступа в операционную систему
    - Контроль и управление доступом к приложениям
    - Мониторинг доступа и использования систем
8. *Разработка и техническая поддержка вычислительных систем*
    - Требования по безопасности систем
    - Безопасность приложений
    - Криптография
    - Безопасность системных файлов
    - Безопасность процессов разработки и поддержки
9. *Управление непрерывностью бизнеса*
    - Процесс управления непрерывного ведения бизнеса
    - Непрерывность бизнеса и анализ воздействий
    - Создание и внедрение плана непрерывного ведения бизнеса
    - Тестирование, обеспечение и переоценка плана непрерывного ведения бизнеса
10. *Соответствие системы основным требованиям*
    - Соответствие требованиям законодательства
    - Анализ соответствия политики безопасности
    - Анализ соответствия техническим требованиям
    - Анализ соответствия требованиям системного аудита

После изучения русской редакции ISO 17799 был разработан вопросник, ответив на вопросы которого получаем подробный отчет о состоянии дел в существующей политики безопасности организации.

Алгоритм работы данного раздела поясним на следующем примере.

При выборе раздела стандарта “Политика безопасности. Организационные меры” пользователю предлагается ответить на следующий вопрос с вариантами ответов:

Существует ли в компании разработанная политика информационной безопасности, все положения которой на практике внедрены в информационную систему?

а) Да

б) Нет

в) Положения политики внедрены частично.

После обработки ответа в таблицу базы данных записывается следующее:

При ответе “Нет” - “Необходимо разработать и внедрить комплексную политику информационной безопасности”.

При ответе “ Положения политики внедрены частично”- Необходимо добиться полного внедрения всех положений политики безопасности в информационную систему компании.

При ответе на остальные вопросы происходят те же действия.

2.5. Разработка функциональных схем элементов автоматизированной системы.

С позиции обеспечения безопасности информации в КС такие системы целесообразно рассматривать в виде единства трех компонент, оказывающих взаимное влияние друг на друга:

- информация;
- технические и программные средства;
- обслуживающий персонал и пользователи.

Поэтому на первом этапе идет определения вида ресурсов, представляющих ценность для компании

Осуществляем выполнение следующего алгоритма:

Вводим блок опроса, предназначенный для получения нашей системой данных, которые в последствии понадобятся для оценки рисков. Блок опроса при взаимодействии с пользователем определяет информацию, функционирующую в данной информационной системе, пользователей системы и аппаратные средства, предназначенные для обработки и хранения информации. Далее все это заноситься в файл базы данных Access. Это самый первый, и наверно даже ключевой этап работы, после проведения которого мы имеем в базе данных определенное количество таблиц , каждая из которых соответствует тому или иному ресурсу.

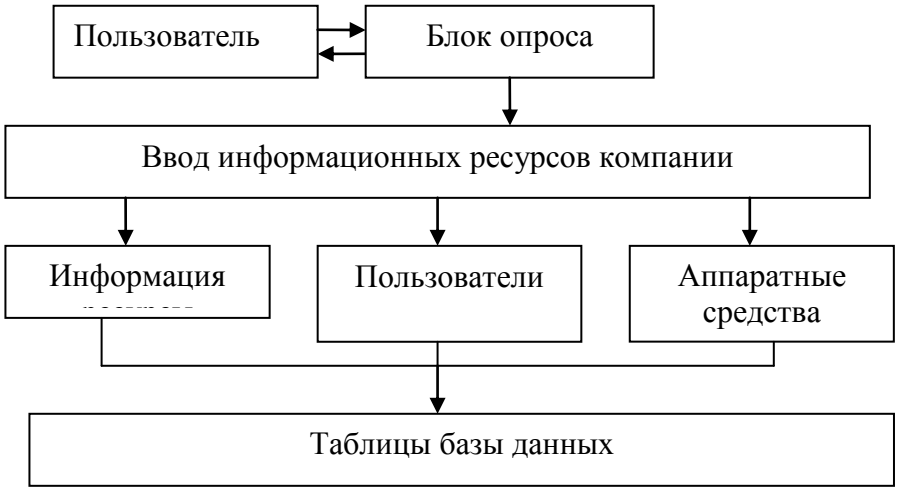

Рисунок 2.1. Схема функционирования блока опроса по выявлению ресурсов компании.

Следующий этап работы позволяет определить места хранения информации (Осуществить привязку данных) и оценить ущерб, который понесет компания в случае реализации одной из трех классических угроз, направленных на информацию. Речь идет об угрозах: конфиденциальности (право на чтение), целостности (право на запись) и отказа в обслуживании (нарушение работоспособности ресурса, на котором хранится ценная информация).

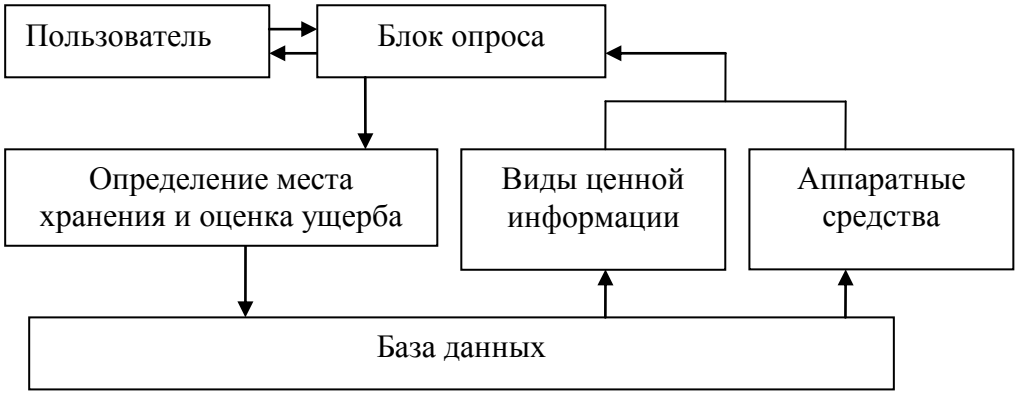

Рисунок 2.2. Схема функционирования блока опроса по привязке данных и оценки ущерба.

Из сформированных таблиц базы данных выводиться информация, циркулирующая в данной системе и аппаратные средства, предназначенные для ее хранения. Блок опроса определяет место хранения и одновременно оценивает ущерб. Полученные данные формируют очередную таблицу.

На следующем этапе работы происходит определение уровня угроз и уровня уязвимости.

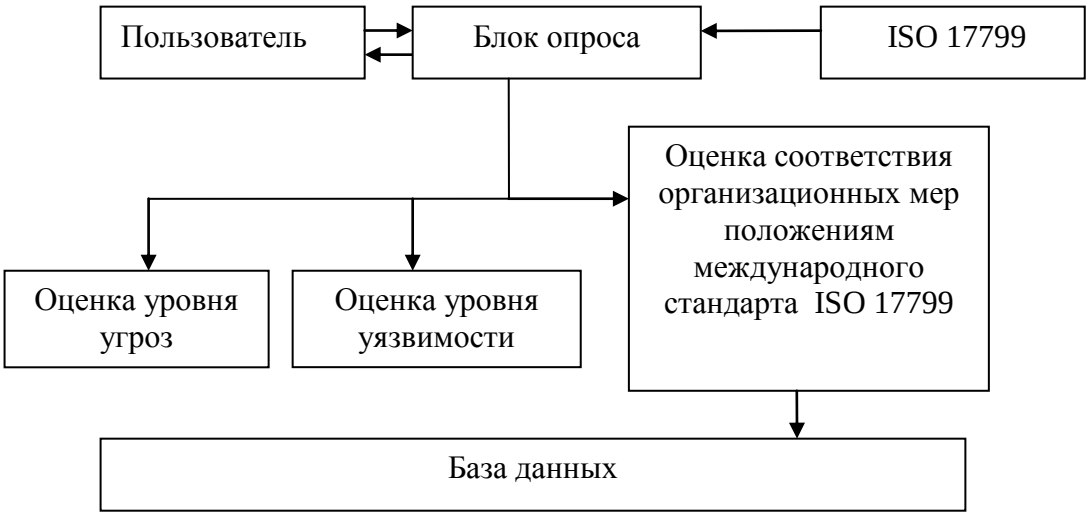

Рисунок 2.3. Схема функционирования блока опроса по оценкам уровня уязвимости, угроз и существующей политики безопасности.

Блок опроса, учитывая ответы на вопросы, оценивает уровни уязвимости и угрозы. Кроме этого происходит формирование в базе данных очередной таблицы с комментариями о не выполненных положениях стандарта.

Теперь осталось заполнить таблицы доступом субъектов системы к объектам системы. Это необходимо для того - чтобы программа, при расчете рисков знала какая категория пользователей (или кто из пользователей) к какому ресурсу имеет доступ, а к какому – нет. Кроме самого доступа, блок опроса определяет и права (чтение, запись, удаление). Блок опроса при взаимодействии с пользователем определяет доступ к ресурсам. Данные о ресурсах и пользователях выводятся на суд пользователю из уже сформированных таблиц базы данных. Полученные данные позволяют пересмотреть оценку уровня угрозы.

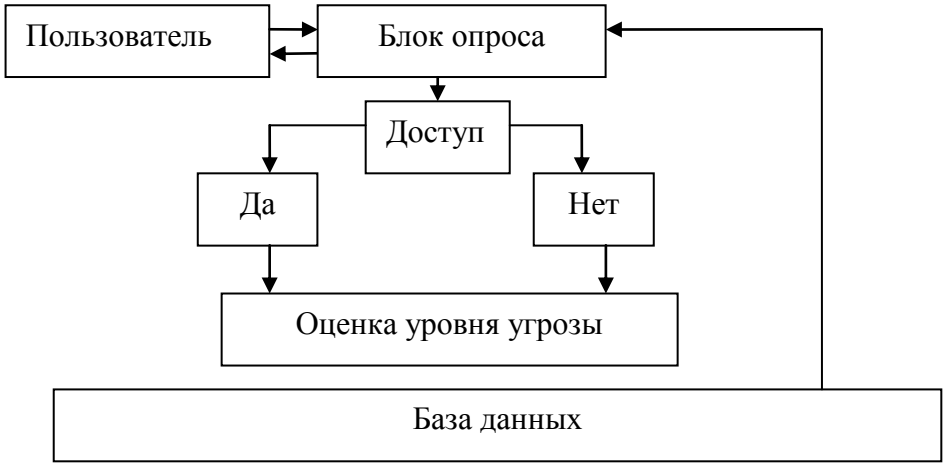

Рисунок 2.4. Схема функционирования блока опроса по выявлению доступа субъектов системы к объектам

Далее с целью определение эффективности системы защиты информации требуется определить и внести в систему полную стоимость затрат на обеспечение информационной безопасности в год.

Блок опроса при взаимодействии с пользователем определяет полную стоимость затрат на обеспечение информационной безопасности. Полученные данные сохраняются в память.

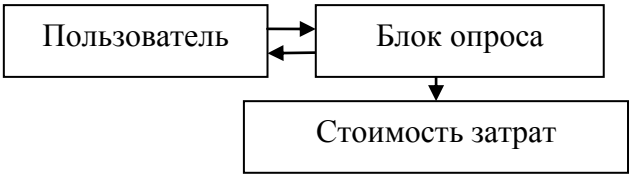

Рисунок 2.5. Схема функционирования блока опроса по выявлению эффективности системы защиты информации.

Следующий этап работы системы происходит анализ рисков.

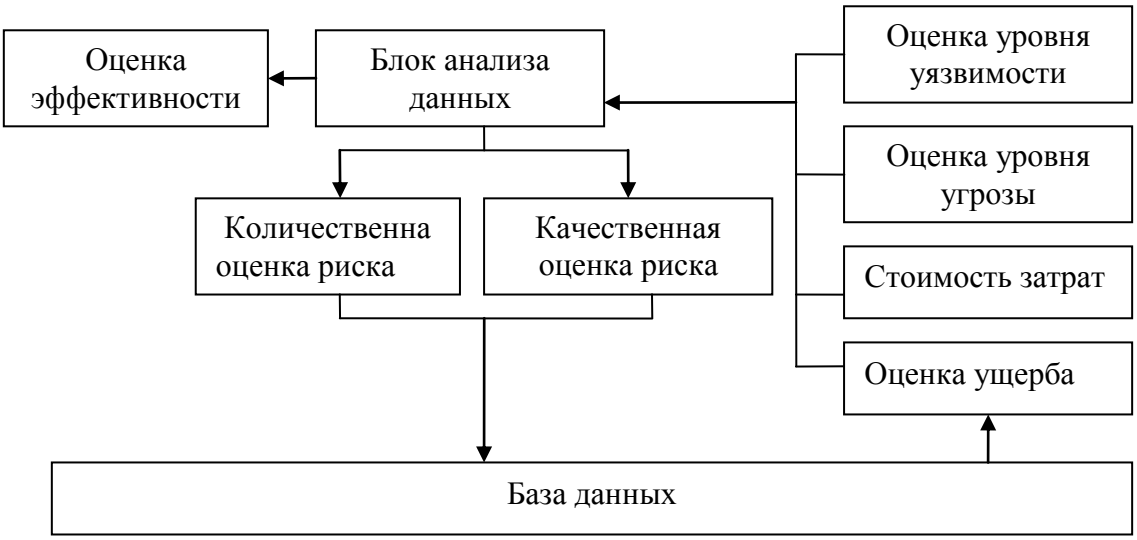

Рисунок 2.6. Схема функционирования блока анализа рисков.

В блок анализа данных поступает информация об оценках уровни уязвимости и угроз и информации о затратах на поддержании системы безопасности. В нем по

выбранной методики происходит анализ рисков , и выдаются качественная и количественная оценки рисков. Полученные данные отображаются в отчете .

2.5. Разработка алгоритма и интерфейса программы анализа информационных рисков.

Из существующих функциональных схем анализа и контроля рисков и проверки политики информационной безопасности компании можно построить алгоритм работы всей системы анализа.

На этом этапе необходимо определить взаимосвязь отдельных функциональных схем в самой системе анализа. Необходимо создать такой алгоритм который позволит с минимальными вложением сил реализовать нашу систему в программном коде. Это позволить проверить правильность построения, верность функционирования и определить эффективность проведенной работы.

На анализе выше стающих функциональных схем и структурной схемы был построен следующий алгоритм.

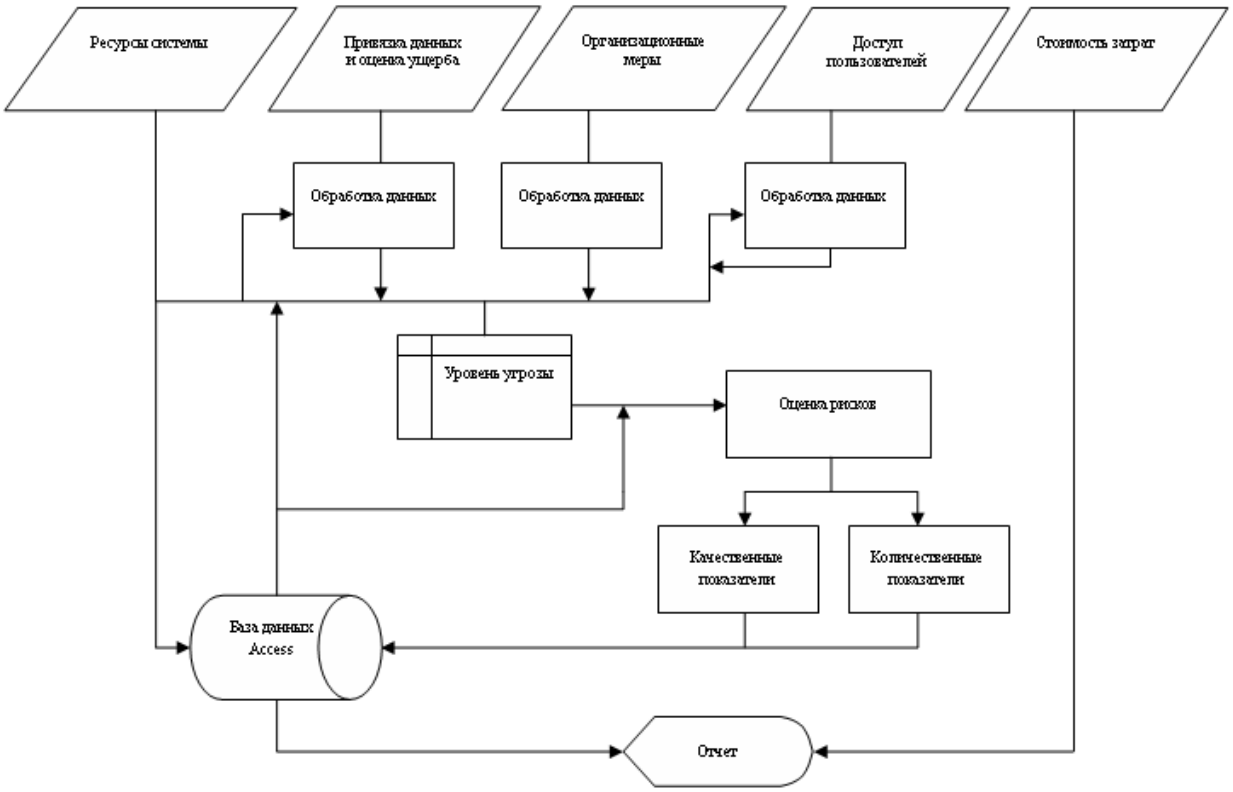

Рисунок 2.7. Алгоритм интерфейса программы анализа информационных рисков.

Этапы функционирования

Первым этапом работы всей системы – является получение необходимой информации для анализа. С помощью блока опроса и дальнейшей обработки , информация заноситься в базу данных. В результате – на начальном этапе заполняются данными три таблицы. В этих таблицах храниться:

1. Таблица”Inform”. Информация об основных категориях информационных ресурсов организации.
2. Таблица”Polzovateli”. Информация о пользователях.
3. Таблица”Server”. Информация о серверах.
4. Таблица”Stanzii”. Информация о рабочих станциях.

На втором этапе данные, после привязке и оценки ущерба заносятся в таблицу ”Stoimost”. На третьем этапе происходит проверка организационных мер на соответствие положениям международного стандарта безопасности ISO 17799. Полученные данные записываются в таблицу “ISO17799”.

На третьем и четвертом этапах формируются данные о доступе, правах доступа и оценки ежегодные затраты на обеспечения информационной безопасности организации, которые поступают в “Блок анализа данных” где после запроса необходимой информации из базы данных Access происходит процесс анализа информационных рисков.

Пятый заключительный этап работы программы, полученные данные используются для формирования отчета.

3. Интерфейс системы.

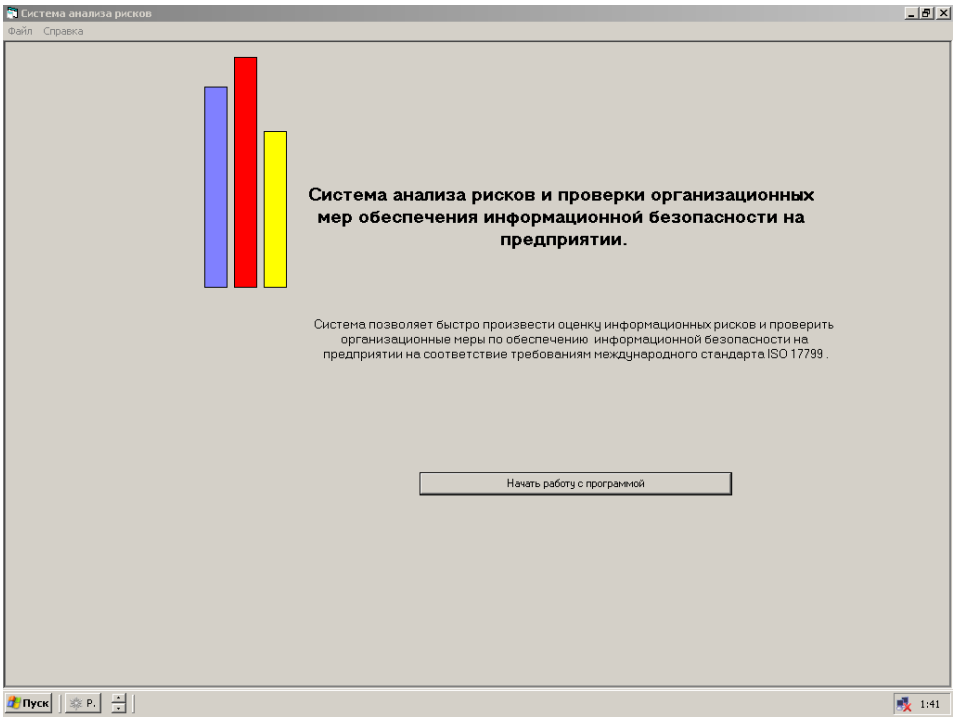

Рисунок.3.1 Главное окно программы

Первым этап. Определения полного списка информационных ресурсов, представляющих ценность для компании.

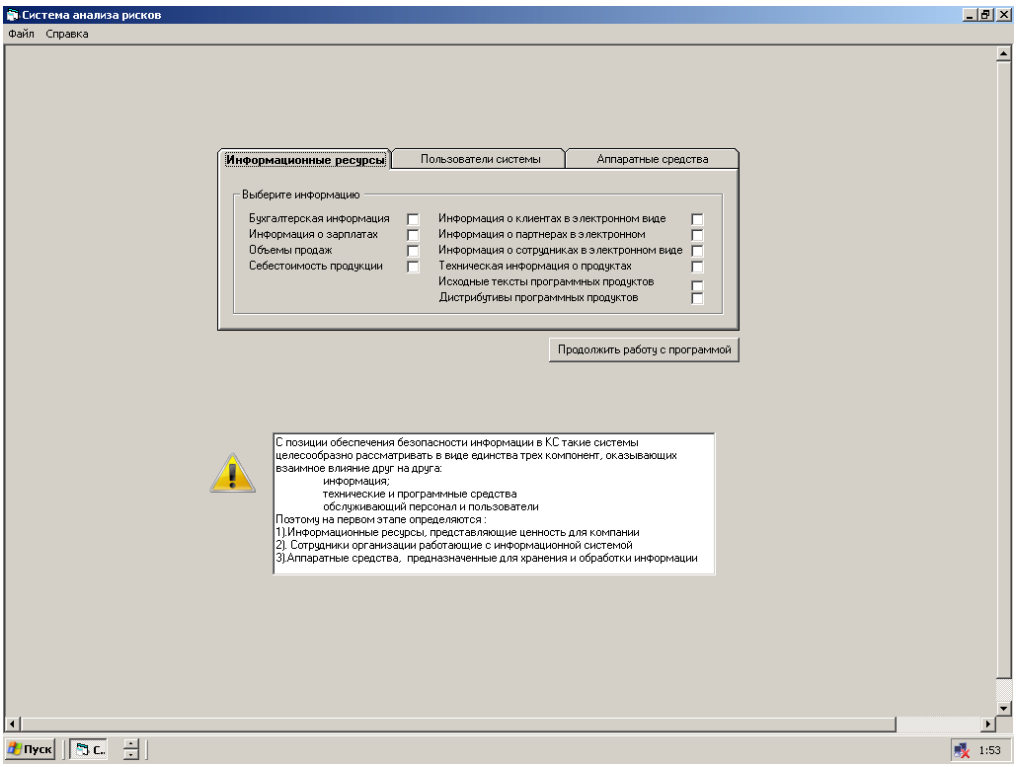

Рисунок 3.2. Интерфейс программы. Вкладка “Информационные ресурсы”.

Данная вкладка позволяет отметить виды информации, циркулирующие в системе: Это может быть:

- Финансовая информация
- Бухгалтерская информация
- Информация о зарплатах
- Объемы продаж
- Себестоимость продукции

Ценная информация

- Информация о клиентах в электронном виде
- Информация о партнерах в электронном виде
- Информация о сотрудниках в электронном виде
- Техническая информация о продуктах
- Исходные тексты программных продуктов
- Дистрибутивы программных продуктов (в том числе и собственные)
- Стратегические планы развития компании в электронном виде

Вкладка “Пользователи системы” дает возможность выбрать из приведенного списка тех пользователей, которые имеют отношение к данной информационной системе.

Это могут быть:

- Системные администраторы
- Офицеры безопасности
- Менеджеры
- Операторы или обычные пользователи

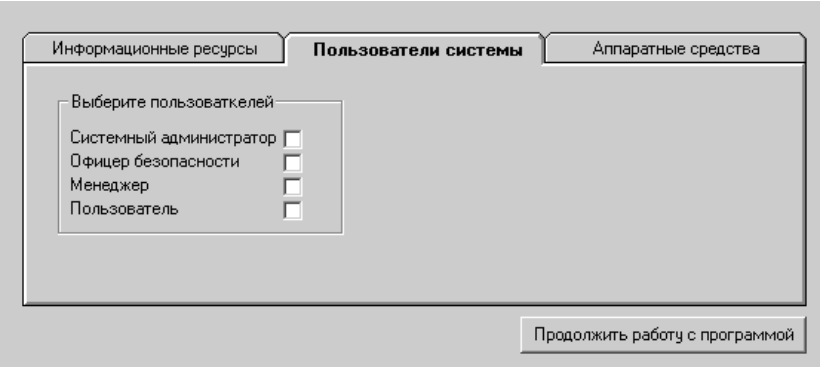

Рисунок 3.3 Интерфейс программы. Вкладка “Пользователи системы”.

Вкладка “Аппаратные средства” позволяет определить, место хранение и обработки информации.

Это могут быть:

- Сервера
- Рабочие станции
- Твердые копии

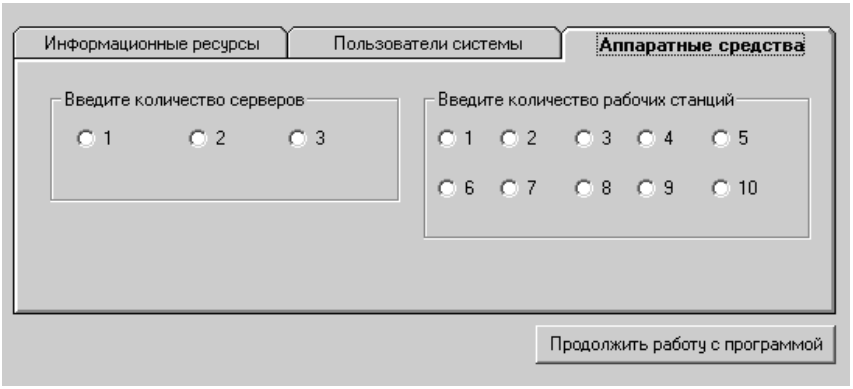

Рисунок 3.4. Интерфейс программы. Вкладка “Аппаратные средства”.

На вкладке приведенной ниже происходит привязка данных. Требуется расположить на каждом из ранее введенных ресурсов все указанные ранее виды ценной информации.

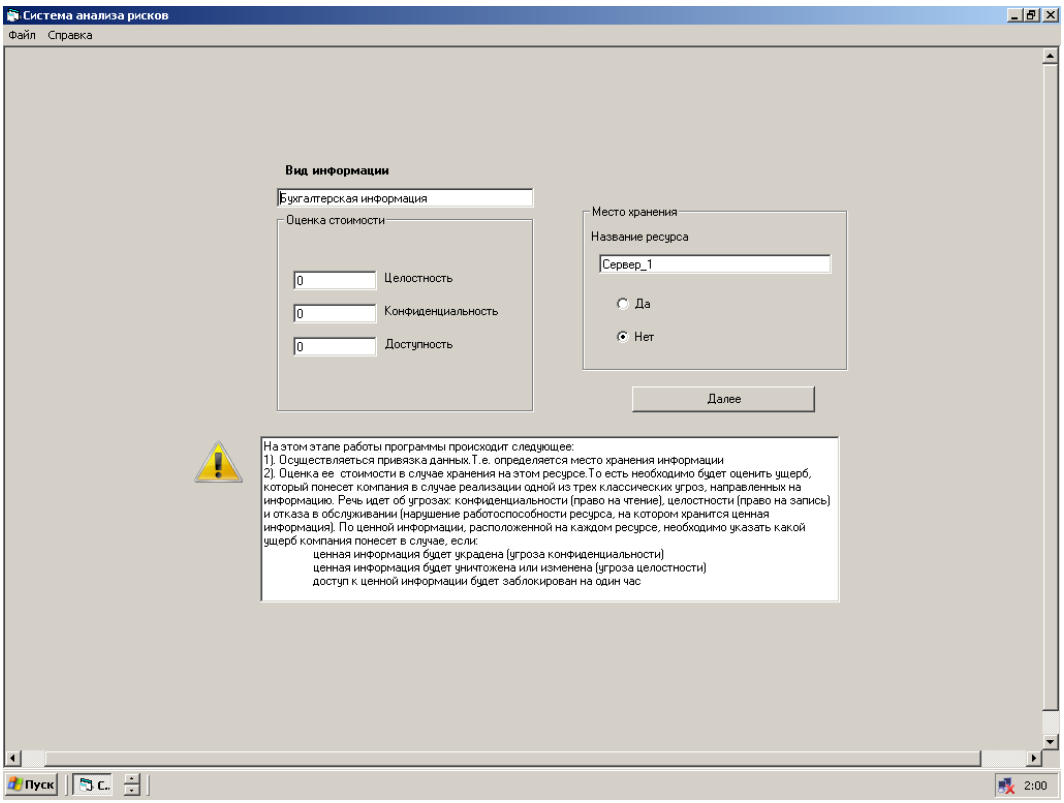

Рисунок 3.5. Интерфейс программы. Вкладка ”Привязка данных”.

Кроме этого на этом этапе работы необходимо еще определить стоимость информации. То есть необходимо оценить ущерб, который понесет компания в случае реализации одной из трех классических угроз, направленных на информацию. Речь идет об угрозах: конфиденциальности (право на чтение), целостности (право на запись) и отказа в обслуживании (нарушение работоспособности ресурса, на котором хранится ценная информация). По ценной информации, расположенной на каждом ресурсе, необходимо указать какой ущерб компания понесет в случае, если:

- ценная информация будет украдена (угроза конфиденциальности)
- ценная информация будет уничтожена или изменена (угроза целостности)
- доступ к ценной информации будет заблокирован на один час

Оценивая ущерб от реализации угроз, необходимо учитывать:

- цену ресурса - затраты на производство;
- стоимость восстановления или создания (покупку) нового ресурса;
- стоимость восстановления работоспособности организации (при работе с искаженным ресурсом, без него, при дезинформации);
- стоимость вынужденного простоя;
- стоимость упущенной выгоды (потерянный контракт);
- стоимость выплаты неустоек, штрафов (за невыполнение обязательств контракта);
- стоимость затрат на реабилитацию подмоченной репутации, престижа, имени фирмы;
- стоимость затрат на поиск новых клиентов, взамен более не доверяющих фирме;
- стоимость затрат на поиск (или восстановление) новых каналов связи, информационных источников.

Часто люди реально даже не представляют , чем владеют. Однако за владельцев оценить информацию не возможно. Предполагаемый злоумышленник может, конечно, оценить туже информацию иначе. Значить кто-то тут ошибается: владелец или злоумышленник. Конечно же , речь идет о приблизительной оценки. Точно оценить информацию очень сложно.

После проделанной работы мы переходим к следующему этапу, этапу “Проверки организационных мер обеспечения информационной безопасности на соответствие положением МСБ ISO 17799.

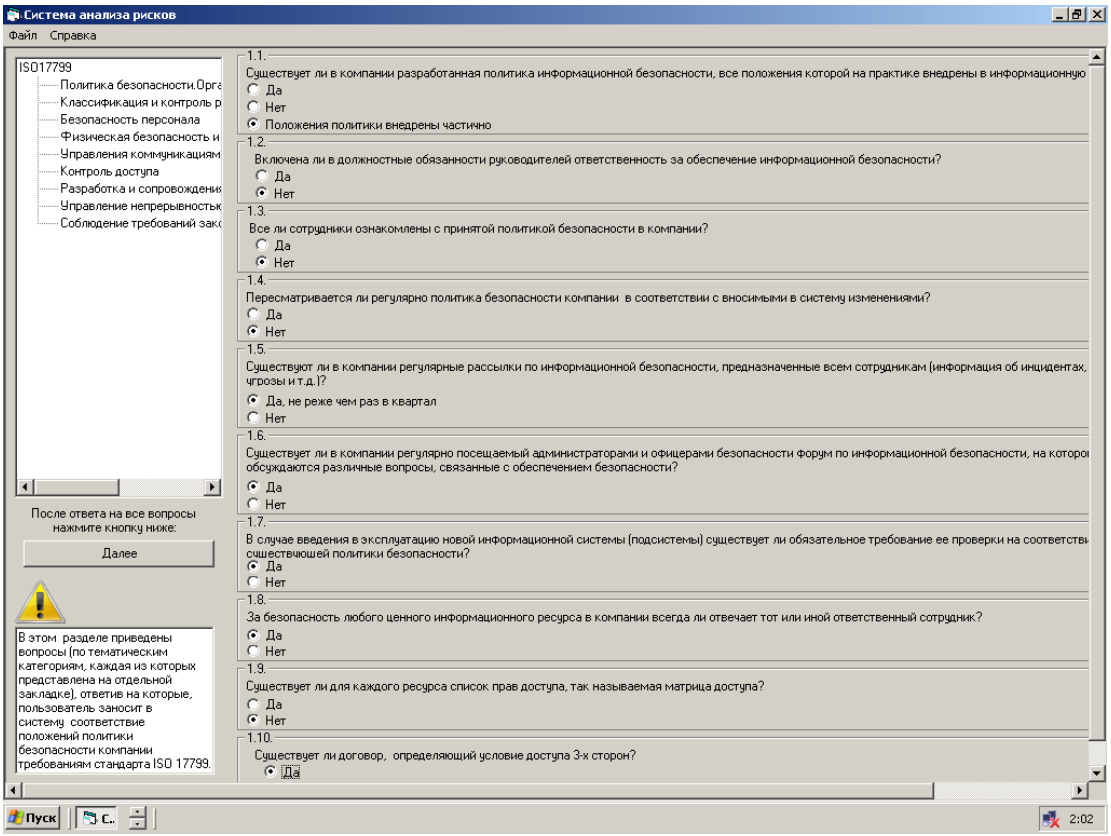

Рисунок 3.6. Интерфейс программы. Вкладка ”Организационные меры”.

Пользователю предлагается ответить на вопросы, разработанные после изучение положений МБО. Вопросы структурированы по разделам стандарта. Выбор раздела осуществляется в левой части экрана щелчком правой кнопки мыши. Вопросы отображаются в правой части. Это форма, как и все остальные, снабжена подсказками.

После ответа на все вопросы, пользователь нажимает кнопку далее и программа переходит к следующему окну.

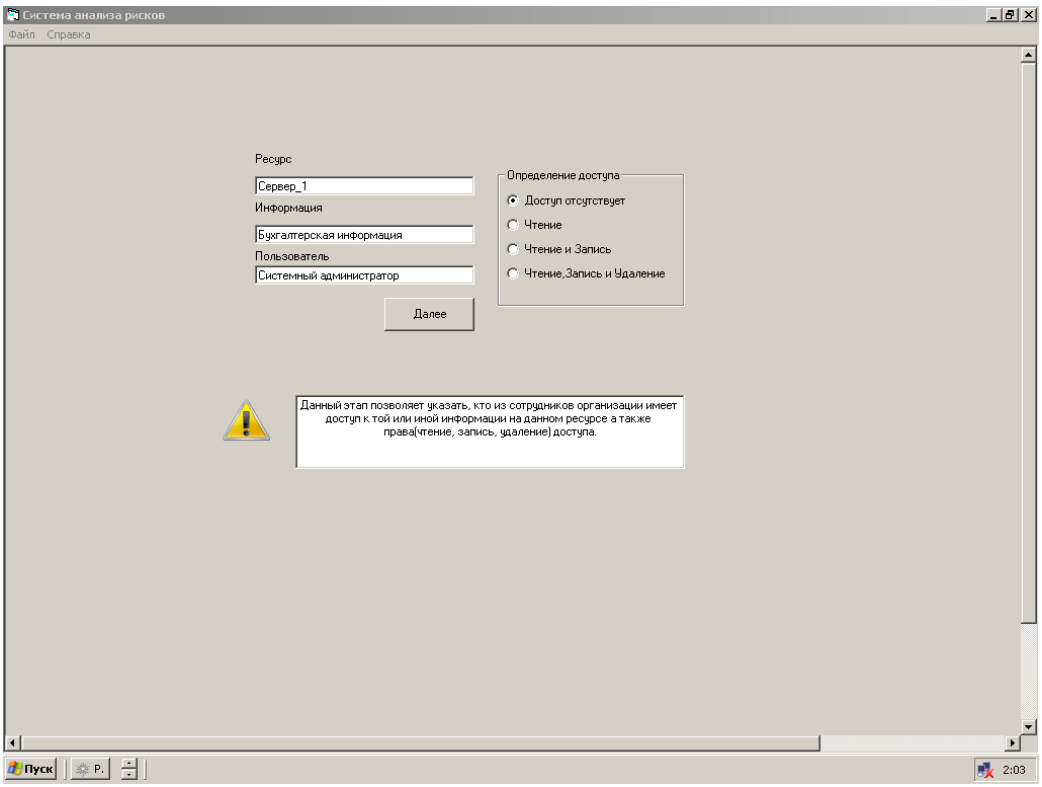

Рисунок 3.7. Интерфейс программы. Вкладка “доступ”.

Здесь необходимо определить доступ пользователей и его права (чтение, запись, удаление) ко всем ресурсам, содержащим ценную информацию. Переходим к следующему окну.

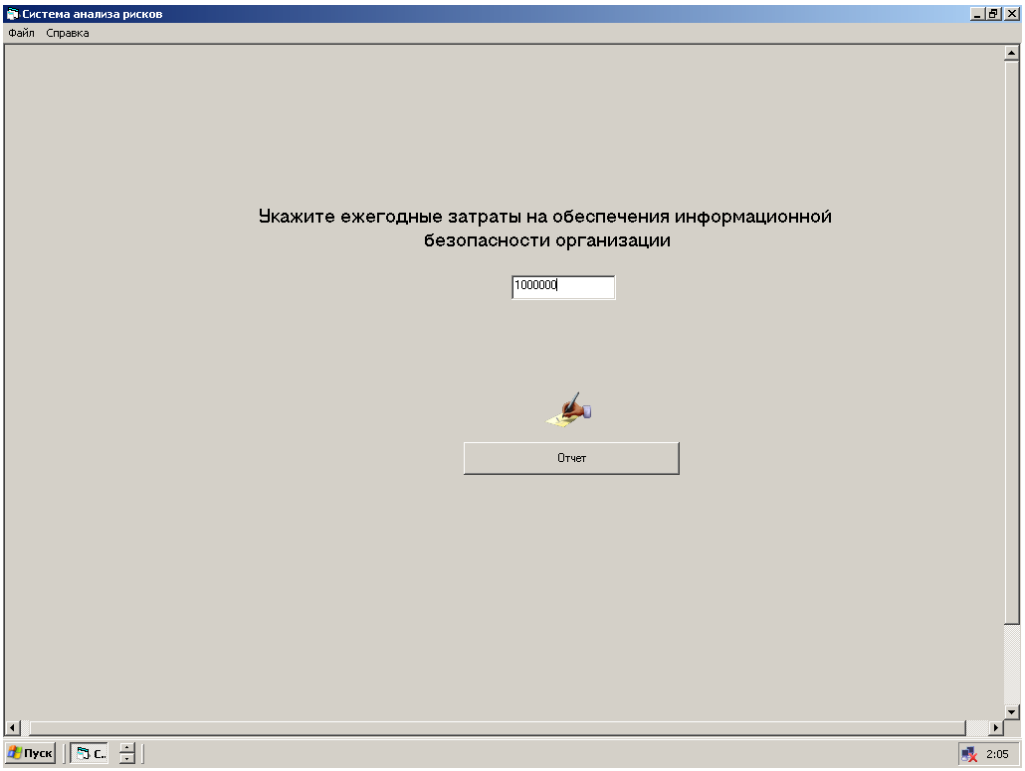

Рисунок 3.8. Интерфейс программы. Оценка затрат на поддержание системы безопасности.

На данном этапе работы с целью определение эффективности системы защиты информации требуется определить и внести в систему полную стоимость затрат на обеспечение информационной безопасности.

В этом случае эффективность можно определить как отношение затрат к потерям которые понесет компания в случае реализации угроз безопасности.

Это могут быть:

- *Затраты на покупку систем защиты информации.* Другими словами, это стоимость лицензии программного обеспечения. Кроме того, необходимо также учесть в данном пункте затраты на аппаратное обеспечение - стоимость одного или нескольких компьютеров, на которых развернуты компоненты системы защиты. Также необходимо учесть затраты на покупку или создание средств технической защиты. Помимо этого, часто система защиты использует дополнительное программное и аппаратное обеспечение, стоимость которого также необходимо учитывать. К такому обеспечению можно отнести базы данных, системы настройки оборудования, системы резервирования, сетевые кабели, тройники, системы бесперебойного питания и т.д. В крупных компаниях, имеющих распределенную корпоративную сеть, не стоит забывать о затратах на внедрение (включая этап предварительного аудита).
- *Затраты на поддержку и обучение* (если она не включена в стоимость системы защиты). Сюда же можно отнести и командировочные расходы IT-специалистов на поездки в удаленные офисы и настройку удаленных компонентов системы обеспечения информационной безопасности.
- *Затраты на управление* (администрирование) системой защиты, которые включают зарплату администраторов безопасности и другого персонала, связанного с системой обнаружения атак и модернизацию ее программно-аппаратного обеспечения. К этой статье расходов относится оплата за услуги аутсорсинговых компаний и реагирование на инциденты безопасности.

Теперь система генерирует отчет и выводит полученные данные на обозрение.

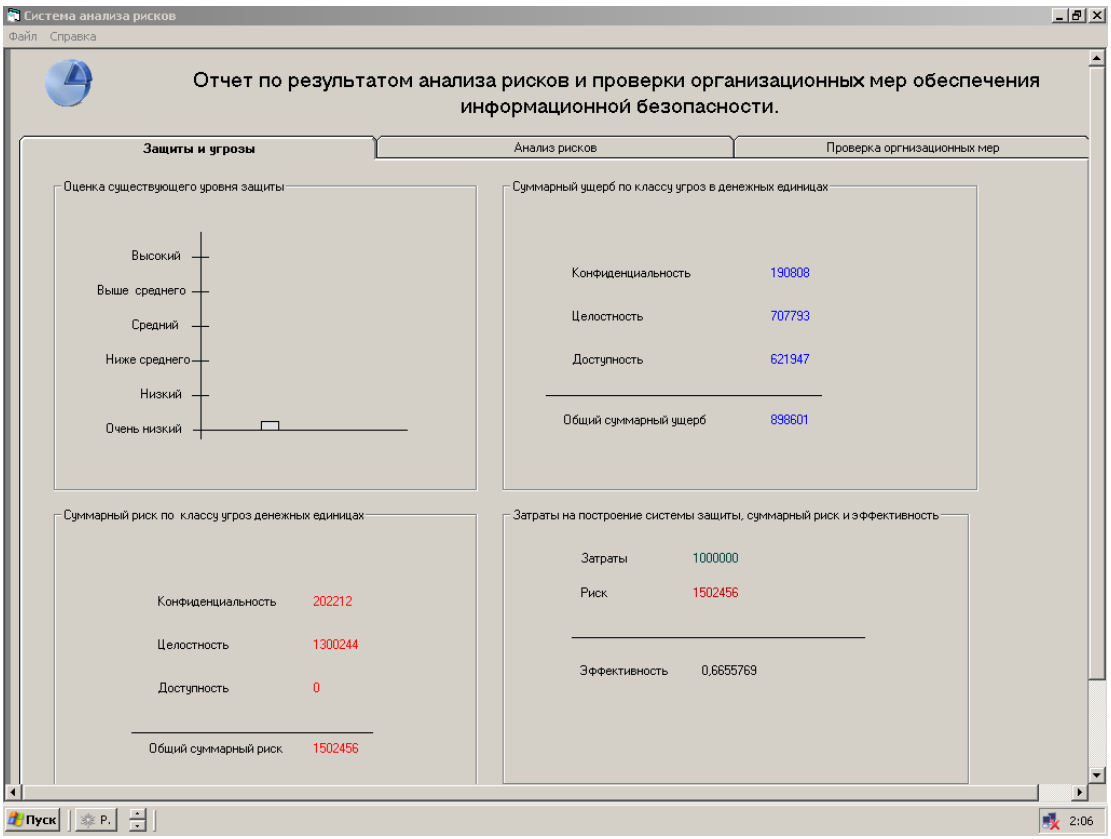

Рисунок 3.9. Интерфейс программы. Вкладка “Защита и угрозы”.

Данная вкладка позволяет пользователю визуально оценить существующий уровень информационной защиты, суммарный риск и ущерб по трем классам угроз и эффективность существующей системы защиты.

При щелчке мыши по вкладке “Анализ рисков” появляются еще две вкладки , демонстрирующие качественные и количественные показатели рисков

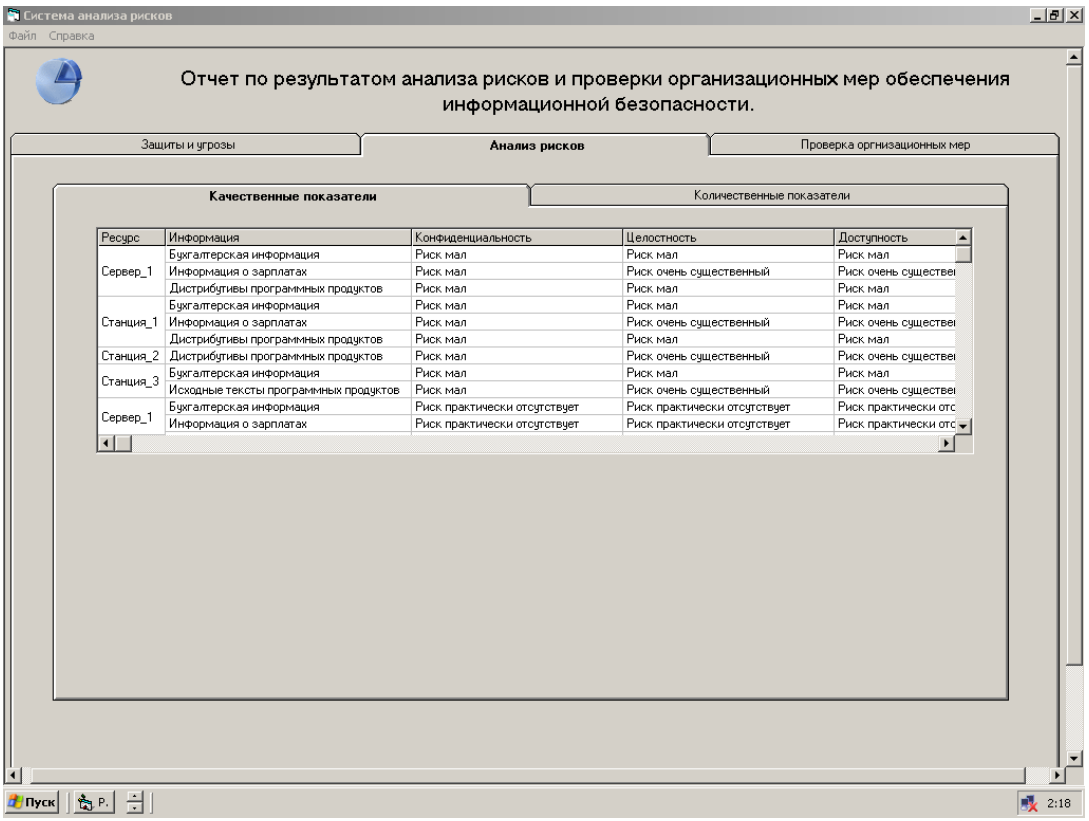

Рисунок 3.10. Интерфейс программы. Вкладка “Анализ рисков. Качественные показатели”.

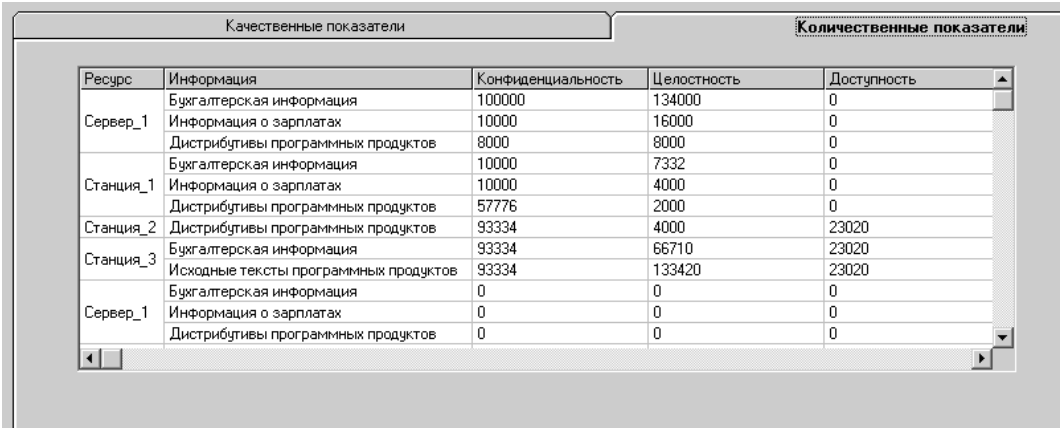

Рисунок 3.11. Интерфейс программы. Вкладка “Анализ рисков. Количественные показатели”.

Последняя вкладка “Проверка организационных мер ” демонстрирует пользователю , количество не соответствующих организационных мер положениям МБО и выводит пояснение.

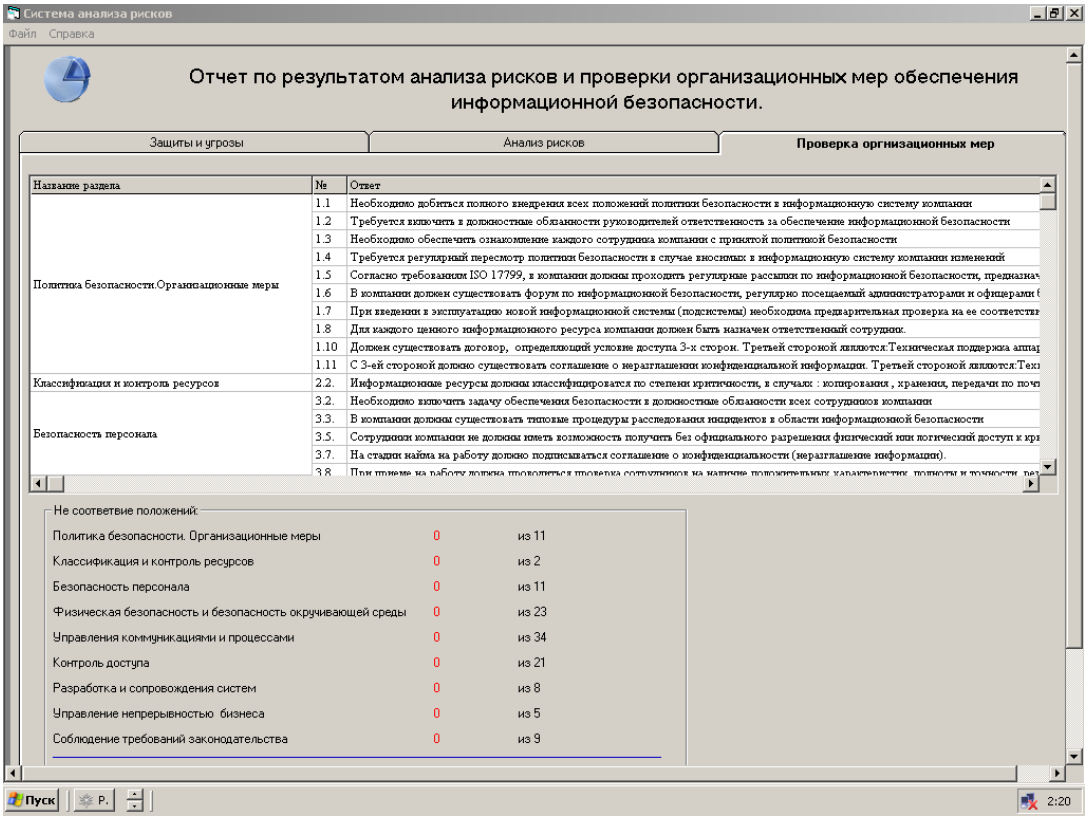

Рисунок 3.12. Интерфейс программы. Вкладка “ Проверка организационных мер ”.

4. Тестирование системы

Данный пункт необходим для проведения проверки верного функционирования расчетного блока программного кода (его части). Тестирование направленно на изучение зависимости потерь организации от некоторых факторов (от классификация злоумышленника, права доступа пользователей системы и организационных мер обеспечения информационной безопасности**).**

Используемая при тестировании программного продукта информация не основывается на конкретных значениях, для конкретного предприятия – это абстрактные данные об абстрактном предприятии, необходимые для процесса тестирования.

Таблица 4.1.Исходные данные для исследования.

Виды информации	Бухгалтерская информация Информация о зарплатах Информация о клиентах в электронном виде Исходные тексты программных продуктов Дистрибутивы программных продуктов (в том числе и собственные) Информация о партнерах в электронном виде
Пользователи системы	Системный администратор Офицеры безопасности Пользователь
Аппаратные средства	Сетевая группа: Один сервер Три рабочих станции

Теперь осуществим привязку данных. Расположим на каждом из ранее введенных ресурсов указанные виды ценной информации.

Таблица 4.2. Привязка данных

Сервер	Исходные тексты программных продуктов Дистрибутивы программных продуктов (в том числе и собственные)
Рабочая станция один	Бухгалтерская информация Информация о зарплатах
Рабочая станция два	Бухгалтерская информация Информация о зарплатах
Рабочая станция три	Информация о клиентах в электронном виде Информация о партнерах в электронном виде

Для определения стоимости информации, необходимо оценить ущерб, который понесет компания в случае реализации трех классических угроз.

В предыдущем шаге мы разместили один и тот же тип информации на двух рабочих станциях. В этом шаге мы еще и оценим их одинаково. В конце тестов мы посмотрим результат и оценим, на сколько правильно работает алгоритм системы.

Таблица 4.3. Оценка информации

Ресурс	Информация	Ущерб, в случае угрозы конфиденциальности, руб.	Ущерб, в случае угрозы целостности, руб.	Ущерб, в случае угрозы доступности, руб.
Сервер	Исходные тексты программных продуктов	80 000	50 000	120 000
	Дистрибутивы программных продуктов	110 000	80 000	170 000
Рабочая станция один	Бухгалтерская информация	5 000	140 000	120 000
	Информация о зарплатах	130 000	260 000	100 000
Рабочая станция два	Бухгалтерская информация	5 000	140 000	120 000
	Информация о зарплатах	130 000	260 000	100 000
Рабочая станция три	Информация о клиентах в электронном виде	150 000	170 000	250 000
	Информация о партнерах в электронном виде	160 000	145 000	300 000

Определение доступа мы произведем по следующей схеме:

1) Ограничим доступ всех пользователей к информации, хранящейся на первой рабочей станции.

2) К тем же видам информации на второй рабочей станции права доступа оценим по разному.

Таблица 4.4.Определение прав доступа пользователей на рабочей станции два

Пользователи	Информация	Права доступа
Системный администратор	Бухгалтерская информация	Чтение , запись, удаление
	Информация о зарплатах	Чтение и запись
Офицер безопасности	Бухгалтерская информация	Чтение , запись, удаление
	Информация о зарплатах	Чтение и запись
Пользователь	Бухгалтерская информация	Чтение и запись
	Информация о зарплатах	Чтение

3) Укажем доступ к информации, хранящейся на сервере и на третей рабочей станции в хаотичном порядке.

Таблица4.5. Определение прав доступа пользователей на рабочей станции три

Пользователи	Информация	Права доступа
Системный администратор	Информация о клиентах в электронном виде	Чтение , запись, удаление
	Информация о партнерах в электронном виде	Чтение
Офицер безопасности	Информация о клиентах в электронном виде	Доступ отсутствует
	Информация о партнерах в электронном виде	Чтение, запись
Пользователь	Информация о клиентах в электронном виде	Доступ отсутствует
	Информация о партнерах в электронном виде	Чтение

Таблица 4.6. Определение прав доступа пользователей на сервере

Пользователи	Информация	Права доступа
Системный администратор	Исходные тексты программных продуктов	чтение
	Дистрибутивы программных продуктов (в том числе и собственные)	Чтение и запись
Офицер безопасности	Исходные тексты программных продуктов	Чтение, запись, удаление
	Дистрибутивы программных продуктов (в том числе и собственные)	Чтение и запись
Пользователь	Исходные тексты программных продуктов	Доступ отсутствует
	Дистрибутивы программных продуктов (в том числе и собственные)	Доступ отсутствует

Далее, для проверки организационных мер, осуществим невыполнение большинства требования международного стандарта ISO 17799. Это позволит увеличить

уровень уязвимости системы. С помощью ответов на вопросы связанных с тем, на сколько сотрудники заинтересованы в неправомерных действиях, мы увеличим уровень угроз. Оценим ежегодные затраты на обеспечения информационной безопасности в 500 тысяч рублей. Процесс тестирования дал следующие результаты.

Таблица 4.7.Результат расчета количественной характеристики рисков

Ресурс	Информация	Риск связанный с угрозой конфиденциальности, руб.	Риск связанный с угрозой целостности, руб.	Риск связанный с угрозой доступности, руб.
Сервер	Исходные тексты программных продуктов	480 000	400 000	960 000
	Дистрибутивы программных продуктов	660 000	640 000	1 020 000
Рабочая станция один	Бухгалтерская информация	30000	840000	720000
	Информация о зарплатах	780000	1560000	600000
Рабочая станция два	Бухгалтерская информация	40000	1120000	960000
	Информация о зарплатах	1040000	2080000	600000
Рабочая станция три	Информация о клиентах в электронном виде	900000	1020000	1500000
	Информация о партнерах в электронном виде	960000	870000	1800000

Таблица 4.8. Результат расчета качественной характеристики рисков

Ресурс	Информация	Риск связанный с угрозой конфиденциальности	Риск связанный с угрозой целостности	Риск связанный с угрозой доступности
Сервер	Исходные тексты программных продуктов	Риск велик	Риск очень велик	Риск очень велик
	Дистрибутивы программных продуктов	Риск велик	Риск очень велик	Риск очень велик
Рабочая станция один	Бухгалтерская информация	Риск велик	Риск велик	Риск велик
	Информация о зарплатах	Риск велик	Риск велик	Риск велик
Рабочая станция два	Бухгалтерская информация	Риск очень велик	Риск очень велик	Риск очень велик
	Информация о зарплатах	Риск очень велик	Риск очень велик	Риск очень велик

Рабочая станция три	Информация о клиентах в электронном виде	Риск велик	Риск велик	Риск велик
	Информация о партнерах в электронном виде	Риск велик	Риск велик	Риск велик

При этом система показала уровень системы защиты как низкий.

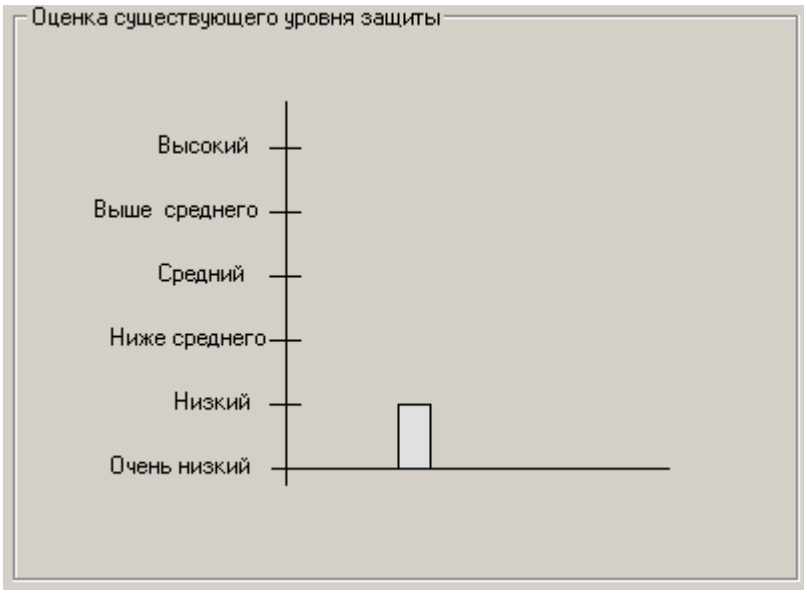

Рисунок 4.1. Оценка уровня защиты. Тест номер один.

Далее проведем следующее испытание программного комплекса. Теперь наоборот, попробуем выполнить как можно больше требований стандарта ISO17799.Это позволит увеличить уровень уязвимости системы и в некоторых случаях уровень угроз. Ответы ответов на вопросы связанные с тем, на сколько сотрудники заинтересованы в неправомерных действиях оставим такими же как и в первом тесте.

Процесс тестирования дал следующие результаты.

Таблица 4.9.Результат расчета количественной характеристики рисков

Ресурс	Информация	Риск связанный с угрозой конфиденциальности, руб.	Риск связанный с угрозой целостности, руб.	Риск связанный с угрозой доступности, руб.
Сервер	Исходные тексты программных продуктов	160000	100000	240000
	Дистрибутивы программных продуктов	220000	240000	340000
Рабочая станция один	Бухгалтерская информация	10000	280000	240000
	Информация о зарплатах	260000	520000	200000

Рабочая станция два	Бухгалтерская информация	10000	420000	240000
	Информация о зарплатах	260000	780000	200000
Рабочая станция три	Информация о клиентах в электронном виде	300000	340000	500000
	Информация о партнерах в электронном виде	320000	290000	600000

Таблица 4.10. Результат расчета качественной характеристики рисков

Ресурс	Информация	Риск связанный с угрозой конфиденциальности	Риск связанный с угрозой целостности	Риск связанный с угрозой доступности
Сервер	Исходные тексты программных продуктов	Риск мал	Риск мал	Риск мал
	Дистрибутивы программных продуктов	Риск мал	Риск существенный	Риск существенный
Рабочая станция один	Бухгалтерская информация	Риск мал	Риск мал	Риск мал
	Информация о зарплатах	Риск мал	Риск мал	Риск мал
Рабочая станция два	Бухгалтерская информация	Риск мал	Риск существенный	Риск существенный
	Информация о зарплатах	Риск мал	Риск существенный	Риск существенный
Рабочая станция три	Информация о клиентах в электронном виде	Риск мал	Риск мал	Риск мал
	Информация о партнерах в электронном виде	Риск мал	Риск мал	Риск мал

Организационные меры не соответствовали 23 положениям международного стандарта ISO 17799.

Рисунок 4.2. Оценка уровня защиты. Тест номер два

Из представленного материала мы видим , что произошло уменьшение риска до определенного уровня. Однако уровень угрозы со стороны сотрудников остался на определенном уровне, и это дало о себе знать. В целом система оценила уровень защиты как выше среднего.

Полученные данные говорят о том, что не соблюдение положений стандарта ISO 17799 приводит к увеличению риска связанного с угрозой конфиденциальности, целостности и доступности. Это в полнее справедливо так как, стандарт определяет базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики.

Мы заметили, что уровень рисков на рабочей станции два выше чем на номер один. Это говорит о том что, предоставление привилегированный прав доступа к информации, увеличивает уровень угрозы. Для борьбы с этим можно предпринять следующие меры:

Для того, чтобы понизить риск вредоносного воздействия со стороны сотрудников, необходимо уже при составлении должности максимально минимизировать количество информационных объектов, к которым пользователь будет иметь доступ впоследствии. В литературных источниках подобный принцип носит название принципа минимизации привилегий (либо прав доступа).

Потери предприятия тем меньше, чем меньше в этих потерях заинтересованы сотрудники данного предприятия. Очевидна необходимость ввода личной ответственности за собственную деятельность в отношении информационных активов компании. Личная ответственность предполагает разделение обязанностей по отношению к объектам, к которым пользователь имеет доступ. Отсюда суть второго результата тестирования: чтобы понизить риск вредоносного воздействия со стороны сотрудников, нужно следовать правилу разделения обязанностей.

При приеме на работу проводить проверку сотрудников на наличие положительных характеристик, полноты и точности резюме, подтверждение заявленного образования и профессиональной квалификации и независимую проверку документов – паспорта.

5. Методика проведения работы

1. Цель работы.

Целью данной работы является ознакомление с методикой анализа рисков, ролью анализа рисков в построении системы защиты, а также ознакомление с международным стандартом информационной безопасности ISO 17799.

2.Теоретическая часть.

Информацию по этому пункту вы в полном объеме найдете в меню “Справка”.

3. Порядок выполнения работы

1. После ознакомление с теорией получите у вашего преподавателя номер варианта на работу. Каждый номер варианта представляет определенную модель информационной системы. Номера вариантов приведены ниже.

Таблица 5.1. Вариант 1.

Название	Компания ”РеалСофт”
Сотрудники	Директор (сотрудник) Системный администратор Офицер безопасности Бухгалтер (сотрудник) Менеджер Программисты (сотрудники)
Информация	Бухгалтерская информация Информация о зарплатах Исходные тексты программных продуктов Дистрибутивы программных продуктов
Аппаратные средства для обработки информации	Два сервера Шесть рабочих станций
Описание	Организация занимается разработкой программного обеспечения. Расположена в отдельном здании. На входе расположена будка с охраной.
Затраты на информационную безопасность в год	100 000

Таблица 5.2. Вариант 2.

Название организации	Нотариальная контора ”Парус”
Сотрудники	Директор Бухгалтер (сотрудник) Менеджер
Информация	Бухгалтерская информация Информация о зарплатах Дистрибутивы программных продуктов Информация о клиентах в электронном виде
Аппаратные средства для обработки информации	Один сервер Три рабочих станции
Описание	Занимается оформление договоров купли-продажи, обмена, дарения жилья,

	автомашин, земельных участков, копий документов. Проводит квалифицированные консультации по нотариальным вопросам Арендуемое помещение на втором этаже. Кроме этой организации в здании расположено еще несколько фирм. На входе существует охрана , которую интересует целью прихода
Затраты на информационную безопасность в год	10 000

Таблица 5.3. Вариант 3.

Название организации	Страховая компания “Под крылом”
Сотрудники	Директор (пользователь) Бухгалтер (пользователь) Системный администратор Менеджеры
Информация	Бухгалтерская информация Информация о зарплатах Информация о клиентах в электронном виде Информация о сотрудниках в электронном виде Дистрибутивы программных продуктов
Аппаратные средства для обработки информации	Один сервер Четыре рабочих станции
Описание	Компания занимается страхованием всех видов деятельности. Расположена в отдельном здании. На входе сидит охранник.
Затраты на информационную безопасность в год	200 000

Таблица 5.4. Вариант 4.

Название организации	Филиал нефтяной компании в Томске “РусНефть”
Сотрудники	Директор (сотрудник) Системный администратор Офицер безопасности Бухгалтер (сотрудник) Менеджер Программисты (сотрудники)
Информация	Бухгалтерская информация Информация о зарплатах Информация о клиентах в электронном виде Дистрибутивы программных продуктов Объемы продаж Себестоимость продукции

Описание	Занимается транспортировкой и переработкой нефти. Расположена в отдельном здании. Существует служба безопасности. На входе охрана регистрирует цель прихода.

Таблица 5.5. Вариант 5.

Название организации	Компьютерная фирма ”Ваш компьютер”
Сотрудники	Директор (сотрудник) Системный администратор Бухгалтер (сотрудник) Менеджеры
Информация	Бухгалтерская информация Информация о зарплатах Дистрибутивы программных продуктов Объемы продаж Информация о партнерах в электронном виде Техническая информация о продуктах
Аппаратные средства для обработки информации	Два сервера Три рабочих станции
Описание	Занимается продажей компьютеров, офисной техники, сетевого оборудования, программного обеспечения. Расположена в отдельном здании. Существует служба охраны.
Затраты на информационную безопасность в год	1 000 000

2. Для того чтобы приступить к работе с “ Системой анализа рисков и проверки организационных мер обеспечения информационной безопасности на предприятия”, необходимо запустить файл Project.exe. Далее система покажет окно с предложением начать работу с программой

3. Выберите те виды информационных ресурсов которые представлены в вашем варианте. Теперь перейдите к вкладке “Пользователи системы”, где надо будет отметить пользователей информационной системы. На вкладке “Аппаратные средства” определите количество серверов и рабочих станций из вашего варианта. Нажмите кнопку ”Продолжить работу с программой”.

4. Укажите на сервере хранение двух любых видов информации из списка, а на рабочих станциях по четыре вида информационных ресурса, желательно разных и оцените предполагаемый ущерб, в случае угроз конфиденциальности, целостности и доступности. Так как данные хранятся на разных ресурсах, то предполагается, что они имеют разную ценность. В случае если информация не храниться на выбранном ресурсе, то ее оценка не имеет смысла - эти данные все равно не будут использованы. В случае затруднения обратитесь к подсказке.

5. Далее система отобразит окно, с вопросами по разделу стандарта в правой части и выбором раздела стандарта в левой части экрана. Отвечать на вопросы лучше всего, начиная с первого раздела “Политика безопасности. Организационные меры”. Оцените систему безопасности выбранной организации, учтите как можно больше недостатков,

так как полное описание организационных мер обеспечения информационной безопасности для представленных вариантов не представляется возможным. Нажмите кнопку “Далее”.

6. Перед вами окно с определением доступа пользователей к информационным ресурсам. Ограничьте доступ к информации на первой выбранной станции. К тем же видам информации на второй рабочей станции, определите разные виды доступа пользователей. На остальных серверах и рабочих станциях виды доступа определите сами.

7. Теперь на экране должно появиться окно для ввода затрат на информационную безопасность. Затраты можно определить из вашего варианта. Это заключительный этап сбора информации о вашей организации. Далее программа генерирует отчет по результатам анализа.

8. Ознакомьтесь с представленным отчетом. Сравните риск и ущерб по трем классам угроз. Оцените на ваш взгляд эффективность системы защиты. Перейдите к вкладке “Анализ рисков”. Сравните данные о риске по трем классом угроз на рабочих станциях , к информации на которых был представлен доступ и к которым нет. Сделайте выводы.

9. Перейдите к вкладке “Проверка организационных мер”. Посмотрите, какое количество организационных мер соответствуют положениям стандарта, и какое нет. Далее вам предстоит ознакомиться с основными положениями международного стандарта безопасности ISO 17999.

10. Сделайте скриншоты трех вкладок отчета и сохраните их в своей отчет по лабораторной работе. Закройте окно программы. Снова откройте файл Project.exe. Повторите 3 и 4 пункт. Попытайтесь в 5 пункте соблюсти как можно больше положений МСБ ISO 17999. Далее повторите 7, 8, 9 пункт. Сделайте выводы.

Контрольные вопросы

1. Дайте определение понятия - Политика информационной безопасности.
2.Что такое процесс анализа рисков? Какова роль анализа рисков в процессе формирования политики безопасности компании.
3. В чем отличие полного анализа рисков от базового?
4.Что понимается под угрозой безопасности информации?
5.На какие два класса делиться все множество потенциальных угроз безопасности информации?
6.В чем заключается оценка рисков по двум факторам?
7.В чем заключается оценка рисков по трем факторам?
8. Дайте определение понятию “Уязвимость”.
9.Дайте определение понятиям “угроза конфиденциальности”, ”угроза целостности” и “угроза доступности”.
10. Назовите основные разделы стандарта ISO 17799.

6. Рекомендуемая литература

1. Егоров Н.А. Комплексная защита информации в компьютерных системах. Учебное пособие. - М.: Логос, 2001. - 264 с.
2. Программный комплекс анализа и контроля рисков информационных систем компаний “Гриф”[Электронный ресурс].Компании Digital Security. http://www.dsec.ru.
3. Программный комплекс проверки политики информационной безопасности компании “Кондор+” [Электронный ресурс]. Компании Digital Security http://www.dsec.ru.
4. Интрасети: Доступ в Интернет, защита /Милославская Н.Г., Толстой А.И. Учебное пособие для вузов . - М.: ЮНИТИ-ДАНА, 2000. – 527 с.
5. Домарев В.В. Защита информации и безопасность компьютерных систем. - Киев: Изда-во "ДиаСофт", 1999. - 480 с.
6. Информационные технологии. Практическое правило управления информационной безопасность. Русский перевод стандарта ISO 17799 [Электронный ресурс].
7. Cobra и КОНДОР [Электронный ресурс].
8. Методики и технологии управления информационными рисками. [Электронный ресурс] // Журнал «IT Manager», №3/2003.
9.Аудит безопасности фирмы: теория и практика: Учебное пособие.- М.: Академический Проект «Парадигма», 2005. - 352 с.
10. Основы безопасности информационных технологий, 2001. //http://www.crime-research.ru.