МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему Разработка методики организации управления информационной безопасностью в телекоммуникационной сети

Исполнитель Ощутинская Ольга Игоревна
(фамилия, имя, отчество)

Руководитель _____
(ученая степень, ученое звание)

Яготинцева Наталья Владимировна
(фамилия, имя, отчество)

«К защите допускаю»
Заведующий кафедрой _____
(подпись)

профессор, доктор технических наук
(ученая степень, ученое знание)

Бурлов Вячеслав Георгиевич
(фамилия, имя, отчество)

«17» февраля 2017 г.

Санкт–Петербург
2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему Разработка методики организации управления информационной безопасностью в телекоммуникационной сети

Исполнитель Ошутинская Ольга Игоревна
(фамилия, имя, отчество)

Руководитель
(ученая степень, ученое звание)

Яготинцева Наталья Владимировна
(фамилия, имя, отчество)

«К защите допускаю»
Заведующий кафедрой
(подпись)

профессор, доктор технических наук
(ученая степень, ученое знание)

Бурлов Вячеслав Георгиевич
(фамилия, имя, отчество)

«_ »_____2017 г.

Санкт–Петербург
2017

Оглавление

Введение

С возникновением Интернета и Windows как часто используемого продукта появилась проблема управления информационной безопасностью. Заполучив доступ к новым технологиям, хакеры стали активно использовать их с целью украсть данные кредитных карт и других видов мошенничества.

Для того, чтобы качественно управлять информационными рисками, специалисты разработали методики, такие как:

– ISO 15408;

– ISO 17799 (BS7799);

– BSI;

– NIST 80030;

– SAC;

– COSO;

– SAS 55/78.

Актуальностью данной работы является разработка продуктивных моделей и методов управления информационной безопасностью телекоммуникационной сети, для уменьшения преступности в сети Интернет.

Целью выпускной квалификационной работы является разработка методики, которая будет регламентировать правила управления информационной безопасностью в телекоммуникационной сети.

Задачи:

– Анализ методов и средств защиты информации телекоммуникационной сети;

– Анализ методов и моделей управления информационной безопасностью;

– Разработать методику организации управления информационной безопасностью телекоммуникационной сети.

Решение данных задач осложняется большим количеством факторов, которые влияют на их выполнение. Самые значимые из них:

– необходимость совмещения технических условий для объединённой работы программных продуктов и оборудования разнообразных производителей;

– необходимость продуктивного использования каналов связи и выполнения условий электромагнитной совместимости;

– необходимость учета перспектив модернизации системы;

– себестоимость и другие.

Разумеется, что в основе решения задач лежат требования международных стандартов и рекомендаций. Обязательным требованием для принятия решения считается выполнение условий национального законодательства, которое регламентирует эту сферу деятельности.

Объектами исследования в работе являются информационная безопасность телекоммуникационной сети и ее управление.

1 Определение области действия системы управления информационной безопасностью телекоммуникационной сети

1.1 Управление информационной безопасностью

Процесс, обеспечивающий конфиденциальность, целостность и доступность информации, активов, услуг организации и ее данных, называется управлением информационной безопасностью.

Управление информационной безопасностью считается одной из составляющих организационного подхода по отношению к управлению безопасностью. Его главной задачей является выполнение продуктивного управления информационной безопасностью всех услуг. Для того, чтобы информация, информационные системы и коммуникации оставались защищенными от воздействия на конфиденциальность, целостность и доступность, существует информационная безопасность.

«Конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

Целостность – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Доступность – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.» [1]

Цель обеспечения информационной безопасности достигается, если:

– информация является доступной в определенное время, а информационные системы неуязвимы по отношению к атакам, способны уйти от них или мгновенно восстановиться;

– доступ к информации получают только те, кто имеет на это соответствующее право;

– информация является корректной, полной и защищенной от неавторизованных поправок.

– обмен информацией с партнерами и другими предприятиями находится под надежной защитой.

Чтобы обеспечение информационной безопасности было целостно и эффективно, нужно рассмотреть процессы полностью, потому что слабое звено может стать проблемой для всей системы.

Процесс управления информационной безопасностью состоит из:

– управления, формирования, распространения и соблюдения Политики информационной безопасности и иных вспомогательных политик, имеющих отношение к информационной безопасности. Политикой информационной безопасности называется та политика, которая определяет подход предприятия к управлению информационной безопасностью;

– понимания согласованных требований предприятия к безопасности; использования контролей безопасности, необходимых для выполнения Политики информационной безопасности и управления рисками, которые связаны с доступом к системам, услугам и информации. Термин «контроль безопасности» в данном случае означает набор контрмер и мер предосторожности, которые аннулируют и уменьшают риски, а также имеют способность противостоять им. Из вышесказанного следует, что контроль безопасности включает в себя проактивные и реактивные действия;

– документирования списка контролей безопасности, действий по их использованию и руководству, а также привязанных к ним рисков;

– контроля всех утрат безопасности и недоразумений, которые связаны с системами и услугами;

– проактивного усовершенствования контролей безопасности и уменьшения возможности возникновения рисков ущерба информационной безопасности;

– интеграции основ информационной безопасности во все операции Управления услуг.

Политика информационной безопасности состоит из:

– реализации основ политики информационной безопасности;

– возможных злоупотреблений основами политики информационной безопасности;

– политики контроля доступа;

– политики эксплуатации паролей;

– политики электронной почты;

– политики Интернета;

– политики антивирусной защиты;

– политики ранжирования информации;

– политики ранжирования документов;

– политики удаленного доступа.

Политика информационной безопасности должна быть утверждена IT-отделом и руководством, она пересматривается только при определенных обстоятельствах.

Необходимость поддержания системы управления информационной безопасности нужно для обеспечения информационной безопасности и управления ею.

«Системой управления информационной безопасностью называется система процессов, руководящих документов, политик, стандартов и средств, которые помогают предприятию достигнуть цель управления информационной безопасностью.» [20] На рисунке 1 представлена структура системы управления информационной безопасностью, которая широко используется предприятиями.

Рисунок 1 – система управления информационной безопасностью

На рисунке 1 представлены пять составляющих структуры системы управления информационной безопасностью:

1) Контроль. Целями контроля являются:

– создание системы управления информационной безопасностью в пределах предприятия;

– создание организационной структуры для реализации, утверждения и подготовки Политики информационной безопасности;

– назначение ответственностей;

– создание документации по контролю.

2) Планирование. Целями планирования являются разработка и рекомендация, годящиеся метрики и методы измерения информационной безопасности. Изначально планирование учитывает особенности и условия конкретного предприятия. К источникам информации для создания требований к информационной безопасности относятся планы, соглашения, стратегии и риски. В контексте информационной безопасности учитываются этическая, законодательная и моральная ответственности.

3) Реализация. Целью реализации является обеспечить подходящие инструменты, контроли и процедуры безопасности для удержания Политики информационной безопасности.

Мероприятия, проводимые в пределах реализации:

– распознавание активов вместе с управлением конфигурациями;

– классификация информации – информационные хранилища и информация классифицируются в соответствии с их значимостью и чувствительностью по отношению к доступности, целостности и конфиденциальности.

4) Оценка. Целями оценки в пределах системы управления информационной безопасностью являются:

– проверка соответствия политики информационной безопасности требованиям к информационной безопасности из SLA и OLA. (SLA – это формальный договор между заказчиком услуги и её поставщиком, который содержит описание услуги, согласованный уровень качества предоставления этой услуги, права и обязанности сторон. OLA – это соглашение между поставщиком ИТ-услуг и другой частью того же предприятия о предоставлении услуг);

– проведение постоянных проверок технической составляющей информационной безопасности для IT-систем;

– предоставление информации для внешних аудиторов и регуляторов при необходимости;

5) Поддержка. Целями поддержки являются:

– усовершенствование соглашений в отношении информационной безопасности, такие как, OLA и SLA;

– улучшение контролей и средств информационной безопасности.

Ключевыми деятельностями в пределах ISM являются:

– формирование, пересмотр и исправление Политики информационной безопасности и набора вспомогательных политик;

– воплощение и выполнение политик информационной безопасности, вдобавок обеспечение их взаимодействия;

– классификация и оценка всех информационных активов и документов;

– применение, пересмотр и исправление набора контролей безопасности, мер по оценке рисков и ответных действий;

– мониторинг и управление утратами безопасности и инцидентами;

– анализ, ведение отчетности и уменьшение влияния утрат в безопасности и инцидентов;

– разработка расписания и проведение аудитов, тестирования и обзоров.

На рисунке 2 представлены ключевые деятельности в пределах ISM.

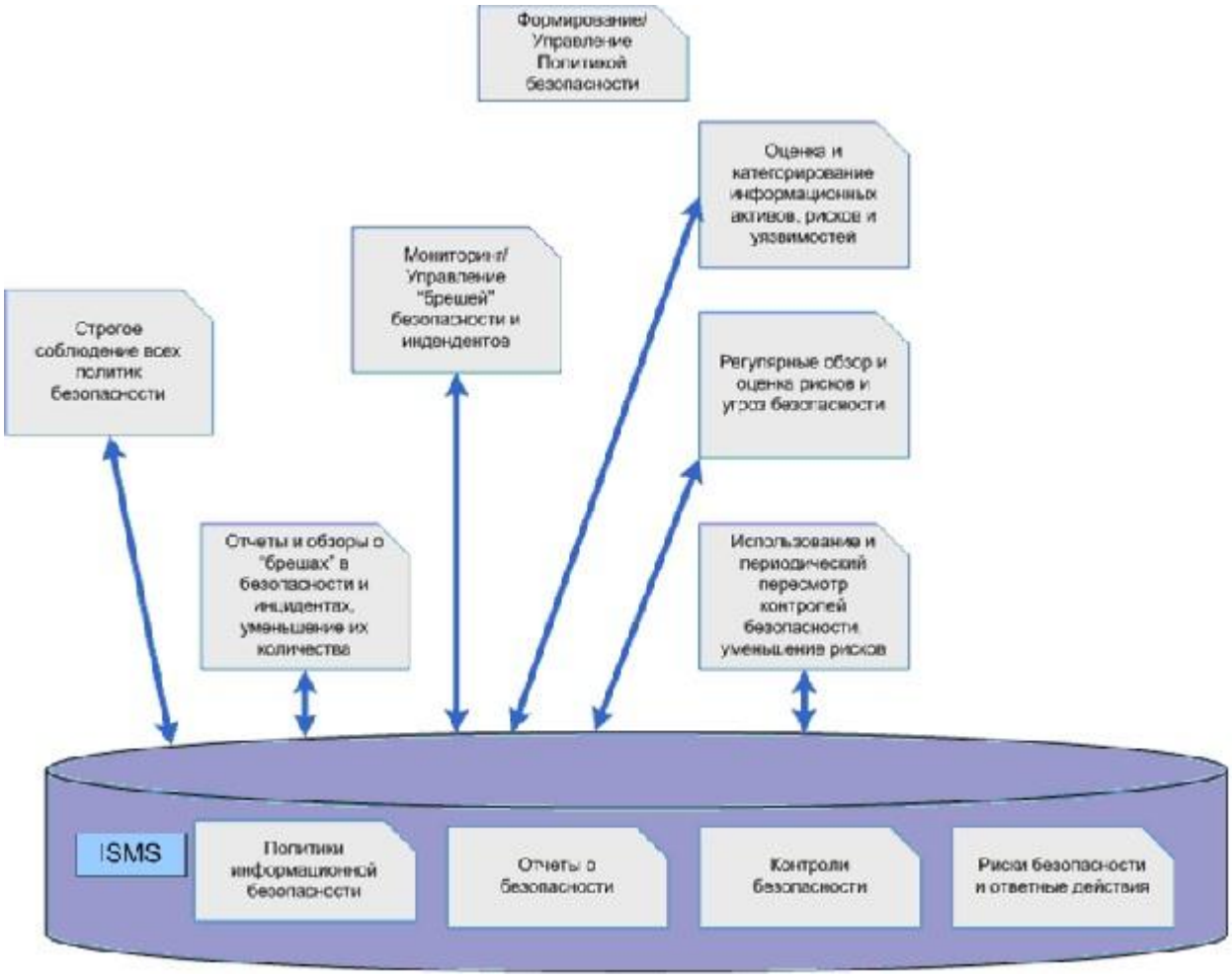

Рисунок 2 – Ключевые деятельности в пределах ISM

Чтобы обеспечить и поддержать Политику информационной безопасности, нужно сформировать и использовать набор контролей

безопасности. Меры безопасности, используемые для устранения инцидентов и верного реагирования при их появлении, представлены на рисунке 3.

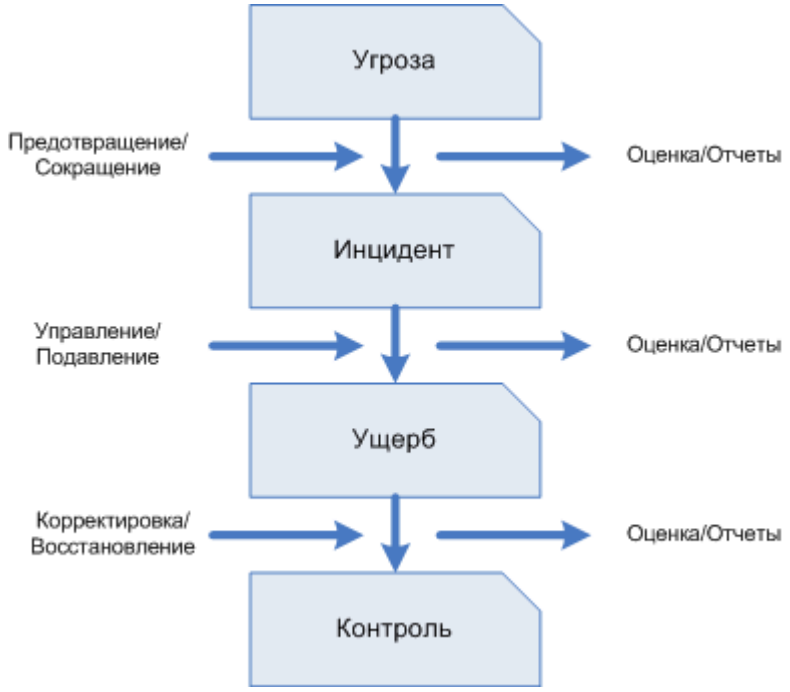

Рисунок 3 – Контроли безопасности

На рисунке 3 представлены четыре стадии.

1) Появление угрозы. Угроза – это все, что неблагоприятно влияет на процесс и прерывает его.

2) Инцидент. Инцидент – это осуществленная угроза. Инцидент является причиной для того, чтобы начать осуществлять контроль безопасности.

3) Результатом инцидента является ущерб.

4) Чтобы управлять или устранять риски применяют контроли безопасности.

Каждой стадии нужно подбирать подходящие меры обеспечения информационной безопасности.

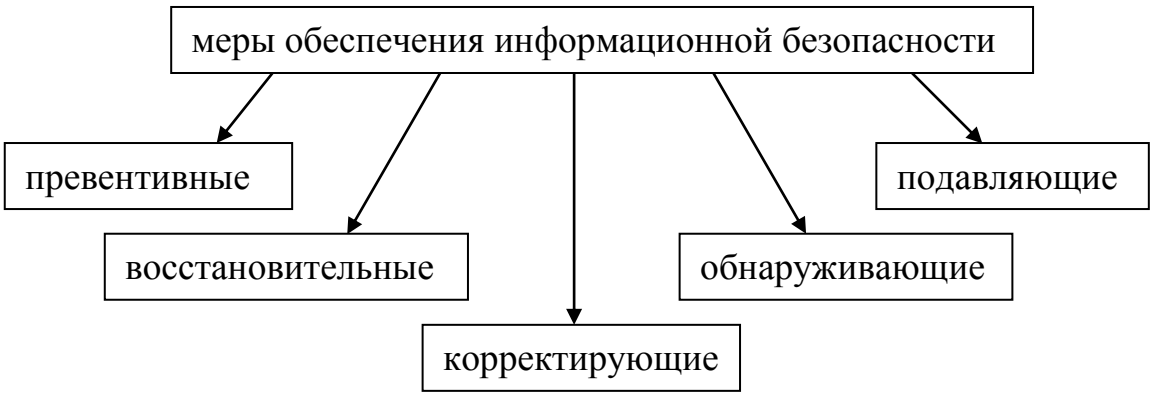

Рисунок 4 – меры обеспечения информационной безопасности

«Превентивные – меры безопасности, которые предотвращают появление инцидента информационной безопасности. Например, распределение прав доступа.

Восстановительные – меры безопасности, направленные на уменьшение потенциального ущерба в случае инцидента. Например, резервное копирование.

Обнаруживающие – меры безопасности, направленные на обнаружение инцидентов. Например, антивирусная защита или система обнаружения вторжений.

Подавляющие – меры безопасности, которые противодействуют попыткам реализации угрозы, то есть инцидентам. Например, банкомат забирает у клиента карту после определенного количества неправильных вводов PIN-кода.

Корректирующие – меры безопасности, направленные на восстановления после инцидента. Например, восстановление резервных копий, откат на предыдущее рабочее состояние и т.п.» [2]

Чтобы оценить риск информации, нужно проанализировать все угрозы, действующие на информационную систему, и уязвимости, благодаря которым возможно выполнение угроз. Смотря на введенные данные владельцем информационной системы, возможно создать модель угроз и уязвимостей, которые актуальны для информационной системы предприятия. Из построенной модели проводится анализ вероятностей выполнения угроз информационной безопасности на ресурсы и в итоге проводятся расчеты рисков.

Базовой угрозой информационной безопасности является ущерб целостности, ущерб конфиденциальности и отказ в обслуживании.

Ресурсом является любой контейнер, который предназначен для хранения информации, который подвержен угрозам информационной безопасности. Например, рабочая станция, сервер или переносной компьютер.

Свойства ресурса: перечень угроз, которые воздействуют на него, и критичность ресурса.

Угрозой является действие, приведшее к нарушению безопасности. Свойство угрозы: перечень уязвимостей, при которых будет реализована угроза.

Уязвимостью является слабое место в информационной системе, приведшее к нарушению безопасности путем выполнения некоторой угрозы. Свойства уязвимости: вероятность и критичность выполнения угрозы через данную уязвимость.

«Телекоммуникационной сетью является передающая среда, которая заканчивается проводной линией, которая предназначена для связи между оборудованием, размещенным в различных зданиях, исключая:

– магистральную систему для электропитания, передачи и распределения электрической энергии, если она используется как передающая среда связи;

– системы кабельного распределения;

– цепи БСНН (безопасность сверхнизкого напряжения), которая соединяет модули оборудования обработки данных.» [29]

Классификация телекоммуникационной сети:

– общественная или частная;

– подвергнутая перенапряжениям от переходных процессов, которые вызваны атмосферными разрядами и испорченностями в системах электропитания;

– подвергнутая продольным напряжениям, которое наводится от проходящих рядом линий электросети или городского электротранспорта.

Рисунок 5 – примеры телекоммуникационных сетей

1.2 Методы и средства защиты информации

1.2.1 Традиционные меры и методы защиты информации

Что обеспечить безопасность информации в офисных сетях нужно провести различные мероприятия, которые объединяются понятием «система защиты информации». Системой защиты информации является совокупность мер, программно-технических средств, морально-этических и правовых норм, которые направлены на противодействие угрозам нарушителей, чтобы свести до минимума возможный ущерб пользователям и владельцам системы.

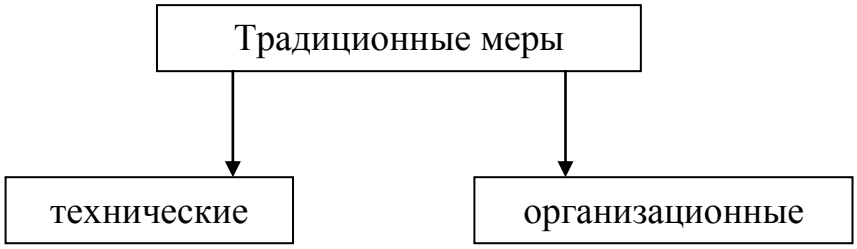

Рисунок 6 – традиционные меры

«К техническим мерам относятся:

– защита от НСД к системе;

– резервирование особо важных компьютерных подсистем;

– организация вычислительных сетей с возможностью перераспределения ресурсов, когда нарушена работоспособность отдельных звеньев;

– установка оборудования обнаружения и тушения пожара;

– установка оборудования обнаружения воды;

– принятие конструкционных мер защиты от саботажа, взрывов, диверсий и хищений;

– установка резервных систем электропитания;

– оснащение помещений замками;

– установка сигнализации и другое.

К организационным мерам относятся:

– охрана серверов;

– тщательный подбор персонала;

– исключение случаев ведения особо важных работ только одним человеком;

– наличие плана восстановления работоспособности сервера после выхода его из строя;

– универсальность средств защиты от всех пользователей.» [3]

«Когда проходит профилактика или ремонт компьютера, может произойти несанкционированный доступ к информации за счет того, что будет прочтена остаточная информация на носителе, несмотря на то, что она была удалена пользователем обычным методом. Есть и другой способ, когда может произойти несанкционированный доступ к информации. Например, будет прочтена информация с носителя в то время, когда его будут транспортировать без охраны внутри объекта или региона.» [21]

Интегральные схемы сейчас являются основой современных компьютерных средств. В цепях питания, в близкорасположенной аппаратуре, в эфире образовываются электромагнитные поля и наводки, трансформируемые в обрабатываемую информацию. Поля появляются благодаря тому, что при работе интегральных схем образуются высокочастотные изменения уровней токов и напряжения. Если расстояние между аппаратным средством и приемником нарушителя уменьшается, то вероятность того, что информация снимется и расшифруется, увеличивается.

«Кража» информации также может произойти, если нарушитель подключит «шпионские» средства к сетевым аппаратным средствам и каналам связи.

Идентификация, защита паролями и аутентификация считаются самыми обычными средствами защиты информации.

Аутентификация и идентификация. Информация, находящаяся в компьютере, по праву принадлежит только тем людям, которые находятся в той или иной должности. Для обеспечения безопасности информации, устранения вероятности несанкционированного доступа, усиления контролирования санкционированного доступа, устанавливаются системы,

которые опознают, подтверждают подлинность объекта или субъекта и разграничивает доступ. Основой таких систем является принцип допуска и исполнения тех обращений к информации, где присутствуют разрешенные полномочия.

Идентификация и аутентификация являются главными понятиями системы. Идентификацией называется тот процесс, когда любому объекту или субъекту присваивается определенное имя или образ. А аутентификацией называется процесс, в котором устанавливается подлинность, то есть проверяется, объект или субъект действительно тот, за кого он себя пытается выдать.

Конечной целью процессов аутентификации и идентификации является пропуск объекта или субъекта к информации не всеобщего пользования, если проверка положительна, или отказ, если проверка отрицательна.

Объектами идентификации и аутентификации являются:

– люди (операторы, пользователи и др.);

– технические средства (рабочие станции, мониторы, абонентские пункты);

– документы (распечатки, ручные и др.);

– магнитные носители информации;

– информация из экрана мониторов и др.

Подлинность объекта устанавливается при помощи аппаратного устройства, программы или человека.

Защита паролями. Паролем называется сочетание символов, которые определяют объект или субъект. Когда выбирается пароль, появляются проблемы с тем, чтобы его размер, стойкость к взлому были достаточны высоки. Если пароль длинный, то вероятность того, что его взломают и угадают, будет маленькой. Длина пароля также зависит от развития технических средств, их быстродействия и элементной базы.

Также нужно периодически менять пароль, чтобы он не был перехвачен, скопирован или похищен. Обычно пользователь вводит пароль в

самом начале сеанса, в редких случаях в конце (если это особо важная или секретная информация). В последнем случае, входной пароль отличается от выходного. В некоторых случаях, пароль запрашивается через определенное время несколько раз.

Пароль используется с целью идентифицировать и установить подлинность терминала, с которого пользователь заходит в систему, а также, чтобы установить подлинность компьютера в отношении к пользователю.

Чтобы идентифицировать пользователя применяются системы, которые сложны в плане технической реализации, чтобы обеспечить проверку подлинности по его индивидуальным данным, таким как, отпечатки пальцев, рисунок линии рук, тембр голоса, радужная оболочка глаз.

В наше время широко распространены физические методы проверки с эксплуатированием носителей кодов паролей. Например, пропуск в контрольно-пропускных системах; именные пластиковые карты, на которых находится имя владельца и его подпись; пластиковые карты с магнитной полоской; пластиковые карты, в которые встраивается микросхема (smart-card); карта оптической памяти и др.

Рисунок 7 – средства защиты

Программные средства защиты информации – это намерено разработанные программы, реализующие функцию безопасности вычислительной системы, осуществляющие функцию ограничения доступа пользователей по паролям, ключам, многоуровневому доступу и т.д. такие программы используются почти в любой операционной системе, которая удобна для пользователя. Такие программные средства созданы для того,

чтобы обеспечить высокую степень защиты системы, и приобрести их можно за достаточно умеренную цену. Если эта система подключается в глобальную сесть, то вероятность того, что защита взломается, намного увеличивается. Поэтому, такие системы защиты лучше использовать в локальных замкнутых сетях, которые не имеют внешний выход.

Программно-аппаратные средства – это устройства, которые реализуются на специализированных или универсальных микропроцессорах, которые не требуют модификаций в схемотехнике, когда алгоритм функционирования измеряется. Такие средства могут легко адаптироваться в разных операционных системах, но они намного лучше защищены. Но их цена немного дороже, варьируется от вида операционной системы. Этот типа средств считается более гибким инструментом, он позволяет внести изменения по любому требованию пользователя. Программно-аппаратные средства способны обеспечить высочайшую степень защиты локальной сети, которая подключается к глобальной сети.

Аппаратные средства – это устройства, реализующие функциональные узлы на сверхбольших интегральных системах (СБИС) с неизменяемым алгоритмом функционирования. Такие средства могут использоваться в различной операционной системе. Цена за них самая высокая. И они вменяют высокие технологические требования на производстве. Но так как их степень защиты лучшая, они обладают иммунитетом к внедрению значимых изменений. Но их использование мало, так как стоимость средств высока и сложна статичность алгоритма.

Программно-аппаратные средства уступают аппаратным в скорости своей работы, но позволяют с легкостью модифицировать алгоритм функционирования, и у них нет тех недостатков, которые имеют программные методы.

К иной группе мер, позволяющих обеспечить сохранность информации и выявить несанкционированные запросы, можно отнести программы обнаружения нарушений в режиме реального времени.

1.2.2 Криптографические методы и средства защиты информации

Ниже представлены направления прикладных и теоретических исследований, которые обладают наивысшим интересом:

– анализ и создание надежности криптографических протоколов и алгоритмов;

– адаптация алгоритмов к любым программным и аппаратным платформам;

– эксплуатирование уже существующих технологий криптографии в новейших прикладных системах;

– возможность использовать технологии криптографии, чтобы защитить интеллектуальную собственность.

Кроссплатформные телекоммуникационные системы создаются на основе единых стандартов на алгоритмы, благодаря интересу к исследованиям адаптации алгоритмов. По закону, алгоритму следует результативно использоваться на любых платформах, как на мобильном телефоне, так и на компьютере.

Средства защиты информации по принципу построения системы аутентификации и ключевой системы делятся на две группы. К первой группе можно отнести средства, которые используют при построении системы аутентификации и ключевой системы симметричные криптоалгоритмы, ко второй можно отнести те, что используют асимметричные.

Для того, чтобы это выяснить, можно провести сравнительный анализ вышеописанных систем. Информация, которая готова к передаче, изначально открыта и незащищена. Она зашифровывается и становится шифрограммой (скрытым текстом или скрытым графическим рисунком исходного документа). В виде шифра он переносится по незащищенному каналу связи. Разрешенный пользователь, после того, как получит это сообщение, расшифровывает его, с помощью обратного преобразования криптограммы.

После этого, выходит начальный вид сообщения, который является открытым, и который доступен для разрешенного пользователя.

Эксплуатирование особого алгоритма подходит методу преобразования в криптографической системе. Действие этого алгоритма начинается особым числом (последовательностью бит), которое называется шифрующим ключом. Отправитель и получатель должен знать особый шифр, и хранить его в секрете, с целью успешного обмена зашифрованной информации.

Безопасность различных систем скрытой связи устанавливается степенью скрытости ключа, который в ней используется. Но, этот самый секретный ключ должен быть узнаваем несколькими пользователями сети, с целью свободного обмена зашифрованной информацией. В этом случае криптографические системы помогают при решении проблемы аутентификации (проверки подлинности) полученной информации. При попытке кражи информации, несанкционированный пользователь получит только шифр, в то время, как санкционированный пользователь будет железно защищен от дезинформации.

Также, информацию можно зашифровать наиболее простым путем – с использованием генератора псевдослучайных чисел. «Использование генератора псевдослучайных чисел заключается в генерации гаммы шифра с помощью генератора псевдослучайных чисел при определенном ключе и наложении полученной гаммы на открытые данные обратимым способом. Этот метод криптографической защиты реализуется достаточно легко и обеспечивает довольно высокую скорость шифрования, однако недостаточно стоек к дешифрованию.» [4]

Эксплуатация ключа, позволяющего зашифровать и расшифровать сообщение, как одной тайной единицы, характерно для самой обычной классической криптографии. Если данные находятся на носителе и их нужно зашифровать, то ключ может позволить произвести шифрование при записывании на носитель, а также произвести расшифровку при чтении с него.

Из вышесказанного можно сделать вывод, что безопасная и надежная криптографическая система должна соответствовать некоторым требованиям:

– процессы шифровки и расшифровки должны быть понятны для пользователя;

– дешифровке скрытых данных следует быть максимально затрудненной;

– содержание передаваемых данных не должно оказывать влияние на производительность криптографического алгоритма.

Асимметричные криптосистемы (системы с открытым ключом) в наше время являются самыми лучшими системами криптографической безопасности. Смысл системы – ключ, который используется для шифровки, отличается от ключа, который используется при расшифровке. Но в этому случае, ключ шифрования известен пользователям всей системы. Однако, расшифровать данные с помощью ключа шифровки невозможно. Для того, чтобы расшифровать информацию, используется секретный ключ, который известен определенному кругу лиц. Если пользователь знает открытый ключ, мала вероятность того, что он сможет определить скрытый ключ. Это означает, что расшифровать данные сможет только тот, кто владеет скрытым ключом.

Ученые считают, что системы с открытым ключом больше созданы для передачи данных, нежели для защиты информации.

В наше время, люди все чаще пытаются защитить какую-либо информацию, что повышает желание специальных государственных служб возможность получить доступ к этой скрытой информации, с целью пресечения незаконной деятельности.

Криптография дает возможность обеспечить безопасность информации в сети Интернет и в наше время активно ведутся исследования по внедрению нужных криптографических механизмов в эту сеть.

1.2.3 Нетрадиционные методы защиты информации

В наше время потребности информатики привели к тому, что возникли нетрадиционные задачи защиты электронной информации. Пример таких задач – аутентификация электронных данных тогда, когда пользователи, которые обмениваются информацией, не имеют доверия по отношению друг другу. Благодаря этой проблеме была создана система электронной цифровой подписи.

Для русской литературы характерны три термина:

– электронная подпись;

– электронно-цифровая подпись (ЭЦП);

– цифровая подпись.

«Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, а также организации, участвующие в документообороте с указанными органами, используют для подписания своих электронных документов электронные цифровые подписи уполномоченных лиц указанных органов, организаций.

Содержание документа на бумажном носителе, которое заверяется печатью и преобразовывается в электронный документ, в соответствии с нормативными правовыми актами или соглашением сторон, может заверяться электронной цифровой подписью уполномоченного лица.

В случаях, которые устанавливаются законами и иными нормативными правовыми актами Российской Федерации или соглашением сторон, электронная цифровая подпись в электронном документе, сертификат которой содержит необходимые при осуществлении данных отношений сведения о правомочиях его владельца, признается равнозначной собственноручной подписи лица в документе на бумажном носителе, заверенном печатью.» [5]

Электронной цифровой подписью называется реквизит электронного документа, который предназначается для безопасности данного электронного документа от подделки.

Последовательность символов, которые получаются при криптографическом преобразовании электронных данных, называется электронной цифровой подписью. Подпись присоединяется ко всем данным по пользователю и дает возможность получателю данных проверить подлинность отправителя. ЭЦП является аналогом собственноручной подписи. Это допускается, если:

– сертификат ключа подписи не потерял свою силу на момент. «Сертификат ключа подписи – это документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи» [6];

– подлинность ЭЦП подтверждается. Подтверждение подлинности ЭЦП в электронном документе означает положительный результат аутентификации с использованием сертификата ключа подписи;

– электронная цифровая подпись используется в соответствии со сведениями, которые указаны в сертификате ключа подписи.

ЭЦП является средством, которое обеспечивает конфиденциальность информации.

Определение человека по собственноручной подписи проверяется с помощью судебно-почерковедческой экспертизы, которая помогает решить задачу по идентификации подписи.

Идентификация ЭЦП означает только то, что человек, поставивший эту подпись, знает закрытый ключ.

1.3 Информационная безопасность предприятия

1.3.1 Концепция информационной безопасности предприятия

Отличительной особенностью коммерческой деятельности от всех остальных считается сравнение доходов и расходов, желание получить максимальную прибыль. Также, наверное, главным признаком коммерческой деятельности считается то, что она существует в условиях жесткой конкуренции. Конкуренция – двигатель коммерческой деятельности, условие выживания предприятий. Тут то и возникает желание сохранить коммерческую тайну от своих конкурентов. Также у конкурентов появляется желание заполучить коммерческую тайну другого предприятия. «Кража» подобной информации без согласия владельцев называется промышленным шпионажем.

Уязвимость информации – неспособность информации самостоятельно противостоять воздействиям, которые нарушают ее установленный статус.

Уязвимость данных может проявляться в различных формах:

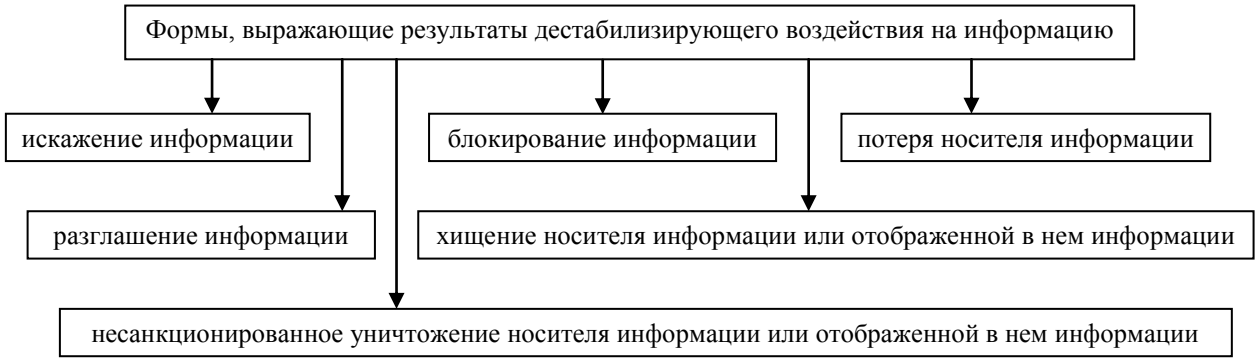

Рисунок 8 – формы уязвимостей

Любые формы уязвимости информации могут быть реализованы в итоге случайного или преднамеренного дестабилизирующего влияния разными способами на носители информации или на саму информацию со стороны причины влияния. Такие источники: люди, технические средства передачи и обработки информации, средства связи, стихийные бедствия и другие.

Способы дестабилизирующего влияния на информацию:

– копия, запись;

– съем, передача;

– заражение программы, когда обрабатывается информация вирусами;

– сбой технологии, когда обрабатывается и хранится информация;

– выход из строя режимов передач и обработок информации и другие.

Утечка или утрата информации являются видами уязвимости, которые становятся следствием реализации форм проявления уязвимости информации.

Потеря информации может произойти с помощью использования технических средств кражи информации.

«Существуют функциональные группы средств препятствованию случайной потери информации, причинами которых могут быть программно-аппаратные сбои или человеческие факторы. Например, копирование информации, улучшение надежности и применение отказоустойчивых компьютерных систем, более рациональное взаимодействие человека и компьютерных систем, уменьшение вреда от различных катаклизмов, запрет проведения неверных действий пользователя.» [24]

Несанкционированное уничтожение носителей информации или хранящейся на них информации, кража или утрата самих носителей, а также блокировка или изменение информации являются причинами потери информации. Потеря бывает полной или частичной, временной или безвозвратной, результат один и тот же – нанесение вреда собственнику информации.

Несанкционированным доступом является незаконное предумышленное завладение конфиденциальной информацией субъектом без права доступа к тем сведениям, которые охраняются.

«Самые распространенные пути НСД к информации:

– перехват электронных излучений;

– принудительное электромагнитное облучение линий связи с целью получения паразитной модуляции несущей;

– применение подслушивающих устройств;

– дистанционное фотографирование;

– перехват акустических излучений и восстановление текста принтера;

– копирование носителей информации с преодолением мер защиты

– маскировка под зарегистрированного пользователя;

– маскировка под запросы системы;

– использование программных ловушек;

– использование недостатков языков программирования и операционных систем;

– незаконное подключение к аппаратуре и линиям связи специально разработанных аппаратных средств, обеспечивающих доступ информации;

– злоумышленный вывод из строя механизмов защиты;

– расшифровка специальными программами зашифрованной информации;

– информационные инфекции.» [7]

Вышеуказанные пути НСД требуют большие технические знания и соответствующие аппаратные или программные разработки со стороны злоумышленника. Для примера, использование технических каналов утечки, являющиеся физическими путями от источника конфиденциальной информации к недоброжелателю, вследствие которых будут получены охраняемые сведения. Технологические и конструктивные несовершенства схемного решения или полученный в результате эксплуатации износ элементов являются причинами возникновений каналов утечки. Вышеперечисленное дает возможность злоумышленникам создать преобразователи, которые действуют на таких же физических принципах, способных образовать подобные каналы передачи информации – каналы утечки.

Существуют примитивные пути НСД:

– кража носителей информации и документальных отходов;

– инициативное сотрудничество;

– побуждение к сотрудничеству со стороны злоумышленника;

– выведывание;

– подслушивание;

– слежка и другие.

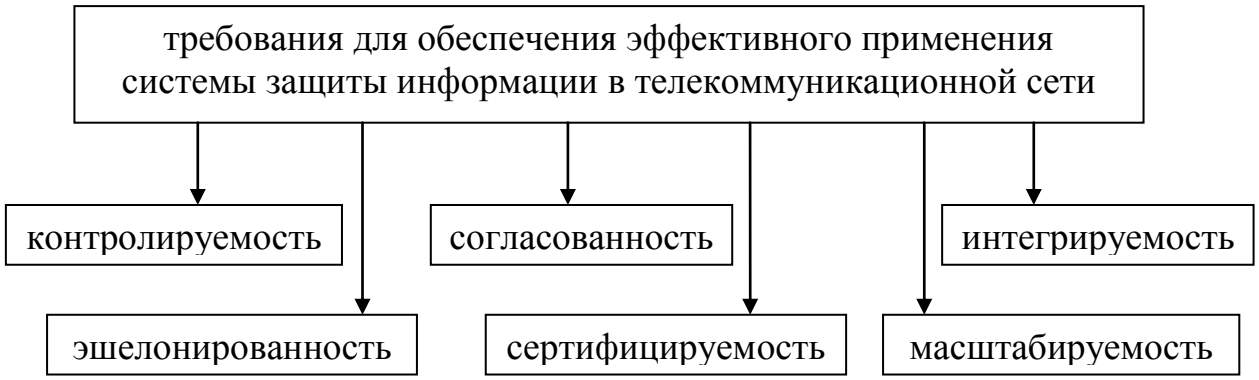

Рисунок 9 – требования для обеспечения эффективности применения защиты

Эшелонированность. У системы защиты есть несколько уровней. Когда защита на каком-нибудь уровне нарушается, другие уровни при этом не должны ослабевать и не должна нарушаться система защиты в целом.

Согласованность. Средства защиты обеспечивают возможность их использования в пределах единой системы, даже если они входят в региональную составляющую телекоммуникационной сети организации.

Интегрируемость. Средства защиты данных оптимально встраиваются в структуру телекоммуникационной сети.

Контролируемость. События, которые связаны с деятельностью систем защиты, контролируется средствами мониторинга безопасности.

Сертифицируемость. Средства, которые применяются при создании системы защиты, удовлетворяют учрежденным требованиям и стандартам.

Масштабируемость. Когда система защиты создается, одновременно должна обеспечиваться возможность ей развиваться вместе с развитием телекоммуникационных сетей организации.

1.3.2 Методы защиты информации в телекоммуникационных сетях предприятия

Если рассматривать защиту информации с точки зрения отраслевого стандарта по информационной безопасности, то ее можно определить, как функционирование, которое служит для снижения вероятности утечки информации, воздействий на информацию извне. Если при ликвидации

утечки данных засекреченная информация подлежит огласке, то задача остальных двух направлений – защитить от одинаковых угроз (блокировка доступа, удаление или изменение информации). Разница заключена в отсутствии или наличии умысла в действиях с данными (рисунок 10).

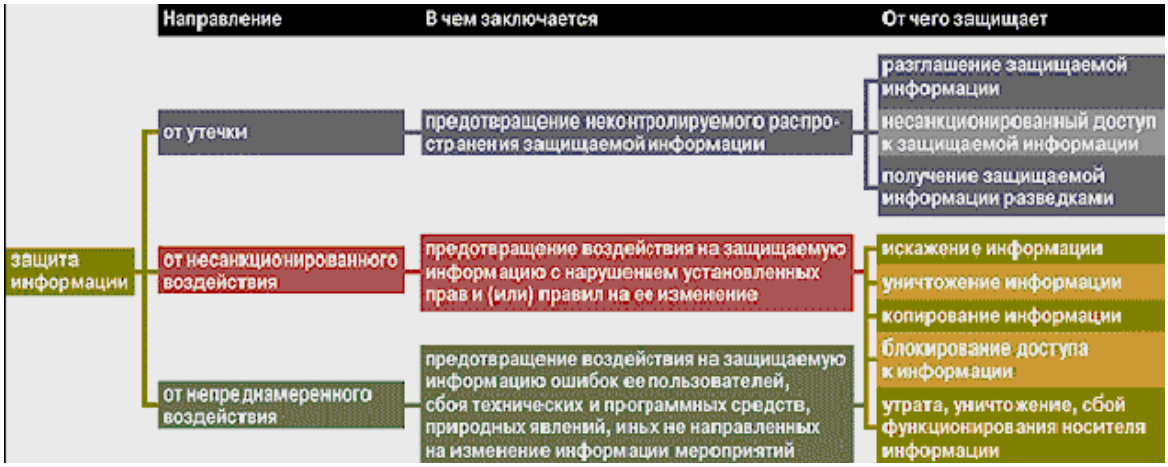

Рисунок 10 – Защита информации на предприятии

Самое большое количество угроз, как и раньше, возникает из-за компьютерных вирусов или атак людей, которые распространяют спам.

Большое количество сетей в наше время на протяжении долгого времени остаются незащищенными от пользователей Интернета. И в данном случае неизвестно, что является самым вредным – подсознательный взлом для кражи информации, или же заведомо организованная атака типа «отказа в обслуживании». Но так как малые и средние организации не создают специальные линии связи, которые защищены, они вынуждены эксплуатировать открытые каналы связи для обмена данными, что может привести к утечке информации.

В локальной сети актуальной задачей является создание безопасной аутентификации пользователей: приклеивание к компьютеру стикера с логином и паролем.

Очень часто в организации не разграничивается доступ между пользователями. Это можно разъяснить так: каждый сотрудник имеет свое место, и он не намеревается занять рабочее место начальства; а отношение к засекреченной информации можно объяснить, как «каждому – по

интересам», и данные, которые открыты нескольким менеджерам, открываются и для большей половины фирмы.

«Сервис-центры также можно обозначить, как центры утечки информации. К ним поступает большое количество носителей информации, на которых сохраняется не до конца удаленная секретная информация.» [23]

Исходя из этого, можно выявить, что залогом успешной работы организации является хорошо продуманная защита информации. Для этого ставятся следующие задачи:

– анализировать угрозы засекреченных данных, поиск слабых мест системы и их уничтожение;

– формировать систему защиты данных - закупать и устанавливать необходимые средства, осуществлять промежуточное тестирование;

– обучать сотрудников, как правильно работать с этими средствами, контролировать и соблюдать регламент их применения;

– разрабатывать технику действий в экстремальной ситуации и проводить постоянные «учения»;

– разрабатывать и реализовывать программу постоянной работы автоматизированной системы и план восстановительных мероприятий (например, при атаке вирусов, сбоя работ и т.п.).

Есть некоторые проблемы, которые появляются при создании системы защиты информации.

«Метод заплаток. «Кусочное» обеспечение информационной безопасности лишь на отдельных направлениях. Следствие – невозможность отразить атаки на незащищенных участках и дискредитация идеи информационной безопасности в целом.

Синдром амебы. Фрагментарное реагирование на каждый новый раздражитель. Часто сочетается с применением «метода заплаток». Следствие – запаздывание с отражением новых угроз, усталость от бесконечной гонки по кругу.

Лекарство от всего. Попытки возложить на одно средство защиты информации все функции обеспечения информационной безопасности (например, стремление отождествить аутентификацию и полный комплекс задач защиты от несанкционированного доступа). Следствие – непрерывный переход, миграция от одного средства защиты к другому, «более комплексному», последующее разочарование и паралич дальнейших действий.

Волшебная палочка. Вторая ипостась поисков «универсального лекарства», искреннее непонимание необходимости дополнения технических мер защиты организационными. Следствие – предъявление завышенных требований к системе или средству защиты.

Стремление к экономии. Желание построить систему защиты на беззатратной основе. Следствие – применение непроверенных и/или нелицензионных средств защиты, отсутствие поддержки со стороны производителей, постоянные попытки разобраться во всем самостоятельно, неэффективные и разорительные, как и любая самодеятельность.» [8]

Проблемы, которые связаны с повышением безопасности информационной сферы, бывают сложные, многоплановые и взаимосвязанные. Государство и общество должны оказывать постоянное, неослабевающее внимание. Постоянное приложение совместных усилий по улучшению средств и методов, которые позволяют верно оценить угрозу безопасности информационной сферы и надлежаще отвечать на них, побуждаются развитием информационных технологий.

Устранение НСД к засекреченной информации, которая циркулирует в телекоммуникационной сети военного и государственного управления, к национальной и международной информации правоохранительных организаций, которые борются с транснациональными организованными преступниками и международными террористами, а в банковских сетях главной задачей считается обеспечение безопасности глобальных данных.

На государственном и коммерческом уровнях в наше время все больше обращают внимание на защиту информации.

Защита информации – применение разных методов и средств, усвоение мер и реализация мероприятий для того, чтобы системно обеспечить надежность любого вида информации (хранимая, передаваемая, обрабатываемая).

Существуют основные задачи, обеспечивающие защиту данных в информационной системе и телекоммуникационной сети. Например:

– допущение к данным только аутентифицированных пользователей;

– проверка подлинности данных;

– защита от кражи данных в процессе их передачи по каналам связи;

– защита от искажения данных.

Защита информации означает:

– обеспечение физической целостности информации, а именно, не искажать и не уничтожать элементы информации;

– не подменять элементы данных при сохранении ее целостности;

– не дать получить информацию пользователям и процессам, которые не имеют соответствующие полномочия;

– удостовериться, что передаваемая информация будет использована только санкционированными пользователями.

Решить проблемы защиты электронной информации можно при помощи криптографического метода, который в свою очередь решает проблему автоматизированной обработки и передачи информации, находящейся под защитой.

Криптографическое преобразование информации считается самым эффективным способом сохранения конфиденциальности, целостности и подлинности информации. Только благодаря их совместной работе с техническим и организационным мероприятием обеспечивается защита от потенциальной угрозы.

2 Методы организации управления информационной безопасностью в телекоммуникационной сети

2.1 Управление информационной безопасностью

Обеспечением информационной безопасности называется непрерывный процесс, основное содержание которого является управление. ИБ невозможно обеспечить разовым мероприятием, поскольку средства защиты нуждаются в постоянном контроле и обновлении. Управлять информационной безопасностью означает управлять пользователями, рисками, ресурсами, средствами защиты и другими. Управление информационной безопасностью считается неотъемлемым элементом управления организацией и дает возможность коллективно пользоваться конфиденциальной информацией, которая обеспечивает ее защиту и защиту вычислительных ресурсов.

Управление информационной безопасностью считается циклическим процессом, который включает:

– осознания степеней необходимости защиты данных;

– сбор и анализ информации о состоянии информационной безопасности в компании;

– оценки информационного риска;

– планирования мер по обработкам риска;

– реализации и внедрения соответствующего механизма контроля;

– распределения ролей и ответственностей;

– обучения и мотивации сотрудников;

– оперативные работы по осуществлениям защитного мероприятия;

– мониторинг функционирований механизма контроля;

– оценки их эффективности и соответствующих корректирующих воздействий.

Чтобы обеспечить необходимый уровень безопасности, в организации создают комплексную систему управления информационной безопасностью

(СУИБ). Целью ее создания считается устранение или уменьшение ущерба, которое злонамеренно наносится несанкционированными пользователями или неумышленно наносится нерадивым персоналом организации в следствии нежелательных воздействий на информацию, ее носителей и процессы обработки.

«Согласно стандарту ISO 27001, система управления информационной безопасностью (СУИБ) - это та часть общей системы управления организации, основанной на оценке рисков, которая создает, реализует, эксплуатирует, осуществляет мониторинг, пересмотр, сопровождение и совершенствование информационной безопасности.» [9]

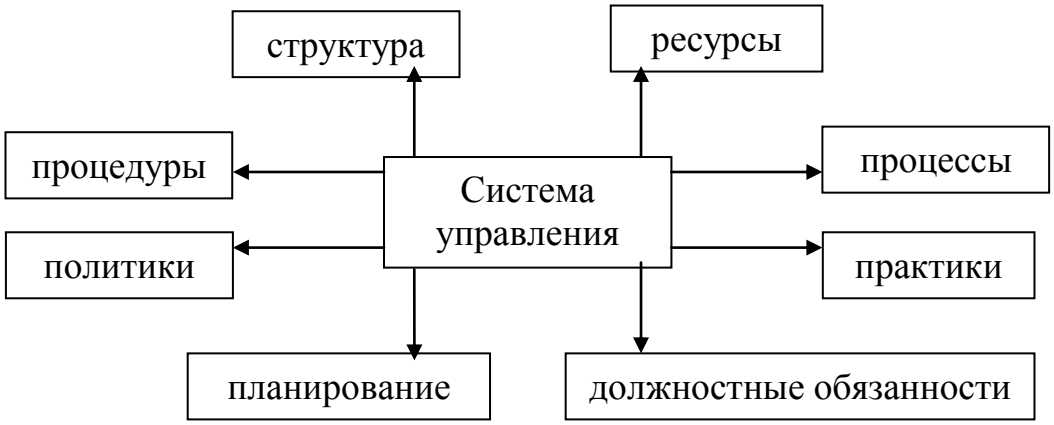

Рисунок 11 – система управления

Основная задача системы – обеспечить необходимый уровень доступности, целостности и конфиденциальности ресурсов ИС.

На основе внедрения СУИБ и ее сертификации на соответствие международным стандартам можно выделить такие преимущества организации, как:

– увеличение управляемости и надежности организации;

– увеличение защиты ключевых процессов организации;

– увеличение доверия к организации, как к партнерам, так и клиентам;

– соответствие требованиям международного стандарта дает возможность подчеркнуть чистоту и прозрачность организации;

– наличие системы управления информационной безопасностью и международного сертификата упрощает процедуру выхода организации на внешний рынок;

– международное признание и увеличение авторитета организации, как на внутренних, так и внешних рынках;

– увеличение прибыли.

Также появляются преимущества при внедрении системы управления информационной безопасностью и ее сертификации на соответствие международным стандартам для структурных подразделений организации:

– систематизация процесса обеспечения ИБ;

– распределение приоритетов организации в сфере ИБ;

– управление ИБ организации в пределах корпоративных политик;

– своевременные выявления и управления рисками;

– уменьшение количества рисков от внешней и внутренней угрозы;

– оптимизация управленческого процесса;

– увеличение продуктивности функционирования системы управления информационной безопасностью и защиты информационной системы;

– увеличение общей корпоративной культуры персонала и вывод управления организацией на новый уровень.

2.2 Важность и сложность проблемы информационной безопасности

Можно рассматривать информационную безопасность на разных уровнях (национальном, корпоративном, персональном, отраслевом), но она все равно останется главным аспектом интегральной безопасности.

Для того, чтобы это доказать, рассмотрим примеры.

«1) В Доктрине информационной безопасности Украины отмечено, что информационная безопасность является неотъемлемой составляющей каждой из сфер национальной безопасности. В то же время информационная безопасность является важной самостоятельной сферой обеспечения национальной безопасности. Именно поэтому развитие Украины как суверенного, демократического, правового и экономически стабильного

государства возможно только при условии обеспечения надлежащего уровня ее информационной безопасности.

2) Американский ракетный крейсер «Йорктаун» был вынужден вернуться в порт из-за многочисленных проблем с программным обеспечением (июль 1998). Таким оказался побочный эффект программы ВМФ США по максимально широкому использованию коммерческого программного обеспечения с целью снижения стоимости военной техники.

3) Заместитель начальника управления по экономическим преступлениям Министерства внутренних дел России сообщил, что российские хакеры с 1994 по 1996 год предприняли почти 500 попыток проникновения в компьютерную сеть Центрального банка России. В 1995 году ими было похищено 250 миллиардов рублей (ИТАР-ТАСС, АР, 17 сентября 1996 года).

4) Как сообщил журнал "Интернет уек" от 23 марта 1998 года, потери крупнейших компаний, вызванные компьютерными вторжениями, продолжают увеличиваться, несмотря на рост затрат на средства обеспечения безопасности. Согласно результатам совместного исследования Института информационной безопасности и ФБР, в 1997 году ущерб от компьютерных преступлений достиг 136 миллионов долларов, что на 36% больше, чем в 1996 году. Каждое компьютерное преступление наносит ущерб примерно в 200 тысяч долларов.

5) В феврале 2001 года двое бывших сотрудников одной из компаний, воспользовавшись паролем администратора, удалили с сервера файлы, составлявшие крупный (на несколько миллионов долларов) проект для иностранного заказчика. К счастью, имелась резервная копия проекта, так что реальные потери ограничились расходами на следствие и средства защиты от подобных инцидентов в будущем. В августе 2002 года преступники предстали перед судом.

6) Одна студентка потеряла стипендию в 18 тысяч долларов в Мичиганском университете из-за того, что ее соседка по комнате воспользовалась их

общим системным входом и отправила от имени своей жертвы электронное письмо с отказом от стипендии.» [10]

Таких примеров существует много, также можно вспомнить случаи, когда нет недостатков в нарушении ИБ. Например, в марте 1999 года опубликовали годовой отчет «Компьютерная преступность и безопасность-1999: проблемы и тенденции». В нем было замечено резкое возрастание количества обращений в правоохранительные органы в связи с компьютерными преступлениями (32% из числа опрошенных); 30% респондентов сказали, что их информационные системы взломали внешние злоумышленники; 57% опрошенных были атакованы по сети Интернет; в 55% случаях были отмечены нарушения со стороны собственного персонала. 33% респондентов ответили «не знаю» на вопрос «были ли замечены взломы ваших ВЭБ-серверов и систем электронной коммерции за последний год?». В аналогичном отчете, который был опубликован тремя годами позже, цифры изменились, но тенденция оставалась такой же: 90% респондентов сказали, что за последний год в их компаниях происходили нарушения информационной безопасности; 80% рассказали о том, что были финансовые убытки от этих нарушений; 44% оценили убытки количественно, общая сумма которых составляла более 455 млн. долларов. Большой ущерб принесли кражи и подлоги (> 170 и 115 млн. долларов). Аналогичная ситуация показана в обзоре «Информейшен Уек», который опубликован 12 июля 1999 года. Только 22% опрошенных рассказали об отсутствии нарушений информационной безопасности. Вместе с увеличением распространения вирусов росло число внешних атак. Рост числа атак не является значимой проблемой. Хуже то, что часто находят новые уязвимые места в программных обеспечениях. В итоге создаются новые виды атак.

В информационном письме Национального центра защиты инфраструктуры США от 21 июля 1999 года говорится, что с 3 по 16 июля 1999 года найдено девять проблем с программным обеспечением, риск применения которых оценивают, как средний или высокий. Среди

«пострадавших» операционных платформ есть почти все разновидности ОС Unix, Windows, MacOS. В таких условиях системы информационной безопасности противостоят внутренней и внешней, автоматизированной и скоординированной атакам. Главная цель недоброжелателей – нарушить все составляющие информационной безопасности (доступность, целостность, конфиденциальность).

2.3 Методы управления рисками информационной безопасности

Управление безопасностью состоит из управления рисками, политик информационной безопасности, процедур, стандартов, руководства, базисов, классификаций данных, организации безопасности и обучения, связанным с вопросами безопасности.

«Процесс управления рисками информационной безопасностью затрагивает информационные риски или будет интегрирован с общими процессами управления рисками в компании, так как риски информационной безопасности касаются подразделений, которые ведут основное направление ее деятельностей, подразделения управления информационных инфраструктур, ИТ-подразделения.» [22]

Рисунок 12 – Процесс управления рисками ИБ

Процесс управления безопасностью – непрерывный. Регулярный пересмотр рисков поддерживает данные о безопасности информационной системы компании в актуальном состоянии, оперативно выявляет новые опасные риски и нейтрализует их экономически целесообразным образом. Вначале идет процесс анализа объектов ИБ и идентификация угроз. Угрозы, которые были проанализированы, классифицируются по выделенному набору факторов, которые характеризуют легкость эксплуатации уязвимостей, и в рамках выбранного вида проводится полное рассмотрение. Прогноз вероятностей угрозы проходит уже на основании свойств уязвимостей и групп вредителей, которые наносят угрозу. В процессах идентификации и оценки уязвимости важно знать экспертный опыт специалиста по информационной безопасности, который выполняет оценку

рисков, и статический материал, который использован, и отчеты по уязвимостям и угрозам в области ИБ.

Разумно выявлять сами угрозы и источники их возникновения для выбора самого подходящего средства защищенности. Для примера, нелегальный вход в систему является следствием подборов паролей или подключений к сети неавторизованных оборудований. Чтобы противодействовать нелегальному входу, нужно иметь личный механизм безопасности.

После того, как пройдет идентификация угроз, оцениваются вероятности ее осуществления и размеры потенциальных ущербов с применением шкал и критерий оценки. Величины ущербов и вероятностей не всегда выражены в абсолютном денежном показателе. «Методы, которые используются для оценки и анализа риска ИБ, применяют порядковую или количественную шкалу. Еще возможно использование трехбалльной шкалы оценки вероятностей и угроз: низкая, средняя или высокая.» [27]

Чтобы оценить тяжесть потери, нужно знать непосредственные расходы на замены оборудований или восстановление данных, порчу репутации, ослабления позиции на рынках и другие отдаленные расходы.

После того, как прошла оценка рисков, выбираются защитные меры, которые направлены на уменьшение риска и реализацию потребности ИБ. «В качестве защитных мер могут использоваться дополнительная настройка программного обеспечения, строгое управление паролями, охрана, механизмы контроля доступа операционных систем, обучение пользователей вопросам безопасности.» [11]

В конце цикла управления рисками информационной безопасностью проходит увеличение осведомленности работников организации в сфере политики безопасности, стандартов и руководств по обеспечению целостности, конфиденциальности и доступности информации.

«Политика безопасности является своеобразным фундаментом для программы безопасности компании. К этой политике нужно относиться

серьезно с самого начала, в нее должны быть заложены идеи постоянной актуализации, обеспечивающие постоянное функционирование всех компонентов безопасности и работу по достижению целей, соответствующих целям организации. Выработка собственной уникальной политики безопасности нужна только для тех организаций, чьи информационные системы и обрабатываемые данные можно считать нестандартными. Для типовой организации можно использовать типовой набор защитных мер, выбранный из наиболее распространенных рисков информационной безопасности в базе международных или локальных стандартов (ISO 27001). При использовании западных стандартов следует провести анализ на соответствие требованиям национального законодательства в области информационной безопасности.» [11]

Разработка политики в области информационной безопасности включает в себя формирование соответствующего комплекта организационно-распорядительной и нормативно-методической документаций, положения по обеспечению информационной безопасности организации и методик проведений внутренних аудитов безопасности.

Внедрения политик информационной безопасности относятся к организационной мере управления безопасностью. Введение в действие политик начинается с того, что происходит ознакомление всех работников с актуальными политиками информационной безопасности и ее главным принципом касательно приобщения вида связи, коммуникации, хранений, использований и передачи информации.

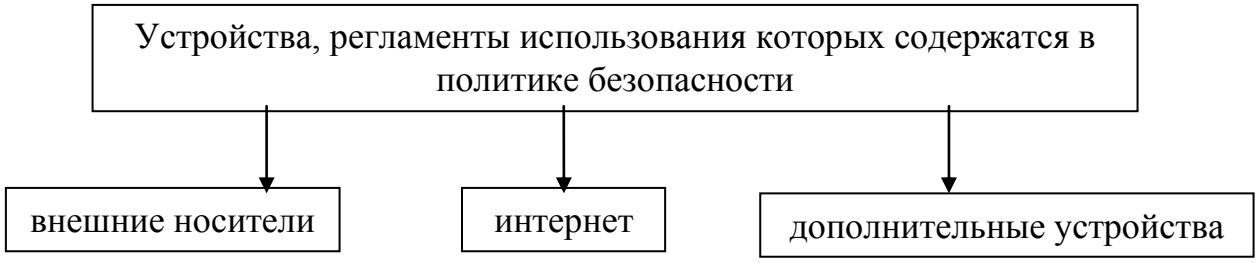

Рисунок 13 – состав политики безопасности

«Внешние носители. Запрет личных носителей, ограничение использования по принципу необходимости, строгий учет используемых носителей, назначение ответственных за информационную безопасность в каждом подразделении.

Интернет. Регламентация получения доступа, использования и контроля использования ресурсов сети Интернет, регламентация использования корпоративной и внешней электронной почты.

Дополнительные устройства. Регламентация самостоятельной установки или подключения дополнительных устройств, таких как USB, Fire-Wire, LPT, COM, IrDA, HDD, Floppy, DVD/CD-ROM, Tape, Modem, Bluetooth, Wi-Fi, мобильные устройства и прочее.» [12]

Некоторые организации используют так называемые «белые списки» устройств, которые могут применяться в соответствии с политиками безопасности, которые регламентированы по определенным производителям, моделям, серийным номерам или по пользователю или группе пользователей.

В политиках безопасности прописываются ограничения:

– запрещают или контролируют использование личного мобильного телефона, фототехник и видеотехник, переносного компьютера, дополнительного устройства передачи данных;

– контролируют помещения и применение видеонаблюдения;

– регламентируют учеты, хранения и использования, контролируют перемещения всех накопителей данных и средств вычислительных техник;

– ограничивают применение факса, модема, телефонной связи;

– разграничивают полномочия пользователя информационной системы с помощью ведения и контроля журнала доступа к критичному ресурсу и применению частной политики безопасности для операционной системы, программного комплекса, коммуникационных оборудований, сети;

– контролируют каналы печати: локальной, сетевой или виртуальной;

– регламентируют жизненный цикл, а также утилизируют цифровые и бумажные носители данных.

Когда вводятся технические ограничения на внешних носителях, программные и аппаратные ограничения рабочей станции, необходимо предусмотреть обязательное шифрование и автоматизированный контроль использований внешнего носителя при помощи специальных программных обеспечений.

Технические разграничения доступов к ресурсу сети Интернет и предоставления доступов только к необходимому ресурсу, или разграничения специального программного обеспечения позволяет произвести контроль использований сети Интернет, исключения взаимодействий с внутренними сетями компании и передачи информации. При помощи технического средства можно провести отключение неиспользуемого устройства, постоянного контроля конфигурации компьютера, а также аппаратное или программное отключения возможностей подключений дополнительного устройства. Можно применить регламентации применения переносного компьютера и внешнего носителя данных, обязательное шифрование всех критически важных данных. Существуют технические ограничения применений факса, модема, учета или аудиозаписи, телефонной связи, исключения возможностей применения личного мобильного телефона, контроля применения копировальных техник при помощи установок на открытые пространства и видеонаблюдения.

Также техническими мерами информационной безопасности могут быть хранение резервного носителя в безопасном хранилище, физическая защита, проектирования и внедрения системы бесперебойных и гарантированных электропитаний, контроля и управления доступами в помещениях и к оборудованиям, видеоконтроля и теленаблюдения.

Чтобы уменьшить уязвимость информационной системы на техническом уровне, необходимо разграничить доступ пользователя информационной системы, адекватно настроить систему безопасности операционной системы, программный комплекс, коммуникационное

оборудование, своевременно обновить систему безопасности и использовать систему обнаружений и предотвращений вторжения.

Чтобы своевременно отследить угрозы информационной безопасности, необходимо предусмотреть специальные технологии обнаружений. Например, предусмотреть:

– компьютерную программу для того, чтобы выявить, нейтрализовать или устранить вредоносные программы;

– систему обнаружений вторжения, собирающие и анализирующие данные из разных областей компьютеров или сетей для выявления возможного нарушения в системе безопасности;

– систему предотвращений вторжений, определяющие потенциальную угрозу и реагирующую на них пока они не начнут использоваться при атаке.

Действие по эффективным управлениям систем информационной безопасности включает регулярные планирования и организации работ с достижениями поставленных целей, разработки и регулярные пересмотры политики и процедуры информационной безопасности. После того, как пройдет разработка или пересмотр политик информационной безопасности, необходимо вовлечь всех работников в процесс обеспечения безопасности, ознакомления с документом, проведения тренинга, назначения ответственного за безопасность в отдельных сегментах. Если определить четкую структуру и распределить полномочия и ответственности за информационную безопасность, то это создаст систему отчетности с прописанным показателем обеспечений информационной безопасности и на ее основе осуществит контроль выполнений всех работ.

«К ключевым факторам успеха системы информационной безопасности можно отнести:

– регулярный пересмотр политики информационной безопасности;

– вовлечение всех сотрудников в процесс обеспечения информационной безопасности;

– своевременность обнаружения и прогнозируемость развития проблем, оценку влияния проблем на цели и управление непрерывностью компании.»[11]

2.4 Обоснование необходимости инвестиции в информационную безопасность предприятия

Существуют причины, которые препятствуют принятию какой-либо меры по обеспечению информационной безопасности в организации:

– ограничения бюджета;

– нехватка поддержки со стороны начальства.

Эти причины возникают, когда начальство не понимает серьезность вопросов, поэтому ИТ-специалистам сложно обосновать, для чего нужно вкладываться в информационную безопасность. Часто люди задумываются о том, что ИТ-менеджеры и начальство говорят на разном языке – финансовом и техническом, но и сами Т-специалисты затрудняются оценить, сколько потребуется потратить денег на обеспечение большой защиты систем организации, к тому же, расходы не должны оказаться напрасными.

Убедить начальство «потратиться» будет гораздо проще, если ИТ-специалист четко представит:

– сколько организация потеряет денег, если будет реализована угроза;

– какую меру нужно предпринять, чтобы повысить уровень защиты, к тому же, не истратить лишние деньги;

– подтвердить все документально.

«Чтобы решить данные задачи, начали разрабатывать программные комплексы анализов и контроля информационного риска. Например, созданный британцами CRAMM, американцами RiskWatch, русскими ГРИФ и другие.» [26]

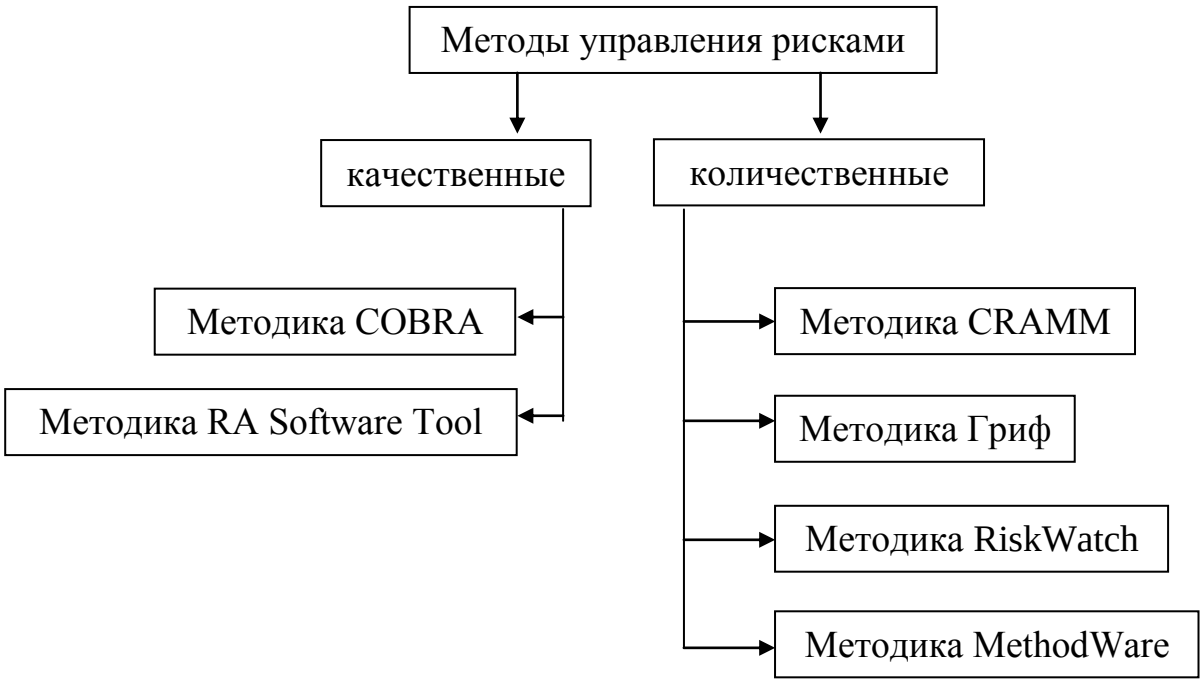

Рисунок 14 – Методы управления рисками

2.5 Качественные методики управления рисками

Качественная методика управления рисками была принята на вооружение в технологически развитых странах многочисленной армией внутренних и внешних IT-аудиторов. Эта методика достаточно популярна и относительно проста, и разработана на основе требования международного стандарта ISO 177992002. В 1993 году было положено начало истории развития, когда Министерство торговли Великобритании обнародовало пособие, которое посвящено практическому аспекту обеспечения информационной безопасности. Пособие было настолько удачным, что им стали пользоваться администраторы безопасности многих предприятий. Позже, в 1995 году, приняли доработанную версию этого пособия в качестве британского стандарта BS7799 «Практические правила управления информационной безопасностью». Стандартом стали пользоваться на добровольной основе в разных странах.

В 1998 году появилась вторая часть стандарта, которая посвящена вопросу аудита информационной безопасности. В 2000 году приняли международный стандарт ISO 17799, на основе стандарта BS7799. В сентябре 2002 года главные положения ISO 17799 пересмотрели и дополнили с учетом

развитий современной информационной технологии и требования к организации режима информационной безопасности. На сегодняшний день является самым распространенным стандартом во всем мире среди компаний, использующих подобный стандарт на добровольной основе.

Стандарт ISO/IEC 17799 – стандарт информационной безопасности, который опубликован в 2005 году компанией ISO и IEC. Его заглавие – «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности». [13]

«Текущая версия стандарта – это переработанная версия, которая опубликована в 2000 году, которая является полной копией Британского стандарта BS 7799-1:1999.» [25]

Стандарт предоставляет лучший практический совет по менеджменту информационной безопасности тем, на ком ответственность за создания, реализации или обслуживания системы менеджмента информационной безопасности. Информационная безопасность определяется стандартом как сохранение конфиденциальности, целостности и доступности.

«Стандарт ISO 17799 содержит две части.

Часть 1. Практические рекомендации по управлению информационной безопасностью, 2002 г., определены основные аспекты организации режима информационной безопасности в компании:

– Политика безопасности.

– Организация защиты.

– Классификация и управление информационными ресурсами.

– Управление персоналом.

– Физическая безопасность.

– Администрирование компьютерных систем и сетей.

– Управление доступом к системам.

– Разработка и сопровождение систем.

– Планирование бесперебойной работы организации.

– Проверка системы на соответствие требованиям ИБ.

Часть 2. Спецификации, 2002 г., рассматривает эти же аспекты с точки зрения сертификации режима информационной безопасности компании на соответствие требованиям стандарта. С практической точки зрения эта часть является инструментом для IT-аудитора и позволяет оперативно проводить внутренний или внешний аудит информационной безопасности любой компании.» [14]

«Качественные методики управления риском на основе требования ISO 17999: методики COBRA и RA Software Tool.» [26]

2.5.1 Методика COBRA

Во второй половине 90-х годов организацией C & A Systems Security Ltd были разработаны одноименная методика и соответствующие инструментарии, чтобы анализировать и управлять информационным риском, которые называются COBRA. Эта методика выполняет в автоматизированных режимах простейшие варианты оценивания информационного риска любой организации. Для этого используются специальная электронная база знаний и процедура логического вывода, которые ориентированы на требования ISO 17799. При желании перечень учитываемого требования дополняют разными требованиями отечественного нормативно-регулирующего органа, такой как, требования руководящего документа Гостехкомиссии при Президенте Российской Федерации.

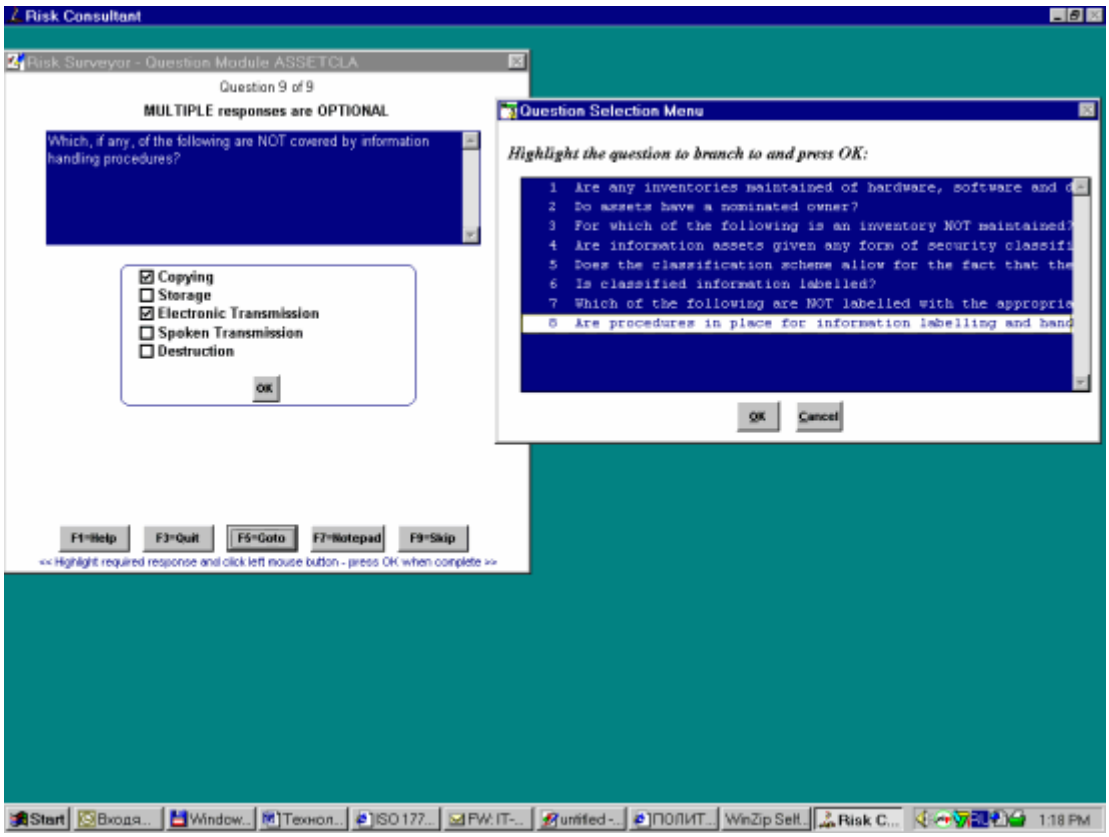

Рисунок 15 – Тематический сборник вопросов Cobra

Методика COBRA представляет требования стандарта ISO 17799 в виде тематического вопросника, на который нужно ответить в ходе оценки риска информационного актива и электронной транзакции организации. Дальше, ответы, которые введены, автоматически обрабатываются, и при помощи соответствующего правила логического вывода создается итоговый отчет с текущими оценками информационных рисков организации и рекомендацией по их управлению.

2.5.2 Методика RA Software Tool

Методику и одноименное инструментальное средство RA Software Tool основали на требованиях международных стандартов ISO 17999 и ISO 13335, некоторых руководств Британского национального института стандартов (BSI), для примера, PD 3002 (Руководство по оценкам и управлениям рисками), PD 3003 (Оценка готовности организации к аудитам в соответствии с BS 7799), PD 3005 (Руководство по выбору системы защиты) и другие.

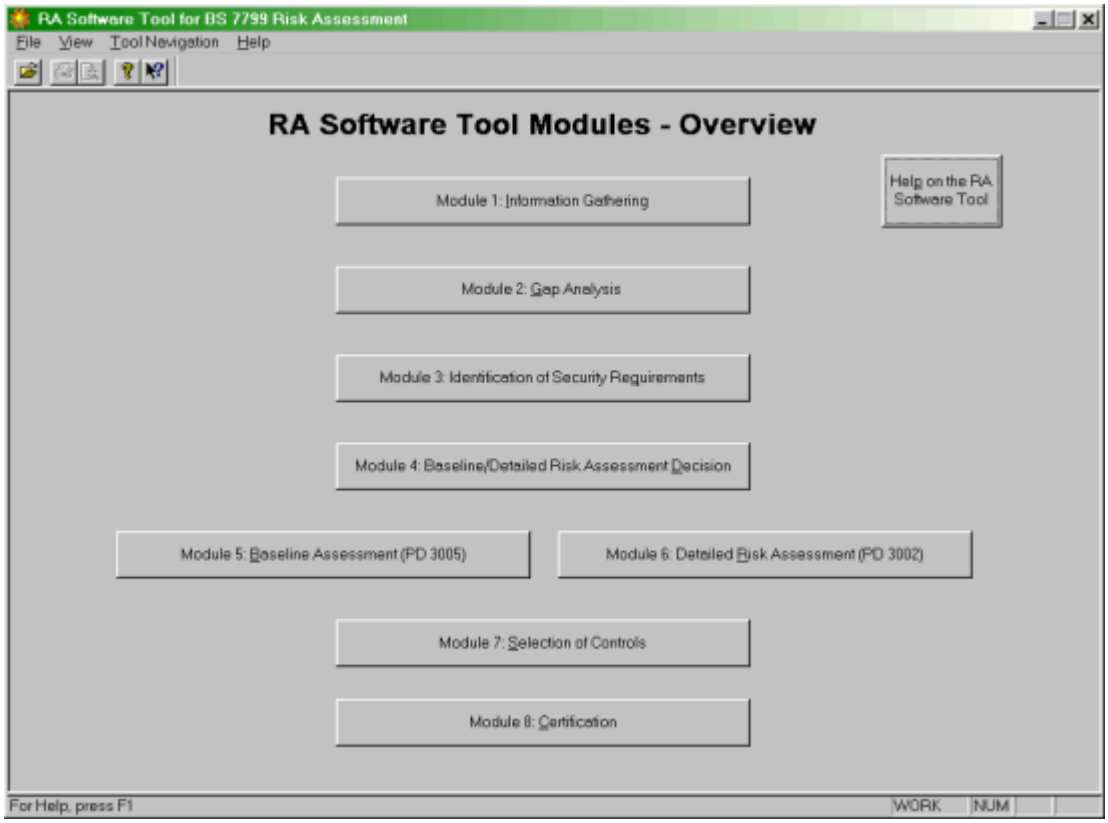

Рисунок 16 – Основные модули методики RA Software Tool

Эта методика выполняет оценку информационного риска в соответствии с требованиями ISO 17799, а при желании в соответствии с более детальными спецификациями руководства PD 3002 Британского института стандартов.

2.6 Количественные методики управления рисками

Актуальность методики обусловлена необходимостями решения различных оптимизационных задач, часто возникающих в реальной жизни. Сутью задач является поиск единственных оптимальных решений, которые существуют.

Для примера, нужно ответить на вопросы: «Как можно достичь максимальный уровень защиты информационных активов организации, при этом остаться в пределах утвержденного квартального бюджета на ИБ?» или «Какую выбрать альтернативу построений корпоративных защит данных, если учесть известные ограничения ресурса организации?»

Решением этих задач является разработка метода и методик количественных оценок и управлений риска на основе структурного

объектно-ориентированного методов системных анализов и проектирований.

Эти методики могут позволить:

– создание модели информационного актива организации с точки зрения безопасности;

– классифицирование и оценивание актива;

– составление списка самой значимой угрозы и уязвимости безопасности;

– ранжирование угрозы и уязвимости безопасности;

– обоснование средства и меры контроля риска;

– оценивание эффективности или стоимости разного варианта защиты;

– формализовать и автоматизировать процедуру оценивания и управлений риском.

Самая известная методика такой группы – методика CRAMM.

2.6.1 Методика CRAMM

В 1985 году Центральное агентство по компьютеру и телекоммуникации Великобритании начало исследовать существующие методы управления информационной безопасностью, чтобы рекомендовать их использование правительственным организациям, которые обрабатывают конфиденциальную информацию. Никакой метод не подошел. Поэтому стали создавать методы, а потом одноименную методику CRAMM, которая соответствует требованиям ССТА. После начали появляться версии методики, которые ориентированы на требования разных государственных и коммерческих компаний.

Основные цели методики CRAMM:

– формализовать и автоматизировать процедуры анализов и управлений рисками;

– оптимизировать расходы на средства контроля и защиты;

– комплексно планировать и управлять риском на всех стадиях жизненного цикла информационной системы;

– сокращать время на разработки и сопровождения корпоративных систем защиты данных;

– обосновать эффективность предлагаемой меры защиты и средства контроля;

– управлять изменением и инцидентом;

– поддерживать непрерывность компании;

– оперативно принимать решения по вопросу управления безопасностью и другие.

Управление риском в методике CRAMM происходит в несколько этапов (рисунок 17).

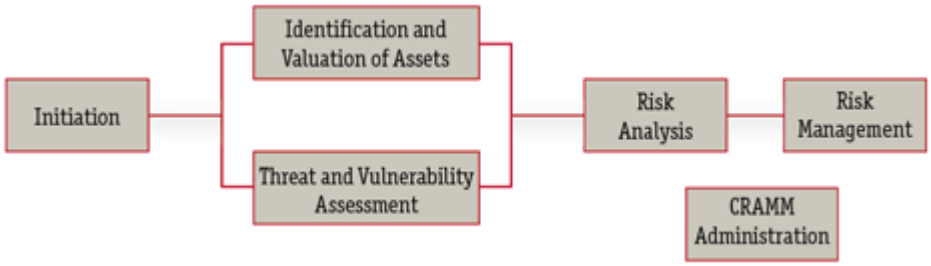

Рисунок 17 – Этапы управления рисками в методике CRAMM

«На первом этапе инициации – «Initiation» – определяются границы исследуемой информационной системы компании, состав и структура ее основных информационных активов и транзакций.

На этапе идентификации и оценки ресурсов – «Identification and Valuation of Assets» – четко идентифицируются активы и определяется их стоимость. Расчет стоимости информационных активов однозначно позволяет определить необходимость и достаточность предлагаемых средств контроля и защиты.

На этапе оценивания угроз и уязвимостей – «Threat and Vulnerability Assessment» – идентифицируются и оцениваются угрозы и уязвимости информационных активов компании.

На этапе анализа рисков – «Risk Analysis» – можно получить качественные и количественные оценки рисков.

На этапе управления рисками – «Risk management» – предлагаются меры и средства уменьшения или уклонения от риска.» [15]

Недостатки метода CRAMM:

– требуется специальная подготовка и высокая квалификация аудитора, чтобы использовать метод;

– больше подходит для аудита существующего ИС, которая эксплуатируется, чем для ИС, которая разрабатывается;

– генерируется программным инструментарием огромное число бумажных документов, которые часто оказываются вредной на практике;

– невозможно создать собственный шаблон отчета или модификацию имеющегося;

– невозможно пользователю внести дополнения в базы знания метода, это приводит к определенным трудностям при адаптации метода к потребности конкретного предприятия;

– существует только английская версия программного обеспечения;

– дорогая лицензия.

2.6.2 Методика Гриф

Чтобы провести полный анализ информационного риска, нужно создать полные модели информационных систем с точки зрения информационной безопасности. Чтобы решить эту задачу ГРИФ имеет простой и понятный для пользователей интерфейс.

Основной задачей системы Гриф является возможность ИТ-специалисту самому дать оценку уровню риска в информационных системах и эффективность существующей практики по обеспечению безопасности организации. Также суметь в цифрах убедить начальство организации в том, что необходимо инвестировать в информационную безопасность.

«На первом этапе метода Гриф проводится опрос ИТ-менеджера с целью определения полного списка информационных ресурсов, представляющих ценность для компании.

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 указанных на предыдущем этапе объектах хранения информации (серверах, рабочих станциях и т. д.). Заключительная фаза – указание ущерба по каждой группе ценной информации, расположенной на соответствующих ресурсах, по всем видам угроз.

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

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

На завершающем этапе необходимо ответить на вопросы по политике безопасности, реализованной в системе, что позволит оценить реальный уровень защищенности системы и детализировать оценки рисков.»[16]

Наличия средств информационной защиты, которые отмечены на первом этапе, не защищает систему в случае их неадекватного применения и нехватки комплексных политик безопасности, которые учитывают аспекты защиты данных, которые включают вопрос об организации защиты, физических безопасностей, безопасности сотрудников, непрерывностях ведения бизнеса и другое.

«Результатом выполнений всех этапов является формирование модели информационных систем с точки зрения ИБ при учете реальных выполнений

требования комплексной политики безопасности, что может позволить перейти к программным анализам введенной информации, чтобы получить комплексную оценку риска и формировать итоговые отчеты.» [28]

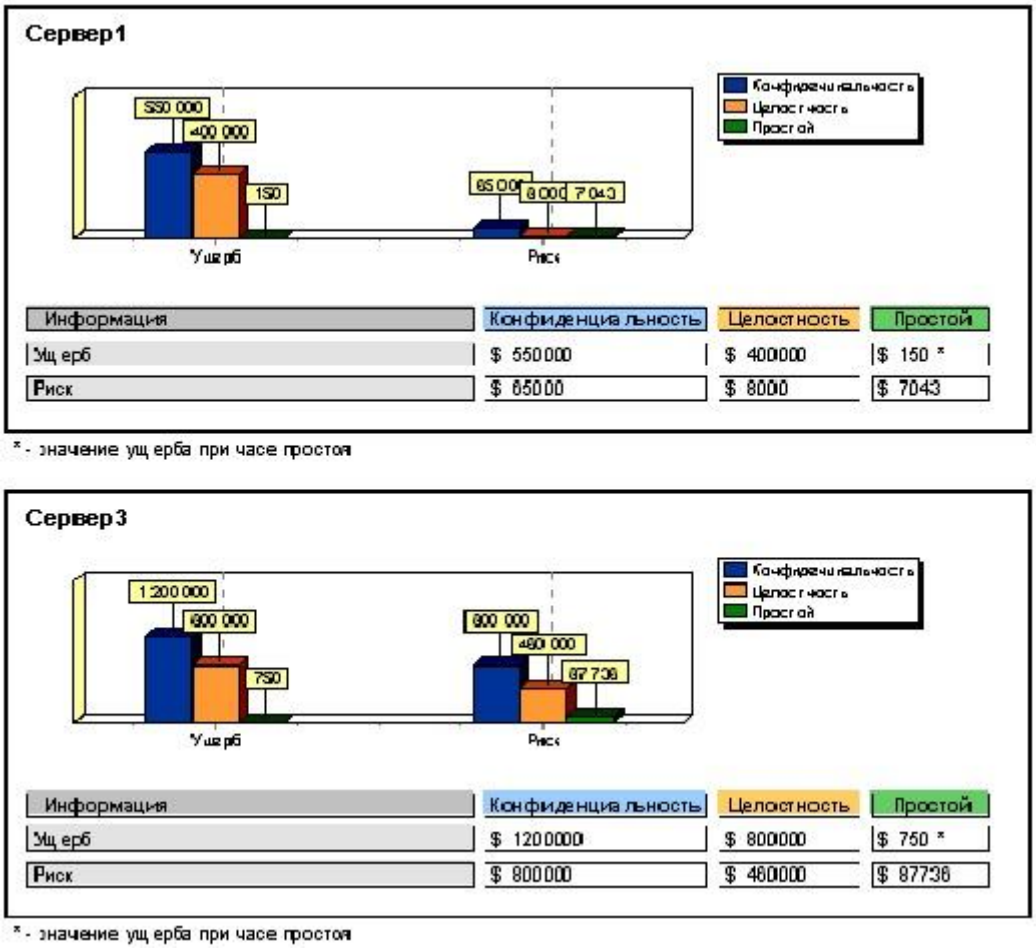

Рисунок 18 – ущерб и риск по ресурсам

Недостатки методики Гриф:

– сложный алгоритм анализа риска, содержащий больше ста параметров который дает точные оценки существующего в информационных системах риска;

– отсутствует привязка к процессам;

– отсутствует возможность сравнивать отчеты на различных этапах внедрения комплекса мер по обеспечению защиты;

– отсутствует возможность добавлений специфичного для конкретной организации требования политик безопасности.

2.6.3 Методика RiskWatch

Программное обеспечение RiskWatch, которое разработано американской организацией RiskWatch – мощное средство, чтобы анализировать и управлять рисками. RiskWatch состоит из программных продуктов для проведения разных видов аудитов безопасности. RiskWatch включает средства аудитов и анализов риска:

«– RiskWatch for Physical Security – для физических методов защиты;

– RiskWatch for Information Systems – для информационных рисков;

– HIPAA-WATCH for Healthcare Industry – для оценки соответствия требованиям стандарта HIPAA;

– RiskWatch RW17799 for ISO17799 – для оценки требованиям стандарта ISO17799.» [17]

В методике RiskWatch критериями, чтобы оценить и управлять рисками, являются «предсказание годовой потери» и оценки «возврата от инвестиции».

RiskWatch может помочь проводить анализы риска и делать обоснованный выбор мер и средств защиты. Методика состоит их четырех фаз.

«Первая фаза является определением предмета исследования. На данном этапе описываются общие параметры организации – тип организации, состав исследуемой системы, базовые требования в области безопасности. Описание формализуется в ряде подпунктов, которые можно выбрать для более подробного описания или пропустить.

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

Вторая фаза – ввод данных, описывающих конкретные характеристики системы. Данные могут вводиться вручную или импортироваться из отчетов, созданных инструментальными средствами исследования уязвимости

компьютерных сетей. На этом этапе подробно описываются ресурсы, потери и классы инцидентов.

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

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

Например, если стоимость сервера $150 000, а вероятность того, что он будет уничтожен пожаром в течение года, равна 0.01, то ожидаемые потери составят $1 500. Дополнительно рассматриваются сценарии «что, если...», которые позволяют описать аналогичные ситуации при условии внедрения средств защиты. Сравнивая ожидаемые потери при условии внедрения защитных мер и без них можно оценить эффект от таких мероприятий.

Четвертая фаза – генерация отчетов. Типы отчетов: краткие итоги; полные и краткие отчеты об элементах, описанных на стадиях 1 и 2; отчет о стоимости защищаемых ресурсов и ожидаемых потерь от реализации угроз; отчет об угрозах и мерах противодействия; отчет о результатах аудита безопасности.» [17]

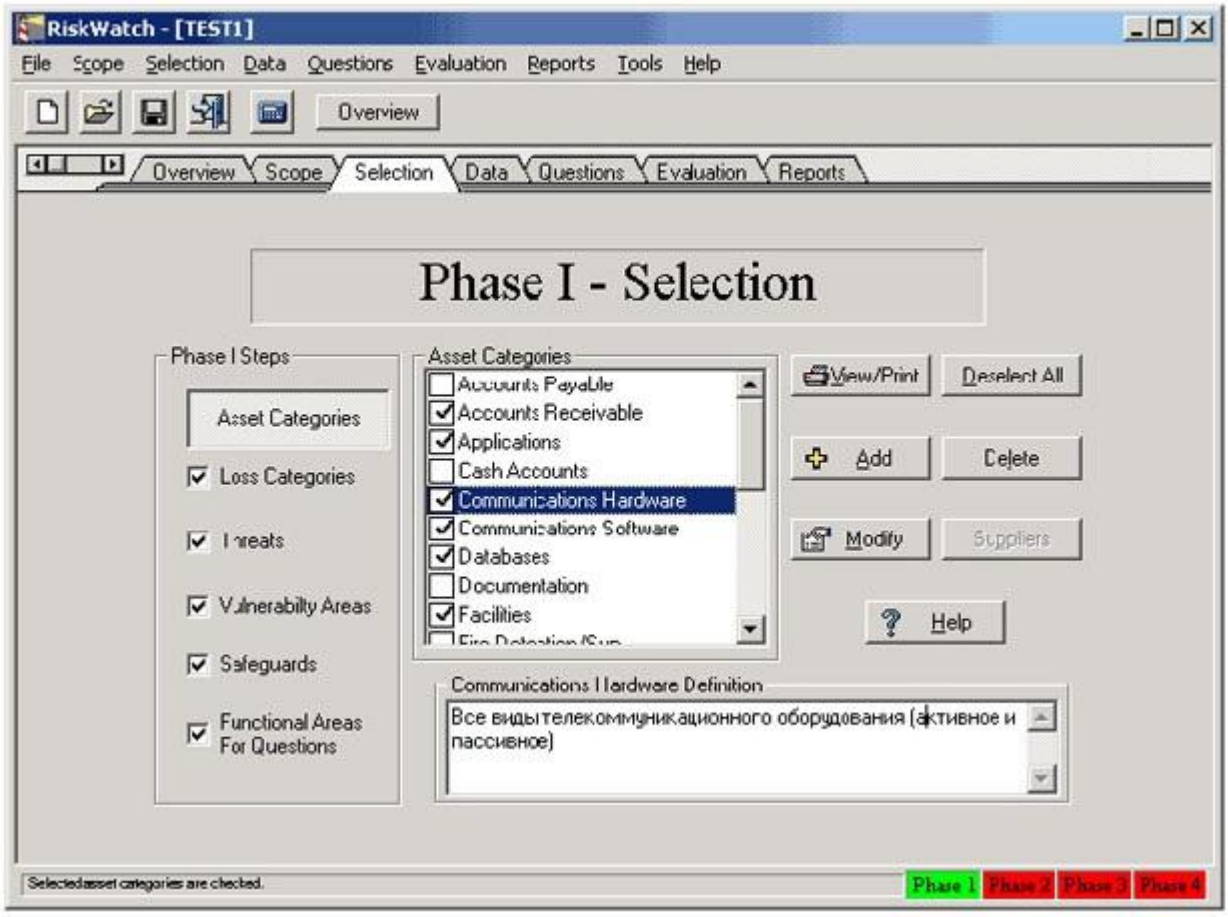

Рисунок 19 – Определение категорий защищаемых ресурсов

Недостаткам RiskWatch:

– проводит анализ риска на программно-техническом уровне защищенности, не учитывает организационный и административный факторы, а также комплексный подход к безопасности информации;

– существует только английская версия программного обеспечения.

– дорогая лицензия – от $15 000 за одно рабочее место для небольшой организации и от $125 000 за корпоративные лицензии.

2.6.4 Методика MethodWare

Компанией MethodWare была разработана своя собственная методика оценок и управления риском и выпущен ряд соответствующих инструментальных средств. «К ним относятся:

– ПО анализа и управления рисками Operational Risk Builder и Risk Advisor. Методика соответствует австралийскому стандарту Australian/New Zealand Risk Management Standard (AS/NZS 4360:1999) и стандарту ISO17799;

– ПО управления жизненным циклом информационной технологии в соответствии с CobiT Advisor 3rd Edition (Audit) и CobiT 3rd Edition Management Advisor. В руководствах CobiT существенное место уделяется анализу и управлению рисками;

– ПО для автоматизации построения разнообразных опросных листов Questionnaire Builder.» [18]

Реализована методика, которая задает модели информационных систем с точки зрения информационной безопасности, идентифицирует риск, угрозу, потерю в результате инцидента. Основные этапы работы: описание контекстов, определение риска, оценка угрозы и возможных ущербов, разработка управляющего воздействия и выработка плана восстановлений и действия в чрезвычайной ситуации. Рассмотрим этапы.

«Описание контекста. На этом этапе происходит описание модели взаимодействий предприятий с внешним миром в нескольких аспектах: стратегическом, организационном, цели, управление рисками, критерии. Стратегический аспект описывает сильные и слабые стороны предприятия с внешних позиций, варианты развития, классы угроз и отношения с партнерами. Организационный контекст описывает отношения внутри предприятия: стратегию, цели на организационном уровне, внутреннюю политику. Контекст управления рисками описывает концепцию информационной безопасности. Контекст целей – основные цели. Критерии оценки – критерии оценки, которые используются при управлении рисками.

Описание рисков. Задается матрица рисков на основе какого-нибудь шаблона. В результате риски будут описаны в соответствии с определенным шаблоном и заданы связи этих рисков с другими элементами модели.

Риски оцениваются по качественной шкале и разделяются на приемлемые и неприемлемые на основе простейшей модели.

Затем выбираются управляющие контрмеры с учетом зафиксированной ранее системы критериев, эффективности взаимодействий и их стоимости. Стоимость и эффективность также оцениваются в качественных шкалах.

Описание угроз. Сначала формируется список угроз. Угрозы определенным образом классифицируются, затем описывается связь между рисками и угрозами. Описание также делается на качественном уровне и позволяет зафиксировать их взаимосвязи.

Описание потерь. Описываются события, которые связаны с нарушением режима информационной безопасности. Потери оцениваются в выбранной системе критериев.

Анализ результатов. В результате построения модели можно сформировать подробный отчет (около 100 разделов), посмотреть на экране агрегированные описания в виде графа рисков.» [18]

Рисунок 20 – Генерация результатов в Risk Advisor

Методика, которая была рассмотрена, автоматизирует разные аспекты управления риском организации. Оценка риска дается в качественной шкале. Подробные анализы факторов риска не предвидены. Сильная сторона методики, которая рассмотрена, – возможность описывать различные связи, адекватные учеты большого количества факторов рисков и маленькая трудоемкость в сравнении с другими методиками.

Современные методы и технология управления информационными рисками оценивают существующие уровни остаточного информационного риска в отечественном предприятии.

2.7 Сравнение методов

Таблица 1. Сравнение рассмотренных методик

	1	2	3	4	5	6	7	8
CRAMM	+	–	+	–	+	–	–	от 2000 до 5000
ГРИФ	–	–	–	+	–	–	+	от 1000
RiskWatch	–	–	–	–	–	+	–	от 10 000
MethodWare	–	+	–	–	–	–	–	от 3000

1 – простой алгоритм анализов риска;

2 – возможно описание разных связей, адекватный учет многих факторов рисков и маленькая трудоемкость;

3 – использование инструментальных средств с повышенными требованиями в области информационной безопасности;

4 – обладает простым интерфейсом;

5 – требуется мало времени на разработки и сопровождения корпоративных систем защиты данных;

6 – проводит анализ рисков на программно-техническом уровне защищенности;

7 – сетевое решение;

8 – цена лицензии за одно рабочее место, доллар.

На сегодняшний день есть ряд методик анализов риска, которые адаптированы к применению в отечественных условиях. Актуально, если качественно выполненные анализы информационного риска позволяют проводить сравнительный анализ «эффективности и стоимости» различных вариантов защищенности, выбирать адекватную контрмеру и средство контроля, оценивать уровни остаточного риска. Кроме этого, инструментальное средство анализов риска, которое основано на

современной базе знания и процедуре логического вывода, строит структурную и объектно-ориентированную модель информационного актива организации, модель угрозы и модель риска, которые связаны с отдельной информационной транзакцией и выявляет такую информационную активу организации, при которой риски нарушений защиты являются критическими, то есть неприемлемыми. Такое инструментальное средство строит разные модели защищенности информационной активы организации, сравнивает по критерии «эффективности и стоимости» разные варианты комплекса мер защищенности и контроля, ведет мониторинг выполнений требования по организации режимов информационной безопасности отечественной организации.

3 Методика выбора правил управления информационной безопасностью телекоммуникационной сети

Алгоритм действия по организации управления информационной безопасностью:

1) Выделяются элементы системы;

2) Проводится функционирование системы;

3) Проводится анализ рисков;

4) Определяются границы исследования;

5) Проводится идентификация ресурсов;

6) Строится модель информационной системы;

7) Определяется ценность ресурсов;

8) Проводится оценка возможного ущерба;

9) Разрабатываются шкалы для выбранной системы параметров;

10) Рассматриваются основные сценарии, которые приводят к различным негативным последствиям, которые описываются в терминах выбранных параметров;

11) Оцениваются угрозы и уязвимости;

12) Группируются активы организации с точки зрения угроз и уязвимостей;

13) Проводятся коррекции результатов;

14) Генерируются варианты мер противодействия, которые адекватны выявленным рискам и их уровням.

Рассмотрим возможности на примере. Надо провести оценку информационного риска корпоративных информационных систем (рис 21).

Рисунок 21 – корпоративная информационная система

Эта схема содержит компоненты системы:

– рабочие места ввода данных, которые поступают из внешнего мира;

– почтовый сервер, куда данные поступают с удаленного узла сети через Интернет;

– сервер обработки, где установлена система управления базами данных;

– сервер резервных копирований;

– рабочие места групп оперативных реагирований;

– рабочее место администратора безопасности;

– рабочее место администратора базы данных.

Далее рассмотрим, как происходит функционирование систем. Данные, которые введены с рабочего места пользователей и поступившие на почтовый сервер, отправляются на сервер корпоративных обработок информации. Затем данные поступают на рабочее место групп оперативных реагирований, и уже там используются соответствующие решения.

Далее проводится анализ риска при помощи разработанной методики и предложим некоторое средство контроля и управления риском, адекватной цели и задачи предприятия.

Определения границы исследований. Этот этап начинается с решения задач определения границы исследуемых систем. Для этого необходимо собрать данные:

– об ответственных за физическую и программную ресурсу;

– о тех, кто является пользователями, и как они пользуются системой, или как будут применять систему;

– о конфигурации систем.

Начальные данные берутся, когда проходит беседа с менеджером проекта, менеджером пользователя или иным персоналом.

Идентификация ресурса и построение моделей системы с точки зрения информационной безопасности. Проходит идентификация ресурса: материальная, программная и информационная, которая содержится в пределах системы. Каждый ресурс относится к одной из предопределенных групп.

Далее строится модель информационных систем с точки зрения информационной безопасности. Для каждых информационных процессов, которые имеют самостоятельные значения со стороны пользователей и которые называются пользовательскими сервисами, строится дерево связей используемого ресурса. В рассмотренном примере будет один подобный сервис. Модели, которые построены, позволяют выделить критичные компоненты.

Ценность ресурсов. Методика определяет ценность ресурса. Этот шаг является обязательным в полных вариантах анализов риска. Ценностью физического ресурса в данном методе является цена их восстановления, если произойдет разрушение. Ценность данных и программного обеспечения определяется:

– недоступностью ресурса в течение определенных периодов времени;

– разрушением ресурса – потерей данных, которые получены во время последнего резервного копирования или их полное уничтожение;

– нарушением конфиденциальности в случаях НСД штатного персонала или посторонних лиц;

– модификацией рассматривания случаев мелких ошибок сотрудников, программной ошибки, преднамеренной ошибки;

– ошибками, которые связанны с передачей данных: отказ от доставки, когда не были доставлены данные, доставка по неправильному адресу.

Критерии для оценки возможного ущерба:

– ущерб репутации предприятия;

– нарушения действующего законодательства;

– вред здоровью сотрудников;

– ущерб, который связан с разглашением персональной информации отдельных лиц;

– ущерб, который связан с разглашением конфиденциальной информации;

– убытки от разглашений данных;

– убытки, которые связаны с восстановлением ресурсов;

– потери, которые связаны с невозможностью выполнения обязательств;

– дезорганизация деятельности.

Совокупность критериев, которая приведена выше, применяется в коммерческих вариантах метода. В иных версиях совокупность будет другой, для примера, в версии, которая используется в правительственных учреждениях, добавляются параметры, которые отражают такие области, как национальная безопасность и международные отношения.

Для информации и программного обеспечения берутся применимые к данной ИС критерии, оценивается ущерб по шкале со значениями от 1 до 10. Для примера, если информация содержит подробности коммерческих конфиденциальных данных, эксперт, который проводит исследования, задает вопрос: как отразится на организации несанкционированный доступ посторонних лиц к этой информации?

Подойдет такой ответ: провал сразу нескольких параметров из выше перечисленных, причем каждый аспект следовало бы разобрать подробнее и присвоить самую высокую из возможных оценок.

Далее разрабатываются шкалы для выбранной системы параметров. Рассмотрим их.

Ущерб репутации организации:

2 – негативная реакция отдельных чиновников, общественных деятелей;

4 – критика в средствах массовой информации, которая не имеет широкого общественного резонанса;

6 – негативная реакция отдельных депутатов Думы, Совета Федерации;

8 – критика в средствах массовой информации, которая имеет последствия в виде крупных скандалов, парламентских слушаний, широкомасштабных проверок и другие;

10 – негативная реакция на уровне Президента и Правительства.

Вред здоровью сотрудников:

2 – маленький ущерб (последствия, не связанные с госпитализаций или длительным лечением);

4 – ущерб среднего размера (необходимо лечение для одного или нескольких сотрудников, но длительных отрицательных последствий нет);

6 – серьезные последствия (длительная госпитализация, инвалидность);

10 – гибель людей.

Убытки, которые связаны с восстановлением ресурсов:

2 – меньше $1000;

6 – в пределах от $1000 до $10 000;

8 – в пределах от $10 000 до $100 000;

10 – больше $100 000.

Дезорганизация деятельности из-за недоступности данных:

2 – нет доступа к данным до 15 минут;

4 – нет доступа к данным до 1 часа;

6 – нет доступа к данным до 3 часов;

8 – нет доступа к данным от 12 часов;

10 – нет доступа к данным более суток.

Далее рассматриваются основные сценарии, которые приводят к различным негативным последствиям, которые описываются в терминах выбранных параметров.

На этом этапе может быть подготовлено несколько типов отчетов (границы системы, модель, определение ценности ресурсов). Если ценность ресурсов низкая, то можно пользоваться базовым вариантом защиты. В этом случае исследователь может перейти от данной стадии сразу к стадии анализа рисков. Однако для адекватного учета потенциального воздействия какой-либо угрозы, уязвимости или комбинации угроз и уязвимостей, имеющих высокие уровни, используют сокращенную версию стадии оценки угроз и уязвимостей. Это позволяет разработать более эффективную систему защиты информации организации.

На этапе оценивания угроз и уязвимостей дается оценка зависимости пользовательских сервисов от определенных классов ресурсов и существующий уровень угрозы и уязвимости.

Затем активы организации группируются с точки зрения угроз и уязвимостей. Для примера, если появилось наличие угрозы пожара или кражи, в качестве класса ресурсов разумно рассмотреть все ресурсы, которые находятся в одном месте (серверный зал, комната средств связи и другие).

При этом оценка уровней угроз и уязвимостей проводится на основе косвенных факторов или на основе прямых оценок экспертов. В первом случае данное программное обеспечение для каждого класса ресурсов и каждого из них генерирует список вопросов, допускающих однозначный ответ.

Уровень угроз оценивается в зависимости от ответов, например:

– очень высокий;

– высокий;

– средний;

– низкий;

– очень низкий.

Уровень уязвимости оценивается в зависимости от ответов, например:

– высокий;

– средний;

– низкий;

– отсутствует.

Может произойти коррекция результатов или начнет использоваться другой метод оценки. На основе этих данных можно рассчитать уровни рисков в дискретной шкале с градациями от 1 до 7 (этап анализа рисков). Полученные уровни угроз, уязвимостей и рисков нужно проанализировать и согласовать с заказчиком. Далее переходим к заключительной стадии метода.

На этом этапе используемый метод генерирует несколько вариантов мер противодействий, адекватных выявленным рискам и их уровням. Контрмеры делятся на группы и подгруппы по следующим категориям:

– обеспечение безопасности на сетевом уровне.

– обеспечение физической безопасности.

– обеспечение безопасности поддерживающей инфраструктуры.

– меры безопасности на уровне системного администратора.

В итоге выполнения этого этапа формируется несколько видов отчетов.

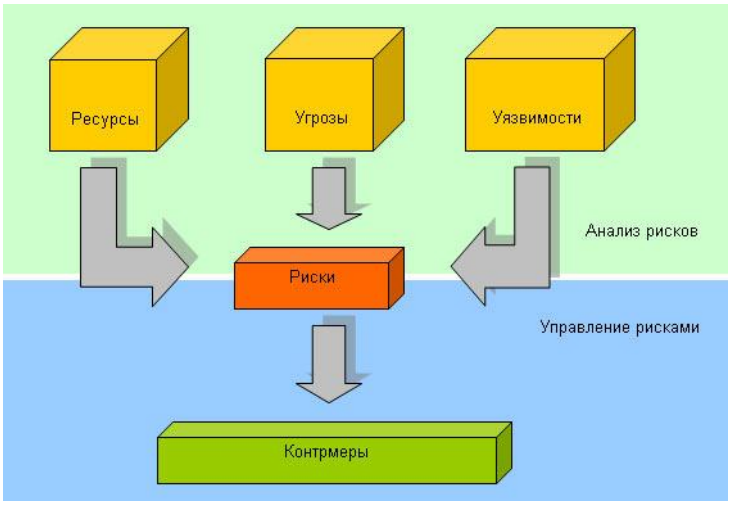

Рисунок 22 – схема проведения обследования объекта

Недостатки данного метода:

– чтобы использовать метод, необходима специальная подготовка и высокая квалификация аудиторов;

– больше подходит для аудита существующего ИС, которая эксплуатируется, чем для ИС, которая разрабатывается;

– генерируется программным инструментарием огромное число бумажных документов, которые часто оказываются вредной на практике;

– невозможно создать собственный шаблон отчета или модификацию имеющегося;

– невозможно пользователю внести дополнения в базы знания метода, это приводит к определенным трудностям при адаптации метода к потребности конкретного предприятия;

– существует только английская версия программного обеспечения;

– дорогая лицензии.

Принцип расчета рисков.

Входные данные:

– ресурсы;

– критичность ресурса;

– отделы, к которым относятся ресурсы;

– угрозы, действующие на ресурсы;

– уязвимости, через которые реализуются угрозы;

– вероятность реализации угрозы через данную уязвимость;

– критичность реализации угрозы через данную уязвимость.

Расчет рисков по угрозе информационной безопасности

1. На первом этапе рассчитываем уровень угрозы по уязвимости Th на основе критичности и вероятности реализации угрозы через данную уязвимость. Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации.

$$\mathrm{Th}_{c,I,a} = \frac{ER_{c,i,a}}{100} \times \frac{P(V)_{c,i,a}}{100},$$

где $ER_{c,i,a}$ – критичность реализации угрозы (указывается в %), $P(V)_{c,i,a}$ – вероятность реализации угрозы через данную уязвимость (указывается в %).

Вычисляем одно или три значения в зависимости от количества базовых угроз. Получаем значение уровня угрозы по уязвимости в интервале от 0 до 1.

2. Чтобы рассчитать уровень угрозы по всем уязвимостям CTh, через которые возможна реализация данной угрозы на ресурсе, просуммируем полученные уровни угроз через конкретные уязвимости по формуле:

2.1. Для режима с одной базовой угрозой:

$$\mathrm{CTh} = 1 - \prod_{i=1}^{n} (1 - Th)$$

2.2. Для режима с тремя базовыми угрозами:

$$\mathrm{CTh_c} = 1 - \prod_{i=1}^{n} (1 - Th_c)$$

$$\mathrm{CTh_i} = 1 - \prod_{i=1}^{n} (1 - Th_i)$$

$$\mathrm{CTh_a} = 1 - \prod_{i=1}^{n} (1 - Th_a)$$

Значения уровня угрозы по уязвимостям получаем в интервале от 0 до 1.

3. Аналогично рассчитываем общий уровень угроз по ресурсу CThR (нужно учесть все угрозы, которые действуют на ресурс).

3.1. Для режима с одной базовой угрозой:

$$\mathrm{CThR} = 1 - \prod_{i=1}^{n} (1 - CTh)$$

3.2. Для режима с тремя базовыми угрозами:

$$\mathrm{CThR_c} = 1 - \prod_{i=1}^{n} (1 - CTh_c)$$

$$\mathrm{CThR_i} = 1 - \prod_{i=1}^{n} (1 - CTh_i)$$

$$\mathrm{CThR_a} = 1 - \prod_{i=1}^{n} (1 - CTh_a)$$

Значение общего уровня угрозы получаем в интервале от 0 до 1.

4. Риск по ресурсу R рассчитываем:

4.1. Для режима с одной базовой угрозой:

R = CThR×D, где D – критичность ресурса. Задается в деньгах или уровнях.

4.2. Для режима с тремя базовыми угрозами:

$R_c = CThR_c \times D_c$

$R_i = CThR_i \times D_i$

$R_a = CThR_a \times D_a$

$$R = (1 - \prod_{i=1}^{3}(1 - \frac{R_i}{100})) \times 100$$

D_c , D_i , D_a – критичность ресурса по трем угрозам. Задается в деньгах или уровнях. R – суммарный риск по трем угрозам. В итоге получаем значение рисков по ресурсу в уровнях или деньгах.

Задание контрмер. Для расчета эффективности введенной контрмеры необходимо пройти последовательно по всему алгоритму с учетом заданной контрмеры. То есть на выходе пользователь получит значение двух рисков – риска без учета контрмеры (Rold) и риск с учетом заданной контрмеры (Rnew).

Эффективность введения контрмеры рассчитываем по формуле (E):

$E = (R_{old} - R_{new}) / R_{old}$

В итоге работы алгоритма пользователь системы получит данные:

– риск реализаций по базовой угрозе для ресурса;

– риск реализаций суммарно по всем угрозам для ресурса;

– риск реализаций по базовой угрозе для информационной системы;

– риск реализаций по всем угрозам для информационной системы;

– риск реализаций по всем угрозам для информационной системы после задания контрмер;

– эффективность контрмеры;

– эффективность комплекса контрмер.

Пример расчета риска информационной безопасности на основе модели угроз и уязвимостей. Рассмотрим расчет рисков для одной угрозы информационной безопасности, так как для остальных угроз риск можно рассчитать аналогично.

1. Входные данные.

Таблица 2. Входные данные

Ресурс	Угрозы	Уязвимости
Сервер (критичность ресурса 100 у.е.)	Угроза 1 Неавторизованное проникновение нарушителя внутрь охраняемого периметра (одного из периметров)	Уязвимость 1 Отсутствие регламента доступа в помещения с ресурсами, которые содержат ценные данные
		Уязвимость 2 Отсутствие системы наблюдения за объектом или существующая система наблюдения охватывает не все важные объекты
	Угроза 2 Неавторизованная модификация информации в системе электронной почты, которая хранится на ресурсе	Уязвимость 3 Отсутствие авторизации для внесения изменений в систему электронной почты
		Уязвимость 4 Отсутствие регламента работы с системой криптографической защиты электронной корреспонденции
	Угроза 3 Разглашение конфиденциальной информации сотрудниками компании	Уязвимость 5 Отсутствие соглашений о конфиденциальности
		Уязвимость 6 Распределение атрибутов безопасности (ключи доступа, шифрования) между несколькими доверенными сотрудниками

Таблица 3. Соотнесение угроза/уязвимость

Угроза/Уязвимость	Вероятность реализации угрозы через данную	Критичность реализации угрозы

	уязвимость в течение года (%), P(V)	через уязвимость (%), ER
Угроза 1/Уязвимость 1	50	60
Угроза 1/Уязвимость 2	20	60
Угроза 2/Уязвимость 3	60	40
Угроза 2/Уязвимость 4	10	40
Угроза 3/Уязвимость 5	10	80
Угроза 3/Уязвимость 6	80	80

2. Уровень угрозы.

Таблица 4. Расчет уровня угрозы

Угроза/Уязвимость	Уровень угрозы (%), Th	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh
Угроза 1/Уязвимость 1	0,3	0,384
Угроза 1/Уязвимость 2	0,12	
Угроза 2/Уязвимость 3	0,24	0,270
Угроза 2/Уязвимость 4	0,04	
Угроза 3/Уязвимость 5	0,08	0,669
Угроза 3/Уязвимость 6	0,64	

3. Общий уровень угроз, которые действуют на ресурс.

Таблица 5. Расчет общего уровня угроз по ресурсу

Угроза/Уязвимость	Угроза/Уязвимость Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh	Общий уровень угроз по ресурсу (%), CThR
Угроза 1/Уязвимость 1	0,384	0,8511
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 3	0,270	
Угроза 2/Уязвимость 4		
Угроза 3/Уязвимость 5	0,669	
Угроза 3/Уязвимость 6		

4. Риск ресурса.

Критичность ресурса (ущерб, который понесет компания от потери ресурса) – 100 у.е. Для угрозы доступность, критичность ресурса задается в час (а не в год, как для остальных угроз). Поэтому, чтобы получить критичность ресурса в год, необходимо умножить критичность ресурса в час на максимально критичное время простоя ресурса за год.

Таблица 6. Риск ресурса

Угроза/Уязвимость	Общий уровень угроз по ресурсу (%), CThR	Риск ресурса (у.е.), R
Угроза 1/Уязвимость 1	0,8511	85,11
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 3		
Угроза 2/Уязвимость 4		
Угроза 3/Уязвимость 5		
Угроза 3/Уязвимость 6		

В результате получили риск ресурса, который рассчитан по модели угроз и уязвимостей.

Рассмотрим итоги, в которых уровень угрозы Th > 0,1.

Итог 1

Контрмеры.Название	Обеспечение безопасности поддерживающей инфраструктуры
Угрозы.Название	Неавторизованная модификация информации в системе электронной почты, хранящейся на ресурсе
Уязвимости.Название	Отсутствие авторизации для внесения изменений в систему электронной почты
Уровень	0,24

Итог 2

Контрмеры.Название	Обеспечение физической безопасности
Угрозы.Название	Неавторизованное проникновение нарушителя внутрь охраняемого периметра
Уязвимости.Название	Отсутствие системы наблюдения за объектом или существующая система наблюдения охватывает не все важные объекты
Уровень	0,12

Итог 3

Контрмеры.Название	Обеспечение безопасности на сетевом уровне
Угрозы.Название	Неавторизованное проникновение нарушителя внутрь охраняемого периметра
Уязвимости.Название	Отсутствие регламента доступа в помещения с ресурсами, содержащими ценную информацию
Уровень	0,3

Итог 4

Контрмеры.Название	Меры безопасности на уровне системного администратора
Угрозы.Название	Разглашение конфиденциальной информации сотрудниками компании
Уязвимости.Название	Распределение атрибутов безопасности между несколькими доверенными сотрудниками
Уровень	0,64

4 Обеспечение безопасности жизнедеятельности администрирования телекоммуникационной системы

Данная инструкция предназначена для предотвращения неблагоприятных воздействий на человека вредного фактора, который сопровождается работой со средствами вычислительной техники и периферийным оборудованием.

Инструкция подлежит обязательному и безусловному выполнению. За невыполнение инструкции нарушители несут ответственность в административном и судебном порядках в зависимости от характера последствий нарушения.

Выполнение правил безопасной работы необходимо для предупреждения производственной травмы.

4.1 Область распространения и порядок применения инструкции

Настоящая инструкция создана для персонала, который пользуется вычислительной техникой и периферийным оборудованием. В инструкции находятся указания, как правильно и безопасно применять электрооборудование в помещении. Требования, которые изложены в инструкции, обязательны, никакие отступления от инструкции не должны быть допущены.

Ниже будут указаны требования, которые распространяются на персонал, использующий вычислительную технику и периферийное оборудование:

Самостоятельно использовать электроаппаратуру может только персонал старше 18 лет, который обучен этому и пригоден по состоянию здоровья, а также имеет квалификацию для выполнения возложенных на него работ.

«Перед тем, как приступить к работе, сотрудники должны прослушать первичный и вводный инструктаж по технике безопасности, где показываются безопасные и рациональные приемы работы. Такой

инструктаж должен повторяться через каждые полгода. Также может проводиться внеплановый инструктаж, который имеет место при изменениях правил по охране труда, изменениях характеров работ сотрудников, или же если обнаруживаются нарушения сотрудниками правил техники безопасности.» [30]

В каждом помещении, где используется электрооборудование, должны висеть инструкции по технике безопасности, которые включают в себя действия при возникновении травм, аварий, пожаров.

Руководитель структурного подразделения несет ответственность за то, чтобы организовать правильное и безопасное использование вычислительной техники и периферийного оборудования; контролировать то, чтобы сотрудники выполняли требования инструкции по технике безопасности.

4.2 Виды опасных и вредных факторов

Сотрудники, которые используют вычислительную технику и периферийное оборудование, могут быть подвержены опасным и вредным воздействиям. «Эти воздействия делятся на группы:

– поражение электрическим током;

– механические повреждения;

– электромагнитное излучение;

– инфракрасное излучение;

– опасность пожара;

– повышенный уровень шума и вибрации.» [19]

Для того, чтобы снизить или предотвратить воздействие вредных и опасных факторов, нужно соблюдать санитарные нормы и правила.

4.3 Требования электробезопасности

Во время использования вычислительной техники и периферийного оборудования каждому сотруднику следует аккуратно и внимательно обращаться с электропроводкой, аппаратами и приборами, и всегда знать, что если не соблюдать правила безопасности, то это может угрожать здоровью и жизни человека.

Чтобы избежать поражения электрическим током, нужно выполнять такие правила безопасности, как:

1. Каждый сотрудник должен следить, чтобы все средства, с помощью которых оборудование подключается к сети (электропроводка, розетки, выключатели) находились в исправном состоянии. Если работник обнаружил какое-либо нарушение, ему следует немедленно обесточить электрооборудование и сообщить об этом в администрацию. Продолжать работу разрешается только после устранения неисправности.

2. Чтобы избежать повреждений изоляции проводов и возникновений коротких замыканий, нужно помнить, что нельзя:

а) навешивать какие-либо предметы на провод;

б) красить шнур и провод;

в) закидывать провода и шнуры на газовые и водопроводные трубы, на батареи отопительной системы;

г) выдергивать штепсельную вилку из розетки за шнур, так как, по правилам, усилие должно быть обязательно приложено к телу вилки.

3. Чтобы исключить поражение электрическим током, также не разрешается:

а) часто включать и выключать компьютер без надобности;

б) дотрагиваться до экрана и тыльной стороны блоков компьютера;

в) работать за компьютером сырыми руками;

г) работать на компьютерах, которые имеют повреждения корпуса, нарушена изоляция проводов, неисправное включение питания, которое имеет признаки электрического напряжения на корпус;

д) закидывать на компьютер и оборудование посторонние предметы.

4. Не разрешается под напряжением вытирать пыль и грязь с электрооборудования.

5. Не разрешается проверять исправность электрооборудования в помещениях, которые не приспособлены для его использования, с полами,

которые являются токопроводящими, сырыми, и не позволяют заземлить доступные металлические части.

6. Ремонт аппаратуры должен производиться только обученными специалистами-техниками, которые соблюдают необходимые технические требования.

7. Не разрешается ремонтировать компьютеры и оборудование, которые находятся под напряжением.

8. Чтобы избежать поражение электрическим током, нельзя прикасаться при эксплуатации электроприбора одновременно к каким-нибудь трубопроводам, батареям отопления, металлическим конструкциям, которые соединены с землей.

9. Если приходится использовать электроприборы во влажных помещениях, необходимо быть предельно осторожными.

10. Если сотрудник обнаружил оборвавшийся провод, то нужно немедленно сообщить об этом руководящему лицу, изолировать людей от контакта с ним. Важно помнить, что прикосновение к проводу опасно для жизни.

11. Чтобы спасти сотрудника, который пострадал от поражения током, необходимо как можно быстрее освободить его от контакта с электричеством.

В любом случае, если работник пострадал, нужно немедленно вызывать врача. До того времени, когда врач прибудет, нужно скорее приступать к оказанию первой медицинской помощи сотруднику.

Оперативно нужно начать делать искусственное дыхание («рот в рот» или «нос в рот»), или наружный массаж сердца.

Искусственное дыхание нужно производить до того момента, пока не прибудет врач.

4.4 Требования по обеспечению пожарной безопасности

Каждому сотруднику не разрешается иметь огнеопасные вещества на своем рабочем месте.

В помещениях нельзя:

а) разжигать огонь;

б) включать электрооборудование при обнаружении запаха газа;

в) курить;

г) сушить одежду на отопительных приборах;

д) перекрывать вентиляционные отверстия в электроаппаратуре.

Началом огня могут быть:

а) искра, которая образуется во время разряда статического электричества;

б) искры от электрооборудования;

в) искры от трения или удара;

г) открытое пламя.

Если в помещении возникла пожароопасная ситуация, то персонал должен сразу же начинать применять меры по ее ликвидации, одновременно с этим, сотрудники обязаны оповестить об это вышестоящие лица.

Каждое помещение, оснащенное электроприборами, в обязательном порядке должны иметь огнетушители типа ОУ-2 или ОУБ-3.

Заключение

В ходе выполнения работы рассмотрено определение рисков информационной безопасности.

Проанализированы методы управления информационной безопасностью, самым надежным и эффективным является метод CRAMM, его использование инструментального средства типа метода при проведении анализа риска информационной системы с повышенным требованием в области информационной безопасности. Что позволяет получить обоснованную оценку существующих и допустимых уровней угроз, уязвимостей и эффективности защиты.

Методы управления информационной безопасностью анализировались по следующим показателям:

– простой алгоритм анализа рисков;

– простым интерфейсом;

– эффективность и надежность метода;

– стоимость метода.

На основе анализа существующих методов управления информационной безопасностью предложена методика выбора правил управления информационной безопасности телекоммуникационной сети, включающая пошаговый алгоритм. На основе этой методики разработана база данных, в которой хранятся сведения об угрозах, уязвимостях, методах устранения. Разработанная база данных позволяет подобрать определенные контрмеры по рассчитанному риску.

Все основные задачи, поставленные в задании к дипломному проекту, были успешно выполнены, а именно:

– изучены методы определения рисков информационной безопасности;

– изучены основные методы управления информационной безопасностью;

– разработана методика управления информационной безопасностью телекоммуникационной сети.

Список использованной литературы

1. Лекция 1: Основы информационной безопасности [Электронный ресурс]. URL:http://www.intuit.ru/studies/courses/697/553/lecture/12442 (дата обращения 11.10.2016)

2. Управление информационной безопасностью [Электронный ресурс]. URL:http://center-yf.ru/data/Menedzheru/upravlenie-informacionnoy-bezopasnostyu.php (дата обращения 23.10.2016)

3. Методы защиты информации в телекоммуникационных сетях [Электронный ресурс]. URL:http://www.bibliofond.ru/view.aspx?id=607503 (дата обращения 13.11.2016)

4. Криптографические методы защиты информации [Электронный ресурс]. URL:https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema6 (дата обращения 17.12.2016)

5. Федеральный закон от 10 января 2002 г. N 1-ФЗ "Об электронной цифровой подписи" [Электронный ресурс].
URL:https://rg.ru/2002/01/10/podpis-dok.html (дата обращения 25.12.2016)

6. Все об ЭЦП [Электронный ресурс].
URL:http://my-ecp.ru/sertifikat-klyuch-ecp/ (дата обращения 09.01.2017)

7. Защита информации в современных ИТ [Электронный ресурс]. URL:http://abc.vvsu.ru/books/inform_tehnolog/page0024.asp (дата обращения 11.01.2017)

8. Первый шаг к безопасности [Электронный ресурс]. URL:https://www.osp.ru/pcworld/2003/10/166666/ (дата обращения 20.01.2017)

9. Как организовать управление ИБ? [Электронный ресурс]. URL:http://www.cnews.ru/reviews/free/security2006/articles/admin/ (дата обращения 24.01.2017)

10. Лекция 1: Понятие информационной безопасности. Основные составляющие. Важность проблемы [Электронный ресурс].

URL:http://www.intuit.ru/studies/courses/13757/10/lecture/296?page=3 (дата обращения 25.01.2017)

11. Методы управления рисками информационной безопасности [Электронный ресурс]. URL:https://econ.wikireading.ru/40318 (дата обращения 25.01.2017)

12. Глава 6. Риски в обеспечении информационной безопасности [Электронный ресурс]. URL:http://litread.in/pages/541673/563000-564000?page=25 (дата обращения 30.01.2017)

13. Стандарты обеспечения информационной безопасности [Электронный ресурс]. URL:http://studopedia.ru/7_112422_standarti-obespecheniya-informatsionnoy-bezopasnosti.html (дата обращения 02.02.2017)

14. Международный стандарт ISO/IEC 17799:2005 [Электронный ресурс]. URL:http://www.delta-f.narod.ru/17799.pdf (дата обращения 03.02.2017)

15. Риски информационной безопасности [Электронный ресурс]. URL:http://www.studfiles.ru/preview/5852002/page:12/ (дата обращения 05.02.2017)

16. Анализ и управление рисками информационной безопасности с помощью системы «ГРИФ» [Электронный ресурс]. URL:http://www.rae.ru/forum2012/15/2437 (дата обращения 08.02.2017)

17. Лекция 4: Методики и программные продукты для оценки рисков [Электронный ресурс].
URL:http://www.intuit.ru/studies/courses/531/387/lecture/8996?page=3 (дата обращения 11.02.2017)

18. Методики и технологии управления информационными рисками [Электронный ресурс]. URL:http://citforum.ru/security/articles/risk/ (дата обращения 13.02.2017)

19. Техника безопасности [Электронный ресурс].
URL: http://www.generallytech.ru/gentecs-70-1.html (дата обращения 14.02.2017)

20. Семененко В. А. Информационная безопасность / В.А. Семененко. – М.:МГИУ, 2011. – 277 с.
21. Шаньгин В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – М.: ДМК, 2014. – 702 с.
22. ДеМарко Том, Листер Тимоти. Управление рисками в проектах по разработке программного обеспечения. – М.: Компания p.m.Office, 2005.
23. Ярочкин В., Шевцова Т. Словарь терминов и определений по безопасности и защите информации. – М., 1996.
24. Симонович С. В. Информатика. Базовый курс. – СПб: Питер, 2001. – 640с
25. Мамаева Л. Н. Управление рисками: Учебное пособие / Л. Н. Мамаева. – М.: Дашков и К, 2013. – 256 с.
26. Милославская Н. Г. Управление рисками информационной безопасности: Учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – М.: РиС, 2014. – 130 с.
27. Плошкин В. В. Оценка и управление рисками на предприятиях: Учебное пособие / В. В. Плошкин. – Ст. Оскол: ТНТ, 2013. – 448 с.
28. Черешкин Д. С. Управление рисками и безопасностью / Д. С. Черешкин. – М.: Ленанд, 2010. – 200 с.
29. Крук Б. И. Телекоммуникационные системы и сети. Учебное пособие в 3-х томах / Б. И. Крук. –М.: ГЛТ, 2012. – 620 с.
30. Занько Н. Г. Безопасность жизнедеятельности / Н. Г. Занько, К. Р. Малаян и др. –СПб.: Лань, 2016. – 696 с.

Приложение 1

Диск с электронной версией диплома, презентацией и базой данных: