Деятельность современной компании невозможна без использования информационных технологий. Эффективное применение информационных технологий является общепризнанным фактором конкурентоспособности компании. Многие предприятия в мире переходят к использованию широких возможностей Интернета и электронного бизнеса. Корпоративные информационные системы (КИС) становятся сегодня одним из главных инструментов управления бизнесом и фактически важнейшим средством производства современной компании. В таких условиях одним из наиболее ценных ресурсов организации является корпоративная информация. Все больше корпоративных систем, приложений и данных становятся доступными из Глобальной сети, вследствие чего компании сталкиваются с возрастающим числом различных угроз для своей информационной инфраструктуры - несанкционированный доступ, вирусная опасность, атаки типа «отказ в обслуживании» и другие виды вторжений, мишенью для которых становятся приложения, компьютерные сети и инфраструктура КИС. Поэтому применение информационных технологий немыслимо без повышенного внимания к вопросам информационной безопасности. Одной из самых актуальных задач, которая стоит сегодня перед разработчиками и поставщиками информационных технологий, является решение проблем информационной безопасности, связанных с широким распространением Интернета, интранета и экстранета. Реализация решений для электронного бизнеса должна обеспечивать хорошую защиту, конфиденциальность транзакций, предоставлять защиту целостности выполнения деловых операций и данных заказчиков, а также гарантировать постоянный доступ к данным. Информация должна быть доступна только тем, кому она предназначена, и скрыта от сторонних наблюдателей. Несанкционированное использование информационного ресурса, его временная недоступность или разрушение могут нанести компании значительный материальный ущерб. На сегодняшний день, юридически сформулированы три принципа информационной безопасности, которая должна обеспечивать: - целостность данных; - конфиденциальность информации; - доступность информации для всех зарегистрированных пользователей. По убеждению экспертов, задача обеспечения информационной безопасности должна решаться системно. Это означает, что различные средства защиты должны применяться одновременно и под централизованным управлением. При этом компоненты системы должны «знать» о существовании друг друга, взаимодействовать и обеспечивать защиту, как от внешних, так и от внутренних угроз. На сегодняшний день существует большой арсенал методов обеспечения информационной безопасности: средства идентификации и аутенфикации пользователей (так называем комплекс ЗА); средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям; межсетевые экраны; виртуальные частные сети; средства контентной фильтрации; инструменты

проверки целостности содержимого дисков; средства антивирусной защиты; системы обнаружения уязвимости сетей и анализаторы сетевых атак. Каждое из перечисленных средств может быть использовано как самостоятельно, так и в интеграции с другими. Это делает возможным создание систем информационной защиты для сетей любой сложности и конфигурации, не зависящих от используемых платформ. Обеспечение информационной безопасности - достаточно дорогой процесс. Прежде всего, надо определить необходимый уровень защищенности. Может быть так, что достаточно просто защитить определенный компьютер системой паролей и закрыть помещение "железной дверью", а возможны случаи, когда кроме многоуровневой системы контроля доступа необходима система шифрования передаваемой информации, например, в радиоканале, с использованием сложного шифра, включая процедуры аутентификации и идентификации. Выбор необходимой степени защиты информации и средств ее обеспечения является важной задачей и должен учитывать ряд параметров: уровень секретности информации; ее стоимость; время, в течение которого она должна оставаться в тайне и т.д. Проблема защиты информационных ресурсов в настоящее время приобретает все большее значение. Задачу управления безопасностью можно рассматривать как задачу оптимизации расходования ресурсов на локализацию угроз. Для этого целесообразно: - правильно идентифицировать источники угроз; - оценить степень серьезности угроз, т.е. оценить уровень ресурсов источника угрозы и цели, которые он ставит; - выделить группы источников угроз по целям, ресурсам, интересам; - произвести оптимальное выделение ресурсов и локализацию угроз. Учитывая то, что оптимизация использования ресурсов производится в зависимости от свойств источников угроз, можно отойти от традиционной схемы классификации видов безопасности (физическая, техническая, экономическая и т.д.) и рассмотреть проблему с точки зрения классификации источников угроз в зависимости от места их возникновения как наиболее общего свойства. Предположив, что субъект безопасности (например, предприятие) имеет внутреннюю среду, внешнюю среду и границу между внутренней и внешней средой, можно классифицировать источники угроз как внутренние, внешние и пограничные. При этом пограничные источники, являются синтетическими, т.е. объединением внутренних и внешних угроз. Это создаёт кумулятивный эффект – суммарная сила воздействия этих угроз на субъект (т.е. вероятный ущерб) увеличивается во много раз, т.е. мультиплицируется. Причиной внешних угроз является борьба конкурирующих субъектов (или систем) за общие ресурсы, а внутренних угроз – наличие внутри субъекта множества элементов (подструктур), для которых привычный режим функционирования стал в силу ряда обстоятельств недопустимым. Целью же угрозы является вывод системы (субъекта) за пределы допустимого состояния. По своему характеру угрозы можно классифицировать следующим образом.

Явной угрозой для системы является такая входящая информация, которая воспринимается как угроза. При этом угроза может быть реальной, а может быть блефом, что определяется при анализе угрозы. Явная угроза предполагает, что за ней последуют определенные действия, наносящие системе ущерб. Но раз следуют конкретные физические действия, то значит, существуют конкретные потенциальные возможности противодействия и защиты с использованием различных способов и алгоритмов. Оценивая серьезность угроз по максимально возможному ущербу или степени влияния на выживание субъекта, можно проранжировать источники угроз по важности следующим образом: пограничные (мультиплицированные) – первые; внутренние – вторые; внешние – третьи. Естественно, что данное ранжирование зависит от конкретного случая. Затем проводится анализ реальности угроз и выделение группы угроз, которые могут нанести максимальный вероятный ущерб при реализации, как все вместе, так и по отдельности (расчет ведется по самому низкому уровню безопасности или максимальному возможному ущербу). Их локализация может быть проведена в ходе единого мероприятия (мероприятие здесь понимается в общем смысле, в том числе создание соответствующей структуры системы безопасности для компании). Таким образом, правильно управляя ресурсами фирмы и производя их оптимальные затраты, можно эффективно решать вопросы безопасности. Важность аналитики при подобном подходе переоценить невозможно[1]. Для решения данной задачи были разработаны программные комплексы анализа и контроля информационных рисков: британский CRAMM (компания Insight Consulting), американский RiskWatch (компания RiskWatch) и российский ГРИФ (компания Digital Security). Рассмотрим далее данные методы и построенные на их базе программные системы. Метод CRAMM (CCTA Risk Analysis and Managment Method) был разработан Агентством по компьютерам и телекоммуникациям Великобритании (Central Computer and Telecommunications Agency) по заданию Британского правительства и взят на вооружение в качестве государственного стандарта. Он используется, начиная с 1985 г., правительственными и коммерческими организациями Великобритании. За это время CRAMM приобрел популярность во всем мире. Фирма Insight Consulting Limited занимается разработкой и сопровождением одноименного программного продукта, реализующего метод CRAMM. Метод CRAMM (www.cramm.com) выбран для более детального рассмотрения, и не случайно. В настоящее время CRAMM - это довольно мощный и универсальный инструмент, позволяющий, помимо анализа рисков, решать также и ряд других аудиторских задач, включая: проведение обследования ИС и выпуск сопроводительной документации на всех этапах его проведения; проведение аудита в соответствии с требованиями Британского правительства, а также стандарта BS 7799:1995 «Code of Practice for Information Security Management»; разработка политики безопасности и плана обеспечения непрерывности бизнеса. В основе метода CRAMM лежит

комплексный подход к оценке рисков, сочетая количественные и качественные методы анализа. Метод является универсальным и подходит как для больших, так и для мелких организаций, как правительственного, так и коммерческого сектора. Версии программного обеспечения CRAMM, ориентированные на разные типы организаций, отличаются друг от друга своими базами знаний (profiles). Для коммерческих организаций имеется Коммерческий профиль (Commercial Profile), для правительственных организаций - Правительственный профиль (Government profile). Правительственный вариант профиля, также позволяет проводить аудит на соответствие требованиям американского стандарта ITSEC (Оранжевая книга>). Грамотное использование метода CRAMM позволяет получать очень хорошие результаты, наиболее важным из которых, пожалуй, является возможность экономического обоснования расходов организации на обеспечение информационной безопасности и непрерывности бизнеса. Экономически обоснованная стратегия управления рисками позволяет, в конечном итоге, экономить средства, избегая неоправданных расходов. CRAMM предполагает разделение всей процедуры на три последовательных этапа. Задачей первого этапа является ответ на вопрос: «Достаточно ли для защиты системы применения средств базового уровня, реализующих традиционные функции безопасности, или необходимо проведение более детального анализа?» На втором этапе производится идентификация рисков и оценивается их величина. На третьем этапе решается вопрос о выборе адекватных контрмер. Методика CRAMM для каждого этапа определяет набор исходных данных, последовательность мероприятий, анкеты для проведения интервью, списки проверки и набор отчетных документов. На первой стадии исследования производится идентификация и определение ценности защищаемых ресурсов. Оценка производится по десятибалльной шкале, причем критериев оценки может быть несколько - финансовые потери, потери репутации и т.д. В описаниях CRAMM в качестве примера приводится такая шкала оценки по критерию "Финансовые потери, связанные с восстановлением ресурсов": - 2 балла - менее $1000; - 6 баллов - от $1000 до $10 000; - 8 баллов - от $10 000 до $100 000; - 10 баллов - свыше $100 000. При низкой оценке по всем используемым критериям (3 балла и ниже) считается, что рассматриваемая система требует базового уровня защиты (для этого уровня не требуется подробной оценки угроз ИБ) и вторая стадия исследования пропускается. На второй стадии идентифицируются и оцениваются угрозы в сфере информационной безопасности, производится поиск и оценка уязвимостей защищаемой системы. Уровень угроз оценивается по следующей шкале: очень высокий, высокий, средний, низкий, очень низкий. Уровень уязвимости оценивается как высокий, средний или низкий. На основе этой информации вычисляется оценка уровня риска по семибальной шкале. На третьей стадии CRAMM генерирует варианты мер противодействия выявленным рискам. Продукт

предлагает рекомендации следующих типов: - рекомендации общего характера; - конкретные рекомендации; - примеры того, как можно организовать защиту в данной ситуации. - CRAMM имеет обширную базу, содержащую описание около 1000 примеров реализации подсистем защиты различных компьютерных систем. Данные описания можно использовать в качестве шаблонов. - Решение о внедрении в систему новых механизмов безопасности и модификация старых принимает руководство организации, учитывая связанные с этим расходы, их приемлемость и конечную выгоду для бизнеса. Задачей аудитора является обоснование рекомендуемых контрмер для руководства организации. - В случае принятия решения о внедрении новых контрмер и модификации старых, на аудитора может быть возложена задача подготовки плана внедрения новых контрмер и оценки эффективности их использования. Решение этих задач выходит за рамки метода CRAMM. - К недостаткам метода CRAMM можно отнести следующее: - использование метода CRAMM требует специальной подготовки и высокой квалификации аудитора; - CRAMM в гораздо большей степени подходит для аудита уже существующих ИС, находящихся на стадии эксплуатации, нежели чем для ИС, находящихся на стадии разработки; - аудит по методу CRAMM - процесс достаточно трудоемкий и может потребовать месяцев непрерывной работы аудитора; - программный инструментарий CRAMM генерирует большое количество бумажной документации, которая не всегда оказывается полезной на практике; - CRAMM не позволяет создавать собственные шаблоны отчетов или модифицировать имеющиеся; - возможность внесения дополнений в базу знаний CRAMM не доступна пользователям, что вызывает определенные трудности при адаптации этого метода к потребностям конкретной организации; - программное обеспечение CRAMM существует только на английском языке; - стоимость лицензии от 2000 до 5000 долл. Программное обеспечение RiskWatch (www.riskwatch.com) является мощным средством анализа и управления рисками. В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности. Оно включает в себя следующие средства аудита и анализа рисков: RiskWatch for Physical Security для физических методов защиты ИС; RiskWatch for Information Systems для информационных рисков; HIPAA-WATCH for Healthcare Industry - дляоценкисоответствиятребованиямстандарта HIPAA (US Healthcare Insurance Portability and Accountability Act); RiskWatch RW17799 for ISO 17799 для оценки требованиям стандарта ISO 17799. В методе RiskWatch в качестве критериев для оценки и управления рисками используются предсказание годовых потерь (Annual Loss Expectancy, ALE) и оценка возврата от инвестиций (Return on Investment, ROI). Семейство программных продуктов RiskWatch имеет массу достоинств. RiskWatch помогает провести анализ рисков и сделать обоснованный выбор мер и средств защиты. Используемая в программе методика включает в себя 4 фазы. В отличие от CRAMM, программа RiskWatch более ориентирована на

точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. Надо также отметить, что в этом продукте риски в сфере информационной и физической безопасности компьютерной сети предприятия рассматриваются совместно. В основе продукта RiskWatch находится методика анализа рисков, которая состоит из четырех этапов. Первый этап - определение предмета исследования. Здесь описываются такие параметры, как тип организации, состав исследуемой системы (в общих чертах), базовые требования в области безопасности. Для облегчения работы аналитика, в шаблонах, соответствующих типу организации ("коммерческая информационная система", "государственная/военная информационная система" и т.д.), есть списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты. Из них нужно выбрать те, что реально присутствуют в организации. Например, категории потерь: - Задержки и отказ в обслуживании; - Раскрытие информации; - Прямые потери (например, от уничтожения оборудования огнем); - Жизнь и здоровье (персонала, заказчиков и т.д.); - Изменение данных; - Косвенные потери (например, затраты на восстановление); - Репутация. - Определение категорий защищаемых ресурсов. Второй этап - 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. Вопросы связаны с категориями ресурсов. - Задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов. Все это используется в дальнейшем для расчета эффекта от внедрения средств защиты. Третий и, наверное, самый важный этап - количественная оценка. На этом этапе рассчитывается профиль рисков, и выбираются меры обеспечения безопасности. Сначала устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих шагах исследования (риск описывается совокупностью этих четырех параметров). Фактически, риск оценивается с помощью математического ожидания потерь за год. Например, если стоимость сервера $150000, а вероятность того, что он будет уничтожен пожаром в течение года равна 0.01, то ожидаемые потери составят $1500. Общеизвестная формула (m=p*v , где m-математическое ожидание, p - вероятность возникновения угрозы, v - стоимость ресурса) претерпела некоторые изменения, в связи с тем, что RiskWatch использует определенные американским институтом стандартов NIST оценки, называемые LAFE и SAFE. LAFE (Local Annual Frequency Estimate) - показывает, сколько раз в год в среднем данная угроза реализуется в данном месте (например, в городе). SAFE (Standard

Annual Frequency Estimate) - показывает, сколько раз в год в среднем данная угроза реализуется в этой "части мира" (например, в Северной Америке). Вводится также поправочный коэффициент, который позволяет учесть, что в результате реализации угрозы защищаемый ресурс может быть уничтожен не полностью, а только частично. 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. RiskWatch включает в себя базы с оценками LAFE и SAFE, а также с обобщенным описанием различных типов средств защиты. Эффект от внедрения средств защиты количественно описывается с помощью показателя ROI (Return on Investment отдача от инвестиций), который показывает отдачу от сделанных инвестиций за определенный период времени. Рассчитывается он по формуле: ROI =, где Costsi - затраты на внедрение и поддержание i-меры защиты; Benefitsi - оценка той пользы (т.е. ожидаемого снижения потерь), которую приносит внедрение данной меры защиты; NPV (Net Present Value) - дает поправку на инфляцию. Четвертый этап - генерация отчетов. Типы отчетов: - Краткие итоги. - Полные и краткие отчеты об элементах, описанных на стадиях 1 и 2. - Отчет от стоимости защищаемых ресурсов и ожидаемых потерях от реализации угроз. - Отчет об угрозах и мерах противодействия. - Отчет о ROI. - Отчет о результатах аудита безопасности. Таким образом, рассматриваемое средство позволяет оценить не только те риски, которые сейчас существуют у предприятия, но и ту выгоду, которую может принести внедрение физических, технических, программных и прочих средств и механизмов защиты. Подготовленные отчеты и графики дают материал, достаточный для принятия решений об изменении системы обеспечения безопасности предприятия. Для отечественных пользователей проблема заключается в том, что получить используемые в RiskWatch оценки (такие как LAFE и SAFE) для наших условий достаточно проблематично. Хотя сама методология может с успехом применяться и у нас. К недостаткам RiskWatch можно отнести: - Такой метод подходит, если требуется провести анализ рисков на программно-техническом уровне защиты, без учета организационных и административных факторов. - Полученные оценки рисков (математическое ожидание потерь) далеко не исчерпывает понимание риска с системных позиций - метод не учитывает комплексный подход к информационной безопасности. - Программное обеспечение RiskWatch существует только на английском языке. - Высокая стоимость лицензии (от 10 000 долл. за одно рабочее место для небольшой компании). ГРИФ - комплексная система анализа и управления рисками информационной системы компании. ГРИФ 2006 из состава Digital Security Office (http://www.dsec.ru/products/grif/) дает полную картину защищенности информационных ресурсов в системе и позволяет выбрать оптимальную стратегию защиты информации компании.

Система ГРИФ: - Анализирует уровень защищенности всех ценных ресурсов компании - Оценивает возможный ущерб, который понесет компания в результате реализации угроз информационной безопасности - Позволяет эффективно управлять рисками при помощи выбора контрмер, наиболее оптимальных по соотношению цена/качество Как работает система ГРИФ: Система ГРИФ 2006 предоставляет возможность проводить анализ рисков информационной системы при помощи анализа модели информационных потоков, а также, анализируя модель угроз и уязвимостей в зависимости от того, какими исходными данными располагает пользователь, а также от того, какие данные интересуют пользователя на выходе. При работе с моделью информационных потоков в систему вносится полная информация обо всех ресурсах с ценной информацией, пользователях, имеющих доступ к этим ресурсам, видах и правах доступа. Заносятся данные обо всех средствах защиты каждого ресурса, сетевые взаимосвязи ресурсов, а также характеристики политики безопасности компании. В результате получается полная модель информационной системы. На первом этапе работы с программой пользователь вносит все объекты своей информационной системы: отделы, ресурсы (специфичными объектами данной модели являются сетевые группы, сетевые устройства, виды информации, группы пользователей, бизнес-процессы). Далее пользователю необходимо проставить связи, т.е. определить к каким отделам и сетевым группам относятся ресурсы, какая информация хранится на ресурсе, и какие группы пользователей имеют к ней доступ. Также пользователь системы указывает средства защиты ресурса и информации. На завершающем этапе пользователь отвечает на список вопросов по политике безопасности, реализованной в системе, что позволяет оценить реальный уровень защищенности системы и детализировать оценки рисков. Наличие средств информационной защиты, отмеченных на первом этапе, само по себе еще не делает систему защищенной в случае их неадекватного использования и отсутствия комплексной политики безопасности, учитывающей все аспекты защиты информации, включая вопросы организации защиты, физической безопасности, безопасности персонала, непрерывности ведения бизнеса и т.д. В результате выполнения всех действий по данным этапам, на выходе сформирована полная модель информационной системы с точки зрения информационной безопасности с учетом реального выполнения требований комплексной политики безопасности, что позволяет перейти к программному анализу введенных данных для получения комплексной оценки рисков и формирования итогового отчета. Работа с моделью анализа угроз и уязвимостей подразумевает определение уязвимостей каждого ресурса с ценной информацией, и подключение соответствующих угроз, которые могут быть реализованы через данные уязвимости. В результате получается полная картина того, какие слабые места есть в информационной системе и тот ущерб, который

может быть нанесен. На первом этапе работы с продуктом пользователь вносит объекты своей информационной системы: отделы, ресурсы (специфичными объектами для данной модели: угрозы информационной системы, уязвимости, через которые реализуются угрозы). Система ГРИФ 2006 содержит обширные встроенные каталоги угроз и уязвимостей. Для достижения максимальной полноты и универсальности данных каталогов, экспертами Digital Security была разработана специальная классификация угроз DSECCT, в которой реализован многолетний практический опыт в области информационной безопасности. Используя каталоги угроз и уязвимостей, пользователь может выбрать угрозы и уязвимости, относящиеся к его информационной системе. Каталоги содержат около 100 угроз и 200 уязвимостей. Далее пользователю необходимо проставить связи, т.е. определить к каким отделам относятся ресурсы, какие угрозы действуют на ресурс и через какие уязвимости они реализуются. Алгоритм системы ГРИФ 2006 анализирует построенную модель и генерирует отчет, который содержит значения риска для каждого ресурса. Конфигурации отчета может быть практически любой, таким образом позволяя пользователю создавать как краткие отчеты для руководства, так и детальные отчеты для дальнейшей работы с результатами. Система ГРИФ 2006 содержит модуль управления рисками, который позволяет проанализировать все причины того значения риска, который получается после обработки алгоритмом занесенных данных. Таким образом, зная причины, Вы будете обладать всеми данными, необходимыми для реализации контрмер и, соответственно, снижения уровня риска. Благодаря расчету эффективности каждой возможной контрмеры, а также определению значения остаточного риска, Вы сможете выбрать наиболее оптимальные контрмеры, которые позволят снизить риск до необходимого уровня с наименьшими затратами. В результате работы с системой ГРИФ строится подробный отчет об уровне риска каждого ценного ресурса информационной системы компании, все причины риска с подробным анализом уязвимостей и оценкой экономической эффективности всех возможных контрмер. Лучшие мировые практики и ведущие международные стандарты в области информационной безопасности, в частности ISO 17799, требуют для эффективного управления безопасностью информационной системы внедрения системы анализа и управления рисками. При этом можно использовать любые удобные инструментальные средства, но, главное - всегда четко понимать, что система информационной безопасности создана на основе анализа информационных рисков, проверена и обоснована. Анализ и управление информационными рисками ключевой фактор для построения эффективной защиты информационной системы. Резюмируя все вышеизложенное, можно прийти к выводу, что задача построения оптимальной структуры системы информационной безопасности как части управляющей подсистемы компании сводится к достаточно изученной задаче построения системы управления

объектом или системы управления производством, если рассматривать это через призму экономических показателей. В общем виде такая система управления производством безопасности, встроенная в систему управления компании, может быть изображена как совокупность двух подсистем, причем система безопасности является частью управляющей подсистемы, представляя собой в большей части систему сбора, анализа и обработки информации, а также выдачу информационных управляющих воздействий по управлению всеми возможными ресурсами компании.