Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Студент: Костюкова А.О.

ИТ 2 курс 4 группа

Преподаватель: Буснюк Н. Н.

Минск 2020

**Практическое занятие №3**

**Тема «Разработка политики информационной безопасности бизнес-компании»**

Цель: Разработать проект политики информационной безопасности бизнес-компании.

**Введение**

В век информационных технологий мы имеем выбор хранения информации, таким образом мы можем хранить её:

* На бумажных носителях;
* На различных цифровых носителях.

Каждый день мы используем устройства, из которых мы считываем довольно большие объёмы информации, либо заносим туда свою информацию, которая может быть сугубо личной, либо открытой для всех, так же это относится и к компании. Так что главной задачей для всех является защита своей информации, что является довольно сложной задачей в связи с развитием технологий и появлением глобальной сети. Модели угроз и нарушителей должны быть основным инструментом менеджмента нашей организации при развертывании, поддержании и совершенствовании системы обеспечения информационной безопасности организации.

Информационные ресурсы в современном обществе являются наиболее значимыми, но при этом, очень уязвимыми т.к. механизм их распространения становится все более гибким и количество возможностей их передачи растет. В связи с этим информационная безопасность — одно из важнейших условий функционирования любой структуры, будь то государственное учреждение или частное предприятие.

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории Беларуси. Поэтому решение вопроса об разработке эффективной политики информационной безопасности на современном предприятии обязательно связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации.

Пока не существует формальных методов нейтрализации угроз безопасности информации. По этой причине разработка мер по защите информации должна производиться на основе знаний и опыта соответствующих специалистов (каждый член бригады, выполняющей лабораторную работу, является специалистом - экспертом по защите конфиденциальной информации). Однако в интересах минимизации ошибок процесс разработки должен соответствовать следующим рекомендациям.

Разработку мер защиты информации целесообразно начинать с угроз, имеющих максимальное значение; далее - с меньшей угрозой, и так далее до тех пор, пока не будут исчерпаны выделенные ресурсы. Такой подход гарантирует, что даже при малых ресурсах хватит ресурсов для предотвращения наиболее значимых угроз. Для каждой угрозы разрабатываются меры (способы и средства) по защите информации.

**Описание структуры компаний «ИКЕА»**



Рис.1 Структура группы компаний «ИКЕА»

Организационная структура кампании состоит из следующих основных отделов:

* Коммерческий департамент;
* Производственный отдел;
* Отдел управления персоналом.

Таким образом, вся деятельность кампании, связанная с реализацией проектов, сосредоточена в этих трёх отделах.

Наряду с основными отделами в кампаниях действует ряд обслуживающих отделов:

* Бухгалтерия;
* Отдел материального снабжения;
* Отдел маркетинга и рекламы;
* Административно-хозяйственный отдел.

*Генеральный директор* — осуществляет общее руководство кампанией.

*Технический директор* — сотрудник, возглавляющий команду, который следит за выполнением работы над реализацией проекта. Он уделяет рабочее время каждому проекту в отдельности. Его задача — слежение за реализацией концепции каждого проекта и координация работы каждого сотрудника, который работает над данным проектом.

*Маркетинговый отдел* — это люди, которые отслеживают состояние дел на рынке услуг, которые предоставляет наша кампания, то есть таргетиврованная реклама в соц. сетях и продвижение новых проектов. Они выясняют, что хорошо продается, а что плохо, какие направления перспективны, а какие нет. Директор по маркетингу определяет размер рекламного бюджета. Сотрудники отдела также занимаются всеми промоушен-материалами и мероприятиями — от каталогов до семинаров для сотрудников. Основная задача маркетингового отдела — увеличение продаж и конкурентоспособности компании.

*Отдел PR* — это люди, которые занимаются пиаром проектов и самой кампании. Они работают с прессой и интернет-аудиторией, организуют встречи с заказчиками.

Эффективность управления деятельностью зависит оттого, насколько грамотно сформирована организационная структура управления и насколько она соответствует цели деятельности организации.

В настоящее время под организационной структурой понимается упорядоченная совокупность устойчиво взаимосвязанных элементов, обеспечивающих функционирование и развитие организации как единого целого. Структура управления определяется также как форма разделения и кооперации управленческой деятельности. Можно сказать, что структура управления есть не что иное, как оптимальное распределение работы, прав и ответственности, порядка и форм взаимодействия между членами коллектива организации.

Составляющими организационных структур являются:

* элементы организационных структур управления — службы или органы аппарата управления, а также отдельные работники этих служб (органов);
* организационные отношения — отношения (связи) между подразделениями организации, уровнями ее управления, персоналом, посредством которых реализуются функции управления;
* уровни управления — совокупность прав, обязанностей и ответственности, характерная для должностных лиц, занимающих определенную ступень в иерархической структуре организации.

**Оценка рисков**

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения:

* антропогенные,
* техногенные,
* естественные (природные).

Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала, так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека. К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные, включая экстремальные климатические условия, метеорологические явления, стихийные бедствия. Источники угроз по отношению к инфраструктуре Главпочтамта могут быть как внешними, так и внутренними.

Источниками внутренних угроз являются:

* сотрудники организации;
* программное обеспечение;
* аппаратные средства.

К информационным угрозам относятся:

* несанкционированный доступ к информационным ресурсам;
* незаконное копирование данных в информационных системах;
* противозаконный сбор и использование информации;
* использование информационного оружия.

К программным угрозам относятся:

* использование ошибок и «дыр» в ПО;
* компьютерные вирусы и вредоносные программы;

К физическим угрозам относятся:

* уничтожение или разрушение средств обработки информации и связи;

**Разработка мер защиты**

Всем сотрудникам компании, в которой установлена система контроля доступа, выдаются специальные электронные пропуска, например, проксимити идентификаторы, представляющие собой пластиковые карты или брелоки, которые содержат персональные коды доступа. Считыватели, устанавливаемые у входа в контролируемое помещение, распознают код идентификаторов. Информация поступает в систему контроля доступа, которая на основании анализа данных о владельце идентификатора, принимает решение о допуске или запрете прохода сотрудника на охраняемую территорию. В случае разрешения доступа, система приводит в действие исполнительные устройства, такие как электромеханические замки, турникеты, автоматические шлагбаумы или приводы ворот. В противном случае двери блокируются, включается сигнализация и оповещается охрана.

Построение надежной защиты включает оценку циркулирующей в компьютерной системе информации с целью уточнения степени ее конфиденциальности, анализа потенциальных угроз ее безопасности и установление необходимого режима ее защиты.

Отдельный раздел законопроекта "О коммерческой тайне", посвященный организации защиты коммерческой информации, определяет необходимый комплекс мероприятий по ее защите:

* установление особого режима конфиденциальности;
* ограничение доступа к конфиденциальной информации;
* использование организационных мер и технических средств защиты информации;
* осуществление контроля за соблюдением установленного режима конфиденциальности.

Установление особого режима конфиденциальности направлено на создание условий для обеспечения физической защиты носителей конфиденциальной информации. Как правило, особый режим конфиденциальности подразумевает:

* организацию охраны помещений, в которых содержатся носители конфиденциальной информации;
* установление режима работы в помещениях, в которых содержатся носители конфиденциальной информации;
* установление пропускного режима в помещения, содержащие носители конфиденциальной информации;
* закрепление технических средств обработки конфиденциальной информации за сотрудниками, определение персональной ответственности за их сохранность;
* установление порядка пользования носителями конфиденциальной информации (учет, хранение, передача другим должностным лицам, уничтожение, отчетность);
* организацию ремонта технических средств обработки конфиденциальной информации;
* организацию контроля за установленным порядком.

Эффективность защиты информации в автоматизированных системах достигается применением средств защиты информации (СЗИ). Под средством защиты информации понимается техническое, программное средство или материал, предназначенные или используемые для защиты информации. В настоящее время на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на несколько групп:

* средства, обеспечивающие разграничение доступа к информации в автоматизированных системах;
* средства, обеспечивающие защиту информации при передаче ее по каналам связи;
* средства, обеспечивающие защиту от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем;
* средства, обеспечивающие защиту от воздействия программ-вирусов;
* материалы, обеспечивающие безопасность хранения, транспортировки носителей информации и защиту их от копирования.

Радикальным способом защиты информации от утечки по физическим полям является электромагнитное экранирование технических устройств и помещений, однако это способ требует значительных капитальных затрат и практически не применяется.

Обеспечение требуемой защиты информационных ресурсов предприятий в этих условиях достигается применением дополнительных инструментальных средств. К их числу относятся:

* средства анализа защищенности операционных систем и сетевых сервисов;
* средства обнаружения опасных информационных воздействий (атак) в сетях.

Средства анализа защищенности операционных систем позволяют осуществлять ревизию механизмов разграничения доступа, идентификации и аутентификации, средств мониторинга, аудита и других компонентов операционных систем с точки зрения соответствия их настроек и конфигурации установленным в организации. Кроме этого, средствами данного класса проводится контроль целостности и неизменности программных средств и системных установок, и проверка наличия уязвимостей системных и прикладных служб. Как правило, такие проверки проводятся с использованием базы данных уязвимостей операционных систем и сервисных служб, которые могут обновляться по мере выявления новых уязвимостей.

В информационной сфере с целью нейтрализации внутренних источников угроз национальной безопасности совершенствуются механизмы реализации прав граждан на получение, хранение, пользование и распоряжение информацией, в том числе с использованием современных информационно-коммуникационных технологий. Государство гарантирует обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удаленного, и возможностям получения информационных услуг. Значимым этапом станет разработка и реализация стратегии всеобъемлющей информатизации, ориентированной на развитие электронной системы осуществления административных процедур, оказываемых гражданам и бизнесу государственными органами и иными организациями, и переход государственного аппарата на работу по принципу информационного взаимодействия. Ускоренными темпами будет развиваться индустрия информационных и телекоммуникационных технологий. Особое внимание будет уделяться последовательному повышению качества, объема и конкурентоспособности национального контента, который призван занимать доминирующее положение внутри страны, и его продвижению во внешнее информационное пространство.

Приоритетным направлением является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством. Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

Специалисты компании IBM выделяют четыре основных этапа построения системы безопасности:

* идентификация информационных рисков и методов борьбы с ними;
* описание мер защиты активов в соответствии с задачами и целями компании;
* описание действий при происшествиях;
* анализ остаточных рисков и принятие решение о дополнительном капиталовложении в методы обеспечения безопасности;

Ответ на вопрос «Что нужно защищать?» - основной аспект политики информационной безопасности, в соответствии со стратегией IBM. Политика должна создаваться с целью минимальных её изменений в будущем. Эффективная политика безопасности должна содержать:

* цели и задачи обеспечения информационной безопасности;
* взаимодействие со стандартами безопасности и законодательством;
* расширение знаний по вопросам информационной безопасности;
* выявление и ликвидация вирусных атак;
* обеспечение непрерывности деятельности;
* установление ролей и обязанностей персонала;
* журналирование инцидентов нарушения безопасности;

Далее идет процесс создания документации, которая содержит правила анализа рисков компании, описание рекомендуемых методов и средств защиты и так далее. Документация может подлежать изменениям в соответствии с актуальными уязвимостями и угрозами.

Однако, помимо правовой основы, система информационной безопасности и её функции по обеспечению состоянию защищенности объекта должны быть реализованы в соответствии с нижеизложенными принципами:

* легитимность (создание системы информационной безопасности, а также реализация мероприятий по защите, не противоречащих законодательству и нормативам);
* комплексность (разрабатываемая система защиты предусматривает комплексную реализацию методов, обеспечивает защиту информационных ресурсов на техническом и организационном уровнях и предотвращает возможные пути реализации угроз);
* постоянность (обеспечивает непрерывную защиту объектов);
* прогрессивность (подразумевает непрерывное развитие средств и методов защиты, в соответствии с развитием технологий и методов атак);
* рациональность (использование экономически выгодных и эффективных средств защиты);
* ответственность (каждый сотрудник ручается за обеспечение безопасности в рамках своих полномочий);
* контроль (предполагает постоянный контроль над обеспечением защиты и своевременное выявление угроз);
* использование действующей системы безопасности (проектируемая система создается на основе действующей системы, с использованием штатных аппаратных и программных средств);
* использование аппаратно - программных компонентов защиты отечественного производства (проектирование системы безопасности предусматривает преобладание отечественных технических средств защиты);
* этапность (проектирование системы безопасности предпочтительнее делать поэтапно);

Проанализировав существующие политики и стандарты информационной безопасности можно утверждать, что для обеспечения надлежащего уровня информационной защиты требуется комплекс мер, включающий в себя функции программного обеспечения, политики безопасности, методы и организационные структуры. В соответствии с этим и с основной целью необходимо выполнить следующие задачи:

* изучить исходную информационную и организационную структуру группы компаний «ИКЕА»;
* по результатам анализа исходной информационной системы определить конкретные угрозы и уязвимости информационной безопасности;
* определить уровень и класс исходной защищенности объекта;
* выявить актуальные угрозы;
* составить модель нарушителя;
* сопоставить исходную систему с требованиями стандартов безопасности;
* разработать политику безопасности и определить действия по обеспечении информационной безопасности;

Выполнение вышеизложенных целей и задач позволит создать эффективную систему информационной безопасности предприятия, отвечающую требованиям законодательства и стандартам информационной безопасности.

Нейтрализации ряда внутренних источников угроз национальной безопасности способствует информационное обеспечение государственной политики, которое заключается в доведении до граждан Республики Беларусь и внешней аудитории объективной информации о государственном курсе во всех сферах жизнедеятельности общества, официальной позиции по общественно значимым событиям внутри страны и за рубежом, о деятельности государственных органов. Важной задачей при этом является расширение каналов и повышение качества информирования зарубежной общественности. Составной частью информационного обеспечения государственной политики выступает информационное противоборство, представляющее собой комплексное использование информационных, технических и иных методов, способов и средств для воздействия на информационную сферу с целью достижения политических, экономических и иных задач либо защиты собственного информационного пространства.

Защита от внешних угроз национальной безопасности в информационной сфере осуществляется путем участия Республики Беларусь в международных договорах, регулирующих на равноправной основе мировой информационный обмен, в создании и использовании межгосударственных, международных глобальных информационных сетей и систем. Для недопущения технологической зависимости государство сохранит роль регулятора при внедрении иностранных информационных технологий.

В интересах обеспечения национальной безопасности создается комплексная система стратегического планирования. Документы стратегического планирования, основой которых являются настоящая Концепция и программы социально-экономического развития Республики Беларусь, формируются, рассматриваются и утверждаются в порядке, предусмотренном законодательством.

Для защиты от внешних угроз национальной безопасности в научно-технологической сфере должно быть обеспечено проведение научных исследований и разработок в области приоритетных для Республики Беларусь технологий, их расширенное воспроизводство в структуре национальной экономики. Развитие индустрии проектирования компонентной базы производств высших технологических укладов обеспечит материально-техническую основу безопасности функционирования критически важных объектов, систем и инфраструктур.

Стратегическим фактором выступает развитие системы доступа к международным электронным базам данных научной и технической информации, создание системы международных научных лабораторий и центров, а также обеспечение наиболее благоприятных экономических и имиджевых условий для проведения исследований в Беларуси и привлечения инвестиций в ее научно-инновационную сферу, создания новых инновационных предприятий.

Наибольшая эффективность защиты информации достигается при комплексном использовании средств анализа защищенности и средств обнаружения опасных информационных воздействий (атак) в сетях. Средства обнаружения атак в сетях предназначены для осуществления контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирование в случаях нападения на узлы корпоративной сети. Большинство средств данной группы при обнаружении атаки в сети оповещают администратора системы, регистрируют факт нападения в журнале системы и завершают соединение с атакующим узлом. Дополнительно, отдельные средства обнаружения атак позволяют автоматически реконфигурировать межсетевые экраны и маршрутизаторы в случае нападения на узлы корпоративной сети.

В информационной сфере с целью нейтрализации внутренних источников угроз национальной безопасности совершенствуются механизмы реализации прав граждан на получение, хранение, пользование и распоряжение информацией, в том числе с использованием современных информационно-коммуникационных технологий. Государство гарантирует обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удаленного, и возможностям получения информационных услуг. Значимым этапом станет разработка и реализация стратегии всеобъемлющей информатизации, ориентированной на развитие электронной системы осуществления административных процедур, оказываемых гражданам и бизнесу государственными органами и иными организациями, и переход государственного аппарата на работу по принципу информационного взаимодействия. Ускоренными темпами будет развиваться индустрия информационных и телекоммуникационных технологий. Особое внимание будет уделяться последовательному повышению качества, объема и конкурентоспособности национального контента, который призван занимать доминирующее положение внутри страны, и его продвижению во внешнее информационное пространство.

Приоритетным направлением является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством. Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

Нейтрализации ряда внутренних источников угроз национальной безопасности способствует информационное обеспечение государственной политики, которое заключается в доведении до граждан Республики Беларусь и внешней аудитории объективной информации о государственном курсе во всех сферах жизнедеятельности общества, официальной позиции по общественно значимым событиям внутри страны и за рубежом, о деятельности государственных органов. Важной задачей при этом является расширение каналов и повышение качества информирования зарубежной общественности. Составной частью информационного обеспечения государственной политики выступает информационное противоборство, представляющее собой комплексное использование информационных, технических и иных методов, способов и средств для воздействия на информационную сферу с целью достижения политических, экономических и иных задач либо защиты собственного информационного пространства.

Защита от внешних угроз национальной безопасности в информационной сфере осуществляется путем участия Республики Беларусь в международных договорах, регулирующих на равноправной основе мировой информационный обмен, в создании и использовании межгосударственных, международных глобальных информационных сетей и систем. Для недопущения технологической зависимости государство сохранит роль регулятора при внедрении иностранных информационных технологий.

Обобщая все вышесказанное и учитывая возможные виды угрозы/атаки на торговую сеть, можем выделить следующие рекомендации, либо советы, следуя которым возможно снизить риски опасного воздействия и их последствий:

* вооруженная охрана магазинов торговой сети и офисов компании;
* четкая и строгая иерархия должностей и полномочий в компании. Каждый должен заниматься строго своим заданием;
* обязательная экстренная связь каждого магазина с милицией и пожарной службой (наличие кнопок экстренного вызова) и четкий инструктаж персонала на случай чрезвычайного происшествия;
* строгий подбор сотрудников с привлечением, при необходимости, милиции;
* защита главных серверов компании (если такие существуют) и важной корпоративной почты;
* использование новейших средств защиты (антивирусные продукты, файерволы) персональных компьютеров сотрудников и обязательное использование лишь лицензионных продуктов;
* разграничение доступа к финансовым отделам. Уборщица не должна знать номер банковского счета фирмы и тем более, его пароля;
* проведение регулярных бесед и инструктажей с сотрудниками;
* наличие как в магазинах, так и в офисах, наглядного отображения плана по работе во время чрезвычайных ситуаций.

Так же, эффективной мерой по защите является проведение тестовых экспериментов по атаке на фирму: наем специализированных людей, которые проведут атаку на сетевые ресурсы компании и выявят пробелы в защите. Данная операция безусловно является дорогостоящей, однако впоследствии, это сэкономит средства компании.

Целями защиты информации являются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

При разработке политики безопасности можно использовать следующую модель (рис. 1), основанную на адаптации Общих Критериев (ISO 15408) и проведении анализа риска (ISO 17799).

Рассматриваются следующие объективные факторы:

* угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;
* уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы; - риск – фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери – прямые или косвенные).

Для создания эффективной политики безопасности предполагается первоначально провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для предприятия на основе заданного критерия. Политику безопасности и соответствующую корпоративную систему защиты информации предстоит построить таким образом, чтобы достичь заданного уровня риска.

Предлагаемая методика разработки политики информационной безопасности современного предприятия позволяет полностью проанализировать и документально оформить требования, связанные с обеспечением информационной безопасности, избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков, оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем, обеспечить проведение работ в сжатые сроки, представить обоснование для выбора мер противодействия, оценить эффективность контрмер, сравнить различные варианты контрмер.

В ходе работ должны быть установлены границы исследования. Для этого необходимо выделить ресурсы информационной системы, для которых в дальнейшем будут получены оценки рисков. При этом предстоит разделить рассматриваемые ресурсы и внешние элементы, с которыми осуществляется взаимодействие. Ресурсами могут быть средства вычислительной техники, программное обеспечение, данные, а также информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (архивах, фондах, банках данных, других информационных системах). Примерами внешних элементов являются сети связи, внешние сервисы и т.п.

При построении модели будут учитываться взаимосвязи между ресурсами. Например, выход из строя какого-либо оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения ИБ.

Эта модель, в соответствии с предлагаемой методикой, строится следующим образом: для выделенных ресурсов определяется их ценность, как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т.д. Затем описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации.

Для управления проектом его следует разбить на иерархические подсистемы и компоненты. В терминах управления проектами структура проекта представляет собой “дерево” ориентированных на продукт проекта компонентов, представленных оборудованием, работами, услугами и информацией, полученными в ходе реализации проекта. Можно сказать, что структура проекта - это организация связей и отношений между его элементами. Формирование структуры проекта позволяет представить его в виде значительно меньших блоков работ вплоть до получения самых мелких, поддающихся непосредственному контролю позиций. Именно такие блоки передаются под управление отдельным специалистам, ответственным за достижение конкретной цели, достигаемой при реализации задач данного блока. Структуризация является неотъемлемой частью общего процесса планирования проекта и определения его целей, а также подготовки плана проекта и матрицы распределения ответственностей и обязанностей.

Особенности доступа к информации в системах передачи данных и в ИС являются внешней характеристикой таких систем. Естественно, доступ к ресурсам не может быть неконтролируемым или неуправляемым: рост стратегиче­ского значения сферы ОИ в разных организациях требует эффек­тивного управления ее ресурсами. Решение проблемы всесторонней защищенности информационных ресурсов в ИС обеспечивает системный подход в силу своей многогранности.

На основе построенной модели можно обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер будут рекомендации по проведению регулярных проверок эффективности системы защиты.

Обеспечение повышенных требований к ИБ предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

По завершении работ, можно будет определить меру гарантии безопасности информационной среды, основанную на оценке, с которой можно доверять информационной среде объекта. Данный подход предполагает, что большая гарантия следует из применения больших усилий при проведении оценки безопасности. Адекватность оценки основана на вовлечении в процесс оценки большего числа элементов информационной среды объекта, глубине, достигаемой за счет использования при проектировании системы обеспечения безопасности большего числа проектов и описаний деталей выполнения, строгости, которая заключается в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

Решение задачи по разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа.

Положительный эффект работы WEB-разработчиков составляет - E0 = 26000 $.

Эффект с учетом несанкционированного доступа - E = 20000 $.

Стоимость установление камер слежение и их коэффициент эффективности - C = 2000 $, K = 10.

1) Эффективность функционирования объекта с учетом воздействия несанкционированного доступа:

E=E₀-∆E;

∆E=E₀-E=26000$-20000$=6000$;

2) Относительная эффективность:

δ= =20000$/26000$=0.77;

3) ∆E₃= *, где K>1;*

∆E₃=6000$/10=600$;

4) ;

=∆E₃=600$;

=26000$-600$-2000$=23400$

*E<*

Полученное функционирование () больше функционирования с несанкционированным доступом, что говорит о том, что внедрение средств защиты является выгодным и имеет положительный эффект (23400$>20000$).

**Вывод**

Важно помнить, что прежде чем внедрять какие-либо решения по защите информации необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия. В частности, политика безопасности должна описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности.

Система информационной безопасности (СИБ) окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот.

Этапы построения политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности.

Опыт показывает, что для достижения удачных решений по защите информации кампаний необходимо сочетание правовых, организационных и технических мер. Это сочетание определяется конфиденциальностью защищаемой информации, характером опасности и наличием средств защиты. В общем случае технические меры безопасности составляют незначительную часть от общих мер защиты (правовых и организационных). Однако ни одну из них упускать нельзя. Каждая мера дополняет другую, и недостаток или отсутствие любого способа приведёт к нарушению защищённости.

Особое внимание при оценке эффективности системы защиты техническими средствами необходимо обратить на их надёжность и безотказность. При их эксплуатации имеют место поломки, сбои, отказы, вследствие чего они не обеспечивают выполнение задачи защиты. Отсюда задача обеспечения надлежащей надёжности технических средств обретает значительную важность, так как уровень, качество и безопасность защиты находятся в прямой зависимости от надёжности технических средств.