Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Практическое задание №3

«Разработка политики информационной безопасности бизнес-компании»

Подготовил: студент ФИТ 2 курса 5 группы Древотень Е.В.

Проверил: асс. Берников В.О.

Цель: Разработать проект политики информационной безопасности бизнес-компании.

Введение

Важность разработки политики информационной безопасности обусловлены тем, что сейчас идёт постиндустриальное общество, где наивысшая ценность – у информации. Независимо от вида представления и хранения информации её возможно потерять, повредить, украсть или “подсмотреть” – получить несанкционированный доступ.

Каждый день миллиарды людей создают или потребляют огромные объёмы данных. При этом почти вся информация – конфиденциальна, то есть доступ к ней должен быть только у определённых людей, в то время как у прочих доступа к ней не будет. Эта информация может быть конфиденциальной в рамках одной компании, семьи или одного человека, группы компаний, государства и т.п. Для обеспечения уверенности, что информация не станет доступна третьим лицам, не будет повреждена специально или случайна вводится политика безопасности.

Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Определение политики информационной безопасности (далее – ИБ) должно сводиться к следующим практическим шагам:

1. Определение используемых руководящих документов и стандартов в области ИБ, а также основных положений политики ИБ, включая:

* управление доступом к средствам вычислительной техники, программа и данным;
* антивирусную защиту;
* вопросы резервного копирования;
* проведение ремонтных и восстановительных работ;
* информирование об инцидентах об области ИБ.

2. Определение подходов к управлению рисками: является ли достаточным базовый уровень защищенности или требуется проводить полный вариант анализа рисков.

3. Структуризация контрмер по уровням.

4. Порядок сертификации на соответствие стандартам в области ИБ. Должна быть определена периодичность проведения совещаний по тематике ИБ на уровне руководства, включая периодический пересмотр положений политики ИБ, а также порядок обучения всех категорий пользователей информационной системы по вопросам ИБ.

В случае, когда нарушения информационной безопасности чреваты тяжелыми последствиями, базовый уровень требований к режиму информационной безопасности является недостаточным. Для того, чтобы сформулировать дополнительные требования, необходимо:

* определить ценность ресурсов;
* к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;
* оценить вероятности угроз;
* определить уровень уязвимости ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Существуют различные подходы к оценке рисков. Выбор под хода зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер.

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.

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.

Описание структуры туристического агентства

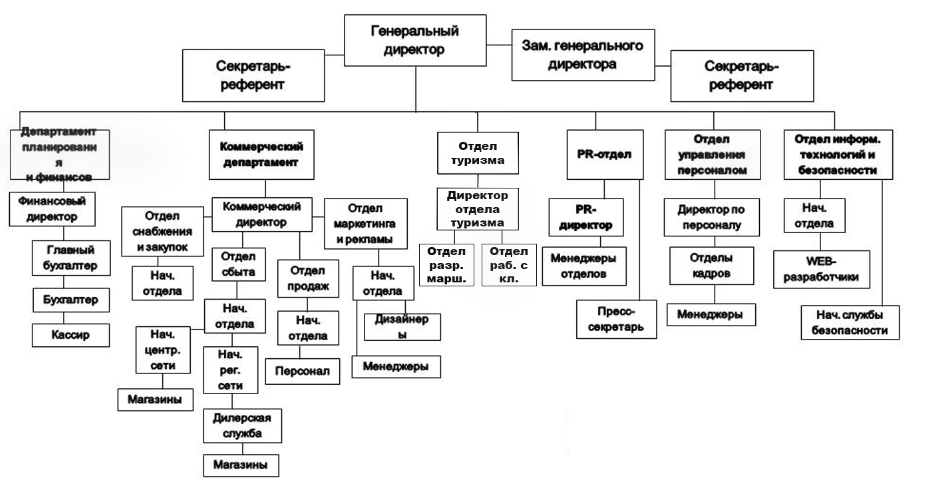


Рис.1 Структура туристического агентства

Организационная структура кампании состоит из следующих основных отделов:

* Коммерческий департамент;
* Отдел туризма;
* 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;
* уничтожение или разрушение средств хранения информации;
* уничтожение или разрушение средств передачи данных;
* частичное или полное повреждение частей средств, предназначенных для хранения или обработки информации;
* временное выведение из строя средств хранения или обработки информации;
* уничтожение или разрушение средств электропитания;
* временная остановка работы системы вследствие отключения электропитания в районе.

Разработка мер защиты

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Существуют различные подходы к оценке рисков. Выбор под хода зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер.

Процесс оценивая рисков содержит несколько этапов.

1. Идентификация ресурса и оценивание его количественных показателей.

2. Оценивание угроз.

3. Оценивание уязвимостей.

4. Оценивание существующих и предполагаемых средств обеспечения.

5. Оценивание рисков.

На основании оценивания рисков выбираются средства, обеспечивающие режим ИБ. Ресурсы, значимые для нормальной работы организации и имеющие определенную степень уязвимости, считаются подверженными риску, если по отношению к ним существует какая либо угроза. При оценивании рисков учитываются потенциальные негативные воздействия от нежелательных происшествий и показатели значимости рассматриваемых уязвимостей и угроз для этих ресурсов.

Риск характеризует опасность, которой может подвергаться система и использующая ее организация. Риск зависит от показателей ценности ресурсов, вероятности реализации угроз для ресурсов и степени легкости, с которой уязвимости могут быть использованы при существующих или планируемых средствах обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков для информационной системы и ее ресурсов. На основе таких данных могут быть выбраны необходимые средства управления ИБ.

При оценивании рисков учитывается:

* ценность ресурсов;
* оценка значимости угроз;
* эффективность существующих и планируемых средств защиты.

На основании политики безопасности строится программа безопасности, которая реализуется на процедурном и программно-техническом уровнях уровне.

К процедурному уровню относятся меры безопасности, реализуемые людьми.

Можно выделить следующие группы процедурных мер:

* управление персоналом;
* физическая защита;
* поддержание работоспособности;
* реагирование на нарушения режима безопасности;
* планирование восстановительных работ.

Управление персоналом заключается в выполнении следующих условий. Во-первых, для каждой должности существовать квалификационные требования по ИБ. Во-вторых, в должностные инструкции должны входить разделы, касающиеся информационной безопасности. В-третьих, каждого работника нужно научить мерам безопасности теоретически и на практике.

Меры физической защиты включают в себя защиту от утечки информации по техническим каналам, инженерные способы защиты и т.д.

Планирование восстановительных работ предполагает:

* слаженность действий персонала во время и после аварии;
* наличие заранее подготовленных резервных производственных площадок;
* официально утвержденную схему переноса на резервные площадки основных информационных ресурсов;
* схему возвращения к нормальному режиму работы.

Поддержание работоспособности включает в себя создание инфраструктуры, включающий в себя как технические, так и процедурные регуляторы и способной обеспечить любой наперед заданный уровень работоспособности на всем протяжении жизненного цикла информационной системы.

Реагирование на нарушение режима безопасности может быть регламентировано в рамках отдельно взятой организации. В настоящее время, осуществляется только мониторинг компьютерных преступлений в национальном масштабе и на мировом уровне.

Основой программно-технического уровня являются следующие механизмы безопасности:

* идентификация и аутентификация пользователей;
* управление доступом;
* протоколирование и аудит;
* криптография;
* экранирование;
* обеспечение высокой доступности и т.д.

Важно управлять информационной системой в целом и механизмами безопасности в особенности. Упомянутые меры безопасности должны опираться на общепринятые стандарты, быть устойчивым к сетевым угрозам, учитывать специфику отдельных сервисов.

Теперь рассмотрим теоретическую модель туристического агентства для разработки модели безопасности. 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.

Рассмотрим решение задачи по анализу эффективности функционирования агентства без дополнительных средств защиты и без них в условиях несанкционированного доступа любого рода.

Допустим, что в данном туристическом агентстве положительный эффект работы Е0=50000 у.е.

Эффект с учётом несанкционированного доступа: Е=35000 у.е.

Стоимость установки охранных систем (сигнализаций): 2200 у.е.; видеонаблюдения: 1000 у.е.; централизированной системы контроля: 1100 у.е.; ПО для защиты локальных цифровых систем: 2750 у.е.; К=25.

ΔЕ=Е0-Е;

ΔЕ=50000-35000=15000;

δ=0,7;

ΔЕз=600;

Ез=50000-600-(2200+1000+1100+2750)=42350;

δз=0,847.

Полученное значение функционирования агентства с добавлением политики безопасности и средств защиты больше, чем при отсутствии средств защиты, что говорит о том, что внедрение средств защиты является выгодным (имеет положительный эффект).

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.

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.

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.