Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Основы Защиты Информации**

**Практическое занятие №3**

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

Студент: Городилов М. П.

ФИТ 2 курс 4 группа

Преподаватель: Буснюк Н. Н.

Минск 2020

**Цели и задачи данной работы**

Задача данной лабораторной работы заключается в изучении информационной системы сохранения данных и недопустимости разглашения их. Также необходимо обеспечить невозможность «утечки» данных, то есть обеспечить сохранения данных, необходимых для входа в различные системы, к примеру, социальны сети, электронные кошельки и др. Необходимо проанализировать все возможные случаи взлома базы данных компании, а также хищения, изменения, уничтожения или модификации информации. Так же следует учитывать нанесение ущерба путем физического воздействия, внедрение шпионских или вирусных программ, воздействие на работающий персонал данного комплекса. На основании полученных результатов разработать план действий при выявлении злоумышленников, их действий, а также реализовать меры противодействия и снижения ущерба, восстановление всей системы издательства при таких ситуациях.

**Введение**

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

* В нашей голове;
* На бумажных носителях;
* На различных цифровых носителях информации к примеру: диски, флэшки и др.

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 IT компании «Авар»**



Рис.1 Структура компании «Авар»

Организационная структура кампании состоит из следующих основных отделов:

* Отдел управления проектами;
* Отдел непосредственной работы над проектами;
* Отдел управления компанией и её сотрудниками.

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.

*Руководитель* — осуществляет общее руководство кампанией.

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

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.

**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. 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.

Необходимый комплекс мероприятий по защите конфиденциальной информации:

* 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. 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.

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.

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 «Авар»;
* 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.

**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 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.

При этом политику безопасности желательно оформить в виде отдельного документа и утвердить руководством предприятия.

Особое внимание при оценке эффективности системы защиты техническими средствами необходимо обратить на их надёжность и безотказность.