Северный Институт Предпринимательства

Кафедра гуманитарных дисциплин

Курсовая работа

По дисциплине «Стратегический менеджмент»

На тему “ Стратегия обеспечения информационной безопасности предприятия ”

Выполнил студент 2 курса

Дневного отделения

Специальности Менеджмент

Шатеневский О.А.

Проверил – Коновалов И.В.

г. Архангельск 2004 г.

Содержание

|  |  |
| --- | --- |
| Введение | 3 |
| 1. Что такое информационная безопасность и её цели | 5 |
| 1. Разработка и внедрение эффективных политик информационной безопасности | 6 |
| 1. Факторы, определяющие эффективность политики безопасности | 7 |
| 1. Оценка риска | 10 |
| 1. Рекомендации по разработке и внедрению эффективных политик | 12 |
| 1. Создание благоприятной среды | 14 |
| 1. Жизненный цикл политики безопасности | 18 |
| 1. Пример неудачной политики | 21 |
| 1. Пример управленческой политики организации | 22 |
| Заключение | 26 |
| Литература | 27 |

Введение

Деятельность любой организации в наше время связана с получением и передачей информации [1]. Информация является сейчас стратегически важным товаром. Потеря информационных ресурсов или завладение секретной информацией конкурентами, как правило, наносит предприятию значительный ущерб и даже может привести к банкротству [1].

За последние 20 лет информационные технологии (ИТ) проникли во все сферы управления и ведения бизнеса [3]. Сам же бизнес из реального мира, давно переходит в мир виртуальный, а поэтому весьма зависим от вирусных, хакерских и прочих атак. По данным Института Компьютерной Безопасности общий ущерб, который нанесли компьютерные вирусы за последние 5 лет, оценивается ***как минимум*** в 54 млрд. долларов, а по данным сайта SecurityLab.ru только за последние десять дней февраля (2004 год) вирусы "съели" астрономическую сумму - около 50 миллиардов долларов. После начала эпидемии MyDoom Министерство национальной безопасности США вообще прировняла вирусные эпидемии к терроризму. Разработчики ПО быстро реагируют на атаки, но постфактум, а не заранее. Пока не существует средств защиты от глобальных эпидемий вирусов.

Первые преступления с использованием компьютерной техники появились в России в 1991 г., когда были похищены 125,5 тыс. долларов США во Внешэкономбанке СССР. В 2003 году в России было возбуждено 1602 уголовных дела по ст.272 («Неправомерный доступ к компьютерной информации») и 165 ("Причинение имущественного ущерба путем обмана и злоупотребления доверием") УК РФ [8].

С 1999 года появилась ещё одна проблема информационной безопасности (ИБ) – Спам. Это анонимная массовая непрошеная рассылка. Сейчас около 30% всех электронных писем являются спамом. Наводнение спама приводит к ежегодным убыткам, оцененным до 20 миллиардов долларов. Спам в пределах одной компании, приводит к убыткам от 600 до 1000 долларов ежегодно, из расчета на одного пользователя.[2] "Спам – это архиважная проблема, грозящая свести на нет большую часть преимуществ электронной почты", – пишет Билл Гейтс в одном из своих регулярных e-mail-обращений к заказчикам.

Также широко распространяется сейчас промышленный шпионаж – устройство стоимостью всего 10$, в случае его удачного размещения, может привести фирму к банкротству. В последнее время участились взломы компьютерных сетей (например несанкционированный доступ (НСД) к информации, обрабатываемой на ПЭВМ) [1].

В наше время злоумышленники могут получить доступ не только к открытой информации, но и к информации, содержащей государственную (в 2003 году ФСБ пресечено более 900 попыток проникновения в информационные ресурсы органов государственной власти России [5]) и коммерческую тайну.

Из всего вышесказанного можно сделать вывод, что в сегодняшней ситуации предприятия должны иметь стратегию ИБ, которая должна основываться на комплексном подходе, осуществлять контроль всех параметров ИБ и иметь подготовку к будущему.

Цель данной работы рассмотреть стратегию ИБ предприятия в виде системы эффективных политик, которые определяли бы эффективный и достаточный набор требований безопасности.

Задачи – определить факторы эффективности ПБ, описать схему разработки и внедрения ПБ, описать жизненный цикл ПБ, раскрыть вопрос создания благоприятной среды, в которой будет внедрятся ПБ.

**1.** **Что такое стратегия информационной безопасности и её цели**

Проанализировав достаточно большое количество литературы, я не нашел четкого определения ИБ, поэтому сформулировал своё – *информационная безопасность это комплекс мер по обеспечению безопасности информационных активов предприятия.* Самое главное в этом определении это то, что ИБ можно обеспечить только в случае комплексного подхода. Разрешение каких-то отдельных вопросов (технических или организационных) не решит проблему ИБ в целом, а вот как раз этого главного принципа большинство сегодняшних руководителей не понимают и вследствие чего являются жертвами злоумышленников.

Стратегия – средство достижения желаемых результатов. Комбинация из запланированных действий и быстрых решений по адаптации фирмы к новым возможностям получения конкурентных преимуществ и новым угрозам ослабления её конкурентных позиций [9]. То есть стратегию информационной безопасности (СИБ) нужно определять с учетом быстрого реагирования на новые угрозы и возможности.

Среди целей ИБ главными можно выделить следующие:

*Конфиденциальность* – обеспечение информацией только тех людей, которые уполномочены для получения такого доступа. Хранение и просмотр ценной информации только теми людьми, кто по своим служебным обязанностям и полномочиям предназначен для этого.

*Целостность* – поддержание целостности ценной и секретной информации означает, что она защищена от неправомочной модификации. Существуют множество типов информации, которые имеют ценность только тогда, когда мы можем гарантировать, что они правильные. Главная цель информационной политики безопасности должна гарантировать, что информация не была повреждена, разрушена или изменена любым способом.

*Пригодность* – обеспечение того, чтобы информация и информационные системы были доступны и готовы к эксплуатации всегда, как только они потребовались. В этом случае, основная цель информационной политики безопасности должна быть гарантия, что информация всегда доступна и поддерживается в пригодном состоянии.

**2.** **Разработка и внедрение эффективных политик информационной безопасности**

Не секрет, что дела с обеспечением ИБ в большинстве российских компаний обстоят не лучшим образом. Общение со специалистами и результаты статистических исследований только укрепляют это мнение. Большинство организаций регулярно терпят убытки, связанные с нарушением ИБ, не способны оценить ущерб или хотя бы обнаружить многие из этих нарушений. Тем более не идет речь о реализации в современных российских организациях полноценной процедуры управления рисками ИБ. Большинство специалистов-практиков даже не берутся за эту "непосильную" задачу, предпочитая руководствоваться при решении проблем ИБ исключительно собственным опытом и интуицией. Убытки от нарушений ИБ могут выражаться в утечке конфиденциальной информации, потере рабочего времени на восстановление данных, ликвидацию последствий вирусных атак и т.п. Убытки могут также выражаться и вполне конкретными "круглыми суммами", например, когда речь идет о мошенничестве в финансовой сфере с использованием компьютерных систем.

Политики безопасности (ПБ) лежат в основе организационных мер защиты информации. От их эффективности в наибольшей степени зависит успешность любых мероприятий по обеспечению ИБ. Часто приходится сталкиваться с неоднозначностью понимания термина "политика безопасности". В современной практике обеспечения ИБ термин "политика безопасности" может употребляться как в широком, так и в узком смысле слова. В широком смысле, ПБ определяется как система документированных управленческих решений по обеспечению ИБ организации. В узком смысле под ПБ обычно понимают локальный нормативный документ, определяющий требования безопасности, систему мер, либо порядок действий, а также ответственность сотрудников организации и механизмы контроля для определенной области обеспечения ИБ. Примерами таких документов могут служить "Политика управления паролями", "Политика управления доступом к ресурсам корпоративной сети", "Политика обеспечения ИБ при взаимодействии с сетью Интернет" и т.п. Использование нескольких специализированных нормативных документов обычно является предпочтительней создания "Общего руководства по обеспечению ИБ организации". Например, в компании Cisco Systems, Inc. стараются, чтобы размер ПБ не превышал 2 страниц. В редких случаях размер ПБ может достигать 4-5 страниц. Содержательная часть типовой русскоязычной ПБ обычно не превышает 7 страниц. Этот подход, однако, не противоречит и созданию объемных Руководств, Положений и Концепций по обеспечению ИБ, содержащих ссылки на множество специализированных ПБ и увязывающих их в единую систему организационных мер по защите информации.

Далее речь пойдет о существующих подходах к разработке эффективных ПБ, без которых невозможно создание комплексной системы обеспечения ИБ организации и разработки стратегии ИБ. Как будет показано, эффективность ПБ определяется качеством самого документа, который должен соответствовать текущему положению дел в организации и учитывать основные принципы обеспечения ИБ, изложенные ниже, а также правильностью и законченностью процесса внедрения [6].

***2.1. Факторы, определяющие эффективность политики безопасности***

Эффективные ПБ определяют необходимый и достаточный набор требований безопасности, позволяющих уменьшить риски ИБ до приемлемой величины. Они оказывают минимальное влияние на производительность труда, учитывают особенности бизнес-процессов организации, поддерживаются руководством, позитивно воспринимаются и исполняются сотрудниками организации.

При разработке ПБ, которая "не рухнет под своим собственным весом", следует учитывать факторы, влияющие на успешность применения мер обеспечения безопасности.

*Безопасность препятствует прогрессу*

Меры безопасности накладывают ограничения на действия пользователей и администраторов ИС и в общем случае приводят к снижению производительности труда. Безопасность является затратной статьей для организации, как и любая другая форма страхования рисков.

Человеческая природа всегда порождает желание получения большего количества информации, упрощения доступа к ней и уменьшения времени реакции системы. Любые меры безопасности в определенной степени препятствуют осуществлению этих естественных желаний.

Представьте себе ситуацию ожидания переключения сигнала светофора. Очевидно, что светофор предназначен для обеспечения безопасности дорожного движения, однако если движение по пересекаемой дороге отсутствует, то это ожидание выглядит утомительной тратой времени. Человеческое терпение имеет предел и если светофор долго не переключается, то у многих возникает желание проехать на красный. В конце концов, светофор может быть неисправен, либо дальнейшее ожидание является неприемлемым.

Аналогично, каждый пользователь ИС обладает ограниченным запасом терпения, в отношении следования правилам политики безопасности, достигнув которого он перестает эти правила выполнять, решив, что это явно не в его интересах (не в интересах дела).

Политики, не учитывающие влияния, которое они оказывают на производительность труда пользователей и на бизнес-процессы, в лучшем случае могут привести к ложному чувству защищенности. В худшем случае такие политики создают дополнительные бреши в системе защиты, когда "кто-то начинает двигаться на красный свет".

Следует учитывать и минимизировать влияние ПБ на производственный процесс, соблюдая принцип разумной достаточности.

*Навыки безопасного поведения приобретаются в процессе обучения*

В отличие, скажем, от инстинкта самосохранения, обеспечение ИБ не является инстинктивным поведением. Это функции более высокого уровня, требующие обучения и периодического поддержания.

Процедуры обеспечения безопасности обычно не являются интуитивными. Без соответствующего обучения пользователи ИС могут и не осознавать ценность информационных ресурсов, риски и размеры возможного ущерба. Пользователь, не имеющий представления о критичности информационных ресурсов (или причинах, по которым их следует защищать), скорее всего, будет считать соответствующую политику неразумной. Даже некоторые навыки самосохранения требуют обучения. (Дети сначала не знают о том, что перед тем, как переходить через дорогу, надо посмотреть сначала налево, а потом – направо). В отличие от инстинктивного, это пример сознательного поведения.

Руководство организации также следует просвещать по вопросам, касающимся ценности информационных ресурсов, ассоциированным с ними рисков и соответствующих политик безопасности. Если руководство не знакомо с политикой безопасности или с ее обоснованием, не приходится рассчитывать на его поддержку. Конечно, руководству не требуется знать технических деталей обеспечения ИБ и конкретных правил, предписываемых политиками. Достаточно сфокусировать его внимание на возможных последствиях нарушений безопасности и связанных с ними потерях для организации.

Следует проводить непрерывную работу по обучению сотрудников и повышению осведомленности руководства организации в вопросах обеспечения ИБ.

*Нарушения политики безопасности являются неизбежными*

В крупных организациях в ИТ-процессы вовлечено большое количество людей, для большинства из которых требования ПБ отнюдь не являются очевидными. Чем сложнее пользователям ИС приспособиться к установленной политике, тем менее вероятной является ее работоспособность. На начальном этапе требования ПБ наверняка будут нарушаться, да и в будущем полностью избежать этого не удастся.

Необходимо осуществлять непрерывный контроль выполнения правил ПБ как на этапе ее внедрения, так и в дальнейшем, фиксировать нарушения и разбираться в их причинах.

Одной из основных форм этого контроля является регулярное проведение как внутреннего, так и внешнего аудита безопасности.

*Чтобы оставаться эффективной, политика безопасности обязана совершенствоваться*

Даже если вам удалось разработать и внедрить эффективную политику безопасности, работа на этом не заканчивается. Обеспечение ИБ – непрерывный процесс. Технологии стремительно изменяются, существующие системы устаревают, а многие процедуры со временем теряют эффективность. Политики безопасности должны непрерывно совершенствоваться для того, чтобы оставаться эффективными.

Работоспособность и эффективность существующих политик должны регулярно проверяться. Устаревшие политики должны пересматриваться [6].

***2.2. Оценка риска***

Перед принятием любых решений относительно стратегии информационной безопасности организации (как на длительный, так и на короткий период времени) мы должны оценить степени уникальных рисков.

Пока организация имеет информацию, представляющую ценность для вас и ваших конкурентов (а может, и просто «случайных» хакеров), она рискует потерей этой информацией. Функция любого информационного механизма контроля безопасности (технического или процедурного) и должна состоять в ограничении этого риска заранее выбранным приемлемым уровнем. Конечно, это истинно и для защитной политики. Политика это механизм контроля за существующими рисками и должна быть предназначена и развита в ответ на имеющиеся и возможные риски. Таким образом, всестороннее осуществление оценки риска должно быть первой стадией процесса создания политики. Оценка риска должна идентифицировать самые слабые области вашей системы и должна использоваться для определения дальнейших целей и средств.

Оценка риска представляет собой комбинацию величин, зависящих от количества информационных ресурсов, имеющих определенную ценность для организации, и уязвимостей, пригодных для использования для получения доступа к этим ресурсам. Собственно, величина уникального риска для конкретной информации – отношение ценности этой информации к количеству способов, которыми данная информация может быть уязвима в структуре вашей корпоративной сети. Очевидно, что чем больше оказывается полученная величина, тем большие средства стоит направить вашей организации на «затыкание» этой дыры.

Конечно, это слишком упрощено и утрированно. Так, при разработке политики неизбежно возникнут вопросы, что некоторые ресурсы, пусть и имеющие для вас ценность, должны быть свободно доступны в Интернете, либо доступ к ним должны иметь и ваши коммерческие партнеры. Но, в целом, хоть и с некоторой условностью, применяется именно описанный подход. Политика, которая учитывает слишком много факторов, многие из которых абсолютно неактуальны, ничем не лучше политики, которая ошибочно не учитывает какого-то важного условия. Разработка политики безопасности является совместным делом руководства компании, которое должно точно определить ценность каждого информационного ресурса и выделяемые на безопасность средств, так и системных администраторов, которые должны правильно оценить существующую уязвимость выбранной информации.

После чего, согласно основным рискам политики, предписывается распределение средств, выделяемых на безопасность. Далее системные администраторы должны определить способы снижения уязвимости информационного ресурса и, основываясь на ценности этого ресурса, согласовать с руководством применяемые методы. Под методами подразумевается не только написание или приобретение и установка необходимых программ и оборудования, но и обучение персонала, разработка должностных инструкций и определение ответственности за их невыполнение [2].

***2.3. Рекомендации по разработке и внедрению эффективных политик***

Учет основных факторов, влияющих на эффективность ПБ, определяет успешность ее разработки и внедрения. Приведенные ниже рекомендации содержат основные принципы создания эффективных политик.

*Минимизация влияния политики безопасности на производственный процесс*

Внедрение ПБ практически всегда связано с созданием некоторых неудобств для сотрудников организации и снижением производительности бизнес процессов. (Однако правильная система мер ИБ повышает эффективность бизнес процессов организации за счет значительного повышения уровня ИБ, являющегося одним из основных показателей эффективности). Влияние мер ИБ на бизнес процессы необходимо минимизировать. В то же время не стоит стремиться сделать меры ИБ абсолютно прозрачными. Для того чтобы понять, какое влияние политика будет оказывать на работу организации, и избежать "узких мест", следует привлекать к разработке этого документа представителей бизнес подразделений, служб технической поддержки и всех, кого это непосредственно коснется.

ПБ – продукт коллективного творчества. Рекомендуется включать в состав рабочей группы следующих сотрудников организации:

* руководителя высшего звена;
* руководителя, ответственного для внедрения и контроля выполнения требований ПБ;
* сотрудника юридического департамента;
* сотрудника службы персонала;
* представителя бизнес пользователей;
* технического писателя;
* эксперта по разработке ПБ.

В состав рабочей группы может входить от 5 до 10 человек. Размер рабочей группы зависит от размера организации и широты проблемной области, охватываемой ПБ.

*Непрерывность обучения*

Обучение пользователей и администраторов информационных систем является важнейшим условием успешного внедрения ПБ. Только сознательное выполнение требований ПБ приводит к положительному результату. Обучение реализуется путем ознакомления всех пользователей с ПБ под роспись, публикации ПБ, рассылки пользователям информационных писем, проведения семинаров и презентаций, а также индивидуальной разъяснительной работы с нарушителями требований ПБ. В случае необходимости на нарушителей безопасности налагаются взыскания, предусмотренные ПБ и правилами внутреннего распорядка.

Пользователи информационных систем должны знать кого, в каких случаях и каким образом надо информировать о нарушениях ИБ. Однако это не должно выглядеть как доносительство. Контактная информация лиц, отвечающих за реагирование на инциденты, должна быть доступна любому пользователю.

*Непрерывный контроль и реагирование на нарушения безопасности*

Контроль выполнения правил ПБ может осуществляться путем проведения плановых проверок в рамках мероприятий по аудиту ИБ.

В организации должны быть предусмотрены меры по реагированию на нарушение правил ПБ. Эти меры должны предусматривать оповещение об инциденте, реагирование, процедуры восстановления, механизмы сбора доказательств, проведения расследования и привлечения нарушителя к ответственности. Система мер по реагированию на инциденты, должна быть скоординирована между ИТ-департаментом, службой безопасности и службой персонала.

Политики должны по возможности носить не рекомендательный, а обязательный характер. Ответственность за нарушение политики должна быть четко определена. За нарушение ПБ должны быть предусмотрены конкретные дисциплинарные, административные взыскания и материальная ответственность.

*Постоянное совершенствование политик безопасности*

ПБ не является набором раз и навсегда определенных прописных истин. Не следует пытаться путем внедрения ПБ решить сразу все проблемы ИБ. Политика является результатом согласованных решений, определяющих основные требования по обеспечению ИБ и отражающих существующий уровень понимания этой проблемы в организации. Для того чтобы оставаться эффективной ПБ должна периодически корректироваться. Должна быть определена ответственность за поддержание ПБ в актуальном состоянии и назначены интервалы ее пересмотра. Политика должна быть простой и понятной. Следует избегать усложнений, которые сделают политику неработоспособной. По этой же причине она не должна быть длинной. Иначе большинство пользователей не смогут дочитать ее до конца, а, если и дочитают, то не запомнят о чем в ней говорится.

*Поддержка руководства организации*

На этапе внедрения ПБ решающее значение имеет поддержка руководства организации. ПБ вводится в действие приказом руководителя организации и процесс ее внедрения должен находится у него на контроле. В ПБ должна быть явным образом прописана озабоченность руководства вопросами обеспечения ИБ. Со стороны координатора рабочей группы по разработке ПБ руководству организации должны быть разъяснены риски, возникающие в случае отсутствия ПБ, а предписываемые ПБ меры обеспечения ИБ должны быть экономически обоснованны [6].

***2.4. Создание благоприятной среды***

Мы пришли к выводу, что эффективность защитной политики пропорциональна поддержке, которую она получает в организации. Таким образом, критически важным условием для успеха в области защиты организации становится организация работы и создание в организации атмосферы, благоприятной для создания и поддержания высокого приоритета информационной безопасности. Чем крупнее организация, тем более важной становится поддержка сотрудников. Далее будет предложено несколько вещей, которые могут быть сделаны для гарантии полной поддержки ПБ руководством организации, что должно существенно увеличить эффективность политики.

*Поддержка управления*

Я уже упоминал об этом ранее, но готов подчеркнуть снова. Самое трудное, с чем мы можем столкнуться в процессе становления защитной политики – это убедить руководство нашей организации в необходимости компьютерной безопасности и вовлечь их в этот процесс, заставить быть причастными к созданию защитной политики (пока гром не грянет, мужик не перекрестится, т.е. в данном случае руководство денег не даст). Здесь невозможно предложить универсального метода, все в данном случае зависит от вашей убедительности и способности к ведению переговоров. Примером может послужить вопрос такого плана: Готов ли Бизнес существенно потратится на защиту информации о самом себе и на защиту сервиса, на котором основано управление компанией [7]? Может быть, помочь в качестве аргументов могут предпринятые вами тестовые проверки уязвимости, или даже демонстрация при руководстве уязвимости компьютерной защиты. В любом случае, без поддержки высокого руководства политика не может преуспеть, поэтому в случае отказа не стоит даже пытаться делать это на свой страх и риск – эта затея обречена на провал.

*Организационная структура*

Независимо от размеров организации, защитная политика должна всегда иметь владельца. В то время как права, обязанности и даже название должности могут меняться от организации к организации, его роль должна быть неизменна. Давайте, для примера, назовем этого человека «руководитель охраны» или «security officer». Это – ответственный руководитель, в обязанности которого входит наблюдать за созданием, распределением, и выполнением политики безопасности. В этом смысле «руководитель охраны» выполняет роль посредника между управлением и пользовательской массой. Очевидно, что этот человек должен подчиняться только высшему руководству компании – генеральному директору, президенту или совету директоров.

Поскольку «руководитель охраны» в конечном счете несет общую ответственность за информационную безопасность всей компании, для того чтобы иметь возможность отстаивать интересы информационной безопасности в ряде случаев он(она) даже может быть членом правления. Как правило, большинство маленьких или средних организаций не могут позволить себе отдельную должность «руководителя охраны», и в этом случае возможно совмещение должностей. Однако, независимо от размеров организации, роль «руководителя охраны» должна быть ясно назначена и его обязанности должны быть четко сформулированы.

*Финансовая поддержка*

Процесс создания системы безопасности всегда требовал и будет требовать инвестиций временных затрат, человеческих ресурсов и финансов. Без достаточного финансового обеспечения любое, даже самое правильное и перспективное усилие в данной области потерпит неудачу. Эта же истина относится и к созданию защитной политики.

В распределении фондов для создания политики мы еще раз видим ценность всесторонней оценки риска. При должном образом осуществленной оценке рисков мы должны получить четкие показатели различных рисков, которым подвергаются информационные ресурсы вашей организации, потенциальные финансовые потери, которые вы можете понести в каждом случае, возможный вред и последствия, и роль, которую политика может играть для смягчения этого риска и минимизации потерь. Эти показатели, вкупе с пониманием ценности ваших информационных ресурсов (которые также можно оценочно получить) должны обеспечить достаточно аргументов для финансовых инвестиций в безопасность.

*Культура безопасности*

Цепь всегда прочна настолько, насколько прочно в ней самое слабое звено, а самое слабое звено в системе безопасности - конечный пользователь. На любое ваше решение по безопасности всегда найдется какой-то деятель из сотрудников, который сумеет найти противодействие. Он может считать себя при этом чуть ли не гением компьютеров, не осознавая зачастую, какой вред он наносит своими действиями безопасности собственной организации. Если ваши пользователи не понимают ценности ваших информационных ресурсов, то мы можем, конечно, вести с ними войну, но она изначально обречена на провал. Вы должны создать культуру безопасности в вашей организации, чему прекрасно способствует имеющаяся политика безопасности. Далее приведены краткие стратегии, которые можно (и нужно) использовать:

*Обучение пользователей* – администраторы могут начать «внутреннюю рекламную кампанию», объясняющую ценность общей безопасности, риски, с которыми они сталкиваются, роль политики и обязанности индивидуальных пользователей.

*Акцентирование внимания на менеджерах* – эти руководители низшего звена обычно и устанавливают «правила игры» для своих подчиненных и наиболее неистово требуют выполнения предписанных вещей, в справедливость которых они лично верят. Если убедить их в потребности в безопасности, то считайте, что половина борьбы выиграна.

*Поддерживать сотрудников* – служащие, в большинстве своем, лояльны компании, в которой они работают. Имеет смысл быть честными со штатом сотрудников в вопросах безопасности и ее воздействии на благополучие организации. Это обычно помогает снизить время, необходимое персоналу для перестройки к новым реалиям работы. Один из способов состоит в том, чтобы ежедневно (еженедельно/ежемесячно) рассылать результаты оценок безопасности и ревизий. Надо быть абсолютно откровенными с персоналом обо всех случаях вирусных атак, взломов и других инцидентах безопасности.

*Положительные эмоции* - поскольку хорошо разработанная политика может (и должна) учитывать затраты на обучение и поддержку персонала, то некоторые сотрудники теперь должны быть вознаграждены за бдительность или просто хорошее выполнение требований безопасности. Этих сотрудников можно отобрать по результатам проверок/ревизий, регулярно проводимых сисадминами. В ряде организаций уже через самое короткое время подавляющее большинство сотрудников будет стремиться получить эти, пусть и небольшие, но очень приятные премии. Неизбежно, безопасность организации при этом резко увеличивается, а такая система наград будет являться прекрасным дополнением к системе штрафов за действия, ведущие к нарушениям информационной безопасности.

*Отрицательные эмоции* – если стимул получения дополнительных премий не оказывает влияния на некоторых сотрудников, то можно рассмотреть метод достижения цели другим путем. В организации должна быть разработана система взысканий с нерадивых и небрежных сотрудников. Все это, как мы уже говорили, должно быть прописано в политике. Фактически, метод кнута и пряника со времен римской Империи и поныне являлся и является весьма действенным.

Принятие политики и получение подписи от каждого сотрудника – каждый сотрудник обязан ознакомиться с политикой безопасности и подписаться под ней. Фактически, в нашем российском менталитете только это вынуждает сотрудников внимательно прочитать и вникнуть в документ. А в случае нарушения только это дает законное юридическое право на взыскание с сотрудника [2].

***2.5. Жизненный цикл политики безопасности***

Разработка ПБ – длительный и трудоемкий процесс, требующего высокого профессионализма, отличного знания нормативной базы в области ИБ и, помимо всего прочего, писательского таланта. Этот процесс обычно занимает многие месяцы и не всегда завершается успешно. Координатором этого процесса является специалист, на которого руководство организации возлагает ответственность за обеспечение ИБ. Эта ответственность обычно концентрируется на руководителе Отдела информационной безопасности, Главном офицере по информационной безопасности (CISO), Главном офицере безопасности (CSO), ИТ-директоре (CIO), либо на руководителе Отдела внутреннего аудита. Этот специалист координирует деятельность рабочей группы по разработке и внедрению ПБ на протяжении всего жизненного цикла, который состоит из пяти последовательных этапов, описанных ниже.

*1. Первоначальный аудит безопасности*

Аудит безопасности – это процесс, с которого начинаются любые планомерные действия по обеспечению ИБ в организации. Он включает в себя проведение обследования, идентификацию угроз безопасности, ресурсов, нуждающихся в защите и оценку рисков. В ходе аудита производится анализ текущего состояния ИБ, выявляются существующие уязвимости, наиболее критичные области функционирования и наиболее чувствительные к угрозам ИБ бизнес процессы.

*2. Разработка*

Аудит безопасности позволяет собрать и обобщить сведения, необходимые для разработки ПБ. На основании результатов аудита определяются основные условия, требования и базовая система мер по обеспечению ИБ в организации, позволяющих уменьшить риски до приемлемой величины, которые оформляются в виде согласованных в рамках рабочей группы решений и утверждаются руководством организации.

Разработка ПБ с нуля не всегда является хорошей идеей. Во многих случаях можно воспользоваться существующими наработками, ограничившись адаптацией типового комплекта ПБ к специфическим условиям своей организации. Этот путь позволяет сэкономить многие месяцы работы и повысить качество разрабатываемых документов. Кроме того, он является единственно приемлемым в случае отсутствия в организации собственных ресурсов для квалифицированной разработки ПБ.

*3. Внедрение*

С наибольшими трудностями приходится сталкиваться на этапе внедрения ПБ, которое, как правило, связано с необходимостью решения технических, организационных и дисциплинарных проблем. Часть пользователей могут сознательно, либо бессознательно сопротивляться введению новых правил поведения, которым теперь необходимо следовать, а также программно-технических механизмов защиты информации, в той или иной степени неизбежно ограничивающих их свободный доступ к информации. Администраторов ИС может раздражать необходимость выполнения требований ПБ, усложняющих задачи администрирования. Помимо этого могут возникать и чисто технические проблемы, связанные, например, с отсутствием в используемом ПО функциональности, необходимой для реализации отдельных положений ПБ.

На этапе внедрения необходимо не просто довести содержание ПБ до сведения всех сотрудников организации, но также провести обучение и дать необходимые разъяснения сомневающимся, которые пытаются обойти новые правила и продолжать работать по старому.

Чтобы внедрение завершилось успешно, должна быть создана проектная группа по внедрению ПБ, действующая по согласованному плану в соответствии с установленными сроками выполнения работ.

*4. Аудит и контроль*

Соблюдение положений ПБ должно являться обязательным для всех сотрудников организации и должно непрерывно контролироваться.

Проведение планового аудита безопасности является одним из основных методов контроля работоспособности ПБ, позволяющего оценить эффективность внедрения. Результаты аудита могут служить основанием для пересмотра некоторых положений ПБ и внесение в них необходимых корректировок.

*5. Пересмотр и корректировка*

Первая версия ПБ обычно не в полной мере отвечает потребностям организации, однако понимание этого приходит с опытом. Скорее всего, после наблюдения за процессом внедрения ПБ и оценки эффективности ее применения потребуется осуществить ряд доработок. В дополнение к этому, используемые технологии и организация бизнес процессов непрерывно изменяются, что приводит к необходимости корректировать существующие подходы к обеспечению ИБ. В большинстве случаев ежегодный пересмотр ПБ является нормой, которая устанавливается самой политикой [6].

***2.6. Пример неудачной политик******и***

Для того чтобы продемонстрировать, каким образом неэффективные политики безопасности, либо их отсутствие, делают систему обеспечения ИБ неработоспособной, начнем с рассмотрения простых примеров неудачных (неэффективных) ПБ. На этих примерах мы увидим, что неудачные ПБ (не соответствующие критериям эффективности), приводят к снижению производительности труда пользователей информационной системы (ИС) и, создавая иллюзию "ложной защищенности", только ухудшают общее положение дел с обеспечением ИБ в организации.

*Кража оборудования*

Производитель электроники приобрел очень дорогостоящее тестовое оборудование для использования в производстве. Отдел безопасности решил, что для обеспечения сохранности этого оборудования необходимо ограничить доступ к нему всего несколькими сотрудниками. На входе в помещение с оборудованием были установлены дорогостоящие электронные замки со смарт-картами. Только старшему менеджеру были выданы ключи от этого помещения. Для выполнения своих обязанностей, помимо старшего менеджера, доступ в помещение с оборудованием был необходим еще 10 сотрудникам, которые не имели собственных ключей и сопровождались в это помещение старшим менеджером.

Первоначально требования данной политики добросовестно выполнялись. Однако вскоре менеджеру надоело выполнять функции по сопровождению сотрудников. Производительность труда снизилась из-за того, что менеджер периодически оказывался недоступен, а кроме него некому было открывать помещение. Отдел безопасности отказался удовлетворить просьбу менеджера о выдаче дополнительных ключей. В итоге была достигнута неформальная договоренность о том, что ключи будут оставляться в ящике стола. Последствия не заставили себя долго ждать ...

Однажды, когда менеджер и его сотрудники были на собрании, оборудование было похищено. Ключа тоже найти не удалось. Отдел безопасности предпринял расследование, которое, однако, успехом не увенчалось. После чего решался вопрос о наказании менеджера, ответственного за хранение ключа.

Просуммируем результаты внедрения данной политики:

* Было потеряно дорогостоящее оборудование
* У менеджеров и сотрудников организации сложилось крайне негативное отношение к любым мерам и политикам обеспечения безопасности
* Ворам удалось избежать ответственности
* Дорогостоящие меры защиты не принесли положительного результата
* Данная ПБ потерпела неудачу, потому что она была неудобной для сотрудников организации, и требования этой политики было легко обойти

Разработчики данной политики не учли ее влияние на производительность труда. Этой ошибки можно было бы избежать, если бы они вовлекли в процесс ее разработки сотрудников организации.

Отдел безопасности также не заметил (или не пожелал заметить) тот факт, что требования данной ПБ не соответствовали бизнес-процессам организации. Наличие внутреннего контроля над внедрением данной ПБ позволил бы выявить это противоречие и разработать более эффективную политику [6].

**3. Пример управленческой политики организации**

В предыдущем разделе я показал как нужно разрабатывать, внедрять и сопровождать политики безопасности. Далее я приведу пример управленческой политики в виде ролей и обязанностей персонала, который непосредственно связан с ИБ.

***Роли и обязанности (общие положения)***

Детально их обязанности будут описаны ниже.

* Руководители подразделений отвечают за доведение поло­жений политики безопасности до пользователей и за контак­ты с пользователями.
* Администраторы локальной сети обеспечивают непрерывное функционирование сети и отвечают за реализацию техничес­ких мер, необходимых для проведения в жизнь политики безопасности.
* Администраторы сервисов отвечают за конкретные сервисы и, в частности, за то, что их защита построена в соответствии с общей политикой безопасности.
* Пользователи обязаны использовать локальную сеть в соот­ветствии с политикой безопасности; подчиняться распоря­жениям лиц, отвечающих за отдельные аспекты безопаснос­ти, ставить в известность руководство обо всех подозритель­ных ситуациях.

***Роли и обязанности (детальное изложение)***

Руководители подразделений обязаны:

* Постоянно держать в поле зрения вопросы безопасности. Следить за тем, чтобы то же делали их подчиненные.
* Проводить анализ рисков, выявляя активы, требующие за­щиты, и уязвимые места систем, оценивая размер возможно­го ущерба от нарушения режима безопасности и выбирая эффективные средства защиты.
* Организовать обучение персонала мерам безопасности. Об­ратить особое внимание на вопросы, связанные с антивирус­ным контролем.
* Информировать администраторов локальной сети и админи­страторов сервисов об изменении статуса каждого из подчи­ненных (переход на другую работу; увольнение и т. п.).
* Обеспечить, чтобы каждый компьютер в их подразделениях имел хозяина или системного администратора, отвечающего за его безопасность и имеющего достаточную квалификацию для выполнения этой роли.

Администраторы локальной сети обязаны:

* Информировать руководство об эффективности существую­щей политики безопасности и о технических мерах, которые могут улучшить защиту.
* Обеспечить защиту оборудования локальной сети, в том чис­ле интерфейсов с другими сетями.
* Оперативно и эффективно реагировать на события, таящие угрозу. Информировать администраторов сервисов о попыт­ках нарушения защиты. Оказывать помощь в отражении уг­розы, выявлении нарушителей и предоставлении информа­ции для их наказания.
* Использовать проверенные средства аудита и обнаружения подозрительных ситуаций.
* Ежедневно анализировать регистрационную информацию, отно­сящуюся к сети в целом и к файловым серверам в особенности.

Пользователи обязаны:

* Знать и соблюдать законы, правила, принятые в норматив­ных документах, политику безопасности, процедуры безо­пасности.
* Использовать доступные защитные механизмы для обеспе­чения конфиденциальности и целостности своей информа­ции.
* Использовать механизм защиты файлов и должным образом задавать права доступа.
* Выбирать хорошие пароли; регулярно менять их. Не записы­вать пароли на бумаге, не сообщать их другим лицам (стратегически важным решением будет разработка отдельной политики управления паролями, руководствуясь которой пользователи бы выбирали свои пароли).
* Помогать другим пользователям соблюдать меры безопасно­сти. Указывать им на замеченные упущения с их стороны.
* Информировать администраторов или руководство о нару­шениях безопасности и иных подозрительных ситуациях.
* Не использовать слабости в защите сервисов и локальной сети в целом.
* Не совершать неавторизованной работы с данными, не создавать помех другим пользователям.
* Всегда сообщать корректную идентификационную и аутентификационную информацию, не пытаться работать от имени других пользователей.
* Обеспечивать резервное копирование информации с жестко­го диска своего компьютера.
* Знать принципы работы зловредного программного обеспе­чения, пути его проникновения и распространения, слабос­ти, которые при этом могут использоваться.
* Знать и соблюдать процедуры для предупреждения проник­новения зловредного кода, для его обнаружения и уничто­жения.
* Знать слабости, которые используются для неавторизован­ного доступа.
* Знать способы выявления ненормального поведения конк­ретных систем, последовательность дальнейших действий, точки контакта с ответственными лицами.
* Знать и соблюдать правила поведения в экстренных ситуа­циях, последовательность действий при ликвидации послед­ствий аварий [1].

Заключение

Эффективные ПБ определяют необходимый и достаточный набор требований безопасности, позволяющих уменьшить риски ИБ до приемлемой величины. Они оказывают минимальное влияние на производительность труда, учитывают особенности бизнес-процессов организации, поддерживаются руководством, позитивно воспринимаются и исполняются сотрудниками организации. Для того чтобы ПБ оставалась эффективной, необходимо осуществлять непрерывный контроль ее исполнения, повышать осведомленность сотрудников организации в вопросах ИБ и обучать их выполнению правил, предписываемых ПБ. Регулярный пересмотр и корректировка правил ПБ необходимы для поддержания ее в актуальном состоянии.

Разработка и внедрение ПБ в организации – процесс коллективного творчества, в котором должны участвовать представители всех подразделений, затрагиваемых производимыми изменениями. Координатором этого процесса является специалист, на которого руководство организации возлагает ответственность за обеспечение ИБ. Этот специалист координирует деятельность рабочей группы по разработке и внедрению ПБ на протяжении всего жизненного цикла, включающего в себя проведение аудита безопасности, разработку, согласование, внедрение, обучение, контроль исполнения, пересмотр и корректировку ПБ.

Для разработки эффективной ПБ, помимо профессионального опыта, знания нормативной базы в области ИБ и писательского таланта, необходимо также учитывать основные факторы, влияющие на эффективность ПБ, и следовать основным принципам разработки ПБ, к числу которых относятся: минимизация влияния на производительность труда, непрерывность обучения, контроль и реагирование на нарушения безопасности, поддержка руководства организации и постоянное совершенствование ПБ [6].

Литература

1. Кирсанов К.А., Малявина А.В., Попов Н.В. «Информационная безопасность: Учебное пособие». – М.:МАЭП, ИИК «Калита», 2000.
2. http://www.securitylab.ru/
3. http://www.rcb.ru/
4. http://www.cnews.ru/
5. http://www.bezpeka.com/ - Украинский Информационный Центр Безопасности
6. http://www.globaltrust.ru/
7. http://www.citforum.ru/
8. http://www.crime-research.ru/ - Центр исследования проблем компьютерной преступности
9. Зайцев Л.Г., Соколова М.И. Стратегический менеджмент: Учебник. – М.: Юристъ, 2002.