Содержание:

ВВЕДЕНИЕ

В деятельности любого предприятия на сегодняшний день есть место получению и передаче информации [1]. Информация сегодня представляет собой стратегически важный товар. Утрата информационных ресурсов или, к примеру, приобретение доступа к засекреченной информации конкурентов в большинстве случаев причиняет предприятию солидный ущерб и даже способна повлечь за собой банкротство [1].

На протяжении последних двадцати лет информационные технологии распространились на все сферы в том, что имеет отношение к управлению и ведению бизнеса [3]. В то же время бизнесу давно свойственно из мира реального мира переходить в виртуальный мир, вот почему бизнес оказался очень уязвим для ряда цифровых угроз, в числе которых вирусные, хакерские и прочие атаки.

Согласно данным исследований, проведенных Институтом Компьютерной Безопасности совокупный ущерб, который был нанесен предпринимателям компьютерными вирусами на протяжении последних 5 лет, оценивается, **по меньшей мере,** в 74 млрд. долларов.

В 1999 году появилась ещё одна проблема, связанная с информационной безопасностью, и эта проблема – спам. Спам представляет собой анонимную, массовую, нежелательную рассылку. На сегодняшний день более 35% общего объема электронной почты представляет собой не что иное, как спам.

Распространение спама влечет за собой ежегодные убытки, по оценкам специалистов составляющие порядка 30 миллиардов долларов. Если говорить о воздействии спама в масштабах одной компании, он влечет за собой убытки от 600 до 1000 долларов каждый год в расчете на одного пользователя.

Широкое распространение получил промышленный шпионаж – размещение устройства стоимостью порядка 10$, в случае удачи, способно привести фирму к разорению. Все чаще случаются взломы компьютерных сетей (к примеру, получение несанкционированного доступа к информации, которая обрабатывается

на ПЭВМ) [1].

Из всего, что было сказано выше, можно сделать однозначный вывод, о том, что в условиях нашего времени предприятиям необходимо обладать стратегией информационной безопасности, которой предписано, основываясь на комплексном подходе, заниматься контролем всех без исключения параметров информационной безопасности и работать с прицелом на будущее. Ведущая роль отводится управлению информационной безоспасностью предприятия, что объясняет высокую актуальность выбранной для написания курсовой работы темы.

В качестве цели представленной работы выступает рассмотрение управления стратегией информационной безопасности на условном предприятии в виде совокупности эффективных политик, которыми определялся бы в достаточной степени эффективный набор мероприятий, отвечающих требованиям безопасности.

В рамках намеченной цели можно выделить следующие задачи:

1. определение факторов эффективности политки безопасности;
2. описание схемы, по которой осуществляется разработка и внедрение политики безопасности;
3. описание жизненного цикла политики безопасности;
4. раскрытие вопроса о формировании благоприятной среды, в которой внедрение политики безопасности будет наиболее успешным.

ГЛАВА 1 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Понятие стратегии информационной безопасности и ее целей

Среди известной литературы отсутствует четкое определение информационной безопасности, но наиболее близким по смыслу является следующее: информационная безопасность представляет собой комплекс мероприятий, направленных на обеспечение безопасности информационных ресурсов предприятия.

Суть этого определения состоит в том, что информационная безопасность может быть обеспечена только при условии комплексного подхода. Разрешение ряда отдельных вопросов (будь то технические или организационные) не решает проблемы информационной безопасности в целом, и это и есть тот фундаментальный принцип, ускользающий от подавляющего большинства сегодняшних руководителей, которые страдают от собственного непонимания, следствием чего являются то, что они становятся жертвами злоумышленников.

Стратегия является средством по достижению желаемого результата, и представляет собой комбинацию ряда действий согласно плану и оперативных решений, направленных на адаптацию фирмы к новым возможностям для получения конкурентных преимуществ и новым угрозам ослабления её конкурентных позиций [9]. Таким образом, стратегия информационной безопасности должна быть определена с учетом быстрого реагирования на новые угрозы и возможности.

Среди целей информационной безопасности в числе главных могут быть выделены следующие:

Конфиденциальность означает, что обеспечивать информацией следует лишь тех людей, которым эта информация необходима для выполнения должностных обязанностей. Подразумевает, что осуществление хранения и просмотра ценной информации выполняют только те люди, кому по служебным обязанностям и полномочиям положено этим заниматься.

Поддержание ценной и секретной информации в целостности предполагает, что она находится под защитой от несанкционированной модификации. Можно привести много примеров таких типов информации, которым свойственно полная утрата ценности в случае, когда отсутствуют гарантии того, что информация достоверна. Главной целью информационной политики безопасности является обеспечение гарантий того, что информация защищена от повреждения, разрушения или изменения любым из возможных способов.

Пригодность состоит в обеспечении того, чтобы доступ к информации и информационным системам был обеспечен при сохранении постоянной готовности к эксплуатации всегда, как только в этом возникнет надобность. В таком случае, основной целью информационной политики безопасности должна быть обеспечение гарантии того, что информация всегда находится в доступе для тех людей, кому по должностным обязанностям она необходима, и постоянно

поддерживается в состоянии, пригодном для использования.

1.2 Понятие политики информационной безопасности

Не является секретом, что в том, что касается обеспечения информационной безопасности в большинстве российских компаний положение сложилось не самое лучшее. В результате общения со специалистами и проведения статистических исследований это мнение только укрепилось. Большинству организаций приходится регулярно терпеть убытки, которые связаны с нарушением информационной безопасности, при этом они лишены способности не то, что оценить ущерб, но даже выявить большую часть из числа подобных нарушений.

И уж вовсе речи не идет о реализации в какой-либо современной российской организации полноценной процедуры, управляющей рисками информационной безопасности. Большинству специалистов-практиков даже не приходит в голову идея взяться за решение этой «непосильной» задачи – они предпочитают в процессе решения проблем информационной безопасности опираться исключительно на собственный опыт и интуицию.

Убытки, связанные с нарушениями в области информационной безопасности могут проявляться как утечка конфиденциальной информации, потеря рабочего времени, связанная с необходимостью восстановления данных, ликвидацией последствий, вызванных вирусными атаками и т.п. Убытки также могут проявиться и в виде определенных «круглых цифр», к примеру, в том случае, когда дело связано с мошенничеством в финансовой сфере при использовании компьютерных систем.

Политика безопасности составляет основу организационных мероприятий, направленных на защиту информации. От того, насколько они эффективны, в большой зависимости находится, насколько успешны будут вообще любые мероприятия, направленные на обеспечение информационной безопасности. Нередко возникают ситуации, когда термин «политика безопасности» понимается неоднозначно.

Современная практика обеспечения информационной безопасности предполагает использование термина «политика безопасности» как в широком, обобщенном, так и в более узком смысле слова. В широком смысле, политика безопасности может быть определена в качестве системы документированных управленческих

решений, направленных на обеспечение информационной безопасности организации.

В узком смысле под политикой безопасности, в большинстве случаев, принято понимать такой тип локального нормативного документа, которым определяются требования безопасности, система мер, либо последовательность действий, а также мера ответственности сотрудников организации и механизмы, направленные на контроль определенной области обеспечения информационной безопасности.

В качестве примеров документов такого рода можно привести «Политику управления паролями», «Политику управления доступом к корпоративным сетевым ресурсам», «Политику обеспечения информационной безопасности в случае взаимодействия с глобальной сетью Интернет» и т.п. Применение ряда узкоспециализированных нормативных документов, как правило, оказывается выгодней разработки «Общего руководства по обеспечению информационной безопасности организации».

К примеру, компания Cisco Systems, Inc. стремится, чтобы размер политики безопасности сохранялся в пределах 2 страниц. В исключительных случаях размер политики безопасности может достигать объема порядка 4-5 страниц. Объем содержательной части типовой русскоязычной политики безопасности в большинстве случаев сохраняется в пределах семи страниц. Такой подход, впрочем, не исключает создания маштабных Руководств, Положений и Концепций обеспечения информационной безопасности, которые могут содержать ссылки на специализированные политики безопасности и увязывать их в единую систему организационных мероприятий, направленных на защиту информации.

В дальнейшей части работы речь пойдет подходах к разработке эффективных политик безопасности, существующих на сегодняшний день. В отсутствие политик безопасности пропадает малейшая возможность создания комплексной системы по обеспечению информационной безопасности организации и становится невозможной разработка полноценной стратегии информационной безопасности.

Эффективность политики безопасности в полной мере определяема качеством, которым обладает документ. Этому документу полагается находиться в соответствии как с текущим положением дел в организации, так и принимать в расчет основные принципы по обеспечению информационной безопасности, которые будут изложены ниже, а также руководствоваться обеспечением

правильности и законченности процесса внедрения [6].

1.3 Факторы, оказывающие влияние на эффективность информационной безопасности

Эффективными политиками безопасности определяется определенный набор требований безопасности, являющийся необходимым и достаточным, позволяющий существенно снизить риски информационной безопасности вплоть до приемлемого уровня. Их влияние на производительность труда минимально, ими учитываются особенности существующих в организации бизнес-процессов, они поддерживаются руководством, их позитивно воспринимают и исполняют сотрудники организации.

В процессе разработки политики безопасности, которая «способна выдержать хотя бы собственный вес», следует принимать в расчет ряд факторов, оказывающих существенное влияние на успешность применения мероприятий по обеспечению безопасности.

Мероприятиями по обеспечению безопасности накладываются ограничения на действия, совершаемые пользователями и администраторами информационной системы в процессе трудовой деятельности, и в большинстве случаев это влечет за собой снижение производительности труда. Безопасность оказывается высокозатратной статьей для каждой организации, как, впрочем, это свойственно любой другой форме страхования рисков.

Человеческой природе всегда присуще желание получить большое количество информации – вне зависимости от реальной потребности в ней, упрощенный доступ к ней и уменьшение времени отклика системы. Любым мероприятиям по обеспечению безопасности в некоторой степени свойственно препятствовать осуществлению этих, вполне, в общем-то, естественных желаний.

Можно проиллюстрировать это на примере. Рассмотрим ситуацию, когда человек ожидает, пока переключится сигнал светофора. Не вызывает сомнений, что назначением светофора является обеспечение требуемого уровня безопасности движения на дороге, тем не менее, в случае, когда движения на пересекаемой дороге нет, то получается, что ожидание оказывается тратой времени – по крайней мере, таким выглядит.

Человеческому терпению присущ предел, и когда светофор в течение долгого времени не переключается, то многие испытывают желание проехать на красный сигнал. В самом деле, светофор ведь может оказаться неисправным, либо может сложиться ситуация, когда дальнейшее ожидание окажется неприемлемо по объективным причинам.

По аналогии с рассмотренным примером, каждому пользователю информационной системы присущ ограниченный запасом терпения, по отношению к соблюдению правил политики безопасности, по достижении которого он начнет их игнорировать, решив, что эти правила идут вразрез с его интересами (интересами дела).

Политики, которыми не учитывается влияние, оказываемое на производительность труда сотрудников предприятия и на бизнес-процессы, существующие в этой организации, даже при благоприятном раскладе могут повлечь за собой ложное чувство защищенности. В худшем раскладе политики такого рода порождают только дополнительные уязвимости в системе защиты, в ситуации, когда «кому-то приходит в голову идея начать движение на запрещающий сигнал светофора».

Следует принимать в расчет и сводить к минимуму влияние, оказываемое политикой безопасности на процесс производства, при условии соблюдения принципа разумной достаточности.

Существенным отличием, к примеру, от инстинкта самосохранения, обеспечения информационной безопасности является то, что это действие не инстинктивно. Это действие является функцией более высшего уровня, и требует определенного обучения и мероприятий, направленных на периодическое поддержание.

Процедуры по обеспечению безопасности, как правило, нельзя назвать интуитивными. В отсутствие должного обучения пользователи информационной безопасности могут даже не отдавать себе отчета в том, какой ценностью обладают информационные ресурсы, риски и какие масштабы может принимать возможный ущерб.

Пользователь, лишенный представления о критической значимости, которую информационные ресурсы имеют для организации (или о том, почему им следует обеспечить должную защиту), вероятнее всего, будет полагать, что соответствующая политика неразумна. Даже некоторым навыкам самосохранения для должного уровня эффективности необходимо обучение. Например, детям вначале неведомо, что, прежде, чем перейти через дорогу, следует бросить взгляд

налево, затем – направо, и переходить, только убедившись, что путь свободен. Это является существенным отличием от инстинктивного поведения и служит примером поведения сознательного.

Руководство организации не менее, и даже более, чем рядовых сотрудников, следует просвещать в том, что касается ценности, которой обладают информационные ресурсы предприятия, ассоциированных с ними рисков и соответствующих политик безопасности. Если руководство не было ознакомлено с политикой безопасности или с ее обоснованием, нет оснований рассчитывать, что оно окажет поддержку.

Несомненно, руководитель не обязан обладать знанием технических подробностей обеспечения информационной безопасности и конкретных правил, которые предписываются политиками. Вполне достаточно акцентировать его внимание на том, какие возможные последствия могут иметь нарушения безопасности и на том, какие потери для организации с этим связаны.

Обязательна к выполнению непрерывная работа, направленная на обучение сотрудников и повышение осведомленности руководства организации в вопросах, связанных с обеспечением информационной безопасности.

Крупные организации характерны вовлеченностью в ИТ-процессы большого количества людей; для большинства из них требования политики безопасности отнюдь не очевидны. Чем больше трудностей вызывает у пользователей информационной системы приспособление к установленной политике, тем меньше вероятность ее эффективной работы. На первоначальном этапе требования политики безопасности наверняка будут нарушаться, да и в дальнейшем избежать этого в полной мере не удастся.

Следует выполнять непрерывный контроль за выполнением правил политики безопасности как на том этапе, когда она внедряется, так и в последующем, фиксировать нарушения и разбираться в их причинах.

Одна из основополагающих форм этого контроля заключается в регулярном проведении как внутреннего, так и внешнего аудита безопасности.

Даже в том случае, если вам удастся осуществить разработку и внедрение эффективной политики безопасности, это вовсе не означает, что работа выполнена. Процесс обеспечения информационной безопасности – непрерывный процесс. Технология стремительно изменяется, существующие системы

утрачивают свою эффективность, в то время как многие процедуры с течением времени становятся не актуальны. Политику безопасности следует непрерывно совершенствовать с тем, чтобы сохранять ее эффективность на неизменно высоком уровне.

Как степень работоспособности, так и уровень эффективности существующих политик необходимо регулярно проверять. Если политика устарела, ее следует пересмотреть[6].

ГЛАВА 2 РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1 Порядок оценки риска

Прежде, чем принимать какое-либо решение в том, что касается стратегии информационной безопасности предприятия (как в долговременной, так и в кратковременной перспективе), в обязательно порядке следует оценить уровень уникальных рисков.

До тех пор, пока организация располагает информацией, могущей представлять ценность не только для вас, но и (очевидно!) ваших конкурентов (возможно, даже просто «случайных» хакеров), сохраняется риск утраты этой информации.

Функцией любой информационной схемы по контролю безопасности (технического порядка или же процедурного) как раз и заключается в том, чтобы ограничивать этот риск, исходя из заранее выбранного приемлемого уровня.

Несомненно, это положение сохраняет свою истинность и для защитной политики. Политика является механизмом, осуществляющим контроль за рисками, существующими на данный момент, или могущими возникнуть в будущем, и ей должно быть предназначенной и развитой в ответ на существующие и потенциальные риски. Резюмируя сказанное, можно с уверенностью утверждать, что своевременно проведенная всесторонняя оценка риска должна составлять первую стадию процесса по созданию политики. Оценке риска полагается осуществлять идентификацию самых слабых областей вашей системы, и ее следует использовать для того, чтобы определить дальнейшие цели и средства.

Оценку риска можно представить в виде комбинации величин, которые зависят от количества информационных ресурсов, которые обладают определенной ценностью для организации, и уязвимостей, которые пригодны для того, чтобы использовать их в целях получения доступа к этим ресурсам.

По большому счету, уровень риска, имеющего уникальную природу, для конкретной информации является отношением ценности этой информации к числу способов, которыми данную информацию может «добыть» в рамках структуры вашей корпоративной сети. Несомненно, что чем большим значением обладает полученная расчетом величина, тем больший объем средств имеет смысл вашей организации адресовать на то, чтобы «заткнуть» эту дыру.

Конечно, это может показаться излишне упрощенным и утрированным. К примеру, в процессе разработки политики неизбежно возникнут вопросы такого плана, что некоторым ресурсам, пусть и имеющим для вас ценность, просто необходимо быть свободно доступными в сети Интернете, либо доступом к ним следует обладать вашим коммерческим партнерам. Тем не менее, в целом, пусть и с некоторыми оговорками, в подавляющем большинстве случаев нашел применение именно описанный подход.

Политика, которой учитывается слишком большое число факторов, многие из которых порой асболютно лишены актуальности, ничем не превосходит политику, которая по причине ошибки исключает из рассмотрения какое-либо важное условие.

Процесс разработки политики безопасности представляет собой совместное дело руководства компании, которому полагается в точности определить, какую ценность имеет каждый информационный ресурс, и какой объем денежных средств выделяется на обеспечение информационной безопасности, и системных администраторов, которым полагается выполнить истинную оценку существующей уязвимости данной информации.

После чего, в соответствии с основными рисками политики, распределяются средства, выделяемые на безопасность. В дальнейшем системным администраторам следует определить способы, направленные на снижение уязвимости информационного ресурса и, опираясь на ценность, которую имеет данный ресурс, осуществить согласование с руководством применяемых методов.

Под методами в данном случае следует понимать не только написание или покупку и установку требуемых программ и оборудования, но также осуществление

обучения персонала, разработку должностных инструкций и предписание ответственности за их невыполнение [2].

2.2 Разработка и внедрение высокоэффективных политик

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

Внедрение политики безопасности практически всегда связано с созданием некоторых неудобств для сотрудников организации и снижением производительности бизнес процессов. (Однако правильная система мер информационной безопасности повышает эффективность бизнес процессов организации за счет значительного повышения уровня информационной безопасности, являющегося одним из основных показателей эффективности).

Влияние мер информационной безопасности 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.

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

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

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

политики безопасности.

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

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

Контроль выполнения правил политики безопасности может осуществляться путем проведения плановых проверок в рамках мероприятий по аудиту информационной безопасности.

В организации должны быть предусмотрены меры по реагированию на нарушение правил политики безопасности. 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 политики безопасности должны быть предусмотрены конкретные дисциплинарные, административные взыскания и материальная ответственность.

Политика безопасности не является набором раз и навсегда определенных прописных истин. Не следует пытаться путем внедрения политики безопасности решить сразу все проблемы информационной безопасности. Политика является

результатом согласованных решений, определяющих основные требования по обеспечению информационной безопасности и отражающих существующий уровень понимания этой проблемы в организации.

Для того чтобы оставаться эффективной политика безопасности должна периодически корректироваться. Должна быть определена ответственность за поддержание политики безопасности в актуальном состоянии и назначены интервалы ее пересмотра. Политика безопасности 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.

На этапе внедрения политики безопасности решающее значение имеет поддержка руководства организации. Политика безопасности вводится в действие приказом руководителя организации и процесс ее внедрения должен находиться у него на контроле. В политике безопасности должна быть явным образом прописана озабоченность руководства вопросами обеспечения информационной безопасности.

Со стороны координатора рабочей группы по разработке политики безопасности руководству организации должны быть разъяснены риски, возникающие в случае отсутствия политики безопасности, а предписываемые политикой безопасности меры по обеспечению информационной безопасности должны быть экономически обоснованы[6].

2.3 Формирование благоприятной среды

В предыдущих разделах был сделан вывод о том, 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 действий, которые могут быть предприняты для обеспечения полной поддержки политики безопасности руководством

организации, что должно существенно увеличить эффективность политики.

Об этом уже упоминалось ранее, но стоит подчеркнуть вновь. 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).

Вне зависимости 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, в качестве примера, назовем этого человека «руководителем 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.

2.4 Понятие жизненного цикла политики безопасности

Разработка политики безопасности – длительный и трудоемкий процесс, требующего высокого профессионализма, отличного знания нормативной базы в области информационной безопасности и, помимо всего прочего, писательского таланта. Этот процесс обычно занимает многие месяцы и не всегда завершается успешно.

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.

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

С наибольшими трудностями приходится сталкиваться на этапе внедрения политики безопасности, 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.

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

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

Первая версия политики безопасности обычно не в полной мере отвечает потребностям организации, однако понимание этого приходит с опытом. Скорее всего, после наблюдения за процессом внедрения политики безопасности 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 информационной безопасности. В большинстве случаев ежегодный пересмотр политики безопасности является нормой, которая устанавливается самой политикой [6].

Заключение

На сегодняшний день известно много различных систем безопасности, которые служат цели обеспечения должной степени защищенности информации, но нет никакой возможности с уверенностью утверждать, что какая-либо одна из них лучше, чем другие.

Как нет и примеров разработки универсальной системы, которая обладала бы совершенной структурой, которую можно было бы взять за основу политики безопасности собственной организации. В каждой частной ситуации следует применять индивидуальный подход к построению системы, осуществляющей управление информационной безопасностью, основываясь на реальных данных, имеющихся в наличии, с привлечением сторонних специалистов в сфере информационной безопасности.

В первую очередь следует четко определить, в чем заключается информационная безопасность для этой конкретной компании и какие действия возможно предпринять с целью ее поддержания. Получив ответ на такой вопрос, можно, взяв его за основу, как фундамент, выполнить проект, а затем реализовать ту модель информационной безопасности, которая отвечала бы требованиям именно этой компании, обеспечивая должный уровень защищенности данных и обладающей наиболее эффективной реализацией.

Процесс разработки и внедрения политики безопасности в организации является результатом коллективного творчества, и в этом процессе следует принимать участие представителям всех подразделений, которые затрагиваются осуществляемыми переменами.

В качестве координатора сего процесса должен выступать специалист, несущий ответственность за надлежащее обеспечение информационной безопасности этого предприятия. Этим специалистом осуществляется координация деятельности рабочей группы, осуществляющей разработку и внедрение политики безопасности все время пока длится жизненный цикл проекта, который включает в себя осуществление аудита безопасности, выполнение разработки, согласования, внедрения, обучения, контроля исполнения, пересмотра и корректировки политики безопасности.

Чтобы разработать эффективную политику безопасности, мало обладать профессиональным опытом, знанием нормативной базы в в сфере информационной безопасности, следует также принимать в расчет ряд основных факторов, оказывающих значимое влияние на эффективность, которую имеет политика

безопасности, и четко соблюдать основные принципы разработки политики безопасности, к числу которых следует отнести следующие: минимизацию влияния, оказываемого политикой безопасности на производительность труда, непрерывное обучение, осуществление контроля и оперативного реагирования на происходящие нарушения безопасности, поддержку руководства компании и непрерывное совершенствование политики безопасности [6].

СПИСОК ЛИТЕРАТУРЫ

1. Кирсанов К.А., Малявина А.В., Попов Н.В. «Информационная безопасность: Учебное пособие». – М.:МАЭП, ИИК «Калита», 2015.
2. Гусев В.С., Демин В.А., Кузин Б.Л. и др. Экономика и организация безопасности хозяйствующих субъектов, 2-е изд. – СПб.: Питер, 2016. – 288 с.
3. Одинцов А.А. Экономическая и информационная безопасность предпринимательства: учеб. пособие для вузов. – М.: академия, 2016. – 336 с.
4. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. Пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 280 с.
5. Курочкин А.С. Управление предприятием: Уч. пособие. – Киев, 2015.
6. Биячуев, Т.А. Безопасность корпоративных сетей / Т.А. Биячуев. – СПб: СПб ГУ ИТМО, 2016.- 161 с.
7. Шахраманьян, М.А. Новые информационные технологии в задачах обеспечения национальной безопасности России/ Шахраманьян, М.А. – М.: ФЦ ВНИИ ГОЧС, 2016.- 222с.
8. Амитан В.Н. Экономическая безопасность: концепция и основные модели // Економічна кібернетика. – 2015. – №3-4. – С.13-20.
9. Башлыков М. Актуальные вопросы информационной безопасности //Финансовая газета. Региональный выпуск. 2016. № 4
10. Волков П. Системы обеспечения информационной безопасности как часть корпоративной культуры современной организации //Финансовая газета. 2016. № 34