Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

«Политика информационной безопасности издательства»

Выполнил:

студент 3 курса 7 группы

специальности ПОИБМС

Кот И.В.

Минск 2020

1. Обоснование актуальности разработки политики информационной безопасности (ПИБ)

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 эти 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.

Вследствие этого, в дополнение к требованиям и рекомендациям стандартов, Конституции, законам и иным руководящим документам приходится использовать ряд международных рекомендаций. В том числе адаптировать к отечественным условиям и применять на практике методики международных стандартов, таких, как ISO 17799, ISO 9001, ISO 15408, BSI, COBIT, ITIL и другие, а также использовать методики управления информационными рисками в совокупности с оценками экономической эффективности инвестиций в обеспечение защиты информации предприятия.

1. Цель и задачи разработки ПИБ

Основной целью является защита информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредство случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а так же минимизация рисков Информационной Безопасности (ИБ).

Для достижения основной цели необходимо обеспечивать эффективное решение следующих задач:

* Своевременное выявление, оценка и прогнозирование источников угроз ИБ.
* Создание механизма оперативного реагирования на угрозы ИБ.
* Предотвращение и/или снижение ущерба от реализации угроз ИБ.
* Защита от вмешательств в процесс функционирования Информационной Системы (ИС) посторонних лиц.
* Соответствие требованиям законодательства по информационной безопасности Республики Беларусь, нормативно-методических документов и договорным обязательствам в части ИБ.
* Обеспечение непрерывности критических бизнес-процессов;
* Достижение адекватности мер по защите от угроз ИБ.
* Изучение партнёров, клиентов, конкурентов и кандидатов на работу.
* Недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями.
* Выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников.
* Повышение деловой репутации и корпоративной культуры.

1. Описание структуры компании

Эффективность управления деятельностью зависит от того, насколько сформировала организационная структура управления и насколько она соответствует цели деятельности организации.

Изда́тельство – предприятие (государственное, общественное, кооперативное или частное) – медиакомпания, которая работает в области литературы, искусства, музыки или науки, и продукция которой может воспроизводиться и распространяться.

Распространение издательской продукции может осуществляться через каналы торговли, интернет, а также непосредственно самим издателем. Распространение может быть как платным, так и бесплатным, в зависимости от целей существования издательства и от его бизнес-модели.

Сущность издательской деятельности – распространение информации и создание прибавочной стоимости объектов авторского права. Издательство, руководствуясь своим опытом, приобретает исключительное право у автора (писателя, художника) на издаваемое произведение, и организует его воспроизведение (изготовление) и распространение. При этом практикуется как гонорар – выплата разового вознаграждения автору Произведения, так и роялти – выплата определённого договором процента от выручки за продажу произведения.

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

Составляющими организационных структур являются:

* Элементы организационных структур управления – службы и органы аппарата управления, а также отдельные работники этих служб(органов).
* Организационные отношения – отношения(связи) между подразделениями организации, уровнями ее управления персоналом, посредством которых реализуются функции управления.
* Уровни управления – совокупность прав, обязанностей и ответственности, характерна для должностных лиц, занимающих определённую ступень в иерархической структуре организации.

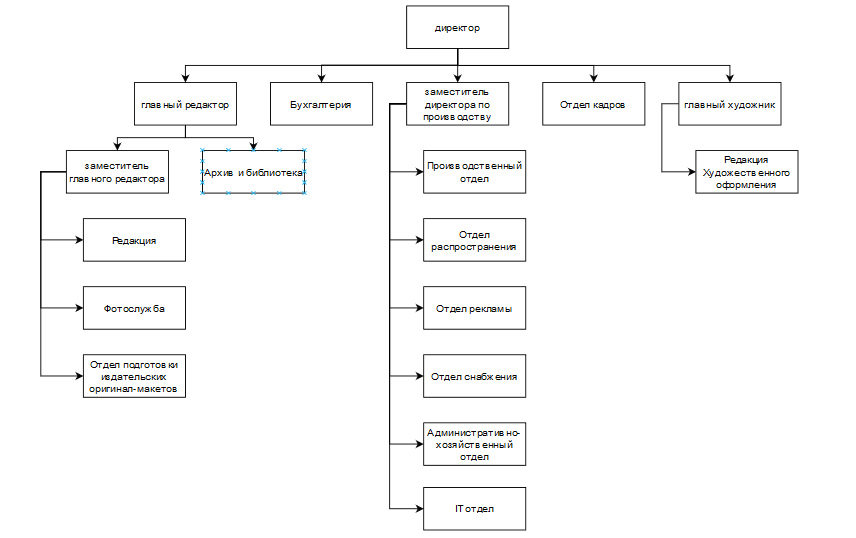


Рисунок 3.1 Организационная структура издательства

Структура издательства (рис. 3.1) имеет вертикальную и горизонтальную градации. При построении управленческой структуры выделяют следующие элементы издательства: компания в целом, директор, заместители, департаменты, отделы. Структура издательства отражает специфику его деятельности и подчинена задаче оптимизации процессов взаимодействия между различными структурными подразделениями компании с целью наиболее эффективного (рационального) использования имеющихся у компании ресурсов и выполнения принятых на себя обстоятельств.

В зависимости от масштабов издательства, его структура может отличаться.

1. Объекты защиты

В деятельности издательства образуются следующие объекты информации:

* коммерческая тайна самой издательства, данные о договорах, финансовых взаимоотношениях, бухгалтерская информация;
* коммерческая тайна клиентов и партнеров организации, данные об их активах, имуществе, платежах;
* персональные данные сотрудников компании и сотрудников клиентов;

Все массивы информации содержатся как на бумажных, так и на электронных носителях. Эти данные могут стать объектом противоправного покушения, их сохранность требует принятия серьезных мер безопасности. Несанкционированный доступ к охраняемым законом сведениям является уголовным преступлением.

Основными объектами обеспечения ИБ в издательстве признаются следующие элементы:

* информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством и внутренними нормативными документами компании к конфиденциальной информации;
* средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети, системы), на которых производится обработка, передача и хранение защищаемой информации.
* программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) автоматизированной системы издательства, с помощью которых производится обработка защищаемой информации;
* процессы издательства, связанные с управлением и использованием информационных ресурсов;
* помещения, в которых расположены средства обработки защищаемой информации;
* рабочие помещения и кабинеты работников издательства, помещения издательства, предназначенные для ведения закрытых переговоров и совещаний;
* персонал издательства, имеющий доступ к защищаемой информации.

Политика применяется ко всем работникам издательства, стажерам, практикантам, контрагентам и иным лицам, так или иначе имеющим доступ к информационным ресурсам издательства или вовлеченным в процессы информационного обмена.

В издательстве должны быть выявлены и оценены с точки зрения их важности все ресурсы. Для всех ценных ресурсов должен быть составлен реестр(перечень). Благодаря информации о ресурсах издательства реализуется защита информации, степень которой соразмерна ценности и важности ресурсов.

В ИС издательства присутствуют следующие типы ресурсов:

* Информационные ресурсы, содержащие конфиденциальную информацию, сведения ограниченного доступа, в том числе информацию о финансовой деятельности издательства.
* Открыто распространяемая информация, необходимая для работы издательства, независимо от формы и вида её представления.
* Информационная структура, включая системы обработки и анализ информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Для каждого ресурса должен быть назначен владелец, который отвечает за соответствующую классификацию информации и ресурсов, связанных со средствами обработки информации, а также за назначение и периодическую проверку прав доступа и категорий, определенных политиками управления доступа.

Все информационные ресурсы, подлежащие защите, должны быть классифицированы в соответствии с важностью и степенью доступа. Классификация информации должна быть документирована и утверждена руководством издательства.

Классификация информации должна проводиться владельцем ресурса, хранящего или обрабатывающего информацию, для определения категории ресурса. Периодически классификация должна пересматриваться для поддержки актуальности её соответствия с категорией ресурса.

Ресурсы, содержащие конфиденциальную или критичную информацию, должны иметь соответствующую пометку.

1. Основные угрозы и их источники

Под угрозами ИБ издательства понимается потенциальная возможность нарушения главных свойств информации.

Опасность нарушителя во многом определяется количеством и степенью важности доступных ему информационных ресурсов. Исходя из этого, наиболее рисковыми категориями следует считать сотрудников, работающих с большими объемами клиентской и финансовой информации.

Фактор, воздействующий на ИВС, – это явление, действие или процесс, результатом которых может быть утечка, искажение, уничтожение данных, блокировка доступа к ним, повреждение или уничтожение системы защиты.

Все дестабилизирующие факторы можно разделить на два класса: внутренние и внешние.

Источниками внутренних угроз являются:

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

Внутренние угрозы могут проявляться в следующих формах:

* ошибки пользователей и системных администраторов;
* нарушения сотрудниками предприятия установленных регламентов сбора, обработки, передачи и уничтожения информации;
* ошибки в работе программного обеспечения;
* отказы и сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся:

* компьютерные вирусы и вредоносные программы;
* организации и отдельные лица;
* стихийные бедствия.

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации:

* информационные;
* программные;
* физические;

К информационным угрозам относятся:

* несанкционированный доступ к информационным ресурсам;
* незаконное копирование данных в информационных системах;
* хищение информации из архива, отделов и баз данных;
* нарушение технологии обработки информации;
* противозаконный сбор и использование информации;

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;
* хищение носителей информации;
* хищение программных или аппаратных ключей и средств криптографической защиты данных;
* воздействие на персонал (шантаж, нападение).
* специфические угрозы безопасности
* возможность отключения электричества, что приведет к сбою незавершенных операций и потере данных.
* угроза возникновения неправильной адресации пакетов.
* угроза проникновения на рабочие места сотрудников людей, не являющихся работниками отделов, которые имеют туда доступ, и попадания на предприятие предметов, способных нанести ущерб.

В общем случае, нарушитель может использовать следующие способы осуществления доступа к защищаемой информации:

* Атаки, основанные на использовании средств защиты от НСД к информации с внесенными в процессе разработки или в процессе транспортировки уязвимостями и недокументированными (не декларированными) возможностями.
* Атаки, основанные на ошибках и внесении уязвимостей и недокументированных (не декларированных) возможностей при создании и накладке системы защиты от НСД.
* Перехват разглашаемых сведений о защищаемой информации, информационной системе и ее компонентах.
* Восстановление защищаемой информации путем анализа выведенных из потребления и ставших после этого доступными нарушителю носителей информации.
* Считывание или восстановление информации по остаточным следам на носителях защищаемой информации, сданных в ремонт, на обслуживание, переданных для использования другими пользователями или для использования за пределами учреждения.
* Негласное (скрытое) изъятие съемных носителей защищаемой информации, аутентифицирующей или ключевой информации.
* Перехват защищаемой информации при ее передаче по каналам связи;
* Хищение съемных носителей защищаемой информации, аутентифицирующей или ключевой информации.
* Целенаправленное искажение защищаемой информации при ее передаче по каналам связи.
* Навязывание ложной (специально сформированной нарушителем) информации через каналы связи.
* Перенаправление потоков данных путем воздействия через каналы связи, не защищенные от НСД к информации организационно-техническими мерами.
* Целенаправленное искажение команд управления, передаваемых по каналам связи.
* Навязывание ложных (специально сформированных нарушителем) команд управления через каналы связи.
* Нарушение связи между компонентами технического комплекса за счет преднамеренной загрузки трафика ложными сообщениями, приводящей к исчерпанию пропускной способности каналов связи.
* Негласная (срытая) модификация защищаемой информации, хранящейся на съемных носителях информации.
* Визуальный просмотр защищаемой информации на экране монитора.
* Ознакомление с распечатанной защищаемой информацией.
* Вывод информации на неучтенные носители (в том числе, вывод на печать), а также с нарушением требований руководящих и нормативных документов, регламентирующих порядок обращения с информацией соответствующей категории доступа.
* Доступ к оставленным без присмотра функционирующим штатным средствам.
* Подбор аутентифицирующей информации пользователей системы.
* Несанкционированный доступ к защищаемой информации с использованием ошибок или уязвимостей штатных средств информационной системы учреждения.
* Модификация аппаратных средств и программного обеспечения.
* Провоцирование сбоев технических средств информационной системы учреждения.
* Внесение неисправностей в технические средства.
* Блокирование или уничтожение информации, аппаратных и программных компонентов.
* Несанкционированный доступ к защищаемой информации в процессе ремонтных и регламентных работ.

Перечисленные способы атак обычно используются в определенных сочетаниях, направленных на достижение конкретной цели.

Основными целями несанкционированного доступа к защищаемой информации являются нарушения:

* Конфиденциальности информации (ее разглашения).
* Целостности (модификации информации или программных и технических средств).
* Достоверности (идентичности объекта тому, что заявлено).
* Доступности (получения санкционированных услуг в приемлемые сроки).
* Подконтрольности (регистрации действий в отношении объекта).

Главной целью злоумышленника является получение конфиденциальной информации.

1. Оценка угроз, рисков и уязвимостей

В издательстве должны быть определены требования к безопасности путём методической оценки рисков. Оценки рисков должны выявить, определить количество и расположить по приоритетам риски в соответствии с критериями принятия рисков и бизнес целями издательства. Результаты оценки должны определять соответствующую реакцию руководство, приоритеты управления рисками ИБ и набор механизмов контроля для защиты от этих рисков.

Показатели ресурсов или потенциальное негативное воздействие на деятельность организации можно определять несколькими способами:

* Количественными (например, стоимостными).
* Качественными (могут быть построены на использовании таких понятий, как, умеренный или чрезвычайно опасный).
* Их комбинацией.

Пример шкалы для численной оценки рисков от несанкционированного доступа (НСД) к информационным ресурсам издательства (таблица 6.1).

Таблица 6.1 – Условная численная шкала для оценки ущерба издательству от НСД

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие информации принесет ничтожный моральных и финансовый ущерб издательству |
| 1 | Ущерб от атаки есть, но он незначителен, основная работа и положение издательства на рынке не затронуты |
| 2 | Работа издательства приостанавливается на некоторое время, за это время издательство несет убытки, но положение на рынке и количество клиентов меняется не значительно |
| 3 | Значительные потери на рынке и в прибыли. От издательства уходит основная часть клиентов. |
| 4 | Потери очень значительны, издательство теряет позиции на рынке. Для восстановления положения требуются крупные финансовые займы. |
| 5 | Издательство прекращает существование |

Пример шкалы вероятности того, что угроза будет реализована, приведен в таблице 6.2.

Таблица 6.2 – Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события (НСД) |
| 0 | Данный вид атаки отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

С помощью данных таблиц можно рассчитать риски, которым могут быть подвержены компоненты системы. На этапе анализа таблицы, риски задаются максимально допустимым уровнем – значением 0,5.

Таблица 6.3 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск  (Ущерб\*Вероятность) |
| Спам  (переполнение почтового ящика) | 1 | 0,4 | 0,4 |
| Копирование жесткого диска из центрального офиса | 3 | 0,1 | 0,3 |
| Непреднамеренный рассказ конфиденциальной информации сотрудниками издательства | 3 | 0,4 | 1,2 |
| Раскрытие основных планов и стратегий развития издательства | 4 | 0,1 | 0,4 |
| Раскрытие личных данных клиентов издательства | 3 | 0,2 | 0,6 |
| Итого | 2.8 | 0.24 | 0.58 |

Если интегральный риск (итого) превышает допустимый уровень, значит в системе безопасности набирается множество мелких проблем, которые также нужно решать комплексно. В этом случае выбираются те атаки, которые «Дают» самый значительный вклад в значение интегрального риска.

Оценка рисков предполагает системное сочетание анализа и оценивания рисков.

Кроме того, оценка рисков и выбор механизмов контроля должны проводиться периодически, чтобы:

* Учесть изменения бизнес-требований и приоритетов.
* Принять во внимание новые угрозы и уязвимости.
* Убедиться в том, что реализованные средства сохранили свою эффективность.

Перед обработкой каждого риска издательство должно выбрать критерии для определения возможности принятия этого риска. Риска может быть принят, если его величина достаточна мала и стоимость обработки нерентабельна для издательства. Такие решения должны регистрироваться.

Для каждого из оцененных рисков должно приниматься одно из решений по его обработке:

* Применение соответствующих механизмов контроля для уменьшения величины риска до приемлемого уровня.
* Сознательно и объективное принятие риска, если он точно удовлетворяет Политике Издательства и критериям принятия рисков.
* Уклонение от риска путём недопущения действий, которые могут быть его причиной.

1. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов

Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности в издательстве функции обеспечения ИБ возложены на IT отдел. На это подразделение возлагается решение следующих основных задач:

* Проведение в жизнь ПИБ.
* Определение требований к защите информации.
* Организация мероприятий и координация работ всех подразделений по вопросам комплексной защиты информации.
* Контроль и оценка эффективности принятых мер и применяемых средств защиты.
* Оказание методической помощи сотрудникам в вопросах обеспечения информационной безопасности.
* Регулярная оценка и управление рисками информационной безопасности в соответствии с установленными процедурами в области управления рисками.
* Выбор и внедрение средств защиты информации, включая организационные, физические, технические, программные и программное-аппаратные средства обеспечения СУИБ.
* Обеспечение минимально-необходимого доступа к информационным ресурсам, основываясь на требованиях бизнес-процессов.
* Информирование, обучение и повышение квалификации работников издательства в сфере ИБ.
* Расследование инцидентов ИБ.
* Сбор, накопление, систематизация и обработка информации по вопросам ИБ.
* Обеспечение необходимого уровня отказоустойчивости ИТ-сервисов и доступности данных для подразделений.

Для решения задач, возложенных на IT-отдел, его сотрудники имеют следующие права:

* Определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей информационной системы в указанной области.
* Получать информацию от пользователей ИС издательства по любым аспектам применения информационных технологий в издательстве.
* Участвовать в проработке технических решений по вопросам обеспечения безопасности информации проектировании и разработке новых информационных технологий.
* Участвовать в испытаниях разработанных информационных технологий по вопросам оценки качества реализации требований по обеспечению безопасности информации.
* Контролировать деятельность пользователей по вопросам обеспечения ИБ.
* Готовить предложения руководству по обеспечению требований ИБ.

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

Рассматриваются следующие объективные факторы:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Вывод

Каждый день появляются новые средства преодоления защитных барьеров, и степень опасности утраты ценных сведений растет, а вместе с ней и риск возможных финансовых потерь. Минимизировать риски можно, пройдя аудит своих систем защиты и получив рекомендации по их модернизации. Мероприятия по аудиту, требующие проведения проверок действующих систем, должны быть спланированы и согласованы таким образом, чтобы свести к минимуму риск прерывания бизнес-процессов. Доступ к средствам и результатам аудита информационных систем должен быть защищен и ограничен с целью предотвращения возможного несанкционированного использования, компрометации или модификации. Пересмотр настоящей Политики и подчиненных документов осуществляется по результатам процесса анализа и оценки либо в случае изменения факторов, влияющих на ее содержание, но не реже одного раза в год.

Следует учитывать, что все предпринимаемые действия должны в полной мере соответствовать требованиям законодательства. В частности, нарушение конфиденциальности данных юридической фирмы и их клиентов зачастую приводит к вымогательству и шантажу, инсайдерской торговле и недобросовестной конкуренции. Это не только нанесет урон репутации – юридическая фирма понесет ответственность – начиная от финансовой и закачивая уголовной