Содержание:

Введение

Информация – это один из самых ценных и важных активов любого предприятия и должна быть надлежащим образом защищена для того что бы её секреты оставались у компании.

Информационная безопасность в современном обществе - одна из самых больших проблем как для организаций, так и для конечных пользователей. В связи с развитием информационных технологий и компьютеризацией экономики одним из важнейших вопросов в деятельности компании становится обеспечение информационной безопасности. Потому что сейчас нету такого места где можно сохранить всю информацию. если кража корпоративной информации может привести к потере прибыли или разработки, то подделка или утечка личной переписки может привести к разрушению вполне счастливой семьи или распаду дружного коллектива. информации — состояние защищенности информационной технологии, обеспечивающее безопасность информации, для обработки которой она применяется, информационную безопасность автоматизированной информационной системы, в которой она реализована.

Раньше её хранили на бумагах и в сейфах, а сейчас её хранят в компьютере, но он не гарантирует сохранности так же, как и всё остальное что сейчас существует.

3

1. Понятие информационной безопасности

Информационная безопасность - предотвращения несанкционированного доступа, использования, раскрытия.

Закон об информации – **Защита** – любое активное или пассивное действие, направленное на достижение определенного состояния или уровня безопасности

объекта в которых бывает многоступенчатые защиты как по рангам, так и по должностям.

2. Основные угрозы информационной безопасности

Угрозы информационной безопасности можно разделить на следующие типы:

- **Естественные** (катаклизмы, независящие от человека: пожары, ураганы, наводнение, удары молнии и т.д.).
- **Искусственные,** которые также делятся на:

- непреднамеренные (совершаются людьми по неосторожности или незнанию);

- преднамеренные (хакерские атаки, противоправные действия конкурентов, месть сотрудников и пр.).

- **Внутренние** (источники угрозы, которые находятся внутри системы).
- **Внешние** (источники угроз за пределами системы)

4

Средства защиты информационной безопасности — это набор технических приспособлений, устройств, приборов различного характера, которые препятствуют утечке информации и выполняют функцию ее защиты.

Средства защиты информации

- **Организационные.** Это совокупность организационно-технических (обеспечение компьютерными помещениями, настройка кабельной системы и др.) и организационно-правовых (законодательная база, статут конкретной организации) средств.
- **Программные.** Те программы, которые помогают контролировать, хранить и защищать информацию и доступ к ней.
- **Технические (аппаратные).** Это технические виды устройств, которые защищают информацию от проникновения и утечки.

- **Смешанные аппаратно-программные.** Выполняют функции как аппаратных, так и программных средств.

Целями защиты информации являются:

· предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям;

· предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

· предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы;

· обеспечение правового режима документированной информации как объекта собственности;

· защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

· сохранение государственной тайны, конфиденциальности, документированной информации в соответствии с законодательством;

· обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

Правовая защита

— это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе.

Как известно, право — это совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в отношении определенных сфер жизни и деятельности государственных органов, предприятий (организаций) и населения (отдельной личности).

Правовая защита информации как ресурса признана на международном, государственном уровне и определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту. На государственном Уровне правовая защита регулируется государственными и ведомственными актами.

Организационная защита

— это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба исполнителям.

Организационная защита обеспечивает:

6

— организацию охраны, режима, работу с кадрами, с документами;

— использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности.

Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты. Влияния этих аспектов практически невозможно избежать с помощью технических средств. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или по крайней мере сводили бы к минимуму) возможность возникновения опасности конфиденциальной информации.

Техническая защита

— это использование различных технических средств, препятствующих нанесению ущерба коммерческой деятельности.

Инженерно-техническая защита (ИТЗ)

по определению — это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации. Первым из них по праву можно считать издание 22 октября 1992 г. двух Указов Президента Российской Федерации «О правовой охране программ для электронно-вычислительных машин и баз данных» и «О правовой охране топологий интегральных микросхем», регламентирующих порядок установления и правовую защиту авторских прав на программные средства компьютерной техники и топологии интегральных микросхем с 1 января 1994 г.

7

Вторым прогрессивным шагом в этом направлении является принятие Государственной Думой и Федеральным Собранием Российской Федерации сразу двух Законов: 20 января — «О связи» и 25 января 1995 г. «Об информации, информатизации и защите информации».

Решающим законодательным аккордом по рассматриваемому кругу проблем можно считать принятие в июне 1996 г. Уголовного кодекса Российской Федерации, устанавливающего уже уголовную ответственность за компьютерные преступления в Российской Федерации и выделяющего информацию в качестве объекта уголовно-правовой охраны [92, гл. 28].

Виды средств защиты информации

Антивирусные программы — программы, которые борятся с компьютерными вирусами и заражёнными файлами.

DLP (Data Leak Prevention) решения – это защита от утечки информации.

Криптографические системы – преобразование информации таким образом, что ее расшифровка становится возможной только с помощью определенных кодов или шифров.

VPN (Virtual Private Network). Виртуальная частная сеть (VPN) дает возможность определить и использовать для передачи и получения информации частную сеть в рамках общедоступной сети.

2.2.1 Правовая защита информации:

Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

8

2.2.4 физическая защита информации

Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Примечания

1 Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

2 К объектам защиты информации могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

Рекомендации по стандартизации «Информационные технологии. Основные термины определения в области технической защиты информации» (Р 50.1.053-2005).

Источник угрозы

Проблемы информационной безопасности связанны с мировоззрением некоторых людей, которым не нравиться какие-либо ситуации. Это могут быть сотрудники которых увольняют или хакер, который пытается забрать базу данных на последок. Да и самое главное распространение в сети появляется пираты, которые делают всю информацию и платные информацию делают бесплатной. Но простым людям больше ничего не надо так как все хотят получить бесплатно и взломанную программу лучше, чем якобы нормальную и покупную. Меньшая часть людей может аргументировать свою правоту в этом вопросе, и все же их доводы не отличаются от доводов обычных преступников. Большая же часть людей совершает эти преступления, не задумываясь, что это вообще плохо.

9

Некоторые люди хотят нагадить своему обидчику поэтому и просят знакомых или находят людей, в интернете которые могут помочь им. Они выполняют самую грязную работу, за которую им заплатили и не задают они не каких вопросов. Самое страшное, что сама среда толкает людей на такой образ деятельности. Человек, использующий интернет перестает быть собой. В интернете у него может быть другое имя, там он может быть кем угодно. И очень непросто связать реального человека сего Альтер-эго из интернета, что дает человеку несказанное чувство свободы и независимости. В интернете нет законодательной и исполнительной власти, и наказание за преступления не будет. При этом человек, скорее всего, даже не задумывается никогда об этом, но он это чувствует и позволяет себе вести себя соответствующим образом.

Но решение проблемы есть, и оно очень трудоёмкая.

Решение проблем

Борьба с информационной преступностью подобна борьбе с преступностью.

Организация интернета не предполагает наличия в себе какой-либо законодательной или исполнительной власти. Регулирующим фактором является запугивание. Страх заставляет пользователей быть более осторожными и при отсутствии необходимости не скачивать лишней музыки, не устанавливать лишний

раз программу. По последнему заявлению, представитель МВД назвал сетевую анонимность приглашением к преступлению. Он добавил, что злоумышленники активно пользуются возможностью спрятаться под псевдонимом или укрыться на территории зарубежного государства и назвал защитников концепции свободного от регулирования интернета, оперирующих терминами "гласность" и "свобода слова" демагогами, потакающими преступникам.

10

Принципы защиты информации

1. **Комплексность.**
2. **Своевременность.**
3. **Непрерывность.**
4. **Активность.**
5. **Законность.**
6. **Обоснованность.**
7. **Экономическая целесообразность.**
8. **Специализация.**
9. **Взаимодействие и координация деятельности.**
10. **Совершенствование.**
11. **Централизация управления.**

Средства защиты информации

1. Физические – различные инженерные средства и сооружения, затрудняющие или исключающие физическое проникновение (или доступ) правонарушителей на объекты защиты и к материальным носителям конфиденциальной информации.

2. Аппаратные – механические, электрические, электронные и другие устройства, предназначенные для защиты информации от утечки, разглашения, модификации, уничтожения, а также противодействия средствам технической разведки.

11

3. Программные – специальные программы для ЭВМ, реализующие функции защиты информации от несанкционированного доступа, ознакомления, копирования,

модификации, уничтожения и блокирования.

4. Криптографические – технические и программные средства шифрования данных, основанные на использовании разнообразных математических и алгоритмических методов.

5. Комбинированные – совокупная реализация аппаратных и программных средств и криптографических методов защиты информации.

Объект защиты – это информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Компьютерный вирус — разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (саморепликация). Вирусы распространяются, внедряя себя в исполняемый код других программ или же заменяя собой другие программы.

Антивирусная программа (антивирус) — изначально программа для обнаружения и лечения вредоносных объектов или инфицированных файлов, а также для профилактики — предотвращения заражения файла или операционной системы вредоносным кодом.

Основные положения Федерального закона «Об информации, информационных технологиях и защите информации»

Феральный закон «Об информации, информационных технологиях и о защите информации» — базовый нормативный документ, юридически описывающий понятия и определения области информационной технологии и задающий принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации, а также регулирует отношения при осуществлении права на поиск, получение, передачу, производство и распространение информации, при применении информационных технологий.

Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями)

Статья 1. Сфера действия настоящего Федерального закона

Статья 18. О признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации

14

Заключение

Методы передачи информации менялись и методы ее защиты. Письма, книги, телеграф, радио, телевидение, компьютеры, локальные сети, интернет. Когда информации было мало, каждый способ был уникален и своеобразен, теперь, когда объем информации стали огромны, появились методики защиты и рекомендации по безопасности. Угроз безопасности стало больше, так же появилось большое количество уязвимых мест, потребовалось изучение принципов и основ сохранения информации, разработка средств защиты, и как результат, появилась полноценная дисциплина, содержащая в себе многочисленные институты и немалый штат специалистов.

15

Список литературы

Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006)

Монография: Карасева М.В. Бюджетное и налоговое регулирование: единство и дифференциация: монография. - М.: КноРус, 2012. - 160 с**.**

Учебник: Правовое обеспечение туризма: учебник. / коллектив авторов ; под общ. ред. Е.Л. Писаревского. — М. : Федеральное агентство по туризму, 2014.- 415 с.

Публикация: Гольц Т.В. Проблемы регулирования защиты прав потребителей в сфере туристического обслуживания в России // Вестник ассоциации вузов туризма и сервиса. – 2010. – №1. – С.53-60.

Диссертация: Поветкина Н.А. Финансовая устойчивость Российской Федерации: правовая доктрина и практика обеспечения: дис. … д-ра юрид. наук. М., 2016. – 458 с.

16