

Понятие информационной безопасности

Под информационной безопасностью понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.

На практике важнейшими являются **три аспекта информационной безопасности:**

- доступность (возможность за разумное время получить требуемую информационную услугу);
- целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного прочтения).

Современная информационная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными.

Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. Компоненты автоматизированной информационной системы можно разбить на следующие группы:

-*Аппаратные средства.* Это компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства – принтеры, контроллеры, кабели, линии связи и т.д.);

-*Программное обеспечение.* Это приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т.д.;

-Данные, хранимые временно и постоянно, на дисках, флэшках, печатные, архивы, системные журналы и т.д.;

Персонал. Пользователи, системные администраторы, программисты и др.

Опасные воздействия на компьютерную информационную систему можно подразделить на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы. Причинами случайных воздействий при эксплуатации могут быть:

аварийные ситуации из-за стихийных бедствий и отключений электропитания;

отказы и сбои аппаратуры;

ошибки в программном обеспечении;

ошибки в работе персонала;

помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия – это целенаправленные действия нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами: недовольством служащего своей карьерой; взяткой; любопытством; конкурентной борьбой; стремлением самоутвердиться любой ценой.

Классификация каналов несанкционированного доступа, по которым можно осуществить хищение, изменение или уничтожение информации:

Через человека:

хищение носителей информации;
чтение информации с экрана или клавиатуры;
чтение информации из распечатки.

Через программу:

перехват паролей;
дешифровка зашифрованной информации;
копирование информации с носителя.

Через аппаратуру:

подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т.д.

Обеспечение информационной безопасности

Формирование режима информационной безопасности – проблема комплексная. Меры по ее решению можно подразделить на пять уровней:

1. Законодательный . Это законы, нормативные акты, стандарты и т.п.

Нормативно-правовая база определяющая порядок защиты информации:

2. Морально-этический. Всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации.

3. Административный. Действия общего характера, предпринимаемые руководством организации. Такими документами могут быть:

приказ руководителя о назначении ответственного за обеспечение информационной безопасности;

должностные обязанности ответственного за обеспечение информационной безопасности;

перечень защищаемых информационных ресурсов и баз данных;

инструкцию, определяющую порядок предоставления информации

сторонним организациям по их запросам, а также по правам доступа к ней сотрудников организации.

4. Физический. Механические, электро- и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей.

5. Аппаратно-программный (электронные устройства и специальные программы защиты информации).

Рекомендации по организации работы в информационном пространстве

1. Перед началом работы необходимо четко сформулировать цель и вопрос поиска информации.

2. Желательно выработать оптимальный алгоритм поиска информации в сети Интернет, что значительно сократит время и силы, затраченные на поиск.

3. Заранее установить временный лимит (2-3 часа) работы в информационном пространстве (просмотр телепередачи, чтение, Интернет).

4. Во время работы необходимо делать перерыв на 5-10 минут для снятия физического напряжения и зрительной нагрузки.

5. Необходимо знать 3-4 упражнения для снятия зрительного напряжения и физической усталости.

6. Работать в хорошо проветренном помещении, при оптимальном освещении и в удобной позе.

7. Не стоит легкомысленно обращаться со спам-письмами и заходить на небезопасные веб-сайты. Для интернет-преступников вы становитесь лёгкой добычей.

8. При регистрации в социальных сетях, не указывайте свои персональные данные, например: адрес или день рождения.

9. Не используйте в логине или пароле персональные данные.

10. Все это позволяет интернет-преступникам получить данные доступа к аккаунтам электронной почты, а также инфицировать домашние ПК для включения их в бот-сеть или для похищения банковских данных родителей.

11. Создайте собственный профиль на компьютере, чтобы обезопасить информацию, хранящуюся на нем.

12. Не забывайте, что факты, о которых вы узнаете в Интернете, нужно очень хорошо проверить, если выбудете использовать их в своей домашней работе. Целесообразно сравнить три источника информации, прежде чем решить, каким источникам можно доверять.

13. О достоверности информации, помещенной на сайте можно судить по самому сайту, узнав об авторах сайта.

14. Размещая информацию о себе, своих близких и знакомых на страницах социальных сетей, спросите предварительно разрешение у тех, о ком будет эта информация.

15. Не следует размещать на страницах веб-сайтов свои фотографии и фотографии своих близких и знакомых, за которые вам потом может быть стыдно.

16. Соблюдайте правила этики при общении в Интернете: грубость провоцирует других на такое же поведение.

17. Используя в своей работе материал, взятый из информационного источника (книга, периодическая печать, Интернет), следует указать этот источник информации или сделать на него ссылку, если материал был вами переработан