Безопасное использование информационных технологий

Company
LOGO

Информационная безопасность - это

- Состояние защищенности информационной среды организации, обеспечивающее её формирование, использование и развитие;
- Состояние сохранности информационных ресурсов и защищенности прав личности и общества в информационной сфере;
- Предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Основные признаки информационной безопасности:

Нормативные документы в области информационной безопасности:

- Международные договоры Российской Федерации;
- Конституция Российской Федерации;
- Федеральные законы;
- Указы Президента Российской Федерации;
- Постановления правительства Российской Федерации;
- Нормативные правовые акты федеральных министерств;
- Нормативные правовые акты субъектов РФ, органов местного самоуправления.

Государственные органы Российской Федерации, контролирующие деятельность в области защиты информации:

- Совет безопасности России;
- Федеральная служба по техническому и экспортному контролю (ФСТЭК);
- Федеральная служба безопасности РФ (ФСБ России);
- Министерство внутренних дел РФ (МВД России);
- Комитет Государственной думы по безопасности;
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

Практические правила управления информационной безопасностью:

- Политика безопасности;
- Организация защиты базы данных;
- Классификация ресурсов и их контроль;
- Безопасность персонала;
- Физическая безопасность;
- Администрирование компьютерных систем и сетей;
- Управлением доступом к информации;
- Разработка и сопровождение информационных систем;
- Планирование бесперебойной работы организации;
- Контроль выполнения требований политики безопасности.

Службы, организующие защиту информации на уровне предприятия:

Направления защиты информационной системы:

- Защита объектов информационной среды;
- Защита процессов, процедур и программ обработки информации;
- Защита каналов связи;
- Подавление побочных электромагнитных излучений;
- Управление системой защиты.

Программно-технические способы и средства обеспечения информационной безопасности:

- Защита объектов информационной среды;
- Защита процессов, процедур и программ обработки информации;
- Защита каналов связи;
- Подавление побочных электромагнитных излучений;
- Управление системой защиты;
- Антивирусные средства;
- Межсетевые экраны;
- Криптотехнические средства: шифрование цифровая подпись;

- Системы резервного копирования;
- Системы бесперебойного питания;
- Системы аутентификации:
  - пароль
  - сертификат
  - биометрия;
- Средства предотвращения взлома корпусов и краж оборудования;
- Средства контроля доступа в помещения

Угроза безопасности -

это действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов компьютера, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства.

Различают два типа угроз:

- Случайные или непреднамеренные (ошибки в программном обеспечении, выходы из строя аппаратных средств, неправильные действия пользователей;
- Умышленные (преследуют определенные цели, связанные с нанесением ущерба пользователям (абонентам) сети.

- **В настоящее время очень развита отрасль правонарушений в сфере информационных технологий. Компьютерные преступники создают программы, которые помогают «скачивать» через Интернет новейшие художественные фильмы, музыку, видеоигры…, что наносит многомиллионный вред людям, несущим ответственность за эту структуру.**
- **Появилась новая профессия – хакер – компьютерный преступник, в среде пользователей это высококвалифицированный программист.**

- Ха́кер (от англ. *hack* — разрубать) — чрезвычайно квалифицированный ИТ-специалист, человек, который понимает самые основы работы компьютерных систем. Это слово также часто употребляется для обозначения компьютерного взломщика, что в общем случае неверно.
- Хакерами называют, например, Линуса ТорвальдсаХакерами называют, например, Линуса Торвальдса, Ричарда СтоллманаХакерами называют, например, Линуса Торвальдса, Ричарда Столлмана и других создателей открытых систем мирового уровня. В России ярким

Многие организации, компании, банки оказываются объектом множества злонамеренных действий:

- вторжение
- вирусная атака
- порча информации
- кража информации…
- кража денежных средств
- кража документов
- кража секретной информации…

Опасный Интернет

Сегодня любую информацию можно найти в Интернете.

Интернет дает колоссальные возможности для развития человека, его информационной «подпитки». С другой стороны - на нем можно и болезненно зациклиться. Что нередко и происходит. Многие с головой уходят в иллюзорно-виртуальный мир, увлеченно общаются с «кибердрузьями», с «киберневестами» и постепенно начинают терять грань, разделяющую реальную, повседневную жизнь с электронными фантомами.

Несомненно, Интернет развивает коммуникативные способности, но, учитывая односложность интернет-реплик и использование смайликов интернет-фанат забывает какие слова надо говорить, как себя держать. Развивается социальная детренированность, а порой – одичание.

В связи с этим появились новые болезни:

- **интернет-психозы**
- **интернет-неврозы**
- **психологический синдром**
- **зомбирование Интернетом**
- **интернет-зависимость,**

которые в конечном итоге могут привести к шизофрении.

Опасный Интернет

Как обезопасить себя ?

- **нужно знать «опасные места» Интернета:**
  - **интерактивные казино,**
  - **сомнительные объявления**
  - **порнография…**
- **установить антивирусную программу;**
- **удалить неиспользуемые сетевые протоколы;**
- **создать учётную запись пользователя с ограниченными правами;**
- **ежедневно отслеживайте состояние вашего лицевого счета.**

Опасности Интернета: защитите ребенка от опасностей Интернета:

Интернет - мощный инструмент для школы и знаний.

В то же время он может быть опасным, предлагая ребенку порнографию, а также личные встречи с нежелательными интернет-друзьями.

Советы родителям :

- Компьютер должен использоваться для изучения;
- Приобретите программу, которая будет блокировать нежелательные сайты для «взрослых»;
- Будьте осведомлены, как ваш ребенок использует компьютер;
- Расспросите ребенка о его Интернет-друзьях;
- Педофилы используют подростковые чаты, чтобы найти там детей. Не разрешайте ребенку вводить какую-либо персональную информацию в чатах;

  Чаты позволяют общаться один на один. Не разрешайте ребенку участвовать в таких беседах.

Советы родителям:

- Убедитесь, что ваш ребенок рассказывает обо всем необычном, что он увидел в Интернете;
- Не позволяйте ребенку посылать или получать картинки по Интернету от тех людей, с кем вы лично не знакомы;
- Не позволяйте вашему ребенку использовать Интернет поздно ночью.