

Информационная безопасность

Подготовили студенты ПНБс-1904-02-00:
Виловатых Екатерина
Сагдуллина Алина
Каграманова Алина

Почему мы выбрали данную тему:

Мы считаем, что для данной необходимо выделить еще немного времени т.к она очень важна.

Как будущие юристы, которые будут защищать права человека, понимая что в современном мире все происходит через интернете и очень важно знать как можно защитить свои права в сети.

Информационная безопасность: понятие

Информационная безопасность (ИБ) - защита личности, общества и государства в информационной сфере.



Задачи информационной безопасности

- Разработка основных направлений гос. политики в области ИБ;
- Развитие и совершенствование системы обеспечения ИБ;
- Разработка федеральных программ;
- Разработка критериев и методов оценки эффективности ИБ;
- Совершенствование нормативно-правовой базы
- Установление ответственности должностных лиц органов гос. власти;
- Координация деятельности органов гос. власти;
- Развитие научно-практических основ обеспечения ИБ;

Задачи информационной безопасности

- Разработка и создание механизмов формирования гос. информационной политики;
- Разработка методов повышения участия государства в ИБ;
- Обеспечение технологической независимости России;
- Разработка современных методов и средств обеспечения ИБ;
- Развитие гос. системы защиты информации;
- Развитие защищенной основы управления государством в разное время;
- Расширение взаимодействия с международными организациями;
- Обеспечение условий для развития российской информационной инфраструктуры;
- Создание единой системы подготовки кадров в области ИБ

Методы обеспечения информационной безопасности

Общие

Частные

Правовые

Экономические

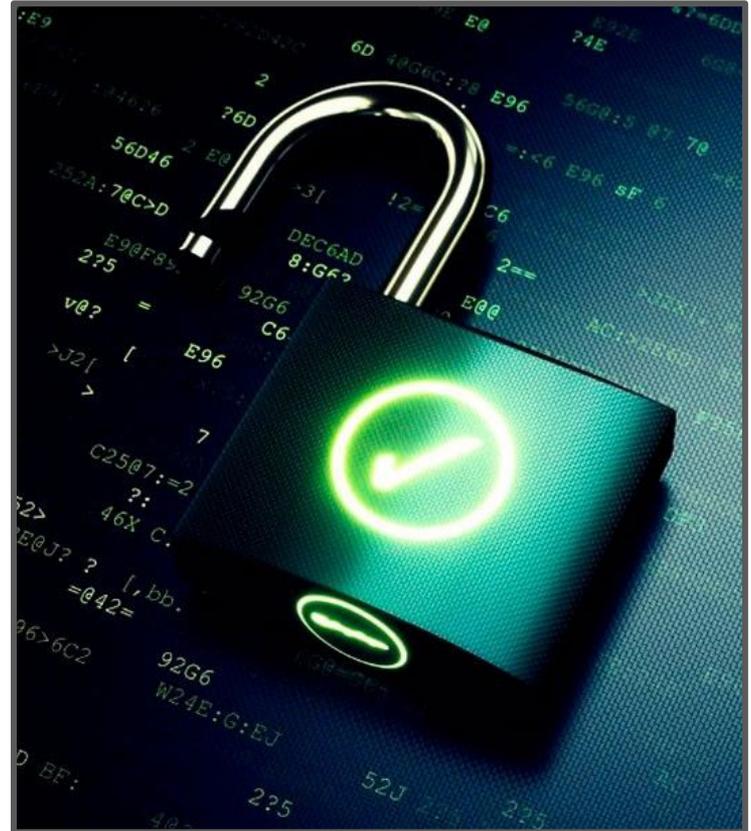
Организационно-технические



Методы обеспечения ИБ: общие правовые методы

Основные направления:

- Законодательное разграничение полномочий;
- Разработка и принятие нормативно-правовых актов РФ;
- Законодательное закрепление приоритета развития сетей связи;
- Определение статуса информационных организаций;
- Создание правовой базы



Методы обеспечения ИБ: общие организационно-технические методы

- Создание и совершенствование системы обеспечения ИБ в России;
- Усиление правоприменительной деятельности;
- Взаимодействия со средствами защиты информации;
- Создание средств и систем предотвращения уничтожений информации;
- Выявление опасных устройств и программ;
- Сертификация средств защиты информации;
- Контроль за действиями персонала в информационных системах

Методы обеспечения ИБ: частные методы

Разделение на методы, связанные спецификой сфер жизнедеятельности личности, общества и государства.



Методы защиты информации:

Сегодня используется шесть основных методов защиты:

- Препятствие;
- Управление доступом;
- Маскировка;
- Регламентация;
- Управление;
- Принуждение;
- Побуждение.



Защита информации и ее уровни.

Федеральный Закон «Об информации, информационных технологиях и о защите информации»
№149-ФЗ от 27 июля 2006г,

Защита информации представляет собой принятие правовых, организационных и технических мер.



Защита информации – это комплекс организационно-технических мероприятий, направленных на обеспечение информационной безопасности.



Уровни защиты информации:

- законодательный;
- административный;
- процедурный;
- программно-технический.



Группы процедурных мер:

- управление персоналом;
- физическая защита информации;
- поддержание работоспособности оборудования;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Программно-технические мероприятия:

- идентификация и проверка подлинности пользователей;
- управление доступом;
- протоколирование и аудит;
- криптография;
- экранирование;
- обеспечение высокой доступности (то есть, принятие всевозможных мер для того, чтобы запрашиваемая пользователями была доступна, чтобы всякого рода проблемы с оборудованием не препятствовали этому).



Защита информации при работе в сети Интернет.

Интернет - глобальная компьютерная сеть, охватывающая весь мир.

Интернет - находка для мошенника. Злоумышленнику созданы все условия: анонимность, сокрытие сведений о себе, доверчивые пользователи.

ФЗ № 98 от 29.07.2004 «О коммерческой тайне»

ФЗ № 152 от 27.07.2006 «О персональных данных»

ФЗ № 5485-1 от 21.07.1993 «О государственной тайне»

ФЗ № 2446-1 от 05.03.1992 «О безопасности»

Классификация средств защиты информации.

Средства защиты информации делятся на две большие группы:

- нормативные;
- технические.

К нормативным средствам относятся:

- законодательные;
- административные;
- морально-этические.

К техническим средствам относятся:

- физические;
- аппаратные;
- программные;
- криптографические.

Защита компьютера пользователя:

1. Надежные пароли.
2. Шифрование данных.
3. Антивирус.
4. Защита беспроводной сети.
5. Родительский контроль
6. VPN .
7. Двухфакторная аутентификация
8. Внимательность и осторожность с почтой.
9. Регулярное обновление программного обеспечения.



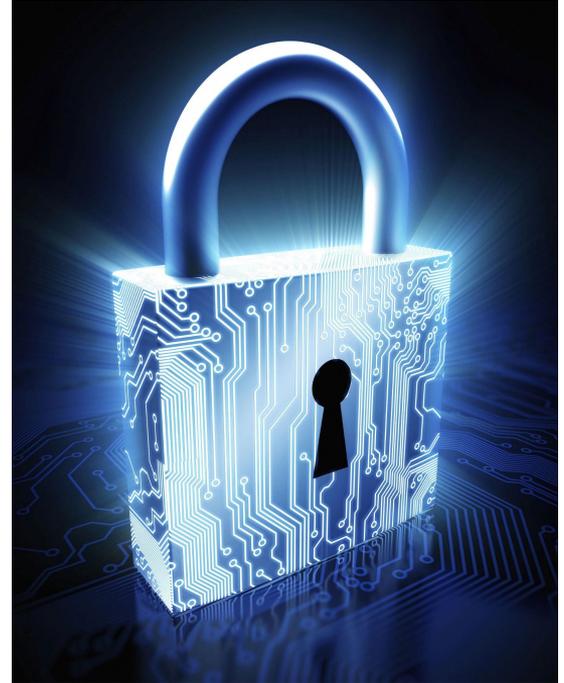
Система защиты информации:

Система защиты информации — это комплекс организационных и технических мер, направленных на обеспечение информационной безопасности предприятия.



Система защиты информации включает:

- Адекватность требования
- Концептуальное единство
- Адаптация к меняющимся условиям
- Удобство применения
- Функциональная самостоятельность
- Адекватное реагирование
- Полнота контроля и экономичность



Вывод:

Развитие информационных технологий побуждает к постоянному приложению совместных усилий по совершенствованию методов и средств, позволяющих достоверно оценивать угрозы безопасности информационной сферы и адекватно реагировать на них.

Защите информации в последнее время уделяется все большее внимания на самых различных уровнях. Поэтому следует быть более подкованным в данном вопросе и не забывать о безопасности в Интернете.