Государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича

Управление процессами информационных систем

Рогачев Виктор Алексеевич

Лекция 10

Безопасность информационных систем

темы:

1. Понятие информационной безопасности (ИБ)
2. Категории ИБ
3. Составляющие и стандарты ИБ
4. Классификаци средств защиты информации
5. Организационная защита объектов информатизации
6. Исторические аспекты ИБ

Информационная безопасность

Информационная безопасность - это процесс обеспечения:

1. конфиденциальности,
2. целостности,
3. доступности,

информации.

Конфиденциальность (от англ. confidence — доверие)

необходимость предотвращения утечки (разглашения) какой-либо информации.

Конфиденциальность в различных областях:

- Конфиденциальность - обязательство неразглашения информации, полученной от партнера,
- Государственная тайна - защищаемые государством сведения в области его деятельности, распространение которых может нанести ущерб безопасности Российской Федерации
- Коммерческая тайна - сведения, позволяющие её обладателю получить коммерческую выгоду

преступления против конфиденциальности в сфере компьютерной информации:

- Противозаконный доступ
- Неправомерный перехват
- Воздействие на данные
- Воздействие на функционирование системы
- Противозаконное использование устройств

Целостность информации

Целостность информации - состояние информации, при котором:

- отсутствует любое её изменение,
- либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Методы обеспечения целостности информации:

- обеспечение отказоустойчивости (резервирование, дублирование, зеркалирование оборудования и данных)
- обеспечение безопасного восстановления (резервное копирование и электронное архивирование информации).

Хеширование (hashing):

преобразование по определённому алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины

- CRC - (Cyclic redundancy check) - Циклический избыточный код
- MD5 - 128-битный алгоритм хеширования
- SHA512 - 512-битный алгоритм хеширования

Хэширование применяется для контрольного суммирования с целью обнаружения ошибок при хранении или передаче, для хранения паролей в системах защиты

Доступность информации

Доступность (availability) информации:

состояние информации, при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно

К правам доступа относятся:

- право на чтение информации
- право на изменение информации
- право на копирование информации
- право на уничтожение информации
- право на изменение ресурсов
- право на использование ресурсов
- право на уничтожение ресурсов

Категории информационной безопасности

Категории ИБ

- конфиденциальность - гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена
- целостность - гарантия того, что информация сейчас существует в ее исходном виде
- доступность - состояние информации, при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно
- аутентичность - гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор

Категории для информационных систем

- надежность - система ведет себя по плану в нормальном и внештатном режимах
- точность - точное и полное выполнение всех команд
- контроль доступа - различные группы лиц имеют различный доступ к информационным объектам
- контролируемость - любой момент может быть произведена полноценная проверка любого компонента программного комплекса
- контроль идентификации - клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает
- устойчивость к умышленным сбоям - при умышленном внесении ошибок в пределах заранее оговоренных норм система будет вести себя так, как оговорено заранее.

Стандарты информационной безопасности

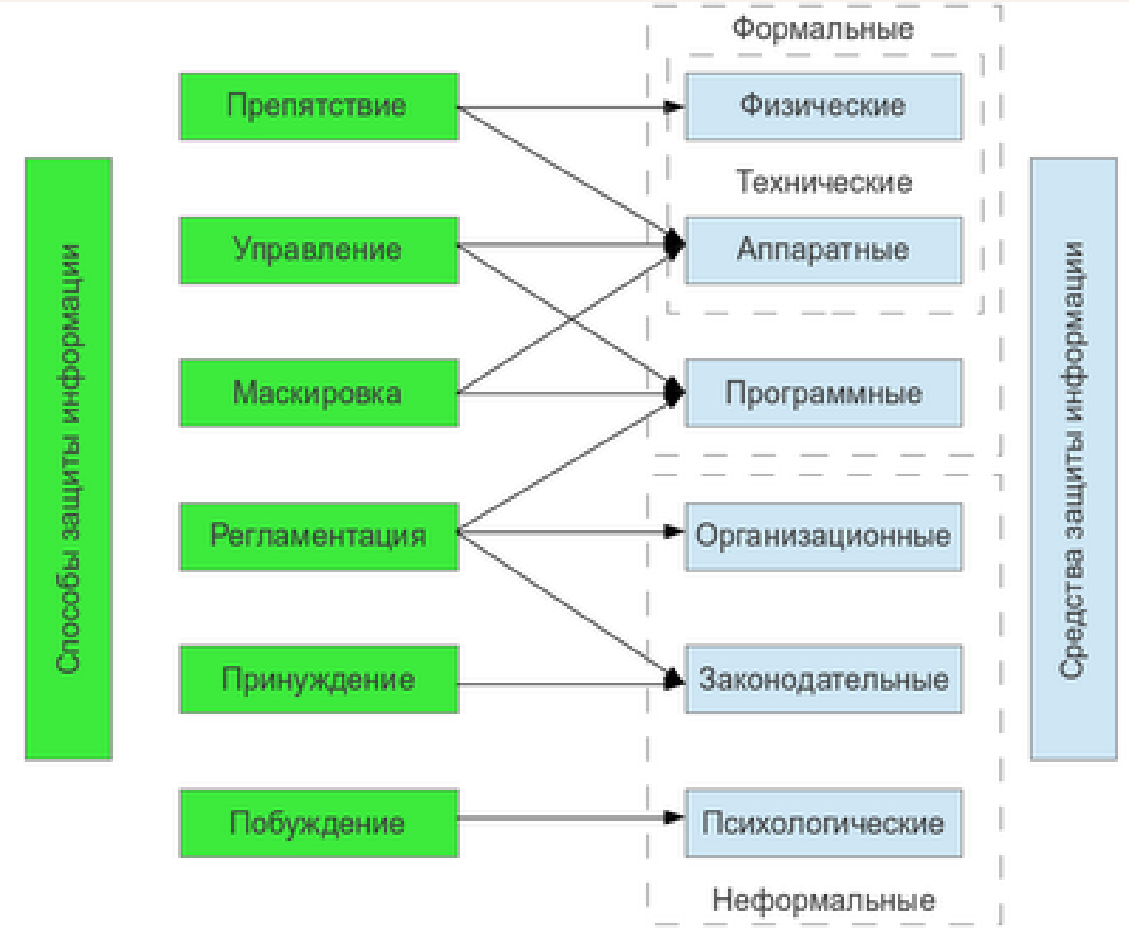
Международные стандарты:

- ISO/IEC 17799:2005 — «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности».
- ISO/IEC 27000 — Словарь и определения.
- ISO/IEC 27001 — «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования».

Государственные стандарты РФ:

- ГОСТ Р 50922-2006 — Защита информации. Основные термины и определения.
- Р 50.1.053-2005 — Информационные технологии. Основные термины и определения в области технической защиты информации.
- ГОСТ Р 51188—98 — Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство.
- ГОСТ Р 51275-2006 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
- ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

Классификация методов и средств защиты информации



Способы (методы) защиты информации

:

- Препятствие - создание на пути угрозы преграды, преодоление которой сопряжено с возникновением сложностей для злоумышленника или дестабилизирующего фактора.
- Управление - оказание управляющих воздействий на элементы защищаемой системы.
- Маскировка - действия над защищаемой системой или информацией, приводящие к такому их преобразованию, которое делает их недоступными для злоумышленника.
- Регламентация - разработка и реализация комплекса мероприятий, создающих такие условия обработки информации, которые затрудняют воздействия дестабилизирующих факторов.
- Принуждение - создание условий, при которых персонал вынужден соблюдать условия обработки информации под угрозой ответственности
- Побуждение - создание условий, при которых персонал соблюдают условия обработки информации по морально-этическим и психологическим соображениям.

Средства защиты информации

:

- Физические средства - механические, электрические, электромеханические, электронные, электронно-механические и т. п. устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.
- Аппаратные средства - различные электронные и электронно-механические и т.п. устройства, схемно встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации.
- Программные средства - специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения с целью решения задач защиты информации.
- Организационные средства - организационно-технические мероприятия, специально предусматриваемые в технологии функционирования системы с целью решения задач защиты информации.
- Законодательные средства - нормативно-правовые акты, регламентирующие права и обязанности по защите информации
- Психологические - моральные нормы или этические правила, соблюдение которых способствует защите информации

Государственные органы РФ, контролирующие деятельность в области защиты информации:

:

- Комитет Государственной думы по безопасности;
- Совет безопасности России;
- Федеральная служба по техническому и экспортному контролю
- Федеральная служба безопасности Российской Федерации
- Федеральная служба охраны Российской Федерации
- Служба внешней разведки Российской Федерации
- Министерство обороны Российской Федерации
- Министерство внутренних дел Российской Федерации
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

Организационная защита объектов информатизации

Организационная защита:

- это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз

основные организационные мероприятия:

- организацию режима и охраны
- организацию работы с сотрудниками
- организацию работы с документами и документированной информацией
- организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;
- организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;
- организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учёта, хранения и уничтожения документов и технических носителей.

Исторические аспекты информационных систем

Этапы:

1. этап - до 1916 года - защита личных сведений человека или сообщества
2. этап - начиная с 1916 года - обеспечение скрытности и помехозащищённости радиосвязи
3. этап - начиная с 1935 года - повышение защищённости радиолокационных средств
4. этап - начиная с 1946 года - ограничение физического доступа к электронно-вычислительным машинам (компьютерам)
5. этап - начиная с 1965 года - физическая защита локальных информационно-коммуникационных сетей
6. этап - начиная с 1973 года - обеспечение информационной безопасности в компьютерных системах с беспроводными сетями передачи данных
7. этап - начиная с 1985 года - обеспечение информационной безопасности глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения.