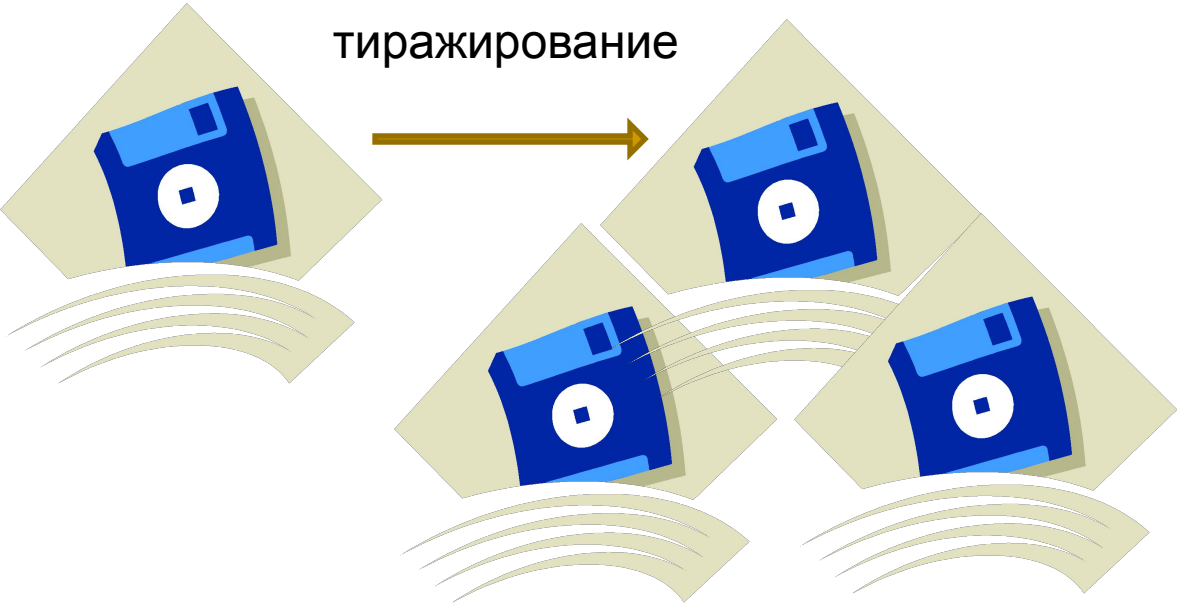
Правовые и этические нормы информационной деятельности человека

Правовое регулирование

Вечная проблема - защита информации. На различных этапах своего развития человечество решало эту проблему с присущей для данной эпохи характерностью. Главная тенденция, характеризующая развитие современных информационных технологий - рост числа компьютерных преступлений и связанных с ними хищений конфиденциальной и иной информации, а также материальных потерь.

Правовое регулирование



Информация – материальный продукт?

Информация = дом = мебель?

Информационный продукт = право собственности

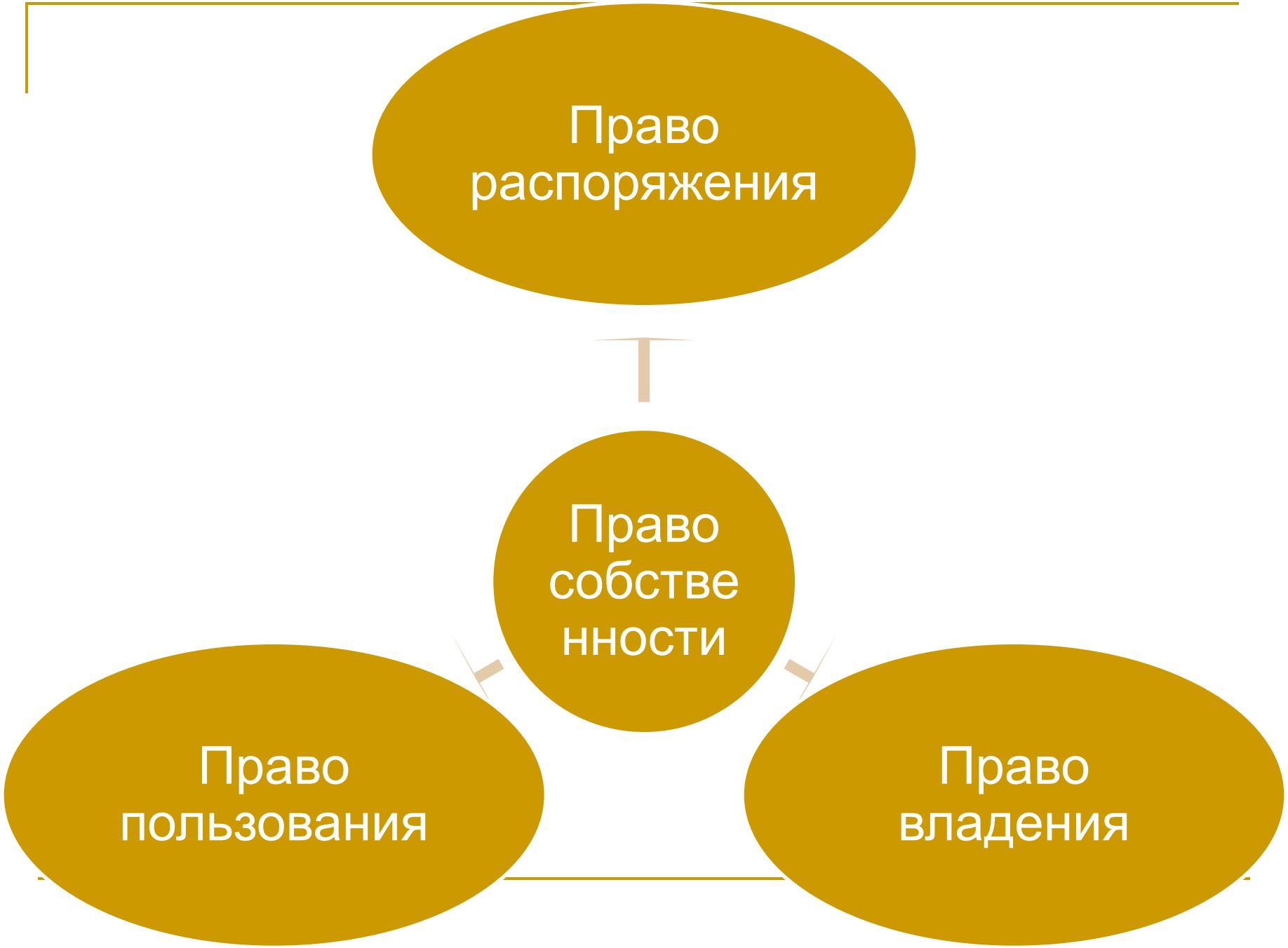
Закон «О правовой охране программ для ЭВМ и баз данных»

Дал юридически точное определение понятий, связанных с авторством и распространением компьютерных программ и баз данных.

Он определил, что *авторское право* распространяется на указанные объекты, являющиеся результатом творческой деятельности автора.

Закон «Об информации, информатизации и защите информации»

законом "Об информации, информатизации и защите информации" определено, что информационные ресурсы являясь объектом отношений физических, юридических лиц и государства, подлежат обязательному учету и защите, как всякое материальное имущество собственника. При этом собственнику предоставляется право самостоятельно в пределах своей компетенции устанавливать режим защиты информационных ресурсов и доступа к ним.


Право распоряжения
Право собственности
Право пользования
Право владения

Право собственности регулируется и охраняется государственной инфраструктурой:

Законы → Суд → Наказание

Знак охраны авторского права

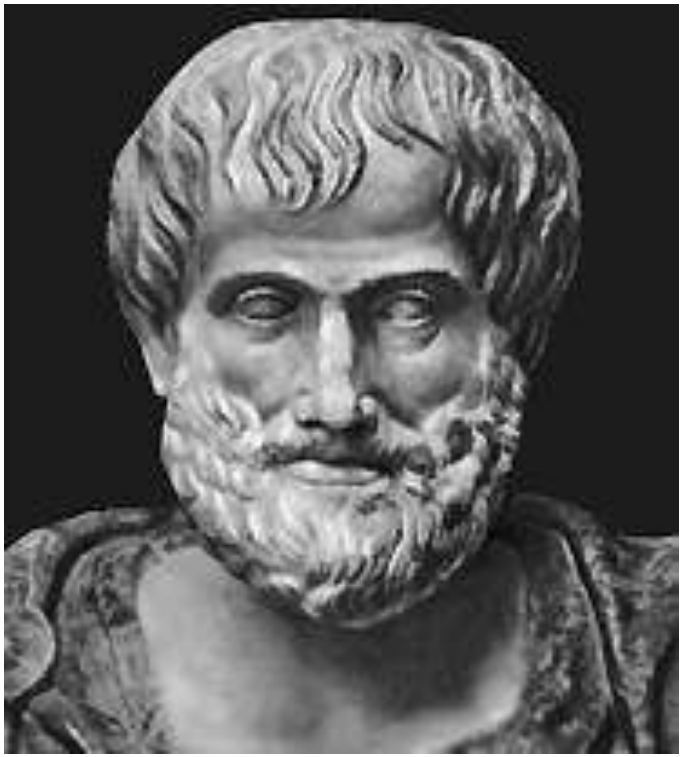
1. ©
2. Имя правообладателя
3. Год первого выпуска программы в свет

В 1996 году в уголовный кодекс был впервые внесен раздел «Преступления в сфере компьютерной информации». Он определил меру наказания за некоторые виды преступлений, ставших, к сожалению, распространенными:

- неправомерный доступ к компьютерной информации;
- создание, использование и распространение вредоносных программ для ЭВМ;
- умышленное нарушение правил эксплуатации ЭВМ и их сетей.

.

Этические нормы



ЭТИКА (греч. ethika, от ethos — обычай, нрав, характер), философская дисциплина, изучающая мораль, нравственность. Как обозначение особой области исследования термин впервые употребляется Аристотелем.

Определение:

Этика – это учение о нравственности, о правилах и нормах поведения людей, об их обязанностях по отношению друг к другу, к обществу, государству ит.п.

Информационная деятельность людей должна быть:

- Честной, точной, корректной
- Объективной в оценке и представлении информации
- Порядочной

Условия формирования этических норм – правовое обеспечение, стабильность власти, политическая и экономическая свобода.

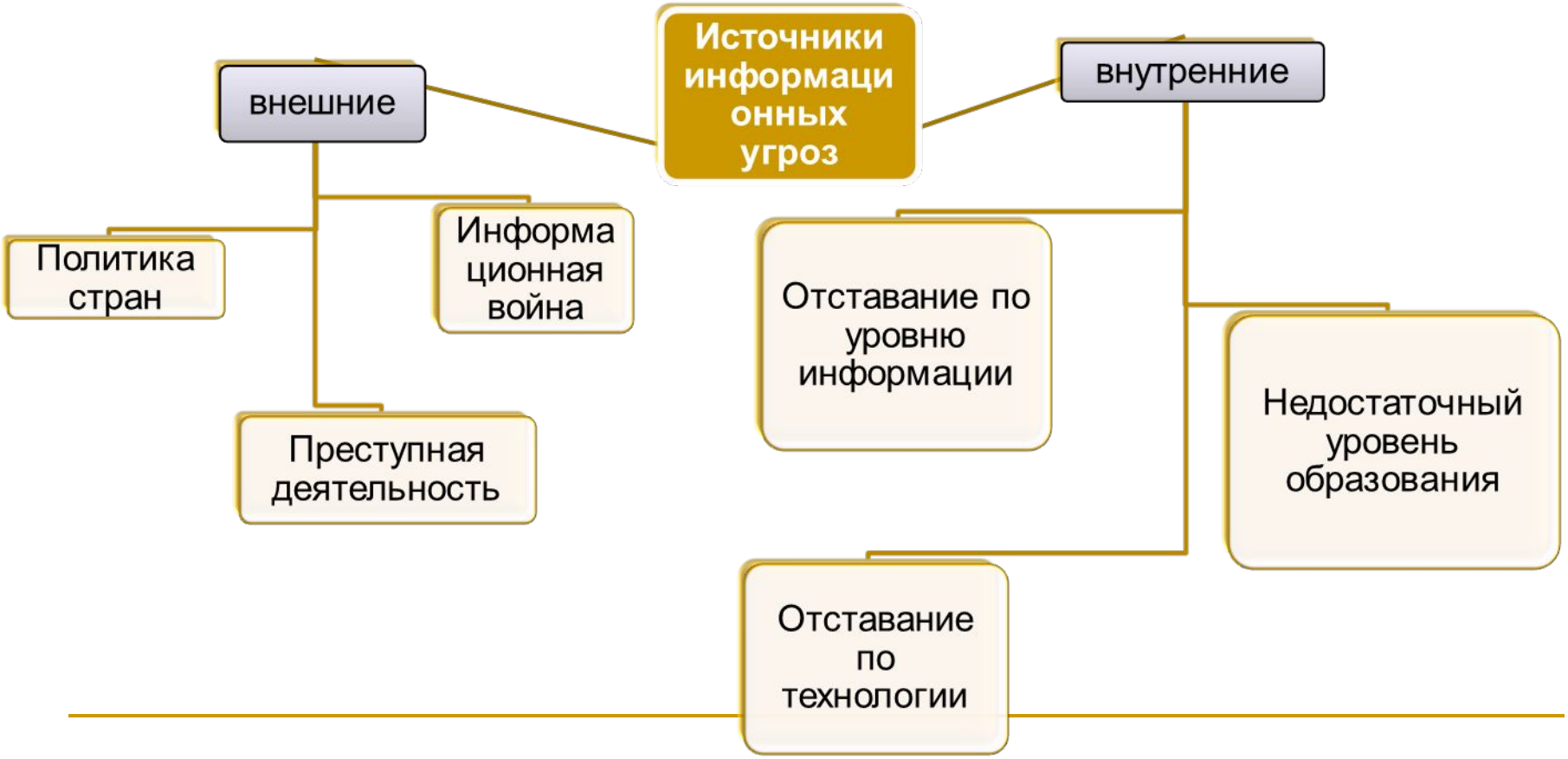
Основные цели и задачи информационной безопасности

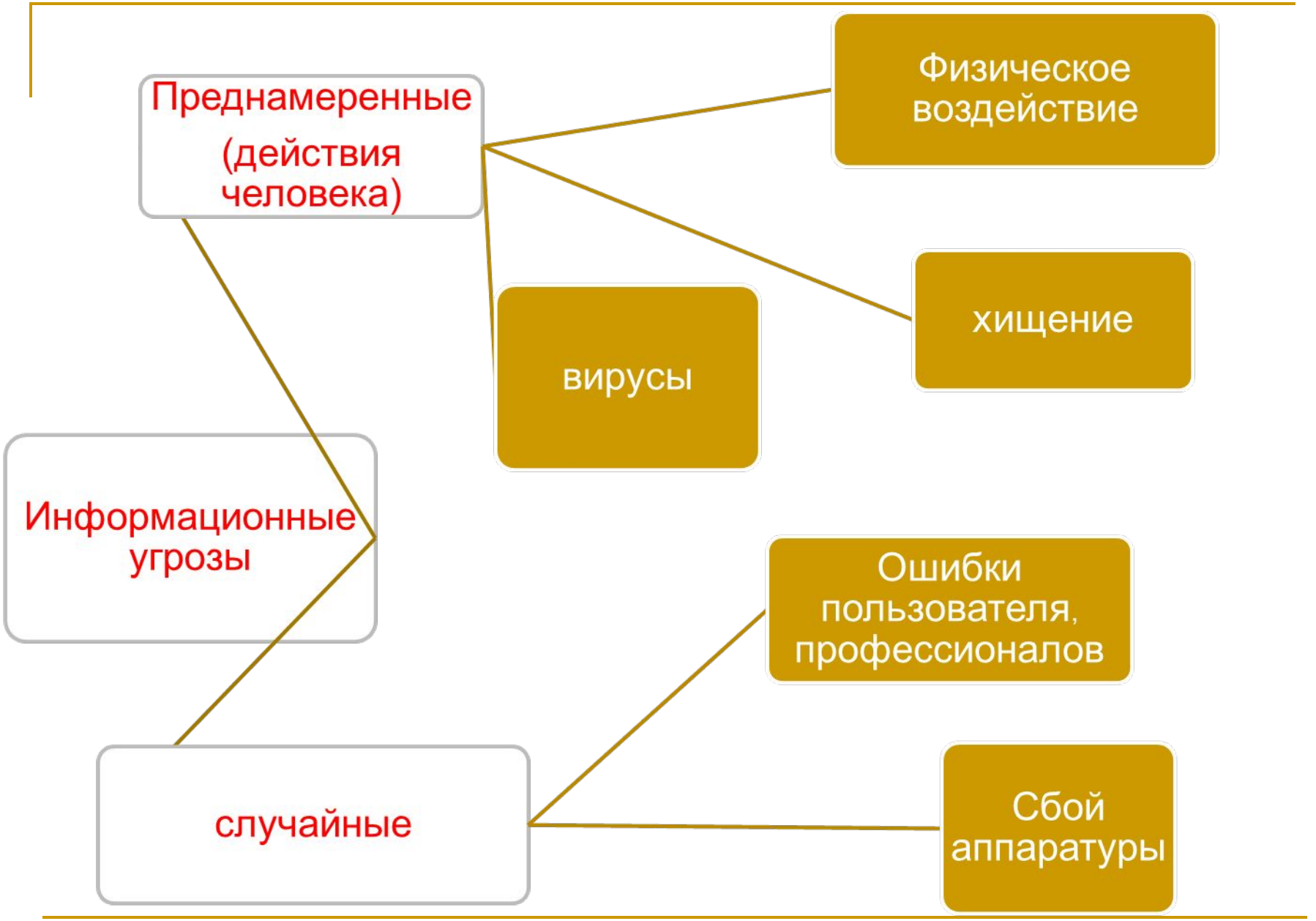
Информационная безопасность – совокупность мер по защите информационной среды общества и человека.

Цели ИБ :

1. Защита национальных интересов
2. Обеспечение общества достоверной информацией
3. Правовая защита человека и общества при получении, распространении и использовании информации.

Что такое информационные угрозы и как они проявляются?




Преднамеренные (действия человека)
Физическое воздействие
вирусы
хищение
Информационные угрозы
случайные
Ошибки пользователя, профессионалов
Сбой аппаратуры

На сегодняшний день сформулированы базовые принципы информационной безопасности, задачами которых является обеспечение:

- *Целостности данных*
- *Конфиденциальности информации*
- *Доступа информации для авторизированных пользователей*

Информация может быть потеряна при передаче, хранении, обработки. Причины:

- Сбои в работе оборудования
- Инфицирование компьютерными вирусами
- Неправильное хранение архивных данных
- Несанкционированный доступ
- Некорректная работа

Виды защиты информации

- Средства физической защиты
- Программные средства(антивирусные средства, системы разграничения полномочий)
- Административные меры защиты (доступ в помещение, разработка стратегий безопасности)

Защита информации от случайного воздействия. Причины:

- Технические: вибрация, скачки напряжения, излучение от электроприборов
- Неисправности кабельной системы(обрыв или короткое замыкание)
- Кратковременное отключение питания

Защита информации от несанкционированного доступа

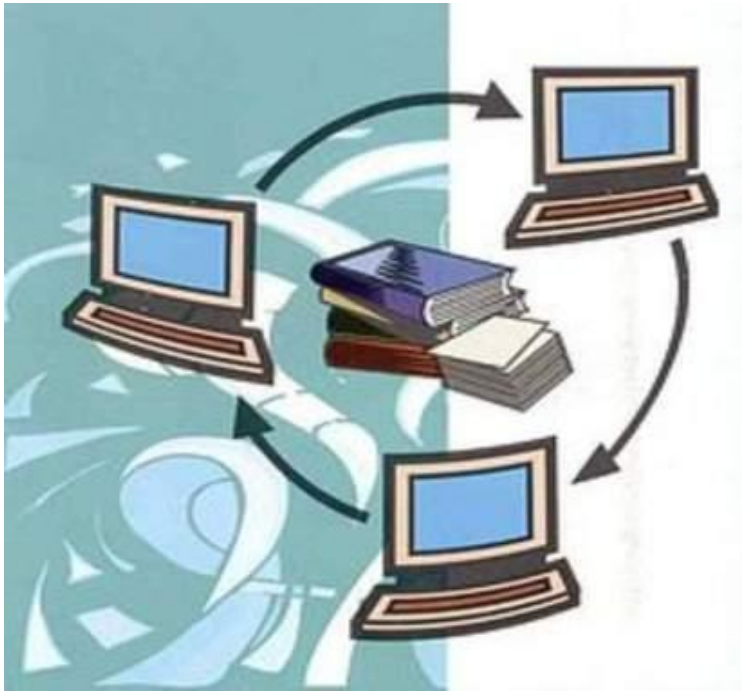
- Хакеры – особый вид IT специалистов, занимающихся взломом паролей, воровством и порчей информации.
- Основной инструмент – программа взломщик, делящая на 2 компонента: программа доступа к удаленным компьютерам по телефонным сетям и словарь вероятных кодов и паролей.

Стратегия защиты

- Шифрование информации
- Установка системы паролей

Защита от несанкционированного копирования включает:

- Защиту сообщений от авторских правах разработчика, выводимой программой на экран или находящихся внутри программы
- Защиту от модификаций программы
- Собственно защиту от незаконного тиражирования программы тем или иным способом.



Виды защиты информации от копирования

- Защита с помощью серийного номера
- Использование технических отличий в машине для программной защиты
- Использование программно – аппаратной защиты

Какие существуют методы защиты информации?

- Ограничение доступа к информации: уровень среды обитания человека (сигнализации, видеонаблюдение), уровень защиты ПК (пароль на ПК)
- Шифрование с помощью специальных алгоритмов
- Контроль доступа к аппаратуре (установка датчиков)
- Законодательные меры.

Система защиты – совокупность средств и технических приемов, обеспечивающих защиту компонентов компьютера, способствующих минимизации риска, которому могут быть подвержены его ресурсы и пользователи.

Существуют различные механизмы безопасности:

- не разглашение паролей доступа в систему;
- шифрование;
- контроль доступа;
- обеспечение целостности данных (архивирование с паролем);
- использование паролей при сохранении документов.

Шифрование используется для реализации службы засекречивания и используется в ряде различных служб. Шифрование бывает симметричным и асимметричным. *Симметричное* основывается на использовании одного и того же секретного ключа для шифрования и дешифрования. *Асимметричное* характеризуется тем, что для шифрования используется один ключ, являющийся общедоступным, а для дешифрования – другой, являющийся секретным.

Цифровая подпись основывается на алгоритмах асимметричного шифрования и включает две процедуры: формирование подписи отправителем и ее распознавание (верификацию) получателем.

Контроль доступа осуществляет проверку полномочий объектов сети (программ и пользователей) на доступ к ее ресурсам.

Обеспечение целостности данных основывается на выполнении взаимосвязанных процедур шифрования и дешифрования отправителем и получателем с последующим сравнением контрольных криптографических сумм.

Механизмы аутентификации обеспечиают одностороннюю и взаимную аутентификацию. На практике эти механизмы совмещаются с шифрованием, цифровой подписью и арбитражем.