Информационная безопасность

Информационная безопасность –

совокупность мер по защите информационной среды общества и человека

Информационные угрозы

Случайные:

Ошибки пользователя

Ошибки в програмировании

Отказ, сбой аппаратуры

Форс-мажорные обстоятельства

Преднамеренные:

Хищение информации

Компьютерные вирусы

Физическое воздействие
на аппаратуру

Каналы, по которым можно осуществить хищение, изменение или уничтожение информации:

Через человека:

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

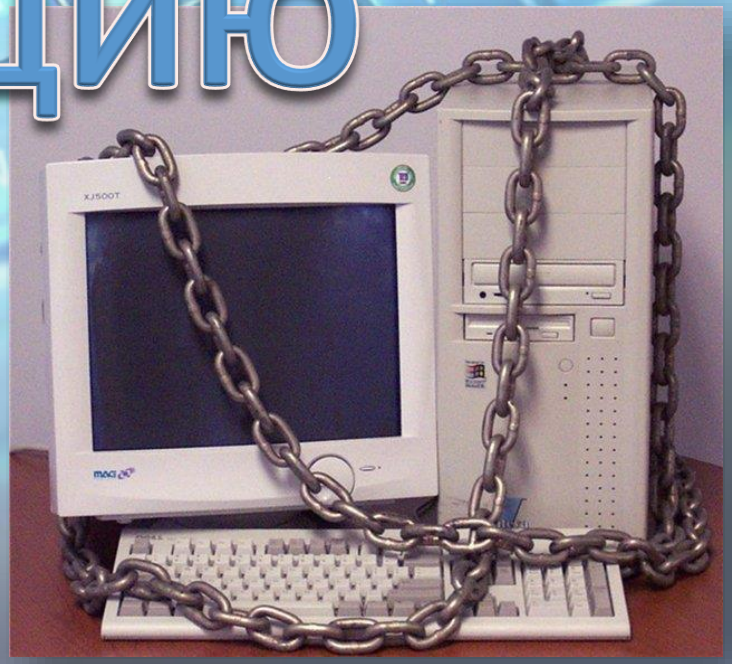
Через программу:

- 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

КАК МОЖНО СОХРАНИТЬ ИНФОРМАЦИЮ ?



СОБЛЮДЕНИЕ РЕЖИМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:

- **законодательный уровень:** законы, нормативные акты, стандарты и т.п.
- **морально-этический уровень:** нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации;
- **административный уровень:** действия общего характера, предпринимаемые руководством организации;
- **физический уровень:** механические, электро- и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей;
- **аппаратно-программный уровень:** электронные устройства и специальные программы защиты информации.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ при использовании программного обеспечения сторонних разработчиков:

commercial software

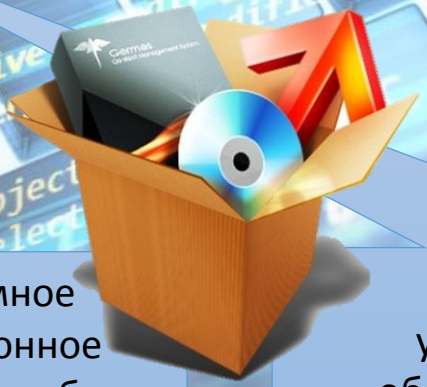
коммерческое программное обеспечение, созданное с целью получения прибыли от его использования другими

demoware или trialware

демонстрационная версия коммерческого программного обеспечения (demoware или trialware), распространяемая бесплатно, но имеющая определенные ограничения функциональности, по сравнению с основной версией

shareware

freeware



бесплатное программное обеспечение, лицензионное соглашение которого не требует каких-либо выплат правообладателю

условно-бесплатное программное обеспечение, использование которого связано с выполнением каких-то условий

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ при использовании программного обеспечения сторонних разработчиков:

- при установке программы необходимо внимательно ознакомиться с содержанием лицензионного соглашением и строго выполнять его;

- не пользоваться «пиратскими» способами преобразования платных программ в бесплатные;

- устанавливать бесплатное (freeware) программное обеспечение, полученное только от надежных источников;

- своевременно производить обновление установленного программного обеспечения.

Во время работы с информацией в сети ИНТЕРНЕТ остерегайтесь:

- веб-сайтов, собирающих или предоставляющих информацию о вас;
- провайдеров интернет-служб или работодателей, отслеживающих посещенные вами страницы;
- вредоносных программ, отслеживающих нажатия клавиш;
- сбора данных скрытыми клиентскими приложениями;
- «скаченной» информации не прошедшей проверку антивирусной программой.

ПОМНИТЕ!

ВАША ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЗАВИСИТ ТОЛЬКО ОТ ВАС!

Контрольные вопросы:

1. Что означает термин «информационная безопасность»?
2. Какие бывают информационные угрозы?
3. Назовите каналы, по которым может осуществляться хищение, изменение, уничтожение информации.
4. По каким направлениям проводятся мероприятия, направленные на соблюдение режима информационной безопасности?
5. Что нужно знать при инсталляции (установке) нового программного обеспечения на компьютер?
6. С какими опасностями можно встретиться во время работы в сети интернет?