Лекция 5. Основные виды и источники атак на информацию

Характерные особенности компьютерных систем – как объекта воздействия угроз безопасности

- **аппаратные средства**
- **программное обеспечение**
- **данные**
- **персонал**

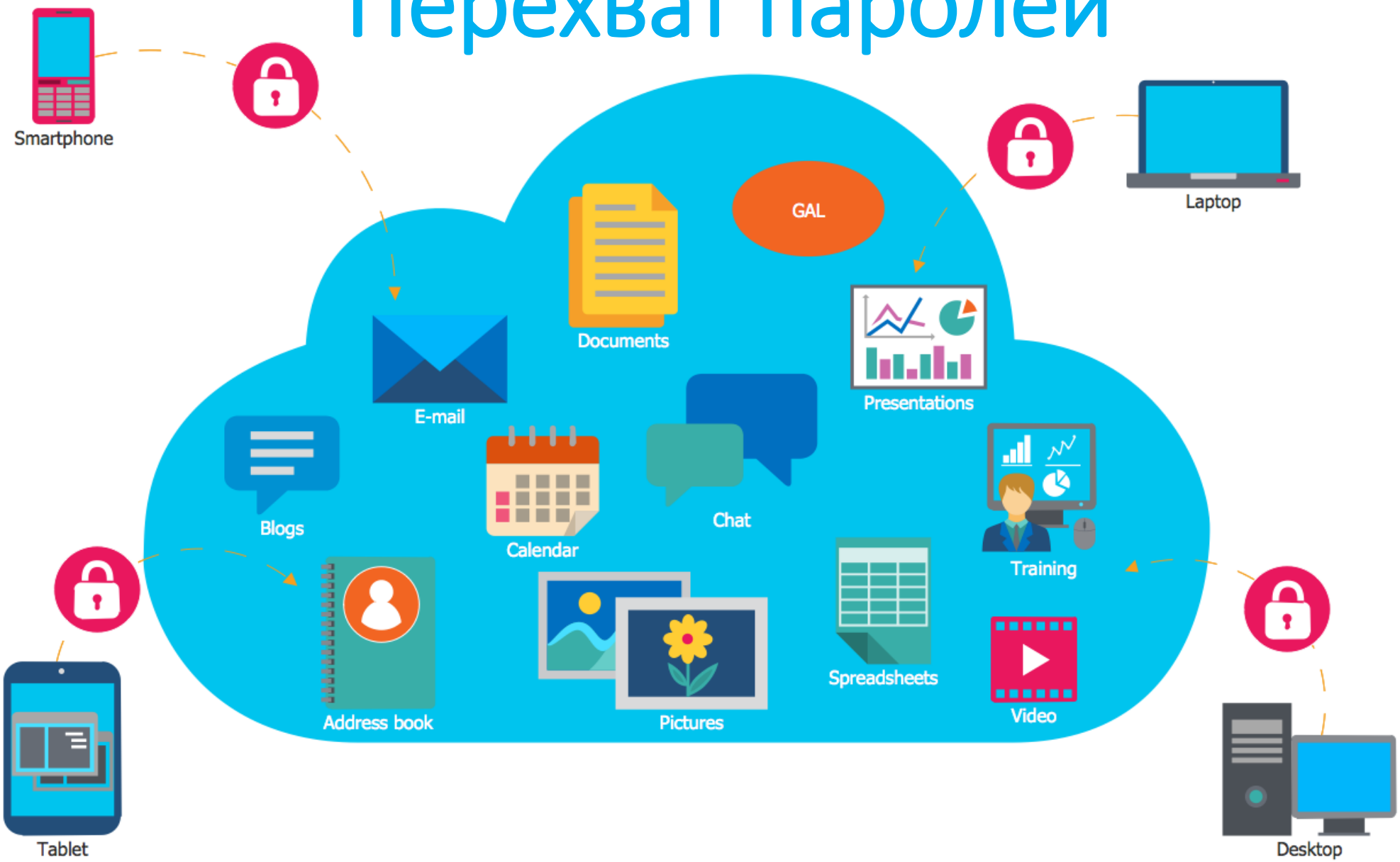
К основным каналам НСДИ

перехват паролей;

«маскарад»;

незаконное использование привилегий.

Перехват паролей



Маскарад

Незаконное использование привилегий

Особой характерной особенностью

Вторжении в компьютерную сеть злоумышленника

При пассивном вторжении

При активном вторжении

Пути и последствия реализации угроз информационной безопасности

нарушение физической целостности

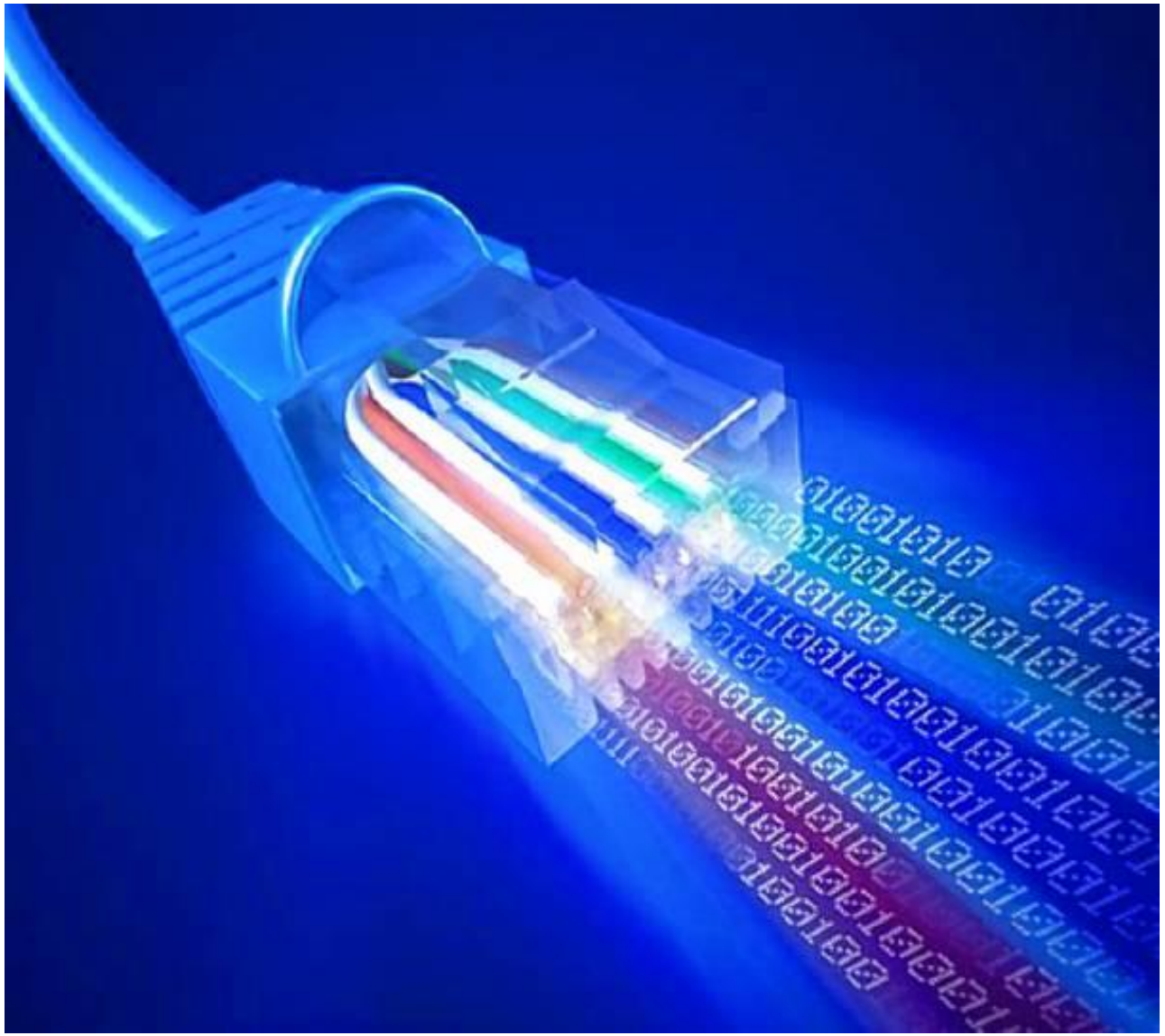
несанкционированная модификация

несанкционированное получение

несанкционированное размножение

Пути реализации угроз безопасности для компьютерных систем

№	Объекты воздействия	Нарушение конфиденциальности информации	Нарушение целостности информации	Нарушение работоспособности системы
1	Аппаратные средства	Несанкционированное подключение; Использование ресурсов; Хищение носителей.	Несанкционированное подключение; Использование ресурсов; Модификация; Изменение режимов.	Несанкционированное изменение режимов; Вывод из строя; Разрушение.
2	Программное обеспечение	Несанкционированное копирование; Хищение; Перехват.	Несанкционированный доступ; Внедрение «троянского коня», «вирусов», «червей».	Несанкционированное искажение; Удаление; Подмена.
3	Данные	Несанкционированное копирование; Хищение; Перехват.	Несанкционированное искажение; Модификация.	Несанкционированное искажение; Удаление; Подмена.
4	Персонал	Разглашение; Передача сведений о системе защиты информации; Халатность.	«Маскарад»; Вербовка; Подкуп персонала.	Уход с рабочего места; Физическое устранение.

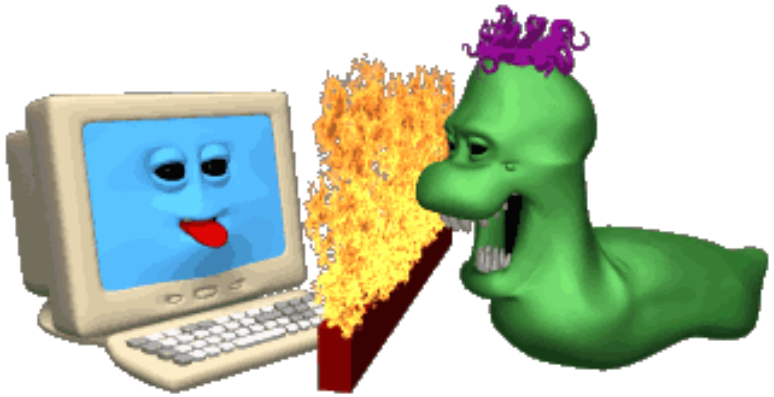


Если объектом воздействия являются аппаратные средства

При воздействии на программное обеспечение

Если в качестве объекта воздействия выступают данные

Воздействия на обслуживающий персонал



Троянский конь

Троянский конь

Уничтожение информации. Выбор объектов и способов уничтожения определяется фантазией автора вредоносной программы.

Перехват и передача информации. В частности, известна программа, осуществляющая перехват паролей, набираемых на клавиатуре.

Целенаправленная модификация текста программы, реализующей функции безопасности и защиты системы.

Компьютерный вирус

Сетевой червь

«червь»
World Wide
Web Worm

“червь”
Морриса

Сетевой червь

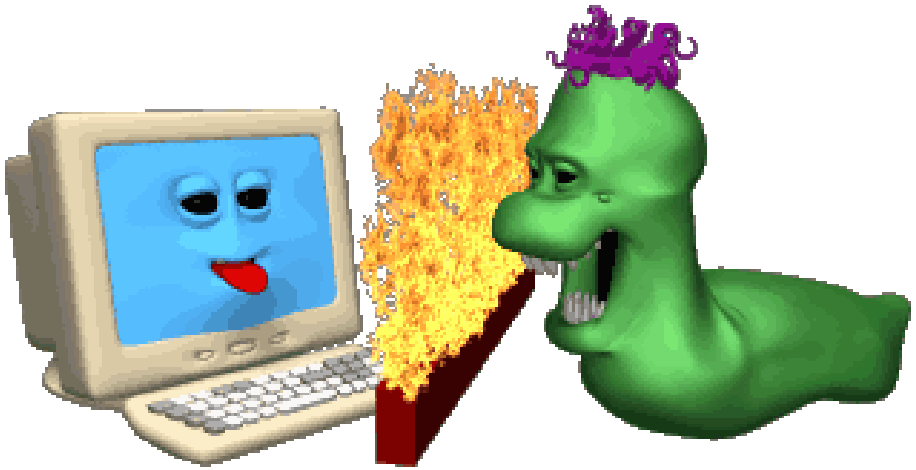
исключение несанкционированного доступа к исполняемым файлам;

тестирование приобретаемых программных средств;

контроль целостности исполняемых файлов и системных областей;

создание замкнутой среды исполнения программ.

Обеспечение информационной безопасности КС



Фрагментарный подход

Комплексный подход

- правовые (законодательные);
- морально-этические;
- административные;
- физические;
- аппаратно-программные;
- технологические.

Первый рубеж защиты

Второй рубеж защиты

Третий рубеж защиты

- процессы функционирования КС;
- использование всех ресурсов систем;
- деятельность персонала;
- порядок взаимодействия пользователей с системами

Административные меры

1	2	3	4	5	6	7	8

Четвертый рубеж защиты

Механические

Электрические

электронные устройства и сооружения

Пятый рубеж защиты

идентификацию (распознавание) и аутентификацию (проверка подлинности) субъектов системы;

разграничение доступа к ресурсам КС;

контроль целостности информации;

обеспечение конфиденциальности информации;

регистрацию и анализ событий, происходящих в системах;

резервирование ресурсов и компонентов КС;

Шестой и заключительный рубеж

создание архивных копий носителей информации;

ручное или автоматическое сохранение обрабатываемых файлов во внешней памяти систем;

регистрация пользователей КС в специальных журналах;

автоматическая регистрация доступа пользователей к тем или иным ресурсам;

разработка специальных инструкций по выполнению всех технологических процедур и процессов.

Спасибо за внимание