ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

ВОПРОСЫ

1. **Понятие и основные виды угроз информационной безопасности.**

2. **Защита информации.**

3. **Компьютерные вирусы и антивирусные программные средства.**

Вопрос 1. Понятие и основные виды угроз информационной безопасности

Информация является ценным продуктом человеческой деятельности, поэтому обеспечение ее защиты является одной из важных задач.

ВИДЫ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

(в зависимости от доступа)

общедоступная информация	информация ограниченного доступа
используется любыми лицами при соблюдении ограничений, установленных федеральными законами	государственная, коммерческая, банковская, врачебная тайны, персональные данные и другие

Угрозам подвергаются, в первую очередь, такие свойства информации как:

- конфиденциальность,
- целостность,
- доступность.

- **Конфиденциальность** – свойство, указывающее на необходимость введения ограничения доступа к информации для определенного круга лиц.

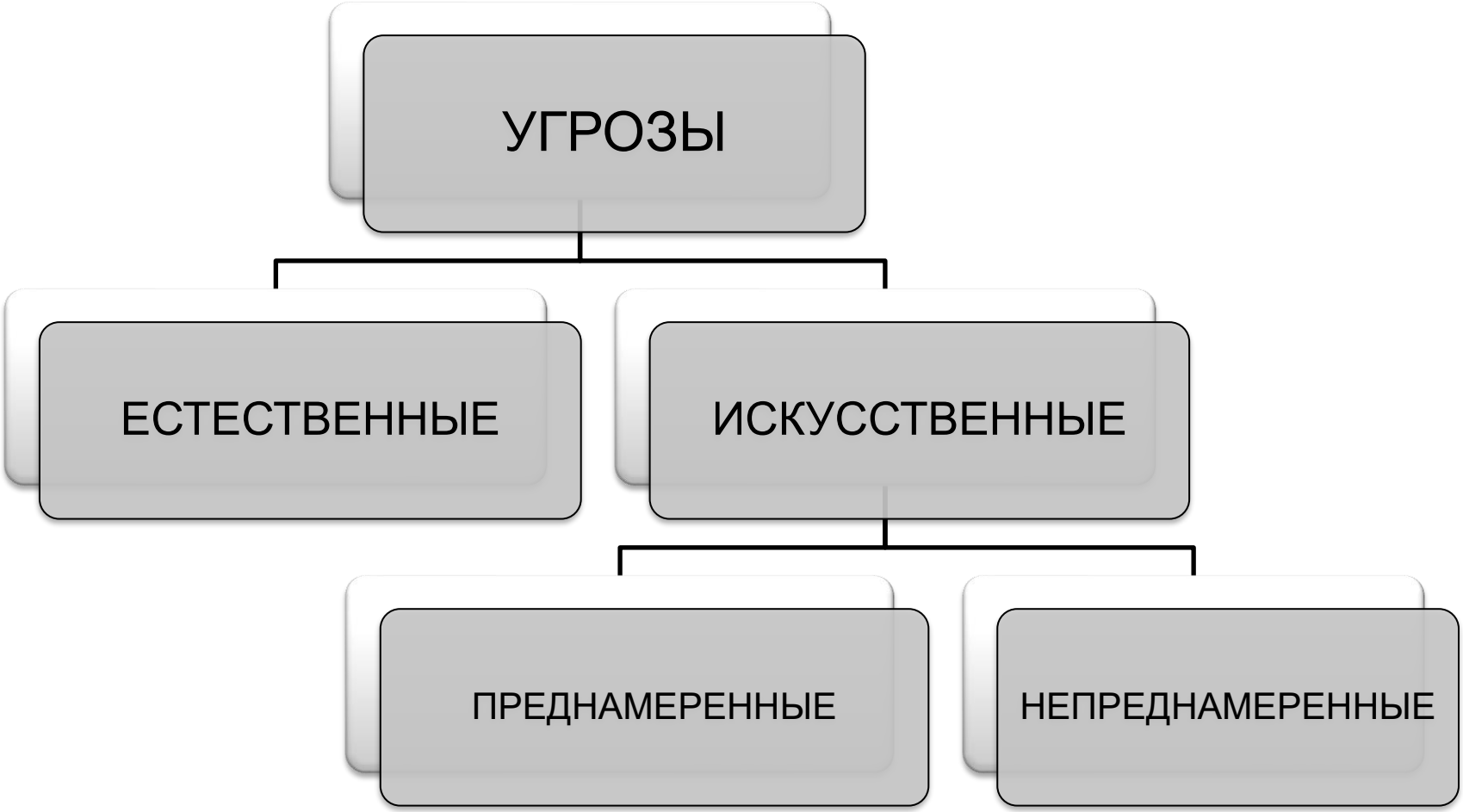
- **Целостность** – свойство информации сохранять свою структуру и содержание в неискаженном виде по отношению к некоторому фиксированному состоянию в процессе передачи и хранения.

- **Доступность** – свойство информации, характеризующее способность обеспечивать своевременный и беспрепятственный доступ пользователей к необходимой информации.

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или) целостности информации.

КЛАССИФИКАЦИЯ УГРОЗ

по методам воздействия на информацию:



Естественные угрозы – это угрозы, вызванные воздействиями объективных физических процессов или стихийных природных явлений, *независящих от человека*.

В зависимости от источников естественные угрозы делятся на:

- ***природные*** (стихийные бедствия, магнитные бури и т. п.)
- ***технические*** (сбои, отказы оборудования).

Искусственные угрозы – это угрозы, вызванные деятельностью человека.

Среди искусственных угроз можно выделить:

- ***непреднамеренные*** (совершенные по незнанию, без злого умысла) угрозы, вызванные ошибками в проектировании компьютерной системы и ее элементов, ошибками в ПО, ошибками в действиях персонала и т.п.;

- ***преднамеренные*** (умышленные) угрозы, связанные с корыстными устремлениями людей.

Компьютерные преступления - это предусмотренные уголовным законодательством общественно опасные действия, в которых объектом или средством преступного посягательства является компьютерная информация.


Компьютерные преступления
связанные с вмешательством в работу компьютеров
использующие компьютеры как необходимые технические средства
несанкционированный доступ к информации
разработка и распространение компьютерных вирусов
преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов
подделка информации
хищение информации
разработка математических моделей организации преступления

УК РФ Глава 28. «ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

Статья 272. Неправомерный доступ к компьютерной информации.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

УК РФ Глава 19 «Преступления против конституционных прав и свобод человека и гражданина»

(уголовное преследование за незаконные действия с общедоступной информацией)

Статья 146 «Нарушение авторских и смежных прав».

Статья 147 «Нарушение изобретательских и патентных прав».

2. ЗАЩИТА ИНФОРМАЦИИ

Согласно **ФЗ** «**Об информации, информационных технологиях и о защите информации**»:

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных :

1) на обеспечение защиты информации от неправомерного доступа, уничтожения, модификации, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2) на соблюдение конфиденциальности информации ограниченного доступа;
3) на реализацию права на доступ к информации.

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

МЕТОДЫ

- препятствие
- управление доступом
- маскировка
- регламентация
- принуждение
- побуждение

СРЕДСТВА

- технические
- программные
- организационные
- законодательные
- морально-этические

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

1. **Препятствие** – метод физического преграждения пути злоумышленнику к защищаемой информации.

2. **Управление доступом** – метод защиты информации за счет регулирования использования всех информационных ресурсов.

Управление доступом включает следующие функции защиты:

- ***идентификацию***, т.е. присвоение объекту или лицу уникального идентификатора, а также процесс ввода имени при входе в информационную систему;
- ***аутентификацию*** – установление подлинности объекта по предъявленному им идентификатору;
- ***проверку полномочий***, устанавливающую, дано ли лицу, и в какой мере, право обращаться к защищенному ресурсу;
- ***регистрацию*** (протоколирование) обращений к защищаемым ресурсам;
- ***реагирование*** (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

3. Маскировка — метод защиты информации путем ее криптографического закрытия.

Основными видами криптографического закрытия являются *шифрование* и *кодирование* защищаемых данных.

4. Регламентация – метод защиты, создающий такие условия обработки, хранения и передачи информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

5. **Принуждение** – метод защиты, при котором пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

6. **Побуждение** – метод защиты, который побуждает пользователя и персонал системы не нарушать установленный порядок за счет соблюдения моральных и этических норм.

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

1.Технические средства – реализуются в виде различных устройств.

Технические средства

Физические
(автономные устройства и системы)

электронно-механическое оборудование охранной сигнализации и наблюдения, замки на дверях, решетки на окнах и т.п.

Аппаратные
(устройства, встраиваемые в аппаратуру либо сопряженные с аппаратурой)

устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации

2. **Программные средства** – программы для выполнения функций, связанных с защитой информации.

3. **Организационные средства** –организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации систем обработки данных для обеспечения защиты информации.

4. Законодательные средства – законодательные акты страны, которыми регламентируются правила использования и обработки информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

5. Морально-этические средства – всевозможные нормы, которые сложились традиционно или складываются по мере распространения вычислительных средств в стране или обществе.

3. КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММНЫЕ СРЕДСТВА

Компьютерный вирус – программа, способная без ведома пользователя, самопроизвольно приписывать себя к файлам и распространяться, нарушая работоспособность программного обеспечения ЭВМ.

ПРИЗНАКИ ПОЯВЛЕНИЯ ВИРУСА

- замедление работы компьютера;
- невозможность загрузки операционной системы;
- частые «зависания» и сбои в работе компьютера;
- прекращение работы или неправильная работа программ;
- увеличение количества файлов на диске;
- изменение размеров файлов;
- периодическое появление на экране монитора посторонних сообщений;
- уменьшение объема свободной оперативной памяти;
- изменение даты и времени создания файлов;
- разрушение файловой структуры (исчезновение файлов, искажение каталогов и др.)


КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ
СРЕДА ОБИТАНИЯ
СТЕПЕНЬ ВОЗДЕЙСТВИЯ НА РЕСУРСЫ
СПОСОБ ЗАРАЖЕНИЯ СРЕДЫ ОБИТАНИЯ
АЛГОРИТМИЧЕСКАЯ ОСОБЕННОСТЬ

ПО СРЕДЕ ОБИТАНИЯ

вирусы делятся на:

- ***загрузочные*** – внедряются в загрузочный сектор диска;
- ***файловые*** – внедряются в основном в исполняемые файлы с расширением .com и .exe;
- ***системные*** – проникают в системные модули и драйверы периферийных устройств;
- ***сетевые*** – обитают в компьютерных сетях;
- ***файлово-загрузочные*** – поражают загрузочные секторы дисков и файлы прикладных программ.

ПО СТЕПЕНИ ВОЗДЕЙСТВИЯ НА РЕСУРСЫ

вирусы подразделяются на:

- **безвредные**
- **неопасные**
- **опасные**
- **разрушительные**

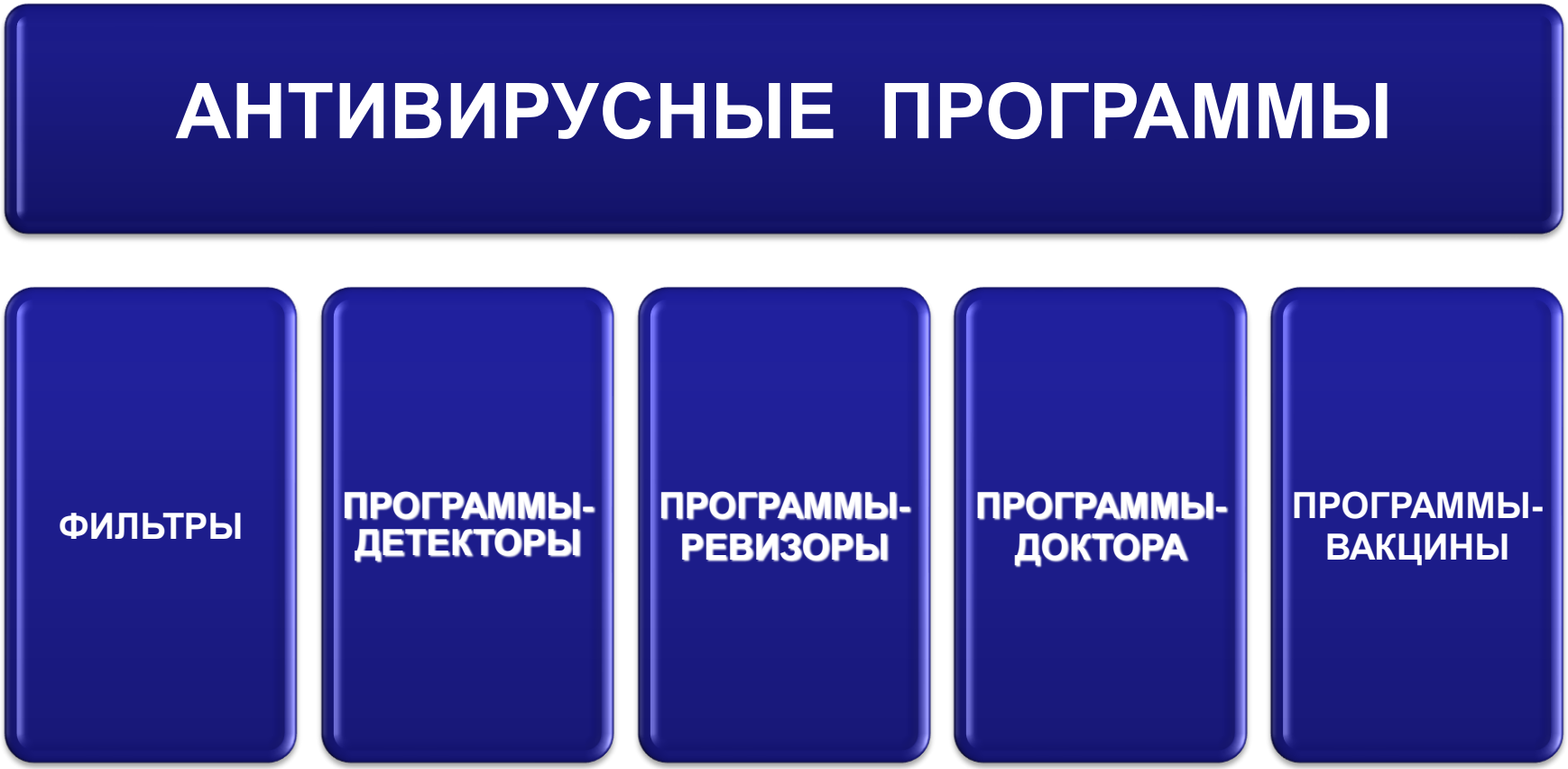
ПО СПОСОБУ ЗАРАЖЕНИЯ СРЕДЫ ОБИТАНИЯ

- ***резидентные вирусы:*** вирус создает свою копию («резидентную копию») в оперативной памяти и заражает все открываемые пользователем файлы. Резидентные вирусы способны «жить» даже после закрытия зараженной программы.
- ***нерезидентные вирусы*** не заражают оперативную память и являются активными ограниченное время.

ПО АЛГОРИТМИЧЕСКОЙ ОСОБЕННОСТИ

- ***Репликаторные программы*** приводят к переполнению основной памяти.
- ***«Троянский конь»*** - программа, которая, маскируясь под полезную программу, выполняет дополнительные функции, о чем пользователь не догадывается.
- ***Логическая бомба*** – используется в основном для разрушения или искажения информации. Начинает действовать при наступлении определенных условий.
- ***Захватчик паролей*** — программы, предназначенные для хищения паролей.
- ***Шифровальщики*** — программы, которые, получив доступ к жесткому диску компьютера, шифруют всю содержащуюся на нем информацию ключом, неизвестным пользователю, с целью последующего шантажа.

Классификация антивирусных программ



ПРОГРАММЫ-ФИЛЬТРЫ

постоянно находятся в оперативной памяти и перехватывают все запросы к операционной системе на выполнение подозрительных действий.

Такими действиями могут быть попытки изменения атрибутов файлов, коррекции исполняемых файлов, записи в загрузочные секторы диска и др.

ПРОГРАММЫ-ДЕТЕКТОРЫ

позволяют обнаруживать файлы, зараженные одним или несколькими известными вирусами.

ПРОГРАММЫ-РЕВИЗОРЫ

запоминают исходное состояние программ, а затем периодически сравнивают текущее состояние с исходным.

При выявлении несоответствий сообщение об этом выдается пользователю.

ПРОГРАММЫ-ДОКТОРА

не только обнаруживают, но и «лечат» зараженные программы или диски, «выкусывая» из зараженных программ тело вируса.

ПРОГРАММЫ-ВАКЦИНЫ

модифицируют программы и диски таким образом, что вирус, от которого производится вакцинация, считает их уже зараженными и не внедряется в них.

В основе работы большинства антивирусных программ лежит принцип поиска сигнатуры вирусов.

Вирусная сигнатура – некоторая уникальная характеристика вирусной программы, которая выдает присутствие вируса в компьютерной системе.

В антивирусные программы входит периодически обновляемая база данных сигнатур вирусов.

Антивирусная программа просматривает компьютерную систему, проводит сравнение и отыскивает соответствие с сигнатурами в базе данных. Пытается вычистить обнаруженный вирус.