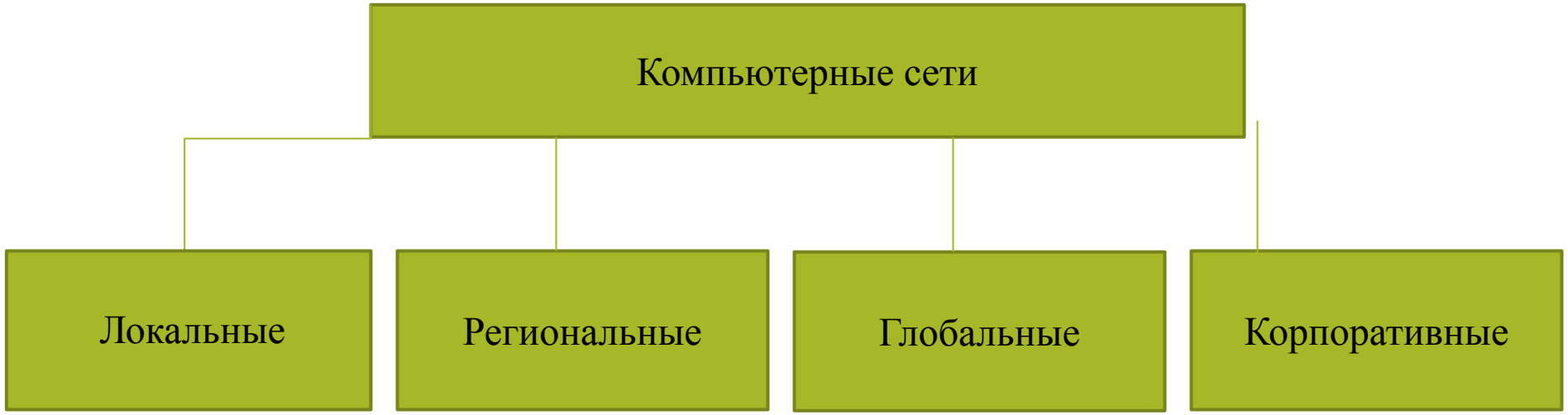
# ЛЕКЦИЯ 3

## Информационная безопасность и защита информации

# Компьютерная сеть

**Компьютерная сеть** — это совокупность компьютеров, объединенных каналами связи и обеспеченных коммуникационным оборудованием и программным обеспечением для совместного использования данных и оборудования.

# Классификация компьютерных сетей



# Виды компьютерных сетей

- **Локальная сеть -** это комплекс программного обеспечения и устройств, объединяющих абонентов, находящихся на незначительной дистанции друг от друга. Как правило, такие системы используются в границах одного предприятия или здания

- **Региональная сеть** – это сеть, существующая обычно в пределах города, района, области, страны. Она связывает абонентов, расположенных на значительном расстоянии друг от друга. Обычно расстояние между абонентами региональной вычислительной сети составляет десятки-сотни километров. Она являются объединением нескольких локальных сетей и частью некоторой глобальной

# Виды компьютерных сетей

- **Глобальная сеть** – это сеть охватывающая большие территории и включающая большое число узлов. Глобальные сети служат для объединения разрозненных сетей так, чтобы пользователи и компьютеры, где бы они ни находились, могли взаимодействовать со всеми остальными участниками глобальной сети.

- **Корпоративная сеть** — это объединение локальных сетей в пределах одной корпорации для решения общих задач. Для корпоративных сетей характерно сочетание централизованной обработки информации с использованием удаленного соединения компьютеров.

# Интернет

- **ИНТЕРНЕТ** (Internet – inter + net – объединение сетей) – всемирная компьютерная сеть, объединяющая миллионы компьютеров в единую информационную систему. Интернет предоставляет широчайшие возможности свободного получения и распространения научной, деловой, познавательной и развлекательной информации.

- **ИНТЕРНЕТ -** глобальная информационная система, выступающая как средство объединения разнообразных информационных компьютерных сетей для передачи информации и обмена ею между странами, регионами, организациями и индивидуальными пользователями. Выступает в качестве квинтэссенции информационно-технической революции и является одним из ее важных аспектов.

# WWW

Термин «WWW» является аббревиатурой от World Wide Web (в переводе с английского — «всемирная паутина»).

Сегодня WWW – это совокупность цифровых источников информации, оформленных в виде гипертекстовых документов (их ещё называют веб-страницами).

# Основные объекты WWW

- Большинство ресурсов всемирной паутины представляет собой гипертекст. Гипертекстовые документы, размещаемые во всемирной паутине, называются **web-страницами.**

- Несколько web-страниц, объединенных общей темой, дизайном, а также связанных между собой ссылками и обычно находящихся на одном и том же web-сервере, называются **web-сайтом**.

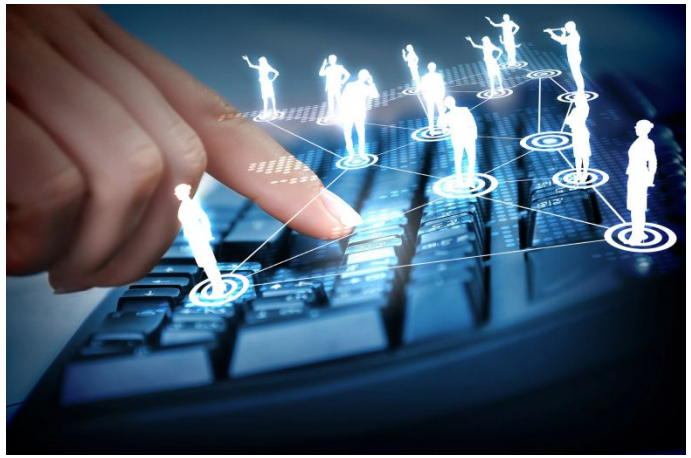
- Для загрузки и просмотра web-страниц используются специальные программы – **браузеры.**

# Интернет как первый цифровой канал коммуникаций

1. **Зарождение** (с 60-х до нач. 90-х) — научно-исследовательские разработки
2. **Распространение** (с нач. 90-х до нач. 2000-х) — начало коммерческого использования
3. **Веб 2.0** (с нач. 2000-х до н.д.) — широкое использование в коммерческих целях, социальные медиа
4. **Мобильный Интернет** (наше время)

# Выгоды интернета для общества

- Оперативный доступ к необходимым информационным ресурсам.
- Уменьшение затрат на получение услуг и товаров
- Возможности самореализации
- Глобализация и расширение коммуникаций



# Риски интернета

- Опасный и вредоносный контент
- Большие объемы некачественной информации
- Интернет-зависимость
- Киберпреступность
- Открытость личных данных

# Информационная безопасность

**Информационная безопасность** – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

# Подсистема обеспечения безопасности информации

**Компьютерная безопасность** обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств компьютера с целью обеспечения доступности, целостности и конфиденциальности, связанных с ним ресурсов.

**Безопасность данных** достигается защитой данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашении.

**Безопасное программное обеспечение** представляет собой общесистемные и прикладные программы и средства, осуществляющие безопасную обработку данных и безопасно использующие ресурсы системы.

**Безопасность коммуникаций** обеспечивается принятием мер по предотвращению предоставления неавторизованным лицам информации, которая может быть выдана системой в ответ на телекоммуникационный запрос.

# Понятие защиты информации

**Защита информации** – это применение различных средств и методов, использование мер и осуществление мероприятий для того, чтобы обеспечить систему надежности передаваемой, хранимой и обрабатываемой информации.

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

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

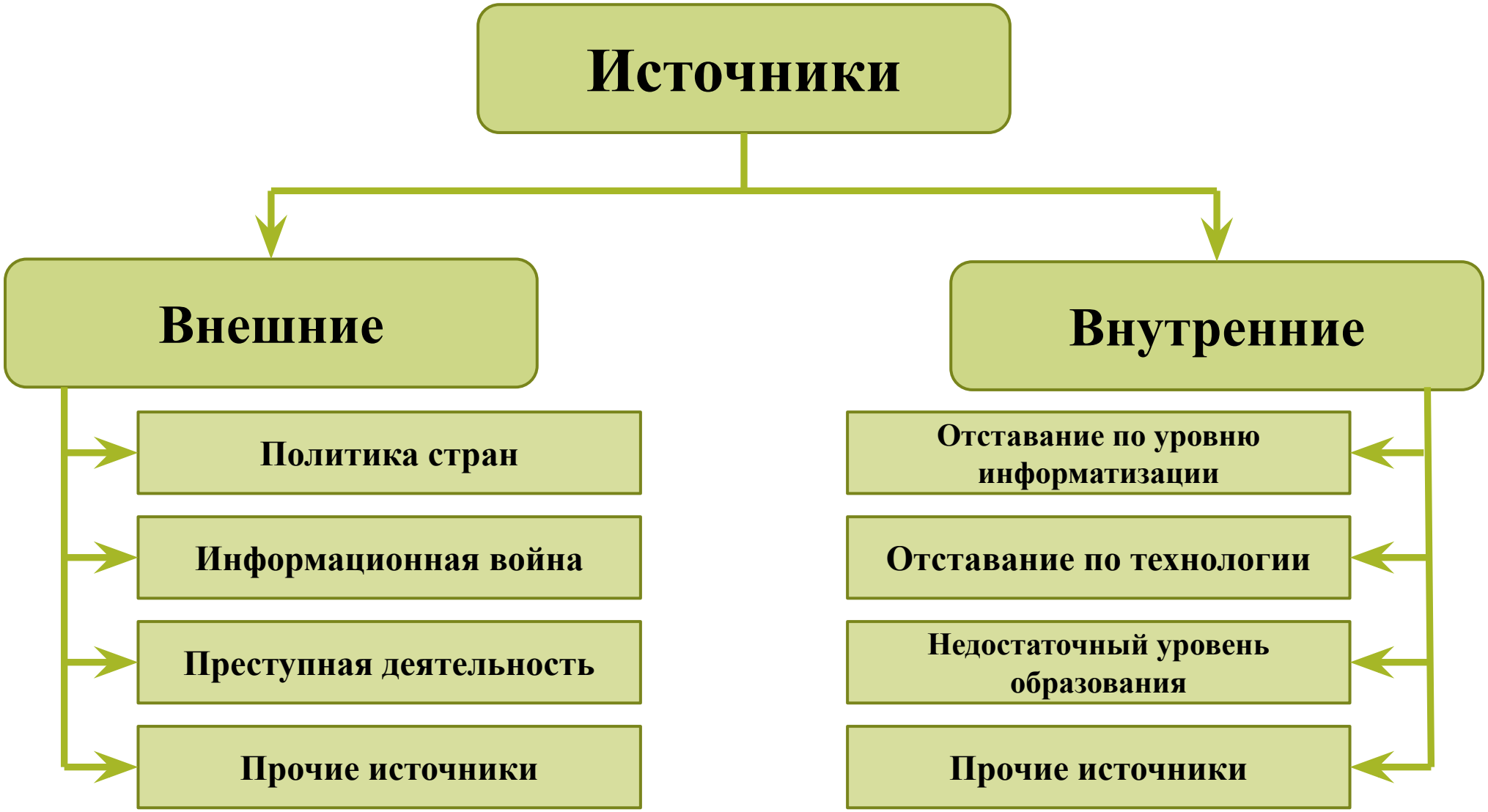
3) реализацию права на доступ к информации.

**Ст. 16 Федерального закона "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ**

# Угрозы безопасности

Угроза безопасности информации – возможность возникновения такого явления или события, следствием которого могут быть нежелательные воздействия на информацию: нарушение физической целостности, логической структуры, несанкционированная модификация информации, несанкционированное получение информации, несанкционированное размножение информации.

# Источники информационных угроз



# Виды информационных угроз

# Политика безопасности

Политика безопасности включает в себя анализ возможных угроз и выбор соответствующих мер противодействия, являющихся совокупностью тех норм, правил поведения, которыми пользуется конкретная организация при обработке информации и ее защите.

В рамках политики безопасности могут использоваться различные средства защиты информации:

- Организационные
- Технические
- Аппаратные
- Программные

# Организационные средства защиты информации

- ***организация работы с сотрудниками*** (подбор и расстановка персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.)
- ***организация работы с документами*** и документированной информацией (разработка, использование, учет, исполнение, возврат, хранение и уничтожение документов и носителей конфиденциальной информации)
- ***организация использования технических средств*** сбора, обработки, накопления и хранения конфиденциальной информации;
- ***организация работы по анализу внутренних и внешних угроз*** конфиденциальной информации и выработке мер по обеспечению ее защиты;
- ***организация работы по проведению систематического контроля за работой персонала*** с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

# Технические средства защиты информации

Для защиты периметра информационной системы создаются:

- системы охранной и пожарной сигнализации;
- системы цифрового видео наблюдения;
- системы контроля и управления доступом (СКУД).

Защита информации от ее утечки техническими каналами связи обеспечивается следующими средствами и мероприятиями:

- использованием экранированного кабеля и прокладка проводов и кабелей в экранированных конструкциях;
- установкой на линиях связи высокочастотных фильтров;
- построение экранированных помещений («капсул»);
- использование экранированного оборудования;
- установка активных систем зашумления;
- создание контролируемых зон.

# Аппаратные средства защиты информации

- Специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
- Устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
- Устройства для шифрования информации (криптографические методы).
- Системы бесперебойного питания:
  - Источники бесперебойного питания;
  - Резервирование нагрузки;
  - Генераторы напряжения.

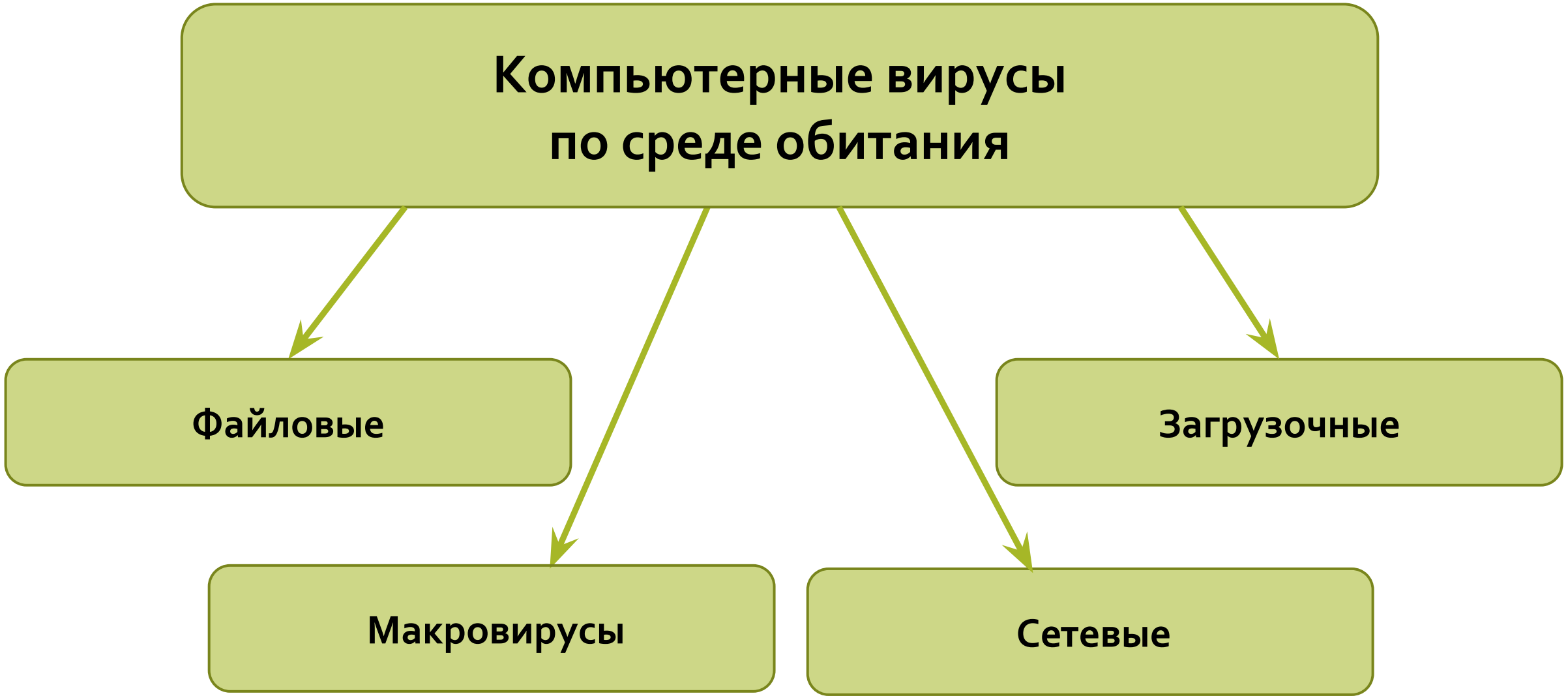
# Программные средства защиты информации

- **Средства защиты от несанкционированного доступа (НСД)**
- **Системы анализа и моделирования информационных потоков (CASE-системы)**
- **Системы мониторинга сетей**
- **Антивирусные средства**
- **Межсетевые экраны**
- **Системы резервного копирования**
- **Цифровая подпись**

# Компьютерный вирус

Автономно функционирующая программа, обладающая одновременно тремя свойствами:

- способностью к включению своего кода в тела других файлов и системных областей памяти компьютера;
- последующему самостоятельному выполнению;
- самостоятельному распространению



Компьютерные вирусы
по среде обитания
Файловые
Загрузочные
Макровирусы
Сетевые

# Файловый вирус

**Файловый вирус** — это вирус, записывающий свой код в тело программного файла, при этом во время запуска программы (или загрузке офисного документа для редактирования) вирус получает управление.

# Макровирусы вирус

**Макровирусы** – это программы, написанные на так называемых макроязыках, встроенных в некоторые системы обработки данных (текстовые и графические редакторы, электронные таблицы и т.д.). Для своего размножения такие вирусы используют возможности макроязыков, они переносятся от одного заражённого файла к другому.

# Сетевые вирусы

**Сетевые вирусы** (черви) – самый опасный вид компьютерных вредоносных ПО, главный принцип работы которых заключается в возможности самостоятельной передачи своего кода на рабочую станцию либо удаленный сервер

# Загрузочные вирусы

**Загрузочный вирус** — такой вирус, который записывает свой код в главную загрузочную запись диска или загрузочную запись  диска. Загрузочный вирус активизируется после загрузки компьютера.

# Каналы распространения вирусов

- размещенные на общедоступных узлах сети Интернет информационные ресурсы, содержащие ссылки на зараженные файлы с элементами управления Active-X;
- локальные компьютерные сети организаций, создающие удобную среду для заражения вирусами объектов на других рабочих станциях и серверах;
- обмен зараженными файлами на съемных носителях между пользователями компьютерной системы;
- использование нелицензионного программного обеспечения и других информационных ресурсов.

# Антивирусное программное обеспечение

***Антивирусная программа (антивирус)*** — любая программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом


# Методы обнаружения компьютерных вирусов

Просмотр (сканирование) проверяемых объектов (системных областей дисковой и оперативной памяти, а также файлов заданных типов) в поиске сигнатур (уникальных последовательностей байтов) известных вирусов. Недостатки: необходимость постоянного обновления баз данных сигнатур известных вирусов, неспособность обнаружить новые компьютерные вирусы.

Эвристический анализ – проверка системных областей памяти и файлов с целью обнаружения фрагментов исполнимого кода, характерного для компьютерных вирусов. Анализируются тысячи различных характеристик каждого файла. Недостатки: длительность процедуры проверки, возможность ложных сообщений о найденных вирусах.

# Роль правового обеспечения информационной безопасности

Основой проведения организационных мероприятий является использование и подготовка законодательных и нормативных документов в области информационной безопасности, которые на правовом уровне должны регулировать доступ к информации со стороны потребителей.

# Первый уровень правового обеспечения информационной безопасности

- Международные (всемирные) конвенции об охране промышленной собственности, об охране интеллектуальной собственности, об авторском праве;
- Конституция РФ (статья 23 определяет право граждан на тайну переписки, телефонных, телеграфных и иных сообщений);
- Уголовный кодекс РФ (статья 272 устанавливает ответственность за неправомерный доступ к компьютерной информации, статья 273 – за создание, использование и распространение вредоносных программ для ЭВМ, статья 274 – за нарушение правил эксплуатации ЭВМ, систем и сетей);
- Федеральный закон «Об информации, информационных технологиях и о защите информации».

# Второй уровень правового обеспечения информационной безопасности

Второй уровень правового регулирования защиты информации составляют подзаконные акты, к которым относятся указы Президента и постановления Правительства РФ, а также определения Конституционного суда РФ, письма Высшего арбитражного суда РФ и постановления пленумов Верховного суда РФ.

- Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера»
- Постановление Правительства РСФСР «О перечне сведений, которые не могут составлять коммерческую тайну» в редакции Постановления Правительства РФ от 03.10.2002 № 731.

# Третий уровень правового обеспечения информационной безопасности

Третий уровень правового обеспечения информационной безопасности составляют государственные стандарты (ГОСТы) в области защиты информации, руководящие документы, нормы, методики и классификаторы, разработанные соответствующими государственными органами (ФСБ, ФСТЭК и др.).

- "ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения« от 27.12.2006 N 373-ст)
- Руководящий документ Государственной технической комиссии при Президенте Российской Федерации (Гостехкомиссии России) «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»

# Четвертый уровень правового обеспечения информационной безопасности

Четвертый уровень правового обеспечения информационной безопасности образуют локальные нормативные акты, положения, инструкции, методические рекомендации и другие документы по комплексной защите информации в КС конкретной организации. К таким нормативным документам относятся:

- Приказ об утверждении перечня сведений, составляющих коммерческую тайну предприятия (организации).
- Разделы в трудовых и гражданско-правовых договорах, заключаемых с сотрудниками и контрагентами предприятия (организации) об обязанности возмещения ущерба за разглашение сведений, составляющих коммерческую тайну предприятия.

# СПАСИБО ЗА ВНИМАНИЕ !