АКАДЕМИЯ
ГРАЖДАНСКОЙ ЗАЩИТЫ
МЧС РОССИИ

Дисциплина «Информационные технологии »

Тема № 3. Основы защиты информации

Лекция 3/1. Защита информации

Учебные вопросы:

1. **Проблемы обеспечения защиты информации.**
2. **Средства защиты информации.**

Литература:

1. Информационные технологии в профессиональной деятельности. Учебное пособие. – Химки: АГЗ МЧС России, 2015.
2. **Касперский Е.В. Компьютерные вирусы. М.СК-пресс.**
3. Информационные технологии: учебник/ И.К.Корнеев, Г.Н. Ксандопуло, В.А. Машурцев; Государственный университет управления. – М.: Велби: Проспект, 2007.

Под **информационной безопасностью** Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Информационная безопасность обеспечивает:

конфиденциальность информации

- свойство информационных ресурсов, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц

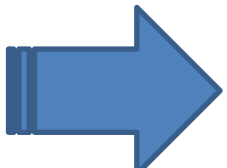
целостность информации и связанных с ней процессов

- неизменность информации в процессе ее передачи или хранения

доступность информации, когда она нужна

- свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц

учет всех процессов, связанных с информацией



Составляющие обеспечения безопасности информации

- Конфиден-циальность
- Целостность
- Доступность

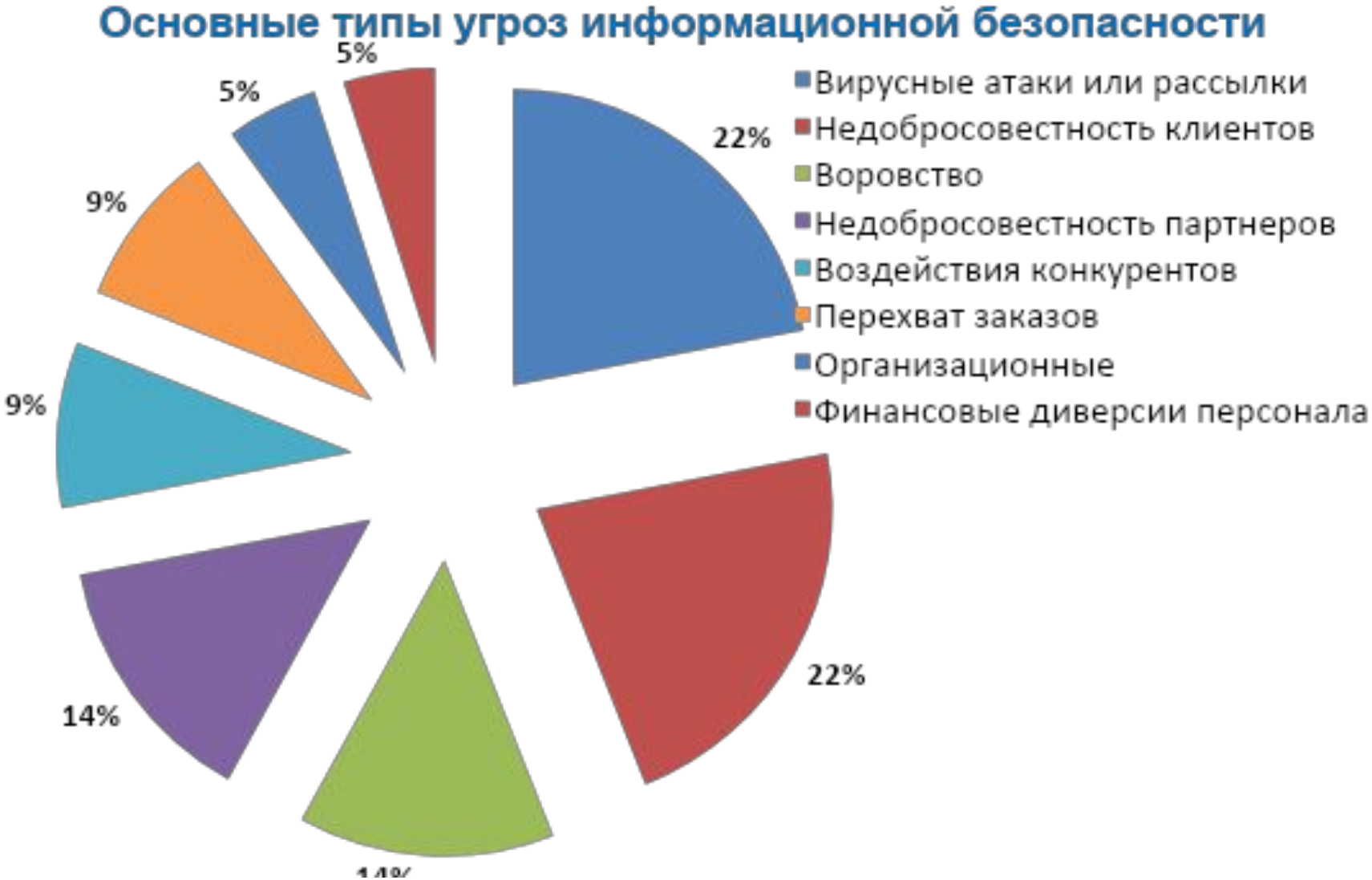
Точки приложения процесса защиты информации к информационной системе

- Аппаратное обеспечение
- Программное обеспечение
- Обеспечение связи (коммуникации)

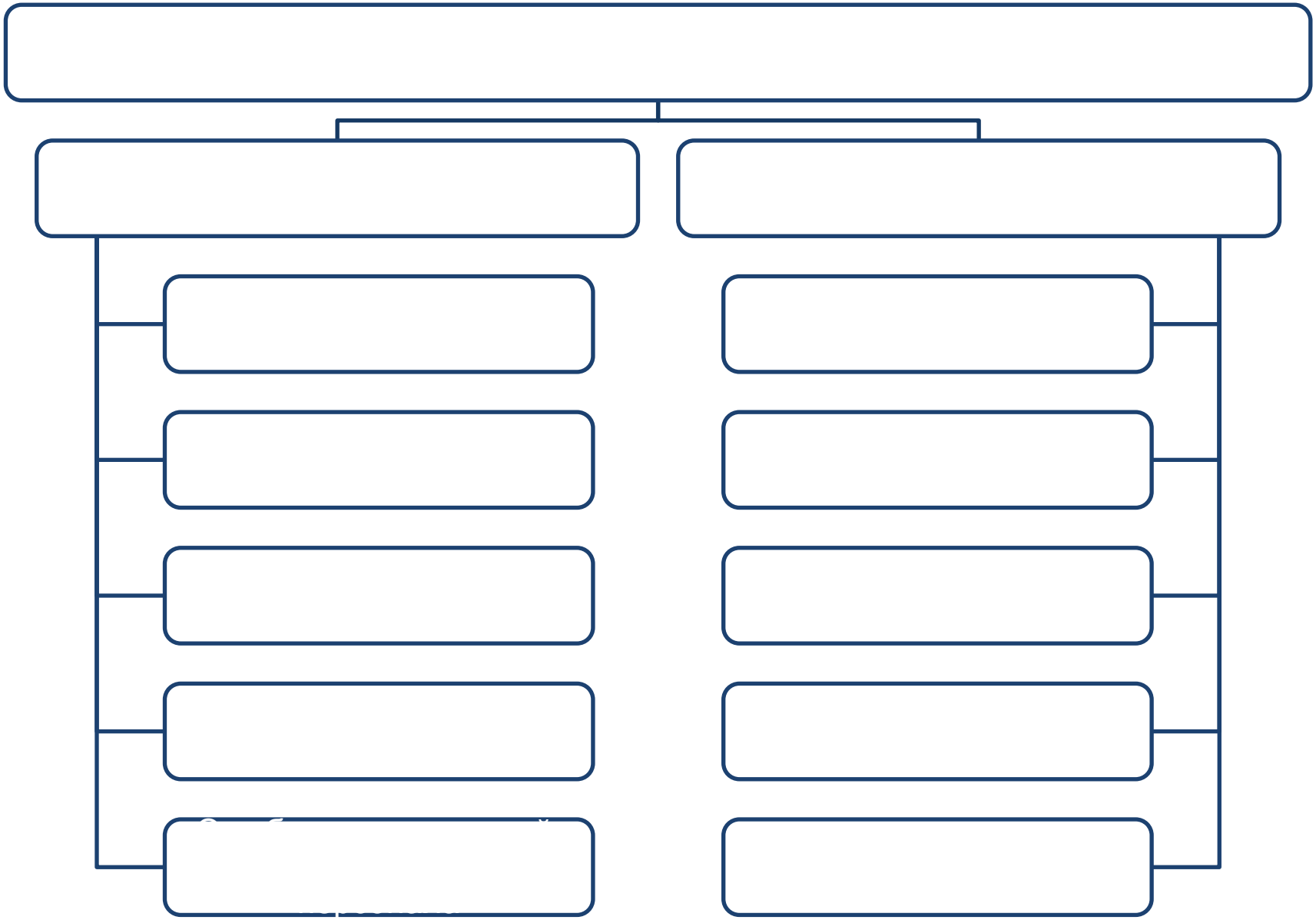
Процедуры (механизмы) защиты

- Защита физического уровня
- Защита персонала
- Организационный уровень

Угроза безопасности компьютерной системы - потенциально возможное происшествие (преднамеренное или нет), которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.



Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называют случайными или непреднамеренными.



Средства защиты информации необходимо применять непосредственно к информации доступ к которой ограничен — это **государственная тайна и конфиденциальные данные**.

Согласно закона РФ от 21.07.1993 N **5485-1**
«О государственной тайне» статья 5. **«Перечень сведений составляющих государственную тайну»** относится:

Сведения в военной области

Перечень сведений, которые могут составлять конфиденциальную информацию, содержится в **указе президента** от 6 марта 1997 г. **№188** «Об утверждении перечня сведений конфиденциального характера».

Согласно федеральному закону от 27.07.2006 **№ 152-ФЗ «О персональных данных»,** статья 4: Персональные данные – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Оператором персональных данных является — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Права на обработку персональных данных закреплено в положениях о государственных органах, федеральными законами, лицензиями на работу с персональными данными, которые **выдает Роскомнадзор или ФСТЭК**.

Компании, которые профессионально работают с персональными данными широкого круга лиц, например, хостинг компании виртуальных серверов или операторы связи, **должны войти в реестр, его ведет Роскомнадзор.**

Государство также определят меру ответственности за нарушение положений законодательства в сфере информационной безопасности. Например, **глава 28 «Преступления в сфере компьютерной информации» в Уголовном кодексе Российской Федерации, включает три статьи**:

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».

2 вопрос:

Средства защиты информации

Комплексная система защиты информации создается на объектах для блокирования (парирования) всех возможных или, по крайней мере, наиболее вероятных угроз безопасности информации.

Согласно закону **№ 149-ФЗ** защиту информации можно разделить на несколько уровней:

Средства защиты информации — это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Организационная защита

организация режима и охраны;	организация работы с сотрудниками;	организация работы с документами и документированной информацией;
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).

Средства и мероприятия по защите информации от ее утечки техническими каналами связи

- 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

Схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных

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:

- Системы обнаружения и предотвращения вторжений;
- Системы предотвращения утечек конфиденциальной информации.

Анализаторы протоколов

Антивирусные средства

Программные средства защиты информации

Межсетевые экраны

Криптографические средства

Системы резервного копирования

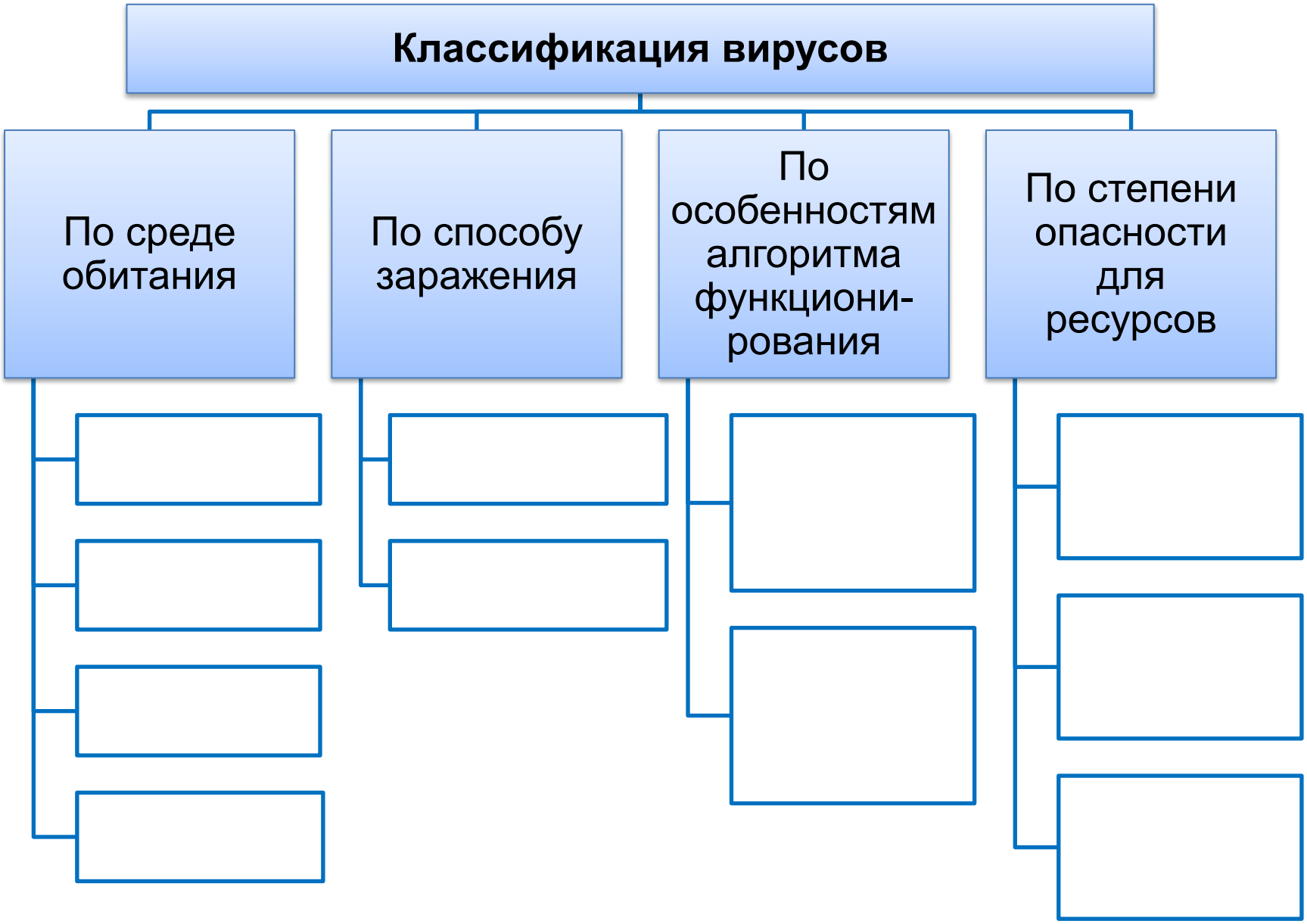
Системы аутентификации:

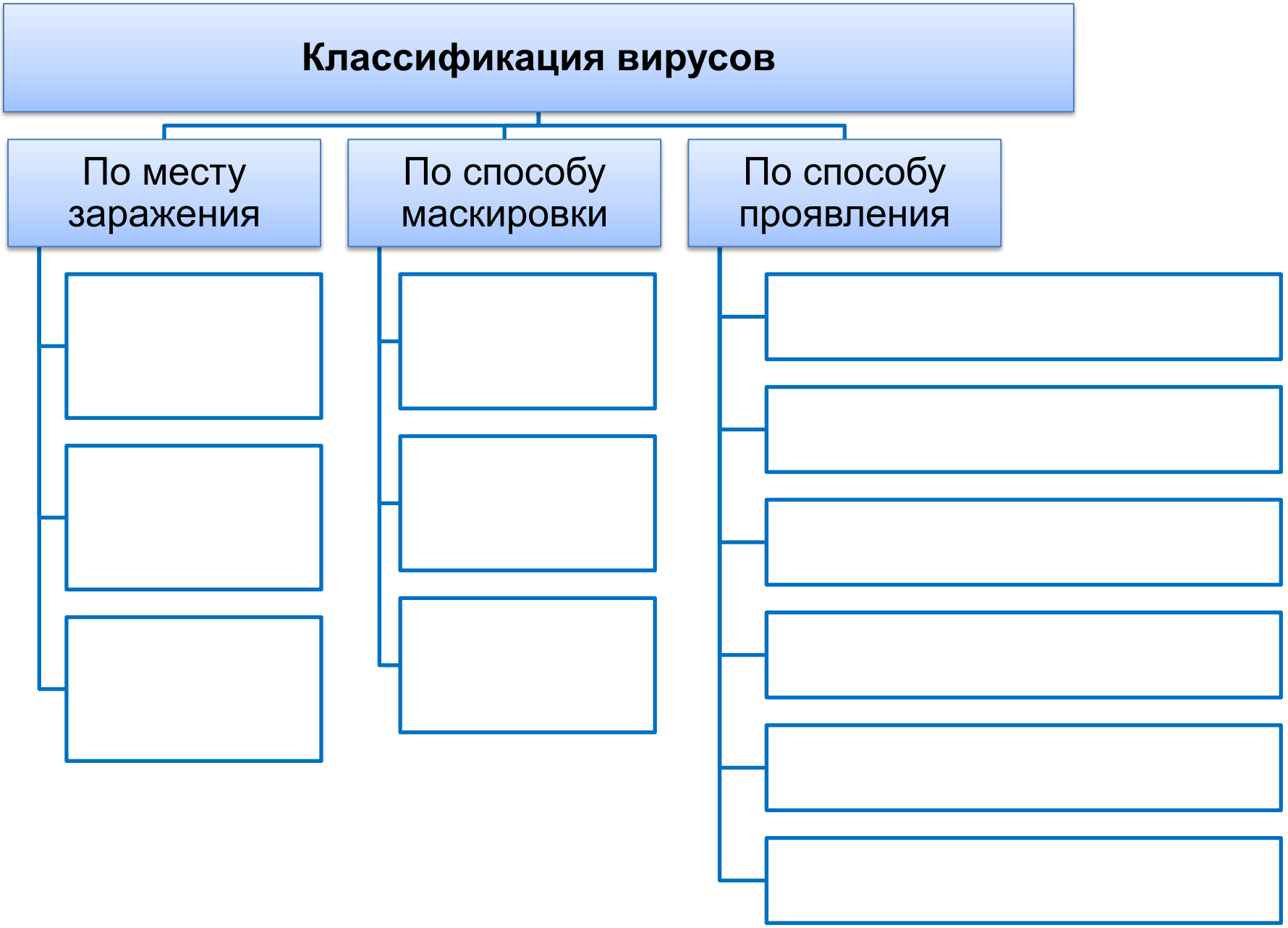
- Пароль;
- Ключ доступа (физический или электронный);
- Сертификат;
- Биометрия.

Инструментальные средства анализа систем защиты

Компьютерный вирус – это специальная программа, наносящая заведомый вред компьютеру, на котором она запускается на выполнение, или другим компьютерам в сети.

Компьютерный вирус – это специально написанная небольшая по размерам программа, которая может «приписывать» себя к другим программам (т.е. «заражать» их), а также выполнять различные нежелательные действия на компьютере.


Классификация вирусов
По среде обитания
По способу заражения
По особенностям алгоритма функциони-рования
По степени опасности для ресурсов


Классификация вирусов
По месту заражения
По способу маскировки
По способу проявления

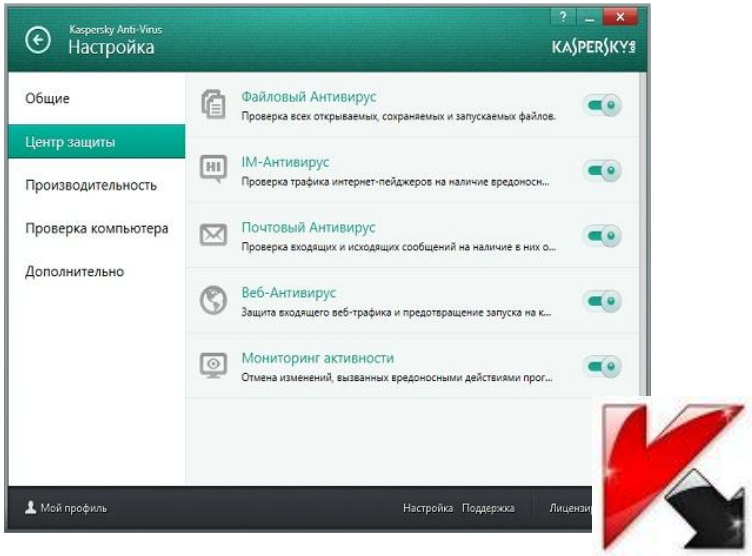
Основные признаки появления в системе вируса

1. Замедление работы некоторых программ.
2. Появление не существовавших раннее «странных» файлов, особенно в каталоге windows или корневом.
3. Внезапно возникающие разнообразные видео и звуковые эффекты.
4. Заметное снижение скорости работы в интернете.
5. Прекращение работы или неправильная работа ранее успешно функционировавших программ.
6. Невозможность загрузки операционной системы.
7. Исчезновение файлов и каталогов или искажение их содержимого.
8. Изменение даты и времени модификации файлов.
9. Неожиданное значительное увеличение количества файлов на диске.
10. Существенное уменьшение размера свободной оперативной памяти.
11. Подача непредусмотренных звуковых сигналов.
12. Частые зависания и сбои в работе компьютера.

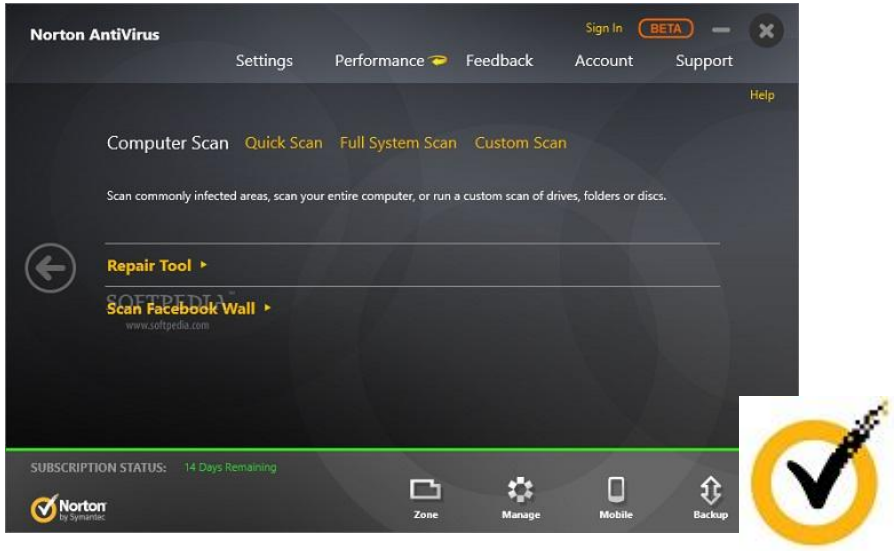
Профилактика заражения

1. Применять только законные программные продукты.
2. Дублировать важную информацию.
3. Регулярно пользоваться антивирусными программами.
4. Особая осторожность при применении носителей информации.
5. При коллективном пользовании, использовать организационные методы борьбы.

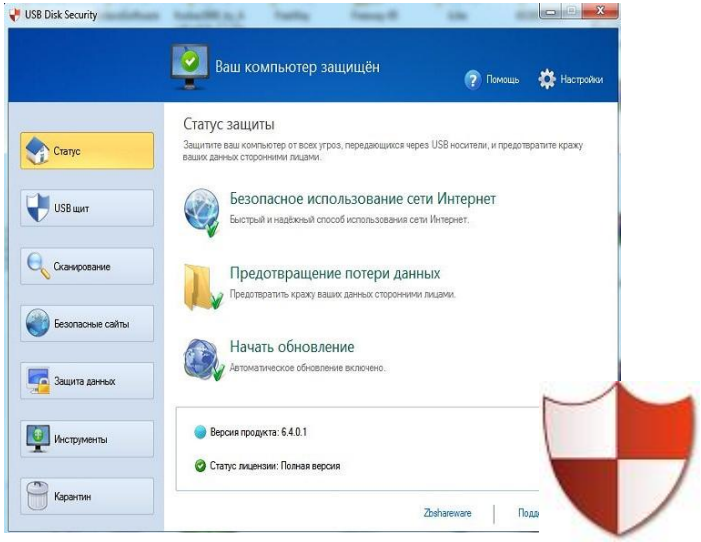
Антивирус Касперского



Norton AntiVirus

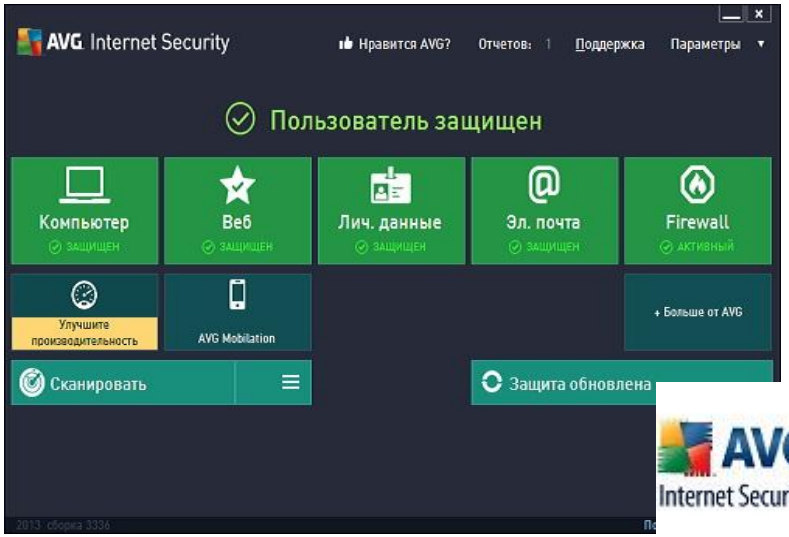


USB Disk Security

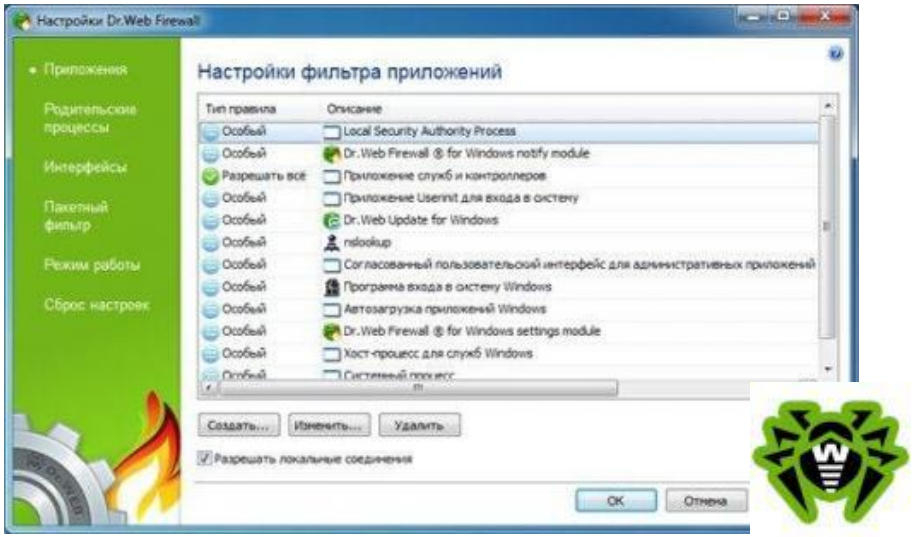


Norton Internet Security

AVG Internet Security

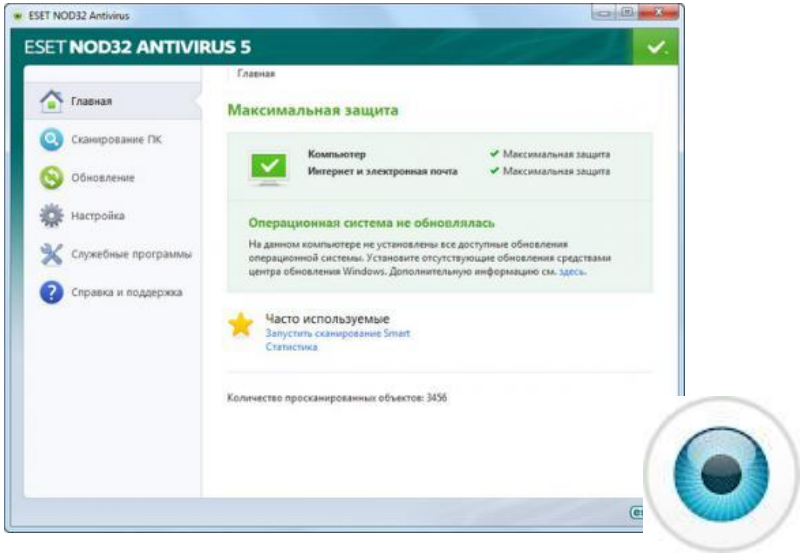


Антивирус Dr.Web



avast! Internet Security

ESET NOD32 Антивирус



Виды антивирусных программ

Детекторы	• позволяют обнаруживать файлы, заражённые одним из нескольких известных вирусов
Фильтры	• оповещают пользователя о всех попытках какой-либо программы записаться на диск, а также о других подозрительных действиях
Программы-доктора или фаги	• находят и «лечат» зараженные вирусами файлы
Ревизоры	• запоминают сведения о состоянии файлов и системных областей дисков, а при последующих запусках – сравнивают их состояние исходным. При выявлении несоответствий об этом сообщается пользователю
Сторожа или фильтры	• располагаются резидентно в оперативной памяти компьютера и проверяют на наличие вирусов запускаемые файлы и вставляемые USB-накопители
Программы-вакцины или иммунизаторы	• модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже заражёнными

Недостатки антивирусных программ

- **Ни одна из существующих антивирусных технологий не может обеспечить полной защиты от вирусов**.
- Антивирусная программа забирает часть вычислительных ресурсов системы, нагружая центральный процессор и жёсткий диск.
- Антивирусные программы могут видеть угрозу там, где её нет (ложные срабатывания).
- Антивирусные программы загружают обновления из Интернета, тем самым расходуя трафик.
- Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы не обнаруживаемыми антивирусным программным обеспечением. Для обнаружения этих «замаскированных» вирусов требуется мощный механизм распаковки, который может дешифровать файлы перед их проверкой. Однако во многих антивирусных программах эта возможность отсутствует и, в связи с этим, часто невозможно обнаружить зашифрованные вирусы.

Тема № 3. Основы защиты информации

3/2. Задание на семинар по дисциплине
Тема: Компьютерные вирусы и антивирусные программные средства

Учебные вопросы:

1. Компьютерные вирусы, классификация вирусов.
2. Безопасность ПК. Современные средства борьбы с вредоносными программами.
3. Правовые вопросы безопасности программного обеспечения (использование и распространение «пиратского» ПО, написание и распространение компьютерных вирусов, и другие правовые проблемы).
4. Киберпреступность.
5. Сообщения об «известных» вирусах и вирусных атаках, их действии на ПК,... и другое ВРЕДОНОСНОЕ ПО!!!!