ЛЕКЦИЯ №6

БАЗОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ: ГЕОИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

- Геоинформационные технологии. Векторные и растровые модели.
- Назначение и основные области использования ГИС.
- Технологии защиты информации.
- Виды угроз и способы защиты информации.

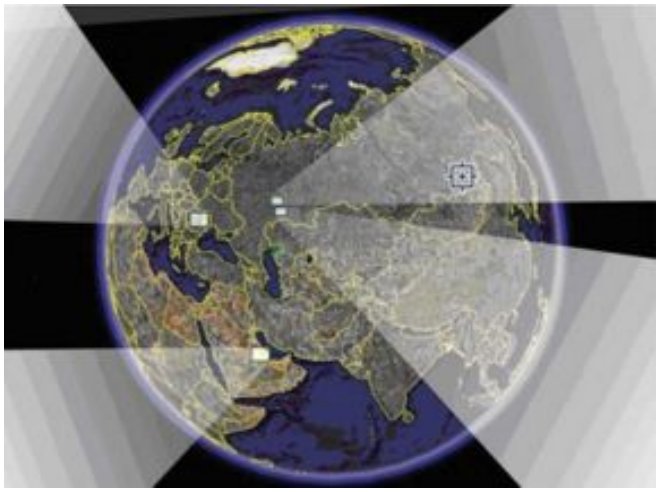
СИСТЕМЫ УПРАВЛЕНИЯ, ОТОБРАЖАЮЩИЕ ИНФОРМАЦИЮ НА ЭЛЕКТРОННОЙ КАРТЕ:

- геоинформационные системы;
- системы федерального и муниципального управления;
- системы проектирования;
- системы военного назначения и т.д.

Геоинформационная система – это компьютерная информационная система, отображающая информацию на электронной карте.

Предназначение ГИС

- **геоинформационные технологии предназначены** для широкого внедрения в практику методов и средств работы с пространственно-временными данными, представляемыми в виде системы электронных карт, и предметно-ориентированных сред обработки разнородной информации для различных категорий пользователей.



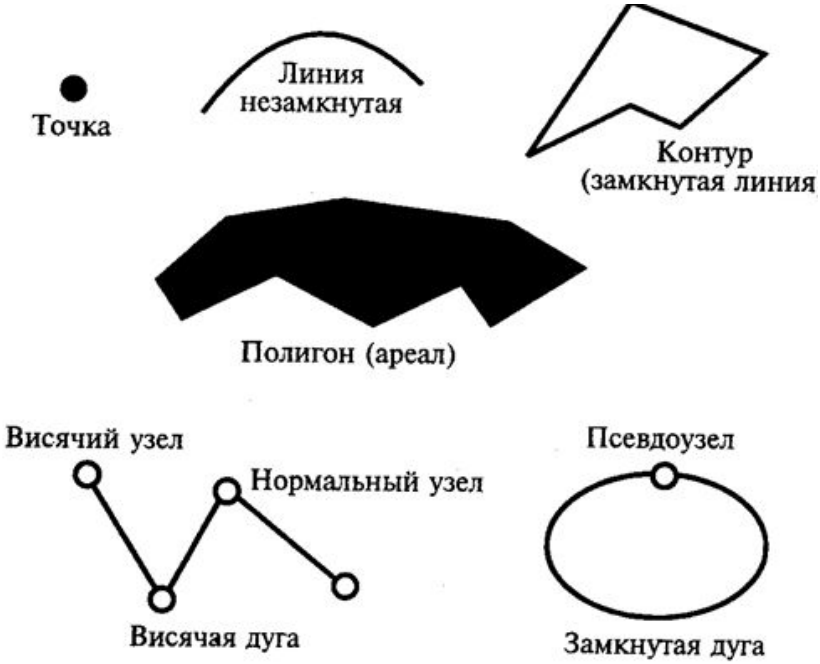
- Графическое представление какой-либо ситуации на экране компьютера подразумевает отображение различных графических образов.
- Графическая информация, которая хранится в ГИС, не является статической.

КЛАСС ДАННЫХ ГИС

Основным классом данных геоинформационных систем (ГИС) являются ***координатные данные***, содержащие геометрическую информацию и отражающие пространственный аспект.

Основные типы координатных данных:

- точка (узлы, вершины)
- линия (незамкнутая)
- контур (замкнутая линия)
- полигон (ареал, район).



Основные группы связей

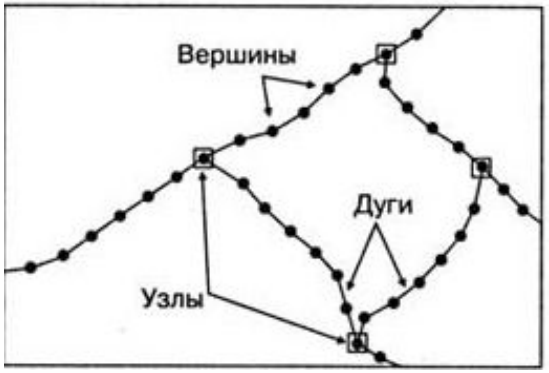
- взаимосвязи для построения сложных объектов из простых элементов;
- взаимосвязи, вычисляемые по координатам объектов;
- взаимосвязи, определяемые с помощью специального описания и семантики при вводе данных.

ВИЗУАЛЬНОЕ ПРЕДСТАВЛЕНИЕ ДАННЫХ

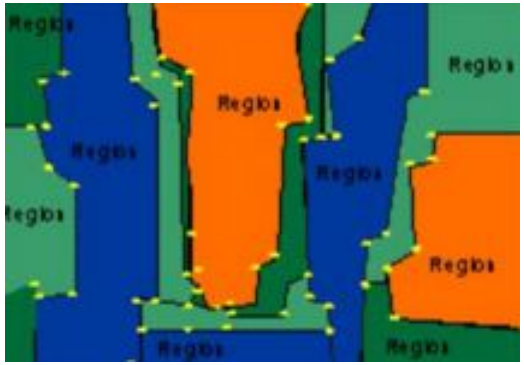
Основой визуального представления данных при использовании ГИС-технологий является графическая среда, основу которой составляют векторные и растровые (ячеистые) модели.

Векторные модели основаны на представлении геометрической информации с помощью векторов, занимающих часть пространства, что требует при реализации меньшего объема памяти.

Используются векторные модели в транспортных, коммунальных, маркетинговых приложениях ГИС.

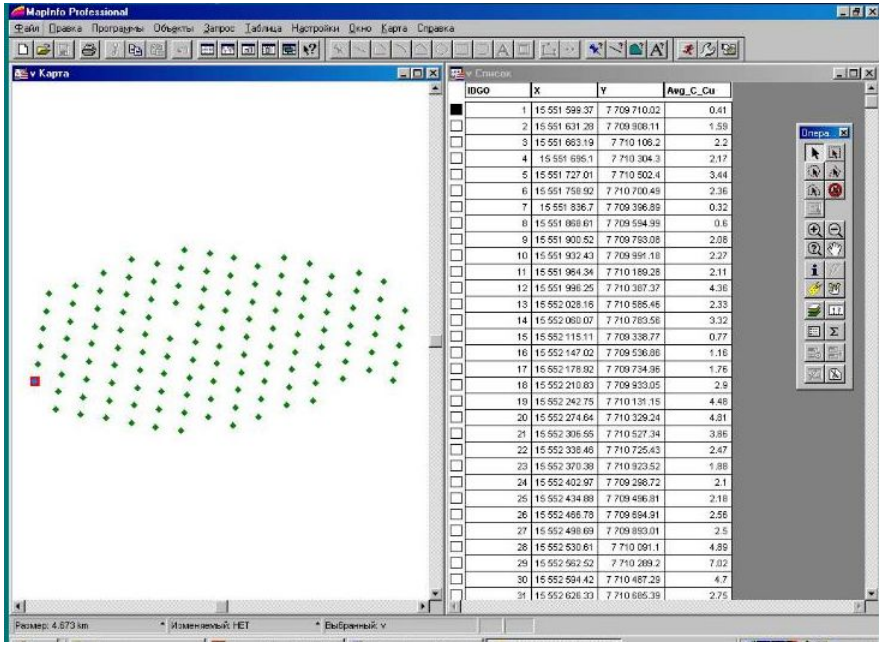


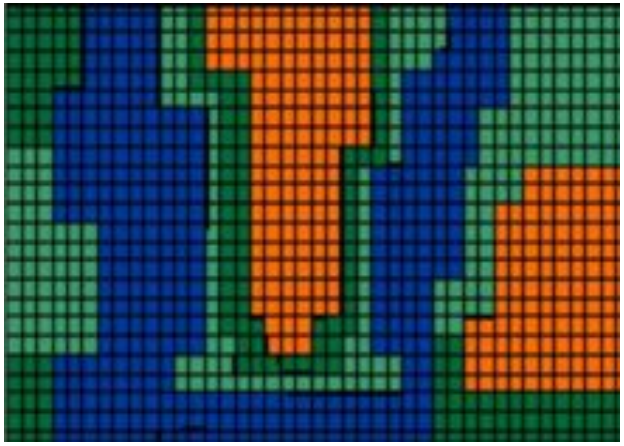
Векторными графическими редакторами являются системы компьютерного черчения.
Форматом векторных графических файлов является формат **WMF**



Растровые модели

- В **растровых** моделях объект (территория) отображается в пространственные ячейки, образующие регулярную сеть.
- Каждой ячейке растровой модели соответствует одинаковый по размерам, но разный по характеристикам (цвет, плотность) участок поверхности.





- Ячейка модели характеризуется одним значением, являющимся средней характеристикой участка поверхности. Эта процедура называется пикселизацией.
- Универсальным форматом растровых графических файлов является формат BMP.

Сопоставление растровых и векторных моделей

- **Векторная** модель содержит информацию о местоположении объекта.
- Векторные модели относятся к бинарным или квазибинарным.

Растровая модель содержит информацию о том, что расположено в той или иной точке объекта.

Растровые модели позволяют отображать полутона.

Основной областью использования растровых моделей является обработка аэрокосмических снимков.

РАЗМЕРНОСТЬ МОДЕЛИ

Применяют:

- двухмерные модели координат (2D)
- трехмерные модели координат (3D).

Двухмерные модели используются при построении карт, а трехмерные – при моделировании геологических процессов, проектировании инженерных сооружений (плотин, водохранилищ, карьеров и др.), моделировании потоков газов и жидкостей.

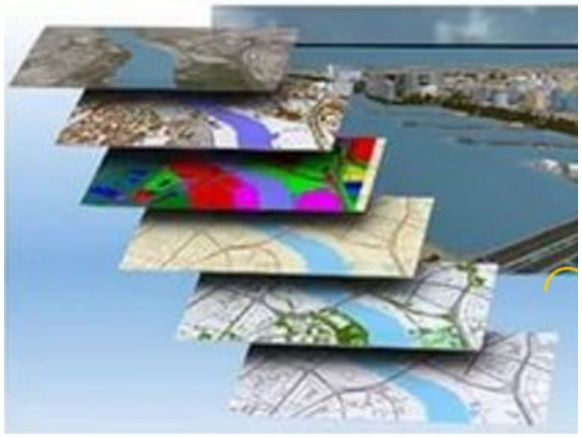
Существуют два типа трехмерных моделей:

- псевдотрехмерные, когда фиксируется третья координата;
- истинные трехмерные.

ОБРАБОТКА ИНФОРМАЦИИ В ГИС

Большинство современных ГИС осуществляет комплексную обработку информации:

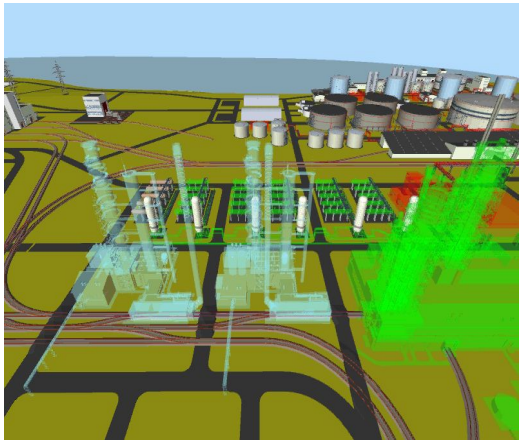
- • сбор первичных данных;
- • накопление и хранение информации;
- • различные виды моделирования (семантическое, имитационное, геометрическое, эвристическое);
- • автоматизированное проектирование;
- • документационное обеспечение.

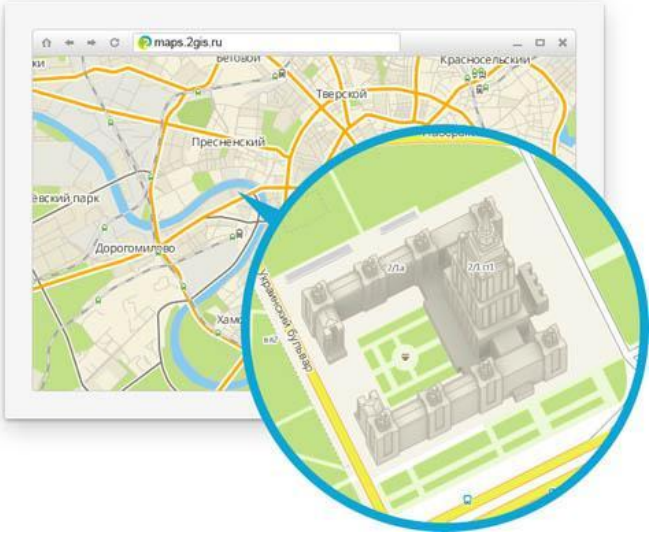


ОБРАБОТКА ИНФОРМАЦИИ В ГИС

Основные области использования ГИС:

- электронные карты;
- городское хозяйство;
- государственный земельный кадастр;
- экология;
- дистанционное зондирование;
- экономика;
- специальные системы военного назначения.





ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

Группы информационных угроз

Все виды информационных угроз можно разделить на две большие группы:

- отказы и нарушения работоспособности программных и технических средств;
- преднамеренные угрозы, заранее планируемые злоумышленниками для нанесения вреда.

Причины сбоев и отказов в работе компьютерных систем:

- нарушения физической и логической целостности хранящихся в оперативной и внешней памяти структур данных, возникающие по причине старения или преждевременного износа их носителей;
- нарушения, возникающие в работе аппаратных средств из-за их старения или преждевременного износа;
- нарушения физической и логической целостности хранящихся в оперативной и внешней памяти структур данных, возникающие по причине некорректного использования компьютерных ресурсов;
- нарушения, возникающие в работе аппаратных средств из-за неправильного использования или повреждения, в том числе из-за неправильного использования программных средств;
- неустраненные ошибки в программных средствах, не выявленные в процессе отладки и испытаний, а также оставшиеся в аппаратных средствах после их разработки.

Способы защиты информации

- внесение структурной, временной, информационной и функциональной избыточности компьютерных ресурсов;
- защита от некорректного использования ресурсов компьютерной системы;
- выявление и своевременное устранение ошибок на этапах разработки программно-аппаратных средств.

Внесение избыточности компьютерных ресурсов

- **Структурная избыточность** компьютерных ресурсов достигается за счет резервирования аппаратных компонентов . Структурная избыточность составляет основу остальных видов избыточности.
- **Внесение информационной** избыточности выполняется путем периодического или постоянного (фонового) резервирования данных на основных и резервных носителях.
- **Функциональная избыточность** компьютерных ресурсов достигается дублированием функций или внесением дополнительных функций в программно-аппаратные ресурсы вычислительной системы для повышения ее защищенности от сбоев и отказов

Например, периодическое тестирование и восстановление, а также самотестирование и самовосстановление компонентов компьютерной системы.

ЗАЩИТА ОТ НЕКОРРЕКТНОГО ИСПОЛЬЗОВАНИЯ ИР

- Защита от некорректного использования информационных ресурсов заключается в корректном функционировании программного обеспечения с позиции использования ресурсов вычислительной системы.
- Выявление и устранение ошибок при разработке программно-аппаратных средств достигается путем качественного выполнения базовых стадий разработки на основе системного анализа концепции, проектирования и реализации проекта.

Виды угроз целостности и конфиденциальности информации

Основным видом угроз целостности и конфиденциальности информации являются преднамеренные угрозы, заранее планируемые злоумышленниками для нанесения вреда:

- *угрозы, реализация которых выполняется при постоянном участии человека;*
- *угрозы, реализация которых после разработки злоумышленником соответствующих компьютерных программ выполняется этими программами без непосредственного участия человека.*

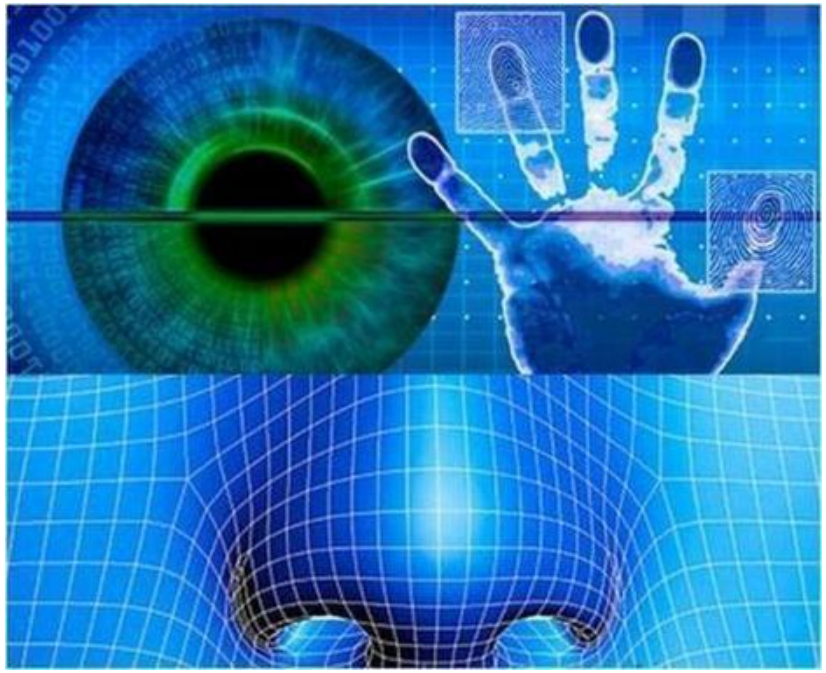
Задачи по защите от угроз

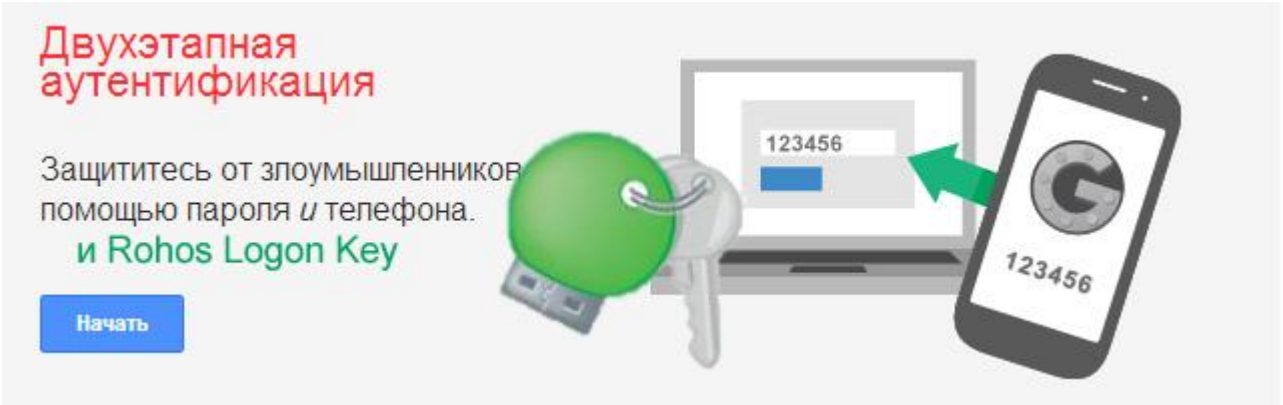
- запрещение несанкционированного доступа к ресурсам вычислительных систем;
- невозможность несанкционированного использования компьютерных ресурсов при осуществлении доступа;
- своевременное обнаружение факта несанкционированных действий, устранение их причин и последствий.

запрещение несанкционированного доступа к ресурсам ВС

- подтверждение подлинности пользователей и разграничение их доступа к информационным ресурсам, включающего следующие этапы:

- идентификация;
- установление подлинности (аутентификация);
- определение полномочий для последующего контроля и разграничения доступа к компьютерным ресурсам.





Идентификация

Идентификатор может представлять собой любую последовательность символов и должен быть заранее зарегистрирован в системе администратора службы безопасности.

В процессе регистрации заносится следующая информация:

- *фамилия, имя, отчество (при необходимости другие характеристики пользователя); уникальный идентификатор пользователя;*
- *имя процедуры установления подлинности;*
- *эталонная информация для подтверждения подлинности (например, пароль);*
- *ограничения на используемую эталонную информацию (например, время действия пароля);*
- *полномочия пользователя по доступу к компьютерным ресурсам.*

Аутентификация

Установление подлинности (аутентификация) заключается в проверке истинности полномочий пользователя.

- Для особо надежного опознания при идентификации используются технические средства, определяющие индивидуальные характеристики человека (голос, отпечатки пальцев, структура зрачка).
- Наиболее массово используемыми являются **парольные методы** проверки подлинности пользователей.

Парольные методы проверки подлинности

Пароли можно разделить на две группы:

- Простые
- Динамически изменяющиеся.

- Простой пароль не изменяется от сеанса к сеансу в течение установленного периода его существования.
- Динамически изменяющийся пароль изменяется по правилам, определяемым используемым методом.

Динамически изменяющийся пароль

Выделяют следующие методы реализации динамически изменяющихся паролей:

- методы модификации простых паролей. Например, случайная выборка символов пароля и одноразовое использование паролей;
- метод «запрос – ответ», основанный на предъявлении пользователю случайно выбираемых запросов из имеющегося массива;
- функциональные методы, основанные на использовании некоторой функции *F* с динамически изменяющимися параметрами (дата, время, день недели и др.), с помощью которой определяется пароль.

Права пользователей по доступу к ресурсам

Различают следующие виды прав пользователей по доступу к ресурсам:

- ***всеобщее (полное предоставление ресурса)***
- ***функциональное или частичное***
- ***временное***

Способы разграничения доступа

- разграничение по спискам (пользователей или ресурсов);
- использование матрицы установления полномочий (строки матрицы – идентификаторы пользователей, столбцы – ресурсы компьютерной системы);
- разграничение по уровням секретности и категориям (например, общий доступ, конфиденциально, секретно);
- парольное разграничение.

Криптографические методы защиты информации

- Защита информации от исследования и копирования предполагает криптографическое закрытие защищаемых от хищения данных.
- Задачей криптографии является обратимое преобразование некоторого понятного исходного текста (открытого текста) в кажущуюся случайной последовательность некоторых знаков, часто называемых шифротекстом, или криптограммой.

В шифре выделяют два основных элемента – алгоритм и ключ.

- Алгоритм шифрования представляет собой последовательность преобразований обрабатываемых данных, зависящих от ключа шифрования.
- Ключ задает значения некоторых параметров алгоритма шифрования, обеспечивающих шифрование и дешифрование информации.

Типы криптографических систем

По способу использования ключей различают два типа криптографических систем:

- **Симметрические**
- **асимметрические.**

- В симметрических (одноключевых) криптографических системах ключи шифрования и дешифрования либо одинаковы, либо легко выводятся один из другого.
- В асимметрических (двухключевых или системах с открытым ключом) криптографических системах ключи шифрования и дешифрования различаются таким образом, что с помощью вычислений нельзя вывести один ключ из другого.

Хищение информации

- Одной из основных угроз хищения информации является **угроза доступа к остаточным данным** в оперативной и внешней памяти компьютера.
- Под остаточной информацией понимают данные, оставшиеся в освободившихся участках оперативной и внешней памяти после удаления файлов пользователя, удаления временных файлов без ведома пользователя, находящиеся в неиспользуемых хвостовых частях последних кластеров, занимаемых файлами, а также в кластерах, освобожденных после уменьшения размеров файлов и после форматирования дисков.

Хищение информации

Основным способом защиты от доступа к конфиденциальным остаточным данным является своевременное уничтожение данных в следующих областях памяти компьютера:

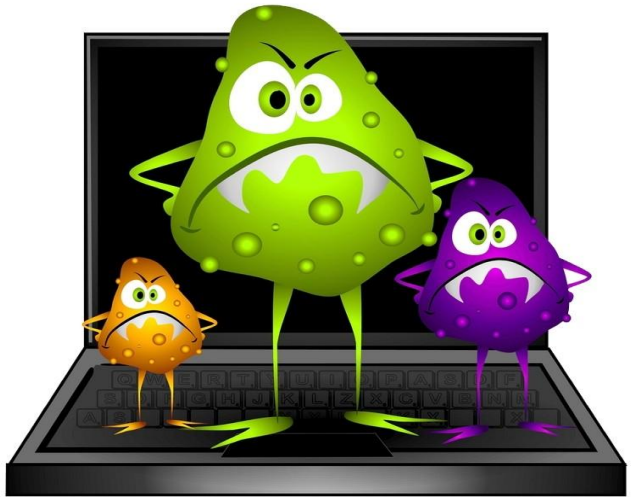
- ***в рабочих областях оперативной и внешней памяти, выделенных пользователю, после окончания им сеанса работы;***
- ***в местах расположения файлов после выдачи запросов на их удаление.***

- Уничтожение остаточных данных может быть реализовано либо средствами операционных сред, либо с помощью специализированных программ.
- Использование специализированных программ (автономных или в составе системы защиты) обеспечивает гарантированное уничтожение информации.

Защита информации от компьютерных вирусов

Выделяют три уровня защиты от компьютерных вирусов:

- • защита от проникновения в вычислительную систему вирусов известных типов;
- • углубленный анализ на наличие вирусов известных и неизвестных типов, преодолевших первый уровень защиты;
- • защита от деструктивных действий и размножения вирусов, преодолевших первые два уровня.



Задачи защиты:

1. обеспечение безопасности обработки и хранения информации в каждом из компьютеров, входящих в сеть;
2. защита информации, передаваемой между компьютерами сети.

- Решение первой задачи основано на многоуровневой защите автономных компьютерных ресурсов от несанкционированных и некорректных действий пользователей и программ, рассмотренных выше.
- Безопасность информации при сетевом обмене данными требует обеспечения их конфиденциальности и подлинности. Защита информации в процессе передачи достигается на основе защиты каналов передачи данных, а также криптографического закрытия передаваемых сообщений.

Спасибо за внимание