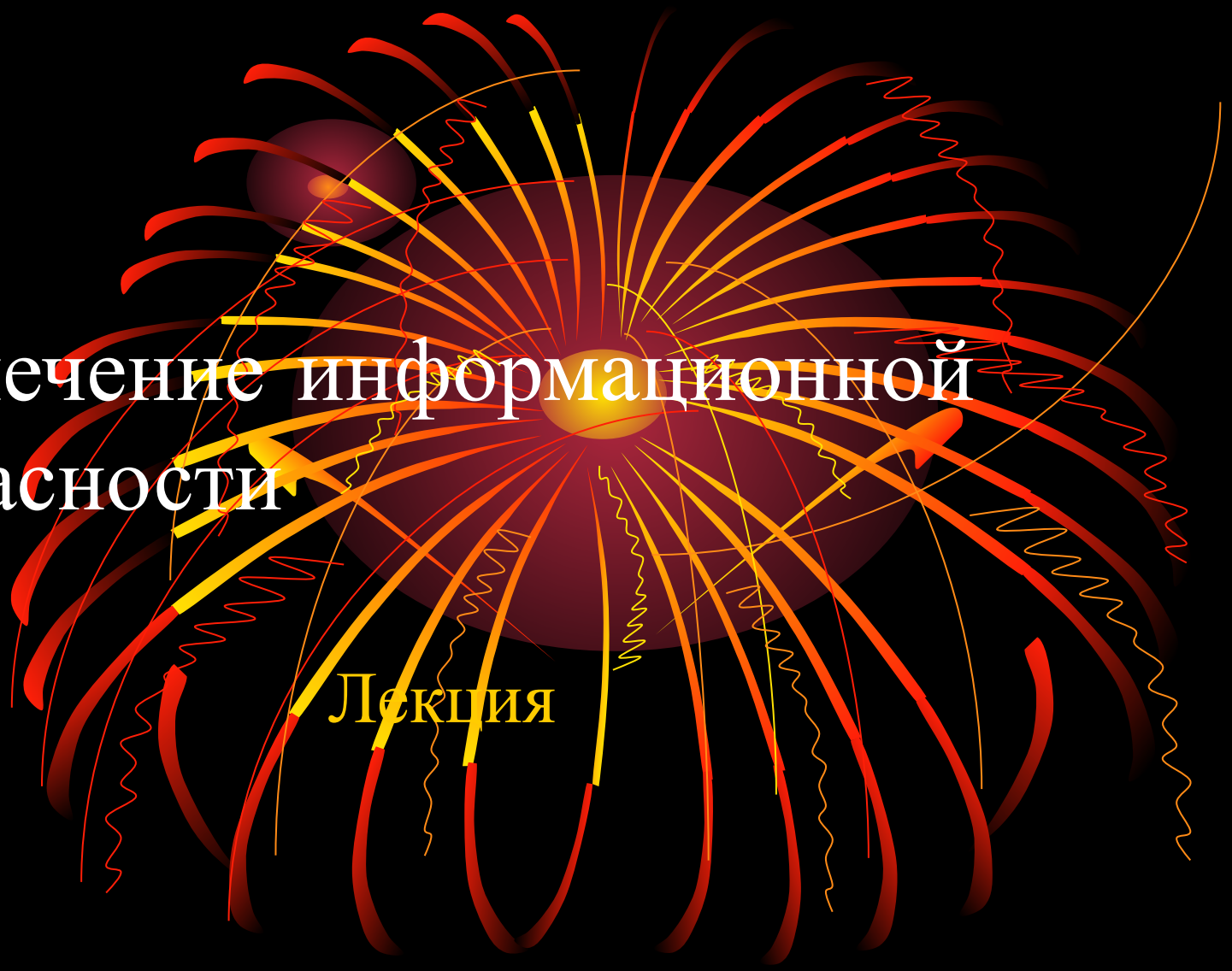
Обеспечение информационной безопасности



Лекция

Информатика часть 1 (книги, имеющиеся в библиотеке ТГАСУ)

1. Могилев А.В. Информатика/ уч. пособие//М.: Академия, 2004. - 840 с.
2. Информатика. Базовый курс / уч. пособие под ред. С. В.Симонович// СПб.: 2002. - 640с.
3. Ляхович В.Ф. Основы информатики/ Уч. пособие // Ростов-на-Дону: Феникс, 2001. - 608с.
4. Могилев А.В. и др. Практикум по информатике/ уч. пособие// М.: Академия, 2002. - 680 с.
5. Безручко В.Т. Практикум по курсу «Информатика»// М.: ФиС, 2003.-270с.

Защита информации от потери и разрушения

Потеря информации на ПК

- Нарушение работы компьютера
- Отключение и сбои питания
- Повреждение носителей информации
- Ошибочные действия пользователя
- Действие компьютерных вирусов
- Несанкционированные умышленные действия других лиц

Средства резервирования

- Программные средства, входящие в состав большинства комплектов Утилит **(Ms BackUp, Norton BackUp)**
- Создание архивов на внешних носителях информации

Восстановление данных

ОСОБЕННОСТИ УДАЛЕНИЯ ФАЙЛОВ

- Стирается первая буква имени файла
- Из **FAT** стирается информация о занятых секторах

НЕОБХОДИМО

- После удаления файла на освободившееся место не была записана новая информация
- Файл не был фрагментирован

ВОССТАНОВЛЕНИЕ

- Программы **Undelete; Unerase**

Защита от уничтожения

- Присвоить файлам атрибут **Read Only (**только для чтения**)**
- Использовать специальные программные средства для сохранения файлов после его удаления пользователем

Защита информации от несанкционированного доступа

Несанкционированный доступ – чтение, обновление или разрушение информации при отсутствии на это соответствующих полномочий

Основные пути получения несанкционированного доступа к информации

- Хищение информации и производственных кодов
- Копирование носителей информации с преодолением мер защиты
- Маскировка под зарегистрированного пользователя
- Мистификация (маскировка под запросы системы)
- Использование недостатков операционных систем и языков программирования

Основные пути получения несанкционированного доступа к информации

- Использование программных закладок и программных блоков типа «троянский конь»
- Перехват электронных излучений
- Перехват акустических излучений
- Дистанционное фотографирование
- Применение подслушивающих устройств
- Злоумышленный вывод из строя механизмов защиты
- И другие

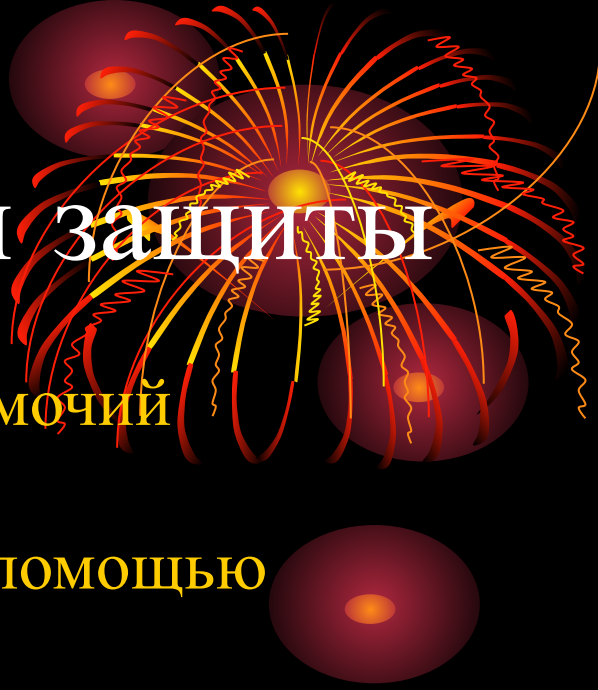
Организационные мероприятия

- Пропускной режим
- Хранение носителей и устройств в сейфе **(USB-**носители**,** монитор**,** клавиатура**)**
- Ограничение доступа лиц в компьютерные помещения

Технические средства защиты

- Фильтры и экраны на аппаратуру
- Ключ для блокировки клавиатуры
- Устройства аутентификации – для чтения отпечатков пальцев, формы руки, радужной оболочки глаза, скорости и приемов печати
- Электронные ключи на микросхемах

Программные способы защиты



- Парольный доступ – задание полномочий пользователя
- Блокировка экрана и клавиатуры с помощью комбинаций клавиш (утилиты)
- Использование средств парольной защиты **BIOS** (на **BIOS** и ПК в целом)

Криптографический способ защиты – шифрование информации при вводе в компьютер

Обеспечение защиты информации в компьютерных сетях

Дополнительные угрозы:

- Электромагнитная подсветка линий связи
- Незаконное подключение к линиям связи
- Дистанционное преодоление систем защиты
- Ошибки в коммутации каналов
- Нарушение работы линий связи и сетевого оборудования

Архитектура безопасности сетей

Под угрозой безопасности понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов сети, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства

Угрозы безопасности

- Случайные угрозы
- Умышленные угрозы

  1. пассивные **(**несанкционированное использование**)**

  2. активные **(**целенаправленное воздействие**)**

Основные угрозы безопасности

- Угрозы раскрытия конфедициальной информации
- Компрометация информации
- Несанкционирование использование ресурсов сети
- Ошибочное использование ресурсов
- Несанкционированный обмен информацией
- Отказ от информации
- Отказ в обслуживании

Службы безопасности сети

1. Аутентификация
2. Обеспечение целостности
3. Засекречивание данных
4. Контроль доступа
5. Защита от отказов

Механизмы безопасности

- Шифрование
- Механизм контроля доступа (парольный доступ, биометрические методы)
- Цифровая подпись (службы аутентификации)

Защита сетей от утечки информации

- Межсетевые экраны
- Брандмауэр – барьер между двумя сетями: внутренней и внешней, обеспечивает прохождение входящих и исходящих пакетов в соответствии с правилами, определенными администратором сети