

Департамент Здравоохранения города Москвы

ГБПОУ ДЗМ

Медицинский колледж 6

---

# ЗАЩИТА ИНФОРМАЦИИ



Выполнил: студент 116 группы  
Каххоров Бахромджон

Проверил: Гришин Г.А.

---

**Компьютеры — это технические устройства для быстрой и точной (безошибочной) обработки больших объёмов информации самого разного вида .**

# Виды и методы защиты информации

Вид защиты	Метод защиты
От сбоев оборудования	<ul style="list-style-type: none"><li>• Архивирование файлов (со сжатием или без);</li><li>• резервное копирование файлов</li></ul>
От случайной потери или искажения информации, хранящейся в компьютере	<ul style="list-style-type: none"><li>• Запрос на подтверждение выполнения команд, изменяющих файлы;</li><li>• установка специальных атрибутов документов и программ;</li><li>• возможность отмены неверного действия или восстановления ошибочно удалённого файла;</li><li>• разграничение доступа пользователей к ресурсам файловой системы</li></ul>

# Виды и методы защиты информации

Вид защиты	Метод защиты
От преднамеренного искажения, вандализма (компьютерных вирусов)	<ul style="list-style-type: none"><li>• Общие методы защиты информации;</li><li>• профилактические меры;</li><li>• использование антивирусных программ</li></ul>
От несанкционированного (нелегального) доступа к информации (её использования, изменения, распространения)	<ul style="list-style-type: none"><li>• Шифрование;</li><li>• установление паролей;</li><li>• «электронные замки»;</li><li>• совокупность административных и правоохранительных мер</li></ul>

# **АРХИВИРОВАНИЕ ФАЙЛОВ**

## **РЕЗЕРВНОЕ КОПИРОВАНИЕ**

---

- создание простой резервной копии;
- создание копии с предварительным сжатием (компрессией) используются специальные программы-архиваторы (WinRar, 7zip и др.);

**Архиватор — компьютерная программа, которая осуществляет сжатие данных в один файл архива для более легкой передачи, или компактного их хранения.**

- при использовании программ автоматического резервного копирования команда данные дублируется на автономный носитель (например, на винчестер). Выход из строя одного из них не приводит к потере информации. Резервное копирование файлов широко используется, в банковском деле.

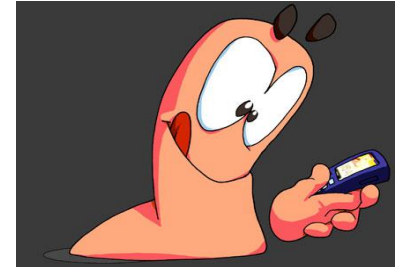
# КОМПЬЮТЕРНЫЙ ВИРУС



— программа ЭВМ, способная без ведома пользователя и вопреки его желанию самопроизвольно размножаться и распространяться, нарушая работоспособность программного обеспечения ЭВМ (отсюда его название по аналогии с болезнетворным вирусом). К. в. впервые появился в начале 1980-х гг. в США.

УК РФ впервые в отечественной практике установил уголовную ответственность за создание, использование и распространение вредоносных программ для ЭВМ (ст. 273). Наказуемым является "создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами".

# КОМПЬЮТЕРНЫЙ ЧЕРВЬ



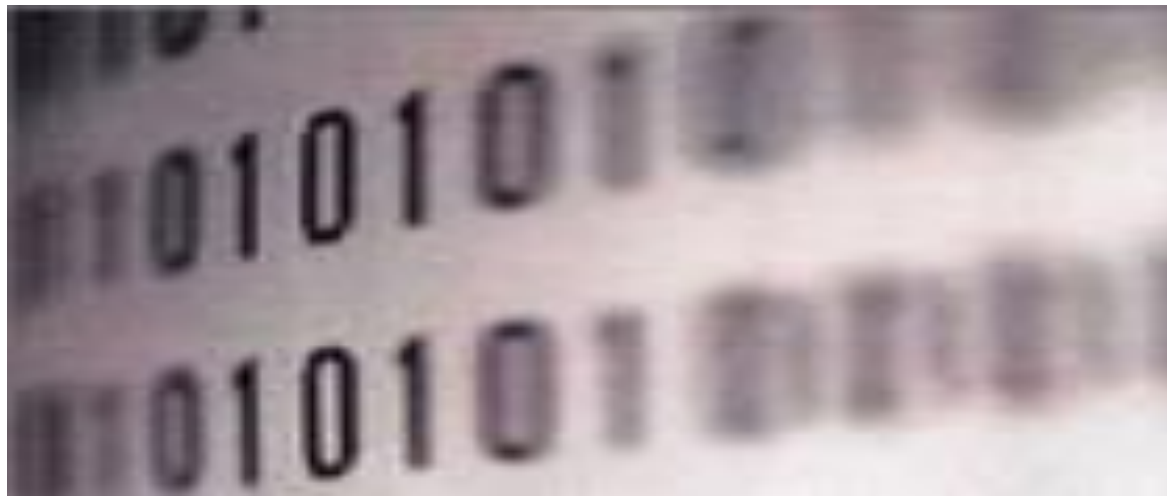
**Компьютерный червь — это программа, разработанная таким образом, чтобы копировать себя с одного компьютера на другой без участия человека. В отличие от компьютерных вирусов черви могут копировать себя автоматически.**

**Черви могут размножаться в больших количествах. Например, червь может отправлять копии себя каждому контакту из адресной книги электронной почты и затем отправлять себя всем контактам из их адресных книг электронной почты.**

# ШИФРОВАНИЕ

---

Шифрование — способ преобразования открытой информации в закрытую и обратно. Применяется для хранения важной информации в ненадёжных источниках или передачи её по незащищённым каналам связи





# ПАРОЛИ

---

**Пароль (фр. parole — слово) — это секретное слово или набор символов, предназначенный для подтверждения личности или полномочий. Пароли часто используются для защиты информации от несанкционированного доступа. В большинстве вычислительных систем комбинация «имя пользователя — пароль» используется для удостоверения пользователя.**



# Ответственность за преступления в области информационных технологий

---

Составы компьютерных преступлений (перечень признаков, характеризующих общественно опасное деяние как конкретное преступление) приведены в главе 28 Уголовного Кодекса РФ (введён в действие 1.1.1997 г.), которая называется “Преступление в сфере компьютерной информации” и содержит 3 статьи:

“Неправомерный доступ к компьютерной информации” (ст. 272);

*Статья 272 предусматривает ответственность за несанкционированный доступ, если это повлекло уничтожение, блокировку, модификацию или копирование информации, нарушение работы вычислительных систем. Обычно несанкционированный доступ осуществляется умышленно (лишение свободы до 2-х лет, и до 5-ти лет, если преступление совершено группой лиц).*

“Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273).

Статья 273. Преступление, предусмотренное ч.1 ст. 273, может быть совершено умышленно и максимальным наказанием является лишение свободы до 3-х лет.

“Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети” (ст. 274).

*Статья 274. Обычно нарушение правил эксплуатации осуществляется умышленно. Преступление наказывается лишением права занимать определённые должности или заниматься определённой деятельностью на срок до 5-ти лет.*

Ответственность за нарушения могут нести лица, достигшие 16 лет.