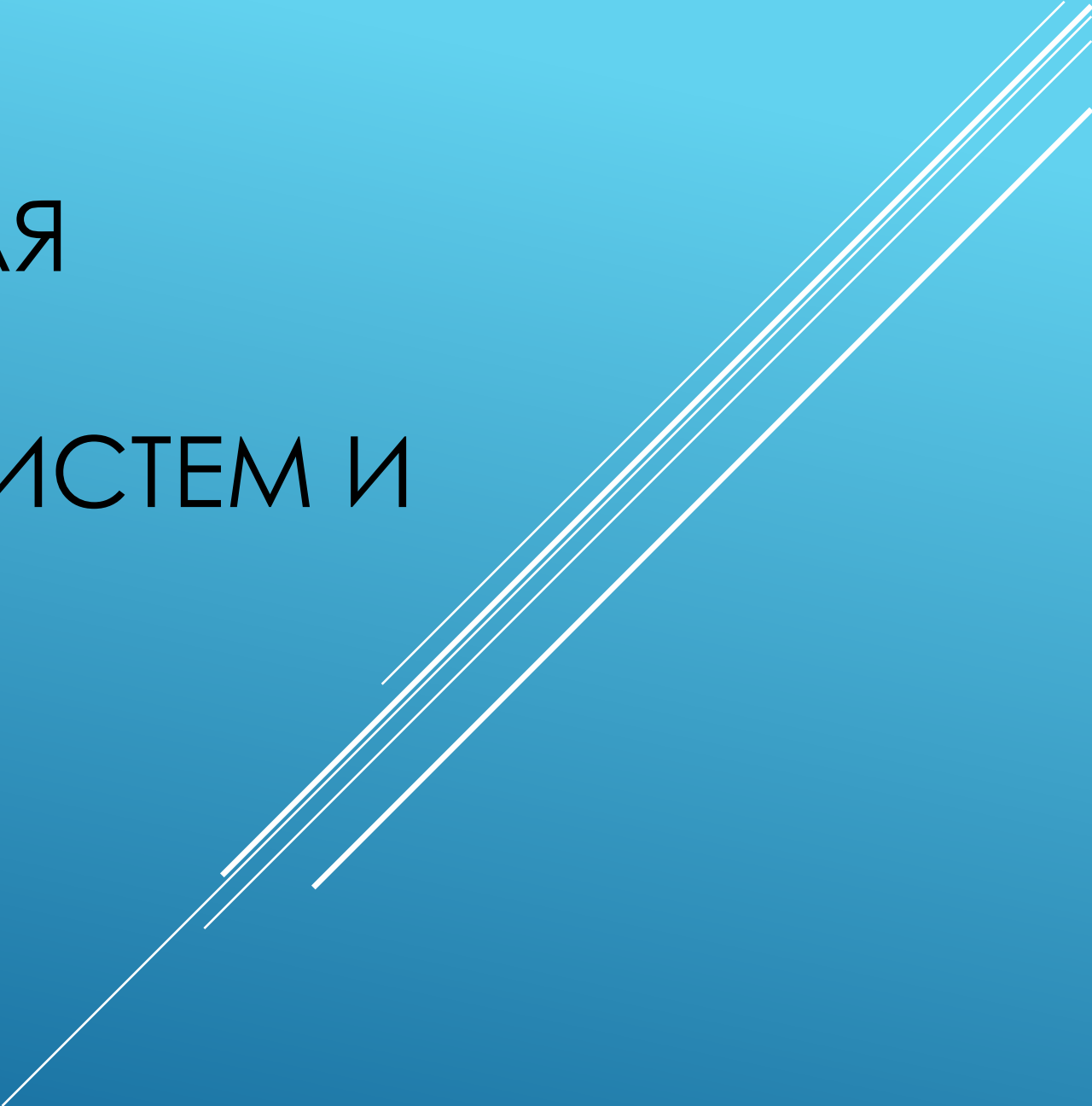


ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ
КОМПЬЮТЕРНЫХ СИСТЕМ И
СЕТЕЙ

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom-left towards the top-right, located in the lower right quadrant of the slide.

- ▶ Компьютерные вирусы одна из главных угроз информационной безопасности. Это связано с масштабом распространения этого явления и, как следствие, огромного ущерба, наносимого информационным системам.
- ▶ Современный компьютерный вирус – это практически незаметный для обычного пользователя "враг", который постоянно совершенствуется, находя все новые и более изощренные способы проникновения на компьютеры пользователей.
- ▶ Необходимость борьбы с компьютерными вирусами обусловлена возможностью нарушения ими всех составляющих информационной безопасности.
- ▶ Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации.
- ▶ Вирусные эпидемии способны блокировать работу организаций и предприятий.

КОМПЬЮТЕРНЫЕ ВИРУСЫ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

- ▶ Основная особенность компьютерных вирусов, заключающаяся в возможности их самопроизвольного внедрения в различные объекты операционной системы, – присуща многим программам, которые не являются вирусами, но именно эта особенность является обязательным (необходимым) свойством компьютерного вируса.
- ▶ Приведем одно из общепринятых определений вируса, содержащееся в ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения".
- ▶ **Программный вирус** – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.

- ▶ Несмотря на все усилия разработчиков антивирусного программного обеспечения до сегодняшнего дня нет достаточно надежных антивирусных средств и, скорее всего, противостояние "вирусописателей" и их оппонентов будет постоянным.
- ▶ Исходя из этого, необходимо понимать, что нет достаточных программных и аппаратных средств защиты от вирусов, а надежная защита от вирусов может быть обеспечена комплексным применением этих средств и, что немаловажно, соблюдением элементарной "компьютерной гигиены".

- ▶ К внешним признакам компьютерного вируса, позволяющим его обнаружить, можно отнести следующие:
 - вывод на экран непредусмотренных сообщений или изображений;
 - подача непредусмотренных звуковых сигналов;
 - изменение даты и времени модификации файлов;
 - исчезновение файлов и каталогов или искажение их содержимого;
 - частые зависания и сбои в работе компьютера;
 - невозможность загрузки ОС;
 - существенное уменьшение размера свободной оперативной памяти;
 - прекращение работы или неправильная работа ранее успешно функционировавших программ;
 - изменение размеров файлов;
 - неожиданное значительное увеличение количества файлов на диске.

- ▶ Однако следует заметить, что перечисленные выше явления необязательно вызываются действиями вируса, они могут быть следствием и других причин.
- ▶ Поэтому правильная диагностика состояния компьютера всегда затруднена и обычно требует привлечения специализированных программ.
- ▶ Для эффективной антивирусной защиты важно понимание путей проникновения вирусов в компьютеры

► Рассмотрим основные пути проникновения вирусов в компьютеры пользователей:

1. Глобальные сети – электронная почта и т.д..
 2. Электронные конференции, файл-серверы ftp.
 3. Пиратское программное обеспечение.
 4. Локальные сети.
 5. Персональные компьютеры "общего пользования".
 6. Сервисные службы
- И др.

ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

Глобальные сети – электронная почта

- ▶ Основным источником вирусов на сегодняшний день является глобальная сеть Интернет, такова расплата за возможность доступа к массовым информационным ресурсам и службам.
- ▶ Наибольшее число заражений вирусом происходит при обмене электронными письмами через почтовые серверы E-mail.

Локальные сети

- ▶ Другой путь "быстрого заражения" – локальные сети.
- ▶ Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или несколько служебных файлов на сервере.
- ▶ Далее пользователи при очередном подключении к сети запускают зараженные файлы с сервера, и вирус, таким образом, получает доступ на компьютеры пользователей.

Персональные компьютеры "общего пользования"

- ▶ Опасность представляют также компьютеры, установленные в учебных заведениях. Если один из студентов принес на своих дискетах вирус и заразил какой-либо учебный компьютер, то очередной вирус будет гулять по всему учебному заведению, включая домашние компьютеры студентов и сотрудников.

Пиратское программное обеспечение

- ▶ Нелегальные копии программного обеспечения, как это было всегда, являются одной из основных "зон риска". Часто пиратские копии, скачиваемые из Интернет или распространяемые на CD-дисках или флешках содержат файлы, зараженные самыми разнообразными типами вирусов.
- ▶ Необходимо помнить, что низкая стоимость программы может дорого обойтись при потере данных.

Сервисные службы

- ▶ Достаточно редко, но до сих пор вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре в сервисных центрах.

СПАСИБО ЗА ВНИМАНИЕ!

The image features a solid blue background. In the center, the text "СПАСИБО ЗА ВНИМАНИЕ!" is written in a bold, white, sans-serif font. To the right of the text, there are several thin, white, parallel lines that originate from the bottom right and extend towards the top right corner, creating a sense of movement and modern design.