**Технологии и методы защиты от кибератак и вредоносных программ**

С ростом использования цифровых технологий увеличивается и количество кибератак, что делает безопасность данных чрезвычайно важной темой. В этой части презентаций студенты могут сосредоточиться на следующих аспектах:

- Типы кибератак и вредоносных программ: необходимо описать основные формы угроз, такие как вирусы, трояны, фишинг, DDoS-атаки и ransomware. Студенты могут также включить примеры крупных кибератак за последние годы.

- Антивирусные программы и их функции: объяснение основ работы антивирусного ПО, сканирования и методов удаления угроз. Обзор популярных антивирусных решений от компаний, таких как McAfee, Norton и Kaspersky.

- Брандмауэры и системы предотвращения вторжений (IPS): как эти механизмы помогают защитить сети от несанкционированного доступа и аномальной активности.

- Шифрование данных: обсуждение методов шифрования данных как одного из наиболее надежных способов защиты конфиденциальной информации при передаче и хранении.

- Аутентификация и управление доступом: использование двухфакторной аутентификации и биометрических данных для повышения безопасности доступа к системе.

- Обучение пользователей и создание культуры кибербезопасности: значение информированности пользователей об угрозах и мерах предосторожности, включая регулярное обновление ПО и осторожность при открытии писем из неизвестных источников.

В заключение, подготовка презентаций на эти темы позволяет студентам сформировать широкое представление как об истории и текущих трендах в области производства ЭВМ, так и о важности и методах обеспечения информационной безопасности. Это способствует не только развитию исследовательских и аналитических навыков, но и повышению их квалификации как будущих специалистов в области информационных технологий.