Кибербезопасность: методы защиты информации в цифровом мире

Клесова Ксения и Белоусова Анжелика ИСП-42 .
Автономное некоммерческое образовательная организация среднего образования Центросоюза Российской Федерации "Сибирский университет потребительской кооперации" города Новосибирск .
Руководитель Верченева Наталия Анатольевна, преподаватель кафедры информатика

ЦЕЛЬ

Рассказать о кибербезопасности и методах защиты информации в цифровом мире

ЗАДАЧИ

- Узнать о наиболее распространенных видах кибератаках
- Выяснить как скорость развития технологий влияет на кибербезопасность
- Познакомиться с защитой информации от кибератаках

Актуальность

Актуальность исследования в области кибербезопасности связана с ростом числа и сложности кибератак, развитием технологий, создающих новые уязвимости, а также влиянием человеческого фактора на безопасность. Кибератаки могут привести к значительным финансовым потерям для организаций и требуют соблюдения ужесточенных законодательных норм. Кроме того, глобальные угрозы подчеркивают необходимость международного сотрудничества для

защиты критической инфраструктуры. **Таким образом,** исследование кибербезопасности является важным для обеспечения защиты информации и повышения устойчивости организаций.

Проблема

Проблема кибербезопасности заключается в увеличении числа и разнообразия кибератак, усложнении технологий и систем, человеческом факторе (ошибки пользователей и социальная инженерия), быстром развитии технологий, отсутствии единых стандартов безопасности, а также значительных экономических последствиях для организаций. Эти факторы создают постоянные вызовы для защиты информации и требуют постоянного внимания и ресурсов.

Самые распространенные виды кибератак

1. Системы удаленного управления (RAT):
Вредоносное ПО, которое позволяет злоумышленникам контролировать зараженные устройства удаленно и получать доступ к конфиденциальной информации
2. Фишинг:
Один из самых популярных методов, при котором злоумышленники отправляют поддельные электронные письма или сообщения, чтобы обманом заставить пользователей раскрыть личные данные, такие как пароли или номера кредитных карт.
2. Вредоносное ПО (Malware):
Включает вирусы, черви, трояны и шпионские программы. Эти программы могут повреждать системы, красть данные или предоставлять злоумышленникам доступ к компьютерам

Для защиты от кибератак нужны:

- *Технические средства: антивирусы, фаерволы, системы обнаружения вторжений, шифрование данных.*
- *Программное обеспечение: обновления, инструменты для управления доступом и мониторинга сети.*
- *Человеческие ресурсы: специалисты по кибербезопасности и обучение сотрудников.*
- *Политики и процедуры: правила безопасности, регулярные аудиты и планы реагирования на инциденты.*
- *Финансовые ресурсы: бюджет на технологии и обучение.*

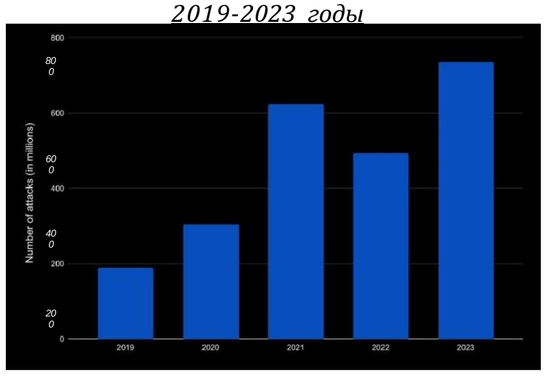
*Кибератака — это преднамеренное действие, направленное на нарушение работы компьютерных систем или сетей с целью получения несанкционированного доступа к данным или причинения вреда. Она может включать фишинг, вредоносное ПО и DDoS-атаки, что приводит к серьезным последствиям для организаций и пользователей.

Что такое кибербезопасность?

Кибербезопасность — это комплекс мер, технологий и процессов, направленных на защиту компьютерных систем, сетей и данных от несанкционированного доступа, атак, повреждений или кражи. Она включает в себя защиту информации как в цифровом виде, так и в процессе ее передачи, а также обеспечение конфиденциальности, целостности и доступности данных.

КРУГОВАЯ ДИАГРАММА ПО ЦЕЛЯМ КИБЕРПРЕСТУПНИКОВ

Гистограмма по количеству атак программ - вымогателей за 2019-2023 годы



Влияние скорости развития технологий на кибербезопасность

Скорость развития технологий значительно влияет на кибербезопасность. С одной стороны, новые технологии могут создавать уязвимости и расширять поверхность атаки, увеличивая количество точек входа для злоумышленников. Автоматизация атак делает их более эффективными, в то время как сложность современных систем затрудняет защиту. Однако одновременно с этим развиваются и средства защиты, такие как системы

обнаружения вторжений и машинное обучение. Быстрое внедрение облачных технологий также вносит новые риски, требующие дополнительных мер безопасности. В итоге, организации должны быть проактивными и постоянно адаптироваться к изменениям в технологическом ландшафте, чтобы эффективно противостоять новым угрозам.