**Лекция №1: Кибербезопасность**

### Цель лекции: сформировать у студентов базовые знания о кибербезопасности, ее принципах, угрозах и способах защиты информации, а также показать значимость кибербезопасности в современных условиях цифровизации и развития информационных технологий.

**Кибербезопасность** – это реализация мер по защите систем, сетей и программных приложений от цифровых атак. Такие атаки обычно направлены на получение доступа к конфиденциальной информации, ее изменение и уничтожение, на вымогательство у пользователей денег или на нарушение нормальной работы компаний.

Реализация мер эффективной кибербезопасности в настоящее время является достаточно сложной задачей, так как сегодня существует гораздо больше устройств, чем людей, а злоумышленники становятся все более изобретательными.

Какие принципы лежат в основе кибербезопасности?

Успешный подход в сфере кибербезопасности выражается в виде многоуровневой защиты, охватывающей компьютеры, сети, программы или данные, которые необходимо обезопасить. Сотрудники, рабочие процессы и технологии должны дополнять друг друга в организациях, чтобы обеспечить эффективную защиту от кибератак.

Кибербезопасность — это сравнительно новая область, хотя криптография намного ее старше. Криптография появилась около тысячи лет назад, а возможно, и раньше, и ее цель — скрыть информацию, то есть сделать ее понятной только отправителю и получателю. В современном цифровом мире все инфраструктуры связаны через интернет, и в результате возникла новая угроза, бороться с которой призвана кибербезопасность.

В сфере кибербезопасности принимают участие две стороны: киберпреступники и киберзащитники. У них примерно один уровень технических знаний, то есть стороны в этом противостоянии равны. Зачастую те, кто проводит атаку, обладают теми же знаниями, что и защитники. Наиболее очевидная цель атаки — получить информацию, которая не должна быть обнародована, то есть она должна быть известна только отправителю и получателю. Этой очевидной областью занимается криптография — кодирование и декодирование информации, которое сегодня происходит при помощи очень сложных вычислительных процедур. Это не значит, что такую информацию нельзя дешифровать, но на это уйдет много времени. Так работает защита: большое количество времени, нужное для вычислений, обеспечивает безопасность информации.

**Сотрудники**

Пользователи должны понимать и соблюдать основные принципы информационной безопасности, такие как выбор надежных паролей, внимательное отношение к вложениям в электронных письмах и резервное копирование данных. Дополнительная информация об [основных принципах кибербезопасности](https://umbrella.cisco.com/blog/2013/10/08/top-ten-important-cyber-security-tips-users/).

**Процессы**

В организации должен быть разработан набор базовых мер по противодействию предпринимаемым и успешно осуществленным атакам. Можно руководствоваться одним [надежным набором мер](https://blogs.cisco.com/security/cisco-and-the-nist-cybersecurity-framework-benefit-from-a-fresh-and-innovative-approach-to-cybersecurity). В этом наборе мер должно объясняться, как определять атаки, защищать системы, выявлять угрозы и противодействовать им, а также восстанавливать работоспособность после осуществленных атак. Посмотреть видео ролик с объяснениями о [пакете решений для кибербезопасности NIST.](https://video.cisco.com/detail/videos/education/video/5155119533001/cisco-and-the-nist-cybersecurity-framework?autoStart=true)

**Технологии**

Технологии являются важнейшим элементом, предоставляющим организациям и отдельным пользователям инструменты, необходимые для защиты от кибератак. Основными компонентами, которые необходимо защитить, являются оконечные устройства, например, компьютеры, интеллектуальные устройства и маршрутизаторы; сети и облачная среда. К наиболее распространенным технологиям, используемым для защиты перечисленных компонентов, относятся межсетевые экраны нового поколения, фильтрация DNS, защита от вредоносного ПО, антивирусное ПО и решения для защиты электронной почты.

**Почему кибербезопасность так важна?**

В современном «подключенном» мире программы расширенной киберзащиты служат на благо каждого пользователя. На индивидуальном уровне атака со взломом киберзащиты может привести к разнообразным последствиям, начиная с кражи личной информации и заканчивая вымогательством денег или потерей ценных данных, например, семейных фотоснимков. Все зависят от критически важной инфраструктуры, например, электростанций, больниц и компаний, предоставляющих финансовые услуги. Защита этих и других организаций важна для поддержания жизнедеятельности нашего общества.

Все получают пользу от исследования киберугроз, которым занимаются специалисты по киберугрозам, например, 250 специалистов из команды Talos, изучающие новые и появляющиеся угрозы, а также стратегии кибератак. Они выявляют новые уязвимости, информируют общественность о важности кибербезопасности и повышают надежность инструментов с открытым программным кодом. Работа этих специалистов делает Интернет более безопасным для каждого пользователя.

# Расширенная защита от вредоносных программ для безопасности электронной почты

## Блокировать атаки по электронной почте

Более 100 миллиардов корпоративных писем обмениваются каждый день. Как и ожидалось, электронная почта стала основным средством для кибератак.

Вопросов для закрепления материала**:**

1. Что такое кибербезопасность и какие задачи она решает?
2. Какие принципы лежат в основе кибербезопасности? Объясните каждый из них.
3. Почему реализация эффективной кибербезопасности в современных условиях является сложной задачей?
4. Как криптография связана с кибербезопасностью? Что такое шифрование и как оно помогает защитить информацию?
5. Какие стороны участвуют в противостоянии киберугроз? Какое у них соотношение знаний и навыков?
6. Какие меры необходимо соблюдать пользователям для обеспечения безопасности своей информации?
7. Как организации могут противодействовать кибератакам и какие меры для этого должны быть разработаны?
8. Какие основные технологии применяются для защиты информационных систем от кибератак?
9. Почему кибербезопасность так важна для защиты критической инфраструктуры, такой как электростанции и больницы?
10. Как специалисты по киберугрозам помогают улучшать безопасность интернета и каких методов они используют для выявления угроз?
11. Какие проблемы могут возникнуть при использовании электронной почты в контексте кибербезопасности?