КОНФИДЕНЦИАЛЬНОСТЬ И ЭТИКА

Курс лекций

Лекция 9. Киберпреступность и киберпреступления

- Киберпреступность: история зарождения, определение, причины роста
- Типы киберпреступлений
- Преступления против кибербезопасности КР
- Киберпреступник: портрет

Киберпреступность

- Термин **«компьютерная преступность»** появился в **1979 году** на Конференции Американской ассоциации адвокатов в г.Даллас, когда были выявлены первые преступления, совершенные с использованием ЭВМ и сформулированы основные признаки компьютерных преступлений

Основные признаки компьютерных преступлений -1979 год

- использование или попытка использования компьютера, вычислительной системы или сети компьютеров с целью получения денег, собственности или услуг, под прикрытием фальшивых предлогов или ложных обещаний, либо выдавая себя за другое лицо;
- преднамеренное несанкционированное действие, имеющее целью изменение, повреждение, уничтожение или похищение компьютера, вычислительной системы, сети компьютеров или содержащихся в них систем математического обеспечения, программ или информации;
- преднамеренное несанкционированное нарушение связи между компьютерами, вычислительными системами или сетями компьютеров.

Киберпреступность

- Началом киберпреступности можно считать преступление, официально зарегистрированное Международной организацией уголовной полиции «Интерпол», совершенное в 1979 г. в г. Вильнюсе. Оператор почтовой связи Н. путем мошенничества с использованием автоматизированного программнотехнического комплекса «Онега» в течение двух лет совершала хищение денежных средств, направляемых государственными органами гражданам в качестве пенсий и пособий по старости. Одновременно с компьютерной осуществлялась обработка бумажных бухгалтерских документов. Несовершенство программного обеспечения «Онеги» и ведение бухгалтерии на различных носителях позволили Н. длительное время создавать излишки подотчетных денежных средств, изымать их из кассы, присваивать и некоторое время уходить от ответственности.

Киберпреступность

- это любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети *(Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями)*

Киберпреступность: понятие

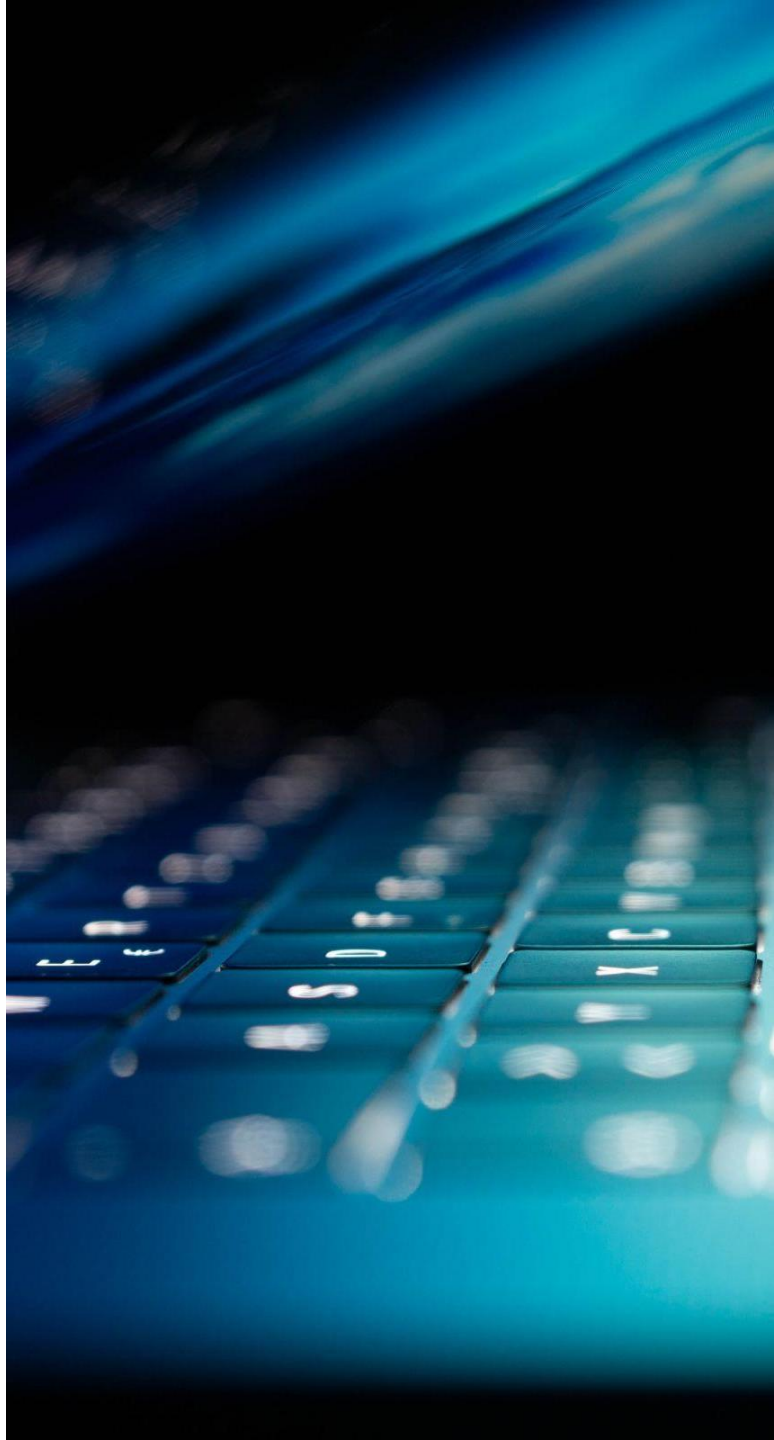
- это незаконные, противоправные действия, которые осуществляются людьми, использующими информационно-телекоммуникационные технологии, компьютеры и компьютерные сети для преступных целей
- это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство
- под киберпреступлением, а равно под преступлением в сфере информационных технологий следует понимать совокупность преступлений, совершаемых с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба, индивиду, организации или государству

Киберпреступность: причины роста

- быстрое освоение и внедрение в свою противозаконную деятельность киберпреступниками новых технологий;
- увеличение числа пользователей Интернета (как правило, из стран с низкими доходами и со слабой общей кибербезопасностью);
- возрастающая простота совершения киберпреступлений, связанная с ростом доступности киберпреступности как сервиса, в рамках которого киберпреступники предлагают ресурсы и приложения за вознаграждение, выступая тем самым в роли пособников;

Киберпреступность: причины роста

- увеличение количества центров киберпреступности, которые теперь включают Бразилию, Индию, Северную Корею и Вьетнам;
- повышение финансовой грамотности злоумышленников верхнего уровня, что среди прочего упрощает монетизацию данных, добытых преступным путем. Монетизация похищенных данных, которая всегда была проблемой для киберпреступников, стала менее сложной в связи с развитием черных рынков и использованием криптовалют.



Типы киберпреступлений:

- Мошенничество с использованием электронной почты и Интернета
- Кража цифровой личности (хищение и использование личных данных)
- Кража данных платежных карт и другой финансовой информации
- Хищение и перепродажа корпоративных данных
- Кибершантаж / атаки с использованием программ-вымогателей (вымогательство денег под угрозой атаки)
- Криптоджекинг (майнинг криптовалют с использованием чужих ресурсов)

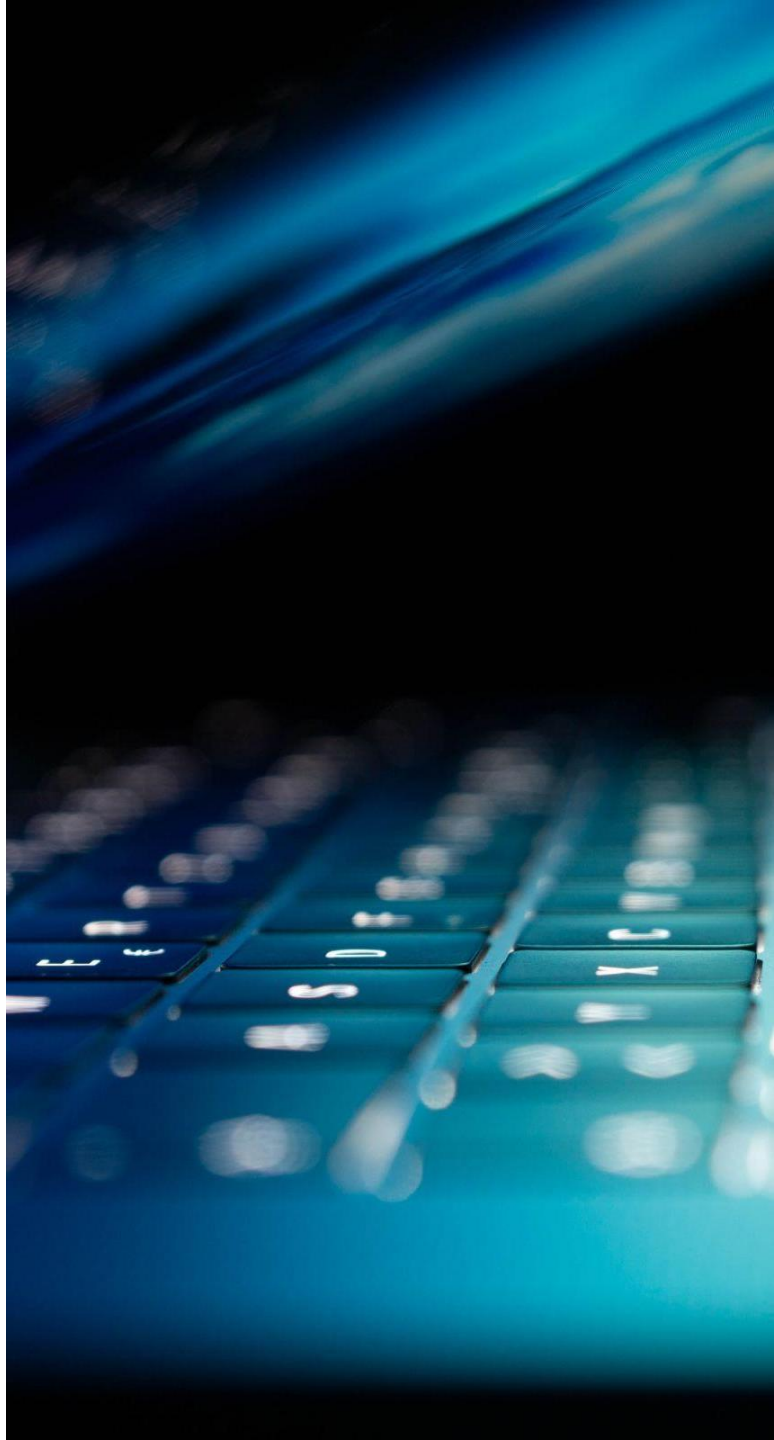
Типы киберпреступлений:

- Кибершпионаж (получение несанкционированного доступа к государственным или корпоративным данным)
- Нарушение работы систем с целью компрометации сети
- Нарушение авторских прав
- Незаконное проведение азартных игр
- Онлайн-торговля запрещенными товарами
- Домогательства, изготовление или хранение детской порнографии

Киберпреступность: данные

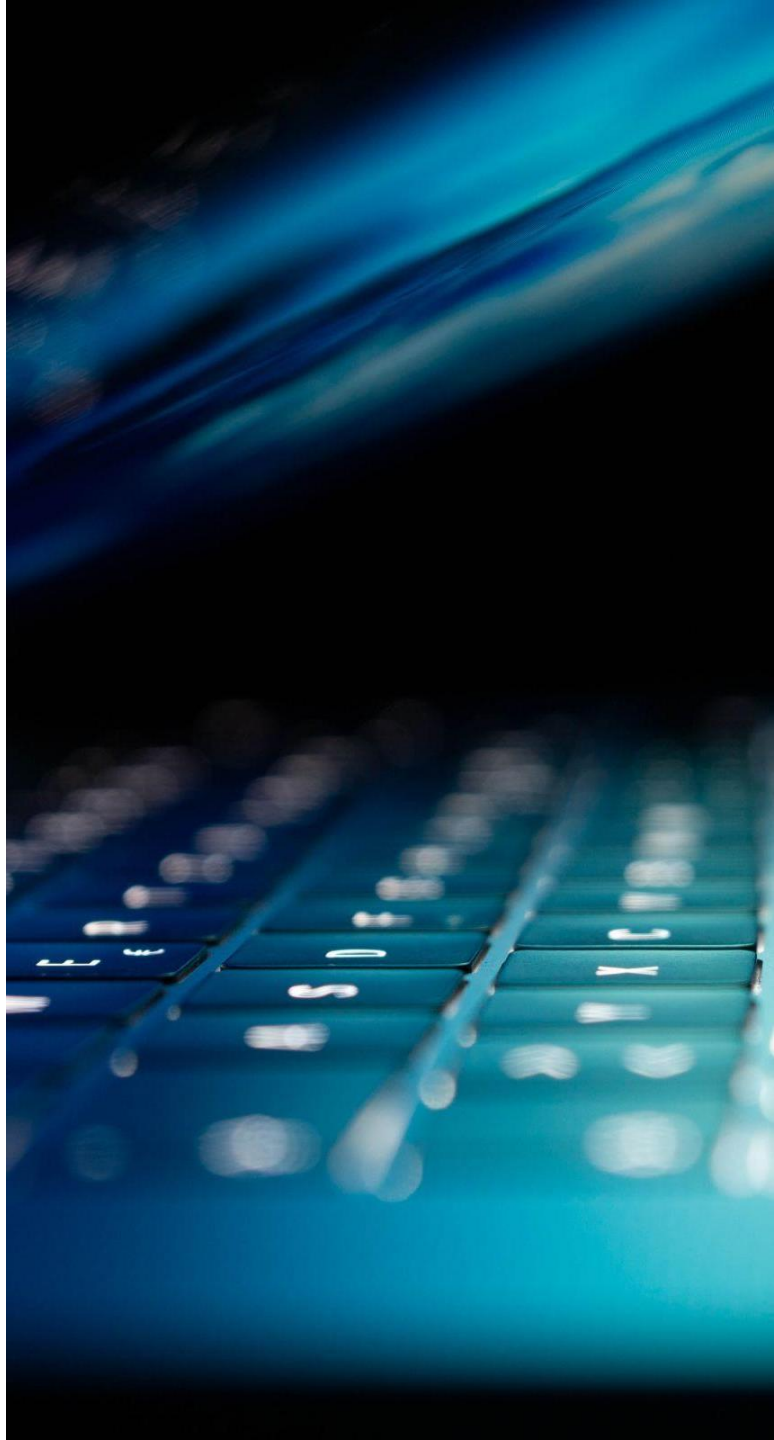
Прогноз на 2024 год глобального ущерба от киберпреступности:

- 8 триллионов долларов в год
- 153.84 миллиарда долларов в неделю
- 21.9 миллиарда долларов в день
- 913.24 миллиона долларов в час
- 15.2 миллиона долларов в минуту



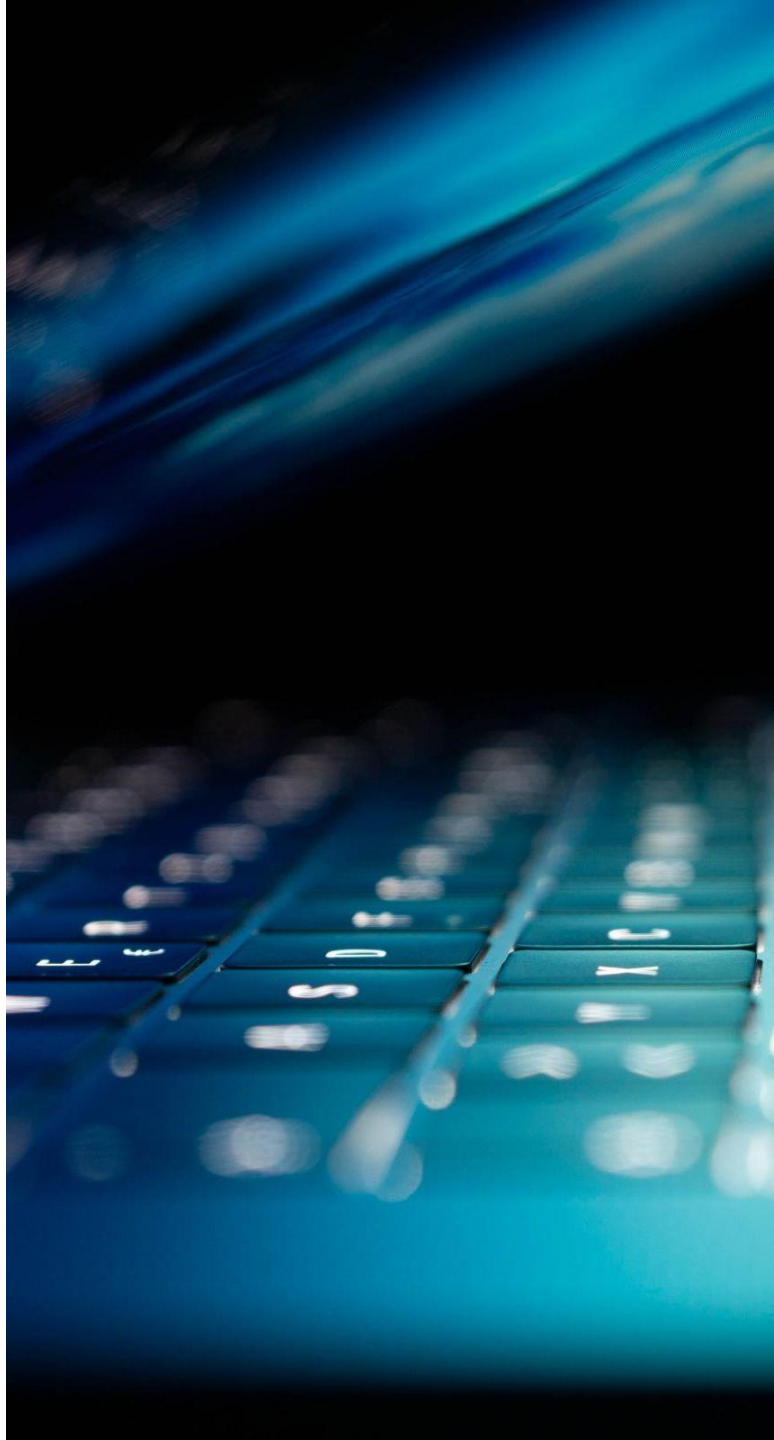
Киберпреступность: данные

с июля 2019 г. по июнь 2020 г. поступило 59,806 сообщений о киберпреступлениях (зарегистрированных преступлений, а не взломов), что в среднем составляет **164 киберпреступления в день или примерно одно каждые 10 минут**



Киберпреступность: данные

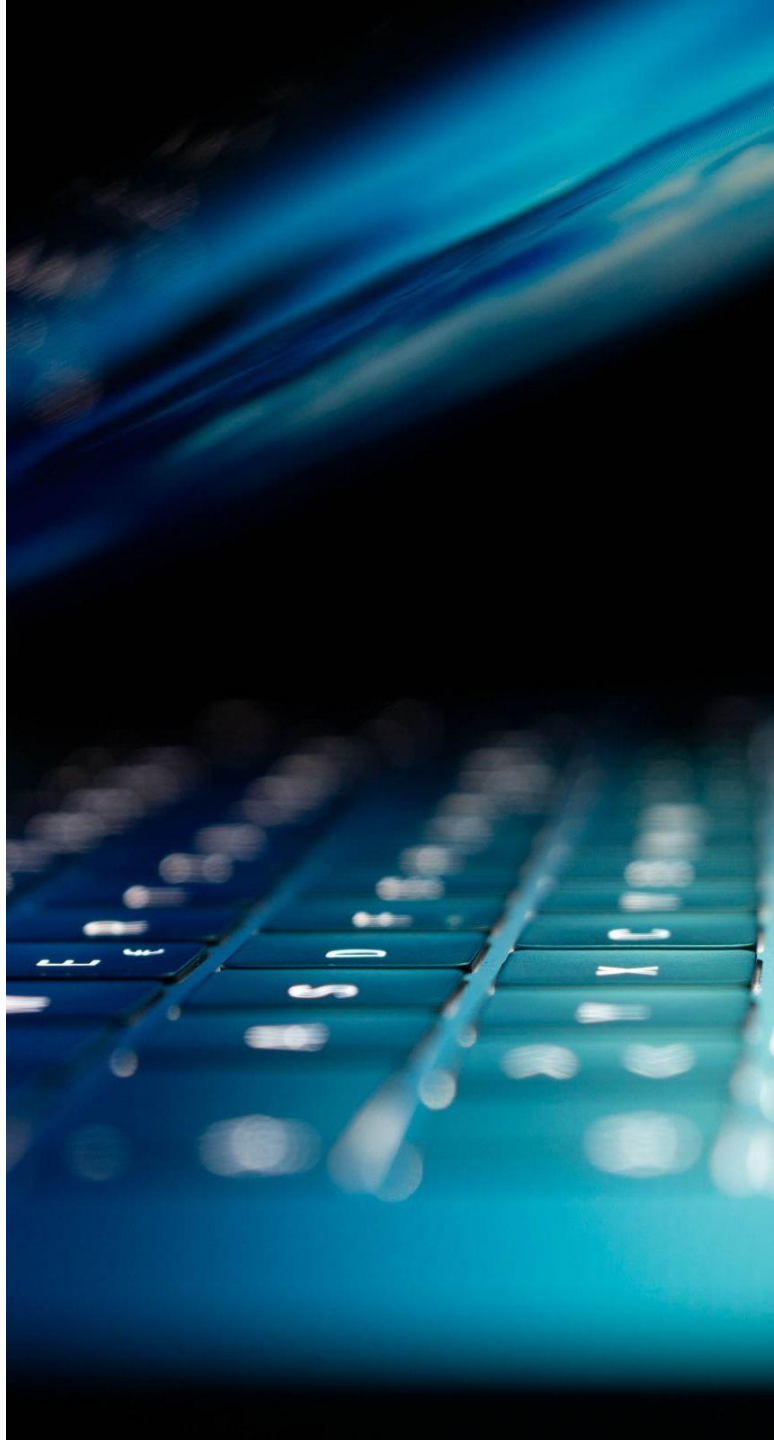
Массовое увеличение вредоносных URL-адресов на 61% с 2022 по 2023 год соответствует **255 миллионов фишинговых атак.**
Было обнаружено, что 76% этих атак были связаны со сбором учетных данных, что является основной причиной нарушений
Домены .com по-прежнему лидируют, когда речь идет о подделке в целях фишинга.
54% фишинговых писем содержали ссылки .com, а 8.9% — ссылки .net.
Наиболее часто используемые бренды для фишинга: **LinkedIn (52%), DHL (14%), Google (7%), Microsoft (6%) и FedEx (6%).**



Киберпреступность: данные

Ежедневно совершалось 1.7 млн атак с использованием программ-вымогателей, что означает, что в 2023 году было совершено 620 млн атак с использованием программ-вымогателей.

Программы-вымогатели — это **тип вредоносного ПО, которое заражает компьютер пользователя и ограничивает доступ к устройству или его данным, требуя денег в обмен на их освобождение** (с использованием криптовалюты, потому что ее трудно отследить). Это один из самых опасных способов взлома.

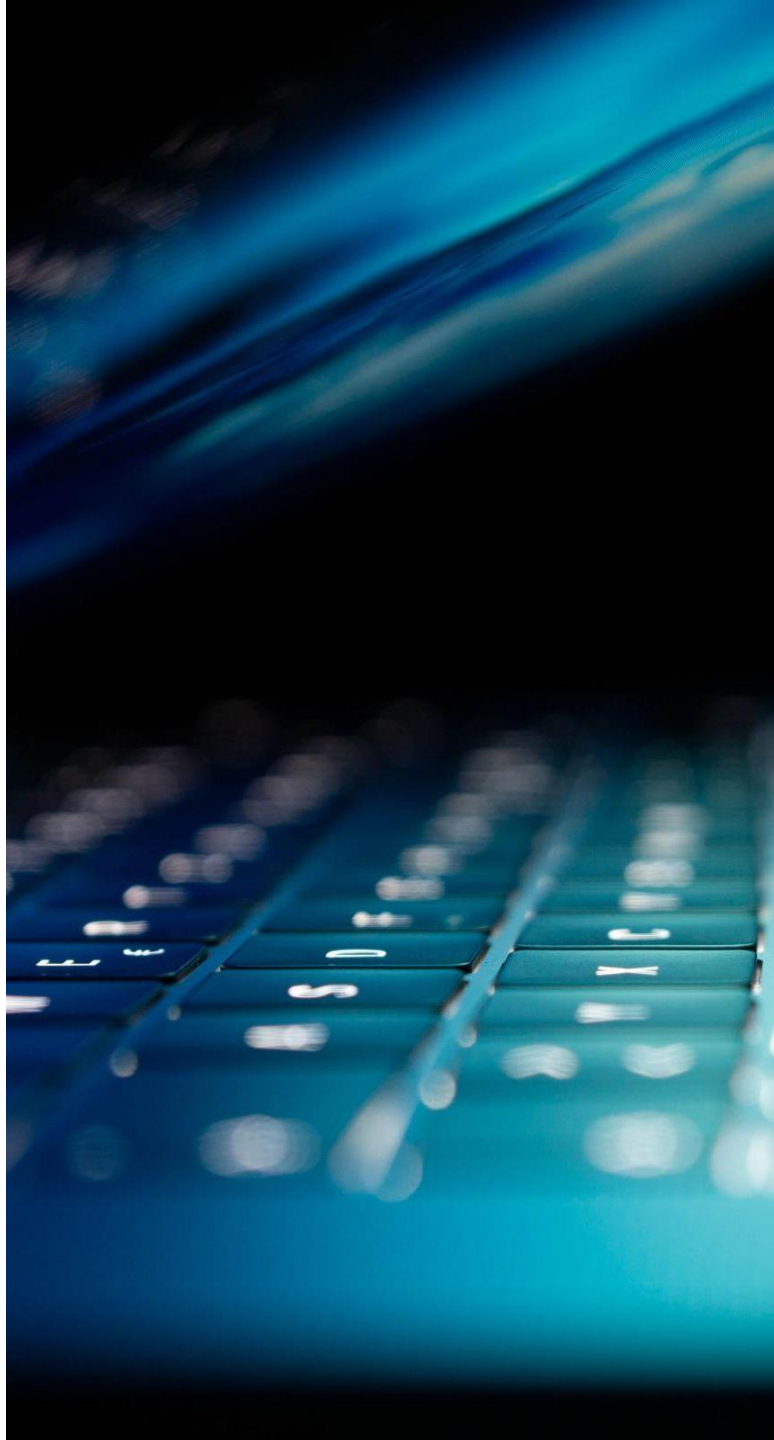


Киберпреступность: данные

Нарушение сети или данных — это самое серьезное нарушение безопасности, влияющее на устойчивость организации и ее учетные записи. Таким образом пострадали **51.5% предприятий**.

Крупнейшей утечкой данных в **2023 году** стала **утечка данных DarkBeam**, в результате которой были раскрыты **3.8 миллиарда личных записей**.

В июле 2022 года Twitter подтвердил, **что данные 5.4 миллиона учетных записей были украдены.**



Киберпреступность

- Конвенция Совета Европы о киберпреступности (Convention on Cybercrime) - принята в ноябре **2001 г.** в г.Будапешт - один из наиболее важных международно-правовых актов
- Конвенция закрепила **4 группы киберпреступлений** (позже с принятием дополнительного протокола количество групп увеличилось до пяти).

•**1 группа – Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем**

– Противозаконный доступ
– Неправомерный перехват
– Воздействие на данные
– Воздействие на функционирование системы
– Противозаконное использование устройств

Киберпреступность

- **2 группа – Правонарушения, связанные с использованием компьютерных средств**
  – Подлог с использованием компьютерных технологий
  – Мошенничество с использованием компьютерных технологий
- **3 группа – Правонарушения, связанные с содержанием данных (контентом)**
  – Правонарушения, связанные с детской порнографией
- **4 группа – Правонарушения, связанные с нарушением авторского права и смежных прав**

Киберпреступность

В начале 2002 г. к Конвенции принят Протокол, добавляющий в перечень киберпреступлений распространение с помощью информационно-телекоммуникационных технологий информации расистского и иного содержания, подстрекательство к насильственным действиям, ненависти или дискриминации отдельного лица или группы лиц на почве расовой, национальной, религиозной или этнической принадлежности

Киберпреступность

В 2000 г. на *X Конгрессе ООН* была принята следующая классификация киберпреступлений. Их разделили на две группы:

1) насильственные (угроза физической расправы, киберпреследования, детская порнография, кибертерроризм)

2) ненасильственные (противоправное нарушение владения в киберпространстве, киберворовство, кибермошенничество, реклама услуг проституции в сети Интернет, незаконный оборот наркотиков с использованием сети Интернет, отмывание денег с помощью электронного перемещения, деструктивное киберпреступление)

Киберпреступность

Предмет преступного посягательства:

a. данные пользователя или организации (логин, пароль, установочные данные)
b. денежные средства на счетах
c. конфиденциальная информация

Способ совершения преступления с:

a. применением вредоносной программы или вируса
b. использованием фишингового сайта
c. использованием банковской карты
d. использованием компьютерной техники и аппаратно-программных комплексов
e. применением фиктивных платежей
f. использованием мобильной связи
g. использованием сети интернет

Преступления против кибер-безопасности Глава 40 УК КР

Статья 319. Несанкционированный доступ к компьютерной информации и электронным документам, в информационную систему или сеть электросвязи

Несанкционированный доступ к чужой охраняемой компьютерной информации и электронным документам, в информационную систему или сеть электросвязи, повлекший уничтожение, блокирование, изменение информации, а равно повлекший нарушение или прекращение работы устройств обработки информации, причинивший умышленно или по неосторожности значительный вред

Преступления против кибер-безопасности Глава 40 УК КР

Статья 319. Несанкционированный доступ к компьютерной информации и электронным документам, в информационную систему или сеть электросвязи

3. Деяние, предусмотренное частью 1 настоящей статьи, совершенное с целью умышленного уничтожения, изменения, блокирования, приведения в непригодное состояние компьютерной информации или электронного документа либо вывода из строя, разрушения информационных систем или сети электросвязи

Преступления против кибер-безопасности Глава 40 УК КР

Статья 320. Создание вредоносных программных продуктов

Создание с целью использования либо распространения программного продукта или внесение изменений в существующие программные продукты, заведомо предназначенные для осуществления несанкционированного доступа и копирования, уничтожения, блокирования, изменения компьютерной информации и электронных документов или нейтрализации средств защиты информации, нарушения работы информационных систем или сети электросвязи, а равно умышленное использование и распространение таких программных продуктов, повлекших причинение значительного ущерба или иного значительного вреда

Преступления против кибер-безопасности Глава 40 УК КР

Статья 321. Кибер-саботаж

Кибер-саботаж, то есть умышленные изменение, уничтожение, блокирование, приведение в непригодное состояние информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций или программы без права вмешательства в работу компьютерных систем, с намерением помешать функционированию программных продуктов или телекоммуникационных систем, а также вывод из строя программных продуктов, оборудования

Преступления против кибер-безопасности Глава 40 УК КР

Статья 322. Массовое распространение электронных сообщений

Массовое распространение электронных сообщений, осуществленное без предварительного согласия адресатов, приведшее к нарушению или прекращению работы программных продуктов, телекоммуникационных систем, оборудования и абонентских терминалов

Типичный киберпреступник?

- Возраст колеблется от 15 до 45 лет
- Свыше 80 % - мужчины
- Больше половины - имеют высшее образование

Группы компьютерных преступников:

- 1) лица, для которых характерно соединение профессионализма в отрасли компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности («идейные» преступники)
- 2) лица, которые страдают различными психическими заболеваниями, затрудняющими общение в реальном мире и вынуждающими их фокусироваться на мире виртуальном, в котором им проще общаться и самоутверждаться
- 3) профессиональные компьютерные преступники

Задания для самостоятельной работы:

Письменно в тетради для СРС заданий

- Выписать характеристику каждого вида киберпреступления, согласно Конвенции ЕС о киберпреступности

ДЕДЛАЙН: двенадцатое семинарское занятие