

КИБЕРПРЕСТУПЛЕНИЯ:

ПОНЯТИЕ И ОТВЕТСТВЕННОСТЬ

ноябрь, 2021 года



ПРАВОВАЯ ONLINE ШКОЛА

"ЮНЫЙ ПРАВОВЕД"

Немного о себе:



Привет! Меня зовут Яроцкая Аня, я студентка 2-го курса юридического факультета Гомельского государственного университета им. Ф.Скорины и участница образовательной клиники "Живое право".

ПРАВОВАЯ ONLINE ШКОЛА

"ЮНЫЙ ПРАВОВЕД"

План занятия



1. Понятие киберпреступления

2. Виды киберпреступлений

3. Статистика по киберпреступлениям

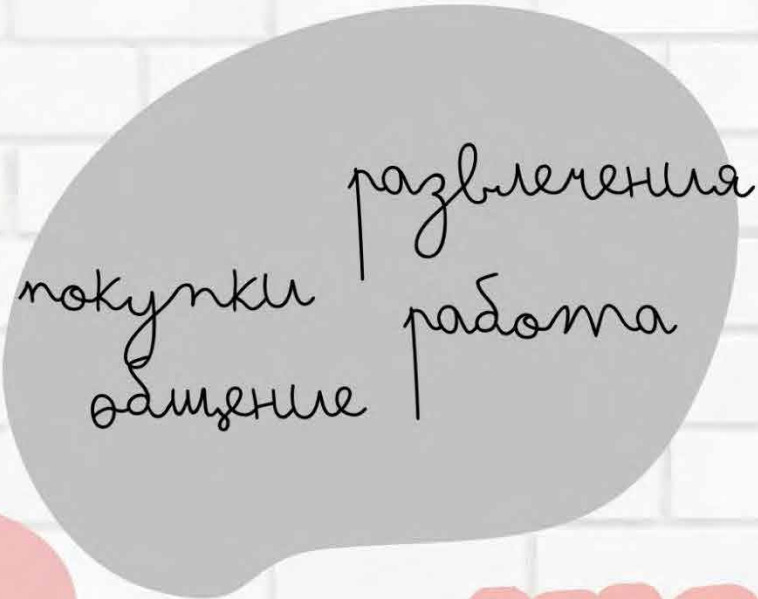
4. Ответственность за киберпреступления

5. Профилактика киберпреступлений

6. Подведение итогов занятия



NETFLIX



WORK

киберпреступность



Что такое киберпреступление?



Киберпреступление — вид правонарушения, непосредственно связанного с использованием компьютерных технологий и сети Интернет, включающий в себя распространение вирусов, нелегальную загрузку файлов, кражу персональной информации, например информации по банковским счетам. Киберпреступлениями считаются те преступления, в которых ведущую роль играют компьютер или компьютерная сеть.

Киберпреступность — это преступность в так называемом виртуальном пространстве.



ПРАВОВАЯ ONLINE ШКОЛА

"ЮНЫЙ ПРАВОВЕД"

какие же есть виды киберпреступлений?

1

Фишинг



Главная цель - заполучение
личных данных (логины,
пароли, код банковской
карты)

2

"Помощь другу"



Киберпространство - социальные сети (преим. Вконтакте) - пользователь получает SMS от друга, страница которого взломана, в котором тот просит о помощи (прислать фото карты или сообщить SMS код), чтобы совершить платёж, так как, например, его карточка заблокирована.

3

Вишинг



Осуществляется звонок на аб.номер потерпевшего (чаще всего Viber). Злоумышленник представляется работником правоохранительных органов или банка (даже называет ФИО) и под вымышленным предлогом (пресечение подозрительной транзакции, повышение уровня безопасности пользования банковской картой) просит сообщить номер карты и CVV-код или паспортные данные.



Свободный доступ к банковской карте.



Легкомыслие потерпевшего: хранение листочка с PIN кодом в сумке или кошельке или в памяти мобильного телефона.



Покупка с предоплатой



Размещение преступниками на виртуальных досках объявлений о продаже каких-либо товаров по «бросовым» ценам. Но для получения товара (якобы посредством почтовой пересылки или службы доставки) требуется перечисление предоплаты.



Шантаж

Злоумышленник может угрожать разглашением различных компрометирующих сведений с целью вымогательства.



ПРАВОВАЯ ONLINE ШКОЛА

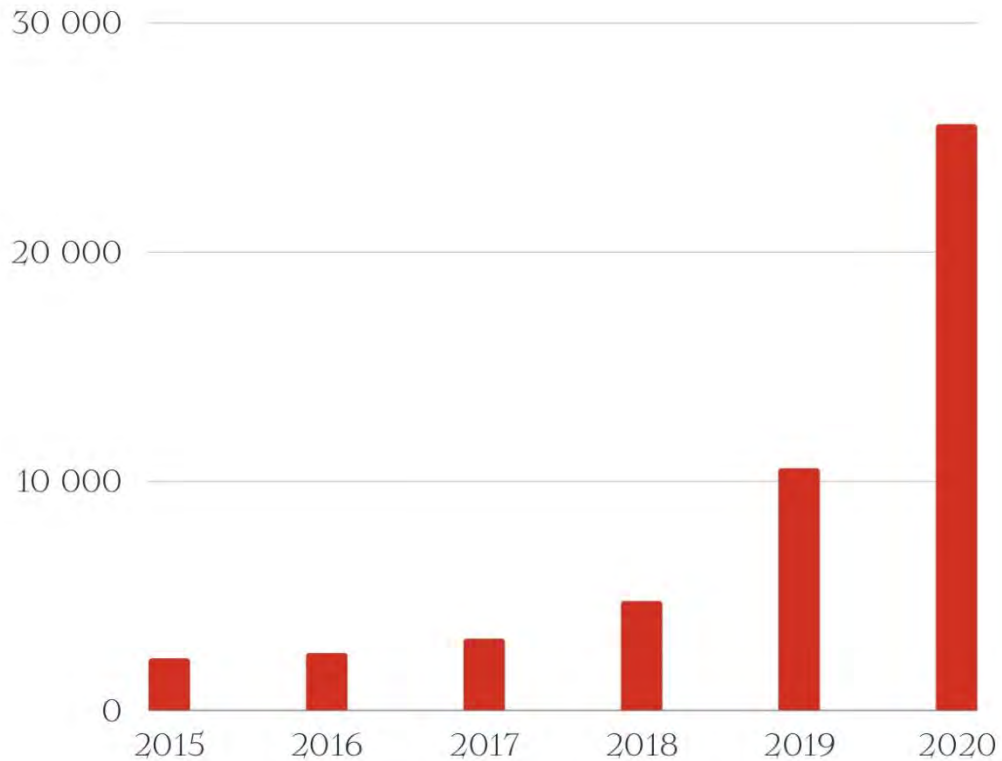
"ЮНЫЙ ПРАВОВЕД"



Иные мошенничества

- Родственник просит пополнить баланс карты через SMS, но просит не перезванивать
- SMS о некоем выигрыше, который можно получить путём оплаты пересылки почтой.
- Мошенник звонит и сразу сбрасывает. Жертва перезванивает и в это время списываются деньги, так как идет переадресация на платный номер.
- Приходит SMS с информацией, что карта взломана и прикреплен номер по которому можно получить помощь. Человек перезванивает, сообщает все персональные данные и его просят подождать звонка другого оператора.





В 2015 – 2 440,
 В 2016 – 2 471,
 В 2017 – 3 099,
 В 2018 – 4 741,
 В 2019 – 10 539,
 В 2020 – 25 561.

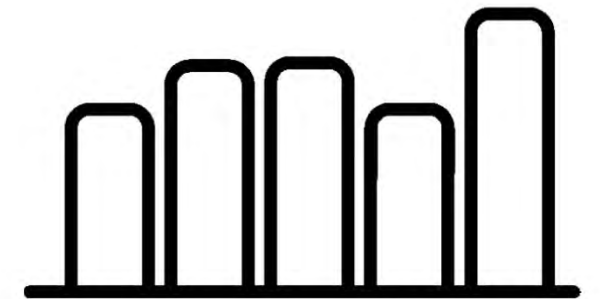
Несмотря на принимаемые меры, на протяжении последних лет в Республике Беларусь наблюдается устойчивый рост количества регистрируемых киберпреступлений.



По данным управления МВД Беларуси, сумма установленного материального ущерба от совершения киберпреступлений в Беларуси в прошлом году составила более шести миллионов рублей.

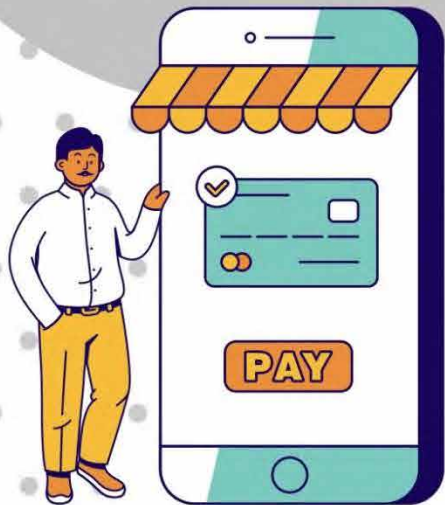
ПРАВОВАЯ ONLINE ШКОЛА

"ЮНЫЙ ПРАВОВЕД"



Факторы, влияющие на развитие киберпреступности в РБ

Уровень компьютерной грамотности граждан недостаточно высок, отстает от скорости внедрения тех или иных компьютерных систем в повседневную жизнь.



Опережающие темпы освоения сети Интернет в Республике Беларусь.

Ускоренный переход многих сфер общественных отношений, включая товарный и денежный обороты, в интернет-пространство



ответственность за киберпреступления

административная
ответственность



уголовная
ответственность

Ответственность за пропаганду и (или) публичное демонстрирование, изготовление и (или) распространение нацистской символики или атрибутики (Ст. **17.10.**), в том числе с использованием сети интернет

Статья **22.6 КоАП** устанавливает ответственность за несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты, — в виде штрафа в размере от 20 до 50 БВ.

Также ст. **22.7 КоАП** предусматривает несколько составов административных правонарушений за нарушение правил защиты информации.

1) посягательства на собственность и квалифицируются по статьям **гл. 24 УК РБ**) – ст. 216 "Причинение имущественного ущерба без признаков хищения", ст. 208 "Вымогательство", ст. 209 "Мошенничество"

2) преступления против информационной безопасности, квалифицируются по статьям **гл. 31 УК РБ**);

3) хищение путем использования компьютерной техники, квалифицируются по **ст. 212 УК РБ**

ПРАВОВАЯ ONLINE ШКОЛА

"ЮНЫЙ ПРАВОВЕД"

Профилактика киберпреступлений

Храните номер
карточки и ПИН-коды
в тайне

Регулярно проверяйте состояние
своих банковских счетов, чтобы
убедиться в отсутствии
«лишних» и странных операций

Не перезванивайте и не
направляйте ответные SMS,
если Вам поступило
сообщение о блокировании
банковской карты. Свяжитесь
с банком, обслуживающим
Вашу карту

Не используйте один
пароль для всех
интернет-ресурсов

Не переводите денежные средства
на счета незнакомых лиц



ПРАВОВАЯ ONLINE ШКОЛА

"ЮНЫЙ ПРАВОВЕД"

Юридический факультет ГГУ им. Ф.Скорины

г. Гомель, ул. Кирова, 119
www.law.gsu.by

ПРАВОВАЯ ONLINE ШКОЛА

"ЮНЫЙ ПРАВОВЕД"

Спасибо за внимание!



Просьба для улучшения и совершенствования качества нашей ONLINE школы заполнить отправленную вам форму обратной связи. Заранее благодарим за помощь

