UDK:420:415.61:398.9

НОВАЯ УГРОЗА ВЕКА: КИБЕРПРЕСТУПЛЕНИЕ ИЛИ «ХАКЕРСКИЕ ИГРЫ»

Мирсанова Нафисахон Бобомуродовна, студентка 3-го курса Каракалпакского Государственного университета имени Бердаха

yunonaeilish@gmail.com

THE NEW THREAT OF THE CENTURY: CYBERCRIME OR "HACKER GAMES"

Mirsanova Nafisakhon Bobomurodovna, third-year student at Karakalpak State University

Аннотация. *В данной статье рассматриваются новые вызовы цифровой реальности – киберпреступность. Было дано новое определение данному термину. Указан важность классификации видов киберпреступлений. Проанализированы характерные качества и причины роста преступностей на цифровом пространстве. Исследованы статистики ущерба возникших из-за хакерских атак. Даны эффективные методы и подходы реализуемые государством к решению данной проблемы.*

Ключевые слова: *киберпреступление, киберпространство, цифровое пространство, хакерская атака, компьютерная система.*

Abstract. *This article discusses the new challenges of digital reality – cybercrime. A new definition of this term was given. The importance of classification of cybercrime types is indicated. The characteristic qualities and causes of the growth of crime in the digital space are analyzed. The statistics of damage caused by hacker attacks are investigated. Effective methods and approaches implemented by the state to solve this problem are given.*

Key words: *cybercrime, cyberspace, digital space, hacker attack, computer system.*

Введение. Мир, в котором мы живем, подобен игре, где достигая новый уровень приобретаем больше возможностей и более трудные испытания. Появление интернета и компьютеров в 60-ые годы прошлого века, на самом деле, было одним из самых удачных прорывов в научном мире, впоследствии образовавший цифровое или, как чаще употребляют, киберпространство. Сущностью, которого, по идее, была служить во благо человечества. Хотя, кто же мог подумать, что эти площадки станут новой уязвимой и беспрепятственной ареной для атак и преступлений, в результате получившее новое название как «киберпреступность». Теперь безопасность тысяч пользователей может оказаться в зависимости от нескольких преступников[1].

Киберпреступность — это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных[2]. Она является следствием глобализации информационно-коммуникационных технологий и появлением международных компьютерных сетей считает кандидат технических наук Гундерич Г. А [3]. В то время как Л.И. Бутова пришла к следующему выводу, что это общественно опасное деяние (в форме действия либо бездействия), которое совершается в информационно-телекоммуникационной

сфере с использованием телекоммуникационных способов и средств, с помощью технических устройств, компьютерных сетей и систем, их программных компонентов в отношении информации, размещенной, используемой, обрабатываемой во всех информационно-телекоммуникационных сетях[4].

Различают следующие виды киберпреступлений:

- **фишинг**
- **фарминг**
- **распространение вирусов**
- **кража персональных данных**
- **кибершпионаж**
- **нарушение авторского права**
- **спам**
- **терроризм**
- **кибербуллинг**
- **кибервымогательства**
- **криптоджекинг**
- **кибершпионаж и т.д**

С нашей точки зрения, киберпреступление – это новый этап информационной войны, охватывающий в себя кражу или взлом данных; распространение психологически-насильственного воздействия, опять таки с помощью информационно-данных, на цифровом пространстве через цифровых инструментов. Допустим, фишинг – это вредоносная ссылка рассылаемая для взлома систем и получения средств с карт. То есть, фишинг и есть информация, а точнее ссылка носящая призывную информацию. Или же возьмем распространение вирусов, которые уничтожают данные содержаемые компьютером.

Анализ литературы.

Если обратить внимание, то трудно заметить единую и точную классификацию видов преступлений во многих нормативно-правовых актах. Данное явление можно четко рассмотреть на примере немецкой и русской юридической науки (Уголовного Кодекса), Конвенции Совета Европы о киберпреступности (Будапештская конвенция):

1) преступления, совершенные посредством высказываний (включая распространение порнографии (§ 184ff. УК ФРГ), изображение насилия (§ 131 УК ФРГ), нанесение оскорблений (§ 185ff. УК ФРГ), экстремистская пропаганда (§§ 130, 86, 86a УК ФРГ);

2) вторжение в личную сферу (включая нарушение конфиденциальности (§ 201 УК ФРГ), нарушение личной сферы жизни посредством произведения съемок (§ 201a УК ФРГ), преследование (§ 238 УК ФРГ);

3) мошенничество и компьютерное мошенничество (включая мошенничество (§ 263 УК ФРГ) и компьютерное мошенничество (§ 263a УК ФРГ);

4) атаки программного и аппаратного обеспечения (включая хищение (компьютерной) информации (§ 202a УК ФРГ), перехват данных (§ 202b УК ФРГ), подготовку к хищению (компьютерной) информации и перехвату данных (§ 202c УК ФРГ), изменение данных (§ 303a УК ФРГ), компьютерную диверсию (§ 303b УК ФРГ);

5) подделка документов при помощи компьютера (включая подделку документов (§ 267 УК ФРГ), фальсификацию данных, существенных для доказательств (§ 269 УК ФРГ), фальсификацию технических данных, записанных в память на электронных носителях (§ 268 УК ФРГ);

6) прочие компьютерные преступления (включая получение выгоды от выполненной работы обманным путем (§ 265a УК ФРГ), азартные игры (§ 284ff. УК ФРГ), повреждение устройств телекоммуникации (§ 317 УК ФРГ)[5].

В то время как Уголовный кодекс Российской Федерации содержит главу 28 «Преступления в сфере компьютерной информации», включающей в себя всего четыре статьи: неправомерный доступ к компьютерной информации(§ 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ(§ 273

УК РФ), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей(§ 274 УК РФ), неправомерное воздействие на критическую информационную инфраструктуру РФ(§ 275 УК РФ)[6].

А в Конвенции киберпреступления разделены на 5 групп:

- преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (противозаконный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование системы, противозаконное использование устройств);
- преступления, для совершения которых используется компьютер (подлог с использованием компьютерных технологий, мошенничество с использованием компьютерных технологий);
- преступления, связанные с содержанием данных (детская порнография);
- преступления, связанные с нарушением авторского права и смежных прав;
- преступления, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем

Обсуждение.

С нашей точки зрения отсутствие общего распределения видов киберпреступлений по категориям относительно определенных свойств или качеств могут способствовать игнорированию новых преступлений совершаемых в цифровом пространстве. В итоге может возникнуть случай, где выявлен наличие действия категорически противоречащее общим принципам права, но при этом не определен факт рассматривающий его в качестве преступления. Данный прогноз обусловлен динамичным и непредсказуемым развитием информационно-коммуникационных технологий и интернета. Поэтому мы решили проанализировать работы исследователей подразделив виды киберпреступлений в зависимости от цели, объекта посягательства и по характеру использования компьютеров и компьютерных систем для выявления более универсальной классификации:

1) Киберпреступления совершаемые ради:

- экономических целей (нанесение экономического ущерба в виде воровства денежных средств и конфиденциальной информации);
- политических целей (нанесение ущерба основным государственным и политическим институтам, подрывающее систему властных отношений и доверия к власти);
- идеологических целей (распространение идей и идеологий с целью вербовки интернет-пользователей в ряды, например, радикальных террористических и националистических группировок);
-социально- психологических целей (нанесение морального, психологического вреда гражданам)[7].

2) Киберпреступления выделяемые по объекту посягательства:

-экономические компьютерные преступления
-компьютерные преступления против личных прав и неприкосновенности частной сферы,
-компьютерные преступления против общественных и государственных интересов[8].

3) Киберпреступления совершаемые с помощью использования компьютеров или компьютерных систем:

-деяния, где компьютеры являются предметами преступлений (похищение информации, несанкционированный доступ; уничтожение или повреждение файлов и устройств и т.п.);
-действия, где компьютеры используются как орудия преступления (электронные хищения и т.п.);
- преступления, где компьютеры играют роль интеллектуальных средств (например, размещение в Интернете порносайтов)[9].

Наиболее подходящим вариантом является группировка киберпреступлений в

зависимости от целей, так как даже непредвиденные преступления в кибер арене будут совершаться из-за определенного мотива и цели. Хотя для назначения санкций или юридической ответственности более уместно будет классифицировать киберпреступления по объекту посягательства, таким образом упростив определения степени тяжести преступления и назначения соответствующего юридического наказания.

Для большинства преступлений, совершаемых в глобальных компьютерных сетях, характерны следующие особенности[10]:

1) Повышенная скрытность совершения преступления, обеспечиваемая спецификой сетевого информационного пространства (развитые механизмы анонимности, сложность инфраструктуры и т.п.);

Неперсонофицируемость, условная анонимность обуславливают сложности в выявлении и в установлении виновных в таких преступных инцидентах информационной безопасности[11];

2) Трансграничный характер сетевых преступлений, при котором преступник, объект преступного посягательства, потерпевший могут находиться на территориях разных государств;

3) Дистанционный характер преступных действий в условиях отсутствия физического контакта преступника и потерпевшего;

4) Возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно. Возможность объединять относительно слабые ресурсы многих отдельных компьютеров в мощное орудие совершения преступления.

Удаленность и транснациональный характер сети Интернет позволяют проводить кибератаки масштабно, причиняя максимальный ущерб*3;

5)Масштабность (киберпространство практически полностью покрывает нашу планету)[12];

Одной из главных причин роста киберпреступности как теневого бизнеса является незначительный риск: поскольку киберпреступность не имеет геополитических границ, правоохранительным органам трудно ловить преступников, а проведение международных расследований и ведение судебных дел стоят больших денег [13];

6) Нестандартность, сложность, многообразие и частое обновление способов совершения преступлений и применяемых специальных средств;

7) Многоэпизодный характер преступных действий при множественности потерпевших;

8) Неосведомленность потерпевших о том, что они подверглись преступному воздействию;

9) Особая подготовленность преступников, интеллектуальный характер преступной деятельности;

10) Невозможность предотвращения и пресечения преступлений данного вида традиционными средствами[10], хотя, в свою очередь, преступления, совершаемые в киберпространстве, в целом полностью копируют состав «классической» вариации преступления, но совершаются с помощью специфических орудий (например, мошенничество в сфере интернет-продаж и покупок)[14];

11) Не ограниченность круг лиц [12].

В отличие от других видов экономической преступности, киберпреступность в настоящее время является наиболее быстрорастущим сегментом, что связано с увеличением численности пользователей компьютеров, подключенных к глобальной сети Интернет[3]. Такая высокая усовершенствованность киберпреступлений создает немалочисленные препятствия при их обнаружении, выявлении и расследовании. Очень важной проблемой при расследовании киберпреступлений является высокая степень не своевременности их выявления, так в 53% случае в проходит более 10 дней с момента совершения преступления до поступления информации о совершенном преступлении[15]. Часто предварительное расследование начинается с запозданием, когда многие доказательства утеряны[16]. В 2020 году в среднем на выявление нарушений

компьютерной безопасности уходило 207 дней[17]. Так как многие жертвы киберпреступников не обращаются за помощью, а в частности многие компании ни всегда афишируют факт воздействия на них компьютерных атак из опасений потери репутации или из-за отсутствия надежды найти виновных и компенсации причиненного ущерба [3]. Т. Ю. Куява отмечает , что киберпреступность превратилась в очень выгодный бизнес, доходы от которого превышают доходы от торговли оружием и наркотикам[18], и не зря так как ущерб одной только экономики США, как сообщается в отчет ФБР о преступлениях в Интернете, от хакерских атак в 2020 году составил 4.2 миллиарда долларов, а в 2021 году выросло до 6.9 миллиарда долларов. [19]. По прогнозам журнала Cybersecurity Ventures ежегодный глобальный ущерб от киберпреступности оценивается в 10.5 триллиона долларов к 2025 году[20].

Ожидается, что киберпреступность будет до 5 раз прибыльнее, чем глобальные транснациональные преступления[17] (например: наркотики и торговля людьми, кража нефти, незаконная добыча и рыболовство, незаконный оборот оружия, который оценивается генерировать от 1.6 до 2.2 трлн долларов в год[21]**) вместе взятые.**

Особенно тревожит тот факт что даже такие крупные и мощные компании как FireEye (занимающейся ИТ-безопасностью)[17] в 2020 году, Crypto.com, Microsoft, News Corp, Красный Крест были подвергнуты кибератаке **в начале 2022 года было подвергнуты взлому и кибератаке[22]. Данная статистика указывает на неизбежность угроз в цифровом пространстве, поэтому обеспечение кибербезопасности должно быть первостепенной задачей и государства, и интернет-пользователей.**

Берова Дж. М., доктор юридических наук, доцент, полковник полиции, заместитель начальника по учебной работе Краснодарского университета МВД России предлагает пользователям соблюдать следующие элементарные правила кибербезопасности, чтобы свести к минимуму риск киберпокушений на безопасность компьютерной системы:

1) Использовать только лицензионное программное обеспечение с возможностью своевременного обновления.
2) Следить за актуальностью антивирусных программ;
3) Нельзя переходить по внешним ссылкам, полученным от неизвестных пользователей;
4) Рекомендуется удалять непрочитанными подозрительные письма от неизвестных пользователей. Открыв его, не переходить по указанным в нем ссылкам на неизвестные ресурсы, не открывать и не скачивать вложения;
5) Главное правило корпоративной безопасности: один компьютер - только для работы с банком, обслуживающим организацию и более ни для чего [23];
6) Не следует использовать электронные носители информации в неизвестных устройствах и наоборот;
7) Целесообразно регулярно делать резервные копии файлов на внешний носитель, постоянно не подключенный к компьютерной системе;
8) Рекомендуется не использовать один и тот же пароль для разных приложений, а также не использовать личные данные в качестве пароля;
9) Если компьютерная система все-таки была атакована, не спешить перечислять денежные средства злоумышленникам, так как нет гарантии того, что вредоносное программное обеспечение будет безвозвратно удалено с компьютера и вымогательство не повторится вновь, а также не скрывать произошедший инцидент компьютерной безопасности, как от руководства, так и от правоохранительных органов, не пытаться самостоятельно переустановить систему. Необходимо незамедлительно сообщить в правоохранительные органы и принять все

меры к сохранению и фиксации следов осуществленной кибератаки [11].

Результаты. Вышеуказанные подходы могут быть обеспечены пользователями самостоятельно, а мы предлагаем следующие подходы для государства для преодоления киберугроз:

1) Создать орган с 2 подразделениями отдельно обеспечивающих кибербезопасность государственных институтов (от хакерской атаки органов, кражи правительственных данных), а также безопасность данных физических и гражданских юридических лиц на цифровом пространстве. Так как жертвами кибератак могут стать как отдельные пользователи, так и коммерческие организации, государственные органы, политические общества и даже целые государства[11];
2) Создать краткий номер на подобии номеров вызова экстренных служб как 101(вызова пожарной службы); 102 (милиции); 103 (скорой помощи) для быстрого и своевременного обращения, в случае хакерской атаки;
3) Способствовать развитию компьютерной криминалистики для разработки рекомендаций по предупреждению и расследованию инцидентов кибербезопасности;
4) Внедрить практику тестирования на уязвимость сеть компьютерных систем для профилактических мер;
5) Увеличить количество специалистов по кибербезопасности и повысить их квалификацию.
6) Делать упор на назначение уголовной ответственности в случае совершения киберпреступления, нежели чем административной.

Скорость появления новых видов киберпреступлений, в разы превышает скорости обеспечения кибербезопасности. Велика вероятность того , что скоро каждая состоятельная личность наряду с личным врачом и юристом, будет иметь белого хакера (специалист по кибербезопасности). Разновидность вышеупомянутых киберпреступлений нуждается в единой и точной классификации для снижения риска вновь возникаемых преступностей в цифровом пространстве.

Заключение. Преимущественно характерные черты как анонимность, дистанционность, масштабность, автоматизированность и не осведомленность потерпевших воспрепятствуют выявлению совершаемых или совершихся преступлений в киберпространстве, обнаружению виновника, своевременному реагированию правоохранительных органов. Трансграничность и отсутствия возможности предотвращения киберпреступлений классическими средствами требует больших средств для борьбы. Постоянный рост жертв, в связи с увеличением количества интернет-пользователей, и практическая неизбежность угроз в цифровом пространстве обязывает внедрению практики синхронного обеспечения безопасной цифровой площади пользователями и государством. При этом статистика показывает важность соблюдения пользователями элементарных правил и принятию государства стратегических и эффективных мер для обеспечения кибербезопасности.

Использованные источники/References

1. В.А. Номоконов, Т.Л. Тропина Киберпреступность как новая криминальная угроза URL:https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza
2. Долгачев А.О. Понятие и особенности киберпреступности // Научный поиск ФГБОУ ВО «Ивановский государственный университет» [Электронный ресурс]. 2017 г. № 9. Режим доступа: https://elibrary.ru/item.asp?id=29674026/
3. Гундерич Г. А. Состояние киберпреступности URL: https://cyberleninka.ru/article/n/sostoyanie-kiberprestupnosti

4. Бутова Л.И. Характеристика и сущность киберпреступлений // Алтайский юридический вестник. 2016. № 3 (15). С. 28–31
5. Marbeth-Kubicki, A. (2010). Computer- und Internetstrafrecht. München: Verlag C.H. Beck
6. Уголовный Кодекс Российской Федерации
7. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение URL: https://cyberleninka.ru/article/n/kiberprestupnost-globalnaya-problema-i-ee-reshenie
8. Бекряшев А.К., Белозеров И.П. Теневая экономика и экономическая преступность / Электронный учебник. 2000
9. Ю.М. Батурин и А.М. Жодзишский выделяют две группы компьютерных преступлений — связанные с вмешательством в работу компьютеров и использующие компьютеры как необходимые технические средства. См.: Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. — М., 1991. — С. 11
10. Осипенко А.Л. Сетевая компьютерная преступность. — Омск, 2009. — С. 109—110
11. Берова Дж.М. Кибератаки как угроза информационной безопасности URL: https://cyberleninka.ru/article/n/kiberataki-kak-ugroza-informatsionnoy-bezopasnosti
12. Shidlovsky A. V. Establishing criminal liability for cybercrime – a new segment in the legal protection of electronic state // Proceedings of the VI International scientific and practical conference. 2018
13. И. М. Глотина Киберпреступность как теневой бизнес URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-tenevoy-biznes
14. Буз С.И. Киберпреступление: понятие, сущность и общая характеристика. URL:https://cyberleninka.ru/article/n/kiberprestupleniya-ponyatie-suschnost-i-obschaya-harakteristika
15. Киберпреступления: основные проблемы расследования // Институт судебных экспертиз и криминалистики [Электронный ресурс]. 2015 Режим доступа: https://ceur.ru/library/articles/obshhie_stati/item196792/
16. Нестерович С.А. Проблемы расследования киберпреступлений, которые стоят перед сотрудниками следственных органов. URL: https://cyberleninka.ru/article/n/problemy-rassledovaniya-kiberprestupleniy-kotorye-stoyat-pered-sotrudnikami-sledstvennyh-organov
17. URL: https://www.websiterating.com/ru/research/cybersecurity-statistics-facts/
18. Бутова Л.И. Характеристика и сущность киберпреступлений // Алтайский юридический вестник. 2016. № 3 (15). С. 28–31
19. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
20. URL: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
21. URL: https://www.stimson.org/2019/preventing-illicit-trafficking-transnational-criminal-organizations/
22. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.10d7f4cf-62e1c2b5-a3c9177b-74722d776562/https/www.techradar.com/uk/features/top-data-breaches-and-cyber-attacks-of-2022
23. Бехметьев А.Е. Кибератаки //Административное право. - №1. - 2017. - С. 17