ОБЗОР, МЕТОДЫ И ПРИЧИНЫ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В КИБЕРПРОСТРАНСТВЕ

ИИВ Академияси курсанти
Сафарова Дилбар Бахрилла Кизи

Аннотация: *Актуальность данной статьи заключается в изучении преступлений, совершаемых в киберпространстве, их видов, а также роли кибербезопасности в предотвращении. Цель данной статьи - определить виды преступлений, совершаемых с использованием информационных технологий, развитие и причины киберпреступлений, их специфические характеристики, понятие киберпространства, статистику преступлений, которые могут быть совершены в нем, определить причинные условия, широко распространить его среди общественности, чтобы предотвратить киберпреступность и в будущем не допустить, чтобы жертвы таких преступлений или субъекты этих преступлений стали жертвами таких преступлений.*

Abstract*: The relevance of this article is the study of crimes committed in cyber space, their types, and the role of cyber security in prevention. The purpose of this article is to determine the types of crimes committed using information technologies, the development and causes of cybercrimes, its specific features, the concept of cyberspace, the statistics of crimes that can be committed in it, and to determine the causal conditions, to promote it to the public in order to prevent cybercrime, and in the future to prevent victims of such crimes or becoming subjects of these crimes.*

Многие преступления, связанные с киберпреступностью, происходят в ситуациях, когда конфиденциальная информация защищена законом. На международном уровне как правительственные, так и неправительственные субъекты участвуют в киберпреступлениях, включая шпионаж, финансовые кражи и другие трансграничные преступления. Киберпреступления, которые пересекают международные границы и включают действия хотя бы одного национального государства, иногда называют кибервойной. Уоррен Баффет называет киберпреступность «проблемой номер один для человечества» и добавляет, что она «представляет реальную угрозу человечеству».

В отчете, опубликованном в 2014 году (при поддержке McAfee), годовой ущерб мировой экономике составил 445 миллиардов долларов. В отчете Cybersecurity Ventures за 2016 год прогнозируется, что глобальный ущерб, причиненный киберпреступностью, вырастет до 6 триллионов долларов в год к 2021 году и до 10,5 триллионов долларов к 2025 году.

По данным исследования, проведенного в 2018 году Центром стратегических и международных исследований (CSIS) в сотрудничестве с McAfee, в 2012 году в результате онлайн-мошенничества с кредитными и дебетовыми картами в США было

потеряно около 1,5 миллиарда долларов, на долю которого приходится примерно один процент мирового мошенничества. ВВП, или 600 миллиардов долларов, каждый год из-за киберпреступлений пропадает любимый человек. В Отчете о глобальных рисках Всемирного экономического форума за 2020 год подтверждено, что организованные агентства по борьбе с киберпреступностью объединяют усилия для ведения преступной деятельности в Интернете, в то время как вероятность их обнаружения и преследования в США составляет менее 1 процента.

Сегодня Интернет стал важной частью повседневной жизни каждого человека. От простого общения до покупок в Интернете — он захватывает мир. Компании также решили продолжить свою деятельность в Интернете. Результатом является рост электронной коммерции. Многие государственные процедуры также выполняются онлайн, и за последний год наблюдается огромный рост электронного финансирования.

По мере роста Интернета росли и связанные с ним опасности. Киберправо действует как щит над киберпространством для предотвращения киберпреступлений. Хотя это непростая задача для законодателей и борьбы с преступностью. Власти взяли на себя задачу создать и обеспечить соблюдение законов для предотвращения незаконной деятельности, происходящей в Интернете.

Предмет международного частного права включает многогранные (личные, имущественные, семейные, трудовые, служебные) отношения. Тщательное усвоение этих правовых положений необходимо для грамотного разрешения проблем и споров, возникающих в связи с социально-экономическими отношениями, сложившимися в нашей республике, с участием физических и юридических лиц других стран.

Киберправо, также известное как право Интернета или киберправо, является частью общей правовой системы, связанной с правовой информатикой, которая регулирует цифровое обращение информации, электронную коммерцию, программное обеспечение и информационную безопасность. Он занимается юридической информатикой и электронными элементами, включая информационные системы, компьютеры, программное и аппаратное обеспечение. Он охватывает многие области, такие как доступ к Интернету и его использование, с различными подтемами, включая свободу выражения мнений и конфиденциальность в Интернете.

Закон о компьютерном мошенничестве и злоупотреблениях был первым законом о кибербезопасности, принятым в 1986 году, под названием CFAA (Закон о компьютерном мошенничестве и злоупотреблениях). Этот закон помогает предотвратить несанкционированный доступ к компьютерам. Также предусмотрены штрафы за нарушение этого закона или участие в любой незаконной деятельности.

В зарубежной юриспруденции интернет-право изначально рассматривалось не как самостоятельная отрасль права, а как комплекс разнонаправленных правовых норм и институтов, относящихся к различным отраслям права и регулирующих отношения, связанные с Интернетом.

Киберправовой обмен информацией включает в себя вопросы разработки программного обеспечения и эксплуатации интернет-ресурсов. Иными словами, киберправо как область юридической науки претендует на изучение всех правоотношений, существующих в неразрывной связи с компьютерными технологиями и/или виртуальным пространством.

Статью 1158 Гражданского кодекса Республики Узбекистан можно дополнить следующим положением: «Особенности определения права, используемого при регулировании правоотношений, развивающихся в сети Интернет, определяются исходя из проявления правовой связи соответствующих правоотношений с правопорядком двух или более стран».

В настоящее время с развитием технологий возникают новые виды преступлений, и это преступления, совершаемые в киберпространстве. Большинство из них связаны с экономическими преступлениями, наносящими серьезный ущерб деловой активности и экономике нашей страны. С точки зрения уголовного права и криминологии активно «обсуждаются» понятие, природа, виды киберпреступности, а также меры борьбы с ней. В целях предотвращения таких новых видов преступлений эффективными мерами рассматриваются уголовно-правовые меры. Однако Уголовный закон не всегда успевает реагировать на эти проблемы киберпреступности.

Киберпреступления считаются международными преступлениями, поскольку в последние годы они совершаются через национальные границы. Основными факторами, влияющими на совершение киберпреступлений в киберпространстве, являются:

- экономический кризис;
- увеличение цен на необходимые товары;
- снижение уровня жизни;
- рост уровня безработицы и т.д.

По данным «Лаборатории Касперского», ежедневно в международном Интернете распространяется более 310 000 зараженных программных вирусов. В 2006 году этот показатель составлял 1,4 тысячи. Это свидетельствует о том, что за последнее десятилетие масштаб кибератак на международную сеть Интернет увеличился как минимум в 200 раз. В настоящий момент кибератаки, осуществляемые посредством вирусов, становятся очень опасными. Большинство распространенных вирусов направлены на кражу финансовой информации путем ослабления глобальной информационной сети, предоставляющей банковские услуги. Согласно анализу 2016 года, наиболее часто используемыми хакерами центрами являются крупные учреждения в сфере банковского дела и финансов, системы, реализующие процессы онлайн-платежей, торговые комплексы, гостиницы и торговые терминалы.

Например, киберпреступная группа Carbanak и ее хакеры SWIFT ежегодно крадут более 1 миллиона долларов у банков и других финансовых учреждений. Число хакерских преступлений и подобных информационных атак сегодня растет, как из-за

больших денежных сумм, вовлеченных в эти виды преступлений, так и из-за сложности их раскрытия. В 2016 году количество и изощренность фишинговых атак, направленных на хищение финансовых средств, возросли. В частности, организация информационных атак через «невидимый крючок» хакеров выросла на 13,4% и составила 47,48% всех хакерских преступлений, направленных на финансовые кибератаки. В частности, известны случаи хищения информации пользователей путем предложения населению оказать банковские услуги, кражи необходимой информации путем создания фейковых банковских систем, атак на банковские системы посредством электронной почты, организации различных интересных акций и викторин в Интернете. В 2016 году количество «троянских» вирусов, направленных на взлом банковских систем, выросло на 30,55% до 1 088 900. Среди них наиболее распространены «Zbot», «Gozi», «Nymaim», «Shiotob» — популярные семейства вредоносных файлов. 17,17 процента людей, подвергшихся атаке такого вируса, были корпоративными пользователями систем. Распространение таких вредоносных файлов в основном наблюдалось в России, Германии, Японии, Вьетнаме и США. Сегодня растет и число малых фирм, несущих финансовые потери из-за подобных вирусов. Число атак на пользователей Android в 2016 году выросло на 430%, достигнув 305 000 по всему миру. В частности, стало известно, что эти вирусы широко распространены в России, Австралии и Украине.

В частности, в России популярны семейства вирусов «Асакуб» и «Свпенг». Данная коллекция вирусов распространяется через сервис Google AdSense, который позволяет владельцу конкретного сайта размещать рекламу на сайте Google. В этом случае пользователь Android, посещающий сайт с рекламой Google, заражается вредоносным файлом и становится «жертвой» хакеров.

Поэтому специалисты в области информационной безопасности советуют владельцам устройств, работающих на операционной системе Android, при использовании Интернета обращаться к надежным источникам. В частности, приобретение вредоносных приложений на мобильные устройства с банковскими и финансовыми приложениями может привести к значительным потерям. На Международном форуме по кибербезопасности (Cyber Security Forum-2017), прошедшем в Москве 7 февраля этого года, были отмечены три самые распространенные на сегодняшний день атаки в мире киберпреступлений. По мнению экспертов, многие пользователи Интернета сегодня становятся жертвами киберпреступлений, похищая данные посредством фишинга, получая доступ к электронным устройствам через мобильные приложения со скрытой целью и просматривая незащищенные каналы связи.

АДАБИЕТЛАР:

1. Киберпреступность и отмывание денег // Евразийская группа по
2. противодействию легализации преступных доходов и финансированию терроризма. / Проект типологического исследования ЕАГ
3. Чугунов А.В. Ч-83 Развитие информационного общества: теории, концепции и программы: Учебное пособие. – СПб.: Ф-т филологии и искусств СПбГУ, 2007.
4. Brown C., Investigating and Prosecuting Cyber Crime: Forensic Dependencies
5. Barriers to Justice // International Journal of Cyber Criminology Vol 9 Issue 1 January – June 2015.
6. Definition of Cybersecurity Gaps and overlaps in standardisation // European
7. Union Agency for Network and Information Security V1.0 December 2015. Heraklion,
8. Бондарь В.В., Киберпреступность – современное состояние и пути борьбы // Юридические записки. 2013. № 2.
9. http:// akadmvd.uz (Ўзбекистон Республикаси ИИВ Академияси);
10. http:// lex.uz (Ўзбекистон Республикаси Қонун ҳужжатлари маълумотлари миллий базаси);
11. http:// uzsci.net (Илмий таълим тармоғи);
12. http:// www.academy.uz (Ўзбекистон Республикаси Фанлар академияси);