Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

The concept of cybercrimes and the necessity of their investigation

Bekzod ATAKULOV[1]

Tashkent State University of Law

ARTICLE INFO

Article history:
Received December 2024
Received in revised form
15 December 2024
Accepted 20 January 2025
Available online
15 February 2025

Keywords:
cybercrime,
cyber criminality,
investigation,
information space,
computer,
internet.

ABSTRACT

This scientific article examines the theoretical and legal aspects of cybercrime, including its definition, methods of prevention, deterrence, and investigation. The author analyzes the legal and practical possibilities for investigating such crimes, emphasizing the need for constant adaptation of criminal legislation in various countries, including the Republic of Uzbekistan. The article also highlights the importance of multilateral international cooperation and the improvement of forensic techniques. Based on the results of the conducted research, specific conclusions and recommendations have been formulated.

DOI: https://doi.org/10.47689/2181-1415-vol6-iss1/S-pp58-64

Kiberjinoyatlar tushunchasi va ularni tergov qilish zarurati

Kalit so‘zlar:
kiberjinoyat,
kiberjinoyatchilik,
tergov-qidiruv ishlari,
axborot makoni,
kompyuter,
internet.

ANNOTATSIYA

Ushbu ilmiy maqolada kiberjinoyatlarning nazariy va huquqiy xususiyatlari, ularning ta’riflari, ularni oldini olish va oldini olish usullari, shuningdek tergov qilish ochib berilgan. Muallif kiberjinoyatchilarni tergov qilishning ba’zi huquqiy va amaliy imkoniyatlarini tahlil qiladi, bu ko‘plab mamlakatlarning, shu jumladan O‘zbekiston Respublikasining amaldagi jinoyat qonunchiligi normalarini ushbu yo‘nalishdagi davlatlarning doimiy ko‘p tomonlama hamkorligiga va sud-tibbiyot texnikasini takomillashtirishga doimiy ravishda moslashtirish orqali amalga oshiriladi. O‘tkazilgan tadqiqotlarni hisobga olgan holda muayyan xulosa va takliflar ishlab chiqildi.

[1] Independent Researcher, Tashkent State University of Law. E-mail: bekatakuloff@gmail.com

Понятие киберпреступлений и необходимость их расследования

Ключевые слова:
киберпреступления,
киберпреступность,
расследование,
информационное
пространство,
компьютер,
интернет.

АННОТАЦИЯ

В данной научной статье рассматриваются теоретико-правовые аспекты киберпреступлений, их определение, способы профилактики, предупреждения и расследования. Автор анализирует правовые и практические возможности расследования таких преступлений, подчеркивая необходимость постоянной адаптации уголовного законодательства различных стран, включая Республику Узбекистан. Также акцентируется внимание на важности многостороннего международного сотрудничества и совершенствования криминалистических методик. По результатам проведенного исследования сформулированы конкретные выводы и предложения.

ВВЕДЕНИЕ

Постоянный рост киберугроз в современном информационном обществе создаёт перед каждым государством очень актуальную задачу – обеспечение надлежащего уровня информационной безопасности. Практика расследования многих видов преступности вызывает опасения в связи с низким уровнем защищенности граждан современного информационного общества, при этом спектр проблем достаточно широк – от технической незащищенности до уязвимости систем обеспечения работы, предназначенных для проведения операций с денежными средствами.

Методологическую основу данной научной статьи составляют различные методы научного познания, включая общенаучные и диалектические подходы, а также методы анализа, синтеза, индукции и дедукции. Кроме того, применяются специально-юридические методы, такие как сравнение, моделирование, прогнозирование и другие.

Теоретическая база исследования основана на трудах и научных публикациях ведущих ученых, среди которых А.К. Расулев [16], В.А. Номоконов [2], Е.М. Якимова [3], М.А. Простосердов [5], а также зарубежные исследователи H. Jahankhani, A. Al-Nemrat, A. Hosseinian-Far [10] и другие.

ОСНОВНАЯ ЧАСТЬ

Киберпреступления представляют собой преступные действия, совершаемые с использованием информационно-коммуникационных технологий (ИКТ) в различных противоправных целях. Ввиду множества научных интерпретаций, на данный момент невозможно дать этому понятию однозначное определение в рамках единого термина. На практике распространенными преступлениями в киберпространстве являются хищения, которые совершаются путем обмана, а именно: платежное мошенничество (с банковских карт); скимминг; вредоносный платежный софт; социальный инжиниринг (незаконное получение информации в корыстных целях); фишинг (получение доступа к конфиденциальным данным личности путем рассылки электронных писем); мошенничество в электронной торговле (хищения, посредством применения

слабых аспектов работы платежных систем интернет-магазинов, платформ для заказа авиабилетов, аренды автомобилей и других); мошенничество с предоплатой [1] и многие другие.

Расследование киберпреступлений – не новый, но до совершенства непроработанный правовой институт, который свойственен как уголовно-процессуальному праву, так и криминалистике. Но правовой фундамент расследования киберпреступлений задаёт именно уголовное право и соответствующее законодательство.

Практика расследования киберпреступлений в Узбекистане достаточно слабая и не еще не внушает уверенности в полноценной защите прав граждан в цифровом пространстве. Есть смысл заметить, что до сих пор в Уголовном кодексе Республики Узбекистан нет законодательного определения «киберпреступление». При этом современная юридическая литература под «киберпреступлениями» понимает «преступления в сфере компьютерной информации», «информационные преступления», «преступления, связанные с компьютерными техническими средствами», «преступления в высоких компьютерных технологиях», «преступления в информационном пространстве» и т.д. Многими учёными была предпринята попытка раскрыть данное определение. Так, исходя из позиции В.А. Номоконова, Т.Л. Тропиной, киберпреступление – это обширный термин, чем компьютерная преступность и точно отражающее преступность в информационном пространстве [2, с.47].

Киберпреступление – это действие, свойственное социальной девиации с целью нанесения экономического, а также других видов ущерба, индивиду, организации или государству посредством любого технического средства с доступом в Интернет. К.Н. Евдокимов дает несколько определений понятию «Компьютерная преступность», ссылаясь на различные мнения исследователей [3, с.98]. С мнениями исследователей можно согласиться, но на наш взгляд, в них не хватает практической опоры и критического анализа.

Согласно Конвенции о киберпреступности, открытой для подписания в Будапеште и вступившей в силу 1 июля 2004 года, киберпреступлениями считаются «деяния, направленные против конфиденциальности, целостности и доступности компьютерных систем, сетей и данных, а также злоупотребления ими» [4].

Надо учесть, что на данный момент большая часть киберпреступлений носит транснациональный характер, в связи с чем проблема обеспечения безопасности в киберпространстве стоит перед всеми государствами, которые признают, что ее успешное решение возможно только при совместных усилиях всех заинтересованных сторон.

Конвенция Совета Европы о киберпреступности, принятая 23.11.2001 года, была особым предметом исследования многих авторов [5, с.232]. Данный документ определил виды киберпреступлений и обязал «договаривающиеся стороны принять законодательные и иные меры, необходимые для того, чтобы квалифицировать деяния в качестве уголовных преступлений согласно внутригосударственному праву» [6]. Также данным документом были определены некоторые процессуальные вопросы, вопросы взаимодействия правоохранительных структур государств и вопросы юрисдикции, предлагая определять ее территориальным признаком государства [7, с.15].

В 2014 году государства – члены Африканского союза приняли Конвенцию о кибербезопасности и защите персональных данных, сделав акцент на безопасности в информационном пространстве в целом и на законодательстве по содействию электронной торговле [8].

Представляет отдельный интерес уголовно-правовое регулирование хищений, совершаемых в киберпространстве, в отдельных зарубежных странах.

В Уголовном кодексе Франции нормы, предусматривающие ответственность за компьютерные преступления, содержатся в трёх книгах («О преступлениях и проступках против личности», «Об имущественных преступлениях и проступках», «О посягательствах на системы автоматизированной обработки данных») [9, с.160].

В странах общего права не предусматривается кодификация законодательства, в связи с чем в Великобритании ответственность за совершение компьютерных преступлений устанавливают различные статуты: Закон о неправомерном использовании компьютера, Закон о телекоммуникациях (обман), Закон об электронном сообщении, а также Закон о защите персональных данных, Закон о телевизионных лицензиях (раскрытие информации), Закон о борьбе с обманом в области социального обеспечения [10, p. 137].

В 1986 году в США принят закон «О мошенничестве и злоупотреблениях, связанных с компьютерами». Этот закон регламентирует нормы по хищениям с применением компьютерных систем [11]. Параграф 1030 главы 47 раздела 18 Свода законов США, устанавливающий ответственность за совершение мошенничества путем доступа к компьютеру, стал частью этого закона [12, с.55].

В Уголовном кодексе ФРГ компьютерное мошенничество выделено в отдельное преступление, параграфом 263а установлена ответственность за действия с целью получения для себя или третьего лица противоправной имущественной выгоды [13, с.524].

Уголовным кодексом Швейцарии предусмотрена ответственность за электронный шпионаж, совершенный с корыстной целью. Так, наказанию подлежит тот, кто с целью собственного незаконного обогащения или обогащения другого приобретает для себя или другого лица данные, собранные или переданные электронным или иным подобным способом (статья 143). Здесь же следует упомянуть, что статья 147 Уголовного кодекса предусматривает уголовную ответственность за мошенническое злоупотребление с установкой для обработки данных [14, с. 138].

Как мы видим, законодатели различных государств по-разному подошли к решению проблемы обеспечения безопасности в информационном пространстве, но несмотря на данную практику, существующую во многих странах, важным аспектом, учитывая её трансграничный характер, остаётся гармонизация норм законодательства государств с учетом норм международного права, что возможно реализовать, используя достижения разработок, принятия и исполнения единого многостороннего документа по расследованию киберпреступлений благодаря прогрессивным правовым методикам.

Рассмотрев вкратце существующий зарубежный опыт в части правовой регламентации и расследования киберпреступлений, необходимо признать, что они подрывают не только компьютерную безопасность общества, информационную безопасность пользователей ЭВМ, но и общественный порядок

государства в целом, и в расследовании такого рода преступлений необходимо проявлять комплексный подход, основанный на совместных действиях многих государств. Ввиду этого есть необходимость подчеркнуть, что на данный момент государствам предстоит совершить много совместной работы по разработке единого подхода к киберпреступности, так как отсутствие общепринятых и нормативно закрепленных дефиниций «Интернет», «киберпреступление», «киберпреступность», «компьютерные преступления», позволяет преступникам избегать ответственности, пользуясь несогласованностью информационно-правовых баз различных государств [15]. Определенный риск представляет и такая тенденция, когда хакеры или иные недобросовестные лица совершают преступные действия из государства, где подобная деятельность не является противозаконной.

В определенной степени расследованию киберпреступлений мешают такие негативные факторы правоприменительной практики, как: пассивность государственных органов, незаинтересованность в быстром реагировании на киберпреступления, относительно слабая информационная (компьютерная) грамотность, пассивность в применении технической оснащенности силовых структур, стереотипность мышления. Решению этих, и многих других факторов поспособствовала бы постоянная работа зарубежных специалистов с национальными на уровне министерств и прокуратуры по принципу «коворкинга», проведение инициативных групп мониторинга за реализацией норм действующего законодательства, усиление общественного контроля, придание ему чёткой законодательной формы и гарантий деятельности в условиях глобализации.

ЗАКЛЮЧЕНИЕ

Проведенное в настоящей научной статье исследование позволило нам прийти к следующему выводу.

Обеспечение кибербезопасности связано с постоянно нарастающей информатизацией общества, ввиду чего методы совершения киберпреступлений только обогащаются, а наука и практика не настолько гибкие и оперативные, что не всегда позволяет «мыслить сознанием преступника». Стало понятным, что в юридической науке относительно слабо разработаны концептуальные методы расследования киберпреступлений с криминалистическим опытом именно тех лиц, которые ранее уже имели аналогичный опыт (например, в контр-атаках в сфере киберпреступлений).

Видится необходимым продолжение усиления международного сотрудничества, взаимодействия соответствующих специализированных органов, которые осуществляют расследование киберпреступлений и борьбу в данной сфере. На наш взгляд, в одиночку справиться со всей преступной массой в сфере киберпространства пока что представляется скорее мало реалистичным, какими бы организационно-правовыми возможностями государство не обладало. Ввиду этого необходимо продолжить работу над следующими направлениями деятельности:

1. Необходимо совершенствовать реализацию уголовно-правовых норм на практике, которые предусматривают ответственность в сфере ИКТ, а также над расширением категорий составов киберпреступлений.

2. Укреплять институциональные основы профилактики киберпреступлений и правонарушений в сети Интернет, привлекая специалистов и широкую публику к информационной грамотности, честности и поощряемым видам правомерного поведения.

3. Следует поддержать мнение отечественных учёных о наделении Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан правом осуществления профилактики правонарушений в сети Интернет [16].

4. Определенное значение будет иметь продолжение работы в части предупреждения и противодействия киберпреступлений, исследовательская работа в части вопросов криминализации, юрисдикции, транснациональных расследований.

5. Необходимо обеспечить применение на практике правового эксперимента, суть которого будет состоять в том, что органы следствия будут применять при расследовании уголовных дел тактику «мыслить, как преступник» и тактику «умное расследование» посредством применения современных достижений цифровых технологий. Но это не единственные методики, которые можно применять в практике расследования киберпреступлений.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

1. Comprehensive Study on Cybercrime. Available at: http:///www.unodc.org

2. Номоконов В.А. Киберпреступность, как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология. Вчера. Сегодня. Завтра. – 2012. – №1 (24). – С. 47.

3. Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ / науч. ред. И.Г. Смирнова; отв. ред. О.А. Егерева, Е.М. Якимова. – М., 2016.

4. Кочкина Э.Л. Определение понятия «Киберпреступление». Отдельные виды киберпреступлений. Журнал «Сибирские уголовно-процессуальные и криминалистические чтения». 2017 г. // Источник: https://cyberleninka.ru/article/n/opredelenie-ponyatiya-kiberprestuplenie-otdelnye-vidy-kiberprestupleniy

5. Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук: 12.00.08. М., 2016. 232 с.

6. Global Programme on Cybercrime. URL: http://www.unodc.orgl

7. Гузеева О.С. Действие Уголовного кодекса России в отношении интернет-преступлений // Законы России: опыт, анализ, практика. 2013. N 10. С. 15-19.

8. African Union Convention on Cyber Security and Personal Data Protection. Adopted by the twenty-third ordinary session of the Assembly held in Malabo Equatorial Qunea, 27 june 2014. URL: https://au.int/en/treaties

9. Уголовный кодекс Франции / науч. ред. Л.В. Головко, Н.Е. Крыловой; пер. с фр. Н.Е. Крыловой. СПб.: Юрид. центр Пресс, 2002. 650 с.

10. Jahankhani H., Al-Nemrat A., Hosseinian-Far A. Cybercrime classification and characteristics // Cyber Crime and Cyber Terrorism Investigator's Handbook. Waltham, 2015. 393 p. – P.137.

11. Чернякова А.В. Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемым с использованием компьютерной информации. Журнал «Юридическая наука и правоохранительная практика». 2018 г. ВАК // Источник: https://cyberleninka.ru/article/n/mezhdunarodnyy-i-zarubezhnyy-opyt-ugolovno-pravovogo-protivodeystviya-hischeniyam-sovershaemym-s-ispolzovaniem-kompyuternoy

12. Хилюта В.В. Хищение с использованием компьютерной техники или компьютерное мошенничество? // Библиотека криминалиста. 2013. N 5 (10). С. 55-65.

13. Уголовный кодекс Федеративной Республики Германии / науч. ред. Д.А. Шестакова; пер. с нем. Н.С. Рачковой. СПб.: Юрид. центр Пресс, 2003. 524 с.

14. Уголовный кодекс Швейцарии / пер. с нем. М.: Зерцало, 2000. 138 с.

15. Net Losses: Estimating the Global Cost of Cybercrime [Электронный ресурс] // Official web-site of Center for Strategic and International Studies URL: http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

16. Расулев А.К. Киберпреступность: причины и условия, личность преступника. Журнал «Review of law sciences». 2020 г. // Источник: https://cyberleninka.ru/article/n/kiberprestupnost-prichiny-i-usloviya-lichnost-prestupnika