УДК 32 **DOI: 10.34670/AR.2023.85.89.010**

Проблема распространения киберпреступности в эпоху глобализации: политические аспекты

Майстренко Григорий Александрович

Кандидат юридических наук, старший научный сотрудник,
Научно-исследовательский институт ФСИН,
125130, Российская Федерация, Москва, ул. Нарвская, 15А;
e-mail: G.Maystrenko@yandex.ru

Майстренко Анна Григорьевна

Кандидат юридических наук,
доцент кафедры гражданско-правовых дисциплин,
Российский университет нефти и газа им. И.М. Губкина;
доцент кафедры гражданского и предпринимательского права,
Всероссийская академия внешней торговли
Министерства экономического развития Российской Федерации,
119285, Российская Федерация, Москва, ул. Пудовкина, 4а;
e-mail: Annamajstrenko@yandex.ru

Аннотация

Статья посвящена комплексному исследованию проблемы киберпреступности в эпоху цифровизации и глобализации. Основное внимание в работе автор акцентирует на глобализации, способствующей прогрессу в различных частях мира и развитии информационных технологий, а также актуальной на сегодняшний день проблеме киберпреступности, оказывающей негативное влияние на современное общество. В статье на основе анализа научных публикаций по данной тематике исследуются различные формы киберпреступлений, их последствия и способы предотвращения, а также связь между киберпреступностью и глобализацией. Целью статьи можно обозначить влияние глобализации на киберпреступность и то, как с ростом глобализации и информационных и коммуникационных технологий обычные преступления заменяются новыми преступлениями современного цифрового мира.

Для цитирования в научных исследованиях

Майстренко Г.А., Майстренко А.Г. Проблема распространения киберпреступности в эпоху глобализации: политические аспекты // Теории и проблемы политических исследований. 2023. Том 12. № 9А. С. 85-91. DOI: 10.34670/AR.2023.85.89.010

Ключевые слова

Кибербезопасность, Интернет, киберпреступность, глобализация, цифровизация.

Введение

Феномен глобализации заключается в том, что мир на наших глазах трансформируется посредством инновационных технологий и расширения международной торговли. Увеличившаяся доступность транспорта и возможность присутствия в нескольких местах одновременно благодаря использованию технологий позволили преступлениям стать более глобальными; они больше не ограничиваются определенной территорией.

Безусловно, информационные и коммуникационные технологии ускорили рост глобализации. Развитие Всемирной сети привело к большему взаимодействию между людьми, предприятиями и правительствами по всему миру. Воздействие глобализации настолько сильно, что оно способствовало взаимозависимости мировых экономик, сообществ, населения и культур [Рыжов, 2018, с. 30]. При этом важно упомянуть о том, что, наряду с прогрессивным и эволюционным воздействием глобализации, она имеет и многочисленные негативные последствия. Ни у кого не вызывает сомнений тот факт, что цифровизация послужила толчком к росту глобализации, в конечном итоге породив киберпреступность. Глобализация содействовала распространению культур, религий и ценностей, но она также способствовала распространению инновационных идей в криминальной сфере.

Основная часть

Глобализация — это неминуемая реальность современного общества, ставшая ключевым звеном нового столетия, разрушившая географические и культурные границы. Стремительное развитие технологий способствовали распространению киберпреступлений по всему миру, а также инновационных методов правонарушений, когда преступник и жертва могут находится за тысячи километров друг от друга [Агаркова, Синицына, 2021, с. 15].

Понятие киберпреступности определяется как преступление, совершенное с использованием Всемирной сети, компьютера, или любого другого электронного гаджета, подключенного к интернету. Кража личных данных с компьютера жертвы, угрозы и шантаж собеседнику в социальных сетях с целью вымогательства денег, клевета в его адрес в социальных сетях и многое другое — все это примеры совершаемых киберпреступлений, число которых постоянно растет. Нужно также отметить появление новых терминов в сфере киберпреступности, таких, как: хакер, фишинг, киберторговля и пр.

В результате мы видим, что совершить кражу или вымогательство становится легче, жертва не может опознать преступника, преступнику легче уйти от наказания в виртуальном мире, в связи с этим появляется ощущение «безнаказанности», которое, в свою очередь провоцирует дальнейший рост киберпреступлений.

Зачастую киберпреступность подразумевает под собой атаку на личные данные отдельных лиц или организаций, их банковские счета. Но не стоит забывать и об отдельном виде преступлений – кибертерроризме, когда с использованием информационных технологий общественность или группу людей подвергают террору, распространяя дезинформацию или угрожая выводом из строя крупной компьютерной сети какой-нибудь компании.

Также нужно отметить киберклевету, как новый вид преступлений, при котором преступник оскорбляет или унижает жертву в социальных сетях, форумах, мессенджерах.

Публикация обидных и клеветнических комментариев в адрес жертвы в социальных сетях, сообщения или звонки жертве на ее мобильный телефон, размещение фотографий жертвы в

социальных сетях — вот некоторые из действий, подпадающих под понятие киберзапугивания. При этом фотографии зачастую редактируются и видоизменяются при помощи различного программного обеспечения.

Также при помощи фоторедакторов происходит кибермошенничество, включающее в себя подделку подписей к электронному документу, изменение содержания конфиденциального документа, создание поддельных цифровых документов и т. д. Сложность заключается в том, что точность подделки бывает настолько высока, что становится практически невозможно отличить оригинал от поддельного документа, личности или подписи.

Нужно признать, что киберпреступления современного мира сложны, запутаны и многие из них никогда не будут раскрыты. На сегодняшний день многие компании по всему миру обращаются к киберстрахованию как к средству снижения рисков взлома, безусловно, не сдерживая при этом рост киберпреступности.

Новые технологии и услуги, такие как расширенное шифрование, двухфакторная аутентификация и менеджеры паролей, способствуют укреплению защиты от киберугроз. Однако, с их распространением, киберпреступники находят новые уязвимости. Нужно отдавать себе отчет в том, что киберпреступность представляет собой угрозу абсолютно для всех активных пользователей Интернета, и эта угроза неуклонно растет [Рыжов, 2018, с. 9-10].

Жизнеспособность бизнеса может быть поставлена под угрозу, если киберпреступники получают доступ к конфиденциальным данным или интеллектуальной собственности, что делает киберпреступность серьезным стратегическим риском, и планы по предупреждению и устранению последствий должны быть у государств в приоритете [Жакупжанов, 2019, с. 76].

В первую очередь, нужно отметить важность грамотно выстроенных процессов управления рисками, оценки уровня привлекательности для киберпреступников и поиск главных уязвимостей сайтов предприятий и организаций. В конечном итоге целью должно стать внедрение кибербезопасности во все бизнес-процессы предприятия [Кувшинова, 2020, с. 55].

Также с учетом быстрого распространения вредоносного программного обеспечения, фишинга важно уметь защитить себя от киберпреступности, выбирая надежные пароли, используя несколько для всех своих учетных записей. Совершать покупки в Интернете необходимо только при безопасном соединении и воздержаться от использования общедоступного Wi-Fi- подключения.

Как было сказано выше, киберпреступность наносит ощутимый ущерб мировой экономике, национальной безопасности и социальной стабильности [Агаркова, Синицына, 2021, с. 15-16]. Будучи новым социальным явлением в век информационных технологий, киберпреступность вызывает обеспокоенность во всем мире из-за высокого охвата разрушительной силы и обширного влияния.

Усилия в области кибербезопасности в первую очередь сосредоточены на применении технических подходов, таких как системы обнаружения и предотвращения вторжений, межсетевые экраны и антивирусное программное обеспечение для смягчения угроз кибератак. Эти методы могут помочь уменьшить негативное воздействие киберпреступности как на уровне организаций, так и отдельных лиц [Кириленко, Алексеев, 2020, с. 898]. Однако эти технические решения в значительной степени не учитывают человеческие и контекстуальные факторы, которые способствуют возникновению проблем.

Киберпреступность представляет собой широкое географическое явление на макроуровне: на некоторые страны приходится непропорционально большое количество киберпреступлений. Эта пространственная неоднородность тесно связана с конкретным социально-экономическим

контекстом. К примеру, страны с более высоким валовым внутренним продуктом на душу населения и лучшей инфраструктурой информационных технологий чаще подвергаются кибератакам [Мордвинов К.В., Удавихина, 2022, с. 83].

Можно говорить о том, что глобальная трансформация в экономической сфере не является чем-то новым, этот процесс начался достаточно давно, движущей силой явилось развитие транспортных и коммуникационных технологий, сделав мир все более единым и открытым. Открытость в эпоху глобализации привела к трансформации различных аспектов, включая экономическую, социальную, политическую, культурную и систему ценностей.

В области культуры глобализация является средством гармонизации отношений между нациями, поэтому так важно предотвращать на раннем этапе распространение глобальных преступлений, которые угрожают спокойствию мирового сообщества [Ковтун, 2021, с. 95].

Экономическая деятельность во всех частях мира все больше зависит от существования информационных технологий (телекоммуникации, средств массовой информации). Например, что касается транзакций, технология электронной коммерции способна объединять продавцов и покупателей со всего мира и осуществлять транзакции купли-продажи с любым электронным устройством, подключенным к сети Интернет. То же самое можно сказать и о технологии электронного перевода средств: отправка денег между экономическими субъектами в отдаленных уголках мира может осуществляться за считанные секунды. Использование технологий также зависит от того, кто их использует. Иными словами, на возникновение экономической преступности влияют различные комплексные факторы, прежде всего фактор человеческий [Самиров, Примаков, Синицын, 2014, с. 78].

Безусловно, киберпреступность, основанная на новейших технологиях, представляет собой серьезную угрозу в эпоху глобальной торговли. На сегодняшний день требуется ужесточение законов для лиц, совершивших киберпреступления, обновления законов и постановлений в экономической сфере [Ляпин, 2021, с. 10].

Заключение

Кибепреступность становится все более сложной частью человеческой цивилизации и даже может рассматриваться как часть проблемы политической системы. Необходимо осознать, что технологические киберпреступления являются продуктом чрезмерной глобальной трансформации в экономической сфере с многомерными измерениями. Таким образом, можно сделать вывод о том, что, осознавая сложность проблемы киберпреступности, необходимы многоаспектные усилия по ее предотвращению. Некоторыми аспектами, которые выделяются или больше всего затрагиваются нынешними глобальными преобразованиями в экономической сфере, являются социальные, культурные, экономические, технологические, политические и правовые аспекты [Бондарь, 2020, с. 156]. Становится очевидно, что неблагоприятная общественно-политическая ситуация нередко провоцирует возникновение технологических экономических преступлений [Дерюгин, 2019, с. 47].

Учитывая вышесказанное, можно констатировать тот факт, что на киберпреступления, являющиеся частью процесса глобализации, необходимо реагировать масштабно, а именно посредством разносторонней макрополитики.

Библиография

1. Агаркова А. А., Синицына В.А. Киберпреступность в современной России. Международный журнал гуманитарных и строительных наук, 2021. № 5-3. – С. 13-16.
2. Бондарь Е.О. Киберпреступность как новая криминальная угроза. Вестник Московского университета МВД России, 2020. № 1. – С. 155-158.
3. Дерюгин Р.А. Киберпреступность в России: современное состояние и актуальные проблемы. Вестник Уральского юридического института МВД России, 2019. № 2. – С. 46-49.
4. Жакупжанов, А.О. Виктимологические факторы киберпреступности // Алтайский юридический вестник. 2019. № 3(27). – С. 75-82.
5. Кириленко В.П., Алексеев Г.В. Гармонизация российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы // Всероссийский криминологический журнал. – 2020. – Т. 14, № 6. – С. 898-913.
6. Ковтун К. А. Банковская киберпреступность как одна из основных проблем современного общества. Теоретическая и прикладная юриспруденция. 2021. № 1 (7). – С. 94-97.
7. Кувшинова, В.С. Криминологическая характеристика киберпреступности. Международный журнал гуманитарных и строительных наук. 2020. № 5-4. С. 53-57.
8. Ляпин, А.Е. Киберпреступность как новый объект статистического анализа // Статистика и Экономика. 2021. Т. 18, № 6. – С. 4-16.
9. Мордвинов К.В., Удавихина У.А. Киберпреступность в России: актуальные вызовы и успешные практики борьбы с киберпреступностью // Теоретическая и прикладная юриспруденция. 2022. № 1(11). – С. 83-88.
10. Самиров Р.Ж., Примаков И.В., Синицын С.Н. [и др.] Киберпреступность как угроза национальной безопасности Российской Федерации // Законность и правопорядок в современном обществе. 2014. № 19. – С. 77-81
11. Рыжов В.Б. Диалектика глобализации и регионализации в правовом пространстве государств и международных организаций [Электронный ресурс] // Международное право и международные организации. 2020. № 1. – С. 29-44. – URL: https://www.e-notabene.ru/mpmag/article_30979.html (дата обращения: 12.09.2023).
12. Рыжов В.Б. Информационная безопасность в государствах Европейского союза: к постановке проблемы // Представительная власть – XX1 век. 2018. № 4. – С. 8-12.
13. АВ Зуев, МП Бородин, АВ Платонов, ЕА Горбаренко Государство как субъект международно-правовых отношений: проблемы теории и практики //Вопросы российского и международного права. – 2023. – Т. 13. – №. 5А. – С. 23.
14. Чешин, А. В. Гражданско-правовые договоры в инвестиционной деятельности / А. В. Чешин // Вопросы российского и международного права. – 2023. – Т. 13, № 4-1. – С. 186-192.
15. Чешин, А. В. Институциональные и организационные аспекты привлечения инвестиций в экономику региона / А. В. Чешин // Государственная служба. – 2019. – Т. 21, № 4(120). – С. 50-57.
16. Чешин, А. В. Гражданско-правовое регулирование иностранных инвестиций в России / А. В. Чешин // International Law Journal. – 2023. – Т. 6, № 6. – С. 51-55.
17. Ошкордина А. А. РАЗВИТИЕ ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ЗДРАВООХРАНЕНИИ //Международный форум Kazan Digital Week-2022. – 2022. – С. 432-438.
18. Лазарева, О. С. Интерактивная методика подготовки специалистов в сфере делового туризма / О. С. Лазарева, Е. А. Магдич // Научный вестник МГУСиТ: спорт, туризм, гостеприимство. – 2022. – № 4(74). – С. 72-79.
19. Implementing the aarhus convention / R. Yerezhepkyzy, A. Egorov, A. Sadvokassov, V. Shestak // European Energy and Environmental Law Review. – 2021. – Vol. 30, No. 4. – P. 120-127.
20. Егоров, А. М. Особенности взаимодействия отечественных спецслужб на северо-западе Российской империи в условиях Первой мировой войны / А. М. Егоров, И. А. Егоров // Метаморфозы истории. – 2023. – № 28. – DOI 10.37490/S230861810025513-4.
21. Мусорина, О. А. Русский язык в советский и постсоветский период / О. А. Мусорина, С. Г. Сорокина. – Пенза : Пензенский государственный университет архитектуры и строительства, 2014. – 132 с. – ISBN 978-5-9282-1064-9. – EDN VTGNLJ.
22. Стратегии социально-экономического развития: философско-мировоззренческие и прикладные исследования : коллективная монография / С. В. Дрожжина, Э. В. Баркова, Ю. В. Буланая [и др.]. – Москва : Архонт, 2022. – 336 с. – ISBN 978-5-6046534-9-4. – EDN PUEIEA.
23. Попова, И. В. Влияние финансового кризиса на эффективность работы банков / И. В. Попова, И. П. Никитина // Бизнес. Образование. Право. – 2016. – № 3(36). – С. 160-163. – EDN WGELPL.
24. Попова, И. В. Повышение финансовой грамотности предпринимателей как основа стабильного функционирования банков / И. В. Попова, И. Е. Лазарева // Северный регион: наука, образование, культура. – 2019. – № 3-4(43-44). – С. 66-70. – EDN BMFSLE.
25. Попова, И. В. Повышение финансовой грамотности предпринимателей-заемщиков / И. В. Попова, И. Е.

Лазарева // Экономика: вчера, сегодня, завтра. – 2020. – Т. 10, № 5-1. – С. 389-397. – DOI 10.34670/AR.2020.40.17.047. – EDN TCXOBR.
26. Попова, И. В. Теоретические подходы к построению платежной системы на основе платформы Blockchain в странах БРИКС / И. В. Попова, И. П. Никитина // Банковские услуги. – 2018. – № 4. – С. 2-6. – EDN UOBYVM

The problem of the spread of cybercrime in the era of globalization: political aspects

Grigorii A. Maistrenko

PhD in Law, Senior Researcher,
Scientific-Research Institute of Federal Penitentiary Service of Russia,
125130, 15a, Narvskaya str., Moscow, Russian Federation;
e-mail: G.Maystrenko@yandex.ru

Anna G. Maistrenko

PhD in Law,
Associate Professor of the Department of Civil Law Disciplines,
Gubkin University;
Associate Professor of Department of Civil and Entrepreneurial Law,
Russian Foreign Trade Academy of the Ministry of Economic Development
of the Russian federation,
119285, 4a, Pudovkina str., Moscow, Russian Federation;
e-mail: Annamajstrenko@yandex.ru

Abstract

The article is devoted to a comprehensive study of the problem of cybercrime in the era of digitalization and globalization. The author focuses his work on globalization, which promotes progress in various parts of the world and the development of information technology, as well as the current problem of cybercrime, which has a negative impact on modern society. Based on an analysis of scientific publications on this topic, the article examines various forms of cybercrime, their consequences and methods of prevention, as well as the connection between cybercrime and globalization. The purpose of the article can be to outline the impact of globalization on cybercrime and how, with the growth of globalization and information and communication technologies, ordinary crimes are being replaced by crimes of the modern digital world.

For citation

Maistrenko G.A., Maistrenko A.G. (2023) Problema rasprostraneniya kiberprestupnosti v ehpokhu globalizatsii: politicheskie aspekty [The problem of the spread of cybercrime in the era of globalization: political aspects]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 12 (9A), pp. 85-91. DOI: 10.34670/AR.2023.85.89.010

Keywords

Cybersecurity, Internet, cybercrime, globalization, digitalization

References

1. Agarkova A. A., Sinitsyna V.A. Cybercrime in modern Russia. International Journal of Humanities and Building Sciences, 2021. No. 5-3. – pp. 13-16.
2. Bondar E.O. Cybercrime as a new criminal threat. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia, 2020. No. 1. – pp. 155-158.
3. Deryugin R.A. Cybercrime in Russia: the current state and current problems. Bulletin of the Ural Law Institute of the Ministry of Internal Affairs of Russia, 2019. No. 2. – pp. 46-49.
4. Zhakupzhanov, A.O. Victimological factors of cybercrime // Altai Legal Bulletin. 2019. No. 3(27). – pp. 75-82.
5. Kirilenko V.P., Alekseev G.V. Harmonization of Russian criminal legislation on countering cybercrime with the legal standards of the Council of Europe // All–Russian Journal of Criminology. - 2020. – Vol. 14, No. 6. – pp. 898-913.
6. Kovtun K. A. Banking cybercrime as one of the main problems of modern society. Theoretical and applied jurisprudence. 2021. No. 1 (7). – pp. 94-97.
7. Kuvshinova, V.S. Criminological characteristics of cybercrime. International Journal of Humanities and Building Sciences. 2020. No. 5-4. pp. 53-57.
8. Lyapin, A.E. Cybercrime as a new object of statistical analysis // Statistics and Economics. 2021. Vol. 18, No. 6. – pp. 4-16.
9. Mordvinov K.V., Udavikhina U.A. Cybercrime in Russia: current challenges and successful practices in combating cybercrime // Theoretical and applied jurisprudence. 2022. No. 1(11). – pp. 83-88.
10. Samirov R.J., Primakov I.V., Sinitsyn S.N. [et al.] Cybercrime as a threat to the national security of the Russian Federation // Legality and law and order in modern society. 2014. No. 19. – pp. 77-81
11. Ryzhov V.B. Dialectics of globalization and regionalization in the legal space of states and international organizations [Electronic resource] // International law and international organizations. 2020. No. 1. – pp. 29-44. – URL: https://www.e-notabene.ru/mpmag/article_30979.html (date of reference: 09/12/2023).
12. Ryzhov V.B. Information security in the states of the European Union: towards the formulation of the problem // Representative power – XX1 century. 2018. No. 4. – pp. 8-12.
13. AV Zuev, MP Borodin, AV Platonov, EA Gorbarenko The state as a subject of international legal relations: problems of theory and practice //Issues of Russian and international law. – 2023. – Vol. 13. – No. 5A. – p. 23.
14. Cheshin, A.V. Civil law contracts in investment activity / A.V. Cheshin // Issues of Russian and international law. - 2023. – vol. 13, No. 4-1. – pp. 186-192.
15. Cheshin, A.V. Institutional and organizational aspects of attracting investments into the economy of the region / A.V. Cheshin // Public Service. – 2019. – vol. 21, No. 4(120). – pp. 50-57.
16. Cheshin, A.V. Civil law regulation of foreign investments in Russia / A.V. Cheshin // International Law Journal. – 2023. – Vol. 6, No. 6. – pp. 51-55.
17. Oshkordina A. A. DEVELOPMENT OF TELECOMMUNICATION TECHNOLOGIES IN HEALTHCARE //International Forum Kazan Digital Week-2022. – 2022. – pp. 432-438.
18. Lazareva, O. S. Interactive methodology for training specialists in the field of business tourism / O. S. Lazareva, E. A. Magdich // Scientific bulletin of MGUSiT: sport, tourism, hospitality. – 2022. – № 4(74). – Pp. 72-79.
19. Implementing the aarhus convention / R. Yerezhepkyzy, A. Egorov, A. Sadvokassov, V. Shestak // European Energy and Environmental Law Review. – 2021. – Vol. 30, No. 4. – P. 120-127.
20. Egorov, A.M. Features of interaction of domestic special services in the North-West of the Russian Empire in the conditions of the First World War / A.M. Egorov, I. A. Egorov // Metamorphoses of history. – 2023. – № 28. – DOI 10.37490/S230861810025513-4.
21. Musorina, O. A. The Russian language in the Soviet and post-Soviet period / O. A. Musorina, S. G. Sorokina. – Penza : Penza State University of Architecture and Construction, 2014. – 132 p. – ISBN 978-5-9282-1064-9. – EDN VTGNLJ.
22. Strategies of socio-economic development: philosophical, ideological and applied research : a collective monograph / S. V. Drozhzhina, E. V. Barkova, Yu. V. Bulanaya [et al.]. – Moscow : Archont, 2022. – 336 p. – ISBN 978-5-6046534-9-4. – EDN PUEIEA.
23. Popova, I. V. The impact of the financial crisis on the efficiency of banks / I. V. Popova, I. P. Nikitina // Business. Education. The right. – 2016. – № 3(36). – Pp. 160-163. – EDN WGELPL.
24. Popova, I. V. Improving the financial literacy of entrepreneurs as the basis for the stable functioning of banks / I. V. Popova, I. E. Lazareva // The Northern region: science, education, culture. – 2019. – № 3-4(43-44). – Pp. 66-70. – EDN BMFSLE.
25. Popova, I. V. Improving the financial literacy of entrepreneurs-borrowers / I. V. Popova, I. E. Lazareva // Economics: yesterday, today, tomorrow. - 2020. – Vol. 10, No. 5-1. – pp. 389-397. – DOI 10.34670/AR.2020.40.17.047. – EDN TCXOBR.
26. Popova, I. V. Theoretical approaches to building a payment system based on the Blockchain platform in the BRICS countries / I. V. Popova, I. P. Nikitina // Banking services. – 2018. – No. 4. – pp. 2-6. – EDN UOBYVM