МЕЖОТРАСЛЕВЫЕ АСПЕКТЫ ИСПОЛНЕНИЯ НАКАЗАНИЙ

Научная статья
УДК 343.9
doi: 10.33463/2687-122X.2024.19(1-4).1.103-110

СОВРЕМЕННЫЕ ОСОБЕННОСТИ, ПРИЧИНЫ, УСЛОВИЯ И СОВЕРШЕНСТВОВАНИЕ МЕР ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Петр Николаевич Кобец[1], Кристина Александровна Краснова[2]
[1] Всероссийский научно-исследовательский институт МВД России, г. Москва, Россия, pkobets37@rambler.ru, https://orcid.org/0000-0001-6527-3788
[2] Северо-Западный филиал Российского государственного университета правосудия, г. Санкт-Петербург, Россия, krasnova_vnii@mail.ru, https://orcid.org/0000-0003-1545-8025

Аннотация. Статья посвящена исследованию детерминант киберпреступности в России и мер противодействия ей. Раскрываются количественные и качественные характеристики киберпреступлений. Выявляются особенности личности преступника и виктимилогические риски граждан в цифровой среде. Авторы приходят к выводу о решающем значении мер профилактики в борьбе с киберпреступностью и необходимости совершенствования законодательства в рассматриваемой сфере.

Ключевые слова: противодействие киберпреступности, вредоносное программное обеспечение, киберпространство, системы безопасности, кибератаки, предупреждение преступности

Для цитирования
Кобец П. Н., Краснова К. А. Современные особенности, причины, условия и совершенствование мер противодействия киберпреступности // Уголовно-исполнительное право. 2024. Т. 19(1–4), № 1. С. 103–110. DOI: 10.33463/2687-122X.2024.19(1-4).1.103-110.

INTERSECTORAL ASPECTS OF SENTENCES EXECUTION

Original article

MODERN FEATURES, CAUSES, CONDITIONS AND IMPROVEMENT OF MEASURES TO COUNTER CYBERCRIME

Petr Nikolaevich Kobec[1], Kristina Aleksandrovna Krasnova[2]
[1] All-Russian Research Institute of the Ministry of Internal Affairs of Russia, Moscow, Russia, pkobets37@rambler.ru, https://orcid.org/0000-0001-6527-3788
[2] Northwestern Branch of the Russian State University of Justice, St. Petersburg, Russia, krasnova_vnii@mail.ru, https://orcid.org/0000-0003-1545-8025

Abstract. The article is devoted to the study of the determinants of cybercrime in Russia and measures to counter it. The quantitative and qualitative characteristics of cybercrimes are revealed. The features of the criminal's personality and the victimological risks of citizens in the digital environment are revealed. The authors come to the conclusion about the crucial importance of preventive measures in the fight against cybercrime and the need to improve legislation in this area.

Keywords: countering cybercrime, malicious software, cyberspace, security systems, cyber attacks, crime prevention

For citation
Kobec, P. N. & Krasnova, K. A. 2024, 'Modern features, causes, conditionsand improvement of measures to counter cybercrime', *Penal law,* vol. 19(1–4), iss. 1, pp. 103–110, doi: 10.33463/2687-122X.2024.19(1-4).1.103-110.

Интернет вещей, компьютерные системы, сотовая телефония в течение последних двух десятилетий XXI в. смогли произвести революционные преобразования во многих сферах жизнедеятельности, в том числе не только в нашем общении, но и в осуществлении банковских операций, совершении покупок, получении новостей и сфере развлечения. В то же время постоянно развивающиеся в условиях 2020-х гг. технологии создают все новые возможности для совершенствования преступной деятельности, роста числа преступлений, которые совершаются в киберпространстве [1]. Технологические достижения предоставили правонарушителям множество новейших цифровых инструментов для совершения традиционных преступлений и разнообразные возможности для совершения различных форм преступлений в цифровом пространстве [2].

Онлайн-преступления принято называть киберпреступлениями. При этом данную разновидность преступных проявлений необходимо рассматривать в качестве широкого общего термина, охватывающего противоправные деяния, которые совершаются при помощи компьютеров, где эта же компьютерная техника применяется во вспомогатель-

ной роли, например, использование компьютера для отправки фишинговых сообщений. Одновременно в понимание киберпреступности «включаются противоправные деяния, совершаемые с использованием компьютеров, которые являются прямым результатом компьютерных технологий и не существовали бы без них, примером может служить несанкционированное проникновение в компьютерную систему» [3, с. 25].

Практически невозможно точно назвать общее число ежегодно совершаемых на планете киберпреступлений, поскольку отсутствуют их единые стандартизированные юридические дефиниции. Вместе с тем имеющиеся статистические данные дают основание утверждать, что показатели киберпреступности имеют тенденцию роста во многих странах, при этом показатели многих форм традиционных преступлений продолжают снижаться.

Согласно официальным данным, за первое полугодие 2022 г. в нашей стране было зафиксировано совершение 249 тыс. преступлений с использованием информационно-телекоммуникационных технологий[1]. Иными словами, каждое четвертое преступное посягательство было совершено с использованием рассматриваемых технологий. При этом преступниками все активнее распространяются шпионские программы, направленные на хищение учетных данных.

Важно отметить, что киберпреступность не только количественно, но и качественно отличается от традиционных преступлений. Прежде всего киберпреступления совершаются с использованием компьютерных систем в качестве инструмента совершения преступлений и, как правило, требуют от преступников определенных технических знаний. Таким образом, по мере развития технологий во всем мире меняется и характер совершения преступлений.

Киберпреступления являются относительно новым видом преступных посягательств, что во многом объясняет неподготовленность мирового сообщества в целом к борьбе с ними. Большинство подобных преступлений редко совершаются одиночками. Как правило, в них участвуют большие группы преступников. Многие их этих преступлений направлены в первую очередь против финансовых и банковских структур, а также простых пользователей. Кроме того, «в атаках на частных лиц учетные данные составили 46 % случаев от общего объема похищенной информации, а особый интерес у киберпреступников продолжают представлять учетные данные различных VPN-сервисов, которые впоследствии реализовываются на теневых форумах»[2].

Многие из киберпреступлений представляют собой преступные атаки, совершаемые в киберпространстве с целью завладения информационными данными как простых пользователей, так и различных компаний и корпораций. Виртуальные атаки происходят в отношении различных учреждений, организаций и корпораций, которые представляют собой набор цифровых информационных атрибутов, определяющих физических лиц, а также различные учреждения, функционирующие в интернет-пространстве. Одним словом, «в цифровую эпоху виртуальные личности являются важными элементами повседневной жизни. Современная киберпреступность подчеркивает центральную роль сетевых компьютерных систем в повседневной жизни, а также хрупкость таких, казалось бы, надежных составляющих, как индивидуальная идентичность» [4, с. 35].

[1] См.: Почти 250 тысяч киберпреступлений совершено за полгода в РФ. URL: https://aif.ru/incidents/pochti_250_tysyach_kiberprestupleniy_sovershenо_za_polgoda_v_rf (дата обращения: 12.12.2022).

[2] Актуальные киберугрозы: I квартал 2022 г. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ (дата обращения: 12.12.2022).

Одним из «важнейших аспектов рассматриваемой преступности является ее нелокальный характер, то есть ее действия могут происходить в юрисдикциях, разделенных огромными расстояниями, что, в свою очередь, приводит к возникновению серьезных проблем у правоохранительных органов» [5, с. 41]. Будучи национальными преступными посягательствами, современные киберпреступления все больше приобретают транснациональный характер, требуя активизации международного сотрудничества для их эффективного противодействия. Кроме того, все чаще возникают проблемы при расследовании киберпреступлений, и все из-за того, что данный вид противоправной деятельности не имеет границ, а в каждом государстве собственные меры ответственности за совершение киберпреступлений [6].

Следует также согласиться с позицией отечественных экспертов, которые отмечают, что сегодня киберпреступностью охватывается весьма широкий спектр противоправных деяний. Это преступные посягательства, связанные с нарушениями конфиденциальности, кражей личных данных, основанные на транзакциях, попытками нарушить работу компьютерного оборудования и телекоммуникационных сетей. Они варьируются от спама, хакерских атак до актов кибертерроризма, то есть использования цифрового пространства для устрашения населения. Все перечисленное является конкретными видами преступных посягательств со множеством потерпевших, несмотря на то что лица, совершающие эти противоправные деяния, находятся в относительной анонимности, которую им обеспечивает цифровое пространство [7].

Таким образом, во все более цифровизирующемся мире киберпреступность представляет мощнейшую угрозу как для отдельных лиц, так и для общества в целом. В настоящее время киберпреступники используют все возможности, которые они видят в сетях, системах и программах. Воспользовавшись этими уязвимыми местами компьютерных систем, они могут нанести серьезный ущерб как простым пользователям, так и целым компаниям, корпорациям и даже государствам.

Апеллируя различными информационными данными, можно прийти к выводу о том, что предпринимаемые попытки противодействия киберпреступлениям, к сожалению, не демонстрируют больших положительных результатов. Общедоступность виртуальных пространств позволила киберпреступности стать повседневным явлением [8].

Широкое распространение киберпреступной деятельности является проблемой при раскрытии и судебном преследовании данных преступлений. Искать виновных в киберпреступлениях и бороться с этим явлением сложно, поскольку киберпреступники используют интернет-пространство для совершения трансграничных кибератак. Интернет-пространство не только позволяет совершать преступления из любого места на планете, но и увеличивает масштаб причиняемого вреда. Кроме того, киберпреступники могут атаковать одновременно несколько человек [9].

Вместе с тем по мере распространения киберпреступности развивалась и ее профессиональная экосистема «для поддержки отдельных лиц и групп, стремящихся получить прибыль от киберпреступной деятельности, и к настоящему времени данная экосистема стала довольно специализированной, включая разработчиков вредоносных программ, операторов-ботнетов, профессиональные группы киберпреступников» [10]. К ней примыкают группы, специализирующиеся на продаже украденного цифрового контента, и другие подобные лица.

Из-за различия в законодательстве для совершения преступлений киберпреступникам проще использовать территории развивающихся стран, «чтобы избежать обнару-

жения и судебного преследования со стороны правоохранительных органов, поскольку в развивающихся странах законы против киберпреступности недостаточно эффективны, а иногда и вовсе отсутствуют. Недостаточно эффективная законодательная база по борьбе с киберпреступностью позволяет киберпреступникам наносить удары из-за границы и оставаться незамеченными. Даже будучи идентифицированными, эти преступники избегают наказания или экстрадиции в страны, которые разработали законы, допускающие судебное преследование данных лиц» [11].

Поскольку преступники, совершая рассматриваемые виды преступлений, пользуются шифрованием, а также иными методами, позволяющими им эффективно скрывать свои персональные данные, их сложно отследить после совершения преступлений, поэтому меры профилактики рассматриваемых преступлений имеют решающее значение в борьбе с киберпреступностью [12]. Приоритетное значение отводится правовым мерам, которые должны устанавливать единые подходы к пониманию противоправных деяний, которые могут быть совершены в телекоммуникационной сфере, несмотря на имеющуюся специфику использования цифровых технологий в отдельных отраслях экономики.

Российская Федерация выступает за сохранение свободного и открытого киберпространства, при этом государство должно всячески усиливать информирование граждан о рисках манипуляций и преступных методах, используемых злоумышленниками в сети Интернет. Правоохранительные органы должны постоянно совершенствовать деятельность по выявлению киберпреступников и предоставлению населению рекомендаций по осуществлению мер самозащиты от киберпосягательств. В то же время важно отметить, что противодействие киберпреступности посредством обучения необходимым мерам безопасности населения в цифровой среде должно стать долгосрочной отраслевой работой, поскольку просвещение общества, а затем последовательное изменение поведения граждан – это та проблема, которой необходимо заниматься уже сегодня.

В настоящее время профилактический потенциал такой работы недооценен. Органы внутренних дел не реагируют на попытки совершения киберпреступлений, отказывая в возбуждении уголовных дел в отсутствие материального ущерба в случаях, когда более просвещенные в цифровых вопросах граждане сообщают о противоправных попытках похитить их денежные средства в приложениях банков или несанкционированно разместить их личные данные в цифровой среде. Но отсутствие реакции правоохранителей на подобные попытки приводит лишь к тому, что преступники продолжают попытки до тех пор, пока не найдут жертву, слабо разбирающуюся в вопросах пользования современными гаджетами до такой степени, что даже не поймет, что в отношении нее совершено противоправное посягательство. Чаще всего такими жертвами становятся пожилые люди, которые наслышаны о современных технологиях, но в силу возраста и недостатка опыта пользования ими не понимающие грань преступного и непреступного, доверчиво сообщая преступникам свои личные данные или передавая им накопления за решение якобы имеющихся проблем в цифровой среде.

Количество научных исследований киберпреступности растет «в геометрической прогрессии, однако при этом большая часть предварительной работы в этой области была сосредоточена на изучении того, чем природа киберпреступности и киберпространства отличается от традиционной преступности» [13]. Вместе с тем нельзя не отметить, что в настоящее время многими государствами по всему миру вкладыва-

ются большие суммы на инвестиции в кибербезопасность. В то же время было бы неплохо, если часть этих ресурсов была бы направлена на разработку инструментов для оценки эффективности работы различных субъектов профилактики по снижению уровня киберпреступности.

К большому сожалению, в настоящее время не хватает основанных на фактических данных исследований, проверяющих эффективность уголовной политики в сфере противодействия киберпреступности. В силу этого чрезвычайно важно, чтобы научные разработки в рассматриваемой сфере превратились в ключевые источники информации для специалистов в сфере кибербезопасности. Эти научные исследования должны прежде всего отвечать на вопрос, каким образом уменьшить число различных форм киберпреступности.

Список источников

1. Краснова К. А. Киберспорт и преступность // Научный портал МВД России. 2021. № 4(56). С. 30–33.

2. Кобец П. Н., Краснова К. А. О современных информационных технологиях, используемых экстремистскими и террористическими организованными группами, и необходимости противодействия киберпреступности // Вестник Дальневосточного юридического института МВД России. 2018. № 2(43). С. 75–79.

3. Иванова Л. В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. № 1. С. 25–33.

4. Зверева Е. Б. Киберпреступность как угроза безопасности современного общества: виды, особенности, методы борьбы и профилактики // Молодой ученый. 2020. № 10(300). С. 35–37.

5. Бочкин Д. В. Способы совершения компьютерных преступлений и использование информационных технологий как способ совершения преступления // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 5(13). С. 40–46.

6. Ушакова Е. В., Ткаченко Д. Г. Киберпреступность в современном мире: популярность или доступность цифровых технологий // Теория права и межгосударственных отношений. 2021. Т. 1, № 1(13). С. 15–27.

7. Жестеров П. В. Влияние цифровой трансформации на уголовную репрессию // Муниципальная служба: правовые вопросы. 2022. № 1. С. 21–24.

8. Кобец П. Н. Отечественные и зарубежные подходы по разработке понятийного аппарата в сфере борьбы с кибертерроризмом и предложения по совершенствованию данного нормотворческого процесса // Правопорядок: история, теория, практика. 2022. № 1(32). С. 94–101.

9. Кобец П. Н. Информационное воздействие как один из современных методов терроризма и меры борьбы с ним // Вестник Краснодарского университета МВД России. 2022. № 1(55). С. 10–14.

10. Кобец П. Н., Краснова К. А. Об общественной опасности киберсталкинга и необходимости его предупреждения // Вестник Восточно-Сибирского института МВД России. 2018. № 3(86). С. 77–83.

11. Сундиев И. Ю. Эволюция вербовочных технологий в цифровую эпоху // Научный портал МВД России. 2018. № 1(41). С. 67–76.

12. Воронин Ю. А., Майоров А. В. Теоретические основы формирования системы противодействия преступности в России // Криминологический журнал Байкальского государственного университета экономики и права. 2013. № 1. С. 7–16.

13. Денисов Н. Л. Негативные изменения киберпреступности в период пандемии и пути противодействия им // Безопасность бизнеса. 2020. № 4. С. 37–42.

References

1. Krasnova, K. A. 2021, 'Esports and Crime', *Scientific Portal of the Ministry of Internal Affairs of Russia,* iss. 4(56), pp. 30–33.

2. Kobets, P. N. & Krasnova, K. A. 2018, 'On modern information technologies used by extremist and terrorist organized groups, and the need to counter Cybercrime', *Bulletin of the Far Eastern Law Institute of the Ministry of Internal Affairs of Russia,* iss. 2(43), pp. 75–79.

3. Ivanova, L. V. 2019, 'Types of cybercrimes under Russian criminal law', *Legal Studies,* iss. 1, pp. 25–33.

4. Zvereva, E. B. 2020, 'Cybercrime as a threat to the security of modern society: types, features, methods of control and prevention', *Young Scientist,* iss. 10(300), pp. 35–37.

5. Bochkin, D. V. 2016, 'Methods of committing computer crimes and the use of information technology as a way of committing a crime', *Siberian Criminal Procedural and Criminalistic Readings,* iss. 5(13), pp. 40–46.

6. Ushakova, E. V. & Tkachenko, D. G. 2021, 'Cybercrime in the modern world: popularity or accessibility of digital technologies', *Theory of Law and Interstate Relations,* vol. 1, iss. 1(13), pp. 15–27.

7. Gesterov, P. V. 2022, 'The impact of digital transformation on criminal Repression', *Municipal Service: Legal Issues,* iss. 1, pp. 21–24.

8. Kobets, P. N. 2022, 'Domestic and foreign approaches to the development of a conceptual apparatus in the field of combating cyberterrorism and proposals for improving this rule-making process', *Law and order: History, theory, practice,* iss. 1(32), pp. 94–101.

9. Kobets, P. N. 2022, 'Information impact as one of the modern methods of terrorism and measures to combat it', *Bulletin of the Krasnodar University of the Ministry of Internal Affairs of Russia,* iss. 1(55), pp. 10–14.

10. Kobets, P. N. & Krasnova, K. A. 2018, 'On the public danger of cyberstalking and the need to prevent it', *Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia,* iss. 3(86), pp. 77–83.

11. Sundiev, I. Yu. 2018, 'The evolution of recruitment technologies into digital epoch', *Scientific Portal of the Ministry of Internal Affairs of Russia,* iss. 1(41), pp. 67–76.

12. Voronin, Yu. A. & Mayorov, A.V. 2013, 'Theoretical foundations of the formation of a crime prevention system in Russia', *Criminological Journal of the Baikal State University of Economics and Law,* iss. 1, pp. 7–16.

13. Denisov, N. L. 2020, 'Negative changes in cybercrime during the pandemic and ways to counter them', *Business Security,* iss. 4, pp. 37–42.

Информация об авторе

П. Н. Кобец – доктор юридических наук, профессор, главный научный сотрудник центра организационного обеспечения научной деятельности;

К. А. Краснова – кандидат юридических наук, доцент, доцент кафедры уголовного права.

Information about the author

P. N. Kobec – Doctor of Law, Professor, Chief Researcher at the Center for Organizational Support of Scientific Activities;

K. A. Krasnova – Candidate of Law, Associate Professor, Associate Professor of the Department of Criminal Law.

Примечание

Содержание статьи соответствует научной специальности 5.1.4. Уголовно-правовые науки (юридические науки).

Статья поступила в редакцию 12.12.2023; одобрена после рецензирования 22.01.2024; принята к публикации 05.02.2024.

The article was submitted 12.12.2023; approved after reviewing 22.01.2024; accepted for publication 05.02.2024..