Дата поступления рукописи в редакцию: 09.07.2026 г.
Дата принятия рукописи в печать: 03.08.2026 г.
DOI: 10.24412/2076-1503-2026-7-697-701

БОБРОВА Ирина Анатольевна,

кандидат психологических наук, доцент,
старший преподаватель кафедры специальной и автомобильной техники
Санкт-Петербургского университета МВД России,

e-mail: mail@law-books.ru

СТАУРСКИЙ Евгений Станиславович,

кандидат технических наук, доцент,
доцент кафедры экономической теории и финансового права
Омской ордена Почета академии МВД России,

e-mail: mail@law-books.ru

К ВОПРОСУ О ПРЕСТУПЛЕНИЯХ, СОВЕРШАЕМЫХ ПОСРЕДСТВАМ СЕТИ ИНТЕРНЕТ: ПОНЯТИЕ, ВИДЫ КИБЕРПРЕСТУПЛЕНИЙ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ

Аннотация. *Автор в своей научной статье рассматривает сущность и различные виды и формы киберпреступлений, способы и методы защиты от злоумышленников, проблемы по профилактике и борьбе с киберпеступлениями осуществляемыми правоохранительными органами на современном этапе в Российской Федерации.*

Ключевые слова: *киберпреступление, интернет, мошенничество, цифровизация, государство, общество, законодательство, правоохранительные органы, сайт, профилактика, безопасность, закон.*

BOBROVA Irina Anatolyevna,

PhD in Psychology, Associate Professor, Senior Lecturer,
Department of Specialized and Automotive Equipment,
St. Petersburg University of the Ministry of Internal Affairs of Russia

STAURSKY Evgeny Stanislavovich,

Candidate of Technical Sciences, Associate Professor,
Associate Professor, Department of Economic Theory and Financial Law,
Omsk Order of Honor Academy of the Ministry of Internal Affairs of Russia

ON THE ISSUE OF CRIMES COMMITTED VIA THE INTERNET: THE CONCEPT, TYPES OF CYBERCRIMES AND METHODS OF COUNTERACTION

Annotation. *In this scientific article, the author examines the nature and various types and forms of cybercrime, methods and techniques for protecting against cybercrime, and the challenges of preventing and combating cybercrime carried out by law enforcement agencies in the Russian Federation today.*

Key words: *cybercrime, internet, fraud, digitalization, government, society, legislation, law enforcement, website, prevention, security, law.*

На современном этапе одной из важнейших задач правоохранительных органов является обеспечение безопасности общества и государства в сфере информационных технологий и интернет-пространства. Данная необходимость вызвана ростом преступлений совершаемых в телекоммуникационных сетях интернет, поскольку именно интернет площадка стало одним из методов и средств реализации различного вида киберпреступлений, начиная от преступлений в сфере посягательства на чужое

имущество граждан заканчивая банальными проявлениями так называемых кибер-вандалов целью которых не какая-либо финансовая выгода, а привлечение внимания к своим возможностям и методам воздействия разрушая целостность критической информационной инфраструктуры потенциальной жертвы, тем самым показывая свое превосходство над возможностями жертв по защите конфиденциальной информации, что носит угрожающий и раскрывающий секретную информацию характер.

Государственные стратегические документы последовательно выделяют неконтролируемый характер интернета как одну из главных угроз национальным интересам. Это объясняется тем, что анонимность, глобальный охват и скрытность онлайн-среды существенно затрудняют государственные усилия по выявлению, пресечению и квалификации преступлений. Как отмечают эксперты, с которыми мы согласны несмотря на то, что быстрое развитие современных информационных технологий и их применения создает определенные пробелы в законодательстве, своевременное совершенствование отраслевых законов приобретает решающее значение для предотвращения масштабного распространения противоправного деяния. В современном социуме, уже известно о различных категориях и видах преступлений в сфере цифровизации, которые подразделяются на различные подвиды, такие как:

Кейлогер, то есть клавиатурный шпион, один из видов вредоносных программных обеспечений, позволяющих злоумышленнику завладеть информацией потенциальной жертвы, в момент работы и применения клавиатуры, в процессе которого набираемая информация в виде текста, автоматический посредством утечки информации передается третьим лицам, вопреки желания жертвы хакера, поскольку данное противоправное действие происходит скрытно.

Логическая бомба – вредоносное программное обеспечение, средство уничтожения, искажения и обнародования конфиденциальной информации в нужный момент для злоумышленника, носит скрытный характер и причиняет значительный ущерб персональному компьютеру и информации потенциальной жертве.

Компьютерный червь, иначе говоря вирус, проникающий в цифровое персональное пространство жертвы и размножающаяся в его информационной среде и передающая информацию сразу нескольким киберпреступникам и иным заинтересованным злоумышленникам.

Приведенный выше перечень интернет ресурсов, применяющихся злоумышленниками в сети интернет, далеко не исчерпывающий, поскольку существует еще множество вредоносных программных обеспечений и применение их зависит от целей и намерений злоумышленников, а также подверженной посягательству категории лиц, поскольку цели преступного сегмента, далеко не случайные пользователи, а в большинстве случаев материально обеспеченные и финансово выгодные злоумышленникам, потому что хакеры, осуществляют свою противоправную деятельность в целях повышения материального благосостояния. Кроме того, хакеры подразделяются на категории орудующих в цифровом пространстве и промышляющих киберджекингом, фишингом, кибершантажом и иными противоправными посягательствами имеющих цель- финансовое обогащение. Располагая информацией, уже ставшей известной о таких проявлениях и возможностях злоумышленников, правоохранительным органам, в целях защиты информации и в целом обеспечения информационной защищенности и безопасности общества и государства предпринимаются различные методы борьбы с данным преступными проявлениями. В связи с чем, повышается эффективность систем безопасности информации, формируются управления и отделы по борьбе с киберпреступностью, в организациях формируются отделы IT- безопасности, и их деятельность с каждым годом расширяется.

Говоря о стремительно возросшем уровне и числе преступлений, что делает киберпреступность достаточно распространенной и опасной, так как такие преступления как взломы паролей от сайтов и страниц, вплоть до заказа специальными службами разных стран у анонимных группировок атак на правительственные организации недружественных стран. Необходимо отметить, что в каждом последующем году количество атак и размеров выплат хакерам увеличиваются. Кибератаки происходят постоянно. Больше всего преступники интересуются образовательными, исследовательскими сайтами, сайтами правительства и военных структур.

Законодательство в сфере кибербезопасности постоянно совершенствуется в ответ на новые угрозы и возрастающие размеры ущерба, причиняемого в результате совершенствования киберпреступлений.

Кроме этого, постоянно ведется работа по активизации деятельности государственных регуляторов и правоохранительных органов по защите интересов государства и общества. На данном этапе киберпреступность считается преступлением глобального масштаба, наносящая ущерб пользователям сети интернет

колосального размера, исчисляющаяся сотни миллиардов долларов и продолжает суммарно возрастать, что обуславливает заинтересованных органов, принимать самые действенные меры по ее противодействию. Следует отметить, что система противодействия киберпреступности в Российской Федерации недостаточно эффективна, поскольку в ней есть и пробелы, и недостатки в организации безопасности информации. Существует некоторый дефицит в высококвалифицированных специалистах способных противодействовать преступности в данной сфере, кроме того, необходимо сформировать и практиковать современные механизмы взаимодействия на мировом уровне и в последующем развивать тесное сотрудничество на транснациональном масштабе. Само понятие киберпреступность можно охаратеризовать как совокупность противоправных проявлений в информационном пространстве, представляющих угрозу безопасности критической информационной инфраструктуре всех пользователей информационных технологий и виртуального пространства или в рамках компьютерной информационной сети и иных интернет-ресурсов.

Также выделяют классификацию киберпреступлений по различным признакам:

1. По способу использования: компьютер является объектом правонарушения; компьютер используется как запоминающее устройство; компьютер используется как средство, способствующее совершению киберпреступления.

2. По наличию насилия: на агрессивные (кибертерроризм, угроза физической расправы, детская порнография) и неагрессивные (киберкража, кибервандализм, кибермошенничество, кибершпионаж, распространение спама и вирусных программ).

3. По способу воздействия выделяют следующие злоупотребления: физические, операционные, программные, электронные.

Киберпреступления вызваны рядом экономических причин, одним из которых является масштабное использование вредоносных компьютерных программ.

Вместе с тем, производители лицензионной продукции, для затруднения деятельности конкурентов и создания зависимости пользователей от их антивирусных программ, создают вредоносные программы.

Порождает наличие киберпреступности и тот факт, что прибыль от киберпреступлений относительно быстрая и ее легко легализовать с помощью компьютерных технологий и киберпреступников, совершающих хищения. Таким образом, киберпреступность значительно влияет на экономические системы начиная от мировой заканчивая финансовой системой, нарушая при этом связи между элементами данных систем.

Информация выступает объектом преступной деятельности в сфере информационных и телекоммуникационных технологий. Зачастую, ее неправомерное использование является конечной или промежуточной целью преступников. Их деятельность направлена на нарушение стабильного функционирования информационных источников в экономических системах, так как информация является базовым экономическим ресурсом.

В связи с этим, наряду с анонимностью и межгосударственностью их деятельности хакеры не позволяют формироваться новым институтам, способным взаимодействовать с иными формациями находя компромиссы. Таким образом, можно сделать выводы, что киберпреступность - очень выгодная сфера преступной деятельности, которая носит организованный и транснациональный характер.

Критическая информационная инфраструктура по существу является объектом и предметом преступления, а информация, хранящаяся на этих объектах, и является предметом кражи в различных видах, содержаниях и значимости. В дальнейшем рассматривая преступления в данной сфере, целесообразно отметить виды и способы совершения преступлений в сфере информации и иных компьютерных инцидентов, таких как, например:

Неправомерное завладение информации;

утечка персональных данных;

Искажение или уничтожение посредствам вредоносных программных обеспечений личных или иной охраняемых сведений;

Кибермошенничество;

Кибершантаж;

Компьютерный абордаж;

Кибератаки, в том числе с использованием DoS атак и т.д.

В виду стремительного развития информационных технологий и увеличения количества активных пользователей сети интернет, возрастает и количество преступлений в сфере информационного пространства, что конечно же обязывает предпринимать новейшие технологии, разработки и методы противодействия данным проявлениям, что создает определенные трудности для правоохранительных органов

В действующем УК РФ есть только одна глава, которая предусматривает ответственность за киберпреступления – глава 28 «Преступления в сфере компьютерной информации», которая

содержит только три статьи, которые привязаны к определенным вредоносным программно-техническим действиям в сети, а именно ст. 272-274 УК РФ.

В частности, статья 272 УК РФ предусматривает ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло ее уничтожение, блокирование, модификацию либо копирование.

Актуально отметить, что фактическое повреждение компьютера, повлекшее уничтожение информации, хранящейся в нем, не влечет за собой последствий, предусмотренных рассматриваемой статьей, потому что объектом преступного посягательства является компьютерная информация, а не носители таковой. Таким образом, основные методы борьбы с киберпреступностью сводятся к нормативно-правовому регулированию и созданию специальных органов. Кроме того, нестандартность, многообразие и обновление способов совершения преступлений в виртуальном пространстве требуют постоянного совершенствования методов борьбы с ними, и зачастую оказываются устаревшими и неэффективными.

В виду чего, объективно важно совершенствовать способы противодействия преступлениям в интернет-пространстве и актуально и необходимо совершенствовать навыки и способности в области компьютерных технологий и программного обеспечения сотрудников правоохранительных органов. Внедрение этих мероприятий даст возможность перейти от пассивного реагирования на противоправные деяния в сети Интернет к активной системе их квалификации, которая будет опираться на принципы законности, технологической нейтральности, соразмерности и защиты прав человека. Лишь при комплексном подходе к развитию административно-юрисдикционной деятельности можно обеспечить стабильный правопорядок в цифровом пространстве, отвечающий современным вызовам и стратегическим задачам государственной политики в области информационной безопасности.

Список литературы:

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ (с изм. от 29 июля 2017 г. № 250-ФЗ) // Собрание законодательства РФ. - 1996. - № 25. - ст. 2954.

[2] Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» // Собрание законодательства РФ. – 2011. – № 27. – ст. 3872. 7.

[3] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. – 2006. – № 31. – ст. 3448. 8.

[4] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. – 2016. – № 50. – ст. 7074.

[5] Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие / А. В. Аносов. – М.: Академия управления МВД России, 2019. – 208 с.

[6] Артамонов В.А. Кибербезопасность в условиях цифровой трансформации социума / В.А. Артамонов // Большая Евразия: развитие, безопасность, сотрудничество. – 2022. – № 1. – С. 777-784.

[7] Ахриева М.М. Киберпреступность в условиях современной экономики / М.М. Ахриева // Международный журнал гуманитарных и естественных наук. – 2021. – № 8-2 (59). – С. 80-82.

[8] Диденко К.В. Некоторые проблемы выявления и предупреждения киберпреступлений / К.В. Диденко // Вестник БЮИ МВД России. – 2020. – № 3. – С. 20-24.

[9] Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения: монография / Е.А. Русскевич. – М.: ИНФРА-М, 2019. – 227 с.

[10] Шикула И.Р., Куркин Е.Н. Киберпреступность в Российской Федерации: основные методы борьбы и проблемы противодействия // Международный журнал экспериментального образования. – 2023. – № 1. – С. 37-41.

References:

[1] Criminal Code of the Russian Federation of June 13, 1996 No. 63-FZ (as amended on July 29, 2017 No. 250-FZ) // Collected Legislation of the Russian Federation. - 1996. - No. 25. - Art. 2954.

[2] Federal Law of June 27, 2011 No. 161-FZ “On the National Payment System” // Collected Legislation of the Russian Federation. - 2011. - No. 27. - Art. 3872. 7.

[3] Federal Law of July 27, 2006 No. 149-FZ “On Information, Information Technologies and Information Protection” // Collected Legislation of the Russian Federation. - 2006. - No. 31. - Art. 3448. 8.

[4] Decree of the President of the Russian Federation of 05.12.2016 No. 646 “On Approval of the Doctrine of Information Security of the Russian Federation” // Collected Legislation of the Russian

Federation. - 2016. - No. 50. - Art. 7074.

[5] Anosov A.V. Activities of internal affairs bodies to combat crimes committed using information, communication and high technologies: a textbook / A. V. Anosov. - Moscow: Academy of Management of the Ministry of Internal Affairs of Russia, 2019. - 208 p.

[6] Artamonov V.A. Cybersecurity in the Context of the Digital Transformation of Society / V.A. Artamonov // Greater Eurasia: Development, Security, Cooperation. - 2022. - No. 1. - P. 777-784.

[7] Akhrieva M.M. Cybercrime in the Context of the Modern Economy / M.M. Akhrieva // International Journal of Humanities and Natural Sciences. - 2021. - No. 8-2 (59). - P. 80-82.

[8] Didenko K.V. Some Problems of Detecting and Preventing Cybercrimes / K.V. Didenko // Bulletin of the Law Institute of the Ministry of Internal Affairs of Russia. - 2020. - No. 3. - P. 20-24.

[9] Russkevich E.A. Criminal Law and “Digital Crime”: Problems and Solutions: Monograph / E.A. Russkevich. - Moscow: INFRA-M, 2019. - 227 p.

[10] Shikula I.R., Kurkin E.N. Cybercrime in the Russian Federation: Main Methods of Combating and Problems of Counteraction // International Journal of Experimental Education. – 2023. – No. 1. – P. 37-41.