

УДК 34

<https://doi.org/10.25587/2587-5612-2025-3-47-53>

Оригинальная научная статья

К вопросу о понятии «цифровая преступность»

А.А. Павлова

Северо-Восточный федеральный университет имени М.К. Аммосова,
г. Якутск, Российская Федерация

E-mail: arzulana@bk.ru

Аннотация

В статье рассматриваются подходы к пониманию термина, обозначающего преступность, совершаемую в виртуальном пространстве с использованием цифровых технологий. Появление интереса к данной теме продиктовано не только широким распространением данного вида преступности, но также и появлением нового направления в криминологической науке – «цифровая криминология», что актуализирует исследования, посвященные цифровой преступности. Для полного понимания исследуемого явления необходимо привести к единообразию определение ключевого термина, обозначающего преступность, совершаемую в виртуальном пространстве с использованием цифровых технологий, что, полагаем, достигнуто в исследовании путем фиксации точной и однозначной дефиниции, устраняющей разночтения и синонимии.

Ключевые слова: цифровая криминология, цифровая преступность, преступность в сфере ИКТ, компьютерная преступность, киберпреступность.

Финансирование. Исследование не имело финансовой поддержки.

Для цитирования: Павлова А.А. К вопросу о понятии «цифровая преступность». *Вестник Северо-Восточного федерального университета имени М.К. Аммосова. Vestnik of North-Eastern Federal University. Серия «Общественные науки. Social science»*. 2025, № 3: С. 47-53. DOI: 10.25587/2587-5612-2025-3-47-53

Original article

On the concept of «digital crime»

A.A. Pavlova

M.K. Ammosov North-Eastern Federal University, Yakutsk, Russian Federation

E-mail: arzulana@bk.ru

Abstract

The article discusses approaches to understanding the term that refers to crime committed in the virtual space using digital technologies. The emergence of interest in this topic is driven not only by the widespread nature of this type of crime, but also by the emergence of a new field in criminology, known as “digital criminology,” which has led to increased research on digital crime. In order to fully understand the phenomenon under study, it is necessary to bring the definition of the key term, which refers to crime committed in the virtual space using digital technologies, to a unified standard. We believe that this has been achieved in the study by providing an accurate and unambiguous definition that eliminates ambiguity and synonymy.

Keywords: digital criminology, digital crime, ICT crime, computer crime, cybercrime

Funding. No funding was received for writing this manuscript.

For citation: Pavlova A.A. On the concept of «digital crime». *Vestnik of North-Eastern Federal University. Social science*. 2025, № 3: P. 47-53. DOI: 10.25587/2587-5612-2025-3-47-53

Введение

В современном мире проблема цифровой преступности становится все более серьезной и опасной, так как захват преступниками конфиденциальной информации может повлечь за собой не только финансовые потери, репутационный ущерб, юридические по-

следствия и угрозу жизни и здоровью людей, а также ущерб компаниям, но и может привести к раскрытию государственных, военных или коммерческих тайн и их использованию в ущерб экономической безопасности и обороноспособности страны. В связи с усилением цифровизации стали более выражены наметившиеся в предыдущие годы, до пандемии «COVID-19», тенденции цифровой преступности, увеличились ее масштабы, разнообразие и причиненный ущерб. Анализ правоохранительной практики в области борьбы с цифровой преступностью показывает, что с каждым годом эта проблема становится все более актуальной из-за стремительного развития технического прогресса и появления новых технологий, которые преступники активно используют в своих целях.

В юридической литературе, правоприменительной практике наблюдается расхождение в понимании рассматриваемого вида преступности, что проявляется в разном применении и толковании терминов «киберпреступность», «цифровая преступность (преступление)», «преступление в сфере компьютерной информации» и др. К основным причинам расхождений можно отнести быстрое развитие технологий, несовершенство терминологии, сложность юридической квалификации, отсутствие единого подхода и т.д.

Единообразное понимание термина цифровой преступности необходимо для эффективной борьбы с ней, создания адекватного правового регулирования, точной квалификации преступлений, улучшения международного сотрудничества и своевременной адаптации к быстрому развитию технологий. Отсутствие четких определений затрудняет выявление и расследование преступлений, а также разработку мер профилактики и защиты информационных систем.

Материалы и методы: базовые положения диалектического метода научного познания явлений и процессов окружающей действительности, позволяющие отразить взаимосвязь теории и практики, форму и содержание предмета исследования; процессы развития и качественных изменений рассматриваемых явлений. Также применялась совокупность общенаучных, частнонаучных (специально-юридических) методов исследования: формально-логического, индукции и дедукции, структурно-функционального и др.

Результаты и обсуждение

Облик современного мира меняется каждый день. Если прошлые два столетия стали этапом стремительного развития промышленности, то XXI век – время расцвета информационных технологий и цифровизации.

Цифровизация – это внедрение современных цифровых технологий в различные сферы жизни и производства. Одним из показателей успешной глобальной цифровизации является открытая информация, которая меняет социальные, политические и бизнес-процессы и должна приводить к улучшению качества жизни.

Современные информационно-телекоммуникационные и цифровые технологии не всегда служат во благо общества. Их стремительное развитие уже спровоцировало возникновение и колоссальный рост преступности, совершаемой в цифровом пространстве, а также ее постоянную трансформацию.

В настоящее время цифровое пространство охватывает все сферы жизнедеятельности государства и общества. Цифровые платформы аккумулируют все ключевые ресурсы – финансы, время, внимание и поля активности людей, групп, сообществ. К ним перетекает от государств доля политической и юридической власти: через внутреннюю регуляторику платформ оказывается влияние на экономику и общество, сопоставимое с правовыми регуляторами – законами. В управлении этими регуляторными механизмами (алгоритмами выдачи, сбора и обработки информации о пользователях, приоритизации информации) все большее участие принимает искусственный интеллект. Мы уже фактически живем в мире,

частично управляемом роботами, но за ними стоят их хозяева – конкретные люди или их структурированные сообщества.

В настоящее время в нормативных источниках и в научной правовой литературе для обозначения преступлений, связанных с использованием информационно-телекоммуникационных и цифровых технологий, активно используются разные термины, обозначающие порой одну и ту же совокупность видов преступных деяний. Вот их неполный примерный перечень: «компьютерная преступность», киберпреступность, «преступность в сфере высоких технологий», «преступность в сфере информационных технологий», «преступность с использованием информационно-коммуникационных технологий», «цифровая преступность» и т.д. Такое положение является фактором, существенно затрудняющим уяснение содержания термина «цифровая преступность», а значит использование его в практике расследования преступлений, совершаемых в цифровом пространстве.

Кроме того, что этот термин понимается и определяется по-разному, отсутствуют и надлежащие статистические данные по этим видам преступлений. В России понятие «цифровая преступность» на законодательном уровне также отсутствует. Для российской криминологической науки понятие «цифровая преступность» также является новым, недостаточно исследованным. Есть зарубежный опыт исследования киберпреступности, но он тоже не дает полной картины и определения тем преступлениям, которые совершаются в сфере цифровых технологий или с их использованием.

Первоначально говорилось о компьютерной преступности. Этот термин впервые был использован в одном из докладов Стэнфордского исследовательского института [1], а содержательное его наполнение постоянно расширялось на международных площадках: на сессиях Конгрессов ООН, в директивах ОЭСР, посвященных проблемам безопасности информационных систем [2]. Впоследствии оно было уточнено на сессии десятого Конгресса ООН по предупреждению преступности и уголовному правосудию в 2000 г., где фактически оно рассматривалось как киберпреступность. Там было определено, что компьютерное преступление касается любого преступного деяния, «которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети, или против компьютерной системы или сети. В принципе, оно охватывает любое преступление, которое может совершаться в электронной среде» [3].

Понятие «информационная преступность» содержится в Соглашении Шанхайской организации сотрудничества и определяется как «использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях» [4].

В целом можно констатировать, что в международных актах понятие «цифровая преступность» практически отсутствует, в основном используется термин «компьютерное преступление», под которым понимается любое деяние, в котором инструментом, целью или местом преступных действий являются компьютеры, компьютерные сети, а также цифровые технологии.

В отечественных исследованиях говорится о преступлениях, совершаемых с использованием информационно-телекоммуникационных сетей и Интернет, к которым авторы относят группу преступлений в сфере компьютерной информации в узком и широком смысле.

По мнению С.В. Складорова и К.Н. Евдокимова, в узком смысле «компьютерная преступность» – это совокупность преступлений, при совершении которых в качестве непосредственного объекта выступают охраняемые законом общественные отношения в сфере безопасного создания, хранения, обработки и передачи компьютерной информации, а предметом являются компьютерная информация, средства ее хранения, обработки, пере-

дачи и защиты, информационно-телекоммуникационные сети, а в широком смысле – это совокупность преступлений, при совершении которых объектом выступают любые общественные отношения в сфере информационных технологий и безопасного функционирования компьютерной информации. При этом компьютерная информация, средства ее создания, хранения, обработки и передачи, информационно-телекоммуникационные сети не только являются предметом преступного деяния, но и используются в качестве средства и орудия совершения преступления. Таким образом, компьютерная преступность в широком смысле соотносится с понятиями «киберпреступность», «интернет-преступность», «преступность в сфере компьютерной информации», как целое и часть, поглощая их по смыслу и содержанию, выступая для них более общим понятием. Структура компьютерной преступности в Российской Федерации включает не только преступления в сфере компьютерной информации, но и большое количество преступных деяний, совершенных с помощью компьютерных и телекоммуникационных технологий, в том числе посредством информационно-телекоммуникационной сети Интернет. При этом в последнее десятилетие российская компьютерная преступность значительно трансформировалась, приобретая высоколатентный, организованный, «профессиональный», трансграничный, транснациональный, политический и экономически направленный характер [5].

По мнению Т. М. Лопатиной, компьютерная преступность – это совокупность совершенных на определенной территории за определенный период преступлений (лиц, их совершивших), непосредственно посягающих на отношения по сбору, обработке, накоплению, хранению, поиску и распространению компьютерной информации, а также преступлений с использованием компьютера в целях извлечения материальной выгоды или иной личной заинтересованности [6].

По мнению Баева М. О. и Скрыль С.В., существует необходимость разграничения (в уголовно-правовом смысле) преступлений в сфере компьютерной информации от иных информационных преступлений, совершаемых с использованием компьютерных средств и новых информационных технологий (разглашение сведений, содержащих служебную тайну в результате доступа к базе данных) [7].

Р. И. Дремлюга считает: «не каждое преступление в сфере компьютерной информации представляет собой интернет-преступление, в то же время такие традиционные преступления, как мошенничество, кража, вымогательство и др., совершенные посредством сети Интернет, – это интернет-преступления. Причем их последствия не обязательно должны наступать в сети Интернет» [8].

Д. В. Добровольский считает: «компьютерная преступность – это совокупность всех преступлений в сфере «информационных технологий», а не только общественно опасных деяний, предметом которых является компьютерная информация» [9].

По мнению Л. М. Старковой, термин «киберпреступность» представляется наиболее обоснованным, поскольку приставка «кибер» содержит указание на связь с наукой кибернетики в ее значении, предложенном и обоснованном в теории Норберта Винера [10].

А.Н. Косенков и Г. А. Черный,, используя синонимичный термин – «киберпреступление», рекомендуют проводить дифференциацию всех киберпреступлений на специальные, ответственность за которые предусмотрена составами главы 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной информации» (далее – глава 28 УК РФ), и общие, ответственность за которые предусмотрена другими нормами Уголовного кодекса РФ [11].

Также следует отметить, что 15 декабря 2022 года Верховный Суд Российской Федерации опубликовал Постановление Пленума № 37 «О некоторых вопросах судебной практи-

ки по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» [12], в тот же день пресс-центр при Верховном суде кратко осветил разъяснение Пленума ВС РФ, что будет являться местом совершения при киберпреступлениях [13], где в своем заголовке обзора материалов СМИ, длинное название уголовные дела о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» заменил на тождественное короткое – «киберпреступления».

Заключение

Вместе с развитием цифровых технологий меняется и преступность. Особенность преступлений, совершаемых в цифровом пространстве, заключается в том, что большая их часть или отдельные этапы подготовительной деятельности совершаются в виртуальной среде, а с постоянным развитием цифровых технологий трансформируется и сама преступность. Если ранее содержание терминов «компьютерная преступность», «преступность с использованием информационно-телекоммуникационных сетей (включая сеть Интернет)» или «информационная преступность» соответствовали реалиям развития технологий и практики борьбы с ними, то сегодня требуется рассматривать данный термин шире – «цифровая преступность». Рост технических возможностей обусловил возможность неправомерных действий посредством цифровых технологий не только в сфере информации, но и в иных сферах человеческой жизнедеятельности.

Таким образом, цифровая преступность – это социальное противоправное явление, включающее в себя совокупность преступлений, совершаемых в сфере цифровых технологий или с их использованием, в том числе включая незаконное завладение и предложение или распространение информации в информационно-телекоммуникационных сетях и в виртуальной среде, дополняющей реальность.

Полагая, такое понимание позволяет рассмотреть более широкий круг составов противоправных деяний, совершаемых в цифровом пространстве. В том числе использование при совершении преступлений виртуальной валюты (криптовалюты). Значимость такого подхода состоит еще и в оптимизации процесса классификации цифровых преступлений, позволит группировать изучаемые объекты в зависимости от потребностей теории и практики, обеспечивая тем самым решение многообразных теоретических и прикладных задач.

Литература

1. Овчинский В.С. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия // [Электронный ресурс]. Москва, 2017. URL: <http://cybersafetyunit.com>
2. Обзор: Директива ОЭСР по проблеме безопасности информационных систем и сетей: формирование культуры обеспечения безопасности // [Электронный ресурс]. URL: <https://www.oecd.org/sti/iesonopmy/15582276.pdf>
3. Справочный документ для семинара-практикума по преступлениям, связанным с использованием компьютерной сети // [Электронный ресурс]. URL: file:///C:/Users/Ekaterina/Downloads/A_CONF.187_10-RU.pdf. С. 4
4. Соглашение между Правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (заключено в г. Екатеринбурге 16.06.2009). Доступ из справочно-правовой системы «Консультант-Плюс».
5. Складаров, С. В. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации / С. В. Складаров, К. Н. Евдокимов. – Текст: непосредственный // Всероссийский криминологический журнал. – 2016. – № . – С. 322-330. // [Электрон-

ный ресурс] //URL: <https://cyberleninka.ru/article/n/sovremennye-podhody-k-opredeleniyu-ponyatiya-struktury-i-suschnosti-kompyuternoy-prestupnosti-v-rossiyskoy-federatsii>

6. Лопатина, Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: специальность 12.00.08. «уголовное право и криминология»: диссертация на соискание ученой степени кандидата юридических наук / Лопатина Татьяна Михайловна ; Всероссийский научно-исследовательский институт МВД России. – Москва, 2006. – 418 с. – Текст: непосредственный.

7. Баев, М. О. Проблема квалификации преступлений в отношении информации компьютерных систем / М. О. Баев, С. В. Скрыль. – Текст: непосредственный // Вестник Воронежского института МВД России. – 2007. – № 1. – С. 30-32.

8. Дремлюга, Р. И. Интернет-преступность: монография / Р. И. Дремлюга. – 1. – Владивосток : Министерство образования и науки Российской Федерации Федеральное агентство по образованию Дальневосточный государственный университет, 2008. – 240 с. – Текст : непосредственный.

9. Добровольский, Д. В. Актуальные проблемы борьбы с компьютерной преступностью: специальность 12.00.08 «уголовное право и криминология; уголовно-исполнительное право»: диссертация на соискание ученой степени кандидата юридических наук / Добровольский Д.В.; Современная гуманитарная академия. – Москва, 2005. – 225 с. – Текст: непосредственный.

10. Старкова, Л. М. Подходы к пониманию и нормативному определению категории “киберпреступность” и смежных понятий в практике региональных международных организаций / Л. М. Старкова. – Текст : непосредственный // Московский журнал международного права. – 2021. – № 4. – С. 123-135.

11. Косенков, А. Н. Общая характеристика психологии киберпреступника / А. Н. Косенков, Г. А. Черный. – Текст: непосредственный // Всероссийский криминологический журнал. – 2012. – № 3. – С. 87-94. // [Электронный ресурс] // – URL: <https://cyberleninka.ru/article/n/obschaya-harakteristika-psihologii-kiberprestupnika>

12. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”: Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. N 37. – Текст: электронный // vsrf.ru: [сайт]. – URL: <https://www.vsrfr.ru/documents/own/?keyword=2022>

13. Верховный суд России определил, что считать местом преступления при киберпреступлениях. – Текст: электронный // vsrf.ru: [сайт]. –URL: https://vsrf.ru/press_center/mass_media/31901/#:~:text=...

References

1. Ovchinsky V.S. Fundamentals of Combating Cybercrime and Cyberterrorism: Anthology // [Electronic resource]. Moscow, 2017. URL: <http://cybersafetyunit.com>

2. Overview: OECD Directive on the Security of Information Systems and Networks: Building a Culture of Security // [Electronic resource]. URL: <https://www.oecd.org/sti/ieconomy/15582276.pdf>

3. Reference document for a workshop on crimes related to the use of computer networks // [Electronic resource]. URL: file: // C:/Users/Ekaterina/Downloads/A_CONF.187_10-RU.pdf. P. 4

4. Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in Ensuring International Information Security (concluded in Yekaterinburg on 16 June 2009). Access from the legal reference system ConsultantPlus.

5. Sklyarov, S. V. Modern Approaches to Defining the Concept, Structure, and Essence of Computer Crime in the Russian Federation / S. V. Sklyarov, K. N. Evdokimov. – Text: direct // All-Russian Journal of Criminology. – 2016. – No. 2. – Pp. 322-330. // [Electronic resource] // URL: <https://cyberleninka.ru/article/n/sovremennye-podkhody-k-opredeleniyu-ponyatiya-struktury-i-suschnosti-kompyuternoy-prestupnosti-v-rossiyskoy-federatsii>

6. Lopatina, T. M. Criminological and Criminal Law Foundations of Countering Computer Crime: Speciality 12.00.08. “Criminal Law and Criminology”: Dissertation for the Degree of Candidate of Legal Sciences / Lopatina Tatyana Mikhailovna; All-Russian Research Institute of the Ministry of Internal Affairs of Russia. – Moscow, 2006. – 418 p.

7. Baev, M. O. The problem of qualification of crimes in relation to information of computer systems / M. O. Baev, S. V. Skryl. – Text: direct // Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. – 2007. – No. 1. – P. 30-32.

8. Dremlyuga, R. I. Internet Crime: A Monograph / R. I. Dremlyuga. – 1. – Vladivostok: Ministry of Education and Science of the Russian Federation, Federal Agency for Education, Far Eastern State University, 2008. – 240 p.
9. Dobrovolsky, D. V. Actual Problems of Combating Computer Crime: Speciality 12.00.08 “Criminal Law and Criminology; Criminal Executive Law”: Dissertation for the Degree of Candidate of Legal Sciences / Dobrovolsky D.V.; Modern Humanitarian Academy. – Moscow, 2005. – 225 p.
10. Starkova, L. M. Approaches to understanding and normative definition of the category “cybercrime” and related concepts in the practice of regional international organizations / L. M. Starkova. – Text : direct // Moscow Journal of International Law. – 2021. – No. 4. – Pp. 123-135.
11. Kosenkov, A. N. General Characteristics of the Psychology of a Cybercriminal / A. N. Kosenkov, G. A. Cherny. – Text: direct // All-Russian Journal of Criminology. – 2012. – No. 3. – Pp. 87-94. // [Electronic resource] // – URL: <<https://cyberleninka.ru/article/n/obschaya-harakteristika-psihologii-kiberprestupnika>>
12. On Certain Issues of Judicial Practice in Criminal Cases on Computer Information Crimes, as Well as Other Crimes Committed Using Electronic or Information and Telecommunication Networks, Including the Internet: Resolution of the Plenum of the Supreme Court of the Russian Federation No. 37 dated December 15, 2022. – Text: electronic // vsrf.ru: [website]. – URL: <https://www.vsrfr.ru/documents/own/?keyword=2022>
13. The Supreme Court of Russia has determined what constitutes a place of crime in cybercrimes. – Text: electronic // vsrf.ru: [website]. – URL: https://vsrf.ru/press_center/mass_media/31901/#:~:text=...

Сведения об авторе

ПАВЛОВА Арзулана Акрамовна – кандидат юридических наук, доцент, заведующий кафедрой «Уголовное право и процесс» юридического факультета, Северо-Восточный федеральный университет имени М.К. Аммосова, г. Якутск, Российская Федерация, e-mail: arzulana@bk.ru

About the authors

PAVLOVA Arzulana Akramovna – Candidate of Judicial Sciences, Associate Professor, Head of the Department of Criminal Law and Process of the Faculty of Law, M.K. Ammosov North-Eastern Federal University, Yakutsk, Russian Federation, e-mail: arzulana@bk.ru

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Conflict of interests

The author declares no relevant conflict of interests.

Поступила в редакцию / Submitted 26.07.2025

Принята к публикации / Accepted 28.08.2025