

DOI: 10.18287/2542-047X-2023-9-3-106-115



**НАУЧНАЯ СТАТЬЯ**

УДК 343.2/.7

Дата поступления: 26.04.2023  
рецензирования: 27.05.2023  
принятия: 25.07.2023

**«Цифровые преступления»: понятие, типология, признаки**

**А. С. Перина**

Санкт-Петербургский юридический институт (филиал) Университета прокуратуры  
Российской Федерации, г. Санкт-Петербург, Российская Федерация  
E-mail: [anzhela.perina@yandex.ru](mailto:anzhela.perina@yandex.ru)

**Аннотация:** Статья посвящена анализу теоретических положений о понятии преступлений, совершаемых с использованием компьютерных, цифровых и иных технологий. В рамках исследования автором проанализированы научные изыскания ученых в части выработки единого обобщающего термина, обозначающего указанный вид преступлений, рассмотрена их типология, а также положения международных документов и законодательства Российской Федерации в указанном вопросе. Автором акцентировано внимание на отсутствие законодательного определения и единого мнения в доктрине уголовного права относительно дефиниции, отражающей сущность использования компьютерных технологий при совершении преступлений, и наличии различных определений, данных и в международных актах, несмотря на назревшую необходимость в нем в условиях стремительного увеличения включенности технологий в механизм совершения преступлений. Автор приходит к выводу о важности введения в научный оборот термина, обозначающего использование современных технологий в преступных целях, предлагая термин «цифровые преступления» и обозначая его преимущества. Статья содержит также признаки указанной группы преступлений. Обозначена авторская типология цифровых преступлений.

**Ключевые слова:** цифровые преступления; виды преступлений; компьютерные преступления; уголовное право; типология преступлений; современные технологии.

**Цитирование.** Перина А. С. «Цифровые преступления»: понятие, типология, признаки // Юридический вестник Самарского университета. 2023. Т. 9, № 3. С. 106–115. DOI: <https://doi.org/10.18287/2542-047X-2023-9-3-106-115>.

**Информация о конфликте интересов:** автор заявляет об отсутствии конфликта интересов.

© Перина А. С., 2023

Анжела Сергеевна Перина – аспирант кафедры уголовного права, криминологии и уголовно-исполнительного права, Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 191104, Российская Федерация, г. Санкт-Петербург, Литейный пр., 44.

**SCIENTIFIC ARTICLE**

Submitted: 26.04.2023  
Revised: 27.05.2023  
Accepted: 25.07.2023

**Digital crimes: concept, typology, signs**

**A. S. Perina**

Saint Petersburg Law Institute (branch) of the University of Prosecutor's Office  
of the Russian Federation, Saint Petersburg, Russian Federation  
E-mail: [anzhela.perina@yandex.ru](mailto:anzhela.perina@yandex.ru)

**Abstract:** The article is devoted to the analysis of theoretical provisions on the concept of crimes committed using computer, digital and other technologies. The study is an analysis of scientific approaches of scientists, the provisions of international documents, legislation of the Russian Federation to the terms that denote the criminal use of digital technologies in the commission of crimes. In addition, the article contains approaches to the typology of the group of crimes under consideration. The author focuses on the lack of a single concept that reflects the essence of crimes committed using modern technologies in the analyzed legal acts and the theory of criminal law. The article as a result of the research contains an indication of the need to create and apply the generalizing concept of there is, since modern technologies are rapidly being incorporated into the mechanism of committing crimes. The author suggests the term «digital crimes» and designates its advantages. The article also contains signs of the specified group of crimes and the author's typology of digital crimes.

**Key words:** digital crime; types of crimes; computer crimes; criminal law; typology of crimes; modern technology.

**Citation.** Perina A. S. «*Tsifrovyye prestupleniya*»: *ponyatie, tipologiya, priznaki* [Digital crimes: concept, typology, signs]. *Iuridicheskii vestnik Samarskogo universiteta* [Juridical Journal of Samara University], 2023, vol. 9, no. 3, pp. 106–115. DOI: <https://doi.org/10.18287/2542-047X-2023-9-3-106-115> [in Russian].

**Information about the conflict of interests:** author declares no conflict of interests.

© Perina A. S., 2023

Angela S. Perina – postgraduate student of the Department of Criminal Law, Criminology and Penal Enforcement Law, Saint Petersburg Law Institute (branch) of the University of Prosecutor's Office of the Russian Federation, 44, Liteyny Avenue, Saint Petersburg, 191104, Russian Federation.

Научно-технический прогресс, бесспорно, положительно влияет на общественное развитие, улучшая качество жизни человека, упрощая важнейшие сферы его деятельности.

Однако технологии, которые появляются в результате его стремительного развития, становятся инструментом для причинения вреда общественным отношениям. При этом появление новых угроз не является единственным его негативным следствием. Не менее опасным становится использование современных технологий при совершении «традиционных» для уголовного закона преступлений, уголовная ответственность за которые уже в нем закреплена. Наряду с общественно опасными деяниями, посягающими на общественный порядок, отношения собственности, причинение вреда посредством использования новейших технологий возможно и личности, ее правам и свободам, которые особо охраняются государством.

Согласно данным отчета Digital 2023<sup>1</sup>, подготовленного организациями We Are Social и Hootsuite, на начало 2023 года 64,4 % населения планеты (т. е. 5,16 млрд из 8,01 млрд человек или минимум 6 из 10 человек) используют сеть Интернет, указанный показатель по сравнению с предыдущим годом увеличился на 1,9 %. При этом 4,76 млрд человек пользуются социальными сетями, что составляет около 60 % от общей численности населения. Статистические сведения, представленные в указанном отчете, показывают, что люди проводят в социальных сетях все больше времени, чем когда-либо.

На основе активного внедрения компьютерных преступлений в повседневную жизнь общества в настоящее время формируется современная модель социального взаимодействия, которая характеризуется анонимностью и дистанционностью общения. При этом личное общение все больше становится второстепенным [1, с. 74]. Появляются новые возможности ввиду расширения многообразия программно-аппаратных средств, электронных и информационно-телекоммуникационных сетей и т. д. Увеличивается доступность технологий для общества, что способствует активному распространению их использования, в том числе злоумышленниками.

Исследователи, неравнодушные к обозначенной проблеме, занимаются поиском обобщающего понятия, которое бы отражало суть феномена использования информационных, цифровых, компьютерных и иных современных технологий в преступных целях, их тесное вплетение в процесс совершения общественно опасного деяния. Такой научный интерес обусловлен необходимостью найти разумный ответ возникающим угрозам в условиях отсутствия конкретной и безальтернативной законодательной и доктринальной дефиниции. При том, что уголовное право

является той отраслью, которая требует ясности терминологии ввиду особенностей содержания его норм, способных оказывать существенное влияние на общественные отношения в обществе, а также важности эффективности правовой нормы в целях выполнения обозначенных задач в уголовном законе. Теоретическое осмысление фундаментальных проблем, новых угроз существующим или возникающим общественным отношениям необходимо и в рамках своевременной адаптации норм уголовного закона к современным реалиям, в том числе происходящей посредством совершенствования юридической техники и введения в правовой оборот новых понятий и терминов [2, с. 69].

Международные документы также содержат в себе обозначения указанного явления. В частности, используются понятия:

«киберпреступление»<sup>2</sup>, как любое противоправное деяние, совершенное посредством электронных операций, целью которого является безопасность компьютерных систем и обрабатываемых ими данных (киберпреступление в узком смысле (компьютерное преступление)), и как любое противоправное деяние, совершенное посредством или связанное с компьютерами, компьютерными системами или сетями, включая незаконное владение и предложение или распространение информации посредством компьютерных систем или сетей (киберпреступление в широком смысле (как преступление, связанное с компьютерами));

«компьютерное преступление», определяемое как любое преступное деяние, «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»<sup>3</sup>;

«преступления, связанные с использованием компьютеров» как запрещаемое законом и/или судебной практикой поведение, которое а) направлено собственно на компьютерную сферу и коммуникационные технологии; б) включает использование цифровых технологий в процессе совершения правонарушения; в) включает использование компьютера как инструмента в процессе совершения иных преступлений, и, соответствен-

<sup>1</sup> SIMON KEMP. DIGITAL 2023: GLOBAL OVERVIEW REPORT. 26.01.2023. URL: <https://datareportal.com/reports/digital-2023-global-overview-report> (дата обращения: 16.04.2023).

<sup>2</sup> Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями. Вена, 10–17 апреля 2000 года. URL: [https://www.unodc.org/documents/congress/Previous\\_Congresses/10th\\_Congress\\_2000/030\\_ACONF.187.15\\_Report\\_of\\_the\\_Tenth\\_United\\_Nations\\_Congress\\_on\\_the\\_Prevention\\_of\\_Crime\\_and\\_the\\_Treatment\\_of\\_Offenders\\_R.pdf](https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/030_ACONF.187.15_Report_of_the_Tenth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders_R.pdf) (дата обращения: 01.04.2023).

<sup>3</sup> Справочный документ для семинара-практикума по преступлениям, связанным с использованием компьютерной сети. 2000. URL: [https://www.unodc.org/documents/congress/Previous\\_Congresses/10th\\_Congress\\_2000/017\\_ACONF.187.10\\_Crimes\\_Related\\_to\\_Computer\\_Networks\\_R.pdf](https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks_R.pdf) (дата обращения: 01.04.2023).

но, компьютер выступает при этом как источник электронных процессуальных доказательств<sup>4</sup>.

«информационное преступление», которое раскрывается как «использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях»<sup>5</sup>;

«преступление в сфере компьютерной информации», которое представляет собой «уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация»<sup>6</sup>;

«деяния в сфере информационных технологий», которое также предполагает совершение именно компьютерных преступлений, за исключением некоторых пунктов.<sup>7</sup>

Несмотря на то, что в более поздних документах Конгресса Организации Объединенных Наций понятия «киберпреступность», «компьютер» стараются обходить, что обусловлено стремительно расширяющимися возможностями информационных и цифровых технологий, которые уже выходят за рамки привязанности к электронным предметам,<sup>8</sup> в настоящее время положения остаются не в полной мере адаптированы к современным реалиям и не отражают результатов стремительного научно-технического прогресса в контексте их использования при совершении преступлений.

На национальном уровне законодательное понятие, раскрывающее сущность преступления, при совершении которого используются компьютерные и иные технологии, также отсутствует.

Тенденции наполнения норм Уголовного кодекса Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 18.03.2023) (далее – УК РФ) признаками, характеризующими преступление в ключе использования при их совершении различных современных технологий, нуждаются в необходимости

<sup>4</sup> Доклад XI Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. Бангкок, 18–25 апреля 2005 г. URL: [https://www.unodc.org/documents/congress/Documentation/11Congress/ACONF203\\_18\\_r\\_V0584411.pdf](https://www.unodc.org/documents/congress/Documentation/11Congress/ACONF203_18_r_V0584411.pdf) (дата обращения: 01.07.2021)

<sup>5</sup> 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 справ.-правовой системы «КонсультантПлюс».

<sup>6</sup> Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации. 2001. Доступ из справ.-правовой системы «КонсультантПлюс».

<sup>7</sup> Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий. 2018. URL: <http://publication.pravo.gov.ru/Document/View/0001202207180005> (дата обращения: 05.04.2023).

<sup>8</sup> Руководство для дискуссий, подготовлено в рамках Четырнадцатого Конгресса ООН по предупреждению преступности и уголовному правосудию. Киото. Япония, 20–27 апреля 2020 года. URL: [https://www.unodc.org/documents/congress/Documentation\\_14th\\_Congress/DiscussionGuide/A\\_CONF234\\_PM1\\_r\\_V1806331.pdf](https://www.unodc.org/documents/congress/Documentation_14th_Congress/DiscussionGuide/A_CONF234_PM1_r_V1806331.pdf). С. 50–56.

наиболее четкого понимания содержательной составляющей термина, отражающего этот признак.

В составах преступлений, входящих в раздел VII УК РФ, содержащий нормы об ответственности за посягательства на личность, включение технологий в элементы объективной стороны состава, обозначено как использование «информационно-телекоммуникационной сети, включая сеть Интернет».

Пунктами 17, 18 Постановления Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «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» (далее – Постановление Пленума ВС РФ от 15.12.2022 № 37) разъяснение содержания указанного признака состоит в дублировании нормы п. 4 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 29.12.2022) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.03.2023).

Однако такой подход не только не способствует уяснению указанного термина, но и ограничивает многообразие технологий, которые могут быть использованы злоумышленниками при совершении преступлений, поскольку современный этап научно-технического прогресса характеризуется, в частности, разработками, тестированием и внедрением в жизнедеятельность общества беспилотных автомобилей и летательных аппаратов, искусственного интеллекта. Их использование в преступных целях напрямую способствует расширению возможностей совершения общественно опасных деяний, в том числе направленных против личности.

В доктрине уголовного права также нет единого мнения относительно понятия, включающего использование компьютерных и иных современных технологий в преступных целях, однако исследователи, неравнодушные к обозначенной проблеме, занимаются его поиском.

Так, использование компьютерных и иных современных технологий при совершении преступлений исследователи отражают в понятиях, которые условно можно разделить на 2 группы:

1) отражающие в самом понятии технологии или их свойства, которые применяются при совершении преступлений: «компьютерные преступления» [3, с. 9; 4, с. 24–25], «информационные преступления» [5; 6, с. 612–614; 7], «киберпреступления» [8; 9], «интернет-преступления» [10; 11], «преступления, совершаемые с использованием информационно-телекоммуникационных технологий (ИТТ)» [12–14];

2) отражающие сферу совершения таких преступлений: «преступления в сфере высоких технологий» [15–17], «преступление в сфере компьютерной информации» [18–21], «преступление в сфере информационных технологий» [22], «пре-

ступления в сфере обращения цифровой информации» [23; 24].

В зарубежной литературе распространение получили два понятия: *cyber crime* и *computer-related crime* [25; 26].

Некоторые авторы в попытках объединить указанные термины пишут о рассмотрении компьютерной преступности в широком смысле, которая включала бы в себя и такие понятия, как «киберпреступность», «интернет-преступность», «преступность в сфере компьютерной информации», поглощая их по смыслу и содержанию, выступая для них более общим понятием [27].

Указанные термины отражают различные аспекты включенности технологий в механизм совершения преступления, что означает наличие многогранности рассматриваемого явления и отсутствие прямого противостояния исследователей друг другу в части конкретных терминов.

Некоторые ученые (Ю. М. Батулин, А. М. Жодзишский [28, с. 11], В. М. Быков, В. Н. Черкасов [29, с. 102]) высказывают сомнения о существовании компьютерных преступлений как специального вида, отмечая, что «правильнее было бы говорить лишь о компьютерных аспектах преступлений, не выделяя их в обособленную группу преступлений». Несмотря на приводимую ими аргументацию, которая включает в том числе позицию о нецелесообразности дифференциации преступлений в зависимости от вида технических средств, применяемых при их совершении, а также модификации традиционных преступлений ввиду вовлеченности в них компьютерных технологий, такой подход не совсем удачен. Недооценка факта существования фактора «включенности» в сущность некоторых общественно опасных деяний компьютерных и иных технологий, отсутствие анализа их юридической специфики может привести к торможению адаптации уголовного закона к постепенной «цифровизации» преступности.

Действительно, излишняя детализированность нового для уголовного права понятия, которое вопреки своему призванию устранить неопределенность нецелесообразно и способно вызвать обратный эффект: не позволит учесть все нюансы реальности и необоснованно создаст ограниченную и тупиковую ситуацию для правоприменителя, сузив пределы уголовно-правовой охраны.

Важность формулирования признаков криминализованных деяний с очевидностью заключается в наиболее точном применении уголовного закона. Кроме того, неконкретность понятий и отсутствие единого подхода к терминологии, применяемой при осуществлении количественного учета и классификации новых способов совершения преступлений в сфере информационных технологий, усложняет определение реальной степени их угроз.

Наличие понятийного аппарата определяет констатацию научной разработанности и актуальности исследований в той или иной сфере. Уголовное право не является исключением. Эволюция преступности в контексте перехода ее в виртуальное

пространство предполагает не только ее научное переосмысление, но и разработку конкретного перечня понятий, характеризующих новый вид преступлений.

Представляется, что все новые и развивающиеся технологии, которые могут нести угрозу общественным отношениям, охраняемым уголовным законом, следует рассматривать как элементы одного явления. Предлагается использовать для его обозначения понятие «*цифровые преступления*». Такой термин может быть применен к любым преступлениям, объединенным в ту или иную группу, входящую в конкретный раздел УК РФ, в том числе и к группе преступлений против личности. Так, *цифровые преступления – это виновные, общественно опасные деяния, запрещенные уголовным законом под угрозой наказания, совершаемые посредством компьютерных, цифровых, информационно-телекоммуникационных и иных современных технологий либо в киберпространстве*.

Стоит отметить, что в соответствии с современным толковым словарем слово «посредством» определяется как «при помощи чего-либо, используя что-либо»<sup>9</sup>. Так, указанное обозначение аналогично употреблению слов «с использованием», «с помощью» применительно к компьютерным и цифровым технологиям в составе объективной стороны.

Введение в научный оборот термина «цифровое преступление» имеет следующие преимущества: 1) позволяет выразить объективно существующую связь с цифровыми технологиями, не ограничиваясь понятиями «компьютер», «сеть Интернет», «смартфоны» и пр.; 2) этимология использованных слов позволяет создать общее представление о группе преступлений, четко отразить суть посягательства, несколько видоизмененного под влиянием цифровизации, выстроить обусловленную технологиями логическую ассоциацию у использующих это понятие; 3) находится в русле тенденций процессов цифровизации и порождаемых ей понятий (связь с законодательной базой, использование в обиходе слов «цифровая» личность, «цифровизация» и пр.).

Кроме того, дополнительным преимуществом может стать и тот факт, что в смежной с уголовным правом науке криминологии группой ученых предложен термин «цифровая преступность» как 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 [30]. Так, подчеркивается единообразие наук криминального цикла в подходах к феномену использования современных технологий при совершении преступлений.

<sup>9</sup> Толковый словарь Ефремовой. Москва, 2000.

Поскольку цифровые преступления могут также развиваться и наполняться все новыми возможностями технологий, представляется целесообразным их типологизировать, что позволит осмыслить явление в его целостности, выявить внутренние взаимосвязи и соподчинения, прогнозировать наличие недостающих звеньев, а также сформулировать критерии отнесения тех или иных преступлений к «цифровым» [31, с. 54].

В научной литературе попытки классифицировать преступность уже имеются. Например, вопрос о типологизации преступлений, совершаемых с использованием компьютерных технологий, в доктрине уголовного права рассмотрен профессором А. Н. Поповым, который отмечает, что компьютерные преступления могут быть представлены: как преступления в сфере компьютерной информации; информационные компьютерные преступления; киберпреступления (интернет-преступления), раскрывая сущность каждого из указанных видов [32].

Еще один ученый, который также предложил классификацию рассматриваемого вида преступлений, это профессор А. Г. Волеводз. Им выделено три категории преступлений: «преступления в сфере компьютерной информации, посягающие на информационные компьютерные отношения; преступления в информационном компьютерном пространстве, посягающие на отношения, возникающие по поводу реализации прав на информационные ресурсы (собственности и т. д.), информационную инфраструктуру и составляющие ее части (ЭВМ, системы и сети ЭВМ, программы для ЭВМ и т. д.); иные преступления, для которых характерно использование компьютерной информации или составляющих ее элементов информационного пространства при совершении деяний, посягающих на иные охраняемые уголовным законом правоотношения (собственности, общественной безопасности и т. д.)» [33].

Е. А. Русскевич сформулировал два уголовно-правовых феномена: «компьютерная преступность» - общественно опасные посягательства на установленный порядок хранения, обработки или передачи компьютерной информации либо эксплуатации информационно-коммуникационных сетей и оконечного оборудования; и «компьютеризированная преступность», которую ученый подразделяет по признакам объекта и по признакам объективной стороны (на простые и квалифицированные) [14, с. 29–31]. Интересным с точки зрения прогностического видения автора представляется, что остальные преступления он называет «потенциально компьютеризированными», то есть те, которые на современном этапе развития общества являются нетипичными для уголовного права, но возможны при дальнейшем развитии общества.

Представляется, что каждая из указанных классификаций дополняет друг друга и раскрывает феномен использования компьютерных технологий при совершении преступлений со своей стороны.

Однако следует отметить, что любая классификация, как и предлагаемая в рамках исследования, имеет условный характер и требует оговорок.

На международном уровне также в рамках объединения усилий стран по противодействию цифровым преступлениям принимаются международные документы, в том числе отражающие типологии таких преступлений.

Например, приложение к постановлению Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств от 27.11.2020 № 51-24 «Рекомендательные типологии новых преступлений, совершаемых с использованием информационных технологий» в рамках положений раздела 5 «Использование информационных технологий с целью совершения преступлений против половой неприкосновенности несовершеннолетних, а также преступлений против здоровья населения и общественной нравственности» содержит указание на два вида преступлений: преступления против половой неприкосновенности несовершеннолетних и склонение несовершеннолетних к совершению самоубийства.

Представляется, что указанная классификация по объекту посягательства не отражает в полной мере всего спектра возможностей технологий для совершения преступлений.

В Конвенции Совета Европы, принятой еще в начале XXI века, выделяется четыре группы правонарушений: 1) преступления против конфиденциальности, целостности и доступности компьютерных данных и систем, 2) правонарушения, связанные с использованием компьютерных средств, 3) правонарушения, связанные с содержанием данных, 4) правонарушения, связанные с нарушением авторского права и смежных прав.

Однако даже на международном уровне попытки классифицировать цифровые преступления сводятся к отражению специфики использования современных технологий при совершении той или иной узкой группы преступлений, не отражая общие признаки сущности современных технологий в составе преступления.

В рамках настоящего исследования всю совокупность преступлений, при совершении которых используются современные технологии, можно разделить на несколько условных групп *по признаку их включенности в состав преступления*.

1. Цифровые, компьютерные и иные современные технологии, используемые в качестве способа или средства совершения преступления. Своего рода **«соисполнительство» человека и технологий**.

В рамках данного вида использование компьютерных технологий является обязательным признаком именно объективной стороны, самого общественно опасного деяния, которое совершается в сопряженности с технологиями. Зачастую такое использование становится непосредственным или одним из необходимых условий достижения преступного результата, хотя может быть и не единственным, но преимущественно обуславливающим его наступление. В рамках указанно-

го типа рассматриваются преступления, совершенные с помощью искусственного интеллекта, беспилотных автомобилей, различных приборов, технических устройств, систем видеонаблюдения, продуктов цифровизации, информационно-телекоммуникационных сетей и т. п.

При этом следует сделать оговорку, что в рамках указанной группы цифровых преступлений подразумевается применение не физических свойств техники, а именно «интеллектуальное» наполнение технологий и их возможности воздействия на внешний мир.

Юридическая конструкция норм подобных преступлений предполагает наличие слов «с использованием», «с применением», «посредством» и т. п.

2. Компьютерные технологии как место совершения преступления. Здесь логичнее говорить о **преступлениях, совершенных в киберпространстве или виртуальном пространстве.**

Включенность в объективную сторону состава в рамках указанной группы цифровых преступлений обусловило признание особого пространства, в котором совершаются общественно опасные деяния. Спецификой таких преступлений является то, что и выполнение деяния, и наступление преступного результата, которое заключается в себе оконченный состав, совершается в киберпространстве, которое «не имеет территориальных границ, кроме стандартов или технических средств, которые регулируют системы доступа и которые не принадлежат правовому миру» [34].

Например, создание фейковой страницы в сети Интернет для распространения порочащих сведений о потерпевшем. Причинение вреда происходит реальному человеку, однако сам процесс выполняется как бы «внутри» цифровых технологий и только с их использованием. В данном случае компьютерные технологии по своей сути уже не вспомогательный элемент в выполнении общественно опасного деяния и не орудие, а место совершения преступления.

Кроме того, данный тип преступлений предполагает также обеспечение признака «публичности», содержащегося в конструкциях некоторых составов (ст. 137 УК РФ, ст. 128.1 УК РФ и др.), поскольку виртуальное пространство предполагает возможность обращения к той или иной информации неограниченного числа пользователей, доступность в любое время и в любой точке мира, а также возможность неконтролируемого распространения информации.

В настоящее время правовое регулирование данной сферы недостаточно разработано, что обуславливает наличие проблем территориальной юрисдикции.

Юридическая конструкция составов, входящих в обозначенную группу преступлений, содержит признак использования цифровых технологий, по смыслу отвечающий на вопрос «где?» совершено преступление, отражая по своей сути пространственное виртуальное место совершения преступления.

3. Компьютерные технологии как объект преступления. В данном случае, когда злоумышленник стремится неправомерно завладеть доступом к тем или иным данным в компьютере или ином устройстве и получает его в процессе выполнения определенных манипуляций с программами и системами компьютерных и цифровых устройств.

Такой тип преступлений можно обозначить как **«собственно компьютерные преступления».**

В данном случае технологии относятся к предмету совершения преступления, а объектом являются общественные отношения, обеспечивающие их безопасность.

Таким образом, указанная классификация позволяет разграничить в науке уголовного права составы преступлений в зависимости от того, каким образом используются достижения научно-технического прогресса для достижения преступного результата, что имеет значение как для квалификации преступлений, так и для совершенствования юридической техники при конструировании составов уголовного закона, разграничения смежных составов между собой и т. д.

Исходя из предлагаемого понятия для исследуемой группы преступлений, их типологии, можно кратко обозначить признаки, которые характеризуют цифровые преступления и позволяют отнести к ним совершаемые общественно опасные деяния.

1. Процесс посягательства на общественные отношения предполагает использование компьютерных, цифровых, информационно-телекоммуникационных и иных современных технологий, их включенность в элементы состава преступления.

2. В процессе выполнения общественно опасного деяния задействовано «интеллектуальное» наполнение технологий, т. е. те возможности, которые они в себе содержат, а не их физические свойства. Например, для причинения смерти используется система искусственного интеллекта, в которой происходит перепрограммирование на отключение систем жизнеобеспечения пациента, поддерживаемое с помощью технологий, а не провада от этих систем для удущья.

3. Такое использование носит преимущественно обуславливающий характер для наступления преступного результата. Оно может быть и не единственным элементом выполнения объективной стороны состава, однако находится в прямой причинно-следственной связи между общественно опасным деянием и наступившими последствиями.

4. Субъектом преступления умышленно используются современные технологии для причинения вреда. Лицо осознает наличие тех или иных свойств у применяемых программно-аппаратных и иных средств, способных обеспечить достижение преступного результата. Более того, виновный обладает необходимыми знаниями пользователя таких систем, позволяющими ему управлять ими и обеспечивать направление для достижения необходимой ему цели.

Таким образом, термин «цифровые преступления», введенный в научный оборот, может спо-

способствовать обогащению науки уголовного права обобщенным обозначением феномена внедрения технологий в механизм совершения преступлений, в частности, направленных против личности. Применение признаков и типологии поможет в объединении преступлений в соответствующую группу и позволит следить за их динамикой, осуществлять прогнозирование преступности и принимать своевременные меры со стороны государства для минимизации причинения вреда общественным отношениям посредством использования технологий.

### Библиографический список

1. Русскевич Е. А. Уголовное право и информатизация // Журнал российского права. 2017. № 8 (248). С. 73–80. DOI: [https://doi.org/10.12737/article\\_597714e7c1b439.52593067](https://doi.org/10.12737/article_597714e7c1b439.52593067). EDN: <https://www.elibrary.ru/zbthcf>.
2. Козаев Н. Ш. Противодействие злоупотреблениям современными технологиями: международно-правовые и уголовно-правовые аспекты. Москва: Юрлитинформ, 2016. 192 с. URL: <https://www.elibrary.ru/item.asp?id=24268901>. EDN: <https://www.elibrary.ru/ulbzkr>.
3. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 8–15. URL: <https://www.elibrary.ru/item.asp?id=29973805>. EDN: <https://www.elibrary.ru/zfxvmm>.
4. Вехов В. Б. Компьютерные преступления: Способы совершения, методики расследования. Москва: Право и закон, 1996. 179 с.
5. Крылов В. В. Информационные компьютерные преступления: учеб. и практ. пособие. Москва: ИНФРА-М: Норма, 1997. 276 с. URL: [https://studylib.ru/doc/2575914/krylov-v.v.-informacionnyie-komp.\\_yuternye-prestupleniya](https://studylib.ru/doc/2575914/krylov-v.v.-informacionnyie-komp._yuternye-prestupleniya).
6. Копылов В. А. Информационное право: вопросы теории и практики. Москва: Юристъ, 2003. 621 с.
7. Гребеньков А. А. Понятие информационных преступлений, место в уголовном законодательстве России и место признаков информации в структуре их состава // Lex Russica (Русский закон). 2018. № 4 (137). С. 108–120. DOI: <https://doi.org/10.17803/1729-5920.2018.137.4.108-120>. EDN: <https://www.elibrary.ru/xmjncx>.
8. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. ... канд. юрид. наук. Владивосток, 2005. 26 с. URL: [https://new-disser.ru/\\_avtoreferats/01002772809.pdf](https://new-disser.ru/_avtoreferats/01002772809.pdf).
9. Чекунов И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: автореф. дис. ... канд. юрид. наук. Москва, 2013. 22 с. URL: <https://www.elibrary.ru/item.asp?id=30392051>. EDN: <https://www.elibrary.ru/zpbuoj>.
10. Гузеева О. С. Преступления, совершаемые в российском сегменте сети Интернет: монография. Москва, 2015. 136 с.
11. Дремлюга Р. И. Интернет-преступность: монография. Владивосток: Изд-во Дальневосточного ун-та, 2008. 238 с. URL: <https://www.elibrary.ru/item.asp?id=19785835>. EDN: <https://www.elibrary.ru/qqzwhn>.
12. Урбан В. В. Преступления, совершаемые с использованием информационно-телекоммуникационных сетей: общая характеристика и уголовно-процессуальные меры по их противодействию // Вестник Восточно-Сибирского института МВД России. 2019. № 1 (88). С. 55–63. DOI: <https://doi.org/10.24411/2312-3184-2019-10005>. EDN: <https://www.elibrary.ru/zatqmx>.
13. Унукович А. С. Понятие преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Государственная служба и кадры. 2021. № 4. С. 278–280. DOI: <https://doi.org/10.24411/2312-0444-2021-4-278-280>. EDN: <https://elibrary.ru/giktyg>.
14. Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. Москва: ИНФРА-М, 2022. 352 с. DOI: <https://doi.org/10.12737/1840963>. EDN: <https://elibrary.ru/mpwvhl>.
15. Козаев Н. Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): монография. Москва: Юрлитинформ, 2015. 217 с. URL: <https://elibrary.ru/item.asp?id=23393321>. EDN: <https://elibrary.ru/trxvbd>.
16. Фоменко А. И. К вопросу об уголовно-правовой охране сферы высоких технологий как необходимого условия стабильного регионального развития // Интеллектуальные ресурсы – региональному развитию. 2015. № 5. С. 217–222. URL: <https://elibrary.ru/item.asp?id=25516464>. EDN: <https://elibrary.ru/vmjumj>.
17. Аносов А. В. Использование технологии блокчейн в процессе формирования и учета криминологической информации // Вестник Казанского юридического института МВД России. 2018. № 2 (32). С. 211–216. DOI: <https://doi.org/10.24420/KUI.2018.32.13968>. EDN: <https://elibrary.ru/urzwim>.
18. Старичков М. В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристика: автореф. дис. ... канд. юрид. наук. Иркутск, 2006. 26 с. URL: <https://telecomlaw.ru/autoref/abstracts/starichkov-120008.htm>.
19. Шибаев Д. В., Лобачев И. В. Содержание понятия «преступление в сфере компьютерной информации» // Российский журнал правовых исследований. 2018. Т. 5, № 4. С. 131–140. DOI: <https://doi.org/10.17816/RJLS18454>.
20. Петрова И. А., Лобачев И. А. Преступления в сфере компьютерной (цифровой) информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств // Журнал прикладных исследований. 2020. № 1. С. 52–62. URL: <https://elibrary.ru/item.asp?id=42850761>. EDN: <https://elibrary.ru/iibnyb>.

21. Кудрявцев В. Л. Преступления в сфере компьютерной информации: общая характеристика // Уголовное законодательство в XXI веке: современное состояние, проблемы трактовки и применения его положений с учетом задач дальнейшего укрепления экономического правопорядка: материалы междунаучно-практической конференции (Нижний Новгород, 1 марта 2012 года) / под ред. А. В. Козлова. Н. Новгород: НИУ ВШЭ, 2012. С. 69–76. URL: <https://www.iauj.net/node/1174>.
22. Мысина А. И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. 2019. № 1. С. 18–27. DOI: <https://doi.org/10.25136/2306-9899.2019.1.29027>. EDN: <https://www.elibrary.ru/geuluc>.
23. Феткулин Р. Р., Арюков А. К. Преступления в сфере цифровой информации: понятие и виды // Baikal Research Journal. 2019. Т. 10, № 3. DOI: [http://doi.org/10.17150/2411-6262.2019.10\(3\).17](http://doi.org/10.17150/2411-6262.2019.10(3).17).
24. Бегисhev И. Р., Бикеев И. И. Преступления в сфере обращения цифровой информации. Казань: Познание, 2020. 300 с. URL: <https://clib.me/b/643072-eldar-rustamovich-begishev-prestupleniya-v-sfere-obrascheniya-tsifrovoy-informatsii/readp>.
25. Dana L. Bazelon, Yun Jung Choi, Jason F. Conaty. Computer Crimes // The American criminal law review. 2006. Vol. 43, issue 2. P. 259–310.
26. Douglas H. Hancock. To What Extent Should Computer Related Crimes be the Subject of Specific Legislative Attention? // Albany Law Journal Science & Technology. 2001, vol. 12, p. 97.
27. Скляр С. В., Евдокимов К. Н. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации // Всероссийский криминологический журнал. 2016. Т. 10, № 2. С. 322–330. DOI: [https://doi.org/10.17150/1996-7756.2016.10\(2\).322-330](https://doi.org/10.17150/1996-7756.2016.10(2).322-330). EDN: <https://www.elibrary.ru/wkesvj>.
28. Батулин Ю. М., Жодзишский А. М. Компьютерная преступность и компьютерная безопасность. Москва: Юрид. лит., 1991. 157 с. URL: <https://www.elibrary.ru/item.asp?id=20854436>. EDN: <https://www.elibrary.ru/rojhoх>.
29. Быков В. М., Черкасов В. Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография. Москва: Юрлитинформ, 2015. 325 с. URL: <https://www.elibrary.ru/item.asp?id=23743587>. EDN: <https://www.elibrary.ru/tzpcmv>.
30. Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С. Цифровая криминология: учебное пособие. Москва, 2021. 244 с. URL: <https://www.elibrary.ru/item.asp?id=46390788>. EDN: <https://www.elibrary.ru/vckoef>.
31. Кудрявцев В. Н., Лунеев В. В. О криминологической классификации преступлений // Государство и право. 2005. № 6. С. 54–66. URL: <https://www.elibrary.ru/item.asp?id=9151612>. EDN: <https://www.elibrary.ru/hsgwwt>.
32. Попов А. Н. Преступления в сфере компьютерной информации: учебное пособие. Санкт-Петербург, 2018. 68 с. URL: [https://www.procuror.spb.ru/izdaniya/2018\\_01\\_07.pdf](https://www.procuror.spb.ru/izdaniya/2018_01_07.pdf).
33. Волеводз А. Г. Правонарушения в информационной сфере: некоторые проблемы ответственности // Информационное общество в России: проблемы становления: сборник научных трудов. Москва, 2002. С. 26–35. URL: <https://www.elibrary.ru/item.asp?id=24749083>. EDN: <https://www.elibrary.ru/uvpesb>.
34. Ramón J. M. Territorio, tiempo y estructura del ciberespacio. 2014. P. 25–26.

## References

1. Russkevich E. A. *Ugolovnoe pravo i informatizatsiya* [Criminal law and informatization]. *Zhurnal rossiiskogo prava* [Journal of Russian Law], 2017, no. 8 (248), pp. 73–80. DOI: [https://doi.org/10.12737/article\\_597714e7c1b439.52593067](https://doi.org/10.12737/article_597714e7c1b439.52593067). EDN: <https://www.elibrary.ru/zbthcf> [in Russian].
2. Kozaev N. Sh. *Protivodeistvie zloupotrebleniyam sovremennymi tekhnologiyami: mezhdunarodno-pravovye i ugolovno-pravovye aspekty* [Counteracting the abuse of modern technologies: international legal and criminal aspects]. Moscow: Yurlitinform, 2016, 192 p. Available at: <https://www.elibrary.ru/item.asp?id=24268901>. EDN: <https://www.elibrary.ru/ulbzkr> [in Russian].
3. Lyapunov Yu., Maksimov V. *Otvetstvennost' za komp'yuternye prestupleniya* [Responsibility for computer crimes]. *Zakonnost'* [Zakonnost Journal], 1997, no. 1, pp. 8–15. Available at: <https://www.elibrary.ru/item.asp?id=29973805>. EDN: <https://www.elibrary.ru/zfxvmn> [in Russian].
4. Vekhov V. B. *Komp'yuternye prestupleniya: Sposoby soversheniya, metodiki rassledovaniya* [Computer crimes: Methods of commission, methods of investigation]. Moscow: Pravo i zakon, 1996, 179 p. [in Russian].
5. Krylov V. V. *Informatsionnye komp'yuternye prestupleniya: ucheb. i prakt. posobie* [Information computer crimes: training and practical guide]. Moscow: INFRA-M: Norma, 1997, 276 p. Available at: [https://studylib.ru/doc/2575914/krylov-v.v.-informatsionnye-komp\\_yuternye-prestupleniya](https://studylib.ru/doc/2575914/krylov-v.v.-informatsionnye-komp_yuternye-prestupleniya) [in Russian].
6. Kopylov V. A. *Informatsionnoe pravo: voprosy teorii i praktiki* [Information law: issues of theory and practice]. Moscow: Yurist', 2003, 621 p. [in Russian].
7. Grebenkov A. A. *Ponyatie informatsionnykh prestuplenii, mesto v ugolovnom zakonodatel'stve Rossii i mesto priznakov informatsii v strukture ikh sostava* [The concept of computer crimes, place in the criminal legislation of Russia and the place of information features in the structure of the elements]. *Lex Russica (Russkii zakon)* [Lex Russica], 2018, no. 4 (137), pp. 108–120. DOI: <https://doi.org/10.17803/1729-5920.2018.137.4.108-120>. EDN: <https://www.elibrary.ru/xmjncx> [in Russian].

8. Tropina T. L. *Kiberprestupnost': ponyatie, sostoyanie, ugovolno-pravovye mery bor'by: avtoref. dis. ... kand. yurid. nauk* [Cybercrime: concept, state, criminal law measures of struggle: author's abstract of Candidate's of Legal Sciences thesis]. Vladivostok, 2005, 26 p. Available at: [https://new-disser.ru/\\_avtoreferats/01002772809.pdf](https://new-disser.ru/_avtoreferats/01002772809.pdf) [in Russian].
9. Chekunov I. G. *Kriminologicheskoe i ugovolno-pravovoe obespechenie preduprezhdeniya kiberprestupnosti: avtoref. dis. ... kand. yurid. nauk* [Criminological and criminal law support for the prevention of cybercrime: author's abstract of Candidate's of Legal Sciences thesis]. Moscow, 2013, 22 p. Available at: <https://www.elibrary.ru/item.asp?id=30392051>. EDN: <https://www.elibrary.ru/zpbuoj> [in Russian].
10. Guzeeva O. S. *Prestupleniya, sovershaemye v rossiiskom segmente seti Internet: monografiya* [Crimes committed in the Russian segment of the Internet: monograph]. Moscow, 2015, 136 p. [in Russian].
11. Dremlyuga R. I. *Internet-prestupnost': monografiya* [Internet crime: monograph]. Vladivostok: Izd-vo Dal'nevostochnogo un-ta, 2008, 238 p. Available at: <https://www.elibrary.ru/item.asp?id=19785835>. EDN: <https://www.elibrary.ru/qqzhwn> [in Russian].
12. Urban V. V. *Prestupleniya, sovershaemye s ispol'zovaniem informatsionno-telekommunikatsionnykh setei: obshchaya kharakteristika i ugovolno-protsessual'nye mery po ikh protivodeistviyu* [Crimes committed with the use of information and telecommunication networks: general characteristics and criminal procedural measures to counter them]. *Vestnik Vostochno-Sibirskogo instituta MVD Rossii* [Vestnik Eastern Siberia Institute of the Ministry of the Interior of the Russian Federation], 2019, no. 1 (88), pp. 55–63. DOI: <https://doi.org/10.24411/2312-3184-2019-10005>. EDN: <https://www.elibrary.ru/zatqmx> [in Russian].
13. Unukovich A. S. *Ponyatie prestuplenii, sovershaemykh s ispol'zovaniem informatsionno-telekommunikatsionnykh tekhnologii* [The concept of crimes committed with the use of information and telecommunication technologies]. *Gosudarstvennaya sluzhba i kadry* [State service and personnel], 2021, no. 4, pp. 278–280. DOI: <https://doi.org/10.24411/2312-0444-2021-4-278-280>. EDN: <https://elibrary.ru/giktgy> [in Russian].
14. Russkevich E. A. *Ugovolnoe pravo i «tsifrovaya prestupnost'»: problemy i resheniya: monografiya* [Criminal law and «digital crime»: problems and solutions: monograph]. Moscow: INFRA-M, 2022, 352 p. DOI: <https://doi.org/10.12737/1840963>. EDN: <https://elibrary.ru/mpwwhl> [in Russian].
15. Kozaev N. Sh. *Sovremennye tekhnologii i problemy ugovolnogo prava (analiz zarubezhnogo i rossiiskogo zakonodatel'stva): monografiya* [Modern technologies and the problems of criminal law (analysis of foreign and Russian legislation): monograph]. Moscow: Yurlitinform, 2015, 217 p. Available at: <https://elibrary.ru/item.asp?id=23393321>. EDN: <https://elibrary.ru/trxvbd> [in Russian].
16. Fomenko A. I. *K voprosu ob ugovolno-pravovoi okhrane sfery vysokikh tekhnologii kak neobkhodimogo usloviya stabil'nogo regional'nogo razvitiya* [To the question of criminal-legal protection of the sphere of high technologies, as necessary preconditions for stable regional development]. *Intellektual'nye resursy – regional'nomu razvitiyu*, 2015, no. 5, pp. 217–222. Available at: <https://elibrary.ru/item.asp?id=25516464>. EDN: <https://elibrary.ru/vmjumj> [in Russian].
17. Anosov A. V. *Ispol'zovanie tekhnologii blokchein v protsesse formirovaniya i ucheta kriminologicheskoi informatsii* [The use of blockchain technology in the process of forming and accounting criminological information]. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii* [Bulletin of the Kazan Law Institute of MIA of Russia], 2018, no. 2 (32), pp. 211–216. DOI: <https://doi.org/10.24420/KUI.2018.32.13968>. EDN: <https://elibrary.ru/urzwim> [in Russian].
18. Starichkov M. V. *Umyslennyye prestupleniya v sfere komp'yuterno informatsii: ugovolno-pravovaya i kriminologicheskaya kharakteristika: avtoref. dis. ... kand. yurid. nauk* [Intentional crimes in the field of computer information: criminal legal and criminological characteristics: author's abstract of Candidate's of Legal Sciences thesis]. Irkutsk, 2006, 26 p. Available at: <https://telecomlaw.ru/autoref/abstracts/starichkov-120008.htm> [in Russian].
19. Shibaev D. V., Lobachev I. V. *Soderzhanie ponyatiya «prestuplenie v sfere komp'yuterno informatsii»* [the Concept of «Crime in the Field of Computer Information»]. *Rossiiskii zhurnal pravovykh issledovaniy* [Russian Journal of Legal Studies], 2018, vol. 5, no. 4, pp. 131–140. DOI: <https://doi.org/10.17816/RJLS18454> [in Russian].
20. Petrova I. A., Lobachev I. A. *Prestupleniya v sfere komp'yuterno (tsifrovoy) informatsii: diskussionnye voprosy opredeleniya ponyatiya, ob'ekta ugovolno-pravovoi okhrany i predmeta posyagatel'stv* [Crimes in sphere of computer (digital) information: debatable issues of definition of the concept, object of criminal legal protection and subject of encroachments]. *Zhurnal prikladnykh issledovaniy* [Journal of Applied Research], 2020, no. 1, pp. 52–62. Available at: <https://elibrary.ru/item.asp?id=42850761>. EDN: <https://elibrary.ru/iibnyb> [in Russian].
21. Kudrjavcev V. L. *Prestupleniya v sfere komp'yuterno informatsii: obshchaya kharakteristika* [Crimes in the field of computer information: general characteristics]. In: *Ugovolnoe zakonodatel'stvo v XXI veke: sovremennoe sostoyanie, problemy traktovki i primeneniya ego polozhenii s uchedom zadach dal'neishego ukrepleniya ekonomicheskogo pravoporyadka: materialy mezhd. nauchno-praktich. konferentsii (Nizhny Novgorod, 1 marta 2012 goda) / pod red. A. V. Kozlova* [Kozlov A. V. (Ed.) Criminal legislation in the XXI century: current state, problems of interpretation and application of its provisions, taking into account the tasks of further strengthening the economic law and order: materials of the International research and practical conference (Nizhny Novgorod, March 1, 2012)]. Nizhny Novgorod: NIU VShE, 2012, pp. 69–76. Available at: <https://www.uaj.net/node/1174> [in Russian].
22. Mysina A. I. *Mezhdunarodno-pravovye osnovy sotrudnichestva gosudarstv po protivodeistviyu prestupleniyam v sfere informatsionnykh tekhnologii* [International Legal Framework for Cooperation between States in Combating Crimes in the Field of Information Technology]. *Mezhdunarodnoe pravo* [International Law], 2019, no. 1, pp. 18–27. DOI: <https://doi.org/10.25136/2306-9899.2019.1.29027>. EDN: <https://www.elibrary.ru/geuluc> [in Russian].

23. Fetkulin R. R., Aryukov A. K. *Prestupleniya v sfere tsifrovoy informatsii: ponyatie i vidy* [Crimes in the Sphere of Digital Information: Concept and Types]. *Baikal Research Journal*, 2019, vol. 10, no. 3. DOI: [http://doi.org/10.17150/2411-6262.2019.10\(3\).17](http://doi.org/10.17150/2411-6262.2019.10(3).17) [in Russian].
24. Begishev I. R., Bikeev I. I. *Prestupleniya v sfere obrashcheniya tsifrovoy informatsii* [Crimes in the sphere of digital information circulation]. Kazan: Poznanie, 2020, 300 p. Available at: <https://clib.me/b/643072-eldar-rustamovich-begishev-prestupleniya-v-sfere-obrascheniya-tsifrovoy-informatsii/readp> [in Russian].
25. Dana L. Bazelon, Yun Jung Choi, Jason F. Conaty. Computer Crimes. *The American criminal law review*, 2006, vol. 43, issue 2, pp. 259–310.
26. Douglas H. Hancock. To What Extent Should Computer Related Crimes be the Subject of Specific Legislative Attention? *Albany Law Journal Science & Technology*. 2001, vol. 12, p. 97.
27. Sklyarov S. V., Evdokimov K. N. *Sovremennye podkhody k opredeleniyu ponyatiya, struktury i sushchnosti komp'yuternoi prestupnosti v Rossiiskoi Federatsii* [Modern approaches to the concept, structure and nature of computer crime in the Russian Federation]. *Vserossiiskii kriminologicheskii zhurnal* [Russian Journal of Criminology], 2016, vol. 10, no. 2, pp. 322–330. DOI: [https://doi.org/10.17150/1996-7756.2016.10\(2\).322-330](https://doi.org/10.17150/1996-7756.2016.10(2).322-330). EDN: <https://www.elibrary.ru/wkesvj> [in Russian].
28. Baturin Yu. M., Zhodzishskiy A. M. *Komp'yuternaya prestupnost' i komp'yuternaya bezopasnost'* [Computer crime and computer security]. Moscow: Yurid. lit., 1991, 157 p. Available at: <https://www.elibrary.ru/item.asp?id=20854436>. EDN: <https://www.elibrary.ru/rojhox> [in Russian].
29. Bykov V. M., Cherkasov V. N. *Prestupleniya v sfere komp'yuternoi informatsii: kriminologicheskie, ugovolno-pravovye i kriminalisticheskie problemy: monografiya* [Crimes in the field of computer information: criminological, criminal law and criminalistic problems: monograph]. Moscow: Yurlitinform, 2015, 325 p. Available at: <https://www.elibrary.ru/item.asp?id=23743587>. EDN: <https://www.elibrary.ru/tzpcmv> [in Russian].
30. Ishchuk Ya. G., Pinkevich T. V., Smolyaninov E. S. *Tsifrovaya kriminologiya: uchebnoe posobie* [Digital criminology: textbook]. Moscow, 2021, 244 p. Available at: <https://www.elibrary.ru/item.asp?id=46390788>. EDN: <https://www.elibrary.ru/vckoef> [in Russian].
31. Kudryavtsev V. N., Lunev V. V. *O kriminologicheskoi klassifikatsii prestuplenii* [On the criminological classification of crimes]. *Gosudartsvo i pravo* [State and Law], 2005, no. 6, pp. 54–66. Available at: <https://www.elibrary.ru/item.asp?id=9151612>. EDN: <https://www.elibrary.ru/hsgwwt> [in Russian].
32. Popov A. N. *Prestupleniya v sfere komp'yuternoi informatsii: uchebnoe posobie* [Crimes in the field of computer information: textbook]. Saint Petersburg, 2018, 68 p. Available at: [https://www.procuror.spb.ru/izdaniya/2018\\_01\\_07.pdf](https://www.procuror.spb.ru/izdaniya/2018_01_07.pdf) [in Russian].
33. Volevodz A. G. *Pravonarusheniya v informatsionnoi sfere: nekotorye problemy otvetstvennosti* [Offenses in the information sphere: some problems of responsibility]. In: *Informatsionnoe obshchestvo v Rossii: problemy stanovleniya: Sbornik nauchnykh trudov* [Information society in Russia: problems of formation: collection of scientific works]. Moscow, 2002, pp. 26–35. Available at: <https://www.elibrary.ru/item.asp?id=24749083>. EDN: <https://www.elibrary.ru/uvpesb> [in Russian].
34. Ramón J. M. Territorio, tiempo y estructura del ciberespacio. 2014, pp. 25–26.