DOI: 10.17803/1729-5920.2023.198.5.049-059

И. Н. Мосечкин*

Понятие преступлений против безопасности цифровой информации

Аннотация. В теории уголовного права существует множество подходов к пониманию понятия и содержания компьютерных преступлений. Часть авторов придерживаются строго нормативного подхода, используя термин «преступления в сфере компьютерной информации» и относя к этой категории деяния, предусмотренные главой 28 УК РФ. Другие авторы оперируют понятиями: «компьютерные преступления», «информационные преступления», «киберпреступления», «преступления в сфере высоких технологий», «интернет-преступления» и др. В работе также представлен анализ зарубежных нормативных актов, демонстрирующий существенную разницу в направлениях регулирования уголовной ответственности за совершение компьютерных преступлений. Отсутствие единого подхода создает препятствия для эффективной научной и законотворческой деятельности.

В статье предпринимается попытка разработать наиболее полное и точное определение, охватывающее преступления, связанные с использованием компьютерных технологий. Автор доказывает, что термин «компьютерный» является несколько устаревшим и требует замены, как ранее использовавшийся в уголовном законе термин «электронно-вычислительная машина». Последние изменения в различных отраслях права характеризуются использованием прилагательного «цифровой», что вполне применимо для уголовного права. Отталкиваясь от концепции «цифровая информация», ранее разработанной учеными-правоведами, автор предлагает формулировку новой дефиниции, охватывающей преступления, связанные с использованием компьютерных технологий. При конструировании дефиниции автор в первую очередь учитывает объект посягательства, а в качестве дополнительных признаков — орудия, средства или способ совершения деяния. По итогам исследования приводится авторское понятие преступлений против безопасности цифровой информации — это общественно опасные деяния, причиняющие вред или ставящие в опасность причинения вреда состоянию защищенности процессов поиска, сбора, хранения, обработки, предоставления, распространения цифровой информации, совершаемые с использованием информационно-телекоммуникационных технологий или нарушением правил их использования.

Ключевые слова: цифровая информация; компьютерная информация; компьютерные преступления; ЭВМ; киберпреступления; цифровые преступления; компьютер; информационно-телекоммуникационная технология; дефиниция; зарубежное законодательство.

Для цитирования: *Мосечкин И. Н.* Понятие преступлений против безопасности цифровой информации // Lex russica. — 2023. — Т. 76. — № 5. — С. 49–59. — DOI: 10.17803/1729-5920.2023.198.5.049-059.

* *Мосечкин Илья Николаевич,* кандидат юридических наук, доцент, доцент кафедры уголовного права, процесса и национальной безопасности Вятского государственного университета (ВятГУ)
Московская ул., д. 36, г. Киров, Россия, 610000
weretowelie@gmail.com

The Concept of Crimes against Digital Data Security

Ilya N. Mosechkin, Cand. Sci. (Law), Associate Professor, Department of Criminal Law, Procedure and National Security, Vyatka State University
ul. Moskovskaya, d. 36, Kirov, Russia, 610000
weretowelie@gmail.com

Abstract. In the theory of criminal law, there are many approaches to understanding the concept and content of computer crimes. Some authors adhere to a strictly normative approach, using the term «crimes in the field of computer information» and referring to this category of acts provided for by Chapter 28 of the Criminal Code of the Russian Federation. Other authors operate with concepts «computer crimes,» «information crimes,» «cybercrimes,» «crimes in the field of high technologies,» «Internet crimes,» etc. The paper also presents an analysis of foreign regulations, demonstrating a significant difference in the directions of regulating criminal liability for computer crimes. The lack of a uniform approach creates obstacles to effective scientific and legislative activity.

The author attempts to develop the most comprehensive and accurate definition covering crimes related to the use of computer technology. The author proves that the term «computer» is outdated and requires replacement, as the term «electronic computing machine» previously used in the criminal law. Recent changes in various branches of law are characterized by the use of the adjective «digital,» which is applicable to criminal law. Starting from the concept of digital information that was earlier developed by legal scholars the author proposes a new definition covering crimes related to the use of computer technology. When forming a definition, the author, first, takes into account the object of encroachment, and as additional features — tools, means or method of committing an act. According to the results of the study, the author gives the concept of crimes against the security of digital information — these are socially dangerous acts that cause harm or put in danger of harming the state of security of the processes of searching, collecting, storing, processing, providing, distributing digital information committed using information and telecommunications technologies or violating the rules of their use.

Keywords: digital information; computer information; computer crimes; computers; cybercrimes; digital crimes; computer; information and telecommunication technology; definition; foreign legislation.

Cite as: Mosechkin IN. Ponyatie prestupleniy protiv bezopasnosti tsifrovoy informatsii [The Concept of Crimes against Digital Data Security]. *Lex russica*. 2023;76(5):49-59. DOI: 10.17803/1729-5920.2023.198.5.049-059. (In Russ., abstract in Eng.).

Изучение научной литературы, а также анализ действующего уголовного законодательства показывает, что в настоящее время нет единого подхода к осмыслению сущности преступлений, связанных с использованием компьютерных технологий, а также к определению их видов.

В Уголовном кодексе Российской Федерации выделена отдельная глава 28, которая называется «Преступления в сфере компьютерной информации». Она охватывает ряд составов, направленных в первую очередь на какое-либо взаимодействие с компьютерной информацией. Количество статей данной главы время от времени пополняется, криминализуются новые общественно опасные деяния, которые, по мнению законодателя, могут создать угрозу безопасности функционирования информационных и телекоммуникационных систем.

В то же время УК РФ запрещает иные деяния, совершаемые с помощью взаимодействия с компьютерными технологиями. Нарушение неприкосновенности частной жизни (ст. 137 УК РФ) часто совершается вследствие неправомерного доступа к информации, содержащейся на смартфонах, ноутбуках или в социальных сетях. Мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ) характеризуется не только использованием платежных карт, но и иных технических устройств. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) и вовсе не может, как следует из названия, совершаться без взаимодействия с компьютерными технологиями.

Таким образом, в УК РФ одни компьютерные преступления сгруппированы в отдельной главе, а другие размещены (в каком-то смысле даже разбросаны) по различным главам. Традиционное упорядочивание уголовного закона по объекту преступления в целом логично и выверено временем, однако оно в некоторой степени создает трудности для теоретического определения сущности преступлений, связан-

ных с использованием компьютерных технологий, и их классификации.

Как верно отмечает Е. А. Русскевич, проблема определения рассматриваемой категории преступлений носит двухуровневый характер. Первый уровень отражает отсутствие общего представления о терминологии компьютерных преступлений. В научной литературе используются различные понятия: компьютерные преступления, информационные преступления, киберпреступления, преступления в сфере высоких технологий, интернет-преступления и многие другие[1].

Второй уровень включает проблему определения того, какие деяния относить к «компьютерным», а какие — нет. При этом сам Е. А. Русскевич выделяет группу преступлений, совершаемых с использованием информационно-коммуникационных технологий, которые, в свою очередь, делятся на компьютерные преступления и компьютеризированные преступления. Компьютерные преступления, по мнению автора, посягают на установленный порядок хранения, обработки или передачи компьютерной информации, а также на порядок эксплуатации информационно-коммуникационных сетей и оконечного оборудования (гл. 28 УК РФ). Компьютеризированные преступления посягают на иные (традиционные) охраняемые законом объекты, однако такие деяния опосредованы информационно-коммуникационной инфраструктурой либо использование информационно-коммуникационных технологий для их совершения является значимо распространенным[2].

Объект посягательства и размещение ряда составов преступлений в гл. 28 УК РФ обусловили появление определения компьютерных преступлений как общественно опасных деяний, посягающих только на безопасность компьютерной информации[3]. Соответственно, остальные деликты, совершаемые с использованием компьютерных технологий, остаются за пределами данной категории. Более того, неправомерный доступ к компьютерной информации может повлечь тяжкие последствия или создать угрозу их наступления (ч. 4 ст. 272 УК РФ), а ведь такие последствия могут иметь место в самых разных сферах жизнедеятельности.

Мы, безусловно, согласны с тем, что плюралистический подход более полно отражает сущность объекта компьютерного преступления по сравнению с монистическим. Соответственно, в качестве объекта могут выступать не только общественные отношения, обеспечивающие безопасность информации, но также охраняющие жизнь и здоровье человека, собственность, иные права и интересы[4].

Изложенное позволяет говорить о том, что категория «компьютерные преступления» является вполне применимой, однако она не может состоять из деяний, исключительно посягающих на безопасность компьютерной информации.

Кроме того, слово «компьютерный» видится нам несколько устаревшим в контексте противодействия преступности. Ранее законодатель отошел от использования в уголовном законе термина «электронно-вычислительная машина» как раз по этим причинам. В действительности к электронно-вычислительным машинам можно отнести компьютеры, смартфоны, умные часы, умные колонки, роботов и массу других вещей, но никто или практически никто не именует их подобным образом. В 2011 г. произошел переход к понятию «компьютерная информация», а соответствующее определение появилось в примечании к ст. 272 УК РФ.

В то же время Гражданский кодекс РФ оперирует такими категориями, как «цифровые права» и «цифровая форма», а не «компьютерные права» и «компьютерная форма». В 2020 г. был принят Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[5], раскрывающий дефиниции «цифровой финансовый актив» и «цифровая валюта». Было бы по меньшей мере странно и

---

1 *Русскевич Е. А.* Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : дис. … д-ра юрид. наук. М., 2020. С. 60.

2 *Русскевич Е. А.* Указ. соч. С. 78.

3 *Гаджиев М. С.* Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан) : дис. … канд. юрид. наук. Махачкала, 2004. С. 9.

4 *Евдокимов К. Н.* Противодействие компьютерной преступности: теория, законодательство, практика : дис. … д-ра юрид. наук. М., 2021. С. 301.

5 СЗ РФ. 2020. № 31 (ч. I). Ст. 5018.

некорректно, если бы они именовались «компьютерный финансовый актив» и «компьютерная валюта». В статье 70 Кодекса административного судопроизводства РФ[6] говорится о том, что письменными доказательствами являются, помимо прочего, документы и материалы, выполненные в форме цифровой и графической записи.

В рамках изложенного целесообразно привести позицию И. Р. Бегишева, в соответствии с которой понятие «цифровая информация» считается общепризнанным. Автор отмечает, что данное понятие является родовым по отношению к понятиям «компьютерная информация» и «электронная информация» и учитывающим принципы работы всех современных информационно-телекоммуникационных систем[7].

Считаем возможным полностью согласиться с мнением И. Р. Бегишева. Словосочетание «цифровая информация» должно прийти на смену устаревшим уголовно-правовым категориям, что поспособствует согласованности с другими отраслями права. В целом оно может быть использовано при совершенствовании уголовного закона.

В зависимости от использования соответствующих технологий и направленности на причинение вреда дополнительному объекту (отношениям в сфере информационной безопасности) Н. В. Летёлкин выделяет категорию «преступления, совершаемые с использованием информационно-телекоммуникационных сетей». По мнению автора, к таким преступлениям относятся деяния, посягающие на общественные отношения в сфере охраны правомерного пользования сетями телекоммуникации. При этом они совершаются посредством технологических систем, предназначенных для хранения и передачи информации, доступ к которым осуществляется с применением средств вычислительной техники (компьютеров)[8].

С одной стороны, весьма логичным представляется подход, в соответствии с которым учитывается способ совершения преступления. Компьютерные деликты как раз и отличаются от прочих тем, что совершаются с использованием определенных технологий. С другой стороны, многие традиционные преступления могут быть реализованы тем же способом. В частности, незаконная игорная деятельность (ст. 171.2 УК РФ) часто осуществляется с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», или средств связи, но вряд ли можно сказать, что она посягает на общественные отношения в сфере охраны правомерного пользования сетями телекоммуникации. К тому же интерактивные ставки организаторами азартных игр в букмекерских конторах и (или) тотализаторах разрешены, поэтому не вполне ясно, почему наличие разрешения исключает указанное посягательство, а его отсутствие — не исключает.

В. Г. Степанов-Егиянц выделяет родовое понятие «компьютерное правонарушение», понимая под ним виновное деяние, осуществляемое с использованием технологий преобразования информации (представленной в виде цифровых данных) и влекущее за собой юридическую ответственность[9].

Необходимо отметить, что при формулировании определения автор явно отталкивался от способа совершения посягательства и общих признаков правонарушений. Указанным родовым понятием охватываются деяния, содержащиеся в КоАП РФ (например, ст. 13.18 «Воспрепятствование уверенному приему радио- и телепрограмм и работе сайтов в сети “Интернет”»), и деяния, содержащиеся в УК РФ[10]. Кроме того, автор рассуждает над тем, что компьютерные правонарушения могут рассматриваться в узком и широком понимании. Узкое понимание охватывает деяния, приводящие к

---

6 Кодекс административного судопроизводства Российской Федерации от 08.03.2015 № 21-ФЗ // СЗ РФ. 2015. № 10. Ст. 1391.

7 *Бегишев И. Р.* Понятие и виды преступлений в сфере обращения цифровой информации : дис. … канд. юрид. наук. Казань, 2017. С. 34.

8 *Летёлкин Н. В.* Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет» : дис. … канд. юрид. наук. Н. Новгород, 2018. С. 5.

9 *Степанов-Егиянц В. Г.* Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект) : дис. … д-ра юрид. наук. М., 2016. С. 58.

10 Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // СЗ РФ. 2002. № 1 (ч. 1). Ст. 1.

нарушению информационных процессов, протекающих в информационно-телекоммуникационных системах, в рамках их технологических функций. Широкое понимание включает посягательства на сознание, психологическое состояние людей.

В науке нередко встречается понятие «преступления в сфере высоких технологий». Под ними понимается совокупность деликтов, совершенных с использованием современных сложных технологий, относящихся к наукоемким отраслям производства или обслуживания[11]. Компьютерные преступления, безусловно, можно отнести к высокотехнологичным. В то же время данная категория охватывает и деяния, имеющие с компьютерными крайне мало общего. Среди них можно назвать преступления в сфере генной инженерии, биоэтики, отдельные экологические правонарушения и др. Соответственно, понятие «преступления в сфере высоких технологий», на наш взгляд, является чрезмерно широким, а потому не подходящим для использования в уголовном законе.

Достаточно часто встречается в литературе понятие «киберпреступление». Его содержание в научных трудах различно. Так, по мнению М. Е. Батухтина, киберпреступлением является любое преступление в электронной сфере, которое совершено при помощи компьютерных средств или виртуальной сети либо против них[12]. С. И. Буз приходит к выводу о том, что к киберпреступлениям относятся любые общественно опасные деяния, если они совершены с помощью информационных технологий либо в информационном пространстве[13].

Данные определения представляют определенный интерес и заслуживают внимания. Считаем необходимым отметить, что для ряда развитых стран (в том числе стран — членов Европейского Союза) характерно именно широкое понимание киберпреступлений. Зачастую к ним относится любое преступление, совершенное в виртуальном пространстве и с использованием информационно-телекоммуникационных технологий (даже убийство).

Но такая позиция не лишена недостатков. Во-первых, чрезмерное расширение перечня любой категории преступления (киберпреступления не являются исключением) затрудняет правоприменение, квалификацию и систему построения уголовного закона. При подобном понимании киберпреступления, и клевета, и вымогательство, и неправомерный доступ к компьютерной информации оказываются в одинаковой категории, что лишает смысла выделение отдельной главы «Преступления в сфере компьютерной информации».

Во-вторых, нам весьма импонирует мнение В. Г. Степанова-Егиянца о том, что абстрактность приставки «кибер», отсутствие ее абсолютного лексического аналога в русском языке излишне усложняет терминологическое поле информационной безопасности. Такая приставка вносит элементы неуместного философского дискурса[14].

И. Р. Бегишев предлагает перейти к категории «преступления в сфере обращения цифровой информации». Автор понимает под данными деликтами предусмотренные уголовным законом виновно совершенные общественно опасные деяния, направленные на нарушение конфиденциальности, целостности, достоверности и доступности охраняемой законом цифровой информации[15].

Можно предположить, что подобный подход основан на сущности объекта и предмета посягательства. Однако автор в категорию преступлений в сфере обращения цифровой информации относит также деяния, предусмотренные статьями 138.1 и 159.6 УК РФ. Можно согласиться с тем, что оборот специальных технических средств, предназначенных для негласного получения информации, направлен как раз на нарушение ее конфиденциальности. Однако мошенничество, в том числе совершенное с

---

[11] *Аносов А. В., Кашапова Е. С.* Понятие преступлений в сфере высоких технологий // Академическая мысль. 2018. № 4 (5). С. 15–19.

[12] *Батухтин М. Е.* Киберпреступления: причины, виды, формы, последствия, направления противодействия // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе : материалы Междунар. науч. конференции адъюнктов, аспирантов, курсантов и студентов. Самара, 2018. Ч. 3. С. 28–31.

[13] *Буз С. И.* Киберпреступления: понятие, сущность и общая характеристика // Юристъ-Правоведъ. 2019. № 4 (91). С. 78–82.

[14] *Степанов-Егиянц В. Г.* Указ. соч. С. 51.

[15] *Бегишев И. Р.* Указ. соч. С. 52.

помощью компьютерных технологий, посягает прежде всего на собственность и осуществляется только ради этого.

И. Г. Чекунов, оперируя понятием «киберпреступление», указывает, что для отнесения какого-либо деяния к такой категории необходимо, чтобы вредоносное программное обеспечение или программно-техническое средство, подключенное к сети или сотовому оператору связи, выступали в качестве орудий или средств преступления[16].

Существует и иная, достаточно радикальная позиция, по поводу существования компьютерных преступлений. Она заключается в том, что данные деликты нецелесообразно выделять в уголовном законе и помещать их в отдельную главу, поскольку они мало чем отличаются от традиционных преступлений и на отдельный объект не посягают. Соответственно, при таком подходе разумным считается распределение составов компьютерных преступлений по главам Уголовного кодекса в зависимости от реального объекта[17].

Отметим, что указанная позиция авторов представляется нам не отвечающей сложившейся действительности и развитию современных информационных технологий. Отдельные компьютерные системы столь важны, что законодатель создал для них специальную категорию — критическая информационная инфраструктура.

Как и в отечественной, в зарубежной литературе не существует единого, четкого, точного и общепризнанного определения преступлений, связанных с использованием компьютерных технологий. Этот факт признается учеными и ведущими научными организациями. Наиболее часто иностранные ученые цитируют два определения. Первое сформулировали D. Thomas (Д. Томас) и B. Loader (Б. Лоадер). По мнению авторов, киберпреступлениями являются совершенные посредством использования компьютера действия, которые являются незаконными или могут быть признаны таковыми, при этом имеют свойство быть осуществленными через глобальные электронные сети[18].

Второе определение сформулировали S. Gordon (С. Гордон) и R. Ford (Р. Форд). В соответствии с ним, к киберпреступлениям относятся любые запрещенные уголовным законом акты, которые были совершены с использованием компьютера, сети или аппаратного устройства[19].

Р. Мур полагает, что следует разграничивать понятия «киберпреступление» и «компьютерное преступление». В частности, по мнению ученого, к киберпреступлению относится любое преступление, если при его совершении использовались компьютер и сеть. «Компьютерное преступление», в свою очередь, включает применение только компьютеров[20].

Другой автор понимает киберпреступление как «трансформацию преступного или иного вредоносного поведения с помощью сетевых технологий»[21]. Следует отметить оригинальность данного определения и в то же время его слабую пригодность для нормативных конструкций в силу неопределенного характера.

Малайзийские исследователи определяют компьютерные преступления как «любые преступные акты, совершаемые в сети “Интернет”» или «незаконное использование информационно-коммуникационных технологий для совершения преступных действий»[22].

В уголовных законах штатов США для описания преступлений, связанных с использова-

---

[16] *Чекунов И. Г.* Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности : дис. … канд. юрид. наук. М., 2013. С. 7.

[17] *Трофимцева С. Ю., Илюшин Д. А., Линьков А. В.* Объект компьютерных преступлений в российском и европейском уголовном праве: сравнительный анализ // Информационное противодействие угрозам терроризма. 2015. № 24. С. 9 ; *Бытко С. Ю.* Некоторые проблемы уголовной ответственности за преступления, совершенные с использованием компьютерных технологий : дис. … канд. юрид. наук. Саратов, 2002. С. 40.

[18] Cybercrime: Law Enforcement, Security and Surveillance in the Information Age / D. Thomas, B. Loader, P. Taylor et al. Routledge, 2000. P. 12.

[19] *Gordon S., Ford R.* On the definition and classification of cybercrime // Journal in computer virology. 2006. Vol. 2, I. 1. P. 13–20.

[20] *Moore R.* Cybercrime: Investigating High-Technology Computer Crime. Routledge, 2014. P. 48.

[21] *Wall D. S.* Cybercrime: The Transformation of Technology in the Networked Age. Cambridge, 2007. P. 61–63.

[22] *Jayabalan P., Ibrahim R., Manaf A. A.* Understanding cybercrime in Malaysia: an overview // Sains Humanika. 2014. Vol. 2, I. 2. P. 109–115.

нием компьютерных технологий, применяются различные юридические конструкции. Имеют место понятия «цифровое преступление» (штат Алабама[23]), «преступления, связанные с компьютером» (штаты Делавер[24], Флорида[25], Нью-Йорк[26]), «киберпреступление» (штат Колорадо[27]), «компьютерное преступление» (штаты Иллинойс[28], Мэн[29]), «незаконные действия в отношении компьютеров и информационных услуг» (штат Невада[30]).

Законы штатов, как правило, содержат большой перечень дефиниций, однако вышеуказанные понятия не раскрываются. Исключением является законодательство штата Невада, содержащее дефиницию «технологическое преступление». Данное понятие охватывает любое преступление, если при его совершении был прямо или косвенно задействован компонент, устройство, система или сеть, которые сами по себе или в сочетании с любым другим таким же элементом способны генерировать, обрабатывать, хранить, извлекать, излучать, передавать, получать, ретранслировать, записывать или воспроизводить любые данные, информацию, изображение, программу, сигнал или звук в технологическом формате, включая аналоговые, цифровые, электронные, электромагнитные, магнитные или оптические технологии.

УК Республики Казахстан содержит главу 7 «Уголовные правонарушения в сфере информатизации и связи», которая включает ряд преступлений, связанных с использованием компьютерных технологий. Многие из них не отличаются от составов, закрепленных в отечественном законе. Однако среди них присутствуют также неправомерные уничтожение или модификация информации (ст. 206 УК РК), неправомерное завладение информацией (ст. 208 УК РК), принуждение к передаче информации (ст. 209 УК РК) и др.[31]

В Уголовном кодексе Республики Беларусь соответствующая глава именуется «Преступления против компьютерной безопасности»[32]. Анализируя объект данных деликтов, В. В. Генюш пришел к выводу о том, что они посягают на состояние защищенности компьютерной информации и компьютерных систем[33].

Законодатель Республики Таджикистан поступил похожим образом. В частности, в Уголовном кодексе[34] находится раздел XII «Преступления против информационной безопасности». При таком наименовании было бы логично разместить в указанном разделе статьи, регламентирующие ответственность за незаконное получение каких-либо защищенных сведений, но этого не сделано.

---

[23] Code of Alabama // URL: https://law.justia.com/codes/alabama/2020/title-13a/ (accessed 25.12.2022).

[24] Delaware Code // URL: https://law.justia.com/codes/delaware/2019/title-11/chapter-5/subchapter-iii/ (accessed 25.12.2022).

[25] Florida Statutes // URL: http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Index&Title_Request=XLVI#TitleXLVI (accessed 24.12.2022).

[26] NY Penal Law // URL: https://ypdcrime.com/penal.law/ (accessed 25.12.2022).

[27] Colorado Revised Statutes // URL: https://law.justia.com/codes/colorado/2020/title-18/article-5-5/section-18-5-5-102/ (accessed 24.12.2022).

[28] Illinois Compiled Statutes // URL: https://law.justia.com/codes/illinois/2021/chapter-720/act-720-ilcs-5/title-iii/ (accessed 23.12.2022).

[29] Maine Revised Statutes // URL: http://www.mainelegislature.org/legis/statutes/17-A/title17-Ach18sec0.html (accessed 24.12.2022).

[30] Nevada Revised Statutes // URL: https://www.leg.state.nv.us/Division/Legal/LawLibrary/NRS/index.html (accessed 23.12.2022).

[31] Уголовный кодекс Республики Казахстан от 03.07.2014 № 226-V // Казахстанская правда. 2014. № 132 (27753).

[32] Уголовный кодекс Республики Беларусь от 09.07.1999 № 275-З // Ведамасці Нацыянальнага сходу Рэспублікі Беларусь. 1999. № 24. Ст. 420.

[33] *Генюш В. В.* Составляющие элементы понятия компьютерной безопасности как объекта уголовно-правовой охраны // Государство и право во времени и пространстве : сборник тезисов докладов Республиканской науч.-практ. конференции с международным участием студентов, магистрантов, аспирантов, 3 декабря 2021 г. Минск, 2022. С. 104–107.

[34] Уголовный кодекс Республики Таджикистан от 21.05.1998 № 574 // Ахбори Маджлиси оли Республики Таджикистан. 1998 г. № 9. Ст. 68–70.

Несмотря на различия в терминологии, можно сказать, что подходы законодателей Республики Беларусь и Республики Таджикистан весьма сходны с отечественными: глава 28 УК РФ размещена именно в разделе «Преступления против общественной безопасности и общественного порядка», а частью общественной безопасности является информационная безопасность.

В Уголовном кодексе Азербайджанской Республики[35] имеется глава 30 «Киберпреступления». Как отмечает Р. Ф. Азизов, такое наименование стало следствием ратификации Конвенции о киберпреступлениях. Однако законодатель не дал объяснения самому значению понятия «киберпреступление», которое, в свою очередь, стало неологизмом не только для юридического, но и для обыденного азербайджанского языка[36].

Указанный подход характерен также для грузинского законодателя. В Уголовном кодексе Грузии[37] содержится глава XXXV «Киберпреступления».

На фоне рассмотренных нормативных актов исключением видится Уголовный кодекс Республики Узбекистан. Глава XX.1 данного нормативного акта охватывает «преступления в сфере информационных технологий». Данная глава, как подчеркивает М. Уразалиев, заменила ранее действовавшую статью 174, что явилось важным шагом законодателя по совершенствованию уголовного закона и установлению ответственности за ряд новейших компьютерных преступлений[38].

В рамках настоящей работы не ставилась цель рассмотреть все понятия и законодательство всех зарубежных стран, изученное количество можно считать достаточным для определения основных направлений в конструировании дефиниции. Исходя из изложенного, можно сделать вывод о том, что среди теоретиков и в нормативных актах различных стран не сложилось единообразного подхода к пониманию преступлений, связанных с использованием компьютерных технологий. Некоторые позиции достаточно похожи между собой, а другие отличаются столь сильно, словно речь идет о принципиально разных деликтах.

Тем не менее очевидным является тот факт, что при разработке подавляющего большинства дефиниций авторы отталкивались от объекта, предмета преступления, орудий, средств или способов, а также места (виртуальное пространство или цифровая среда) совершения деяния. В целом данная особенность должна быть учтена при формулировании авторского определения, однако необходимо понять, целесообразно ли учитывать все указанные признаки одновременно?

Уголовный кодекс Российской Федерации систематизирован в зависимости от объекта преступления. В большинстве случаев это правило систематизации соблюдается, что облегчает квалификацию и отдельные законотворческие процедуры, а также поиск нужной нормы. При формулировании криминологического определения компьютерных преступлений объект может и не учитываться. Однако при формулировании уголовно-правового определения без учета объекта, на наш взгляд, обойтись нельзя.

Орудия, средства или способы совершения компьютерных преступлений уникальны. Такие деяния не могут совершаться без использования определенных технологий или без нарушения правил обращения с ними. В этом кроется их принципиальное отличие от других деликтов. В то же время некоторые преступления, в том числе и достаточно традиционные, также могут совершаться с использованием компьютерных технологий: нарушение неприкосновенности частной жизни (ст. 137 УК РФ) или незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ). Соответственно, само по себе применение компьютерных технологий при совершении преступления не может быть использовано в качестве единственного уникального признака какой-либо категории деликтов, поскольку такая категория рискует стать чрезмерно широкой.

---

[35] Уголовный кодекс Азербайджанской Республики от 30.12.1999 № 787-IQ // Сборник законодательных актов Азербайджанской Республики. 2000. № 4.

[36] *Азизов Р. Ф.* Развитие уголовного законодательства в сфере борьбы с киберпреступлениями в Азербайджанской Республике // Вестник Санкт-Петербургского университета. Право. 2015. № 1. С. 123–129.

[37] Уголовный кодекс Грузии от 22.07.1999 № 2287 // Законодательный вестник Грузии — ЗВГ. 1999. № 41 (48).

[38] *Уразалиев М.* Эволюция развития уголовного законодательства Узбекистана в сфере противодействия компьютерной преступности // Review of law sciences. 2020. Т. 2. № 1. С. 159–163.

Место совершения преступления, на наш взгляд, представляется признаком, который не следует учитывать при формулировании определения. Компьютерные преступления действительно совершаются в виртуальном (цифровом) пространстве, однако в нем также совершаются иные общественно опасные деяния. Клевета (ст. 128.1 УК РФ) или незаконные организация и проведение азартных игр (ст. 171.2 УК РФ), например, могут не выходить за рамки интернет-среды, но это не делает их компьютерными преступлениями. В то же время данные деликты совершаются и вне интернет-среды.

Если же исходить из того, что преступления вроде неправомерного доступа к компьютерной информации отличаются тем, что не могут выходить за пределы цифрового пространства, то как тогда объяснить наличие тяжких последствий (ч. 4 ст. 272 УК РФ), которые могут проявляться в виде банкротства организации, нарушения транспортной инфраструктуры или аварий? Хотя само преступление совершается в цифровом пространстве, общественно опасные последствия могут выходить за его пределы. Наконец, с развитием цифровизации множество рутинных процессов человеческой жизнедеятельности стали носить цифровой характер, поэтому отделение виртуального от реального стало несколько затруднительным, а в ряде случаев — нецелесообразным. В качестве примера можно привести хищение цифрового финансового актива или цифровой валюты.

Таким образом, главным компонентом, от которого следует отталкиваться при разработке дефиниции рассматриваемой категории преступления, является объект. Орудия, средства или способ совершения деяния могут являться дополнительным признаком, позволяющим проводить отграничение от других деликтов. Кроме того, как уже было аргументировано выше, конструкция «компьютерная информация» является неполной, устаревшей и противоречащей положениям иных отраслей права. Последние изменения в законодательстве, регулирующем смежные отношения, сопровождаются употреблением прилагательного «цифровой», что видится нам правильным и заслуживающим одобрения. Полагаем, что именно «цифровая» особенность должна быть учтена при систематизации национального законодательства. Отметим, что само понятие цифровой информации точно и полно раскрыто И. Р. Бегишевым, что делает возможным использование понятия при совершенствовании уголовного закона[39].

На основе проведенного исследования считаем целесообразным предложить понятие «преступления против безопасности цифровой информации», под которым следует понимать общественно опасные деяния, причиняющие вред или ставящие в опасность причинения вреда состоянию защищенности процессов поиска, сбора, хранения, обработки, предоставления, распространения цифровой информации, совершаемые с использованием информационно-телекоммуникационных технологий или нарушением правил их использования.

БИБЛИОГРАФИЯ

1. *Азизов Р. Ф.* Развитие уголовного законодательства в сфере борьбы с киберпреступлениями в Азербайджанской Республике // Вестник Санкт-Петербургского университета. Право. — 2015. — № 1. — С. 123–129.
2. *Аносов А. В.*, *Кашапова Е. С.* Понятие преступлений в сфере высоких технологий // Академическая мысль. — 2018. — № 4 (5). — С. 15–19.
3. *Батухтин М. Е.* Киберпреступления: причины, виды, формы, последствия, направления противодействия // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе : материалы Междунар. науч. конференции адъюнктов, аспирантов, курсантов и студентов. Ч. 3. — Самара, 2018. — С. 28–31.
4. *Бегишев И. Р.* Понятие и виды преступлений в сфере обращения цифровой информации : дис. … канд. юрид. наук. — Казань, 2017. — 204 с.
5. *Бегишев И. Р.* Цифровая информация: понятие и сущность как предмета преступления по российскому уголовному праву // Академический юридический журнал. — 2011. — № 2. — С. 47–55.

[39] *Бегишев И. Р.* Цифровая информация: понятие и сущность как предмета преступления по российскому уголовному праву // Академический юридический журнал. 2011. № 2. С. 47–55.

6. *Буз С. И.* Киберпреступления: понятие, сущность и общая характеристика // Юристъ-Правоведъ. — 2019. — № 4 (91). — С. 78–82.
7. *Бытко С. Ю.* Некоторые проблемы уголовной ответственности за преступления, совершенные с использованием компьютерных технологий : дис. … канд. юрид. наук. — Саратов, 2002. — 204 с.
8. *Гаджиев М. С.* Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан) : дис. … канд. юрид. наук. — Махачкала, 2004. — 168 с.
9. *Генюш В. В.* Составляющие элементы понятия компьютерной безопасности как объекта уголовно-правовой охраны // Государство и право во времени и пространстве : сборник тезисов докладов Республиканской науч.-практ. конференции с междунар. участием студентов, магистрантов, аспирантов, 3 декабря 2021 г. — Минск, 2022. — С. 104–107.
10. *Евдокимов К. Н.* Противодействие компьютерной преступности: теория, законодательство, практика : дис. … д-ра юрид. наук. — М., 2021. — 557 с.
11. *Летёлкин Н. В.* Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет» : дис. … канд. юрид. наук. — Н. Новгород, 2018. — 218 с.
12. *Русскевич Е. А.* Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : дис. … д-ра юрид. наук. — М., 2020. — 499 с.
13. *Степанов-Егиянц В. Г.* Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект) : дис. … д-ра юрид. наук. — М., 2016. — 389 с.
14. *Трофимцева С. Ю.*, *Илюшин Д. А.*, *Линьков А. В.* Объект компьютерных преступлений в российском и европейском уголовном праве: сравнительный анализ // Информационное противодействие угрозам терроризма. — 2015. — № 24. — С. 3–11.
15. *Уразалиев М.* Эволюция развития уголовного законодательства Узбекистана в сфере противодействия компьютерной преступности // Review of law sciences. — 2020. — Т. 2. № 1. — С. 159–163.
16. *Чекунов И. Г.* Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности : дис. … канд. юрид. наук. — М., 2013. — 223 с.
17. Cybercrime: Law Enforcement, Security and Surveillance in the Information Age / D. Thomas, B. Loader, P. Taylor et al. — Routledge, 2000. — 316 p.
18. *Gordon S.*, *Ford R.* On the definition and classification of cybercrime // Journal in computer virology. — 2006. — Vol. 2, I. 1. — P. 13–20.
19. *Jayabalan P.*, *Ibrahim R.*, *Manaf A. A.* Understanding cybercrime in Malaysia: an overview // Sains Humanika. — 2014. — Vol. 2, I. 2. — P. 109–115.
20. *Moore R.* Cybercrime: Investigating High-Technology Computer Crime. — Routledge, 2014. — 312 p.
21. *Wall D. S.* Cybercrime: The Transformation of Technology in the Networked Age. — Cambridge, 2007. — 288 p.

Материал поступил в редакцию 19 января 2023 г.

REFERENCES

1. Azizov RF. Razvitie ugolovnogo zakonodatelstva v sfere borby s kiberprestupleniyami v Azerbaydzhanskoy Respublike [Development of criminal legislation in the field of combating cybercrime in the Republic of Azerbaijan]. *Vestnik of St. Petersburg University. Law.* 2015;1:123-129. (In Russ.).
2. Anosov AV, Kashapova ES. Ponyatie prestupleniy v sfere vysokikh tekhnologiy [The concept of crimes in the field of high technologies]. *Akademicheskaja mysl'*. 2018;4(5):15-19. (In Russ.).
3. Batukhtin ME. Kiberprestupleniya: prichiny, vidy, formy, posledstviya, napravleniya protivodeystviya [Cybercrime: causes, types, forms, consequences, directions of counteraction]. In: Problems and prospects of development of the penal system of Russia at the present stage: Proceedings of the International Conference of Adjuncts, Graduate Students, Cadets and Students. Part 3. Samara; 2018. (In Russ.).
4. Begishev IR. Ponyatie i vidy prestupleniy v sfere obrashcheniya tsifrovoy informatsii: dis. … kand. yurid. nauk [The concept and types of crimes in the sphere of digital information circulation: Cand. Sci. Diss.]. Kazan; 2017. (In Russ.).

5. Begishev IR. Tsifrovaya informatsiya: ponyatie i sushchnost kak predmeta prestupleniya po rossiyskomu ugolovnomu pravu [Digital information: the concept and essence as the subject of a crime under Russian criminal law]. *Academic Legal Journal*. 2011;2:47-55. (In Russ.).
6. Buz SI. Kiberprestupleniya: ponyatie, sushchnost i obshchaya kharakteristika [Cyber Crimes: Concept, Essence and General Characteristic]. *Jurist-Pravoved*. 2019;4(91):78-82. (In Russ.).
7. Bytko SYu. Nekotorye problemy ugolovnoy otvetstvennosti za prestupleniya, sovershennye s ispolzovaniem kompyuternykh tekhnologiy: dis. … kand. yurid. nauk [Some problems of criminal liability for crimes committed using computer technology: Cand. Sci. (Law) Diss.]. Saratov; 2002. (In Russ.).
8. Gadzhiev MS. Kriminologicheskiy analiz prestupnosti v sfere kompyuternoy informatsii (po materialam Respubliki Dagestan): dis. … kand. yurid. nauk [Criminological analysis of crime in the field of computer information (based on the materials of the Republic of Dagestan): Cand. Sci. (Law) Diss.]. Makhachkala; 2004. (In Russ.).
9. Genyush VV. Sostavlyayushchie elementy ponyatiya kompyuternoy bezopasnosti kak obekta ugolovno-pravovoy okhrany [The constituent elements of the concept of computer security as an object of criminal law protection]. In: State and law in time and space: a collection of abstracts of reports of the Republican Scientific and Practical Conference with international participation of Students, Undergraduates, Postgraduates. December 3, 2021. Minsk; 2022. (In Russ.).
10. Evdokimov KN. Protivodeystvie kompyuternoy prestupnosti: teoriya, zakonodatelstvo, praktika: dis. … d-ra yurid. nauk [Countering computer crime: theory, legislation, practice: Dr. Sci. (Law) Diss.]. Moscow; 2021(In Russ.).
11. Letelkin NV. Ugolovno-pravovoe protivodeystvie prestupleniyam, sovershaemym s ispolzovaniem informatsionno-telekommunikatsionnykh setey, vklyuchaya set «Internet»: dis. … kand. yurid. nauk [Criminal legal counteraction to crimes committed using information and telecommunication networks, including the Internet: Cand. Sci. (Law) Diss.]. N.Novgorod; 2018. (In Russ.).
12. Russkevich EA. Differentsiatsiya otvetstvennosti za prestupleniya, sovershaemye s ispolzovaniem informatsionno-kommunikatsionnykh tekhnologiy, i problemy ikh kvalifikatsii: dis. … d-ra yurid. nauk [Differentiation of responsibility for crimes committed using information and communication technologies and problems of their qualification: Dr. Sci. (Law) Diss.]. Moscow; 2020. (In Russ.).
13. Stepanov-Egiyants VG. Metodologicheskoe i zakonodatelnoe obespechenie bezopasnosti kompyuternoy informatsii v Rossiyskoy Federatsii (ugolovno-pravovoy aspekt): dis. … d-ra yurid. nauk [Methodological and legislative provision of computer information security in the Russian Federation (criminal law aspect): Dr. Sci. (Law) Diss.]. Moscow; 2016. (In Russ.).
14. Trofimtseva SYu, Ilyushin DA, Linkov AV. Obekt kompyuternykh prestupleniy v rossiyskom i evropeyskom ugolovnom prave: sravnitelnyy analiz [The object of computer crimes in Russian and European criminal law: comparative analysis]. *Information Counteraction to Threats of Terrorism*. 2015;24:3-11 (In Russ.).
15. Urazaliev M. Evolyutsiya razvitiya ugolovnogo zakonodatelstva Uzbekistana v sfere protivodeystviya kompyuternoy prestupnosti [The evolution of the development of the criminal legislation of Uzbekistan in the field of countering computer crime]. *Review of Law Sciences*. 2020;2(1):159-163. (In Russ.).
16. Chekunov IG. Kriminologicheskoe i ugolovno-pravovoe obespechenie preduprezhdeniya kiberprestupnosti: dis. … kand. yurid. nauk [Criminological and criminal law support for the prevention of cybercrime: Cand. Sci. (Law) Diss.]. Moscow; 2013. (In Russ.).
17. Thomas D, Loader B, Taylor P, et al. Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. Routledge; 2000.
18. Gordon S, Ford R. On the definition and classification of cybercrime. *Journal in computer virology*. 2006;2, I(1):13-20.
19. Jayabalan P, Ibrahim R, Manaf AA. Understanding cybercrime in Malaysia: an overview. *Sains Humanika*. 2014;2, I(2):109-115.
20. Moore R. Cybercrime: Investigating High-Technology Computer Crime. Routledge; 2014.
21. Wall DS. Cybercrime: The Transformation of Technology in the Networked Age. Cambridge; 2007.