УДК 343.985
DOI 10.18413/2712-746X-2020-44-2-315-322

К вопросу о содержательных аспектах киберпреступности

Долженко Н.И., Хмелевская И.Г.
Белгородский государственный национальный исследовательский университет,
Россия, 308015, г. Белгород, ул. Победы, 85
E-mail: dolzhenko@bsu.edu.ru, 1199147@bsu.edu.ru

Аннотация. Рассматрены понятия «киберпреступность» и «киберпреступление», базисной составляющей которых выступает киберпространство как особая сфера деятельности в информационном пространстве. Возникновение данных понятий обусловлено глобальной компьютеризацией общества, которая и определяет непрекращающуюся модернизацию информационных технологий и появление новых видов преступлений, совершаемых с помощью киберпространства. Однако в настоящее время как в рамках международных актов, так и в отечественном законодательстве отсутствуют общепринятые дефиниции указанных понятий наряду с отсутствием единого подхода к определению их содержательного аспекта. Кроме того, не существует единого мнения и относительно перечня киберпреступлений. В связи с чем возникает необходимость в детальной проработке национального законодательства и международных актов, которые предусматривают ответственность за совершение киберпреступлений.

Ключевые слова: киберпреступление, киберпространство, компьютерные преступления, информационные технологии.

Для цитирования: Долженко Н.И., Хмелевская И.Г. 2020. К вопросу о содержательных аспектах киберпреступности. NOMOTHETIKA: Философия. Социология. Право. 45 (2): 315–322. DOI 10.18413/2712-746X-2020-44-2-315-322

To the question of the content aspects of cyber crime

Natalia I. Dolzhenko, Irina G. Khmelevskaya
Belgorod National Research University,
85 Pobeda St, Belgorod, 308015, Russia
E-mail: dolzhenko@bsu.edu.ru, 1199147@bsu.edu.ru

Abstract. In the realities of modern society, it is almost impossible to imagine a full life without information technology. They have penetrated and are widely used in all spheres of human activity; however, in addition to the goals of optimizing various processes, recently information technologies often become a platform for committing crimes. The global computerization of society, mediated by the rapid development of technology, has led to the emergence of concepts such as “cybercrime” and “cybercrime”. The article discusses these concepts, the main component of which is cyberspace as a special area of activity in the information space. Despite the fact that every year the number of committed cybercrimes increases, both in international documents and in the legislation of the Russian Federation, there are still no generally accepted definitions of these concepts along with the lack of a unified approach to determining their substantive aspect. The authors analyze the views of modern scientists on the definition of the concepts of "computer crime", "cybercrime." It is noted that in the Russian legal doctrine the category “computer crime” is mainly used. In addition, there is no consensus on the list of

cybercrimes. In this regard, there is a need for a detailed study of national legislation and international acts, including responsibility for committing cyber crimes.

Keywords: cybercrime, cyberspace, computer crime, information technology.

For citation: Dolzhenko N.I., Khmelevskaya I.G. 2020. To the question of the content aspects of cyber crime. NOMOTHETIKA: Philosophy. Sociology. Law series. 45 (2): 315–322 (in Russian). DOI 10.18413/2712-746X-2020-44-2-315-322

Введение

В реалиях современного общества уже невозможно представить полноценную жизнь без информационных технологий. Они проникли и широко используются во всех сферах деятельности человека. Однако помимо целей оптимизации различных процессов информационные технологии зачастую становятся платформой для совершения преступлений. На данный момент в нашей стране и за рубежом интенсивно осуществляется процесс внедрения информационных технологий путем создания информационных баз с хранением в них конфиденциальных данных. К ним можно отнести информационные базы налогоплательщиков ФНС РФ, базы правоохранительных органов, банковских структур и т.п. Именно такого рода информация чаще всего похищается и используется злоумышленниками для совершения преступлений.

Глобальная компьютеризация общества, опосредованная стремительным развитием технологий, привела к возникновению таких понятий, как «киберпреступность» и «киберпреступление».

Отметим, что статистические данные свидетельствуют о значительном росте количества киберпреступлений в последнее время. Так, за период январь–декабрь 2019 года органами МВД России зарегистрировано более 294 тысяч преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что превышает на 70 % показатель за аналогичный период прошлого года.

Половина таких преступлений совершается с использованием сети «Интернет», а более трети – с помощью средств мобильной связи. Среди наиболее часто встречающихся видов киберпреступлений фигурируют неправомерный доступ к информации, создание и распространение вредоносных утилит.

Определение понятий «киберпреступность» и «киберпреступление»

Несмотря на значительное число совершаемых киберпреступлений, на сегодняшний день ни в международных актах, ни в рамках отечественного законодательства не существует легальных дефиниций «киберпреступности» и «киберпреступления». Более того, в современной доктрине права нет единого подхода к содержательному аспекту данных понятий.

Так, согласно мнению экспертов Организации Объединенных Наций, понятием «киберпреступность» охватывается любое преступление, совершаемое посредством эксплуатации компьютерной системы (сети), в ее рамках либо против нее [Ищенко, 2015, с. 336]. По мнению Е.П. Ищенко [2015, с. 336], под «киберпреступностью понимаются преступления в сфере высоких информационных технологий, совершаемые злоумышленниками, использующими эти технологии в противоправных целях». Другие авторы определяют киберпреступность через понятие «киберпространство» [Вепрев, Нестерович, 2018]. Киберпреступность, с их точки зрения, – это преступность в киберпространстве.

Сам термин «киберпространство» в Российской Федерации на официальном уровне впервые был использован лишь в 2013 году. В Проекте Концепции Стратегии кибербезопасности Российской Федерации под киберпространством понимается «сфера деятельно-

сти в информационном пространстве, образованная совокупностью коммуникационных каналов сети «Интернет» и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)»[1].

Приведенная дефиниция подчеркивает ключевые особенности киберпространства, в наибольшей степени раскрывает его природу, так как, во-первых, отражает отношение киберпространства к информационному пространству как частного к общему, а во-вторых, специально обращает внимание на тот факт, что информационно-телекоммуникационные сети (в том числе и сеть Интернет) являются материальными составляющими киберпространства.

Взяв за основу термин «киберпространство», В.А. Номоконов и Т.Л. Тропина определяют киберпреступность как «совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных» [Номоконов, Тропина, 2012, с. 48].

В свою очередь, М.А. Простосердов [2016] также использует термин «киберпространство», но уже для раскрытия содержания понятия «киберпреступление». Под киберпреступлением он понимает «преступление, причиняющее вред разнородным общественным отношениям, совершаемое дистанционно, путем использования средств компьютерной техники и информационно-телекоммуникационных сетей и образованного ими киберпространства» [Простосердов, 2016, с. 43]. В приведенном определении киберпространство выступает в качестве непосредственного средства совершения преступления.

По нашему мнению, определение сущности понятий «киберпреступность» и, соответственно, «киберпреступление» через понятие «киберпространство» представляется разумным, поскольку его использование позволяет не только наиболее полно раскрыть особенности явлений, которые происходят в различных информационных сетях, но и охватить гораздо больший круг общественных отношений: так, конкретное преступление не будет ограничиваться отдельно взятыми объектом посягательства и информационно-телекоммуникационной сетью, что опосредует возможность отнесения к киберпреступлениям как неправомерного доступа к компьютерной информации, так и, к примеру, мошенничества в сети Интернет.

Однако отметим, что ряд авторитетных ученых придерживается мнения о том, что использование понятия «киберпространство» в отечественной юридической науке пока находится под вопросом [Дремлюга, 2008]. Более того, в целях избежания чрезмерного использования англицизмов в наши дни целесообразно обращаться к иной терминологии [Степанов-Егиянц, 2005]. В настоящее время наряду с термином «киберпреступность» в отечественной юридической науке зачастую используются такие понятия, как «преступления в сфере компьютерной информации» и «преступления, совершаемые с использованием информационных технологий».

В научной литературе можно встретить разные подходы к их пониманию и использованию. Позиция одних ученых заключается в том, что существует разница между этими терминами [Шевко, 2016]. Сторонники второй точки зрения считают, что поскольку данные понятия используются для названия одних и тех же общественно-опасных деяний, то

[1] Проект Концепции стратегии кибербезопасности Российской Федерации. URL: http://council.gov.ru/media/files/ ru (дата обращения: 15.01.2020)

их можно считать равнозначными [Акимов, 2017]. Представляется, что вторую позицию нельзя признать верной.

Во-первых, в соответствии с нормами УК РФ преступления в сфере компьютерной информации, образуют всего четыре состава (ст. 272–274.1)[1]. Это законодательное определение преступлений.

Понятием «преступления, совершаемые с использованием компьютерных технологий», охватываются все преступные деяния, которые посягают на компьютерную информацию и совершаются с использованием компьютерных технологий» [Авдеева, Бобрицкий, 2015]. То есть термин «преступления, совершенные с использованием информационных технологий» является обобщающим как для указанных в Главе 28 УК РФ, так и для всех преступлений, которые в принципе можно совершить с использованием информационных технологий.

Совершенно очевидно, что и термин «киберпреступность» трактуется гораздо шире так как по смыслу включает себя оба понятия.

Кроме того, если обратиться к первоисточнику – иностранной терминологии – можно заметить, что за рубежом понятия «computercrime» и «cybercrime» имеют содержательные различия. Первым термином охватываются только преступления, посягающие на компьютерные данные, в то время как второй включает в себя преступные деяния с использованием как глобальных сетей, информационных технологий, так и компьютеров. [Валько, 2016], что также доказывает более широкое значение понятия «киберпреступность».

Научные труды зарубежных исследователей, среди которых Morrison P. [Morrison, 1991], Colin B. [Colin, 1997], Parker Donn B. [Parker, 1998], Brenner S.W. [Brenner, 2002], Shelley, Louise I. [Shelley, 2003], Williams P. [Williams, 2005], Sieber U. [Sieber, 2007] и др., посвящены анализу киберпреступности, содержат представления об этом явлении. Однако данные исследования практически не имеют отношения к Российскому пространству и не охватывают российское законодательство. Несмотря на это, они дают устойчивые теоретические основы в целях изучения киберпреступности в глобальном направлении.

Вопросы типологии киберпреступлений

Отметим, что сегодня нет единого мнения и относительно перечня киберпреступлений. Так, по информации Управления ООН по наркотикам и преступности обширный диапазон киберпреступлений условно можно разделить на три группы: совершаемые с целью извлечения материальной выгоды; связанные с использованием информации, хранящейся в компьютерах; направленные против целостности, конфиденциальности и доступности компьютерных систем[2].

В свою очередь, Конвенция о киберпреступности, подписанная в г. Будапеште, содержит более детальную градацию, где киберпреступления сосредоточены уже в 5 группах[3]. Стоит заметить, что упомянутая Конвенция стала первым официальным документом, содержащим классификацию киберпреступлений.

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 16.10.2019). СПС КонсультантПлюс. http://www.consultant.ru/document/cons_doc_LAW_10699/

[2] Всестороннее исследование проблемы киберпреступности. Проект, февраль 2013 года. URL: ttps://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf (дата обращения: 18.01.2020).

[3] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.). URL: https://base.garant.ru/4089723/ (дата обращения: 20.01.2020).

Однако Российская Федерация не участвует в Будапештской Конвенции о киберпреступности, находя некоторые ее положения неприемлемыми. В частности, камнем преткновения выступает пункт «b» статьи 32 документа, который предусматривает возможность доступа одного государства к данным, хранящимся на территории другого государства, без его согласия. По мнению российской стороны, приведенная норма может привести к нарушению принципа государственного суверенитета[1].

Кроме того, директор департамента МИД Российской Федерации по вопросам новых вызовов и угроз И.И. Рогачев считает, что Будапештская Конвенция значительно устарела и имеет большое количество недостатков, так как была разработана еще в 1997–2001 годах, когда киберпреступления сами по себе были гораздо проще. Она закрепляет лишь девять видов киберпреступлений, а по заявлению А.В. Крутских – спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, – можно говорить о выделении уже тридцати самостоятельных видов.

Стоит отметить, что в конце декабря 2019 года Генеральная Ассамблея Организации Объединенных Наций приняла предложенную Российской Федерацией резолюцию, дающую начало разработке международной конвенции для борьбы с киберпреступностью. Причем данная инициатива не противопоставляется вышеуказанной Будапештской конвенции, а предполагает ее модернизацию.

Отечественный законодатель избрал собственный подход в типологии киберпреступлений. В настоящее время ответственность именно за преступления в сфере компьютерной информации предусмотрена 28 главой Уголовного кодекса РФ и включает в себя всего лишь 4 состава. При этом следует учесть тот факт, что к киберпреступлениям возможно отнести и другие составы, закрепленные в Уголовном кодексе Российской Федерации, не охваченные указанной главой, к примеру, мошенничество с использованием электронных средств платежа (статья 159.3), мошенничество в сфере компьютерной информации (статья 159.6) и т. д.

Исследователи отмечают, что законодателем не уделяется должного внимания к отдельным составам киберпреступлений:

– кибертерроризм – это использование информационных технологий для осуществления террористической деятельности;

– киберторговля наркотиками – это создание сайтов по продаже наркотических-средств с внедрением наркоторговцами новейших технологий кодирования сообщений;

– кибер-порнография – это создание преступниками сайтов, где пользователи размещают и соответственно распространяют порнографические видеозаписи и фотографии [Сидоренко, 2020].

Для решения этих важнейших проблем необходимо совершенствование правовых механизмов УК РФ. Добиться этого можно путем усовершенствования уже имеющихся статей УК РФ или же с помощью разработки новых статей УК РФ, которые будут дополнять уже имеющиеся. Также следует предпринять дополнительные шаги к изучению уголовно-правовой типологии киберпреступлений.

Заключение

Подводя итоги, отметим, что в реалиях современного общества наиболее оптимальным термином, охватывающим всю совокупность преступлений в сфере информационно-телекоммуникационных сетей, выступает термин «киберпреступность», что опосре-

[1] Распоряжение Президента РФ от 22 марта 2008 г. № 144-рп «О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности». URL: https://base.garant.ru/2565696/#block_1(дата обращения: 22.01.2020).

довано более широкой сферой его применения по сравнению с иными понятиями, употребляющимися в отношении совокупности указанных преступных деяний. Подчеркнем, что, на наш взгляд, базисной составляющей понятия «киберпреступность» выступает киберпространство как особая сфера деятельности в информационном пространстве.

Мы полагаем, что необходимо детально проработать национальное законодательство и международные акты, предусматривающие ответственность за совершение киберпреступлений. Данная необходимость вызвана непрекращающейся модернизацией информационных технологий, опосредующих появление новых видов преступлений, совершаемых с помощью киберпространства.

Список источников

1. ГА ООН приняла резолюцию России по разработке конвенции для борьбы с киберпреступлениями. URL: https://tass.ru/mezhdunarodnaya–panorama/7439717 (дата обращения: 24.01.2020).

2. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.). URL: https://base.garant.ru/4089723 (дата обращения: 20.01.2020).

3. Проект Концепции стратегии кибербезопасности Российской Федерации. URL: http://council.gov.ru/media/files/ ru (дата обращения: 15.01.2020).

4. Распоряжение Президента РФ от 22 марта 2008 г. № 144–рп «О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. № 557–рп «О подписании Конвенции о киберпреступности». URL: https://base.garant.ru (дата обращения: 22.01.2020).

5. Состояние преступности в России за январь–ноябрь 2019 г. URL: https://genproc.gov.ru/ (дата обращения: 03.01.2020).

6. Уголовный кодекс Российской Федерации от 13.06.1996 № 63–ФЗ (ред. от 16.10.2019 г.). СПС Консультант Плюс.

Список литературы

1. Авдеева Г. К., Бобрицкий С.М. 2015. Инновации в борьбе с преступлениями, совершаемыми с использованием информационных технологий. Современная криминалистика: проблемы, тенденции, перспективы: сборник материалов Международной научно–практической конференции. 22.12.2015. Москва: 327–337.

2. Акимов В.В. 2017. Криминалистическая особенность киберпреступлений. Центр исследования компьютерной преступности. М.: 54–55.

3. Валько Д.В. 2016. Киберпреступность в России и мире: сравнительный анализ. Управление в современных системах, 3(10): 29–40.

4. Вепрев С.Б., Нестерович С.А. 2018. Киберпреступность как новая форма преступности. Расследование преступлений: проблемы и пути их решения, 3(21):78–82.

5. Всестороннее исследование проблемы киберпреступности. Февраль 2013 г. Организация Объединенных Наций, Нью-Йорк. URL: https://www.unodc.org/documents /organized–crime/cybercrime/Cybercrime_Study_Russian. (дата обращения: 18.01.2020).

6. Ищенко Е.П. 2015. О криминалистическом обеспечении раскрытия и расследования киберпреступлений. В кн.: Деятельность правоохранительных органов в современных условиях: сборник материалов 20-й международной научно-практической конференции. В 2 томах. Том 1. Иркутск: 336–337.

7. Номоконов В.А. Тропина Т.Л. 2012. Киберпреступность как новая криминальная угроза. Криминология: вчера, сегодня, завтра, 24: 45–55.

8. Простосердов М.А. 2016. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им. Диссертация … кандидата юридических наук. Москва: 232.

9. Тропина Т.Л. 2005. Киберпреступность: понятие, состояние, уголовно–правовые меры борьбы. Диссертация … кандидата юридических наук. Владивосток: 234 с.

10. Шевко Н.Р. 2016. Особенности раскрытия и расследования киберпреступлений: проблемы и пути решения. Юридические науки. М.: 11–14

11. Brenner S.W. 2002. The emerging consensus on criminal conduct in cyberspace. UCLA Journal of Law and Technology. № 3. URL: http://www.lawtechiournal. com/articles/2002/Q3 020625 goodmanbrenner.php (дата обращения: 12.01.2020).

12. Colin B. 1997. The Future of Cyberterrorism. Crime and Justice International. March: 15–18.

13. Morrison P. 1991. Computer Crime. The Improvement of Investigative Skills. Final Report Part One: 89.

14. Sieber U. 2007. Legal Aspects of Computer–Related Crime in the Information Society. URL: http://europa.eu.int/lSPO/legal/en/comcrime/sieber.doc (дата обращения: 01.02.2020).

15. Shelley Louise I. 2003. Organized Crime, Terrorism and Cybercrime. Security Sector Reform: Institutions, Society and Good Governance. Baden–Baden: 303–312.

16. Williams P. 2005. Organized Crime and Cybercrime: Synergies, Trends and Responses. URL: http://www.iwar.org.uk/ecoespionage/resources/transnational–crime/g,i07.htm (дата обращения: 15.01.2020).

References

1. Avdeeva G.K. 2015. Innovacii v bor'be s prestuplenijami, sovershaemymi s ispol'zovaniem informacionnyh tehnologij. [Innovation in the fight against crimes committedusing information technology]. Sovremennaja kriminalistika: problemy, tendencii, perspektivy: sbornik materialov Mezhdunarodnoj nauchno-prakticheskoj konferencii. 22.12.2015. M.: 327–331.

2. Akimov V.V. 2017. Kriminalisticheskaya osobennost' kiberprestuplenij. [The forensic feature of cybercrime]. Centr issledovaniya komp'yuternoj prestupnosti. M.: 54–55.

3. Valko D.V. 2016. Kiberprestupnost' v Rossii i mire: sravnitel'nyj analiz. [Cybercrime in Russia and in the world: a comparative analysis]. Upravlenie v sovremennykh sistemakh, 3(10): 29–40.

4. Veprev S.B., Nesterovich S.A. 2018. Kiberprestupnost' kak novaya forma prestupnosti. [Cybercrime as a new form of crime]. Rassledovanie prestuplenij: problemy i puti ikh resheniya, 3(21): 78–82.

5. A comprehensive study of the problem of cybercrime. 02.2013, URL: https://www.unodc.org/documents/organized–crime/cybercrime/Cybercrime_Study_Russian. (Date of appeal: 01/18/2020). (in Russian)

6. Ishchenko E.P. 2015. O kriminalisticheskom obespechenii raskrytija i rassledovanija kiberestuplenij. [On the forensic support of the disclosure and investigation of cybercrime]. In: Dejatel'nost' pravoohranitel'nyh organov v sovremennyh uslovijah: sbornik materialov 20-j mezhdunarodnoj nauchno-prakticheskoj konferencii. [Activity of law enforcement agencies in modern conditions: collection of materials of the 20th international scientific and practical conference]. In 2 vol. Vol. 1. Irkutsk: 336–337.

7. Nomokonov V.A. Tropina T.L. 2012. Kiberprestupnost' kak novaya krimi–nal'naya ugroza. [Cybercrime as a new criminal threat]. Criminology: yesterday, today, tomorrow, 24: 45–55.

8. Prostoserdov M.A. 2016. E`konomicheskie prestupleniya, sovershaemy`e v kiberprostranstve, i mery` protivodejstviya im. [Economic crimes committed in cyberspace and countermeasures against them]. The dissertation... candidate of legal sciences. M., 232 p.

9. Tropina T.L. 2005. Kiberprestupnost`: ponyatie, sostoyanie, ugolovno–pravovy`emery` bor`by` [Cybercrime: concept, condition, criminal law measures]. Dissertation ... of the candidate of legal Sciences.Vladivostok: 234 p.

10. Shevko N.R. 2016. Osobennosti raskrytiya i rassledovaniya kiberprestuplenij: problemy i puti resheniya. [Features of the disclosure and investigation of cybercrime: problems and solutions]. YUridicheskie nauki. M.: 11–14.

11. Brenner S. W. 2002. The emerging consensus on criminal conduct in cyberspace. UCLA Journal of Law and Technology. № 3. URL: http://www.lawtechiournal. com/articles/2002/Q3 020625 goodmanbrenner.php (date of appeal: 12.01.2020).

12. Colin B. 1997. The Future of Cyberterrorism. Crime and Justice International. March: 15–18.

13. Morrison P. 1991. Computer Crime. The Improvement of Investigative Skills. Final Report Part One: 89 p.

14. Sieber U. 2007. Legal Aspects of Computer–Related Crime in the Information Society. URL: http://europa.eu.int/lSPO/legal/en/comcrime/sieber.doc (date of appeal: 01.02.2020).

15. Shelley Louise I. 2003. Organized Crime, Terrorism and Cybercrime. Security Sector Reform: Institutions, Society and Good Governance. Baden–Baden: 303–312.

16. Williams P. 2005. Organized Crime and Cybercrime: Synergies, Trends and Responses. URL: http://www.iwar.org.uk/ecoespionage/resources/transnational–crime/ (date of appeal: 15.01.2020).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Должeнко Наталья Игоревна, кандидат юридических наук, доцент, доцент кафедры судебной экспертизы и криминалистики Белгородского государственного национального исследовательского университета, Белгород, Россия

Хмелевская Ирина Геннадиевна, студентка юридического института Белгородского государственного национального исследовательского университета, Белгород, Россия

INFORMATION ABOUT THE AUTHORS

Natalia I. Dolzhenko, candidate of law, associate Professor, associate Professor of the Department of forensic science and criminalistics of the Belgorod state national research University, Belgorod, Russia

Irina G. Khmelevskaya, student of the law Institute of the Belgorod state national research University, Belgorod, Russia