УДК 343.741 DOI: 10.14529/law220102

УГОЛОВНОЕ ЗАКОНОДАТЕЛЬСТВО ЗАРУБЕЖНЫХ СТРАН ОБ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ В ИНФОРМАЦИОННО-ЦИФРОВОЙ СРЕДЕ

Ю. А. Воронин, Т. В. Кухтина
Южно-Уральский государственный университет, г. Челябинск

В статье анализируются нормы зарубежного уголовного законодательства об ответственности за общественно опасные деяния в информационно-цифровой среде. Авторы отмечают наличие существенных различий в подходах к формулированию составов преступлений данной категории в различных государствах. Кроме того, в статье подчеркивается широкий разброс при определении видов и жесткости санкций в уголовном законодательстве различных стран мирового сообщества применительно к сходным по своим характеристикам разновидностям так называемой высокотехнологичной преступности. В этой связи представляются практически важными выводы о необходимости более детальной проработки и унификации составов информационно-цифровых преступлений в целях более эффективной борьбы с ними, в особенности с их транснациональной разновидностью. Причем это обязательно должно находить динамичное и синхронизированное отражение в уголовном законодательстве на национальном и международном уровнях.

Ключевые слова: информационно-цифровая среда, информационные технологии, уголовно-правовое регулирование информационно-цифровой преступности, уголовное законодательство зарубежных стран, уголовная ответственность.

1. Бесспорным фактом является то обстоятельство, что XXI век с особой остротой продемонстрировал необходимость решения проблемы информационно-цифровой преступности, с которой сегодня неизбежно сталкивается практически каждое государство. Нарастающая год от года динамика этих преступлений, зачастую носящих международный характер, диктует необходимость совершенствования и унификации уголовного законодательства стран мирового сообщества. Именно поэтому, как отмечалось в двух принятых в 2001 году Генеральной Ассамблеей ООН резолюциях о борьбе с преступным использованием информационных технологий (№ 55/63 и 56/121), сотрудничество государств в указанной области предполагает в числе целого ряда других мер, введение в их национальное законодательство норм об ответственности за преступления с использованием информационно-цифровых технологий и обеспечение сохранности компьютерных систем от несанкционированного вмешательства с преступной целью [8].

Речь, в сущности, идет о преступных деяниях, совершаемых посредством использования информационных компьютерных систем, выступающих либо предметом несанкционированного доступа к компьютерной информации, либо средством осуществления общественно опасных посягательств в виртуально-цифровой среде [12, с. 37–44]. И в этом смысле, особенно адекватной представляется формулировка, предложенная в Соглашении о сотрудничестве в области обеспечения международной информационной безопасности между правительствами государств – членов ШОС [1, с. 13]. В упомянутом документе информационная преступность определяется как использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях [7, с. 69].

Таким образом, с учетом терминологии международных документов, а также бытующих в законодательстве многих стран и в юридической литературе синонимов понятия анализируемого явления («компьютерная преступность», «кибепреступность в широком смысле слова», «преступления в сфере высоких информационных технологий»), наиболее широкой и одновременно оптимальной является категория «информационно-цифровая преступность». Такой подход действительно выглядит наиболее приемлемым, поскольку, как правило, он применим к соответствующей характеристике преступного использования центральных процессоров, серверов, персо-

нальных компьютеров, планшетов, смартфонов, бортовых компьютеров транспортных средств, мультимедийных устройств (MP3-плееров, игровых автоматов, цифровых фотоаппаратов). К этой же группе относятся такие носители данных, как жесткие диски, карты памяти USB или флеш-карты. К данной многочисленной группе уголовнонаказуемых деяний принято относить такие достаточно типичные преступления в виртуальном пространстве, как противозаконные доступ или перехват данных компьютерных систем; противодействие их функционированию путем распространения вредоносных программ; использование компьютерных технологий для подлога, онлайн-мошенничества, нарушения авторских прав, правонарушений, связанных с детской порнографией, и многие другие [7, с. 71–101]. Все упомянутое, на наш взгляд, позволяет констатировать, что цифровая (или информационно-цифровая) преступность представляет собой широкий круг общественно опасных деяний, совершенных в информационно-коммуникационной среде с использованием цифровой информации и информационно-телекоммуникационных технологий [2, с. 76].

2. К сожалению, изучение существующего правотворческого опыта разных стран применительно к данной разновидности преступлений свидетельствует, что сегодня даже при наличии сходства в трактовке ряда уголовно-правовых характеристик многих составов одновременно существуют и серьезные различия в подходе к их формулированию. В этой связи показателен конспективный аналитический обзор исторически складывавшейся ситуации и динамики изменений в этих нормах уголовного законодательства и в правоприменительной практике различных государств.

Так, по мнению ряда специалистов, в частности М. В. Ступень [9], А. А. Несмеянова [6, с. 43–48], Е. В. Громова [4, с. 30–35], наиболее быстрому и постоянному изменению подвергалось уголовное законодательство прежде всего Соединенных Штатов Америки. Связано это с несколькими причинами. Среди них следует отметить адаптивность англосаксонской правовой системы, позволяющей быстро реагировать на изменяющуюся ситуацию, и особенность финансовой системы США, где большая часть денег находится в безналичном формате. С этим связаны, кстати, и данные уголовной статистики, свидетельствующие о том, что 44 % всех киберпреступлений в стране приходится на похищение денег с кредитных карт, 16 % – на кражу секретной информации экономического характера [6, с. 47]. Неуклонным ростом этой статистики во многом объясним и динамизм законодательных изменений. Хотя в США с октября 1984 года довольно эффективно действовал базовый федеральный уголовный закон об ответственности за преступления в сфере высоких технологий (Computer Fraudand Abuse Act, CFAA), однако ему постоянно сопутствовали неоднократные дополнения, в частности в 1986, 1994, 1996 гг., логическим завершением которых стало воплощение всего этого конгломерата правовых норм главным образом в самостоятельный упорядоченный параграф 1030, а также параграф 1029 (и некоторые др.) Титула 18 Свода законов США [10]. Среди предусмотренных этими нормами уголовно-правовых деликтов упомянуты, в частности, несанкционированный доступ к компьютерной информации, умышленное или неосторожное повреждение защищенных компьютеров, компьютерный шпионаж, компьютерное мошенничество, хищение интеллектуальной собственности, угрозы, вымогательство и шантаж, совершаемые с использованием компьютерных технологий, и ряд других составов преступлений. Закон неоднократно изменялся, прежде всего в сторону ужесточения санкций, предусматривающих крупные штрафы и длительные сроки лишения свободы. Так, в целом ряде случаев – при проникновении в транспортные каналы связи, энергосети, системы управления водоснабжением – сроки тюремного заключения теперь могут достигать 30 лет, причем без права на досрочное освобождение от назначенного судом наказания. Стоит отметить при этом, что поскольку американское законодательство не унифицировано, то на уровне отдельных штатов перечень составов, видов и диапазона наказаний за данную категорию общественно опасных деяний может варьироваться в еще более широком диапазоне. В частности согласно УК штата Техас в зависимости от суммы ущерба, причиненного несанкционированным доступом в компьютерную систему, наказание в виде лишения свободы может быть назначено в пределах от 180 дней до 99 лет. Правда, предусмотрен также альтернативный вариант уголовно-

правовой санкции в виде различных сумм штрафа [5].

В Великобритании базовым законом, регулирующим вопросы уголовной ответственности за киберпреступления, является Закон о злоупотреблении компьютерами 1990 года. Однако правовое регулирование в этой сфере, как и в США, не отличается единообразием. Так, помимо упомянутого законодательного акта, парламент Великобритании принял целый ряд статутов, определяющих уголовную ответственность за две разновидности общественно опасных деяний в информационно-цифровой сфере, обладающих определенной спецификой. Во-первых, речь идет об ответственности за компьютерные преступления (computercrimes), касающиеся «неуполномоченного доступа к компьютерным данным», когда лицо использует компьютер для доступа к любой программе или данным, содержащимся в компьютере, если этот доступ является заведомо неправомочным и предназначен для уничтожения, блокирования, модификации либо копирования компьютерной информации. Типичные виды наказания – крупные суммы штрафа и тюремное заключение на срок от 6 месяцев и более. Вторая группа статутов, затрагивающих сферу киберпространства, устанавливает более жесткую ответственность за многочисленные преступления с непосредственным использованием интернета (internet-relatedcrimes). Среди них – различные корыстные общественно опасные деяния, а также (начиная с 2000 года) террористические действия, связанные с вмешательством или серьезным нарушением электронных систем [5].

Что касается УК ФРГ, то здесь криминализация деяний в информационно-цифровой сфере отражена, во-первых, в самостоятельном составе несанкционированного доступа к компьютерной информации (ст. 202 УК ФРГ) с целью получения выгоды для себя или других лиц. Речь идет о компьютерных данных, носящих особо охраняемый характер, передающихся электронным, магнитным и иным виртуальным способом и находящихся под специальной защитой от неправомерного доступа. Подобные действия влекут наказание в виде лишения свободы до 3 лет. Во-вторых, немецкий законодатель предусмотрел такой доступ в качестве способа совершения других преступлений, придав ему статус квалифицирующего обстоятельства и предусмотрев более жесткие санкции. Кроме того, п. b ст. 303 УК ФРГ к числу отягчающих отнес и ряд иных способов. К их числу, в частности, отнесены такие действия, как DNS-атаки и создание вредоносных программ с вмешательством в обработку компьютерных данных путем уничтожения, повреждения, изменения компьютерной системы, являющиеся существенными для бизнеса, деятельности предприятий и госорганов. Учитывая повышенную опасность подобных преступлений, немецкий законодатель предусмотрел и более суровый размер наказания – лишение свободы на срок до 5 лет [5].

Пожалуй, самую решительную борьбу с момента появления информационно-цифровых и прежде всего компьютерных преступлений демонстрируют Нидерланды. Для координации этой активности здесь был создан Консультативный комитет по киберпреступности, разработавший рекомендации относительно внесения законодательных новелл в уголовный и уголовно-процессуальный кодексы, а также предложивший оптимальную классификацию данной категории преступлений. Так, в соответствии с УК Нидерландов (ст. 139c) умышленное с корыстной целью использование тем или иным лицом технических устройств для перехвата или записи данных, идущих по телекоммуникационным системам или присоединенному оборудованию, наказывается штрафом или лишением свободы на срок до 1 года. Кроме того, лицо, снабжающее других субъектов средствами для незаконного перехвата и записи данных, передаваемых по автоматизированным или телекоммуникационным системам, подлежит наказанию в виде штрафа или лишения свободы на срок до 6 месяцев (ст. 139d). Наконец, лицо, обладающее данными, о которых оно знает или должно знать, что они получены в результате незаконного прослушивания, записи или перехвата данных автоматизированных или телекоммуникационных систем, также подлежит наказанию в виде штрафа или лишения свободы на срок до 6 месяцев (ст. 139e УК). Помимо этого, Законом о компьютерных преступлениях 1993 года перечень статей Уголовного кодекса Нидерландов о компьютерных преступлениях был дополнен целым рядом новых составов, в частности, о несанкционированном доступе в компьютерные сети и копировании их данных, компьютерном саботаже, распространении вирусов,

компьютерном шпионаже. Наряду с этим, во многие составы кодекса об уголовной ответственности за совершение так называемых традиционных общеуголовных преступлений (подлог, мошенничество, вымогательство и др.) были включены положения, позволяющие учитывать в процессе правоприменения специфику совершения таких преступлений в информационно-цифровой среде или с помощью информационно-цифровых технологий [5].

Таким образом, обзор уголовного законодательства упомянутых выше государств свидетельствует о том, что, пожалуй, самой характерной чертой, свойственной большинству их уголовных кодексов (или нормам прецедентного права), является отсутствие унифицированного подхода к формулированию составов так называемых информационно-цифровых преступлений. И хотя все обилие разнообразных криминальных деликтов рассматриваемой категории условно можно дифференцировать на относительно самостоятельные группы в зависимости от того или иного (главным образом, родового или видового) объекта посягательства, однако такая классификация на деле выглядит достаточно умозрительной и неизбежно будет разниться от государства к государству. Между тем, на наш взгляд, понастоящему успешное противодействие этим преступлениям – учитывая их транснациональную распространенность и, зачастую, их международный характер – требует единообразных законодательных подходов к определению оснований и мер уголовной ответственности за их совершение. В целом же реализация рассмотренных элементов стратегии противодействия цифровой преступности может принести положительные результаты лишь при реальном налаживании международного сотрудничества в деле разработки и принятия информационно-цифровых и законодательных стандартов в борьбе государств с криминализацией киберпространства [1, с. 13, 16, 39; 3, с. 176–185]. Пока же, к сожалению, далеко не все страны реально стремятся к практическому осуществлению международных договоренностей о сотрудничестве в этой области [11, С. 6, 7–11].

Литература

1. Воронин, Ю. А. Стратегические направления противодействия преступности в цифровой сфере: страноведческий анализ / Ю. А. Воронин, И. М. Беляева, Т. В. Кухтина // Вестник Южно-Уральский государственный университет. Серия «Право». – 2020. – Т. 20. – № 2. – С. 12–18.

2. Воронин, Ю. А. Преступления в сфере обращения цифровой информации и их детерминанты / Ю. А. Воронин // Научно-практический журнал «Виктимология». – 2020. – № 1 (23). – С. 74–83.

3. Воронин, Ю. А. Криминогенные факторы в информационно-цифровой среде / Ю. А. Воронин // В кн.: Smart Law for Smart Industry: сб. научных статей / под ред. Е. В. Титовой, Т. П. Подшивалова. – М.: Издательство «Проспект», 2020. – С. 176–185.

4. Громов, Е. В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше) / Е. В. Громов // Вестник Томского государственного педагогического университета. Серия: Гуманитарные науки (Юриспруденция). – 2006. – Вып. 11 (62). – С. 30–35.

5. Законодательство о киберпреступлениях в зарубежных странах: подборка РИА НОВОСТИ / ria.ru.

6. Несмеянов, А. А. Основные проблемы борьбы с преступлениями в сфере высоких технологий / А. А. Несмеянов // Вестник Восточно-Сибирского института МВД России. – 2014. – № 4. – С. 43–48.

7. Овчинский, В. С. Криминология цифрового мира: учебник / В. С. Овчинский. – М.: Норма: ИНФРА-М, 2018. – 351 с.

8. Резолюции Генеральной Ассамблеи ООН 55/63 от 22 января 2001 г. и 56/21 от 19 декабря 2001 г. «Борьба с преступным использованием информационных технологий».

9. Stupen M. V. URL: http://journalpro.ru/articles/sravnitelnyy-analiz-kiberprestup-leniy-v-rossi-i-zarubezhnykh-stranakh.

10. Federal Criminal Codeand Rules / Title 18 – Crimeand Criminal Procedure & 1029, 1030/ WestGroup, St. Paul. Minn, 1999.

11. Усилинский, Ф. А. Кибертерроризм в России: его свойства и особенности / Ф. А. Усилинский // Право и кибербезопасность. – 2014. – № 1. – С. 6–11.

12. Чекунов, И. Г. Киберпреступность: понятие и классификация / И. Г. Чекунов // Российский следователь. – 2012. – № 2. – С. 37–44.

Воронин Юрий Александрович – доктор юридических наук, профессор кафедры уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет, г. Челябинск. E-mail: voroninya@yandex.ru.

Кухтина Татьяна Владимировна – старший преподаватель кафедры уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет, г. Челябинск. E-mail: upiuip@mail.ru.

Статья поступила в редакцию 21 сентября 2021 г.

DOI: 10.14529/law220102

FOREIGN CRIMINAL LEGISLATION ON CRIMINAL LIABILITY IN THE INFORMATION-DIGITAL ENVIRONMENT

Yu. A. Voronin, T. V. Kukhtina
South Ural State University, Chelyabinsk, Russian Federation

The article analyzes the norms of foreign criminal legislation on liability for socially dangerous acts in the information and digital environment. The authors note that there are significant differences in the approaches to the formulation of offenses of this category in different states. In addition, the article emphasizes a wide range in determining the types and severity of sanctions in the criminal legislation of various countries of the world community in relation to varieties of the so-called high-tech crime that are similar in their characteristics. In this regard, the conclusions about the need for a more detailed study and unification of the elements of information and digital crimes in order to more effectively combat them, especially their transnational variety, seem to be practically important. Moreover, this must necessarily find a dynamic and synchronized reflection in the criminal legislation at the national and international levels.

Keywords: information-digital environment, information technologies, criminal law regulation of an information-digital crime, foreign criminal law regulation and criminal legislation, criminal liability.

References

1. Voronin Û. A., Belâeva I. M., Kuhtina T. V. [Strategic directions of combating crime in the digital sphere: country-specific analysis]. *Vestnik Ûžno-Ural'skij gosudarstvennyj universitet. Seriâ «Pravo» [Bulletin of the South Ural State University. Series "Law"]*, 2020, Vol. 20, no. 2, pp. 12–18. (in Russ.)

2. Voronin Û. A. [Crimes in the sphere of digital information circulation and their determinants]. *Naučno-praktičeskij žurnal «Viktimologiâ» [Scientific and practical journal "Victimology"],* 2020, no. 1 (23), pp. 74–83. (in Russ.)

3. Voronin Û. A. *Kriminogennye faktory v informacionno-cifrovoj srede* [Criminogenic factors in the information and digital environment]. *V kn.: Smart Law for Smart Industry: sb. naučnyh statej* [In the book: Smart Lab for Smart Industry: collection of scientific articles]. Moscow, 2020, pp. 176–185.

4. Gromov E. V. [The development of criminal legislation on crimes in the field of computer information in foreign countries (USA, Great Britain, Germany, the Netherlands, Poland)]. *Vestnik Tomskogo gosudarstvennogo pedagogičeskogo universiteta. Seriâ: Gumanitarnye nauki (Ûrisprudenciâ) [Bulletin of Tomsk State Pedagogical University. Series: Humanities (Jurisprudence)],* 2006, Vyp. 11 (62), pp. 30–35. (in Russ.)

5. Zakonodatel′stvo o kiberprestupleniâh v zarubežnyh stranah: pod-borka RIA NOVOSTI / ria.ru [Legislation on cybercrime in foreign countries: a selection of RIA NOVOSTI / ria.ru].

6. Nesmeânov A. A. [The main problems of combating crimes in the field of high technologies]. *Vestnik Vostočno-Sibirskogo instituta MVD Rossii [Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia]*, 2014, no. 4, pp. 43–48. (in Russ.)

7. Ovčinskij V. S. *Kriminologiâ cifrovogo mira* [Criminology of the digital world]. Moscow, 2018, 351 p.

8. Rezolûcii General′noj Assamblei OON 55/63 ot 22 ânvarâ 2001 g. i 56/21 ot 19 dekabrâ 2001 g. «Bor′ba s prestupnym ispol′zovaniem informacionnyh tehnologij» [UN General Assembly resolutions 55/63 of January 22, 2001 and 56/21 of December 19, 2001. "The fight against the criminal use of information technologies"]

9. Stupen M. V. URL: http://journalpro.ru/articles/sravnitelnyy-analiz-kiberprestupleniy-v-rossi-i-zarubezhnykh-stranakh.

10. Federal Criminal Codeand Rules / Title 18 – Crimeand Criminal Procedure & 1029, 1030/ WestGroup, St. Paul. Minn, 1999.

11. Usilinskij F. A. [Cyberterrorism in Russia: its properties and features]. *Pravo i kiberbezopasnost' [Law and cybersecurity]*, 2014, no. 1, pp. 6–11. (in Russ.)

12. Čekunov I. G. [Cybercrime: concept and classification]. *Rossijskij sledovatel' [Russian Investigator]*, 2012, no. 2, pp. 37–44. (in Russ.)

Yuri Alexandrovich Voronin – Doctor of Sciences (Law), Professor of the Department of Criminal and Criminal-Executive Law, Criminology, South Ural State University, Chelyabinsk, Russian Federation. E-mail: voroninya@yandex.ru.

Tatyana Vladimirovna Kukhtina – Research assistant of the Department of Criminal and Criminal-Executive Law, Criminology, South Ural State University, Chelyabinsk, Russian Federation. E-mail: upiuip@mail.ru.

Received 21 September 2021.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Воронин, Ю.А. Уголовное законодательство зарубежных стран об ответственности за преступления в информационно-цифровой среде / Ю, А. Воронин, Т. В. Кухтина // Вестник ЮУрГУ. Серия «Право». – 2022. – Т. 22, № 1. – С. 13–18. DOI: 10.14529/law220102.

FOR CITATION

Voronin Yu. A., Kukhtina T. V. Foreign criminal legislation on criminal liability in the information-digital environment. *Bulletin of the South Ural State University. Ser. Law*, 2022, vol. 22, no. 1, pp. 13–18. (in Russ.) DOI: 10.14529/law220102.