УДК 343.97 © П. Н. Кобец, 2022
DOI: 10.24412/1999-625X-2022-285-101-105

Правовые основы предупреждения киберпреступлений: отечественный и зарубежный опыт

П. Н. Кобец, ВНИИ МВД России, г. Москва
✉ pkobets37@rambler.ru

Ежегодный рост киберпреступлений не только угрожает доверию российского общества к процессам цифровизации, но и подрывает безопасность всей страны. Однако уголовно-правовые составы действующего российского законодательства, предусматривающие ответственность за рассматриваемые преступления, не адаптированы к новым видам преступных посягательств, совершаемых в области информационно-коммуникационных технологий. В связи с этим совершенствование правовых основ по активизации борьбы с киберпреступлениями на основе изучения положительного зарубежного опыта выступает в качестве базиса комплекса мер, связанных с предупреждением киберпреступлений в нашей стране.

Ключевые слова: киберпреступления; компьютерная преступность; правовое регулирование; уголовное законодательство; информационные данные; информационное пространство; информационные технологии.

Legal Basis for Cybercrime Prevention: Domestic and Foreign Experience

P. N. Kobets, All-Russian Research Institute of the Russian Ministry of Internal Affairs, Moscow
✉ pkobets37@rambler.ru

The annual growth of cybercrime not only threatens the trust of the Russian society in digitalization processes, but also undermines the security of the entire country. However, the corpus delicti covered by the current Russian legislation providing for responsibility for the crimes under study are not adapted to the new types of criminal attacks committed in the field of information and communication technologies. In this regard, the improvement of the legal framework for intensifying the fight against cybercrime based on the study of positive foreign experience serves as the foundation for the entire range of measures related to the prevention of cybercrime in our country.

Keywords: cybercrime; computer-related crimes; legal regulation; criminal laws; information data; information space; information technologies.

Современный цифровой век не только ввел новейшие технологии и предложил иные виды производств, он привел к появлению нового вида преступности, в которой преступники используют технологические достижения в киберпреступных целях. В результате возникла относительно новая разновидность преступных проявлений, называемая киберпреступностью, а правоохранители пытаются успевать совершенствовать правовое регулирование, направленное на противодействие этому виду преступности, созданного эволюцией цифровой эпохи. Во всем мире совершенствование правового регулирования киберпреступности становится отдельной областью уголовного законодательства. Она постоянно развивается, чтобы гарантировать обществу, что его правовая система идет в ногу с технологическими достижениями.

В начале нового тысячелетия средствами массовой информации, отечественными и зарубежными исследователями и в целом международным сообществом стали активно использоваться различные понятия и термины, которые обозначают противоправные явления в информационном пространстве (например, киберпреступность, компьютерная преступность, преступность в сфере информационных технологий, преступность в сфере информационного пространства, кибербуллинг, киберсталкинг и т. д). Журналисты, население, простые граждане многие из понятий пытаются употреблять в качестве синонимов, однако они не тождественны, несмотря на то что в какой-то степени близки по смыслу. Эти термины различны по своему объему и не могут выступать в качестве синонимов. Так, в международных отношениях как общепринятое наименование при обозначении и характеристике рассматриваемой категории противоправных деяний появилось понятие киберпреступности, которое все чаще применяли в названиях международных нормативных правовых актов, различных документов, а также в международно-правовой практике и деятельности организаций. Постепенно киберпреступность выделилась в качестве отдельной, составной области преступности.

Расследование и судебное преследование киберпреступлений становятся все более международными, и в этом процессе участвуют многочисленные агентства по всему миру. Таким образом, физические и юридические лица могут стать объектом параллельных уголовных расследований и судебных преследований, поднимающих сложные юрисдикционные и процессуальные вопросы. По своей природе киберпреступность не имеет границ, поэтому подверженность наказаниям за пределами юрисдикции физических лиц и бизнеса все чаще является реальной возможностью.

О всплеске киберпреступности в нашей стране было заявлено 4 декабря 2020 г. Президентом Российской Федерации В. В. Путиным в основной дискуссии конференции по искусственному интеллекту Artificial Intelligence Journey 2020 на тему «Искусственный интеллект — главная технология XXI века»[1]. Глава государства отметил, что в 2020 г. рост количества преступных посягательств в нашей стране с использованием IT-технологий превысил 75%, и это, по словам В. В. Путина, большая проблема и вызов, которому должно противостоять государство совместно со специалистами. Президент РФ озвучил, что эффективность борьбы с преступностью должна обеспечиваться не увеличением и ужесточением санкций за совершенные правонарушения, а неотвратимостью наказания.

Министр внутренних дел Российской Федерации В. А. Колокольцев также неоднократно подчеркивал необходимость противодействия киберпреступности, в частности, функционированию анонимных сервисов, анонимных sim-карт, использованию различных мессенджеров для преступных целей. Он отмечал, что обозначенные проблемы можно решить при условии реализации вопросов, связанных с правовым регулированием Интернета и повышением ответственности за размещение противоправного контента[2].

Существует уверенность в том, что Российская Федерация и дальше будет активно защищать право на неприкосновенность частной жизни, и это будет подтверждаться всякий раз, когда это необходимо. Однако поскольку масштабы и серьезность угроз киберпреступности продолжают прогрессировать, все субъекты борьбы с преступностью в нашей стране должны признать: одного совершенствования программного обеспечения в сфере обеспечения кибербезопасности недостаточно. Эффективно бороться со всеми проявлениями киберпреступности возможно при возникновении условий, при которых технологии в сфере кибербезопасности становятся эффективными только в том случае, если в обществе осознают необходимость процессов противодействия данному явлению и должным образом стремятся к их совершенствованию.

Проблематика, связанная с ответственностью за рассматриваемые преступления, исследуется как отечественными, так и зарубежными правоведами не первый год, однако до окончательного решения всех вопросов по данной теме пока нет. На отдельные проблемы исследователи имеют, как правило, собственные точки зрения. Поэтому теория уголовного права до настоящего времени не располагает единым пониманием киберпреступности как предмета преступного посягательства. В том числе в недостаточной мере учтены проблемы развития терминологии в сфере киберпреступности, есть множественные пробелы в уголовном законодательстве по вопросам, регулирующим уголовную ответственность за совершение новейших киберпреступлений.

В России и за рубежом существует большое разнообразие преступлений, подпадающих под понятие «киберпреступность», и с каждым годом их количество только увеличивается. В широком смысле эти противоправные деяния можно разделить на

[1] *Путин* заявил о всплеске киберпреступности. URL: https://rg.ru/2020/12/04/putin-zaiavil-o-vspleske-kiberprestupnosti.html / (дата обращения: 10.12.2021).

[2] *Колокольцев*: неконтролируемое развитие компьютерных технологий угрожает безопасности РФ. URL: https://tass.ru/politika/6170300 (дата обращения: 10.12.2021).

две категории: первая — это деяния, направленные на компьютерную технику или другие устройства для несанкционированного доступа к информации и перехвата информационных данных. Часто преступления такого рода называют компьютерными преступлениями. Вторая группа — преступления, в которых компьютеры или другие цифровые устройства являются ключевыми компонентами для совершения таких противоправных деяний в киберпространстве, как хищения, вымогательство, жестокое обращение с детьми, кибersталкинг и др.

Важно отметить, что понимание киберпреступности само по себе во многом шире термина «компьютерная преступность». Кроме того, термин «киберпреступность» (cybercrime) как нельзя точно раскрывает природу феномена преступности информационного пространства, подчеркивая ее связь с компьютерными, информационными технологиями, глобальными телекоммуникационными системами и сетями, тогда как термином «компьютерная преступность» (computer crime) в основном обозначают преступления, совершаемые в отношении компьютеров либо информационных данных, которые хранятся на них [1, с. 67].

Анализ использованных отечественной и международной правовой практикой подходов, определяющих киберпреступность, позволяет автору характеризовать ее как комплексное явление, которое включает в себя ряд категорий и криминальных действий, в частности кражу, мошенничество, вымогательство и другие виды преступлений, которые совершаются при помощи электронных сетей и информационных систем [2, с. 72, 100]. Кроме того, это деятельность, связанная с размещением незаконной информации и данных в телекоммуникационных сетях, а также с совершением атак в отношении информационных сетей, блокированием программного обеспечения на различных сайтах, нарушением авторских и смежных прав.

В целях борьбы с компьютерной преступностью в России главой 28 УК РФ «Преступления в сфере компьютерной информации» (ст. ст. 272–274) предусматривается ответственность специальными составами, криминализирующими такие противоправные действия, как неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ), а также неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274[1] УК РФ).

Мы согласны с позицией многих ведущих специалистов, по мнению которых, перечисленные уголовно-правовые составы не адаптированы к новым видам преступных посягательств, совершаемых в области информационно-коммуникационных технологий [3, с. 181; 4, с. 150]. При этом указанные проблемные вопросы могут успешно решаться на основе изучения и дальнейшего использования положительной зарубежной законодательной и правоприменительной практики. Например, в законодательстве некоторых зарубежных стран, в частности в УК ФРГ, есть уголовно-правовые нормы, предусматривающие санкции за противоправные деяния в сфере информационных телекоммуникационных технологий. К ним относятся действия по незаконному приобретению информационных данных; деяния, нарушающие тайну телекоммуникационной связи; действия, связанные с подделкой либо использованием подложных технических записей и данных, которые имеют доказательственное значение; действия по уничтожению, изменению или приведению в негодность данных, устройств, которые предназначены для обработки данных; деяния, связанные с подделкой платежных карт и бланков еврочеков[3]. Кроме того, в Германии уголовно-правовые нормы, регламентирующие ответственность за противоправные деяния в киберпространстве, подвержены постоянному совершенствованию и модификации. Так, несколько раз менялись дефинитивные части уголовно-правовых норм, которые регламентируют ответственность за совершение киберпреступлений [5, с. 11].

В Уголовный кодекс Франции включена специальная глава «О посягательствах на системы автоматизированной обработки данных», в которой в качестве санкции к некоторым составам применяют запрет сроком не менее чем на пять лет на использование кредитных карт, в результате которого осужденный обязан возвратить кредитную карту банку. Помимо этого, за рассматриваемые виды преступных посягательств к уголовной ответственности могут быть привлечены не только физические, но и юридические лица[4].

В ряде иностранных государств, в частности Пакистане, в соответствии с Декретом «О предотвращении электронных преступлений» в качестве санкции за кибератаки, повлекшие гибель людей, предусмотрена смертная казнь либо пожизненное лишение

[3] *Уголовный* кодекс ФРГ. URL: http://okpravo.ru/zarubezhnoe-pravo/ugolovnoe-pravo-zarubezhnyh-stran (дата обращения: 10.12.2021).

[4] *Уголовный* кодекс Франции. Принят в 1992 г. Вступил в силу с 1 марта 1994 г. с изм. и доп. на 1 янв. 2002 г. / науч. редактирование Л. В. Головко, Н. Е. Крыловой ; пер. с фр. и предисл. Н. Е. Крыловой. СПб., 2002.

свободы. Данным законодательным актом предусмотрена такая уголовная ответственность за иные киберпреступления, в том числе за незаконный доступ к вычислительным системам, их повреждение и др. Указанные преступные деяния наказываются лишением свободы на срок от трех до десяти лет[5].

Базовый нормативный правовой акт, регламентирующий привлечение к ответственности за совершение преступлений в сфере информационно-телекоммуникационных технологий, — Закон о неправомерном использовании компьютеров 1990 (Computer Misuse Act 1990) — был принят Парламентом Соединенного Королевства[6]. Этот Закон рассматривается как надежный и гибкий законодательный акт с точки зрения борьбы с киберпреступностью, поэтому он стал моделью, на основе которой несколько других стран, включая Канаду и Ирландскую Республику, впоследствии были заняты разработкой своих собственных законов об информационной безопасности. Для поддержания Закона в актуальном состоянии принято несколько поправок. В настоящее время к рассматриваемым видам преступлений относятся различные деяния в сфере информтехнологий.

Первым государством в мире, принявшим закон о необходимости защиты информационных данных, являются Соединенные Штаты Америки [6, с. 59]. Сегодня в этой стране насчитывается около 500 развернутых и отлично проработанных нормативных правовых актов, которые достаточно полно отражают вопросы информационной безопасности и посвящены уголовно-правовому регулированию правоотношений по использованию информационно-телекоммуникационного пространства и технологий.

Главной страной в мире, в которой самое большое число как физических, так и юридических лиц, пользующихся интернетом, является Китайская Народная Республика. Это наиболее уязвимая страна в сфере кибербезопасности, поэтому в Китае заинтересованы в принятии различных законодательных мер по противодействию киберпреступности.

Впервые меры уголовной ответственности в сфере обеспечения компьютерной безопасности в КНР введены постановлением Госсовета КНР от 18 февраля 1994 г. № 147 «О компьютерной безопасности информационных систем» [7, p. 14]. Через три года были предприняты новые шаги в сфере борьбы с киберпреступностью, которые законодательно закреплены новой редакцией Уголовного кодекса Китая, вступившего в силу в 1997 г. [8, с. 68]. Китайское законодательство по противодействию киберпреступности продолжало активно развиваться в условиях начала нового тысячелетия и в настоящее время располагает достаточным количеством уголовно-правовых норм, которые посвящены борьбе с рассматриваемым видом преступности.

Помимо уголовно-правовых норм Раздела II Особенной части Главы 6 «Преступления против порядка управления и общественного порядка» УК КНР, устанавливающих уголовную ответственность за противоправные деяния, связанные с незаконным вторжением в компьютерные информационные системы, совершение различных незаконных действий при помощи компьютерных информационных систем, деяния, связанные с умышленным созданием и распространением компьютерных вирусов и иных программ деструктивного характера и др. (ст. ст. 285–287-2 УК КНР), устанавливается уголовная ответственность за совершение финансового мошенничества, кражи, коррупции, хищения государственной тайны или других преступлений, совершенных при помощи компьютера (ст. 287 УК КНР). Также в соответствии с нормой УК КНР возможно привлечь лицо к уголовной ответственности за оскорбление через информационную сеть, которое привело к серьезным последствиям (ст. 246 УК КНР)[7].

Интернет-пользователи КНР не имеют возможности доступа к сайтам, которые распространяют сведения террористического характера. Китай, столкнувшийся с проявлениями кибертерроризма одним из первых, показал всему мировому сообществу, что бороться с кибертерроризмом не только необходимо, но и возможно на основе развития антитеррористического законодательства и совершенствования антитеррористической практики [9, p. 11].

Важными в сфере правоприменительной практики противодействия киберпреступности в настоящее время остаются решаемые на международном уровне вопросы, связанные с совершенствованием юридической техники и разработкой юридических терминов. Так, большую роль сыграло предложенное ЮНЕСКО понятие, определяющее информационные технологии как комплекс взаимосвязанных научных, технологических, инженерных дисциплин, изучающих методы эффективной организации охраны труда людей, занятых обработкой и хранением информации; вычислительную технику и методы, связанные с организацией и взаимодействием с людьми и производственным оборудованием, их практиче-

[5] *В Пакистане* введена смертная казнь за кибертерроризм. URL: https://www.securitylab.ru/news/362634.php (дата обращения: 10.12.2021).

[6] *Computer* Misuse Act 1990. URL: https://www.legislation.gov.uk/ukpga/1990/18/contents (дата обращения: 10.12.2021).

[7] *Уголовный* кодекс Китая / под ред. проф. А. И. Коробеева и проф. А. И. Чучаева, пер. с китайского проф. Хуан Даосю. М., 2017.

ские приложения, а также социальные, экономические и культурные проблемы [10, с. 65].

В заключение отметим, что сегодня как никогда важно сокращение имеющегося разрыва между практической и законодательной деятельностью в сфере информационной безопасности. Такой разрыв по большей степени объясняется темпами развития информационной сферы, за которой не всегда успевает законодательная, затягивая процессы, связанные с разработкой и принятием нормативных правовых актов. В связи с этим необходимо совершенствовать отечественное законодательство по противодействию киберпреступности. Данную работу важно строить на основе изучения положительного зарубежного опыта по законодательному регулированию противодействия киберпреступности, не только внося изменения в действующие отечественные законодательные нормы, но и делая акценты на принятии новых законодательных норм, соответствующих современным реалиям.

Список литературы

1. *Журавленко Н. И., Шведова Л. Е.* Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере // Общество и право. 2015. № 3(53).

2. *Смирнов А. А.* Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза : монография. М., 2012.

3. *Кобец П. Н.* Особенности киберпреступности в период пандемии COVID-19: состояние и дальнейший прогноз // Ученые записки Казанского юридического института МВД России. 2021. № 2(12).

4. *Номоконов В. А., Тропина Т. Л.* Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. Научный журнал. 2013. № 5(10).

5. *Тропина Т. Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : монография. Владивосток, 2009.

6. *Волеводз А. Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., 2001.

7. *Li P.* Ordinance of the People's Republic of China on the Protection of Computer Information System Security // Chinese Law & Government. 2010. Vol. 43, iss. 5.

8. *Шивдяков Л. А.* Кибертерроризм как новая и наиболее опасная форма терроризма // Защита информации. Инсайд. 2009. № 2(26).

9. *Navarria G.* China: the Party, the Internet, and power as shared weakness // Global Change, Peace and Security. 2016. Vol. 29.

10. *Федотова Е. Л.* Информационные технологии и системы : учеб. пособие. М., 2011.