УДК 343.3
DOI 10.33463/1999-9917.2019.27(1-4).1.080-086

ЕЛЕНА ВЛАДИМИРОВНА НЕЧАЕВА,
кандидат юридических наук, доцент,
доцент кафедры уголовно-правовых дисциплин,
Чувашский государственный университет имени И. Н. Ульянова,
г. Чебоксары, Российская Федерация,
e-mail: nechaeva_ev@mail.ru;
ЭЛЬВИРА ЮРЬЕВНА ЛАТЫПОВА,
кандидат юридических наук, доцент,
доцент кафедры уголовного права и процесса,
Казанский инновационный университет имени В. Г. Тимирясова,
г. Казань, Российская Федерация,
e-mail: elatypova@ieml.ru;
ЭДУАРД МАГАСУМЬЯНОВИЧ ГИЛЬМАНОВ,
старший преподаватель кафедры уголовного права и процесса,
Казанский инновационный университет имени В. Г. Тимирясова,
г. Казань, Российская Федерация,
e-mail: elegys@mail.ru

ПОСЯГАТЕЛЬСТВА НА ЦИФРОВУЮ ИНФОРМАЦИЮ: СОВРЕМЕННОЕ СОСТОЯНИЕ ПРОБЛЕМЫ

Для цитирования
Нечаева, Е. В. Посягательства на цифровую информацию: современное состояние проблемы / Е. В. Нечаева, Э. Ю. Латыпова, Э. М. Гильманов // Человек: преступление и наказание. – 2019. – Т. 27(1–4), № 1. – С. 80–86. – DOI : 10.33463/1999-9917.2019.27(1-4).1.080-086.

Аннотация. В статье рассматривается современное состояние проблемы уголовной ответственности за посягательства на цифровую информацию, их динамика и влияние на технологический и промышленный потенциал России, а также негативные последствия совершения преступлений в сфере цифровой информации. Широкое использование информационно-коммуникационных технологий является неотъемлемым требованием времени, представляя собой индикатор развития экономики. Однако поступательному развитию информационно-коммуникационных технологий мешает увеличение доли информационной преступности.

Анализируются статистические данные о преступлениях, совершенных с использованием компьютерных и телекоммуникационных технологий, делается вывод о постоянном увеличении их количества. Определяются приоритетные задачи в рассматриваемой сфере: необходимость коррекции действующего за-

конодательства как не соответствующего требованиям развития информационного пространства, в частности закрепление термина «цифровая информация» вместо устаревшего «компьютерная информация»; исследование способов использования цифровой информации при совершении преступлений ряда других групп (доведение до самоубийства, страховое мошенничество, незаконный оборот наркотических средств и т. п.); использование математических методов для прогнозирования преступности в сфере цифровой информации; рассмотрение возможности применения в отношении лиц, совершивших посягательства на цифровую информацию, наказания в виде обязательных, исправительных и принудительных работ; обсуждение проблемы использования вредоносного программного обеспечения, которое устанавливается без ведома пользователя, а также возможности привлечения к дисциплинарной ответственности за неосмотрительные действия лица, обязанного соблюдать необходимые требования пользователя; освещение проблемы обезличивания информации, собираемой и передаваемой различными мессенджерами; критический взгляд на потенциал иностранных государств как угрозу национальным интересам в сфере информационно-коммуникационных технологий.

Ключевые слова: цифровая информация, компьютерная информация, преступления, интернет, вредоносные программы, негласное получение информации, информация, неправомерный доступ к компьютерной информации.

Укрепление обороноспособности страны и ее национальной безопасности во многом зависит от активного развития информационного общества как в глобальном, так и в национальном масштабе. Современные информационно-телекоммуникационные устройства обладают поистине огромным потенциалом, однако процесс их активного использования во всех сферах общества неизбежно повлек за собой ряд негативных явлений, таких как неуклонный рост числа преступлений в сфере обращения цифровой информации. Это подтверждает необходимость анализа современного состояния проблемы уголовной ответственности за посягательства на цифровую информацию, а также смежных вопросов уголовной ответственности за совершение преступлений с использованием компьютерных и телекоммуникационных технологий.

Целесообразно провести исследование общественных отношений, складывающихся в сфере уголовно-правовой регламентации посягательств на цифровую информацию, целью которого является уяснение уголовно-правовой природы посягательств на цифровую информацию, а также обоснование предложений по совершенствованию и повышению эффективности уголовного законодательства в области регламентации уголовной ответственности за отдельные виды преступлений в сфере цифровой информации и практики применения наказания за преступления данной группы.

Уголовный кодекс Российской Федерации (УК РФ) использует термин «преступления в сфере компьютерной информации», однако считаем, что такое определение является чрезмерно узким в связи с тем, что современное развитие науки и техники привело к повсеместному использованию именно цифровой, а не компьютерной информации. Можно поддержать мнение И. Р. Бегишева о том, что «под цифровой информацией понимаются сведения (сообщения, данные), обращающиеся в информационно-телекоммуникационных устройствах, их системах и сетях» [1, с. 9]. Отметим, что в нормативно-правовых актах Российской Федерации используются синонимичные термины «компьютерная

информация», «цифровая информация» и «электронная информация», что неизбежно приводит к определенной путанице в терминологии. Следует также иметь в виду, что содержание данных понятий, несмотря на их несомненную близость, различно. При этом наиболее полным из указанных терминов является именно используемый нами «цифровая информация», так как в конечном итоге вся информация, используемая в информационно-телекоммуникационных сетях, сводится к использованию определенной последовательности нулей и единиц.

Аналогичная нестабильность в толковании данного понятия присутствует и в криминологии, где используются термины «компьютерная преступность», «преступность в сфере высоких технологий», «преступность в сфере компьютерной информации» [2, с. 133].

Можно констатировать, что в настоящее время понятие «информационная безопасность» только проходит стадию своего развития, и само понятие только формируется и наполняется специфическим содержанием.

К посягательствам на цифровую информацию, по нашему мнению, следует относить деяния, предусмотренные ст. 138.1 «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации», ст. 159.6 «Мошенничество в сфере компьютерной информации», ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» и ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» УК РФ. Отметим, что последний из указанных составов (ст. 274.1 УК РФ) был введен в УК РФ только 26 июля 2017 г. (Федеральный закон № 194-ФЗ). Необходимо также иметь в виду, что цифровая информация может использоваться и для совершения преступлений других групп, например, доведения до самоубийства [3, 4], совершения сексуальных домогательств в отношении несовершеннолетних или иных лиц и др. В частности, страховое мошенничество также может совершаться при помощи информационно-телекоммуникационных технологий (ИТК) [5, с. 79]. Широкое распространение получил незаконный оборот наркотиков посредством информационно-телекоммуникационных сетей [6, с. 349–353].

Посягательства на цифровую информацию могут выражаться также в использовании ИКТ с целью пропаганды идеологии терроризма, ксенофобии, экстремизма, распространения идей национальной исключительности, дестабилизации общественно-политической обстановки в стране и т. п.

На изощренность методов, способов и средств совершения посягательств на цифровую информацию указывается даже в Доктрине информационной безопасности Российской Федерации, что подтверждается и статистическими данными. Так, по состоянию на 1997 г. в России было зарегистрировано только 23 преступления в сфере компьютерной информации, тогда как в 2016 г. их было уже 1748 [7], однако реальные цифры намного превышают данные официальной статистики [1].

В 2017 г. официальные данные свидетельствуют о наличии 90 587 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, из которых раскрыто 20 424: среди преступлений, предварительное следствие по которым обязательно, зарегистрировано 62 404, а раскрыто из них 15 986, раскрываемость при этом составила всего 28,1 %, что подтверждает наш вывод о значительной латентности исследуемых посягательств [8]. Непосредственно в сфере компьютерной информации совершено 1883 преступления, 726 из которых было раскрыто. Что касается престу-

плений, предварительное следствие по которым необязательно, то с использованием компьютерных и телекоммуникационных технологий совершено 28 183 преступления, из которых раскрыто 27 680 (98,2 %), то есть практически все совершенные таким способом деяния.

За первые восемь месяцев 2018 г. (январь – август) с использованием компьютерных и телекоммуникационных технологий совершено 107 980 преступлений, из которых раскрыто 20 075. Количество преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, по которым обязательно предварительное расследование, за данный период составило 80 419, из которых раскрыто 21 081. Непосредственно в сфере компьютерной информации совершено 1653 преступления, из которых раскрыто 383 (28,1 %). Число преступлений, предварительное следствие по которым необязательно, с использованием компьютерных и телекоммуникационных технологий составило 27 561, из которых раскрыто 27 126 (98,4 %) [9], что вполне согласуется с данными за 2017 г.

Для прогнозирования преступности в сфере цифровой информации можно использовать математические формулы, предложенные некоторыми авторами, которые справедливо отмечают, что методы математического прогнозирования отличаются объективностью, достоверностью и точностью поучаемых результатов при условии правильного выбора математической модели [10].

Под посягательством на цифровую информацию следует понимать предусмотренное уголовным законом виновно совершенное общественно опасное деяние, нарушающее конфиденциальность, целостность, достоверность и доступность цифровой информации, охраняемой законом.

Данное положение поддерживается и И. Р. Бегишевым, обоснованно указывающим, что защищаемыми свойствами цифровой информации ограниченного доступа является ее конфиденциальность, целостность и достоверность, а общедоступной информации – ее целостность, достоверность и доступность [1, с. 10].

В частности, производитель антивирусного программного обеспечения компания AVIRA утверждает, что ежедневно в мире совершается более 4,4 млн веб-атак, в связи с чем каждому пользователю Интернета необходима надежная защита, и предлагает для этого новый программный антивирусный продукт Internet Security Suite.

Интересным и перспективным представляется использование в отношении лиц, совершающих посягательства на цифровую информацию, принудительных, исправительных или обязательных работ. Принудительный труд зарекомендовал себя как средство действенного исправительного воздействия не только в России, но и в зарубежных странах [11, с. 97–102; 12, с. 41–46]. Не менее эффективно использование в качестве дополнительного наказания лишения права заниматься определенной деятельностью [13], а также принудительных работ [14, с. 45–49], которые, к сожалению, не получили до сих пор практического применения.

В отношении государственных служащих, допустивших совершение посягательств на цифровую информацию, необходимо предусмотреть процедуру привлечения к дисциплинарной ответственности. В то же время следует тщательно избегать привлечения к уголовной ответственности лиц, которые могли совершить посягательство на цифровую информацию случайно, так как часто лицо, допустившее такое правонарушение, не осознает и не допускает для себя саму возможность его совершения, однако вследствие элементарной неосмотрительности все же совершает такое правонарушение. Например, это может касаться ситуации загрузки какой-либо программы или приложения из GooglePlay либо AppStore.

Достаточно часто пользователь незаметно для себя скачивает вредоносное программное обеспечение, когда приобретает его в AppStore или GooglePlay. Такое программное приложение может, например, активировать динамики и слушать звуки вокруг, передавая полученную информацию заинтересованным лицам (рекламодателям и др.), либо снимать данные пользователя о его онлайн-картах, паролях, логинах, с помощью чего мошенники могут атаковать телефон пользователя или снять с его электронных карт деньги. Приложения могут собирать довольно детальную информацию о пользователе, вплоть до истории браузера или домашнего адреса и мест нахождения пользователя, что может использоваться для предложения пользователю так называемой таргетированной рекламы [15].

Определенные проблемы возникают в отношении метаданных, которые собираются отдельными мессенджерами (например, WhatsApp, Google и др.), передающими эти данные в обобщенном виде рекламным компаниям. SEO-специалисты считают это стандартной практикой, о которой пользователь извещается при ознакомлении с политикой конфиденциальности этих мессенджеров. Только при согласии с ним пользователь получает возможность продолжить работу с конкретным мессенджером. Поисковик в процессе работы анализирует текст, отправляемый пользователем.

WhatsApp, например, объясняет: «Мы сотрудничаем со сторонними организациями, которые помогают нам обеспечивать работу, предоставлять, совершенствовать, анализировать, настраивать, поддерживать и продвигать наши сервисы. Предоставляя информацию этим организациям, мы требуем, чтобы они использовали ваши данные в соответствии с нашими инструкциями».

Обязательным требованием является необходимость обезличивания передаваемой информации, что исключает возможность получения данных о конкретном адресате. Однако можно отметить некое пересечение использования цифровой информации и личной безопасности пользователя, а также возможного совершения при помощи цифровой информации преступлений религиозного, экстремистского [16] и террористического характера.

Несмотря на то что разработчики передают данные на сервере в обезличенном и зашифрованном виде, злоумышленники могут перехватить необходимую им информацию и расшифровать ее. Такие атаки получили собственное наименование MITM (Man in the middle), и в качестве противодействия им разработчики должны проверять свои приложения на предмет возможных посягательств со стороны злоумышленников [15].

Доминирующим фактором развития информационно-телекоммуникационных технологий является действующее законодательство страны, включая уголовное, что отражает как государственную политику в указанной сфере, так и правила поведения юридических и физических лиц на территории России. Считаем, что к законодательству в сфере ИКТ можно относить весь комплекс общественных отношений, связанных с производством информации, ее распространением, использованием и обеспечением доступа к ней, как свободного, так и ограниченного (конфиденциальность информации).

Предлагаем изменить название ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ на более соответствующее ее содержанию – «Мошенничество с использованием цифровой информации». Данное предложение неоднократно высказывалось учеными-теоретиками (например, И. Р. Бегишевым [1, с. 22]), однако законодатель данное предложение пока не воспринимает.

Необходимо также выработать математическую модель предупреждения посягательств на цифровую информацию для реализации возможности определить будущее

и спрогнозировать результаты социальных, экономических и политических изменений. Данное положение подкрепляется выводами С. В. Максимова и др. [17]. Это подтверждается и возрастающим потенциалом иностранных государств в сфере ИКТ, и возникающими в связи с этим вызовами и угрозами в научной сфере, в работе государственных органов власти, промышленных комплексов и др.

Библиографический список

1. Бегишев И. Р. Понятие и виды преступлений в сфере обращения цифровой информации : автореф. дис. … канд. юрид. наук. Казань, 2017. 31 с. URL : http://kpfu.ru/dis_card?p_id=2404 (дата обращения: 28.10.2018).

2. Мочалов И. А., Шалагинова О. Б. Преступность в сфере информационно-телекоммуникационных технологий как угроза национальной безопасности страны // Преступность в сфере информационно-телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2016. № 1. С. 131–136.

3. Бастрыкин А. И. Преступления против несовершеннолетних в интернет-пространстве: к вопросу о виктимологической профилактике и уголовно-правовой оценке // Всероссийский криминологический журнал. 2017. Т. 11. № 1. С. 5–12. DOI : 10.17150/2500-4255.2017.11(1). 5-12.

4. Бычкова А. М., Раднаева Э. Л. Доведение до самоубийства посредством использования интернет-технологий: социально-психологические, криминологические и уголовно-правовые аспекты // Всероссийский криминологический журнал. 2018. Т. 12. № 1. С. 101–115. DOI : 10.17150/2500-4255.2018.12(1).101-115.

5. Латыпова Э. Ю. Страховое мошенничество как посягательство на права потребителей: проблемы и перспективы // Актуальные проблемы правового регулирования и правоприменительной практики в сфере защиты прав потребителей : материалы Всерос. науч.-практ. конф. / отв. ред. Г. П. Кулешова, И. Г. Гараев. М., 2017. С. 78–81.

6. Умаров М. Р., Нечаева Е. В. Незаконный оборот наркотиков в Интернете // Уголовно-правовая превенция в сфере оборота наркотических средств или психотропных веществ, алкогольной и спиртосодержащей продукции (региональный аспект) : сб. материалов Всерос. науч.-практ. конф. Чебоксары, 2015. С. 349–353.

7. Статистика и аналитика // Официальный сайт МВД России. URL : https://mvd.ru/Deljatelnost/statistics (дата обращения: 28.09.2018).

8. Общие сведения о состоянии преступности // Состояние преступности в России за январь – декабрь 2017 года. URL : https://file:///C:/Users/123/Documents/Downloads/Sostoyanie_prestupnosti_yanvary-dekabry_2017.pdf (дата обращения: 28.09.2018).

9. Общие сведения о состоянии преступности // Состояние преступности в России за январь – август 2018 года. URL : https://file:///C:/Users/123/Documents/Downloads/Sb_1808.pdf (дата обращения: 28.09.2018).

10. Цифровая криминология: математические методы прогнозирования / А. П. Суходолов [и др.]. Ч. 2 // Всероссийский криминологический журнал. 2018. Т. 12. № 3. С. 323–329.

11. Krymov, A., Rodionov, A. & Skiba, A. 2017, ‘Certain Aspects of the Interbranch Regulation of the Convictis’ Labor Organization in France’, Journal of Advanced Research in Law and Economics, vol. VIII, iss. 1(23), pp. 97–102, DOI : 10/14505/jarle.v8.1(23).11.

12. Крымов А. А., Родионов А. В., Скиба А. П. Правовое регулирование организации труда осужденных в пенитенциарных учреждениях Германии // Юридическая наука и практика // Вестник Нижегородской академии МВД России. 2017. № 1. С. 41–46.

13. Гильманов Э. М., Латыпова Э. Ю. Некоторые проблемы наказания за незаконный поиск и (или) изъятие археологических предметов из мест залегания // Правовые и нравственные аспекты обеспечения безопасности личности и государства на современном этапе политических и экономических санкций : сб. материалов Всерос. науч.-практ. конф. : в 2 ч. / отв. ред. Н. В. Хураськина. М., 2016. Ч. 2. С. 361–363.

14. Нечаева Е. В. Перспективы трансформации наказания в виде принудительных работ // Уголовно-исполнительное право. 2018. Т. 13. № 1. С. 45–49.

15. Как узнать, что вас прослушивают через ваши гаджеты. URL : https://hi-tech.mail.ru/review/proshchaj-lichnoe-prostranstvo-kto-i-kak-proslushivaet-nashi-gadzhety/#a02 (дата обращения: 05.11.2018).

16. Ярусова А. С., Латыпова Э. Ю. Мотив национальной или религиозной ненависти или вражды как элемент преступлений террористического характера // Правовые и нравственные аспекты обеспечения безопасности личности и государства на современном этапе политических и экономических санкций : сб. материалов Всерос. науч.-практ. конф. : в 2 ч. / отв. ред. Н. В. Хураськина. М., 2016. Ч. 2. С. 593–597.

17. Максимов С. В., Васин Ю. Г., Утаров К. А. Цифровая криминология как инструмент борьбы с организованной преступностью // Всероссийский криминологический журнал. 2018. Т. 12. № 4. С. 476–484. DOI : 10.17150/2500-4255.2018.12(4).476-484.