УДК 343.98:004.056(470)
DOI 10.17150/2500-4255.2019.13(3).416-425

КИБЕРПРЕСТУПНОСТЬ В РОССИЙСКОЙ ФЕДЕРАЦИИ: КРИМИНОЛОГИЧЕСКИЙ И УГОЛОВНО-ПРАВОВОЙ АНАЛИЗ СИТУАЦИИ

А.И. Коробеев, Р.И. Дремлюга, Я.О. Кучина
Дальневосточный федеральный университет, г. Владивосток, Российская Федерация

Информация о статье

Дата поступления
14 марта 2019 г.

Дата принятия в печать
7 июня 2019 г.

Дата онлайн-размещения
4 июля 2019 г.

Ключевые слова
Искусственный интеллект; интеллектуальные системы; киберпреступления; интернет-преступления; право кибербезопасности; средства совершения преступлений; общественная опасность; квалифицирующие признаки

Финансирование
Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта № 18-29-16129

Аннотация. Бурное развитие в мире коммуникационных систем с использованием для распространения информации компьютерной техники привело к появлению новых общественных отношений, нуждающихся в уголовно-правовой защите. Не осталась в стороне и Российская Федерация, которая пусть и поздно включилась в гонку высоких технологий, но развитие ее правовых норм в этой области не отстает от мировых тенденций. Не является исключением и право, направленное на борьбу с киберпреступностью и киберпреступлениями. Формирование глобального информационного пространства порождает неизвестные ранее угрозы национальной и международной безопасности. Ключевые характеристики информационного пространства, такие как трансграничность, анонимность, быстрота, сложность установления источника действий в Сети, обусловили рост количества пользователей информационных технологий, а также повысили привлекательность информационной инфраструктуры с точки зрения возможности использования Интернета в преступных целях. Противодействие этим угрозам стало важной составляющей комплекса мер по обеспечению безопасности на национальном и глобальном уровнях. Авторами статьи дана сравнительная оценка уровня киберугроз в России, сформулирована обобщенная оценка места киберпреступности среди глобальных угроз и экономического ущерба от киберпреступлений. Рассмотрены основные источники киберугроз, критические проблемы и технологии. Спрогнозированы возможные угрозы в свете внедрения систем искусственного интеллекта. Кроме того, проведен анализ действующих уголовно-правовых норм, запрещающих противоправную деятельность в сети Интернет, уделено внимание дискуссионным и проблемным вопросам науки и практики.

CYBERCRIMES IN THE RUSSIAN FEDERATION: CRIMINOLOGICAL AND CRIMINAL LAW ANALYSIS OF THE SITUATION

Alexander I. Korobeev, Roman I. Dremlyuga, Yaroslava O. Kuchina
Far Eastern Federal University, Vladivostok, the Russian Federation

Article info

Received
2019 March 14

Accepted
2019 June 7

Available online
2019 July 4

Keywords
Artificial intelligence; intellectual systems; cybercrime; Internet crimes; cybersecurity law; means of committing crimes; public danger; qualifying features

Acknowledgements
The study was carried out with the financial support of the Russian

Abstract. The rapid development of communication systems and the use of computer equipment for the exchange of information lead to the emergence of new social relations that require criminal law protection. The Russian Federation does not stay away from this, and although it joined the high tech race late, the development of its legal norms in this sphere follows global trends. Law aimed at counteracting cybercrimes is no exception. The emergence of the global information space gives rise to previously unknown threats to national and international security. Key characteristics of information space, such as its trans-border character, anonymity, speed, difficulty of identifying the actor in the network have led to the growth in the number of IT users and increased the attractiveness of the information infrastructure from the standpoint of using the Internet for criminal purposes. Counteracting these threats has become an important element of the complex of measures to ensure security at the national and the global levels. The authors of the article present the comparative evaluation of the level of cyber-threats in Russia, offer a generalized assessment of the place that cybercrimes hold among other global threats and of the economic damage inflicted by cybercrimes. They examine the key sources of cyber threats, the critical problems and technologies. The authors also make a prediction of the possible threats associated with the introduction of artificial intelligence sys-

Foundation for Basic Research in the framework of the research project No. 18-29-16129

tems. Besides, they carry out the analysis of the current criminal law norms which prohibit illegal activities in the Internet and pay attention to the debatable scientific and practical issues.

Мы живем во время, когда киберпространство как часть общего информационного пространства стало важным объектом правовых, политических, экономических отношений. Практически каждая современная отрасль науки и техники использует цифровые технологии и технику. Поэтому с начала 2000-х гг. набирает силу и ширится теория о том, что, нарушив работу этих сетей, можно вывести из строя целое государство [1]. А ряд происшествий, ставших достоянием общественности, например массированные атаки хакеров на крупные учреждения и организации по всему миру в 2017 г. [2, p. 101–102], позволяет объяснить актуальность изучения киберпреступности по всему миру.

Президент Российской Федерации В.В. Путин в своем выступлении на Петербургском международном экономическом форуме в 2017 г. подчеркнул значимость развития в России сектора цифровой экономики [3]. Программа развития цифровой экономики в любом государстве мира подразумевает внедрение в сферу регулирования общественных отношений новых подходов, связанных с оборотом компьютерной информации [2; 4]. Вот почему одним из основных элементов российской государственной политики по развитию цифровой экономики является обеспечение информационной безопасности[1], ибо с увеличением масштабов цифровизации экономики возрастает роль защиты публичной и частной информации от преступных посягательств [5].

Интернет пришел в Россию намного позже, чем в страны Северной Америки и Европы, в 1994 г., и рассматривался прежде всего как инструмент создания независимого информационного пространства, не несущий негативных последствий. Первые нормы, предусматривающие уголовную ответственность за киберпреступления, появились в отечественном законодательстве только с принятием в 1996 г. Уголовного кодекса Российской Федерации и введением гл. 28 «Преступления в сфере компьютерной информации».

При этом компьютерные преступления в нашей стране совершались задолго до вступления УК РФ 1996 г. в силу. Вероятно, первым широко известным киберпреступлением в СССР было вторжение в систему автомобильного заводского конвейера в 1983 г. [6, с. 157–161]. В те годы компьютер служил всего лишь объектом, средством или инструментом различных посягательств на государственную и общественную безопасность, личные и демократические права или на собственность.

Анализируя научные исследования в области киберпреступности, мы можем заключить, что большинство отечественных статей и монографий на эту тему представляет ее как тотальную и неотвратимую угрозу современному порядку, единственным способом борьбы с которой является ограничение киберотношений и контроль над ними [7, с. 9–10]. Одновременно высказываются мнения, почему это невозможно: скорость развития высоких технологий, доход, приносимый ими, и прочие положительные стороны виртуализации делают такие ограничения утопическими [8, p. 24–26].

После введения в действие УК РФ статистика отразила чрезвычайно быстрый рост количества киберпреступлений. Если в 1997 г. их было зарегистрировано только 30, то в 2000 г. — уже 760, а в 2017 г. — 1 883. Общее число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, в 2018 г. достигло 90 тыс.[2] Большинство преступлений (60–70 %) было квалифицировано по ст. 272 УК РФ. Второе место заняли преступления, связанные с созданием, использованием и распространением компьютерных вирусов (ст. 273 УК РФ). Нарушения правил эксплуатации ЭВМ (ст. 274 УК РФ) составили наименьшую долю среди всего числа зарегистрированных компьютерных преступлений [9].

При этом общественное мнение не признавало опасности киберпреступлений. Существовавшая в обществе концепция абсолютной свободы распространения информации, ограниченного только УК РФ и промышленными

[1] Об утверждении программы «Цифровая экономика Российской Федерации» : распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р // Собрание законодательства РФ. 2017. № 32. Ст. 5138.

[2] Генпрокуратура: число кибермошенничеств в РФ в 2018 году выросло в 7 раз // Вести. Экономика. 2018. 7 авг. URL: https://www.vestifinance.ru/articles/89268.

стандартами, низкий уровень интернетизации населения и прочие факторы привели к отсутствию контроля над оборотом информации в Интернете. Хакеры зачастую признавались гениальными людьми, которые случайно или в силу любопытства нарушают закон, а их деятельность не отождествлялась с преступлением, особенно на фоне резкого роста насильственной преступности, свойственной России в то время.

Напомним, что в тот период среднегодовой рост числа убийств составлял 20 %, а рост количества всех преступлений — 13 %, тогда как прирост населения выражался цифрой 0,4 % [10, с. 65]. Реальную угрозу представляла организованная преступность: более 150 преступных объединений контролировало до 40 тыс. государственных предприятий и 90 % частных [11, p. 443; 12, с. 22–28]. Это привело к тому, что основные ресурсы правоохранительных органов были брошены отнюдь не на борьбу с зарождающейся киберпреступностью.

Ситуация изменилась только после 2010 г., когда законодатель выставил серьезный заградительный барьер на пути незаконного распространения информации. Очевидным решением стало создание правовой базы, которая обязывала провайдеров Интернета ограничивать доступ к такой информации. Был создан специальный правительственный орган, ответственный за ограничения в киберпространстве, — Федеральная служба по надзору в сфере связи, информационных технологий и средств массовой информации, также известная как Роскомнадзор[3], действующая в соответствии с Временным регламентом исполнения государственной функции создания, формирования и ведения единой автоматизированной системы[4].

В 2012 г. был разработан и введен в действие Единый реестр доменных имен, индексов страниц сайтов в Интернете и сетевых адресов, позволяющих идентифицировать сайты в Интернете, предоставляющие информацию, распространение которой запрещено в Российской Федерации[5]. Реестр дает возможность на основании решения суда добавить в него адрес сайта, распространяющего незаконный контент или информацию, и тем самым осуществляет так называемую фильтрацию незаконного контента хостинг-провайдерами.

Личные данные российских граждан, которые пользуются услугами иностранных компаний, должны храниться на серверах, физически расположенных в России. Целью нововведения было преодолеть проблему юрисдикции в отношении цифровых данных, принадлежащих гражданам России. Новый режим введен ст. 18 Федерального закона «О персональных данных» № 152-ФЗ в 2014 г., которая гласит, что при сборе личных данных, например посредством Интернета, оператор должен обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, модификацию) и извлечение персональных данных граждан Российской Федерации посредством баз данных, расположенных на территории Российской Федерации.

В 2017 г. законодатель внес изменения в Уголовный кодекс, добавив ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации». Согласно этой статье, преступным считается «создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации». Таким образом, основным инструментом борьбы с преступлениями в Интернете по-прежнему остается гл. 28 УК РФ.

В гл. 28 Уголовного кодекса России законодатель криминализировал наиболее опасные виды посягательств на отношения в сфере цифровой экономики, или, иными словами, компьютерные отношения. К ним относятся:

– неправомерный доступ к компьютерной информации (ст. 272 УК);

– создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК);

[3] URL: http://roskomnadzor.ru.

[4] Временный регламент исполнения государственной функции создания, формирования и ведения единой автоматизированной системы «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено» : утв. Роскомнадзором 1 нояб. 2012 г. URL: http://www.consultant.ru/document/cons_doc_LAW_151301.

[5] URL: https://eais.rkn.gov.ru/faq.

– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК);

– неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК).

То есть отнюдь не все деяния, под которыми в литературе подразумевают преступления в киберпространстве, входят в понятие «преступления в сфере компьютерной информации». Ими признаются лишь те деяния, что посягают на общественные отношения, касающиеся безопасности компьютерной информации. Согласно будапештской Конвенции о преступности в сфере компьютерной информации от 23 ноября 2001 г., такие преступления входят в категорию преступлений против конфиденциальности, целостности и доступности компьютерных данных.

Объектом рассматриваемых преступлений являются общественные отношения в сфере обеспечения конфиденциальности, целостности и доступности компьютерной информации; сохранности и неприкосновенности средств хранения, обработки и передачи такой информации. В качестве предмета выступают компьютерная информация; средства хранения, обработки или передачи компьютерной информации; информационно-телекоммуникационные сети; оконечное оборудование. Понятие «компьютерная информация» раскрывается в примечании 1 к ст. 272 УК. Под ней понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Что касается самих средств хранения, обработки и передачи компьютерной информации, то ими являются ее материальные носители независимо от распространенности их использования. Сюда входят дискеты, жесткие и оптические диски, карты памяти, флеш-карты, внешние жесткие диски и т.д. Инструментом обработки компьютерной информации служит электронное устройство, предназначенное для ее автоматической обработки путем выполнения заданий, определенных последовательностью операций. Иными словами — компьютер, причем не только ПК, но и все, что обрабатывает цифровую информацию (телефон, фотоаппарат, планшет и др.), а также аналоговый аппарат (к примеру, автопилот).

Объективная сторона деяний, совершенных в сфере компьютерной информации, может быть выражена в форме как действий (ст. 272, 273 УК), так и бездействия (ст. 274, 274.1 УК). Все составы (кроме деяний, предусмотренных ч. 1 ст. 273 и ч. 1 ст. 274.1 УК) — материальные, а последствиями в основных составах компьютерных преступлений выступают уничтожение, блокирование, модификация, копирование компьютерной информации, крупный ущерб, вред.

Уничтожение компьютерной информации означает приведение ее полностью в непригодное для использования по своему функциональному назначению состояние (например, стирание ее с жесткого диска). Блокирование информации предполагает создание препятствий к свободному доступу к информации при сохранении самой информации. Модификацией информации признается внесение любых изменений в исходную информацию без согласия правообладателя. Копирование информации представляет собой ее воспроизводство в любой материальной форме.

С субъективной стороны лишь создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК), а также неправомерное воздействие на критическую информационную структуру Российской Федерации (ч. 1 и 2 ст. 274.1 УК) предполагают только умышленную форму вины. Остальные компьютерные преступления могут совершаться как с умыслом, так и по неосторожности.

Субъектом преступлений, предусмотренных ст. 272, 273 УК, является лицо, достигшее 16-летнего возраста. Субъект преступления, предусмотренного ст. 274 УК, — специальный. Им может быть только лицо, на которое возложена обязанность соблюдать правила эксплуатации средств хранения, обработки, передачи компьютерной информации, информационно-телекоммуникационных сетей или оконечного оборудования.

Квалифицированными и особо квалифицированными видами компьютерных преступлений выступают те же деяния, совершенные из корыстной заинтересованности, группой лиц по предварительному сговору, организованной группой, лицом с использованием своего служебного положения, с причинением тяжких последствий или созданием угрозы их наступления.

Отметим, что с момента введения в УК РФ самостоятельной главы 28 «Преступления в сфере компьютерной информации» достаточно серьезной оставалась проблема устаревшей терминологии. Лишь 7 декабря 2011 г. из дис-

позиций всех норм, входящих в главу, был исключен термин «электронно-вычислительная машина (ЭВМ)», благодаря чему заметно расширилась сфера применения соответствующих норм. Существенно изменилась и их редакция. Так, в ст. 272 УК появилось примечание, раскрывающее понятие компьютерной информации, а в 2017 г. глава пополнилась новой статьей — ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

При этом нововведение породило ряд новых правовых проблем. Причина их заключается в том, что любые сигналы напрямую связаны с носителями информации и средствами их хранения. В зависимости от этого они могут быть электрическими, электромагнитными, оптическими и т.д. В УК РФ, однако, речь идет исключительно об электрических сигналах. Между тем информация преобразуется в электрический сигнал лишь в момент обработки и ее конечной передачи. В этой связи в теории уголовного права существует предложение уточнить формулировку, назвав электрический сигнал конечным, т.е. уже поступившим в вычислительное устройство.

С другой проблемой судебная практика сталкивается при применении ст. 273 УК РФ. Прежняя редакция этой нормы предусматривала в качестве вредоносных программ только такие программы, которые заведомо приводили к преступным последствиям. Так уголовный закон боролся с неправомерной деятельностью достаточно ограниченного круга лиц (хакеров, компьютерных мошенников и т.д.).

Новая редакция ст. 273 УК позволяет расширить применимость нормы до практически любого пользователя нелицензированного программного обеспечения. Статья в нынешнем ее виде приравняла к вредоносным компьютерным программам и те, что предназначены для нейтрализации средств защиты компьютерной информации [12, с. 24]. Вредоносными программами могут теперь считаться все так называемые патчи, кейгены, кряки и подобное программное обеспечение [13, с. 152]. Как следствие, к уголовной ответственности по ст. 273 УК могут привлекаться не только создатели и распространители «варезного» софта (что имело место и ранее), но и рядовые пользователи, каковыми являются представители большей части российского компьютерного сообщества.

В соответствии же с положениями постановления Пленума Верховного Суда РФ «О практике рассмотрения судами уголовных дел о нарушениях авторских, смежных, изобретательских и патентных прав, а также о незаконном использовании товарного знака» от 26 апреля 2007 г. сбытчиками (распространителями) вредоносного программного обеспечения в виде «незарегистрированного» софта будут считаться лица, оказывающие содействие в его распространении, например путем размещения гиперссылки на ресурс, где осуществляется физическое хранение файла. С учетом наработанной в правоохранительных органах практики вычислить лицо, разместившее ссылку на «взломанный» софт, и привлечь его к уголовной ответственности не составит особой сложности [14, с. 135].

В процессе квалификации компьютерных преступлений одной из проблем является отграничение этих преступлений от смежных преступных деяний. В частности, возникает вопрос: правомерно ли пиратское тиражирование компьютерных программ квалифицировать только по ст. 146 УК, а хищение денежных средств с использованием компьютерных сетей — только по ст. 158 и 159 УК? Или в этих случаях требуется дополнительная квалификация еще и по статьям об ответственности за компьютерные преступления?

Мнения ученых по этому поводу разделились. Одни из них полагают, что компьютер в подобных ситуациях является только средством совершения преступлений, а потому квалификация по совокупности не может иметь места [15, с. 191–193]. Другие же настаивают на необходимости дополнительного вменения компьютерных преступлений [16, с. 15].

Нам представляется, что в описанных выше ситуациях мы сталкиваемся с идеальной совокупностью преступлений. При хищении безналичных денег с помощью компьютера путем неправомерного доступа к охраняемой законом компьютерной информации с последующей модификацией или копированием этой информации злоумышленник не только посягает на отношения собственности, но и одновременно причиняет вред другой группе общественных отношений, связанных с обеспечением конфиденциальности охраняемой компьютерной информации. В результате мы имеем идеальную совокупность преступлений против собственности (ст. 158 и 159 УК) и в сфере компьютерной информации (ст. 272 УК). Аналогичную совокупность можно обнаружить и в случае нарушения авторских прав путем сбыта контрафактных эк-

земпляров произведений, полученных в процессе неправомерного доступа к охраняемой компьютерной информации.

Серьезным вызовом является широкое использование систем искусственного интеллекта — компьютерных систем или программ, имитирующих один или несколько аспектов интеллектуального поведения, обладающих более высокой по сравнению с другими компьютерными системами или программами степенью самодетерминированности (автономности) и независимости от воли разработчика или пользователя. Некоторые интеллектуальные системы способны к обучению и самообучению. Уже сейчас такие системы могут активно применяться для выявления слабостей потенциальных жертв мошенничества, а также имитации деятельности человека.

Вот несколько небольших примеров. Одна из интеллектуальных систем может с высокой степенью достоверности установить сексуальную ориентацию человека по его фотографии, размещенной в социальных сетях[6]. Другая способна распознать политические убеждения и уровень интеллекта[7]. Подобные системы могут быть применены для манипуляции волей избирателя на выборах [17, p. 938–939]. Их использование несет в себе значительную общественную опасность.

Существуют интеллектуальные системы, имитирующие голос[8] или видеоизображение человека[9] [18]. С их помощью можно создавать аудио- и видеозаписи для манипуляции людьми. То есть системы искусственного интеллекта являются не просто очередным компьютерным средством совершения преступлений, они угрожают всему существующему публичному порядку, провоцируя «информационный апокалипсис» [19], в котором факт становится неотличимым от вымысла, и люди перестают пытаться понять разницу. Это подрывает доверие к любой информации и может дестабилизировать общество.

В целом же можно заключить, что в современной российской юридической науке утвердилось несколько теорий относительно общественной опасности киберпреступности. Первая теория касается такого преступления, как кибертерроризм, и его соотношения с общим уровнем проявления экстремизма и терроризма как в России, так и во всем мире. Ученые отмечают, что современные достижения научно-технического прогресса увеличивают вероятность применения изначально мирных технологий в качестве средств проведения кибератак, причем подобное их использование во вред порой даже не осознается создателями технологий [20, p. 305].

Мы не можем согласиться с этой позицией в силу того, что считаем ошибочным рассматривать интернет-технологии и новые кибертехнологии как источник угрозы сами по себе. С учетом общей истории развития терроризма и экстремизма высокие технологии должны восприниматься как средства и способы совершения указанных преступлений. Соответственно, мы полагаем неправильным выделять кибертерроризм и киберэкстремизм как новые виды преступлений — это лишь способы выражения привычной преступности, меры борьбы с которой не должны быть отделены от борьбы с терроризмом и экстремизмом вообще. Использование террористами Интернета и компьютерных систем для воздействия на большие массы людей посредством быстрого и дешевого распространения информации, по сути, представляет собой современный аналог печатной агитации и пропаганды, которые применялись ими до широкого внедрения компьютерных технологий в современную жизнь.

Также высказываются мнения о том, что возрастание изощренности кибертеррористических актов обусловлено тем, что на сегодняшний день у кибертеррористов есть реальная возможность нарушить нормальное функционирование критически важных объектов государства (ядерных реакторов, биологических и химических лабораторий и иных подобных объектов), что повлечет за собой неисчислимое количество жертв [ibid., p. 306–310]. В противовес им приводятся данные, согласно которым основными формами киберпреступлений являются оскорбление, клевета и преследование [21], за ними следуют мошенничество [22], шантаж и вымогательство, хищение денежных средств и пр. [23], а анархические группировки в Интер-

[6] New AI can guess whether you're gay or straight from a photograph. URL: <https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph>.

[7] Face-reading AI will be able to detect your politics and IQ, professor says. URL: <https://www.theguardian.com/technology/2017/sep/12/artificial-intelligence-face-recognition-michal-kosinski>.

[8] URL: https://lyrebird.ai ; https://www.technologyreview.com/the-download/610386/a-new-algorithm-can-mimic-your-voice-with-just-snippets-of-audio.

[9] URL: https://www.fakeapp.org.

нете — так называемый теневой Интернет — сосредоточены на борьбе с интеллектуальными правами и цензурой вообще, а вовсе не на преступлениях ненависти. Поэтому мы считаем в корне неверным смешивать киберпреступников и террористов, использующих интернет-мощности для пропаганды и вовлечения лиц в реальные террористические преступления, и не согласны с выделением признаков, свидетельствующих об улучшении технической оснащенности кибертеррористов, а также с выделением кибертерроризма в качестве «технологического вида терроризма» [24, p. 17–18].

Другая теория состоит в выделении тенденции превращения киберпреступности в долговременный фактор политического и экономического процесса. По мнению ее адептов, это обусловлено отсутствием крупных успехов в противодействии киберпреступности за последнее десятилетие, формированием новых предпосылок к ее дальнейшему распространению [25; 26]. Некоторые исследователи спорят с данной теорией, доказывая, что интернетизация населения ведет к снижению негативной социальной активности, переводя ее в так называемые сетевые войны, не имеющие реальных жертв, или позволяя лицам, не имеющим возможности повысить свое финансовое положение в силу различных социально-экономических причин, найти удаленную работу через Интернет, получить финансовую поддержку своих проектов, повысить уровень образования за счет обучающих онлайн-платформ и пр. [27; 28].

Подобные точки зрения высказывались, когда в Уголовный кодекс были введены дополнительные составы преступлений о доведении до самоубийства (ст. 110.1 и 110.2 УК РФ), где в числе средств и способов их совершения присутствует Интернет и кибертехнологии. Их авторы, ссылаясь на статистику, отмечали, что соотношение числа самоубийств обратно пропорционально распространению Интернета, поскольку в виртуальном пространстве человеку проще найти поддержку, общение по интересам, психологическую, социальную, финансовую и даже правовую помощь в силу отсутствия физического ограничения и доступности информации [29; 30].

Кроме того, хотелось бы отметить, что устойчивая тенденция к выделению киберпреступности в отдельный вид на самом деле представляет собой эволюцию существующих преступлений, а именно способов и средств их совершения. Так, в России распространена ошибочная квалификация такого преступления, как нарушение неприкосновенности частной жизни (ст. 137 УК РФ), по ст. 272 УК РФ («Неправомерный доступ к компьютерной информации»), если преступление было совершено с использованием кибертехнологий, а проще говоря, посредством доступа к электронной почте, социальным сетям, мессенджерам и пр. Причина этого, на наш взгляд, заключается в излишней криминализации дополнительных способов совершения преступлений или даже целых составов, где в объективной стороне указаны компьютерная информация, цифровые технологии, сеть Интернет и т.д. Кроме того, часто такие технологии воспринимаются законодателем одномерно, без учета их своеобразия и практически полной урегулированности действующим правом в силу информационной основы существования. Примером таких отношений могут быть не только компьютерная информация как таковая, но и криптовалюта, беспилотные авиационные системы, блокчейн, облачные технологии.

Иными словами, на данном этапе развития права и его попыток соответствовать переходу мирового сообщества к эпохе цифровых технологий наука и практика все чаще сталкиваются с ошибочным восприятием цифровой реальности. Например, в случае оценки общественной опасности кибертерроризма часто происходит смешение киберпреступности, кибершпионажа и терроризма в один вид преступной деятельности, тогда как, по нашему мнению, эта точка зрения опасна и даже разрушительна для юридической и правоохранительной деятельности, поскольку ведет к созданию конспирологических теорий о несуществующем виде преступных организаций.

Экстремизм в Интернете тоже представляется законодателю чрезмерно общественно опасным, поскольку совершение его специальным способом — с помощью сети Интернет, по мнению законодателя, отягчает общественную опасность деяния в силу практически неограниченного публичного доступа к публикации или выступлению. Мы, нисколько не оспаривая значимость объекта этих преступлений, все же считаем более обоснованной иную точку зрения, высказанную, например, М.И. Халиковым. Он совершенно справедливо утверждает, что важным для отделения экстремизма от иных преступлений является идеологический компонент, поскольку «определенная идеология есть мотивация экстремизма как деятельности» [31, с. 210].

Здесь, как и в случае с целым рядом других преступлений, имеет место серьезное заблуждение. Подобно тому как хулиганский мотив зачастую выдается за мотив политической, религиозной, национальной, расовой и иной ненависти или вражды либо за мотив ненависти или вражды в отношении какой-либо социальной группы, так и иные составы («классические» для уголовных законов не только России, но и иностранных государств) нередко обретают «двойников» в виде норм-аватаров, весьма несовершенных с точки зрения теории уголовно-правового запрета. И тогда умышленное причинение вреда или уничтожение чужого имущества криминализируется применительно к компьютерной информации в качестве неправомерного доступа, повлекшего ее уничтожение, а мошенничество получает «дубликат-клон» в виде мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ), по сути представляя собой объявление наказуемым отдельного способа совершения этого преступления. Такая законотворческая практика приводит к тому, что подобная статья становится казуальной, т.е. требующей разъяснения ее смысла для каждого конкретного дела. Отсутствие же надлежащего толкования может привести как к неправомерному отказу в возбуждении уголовного дела, так и к привлечению к уголовной ответственности лица, в действиях которого нет состава преступления, либо если этим лицом совершено иное деяние, запрещенное УК РФ.

Подавление технологического развития в целом, излишняя бюрократизация этого процесса и искусственное его торможение вызывают еще больший всплеск киберпреступлений. В таких случаях деятельность, которая могла бы быть законной и регулируемой, уходит в тень, отвлекает правоохранителя от реальных угроз, не позволяя ему определить, идет ли речь об изменении методов и способов совершения уже существующих преступлений (в частности, использовании новых технологий теми же преступниками), что были ранее, или же общество действительно сталкивается с новой угрозой, для борьбы с которой стоит создавать новые направления в уголовной политике, праве, криминологии и безопасности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Будко М.В. Киберпреступность как порожденная информатизацией угроза мировой экономике / М.В. Будко // Экономика и социум. — 2015. — № 2-1 (15). — С. 776–779.

2. Irwin A.S.M. Double-Edged Sword: Dual-Purpose Cyber Security Methods / A.S.M. Irwin // Cyber Weaponry / (ed.) H. Prunckun. — Cham : Springer, 2018. — P. 101–112.

3. Путин В. Внедрить цифровые технологии во все сферы жизни / В. Путин // Российская газета. — 2017. — 1–3 июня.

4. Governance Strategies for a Sustainable Digital World / I. Linkov [et al.] // Sustainability. — 2018. — Vol. 10, iss. 2. — P. 440.

5. Ali M.A. An Empirical Investigation of the Relationship between E-government Development and the Digital Economy: the Case of Asian Countries [Electronic resource] / M.A. Ali, M.R. Hoque, K. Alam // Journal of Knowledge Management. — 2018. — Vol. 22, iss. 5. — Mode of access: https://www.emeraldinsight.com/doi/abs/10.1108/JKM-10-2017-0477.

6. Кононова Е.Н. Современные проблемы борьбы с компьютерными преступлениями / Е.Н. Кононова // Известия высших учебных заведений. Правоведение. — 1997. — № 2. — С. 157–161.

7. Гапоненко В.Ф. Обеспечение экономической безопасности государства путем противодействия экономической преступности в системе современных информационных технологий / В.Ф. Гапоненко, Д.В. Тайгильдин // Механизм экономико-правового обеспечения национальной безопасности: опыт, проблемы, перспективы : материалы 8-й междунар. науч.-практ. конф., Краснодар, 28–30 апр. 2015 г. — Краснодар, 2015. — С. 3–10.

8. Saviotti P.P. Present Development and Trends in Evolutionary Economics / P.P. Saviotti, J.S. Metcalfe // Evolutionary Theories of Economic and Technological Change: Present Status and Future Prospects. — Chur : Harwood Academic Publishers, 1991. — P. 1–30.

9. Дремлюга Р.И. Интернет-преступность / Р.И. Дремлюга. — Владивосток : Изд-во Дальневост. гос. ун-та, 2008. — 240 с.

10. Бадов А.Д. География преступности в России: изменения за постсоветский период / А.Д. Бадов // Вестник Московского университета. Сер. 5, География. — 2009. — № 2. — С. 64–69.

11. Kuznetsova N.F. Crime in Russia: Causes and Prevention / N.F. Kuznetsova // Demokratizatsiya. — 1994. — Vol. 2, № 3. — P. 442–452.

12. Гаврилов В.М. Противодействие преступлениям, совершенным в сфере компьютерной и мобильной коммуникаций организованными преступными группами / В.М. Гаврилов. — Саратов : Сателлит, 2009. — 191 с.

13. Актуальные проблемы уголовного права. Часть Особенная : учебник / Л.В. Иногамова-Хегай [и др.]. — М. : Проспект, 2018. — 224 с.

14. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзишский. — М. : Юрид. лит., 1991. — 160 с.

15. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы / Т.Л. Тропина. — Владивосток : Изд-во Дальневост. ун-та, 2009. — 237 с.

16. Ляпунов Ю. Ответственность за компьютерные преступления / Ю. Ляпунов, В. Максимов // Законность. — 1997. — № 1. — С. 8–15.

17. Elections with Few Voters: Candidate Control Can Be Easy / J. Chen [et al.] // Artificial Intelligence Research. — 2017. — Vol. 60. — P. 937–1002.

18. Roose K. Here Come the Fake Videos, Too [Electronic resource] / K. Roose. — Mode of access: https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html.

19. Stover D. Garlin Gilchrist: Fighting Fake News and the Information Apocalypse / D. Stover // Bulletin of the Atomic Scientists. — 2018. — Vol. 74, iss. 4. — P. 283–288.

20. Analyzing the Threat of Unmanned Aerial Vehicles (UAV) to Nuclear Facilities / A. Solodov [et al.] // Security Journal. — 2018. — Vol. 31, iss. 1. — P. 305–324.

21. Digital Poly-Victimization: The Increasing Importance of Online Crime and Harassment to the Burden of Victimization / S. Hamby [et al.] // Journal of Trauma & Dissociation. — 2018. — Vol. 19, № 3. — P. 383–384.

22. Батаева Т.А. Актуальные проблемы борьбы с мошенничеством в сфере компьютерной информации / Т.А. Батаева // Наука в современном обществе: закономерности и тенденции развития : материалы междунар. науч.-практ. конф., Уфа, 28 сент. 2016 г. : в 2 ч. — Уфа, 2016. — Ч. 2. — С. 143–145.

23. Reep-van den Bergh C.M.M. Victims of Cybercrime in Europe: a Review of Victim Surveys [Electronic resource] / C.M.M. Reep-van den Bergh, M. Junger // Crime Science. — 2018. — Vol. 7, iss. 1. — Mode of access: https://doi.org/10.1186/s40163-018-0079-35.

24. Cullen F.T. Technology and Terrorism / F.T. Cullen ; ed. D. Clarke. — London : Routledge, 2017. — 244 p.

25. Демьянова Т.А. Киберпреступность как угроза безопасности современного общества / Т.А. Демьянова, П.А. Потиенко // Вестник Московского института государственного управления и права. — 2018. — № 2 (22). — С. 12–14.

26. Комлев Ю.Ю. Девиантность и преступность в эпоху high-tech, консьюмеризма и глэм-капитализма / Ю.Ю. Комлев // Вестник Казанского юридического института МВД России. — 2018. — № 1 (31). — С. 23–34.

27. Киселева С.О. Как молодому специалисту найти хорошую работу / С.О. Киселева // Актуальные проблемы социально-экологической культуры : сб. науч. тр. / отв. ред. Б.Г. Акчурин. — Уфа, 2018. — С. 125–131.

28. Карабанова Н.М. Стресс-менеджмент: «цена» стресса / Н.М. Карабанова // Управление в социально-экономических системах : материалы науч.-практ. конф., Владимир, 24–27 апр. 2012 г. — Владимир, 2012. — С. 642–646.

29. Дюмаева С. Существует ли на самом деле рост подросткового суицида? [Электронный ресурс] / С. Дюмаева // The Village. — Иркутск, 2017. — Режим доступа: https://www.the-village.ru/village/city/asking-question/258242-suicide.

30. Добрикова Е. Эксперты: «антисуицидальный» законопроект нуждается в доработке [Электронный ресурс] / Е. Добрикова. — Режим доступа: http://www.garant.ru/news/1103246.

31. Халиков М.И. Экстремизм (уголовно-правовой аспект) / М.И. Халиков // Вестник Удмуртского университета. Сер. «Экономика и право». — 2008. — Вып. 2. — С. 210– 216.

REFERENCES

1. Budko M.V. Cybercrime as a threat to global economy caused by informatization. *Ekonomika i sotsium = Economics and Society,* 2015, no. 2-1 (15), pp. 776–779. (In Russian).

2. Irwin A.S.M. Double-Edged Sword: Dual-Purpose Cyber Security Methods. In Prunckun H. (ed.). *Cyber Weaponry.* Cham, Springer, 2018, pp. 101–112.

3. Putin V. Introduce digital technology in all spheres of life. *Rossiiskaya Gazeta,* 2017, June 1–3. (In Russian).

4. Linkov I., Trump B.D., Poinsatte-Jones K., Florin M.-V. Governance Strategies for a Sustainable Digital World. *Sustainability,* 2018, vol. 10, iss. 2, pp. 440.

5. Ali M.A., Hoque M.R., Alam K. An Empirical Investigation of the Relationship between E-government Development and the Digital Economy: the Case of Asian Countries. *Journal of Knowledge Management,* 2018, vol. 22, iss. 5. Available at: https://www.emeraldinsight.com/doi/abs/10.1108/JKM-10-2017-0477.

6. Kononova E.N. Modern Problems of Struggle with Computer Crimes. *Izvestiya vuzov. Pravovedenie = Bulletin of Higher Educational Establishments. Jurisprudence,* 1997, no. 2, pp. 157–161. (In Russian).

7. Gaponenko V.F., Taigildin D.V. Ensuring the economic security of the state by counteracting economic crimes in the system of modern information technology. *Mekhanizm ekonomiko-pravovogo obespecheniya natsional'noi bezopasnosti: opyt, problemy, perspektivy. Materialy 8-i mezhdunarodnoi nauchno-prakticheskoi konferentsii, Krasnodar, 28–30 aprelya 2015 g.* [The Mechanism of Criminal Law Support of National Security: Experience, Problems, Prospects. Materials of the 8th International Scientific and Practical Conference, Krasnodar, April 28–30, 2015]. Krasnodar, 2015, pp. 3–10. (In Russian).

8. Saviotti P.P., Metcalfe J.S. Present Development and Trends in Evolutionary Economics. *Evolutionary Theories of Economic and Technological Change: Present Status and Future Prospects*. Chur, Harwood Academic Publishers, 1991, pp. 1–30.

9. Dremlyuga R.I. *Internet-prestupnost'* [Internet Crime]. Vladivostok, Far-Eastern Federal University Publ., 2008. 240 p.

10. Badov A.D. Geography of Crime in Russia: Changes During the Post-Soviet Period. *Vestnik Moskovskogo universiteta. Seriya 5, Geografiya = Moscow University Bulletin. Series 5, Geography,* 2009, no. 2, pp. 64–69. (In Russian).

11. Kuznetsova N.F. Crime in Russia: Causes and Prevention. *Demokratizatsiya,* 1994, vol. 2, no. 3, pp. 442–452.

12. Gavrilov V.M. *Protivodeistvie prestupleniyam, sovershennym v sfere komp'yuternoi i mobil'noi kommunikatsii organizovannymi prestupnymi gruppami* [Counteracting computer and mobile communications crimes committed by organized criminal groups]. Saratov, Satellit Publ., 2009. 191 p.

13. Inogamova-Khegai L.V., Kibal'nik A.G., Klenova T.V., Korobeev A.I., Lopashenko N.A. *Aktual'nye problemy ugolovnogo prava. Chast' Osobennaya* [Actual Problems of Criminal Law. Special Part]. Moscow, Prospekt Publ., 2018. 224 p.

14. Baturin Yu.M., Zhodzishsky A.M. *Komp'yuternaya prestupnost' i komp'yuternaya bezopasnost'* [Computer Crime and Computer Security]. Moscow, Yuridicheskaya Literatura Publ., 1991. 160 p.

15. Tropina T.L. *Kiberprestupnost': ponyatie, sostoyanie, ugolovno-pravovye mery bor'by* [Cybercrime: concept, condition, criminal law measures of counteraction]. Vladivostok, Far-Eastern Federal University Publ., 2009. 237 p.

16. Lyapunov Yu. Responsibility for Computer Crimes. *Zakonnost' = Legality,* 1997, no. 1, pp. 8–15. (In Russian).

17. Chen J., Faliszewski P., Niedermeier R., Talmon N. Elections with Few Voters: Candidate Control Can Be Easy. *Artificial Intelligence Research,* 2017, vol. 60, pp. 937–1002.

18. Roose K. *Here Come the Fake Videos, Too.* Available at: https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html.

19. Stover D. Garlin Gilchrist: Fighting Fake News and the Information Apocalypse. *Bulletin of the Atomic Scientists,* 2018, vol. 74, iss. 4, pp. 283–288.

20. Solodov A., Williams A., Hanaei S.A., Goddard B. Analyzing the Threat of Unmanned Aerial Vehicles (UAV) to Nuclear Facilities. *Security Journal,* 2018, vol. 31, iss. 1, pp. 305–324.

21. Hamby S., Blount Z., Smith A., Taylor E. Digital Poly-Victimization: The Increasing Importance of Online Crime and Harassment to the Burden of Victimization. *Journal of Trauma & Dissociation,* 2018, vol. 19, iss. 3, pp. 382–398.

22. Bataeva T.A. Urgent problems of counteracting fraud in the sphere of computer information. *Nauka v sovremennom obshchestve: zakonomernosti i tendentsii razvitiya. Materialy mezhdunarodnoi nauchno-prakticheskoi konferentsii, Ufa, 28 sentyabrya 2016 g.* [Science in the contemporary society: patterns and development trends. Materials of International Scientific and Practical Conference, Ufa, September 28, 2016]. Ufa, 2016, pt. 2, pp. 143–145. (In Russian).

23. Reep-van den Bergh C.M.M., Junger M. Victims of Cybercrime in Europe: a Review of Victim Surveys. *Crime Science,* 2018, vol. 7, iss. 1. Available at: https://doi.org/10.1186/s40163-018-0079-35.

24. Cullen F.T.; Clarke D. (ed.). *Technology and Terrorism.* London, Routledge, 2017. 244 p.

25. Demyanova T.A., Potienko P.A. Cybercrime as a threat to the security of modern society. *Vestnik Moskovskogo instituta gosudarstvennogo upravleniya i prava = Bulletin of Moscow University of State Management and Law,* 2018, no. 2 (22), pp. 12–14. (In Russian).

26. Komlev Yu.Yu. Deviation and Crimes in Time of High-Tech, Consumerism and Glamour Capitalism. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Kazan Law Institute of MIA Russia,* 2018, no. 1 (31), pp. 23–34. (In Russian).

27. Kiseleva S.O. How a new graduate can land a good job. In Akchurin B.G. (ed.). *Aktual'nye problemy sotsial'no-ekologicheskoi kul'tury* [Actual Problems of Social and Ecological Culture]. Ufa, 2018, pp. 125–131. (In Russian).

28. Karabanova N.M. Stress management: the «price» of stress. *Upravlenie v sotsial'no-ekonomicheskikh sistemakh. Materialy mezhdunarodnoi nauchno-prakticheskoi konferentsii, Vladimir, 24–27 aprelya 2012 g.* [Management in Social and Economic Systems. Materials of International Scientific and Practical Conference, Vladimir, April 24–27, 2012]. Vladimir, 2012, pp. 642–646. (In Russian).

29. Dyumaeva S. *Sushchestvuet li na samom dele rost podrostkovogo suitsida?* [Is the number of teenage suicides really growing?]. Available at: https://www.the-village.ru/village/city/asking-question/258242-suicide. (In Russian).

30. Dobrikova E. *Eksperty: «antisuitsidal'nyi» zakonoproekt nuzhdaetsya v dorabotke* [Experts: «anti-suicidal» draft law needs improvement]. Available at: http://www.garant.ru/news/1103246. (In Russian).

31. Khalikov M.I. Extremism (Criminal and Legal Aspect). *Vestnik Udmurdskogo universiteta. Seriya «Ekonomika i pravo» = Bulletin of Udmurt University. Series «Economics and Law»,* 2008, iss. 2, pp. 210– 216. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Коробеев Александр Иванович — заведующий кафедрой уголовного права и криминологии Дальневосточного федерального университета, доктор юридических наук, профессор, г. Владивосток, Российская Федерация; e-mail: akorobeev@rambler.ru.

Дремлюга Роман Игоревич — доцент кафедры международного публичного и частного права Дальневосточного федерального университета, кандидат юридических наук, г. Владивосток, Российская Федерация; e-mail: dremliuga.ri@dvfu.ru.

Кучина Ярослава Олеговна — доцент кафедры уголовного права и криминологии Дальневосточного федерального университета, кандидат юридических наук, доцент, LL.M., г. Владивосток, Российская Федерация; e-mail: kuchina.yao@dvfu.ru.

ДЛЯ ЦИТИРОВАНИЯ

Коробеев А.И. Киберпреступность в Российской Федерации: криминологический и уголовно-правовой анализ ситуации / А.И. Коробеев, Р.И. Дремлюга, Я.О. Кучина // Всероссийский криминологический журнал. — 2019. — Т. 13, № 3. — С. 416–425. — DOI: 10.17150/2500-4255.2019.13(3).416-425.

INFORMATION ABOUT THE AUTHORS

Korobeev, Alexander I. — Head, Chair of Criminal Law and Criminology, Far Eastern Federal University, Doctor of Law, Professor, Vladivostok, the Russian Federation; e-mail: akorobeev@rambler.ru.

Dremlyuga, Roman I. — Ass. Professor, Chair of International Public and Private Law, Far Eastern Federal University, Ph.D. in Law, Vladivostok, the Russian Federation; e-mail: dremliuga.ri@dvfu.ru.

Kuchina, Yaroslava O. — Ass. Professor, Chair of Criminal Law and Criminology, Far Eastern Federal University, Ph.D. in Law, Ass. Professor, LL.M., Vladivostok, the Russian Federation; e-mail: kuchina.yao@dvfu.ru.

FOR CITATION

Korobeev A.I., Dremlyuga R.I., Kuchina Ya.O. Cybercrimes in the Russian Federation: criminological and criminal law analysis of the situation. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2019, vol. 13, no. 3, pp. 416–425. DOI: 10.17150/2500-4255.2019.13(3).416-425. (In Russian).