УДК 340

Вишневецкий Кирилл Валерьевич
доктор юридических наук, профессор,
начальник кафедры уголовного права и криминологии,
Краснодарский университет МВД России
kvishnevecky@mail.ru
Кашкаров Алексей Александрович
доктор юридических наук, доцент,
начальник кафедры уголовного права и криминологии,
Крымский филиал Краснодарского университета МВД России
kashkarov79@yandex.ru
Кашкаров Александр Александрович
кандидат юридических наук,
доцент кафедры уголовно-правовых дисциплин,
Крымский юридический институт - филиал
Университета прокуратуры Российской Федерации
kashkarov79@yandex.ru
Kirill V. Vishnevetskiy
doctor of law, Professor
Head of criminal law Department and criminology
Krasnodar University of the Ministry of internal
Affairs of Russia kvishnevecky@mail.ru
Alexey A. Kashkarov
doctor of Law, Associate Professor,
Head of the Department of Criminal Law and
Criminology Crimean Branch
of the Krasnodar University of the Ministry of
Internal Affairs of Russia
kashkarov79@yandex.ru
Alexander A. Kashkarov
candidate of jurisprudence, associate professor Chair of
Criminal Law Disciplines Crimean Law Institute (branch)
University of the Prosecutor's Office of the Russian Federation
kashkarov79@yandex.ru

Общественная опасность и криминализация создания, размещения, обслуживания и использования имитации информационного ресурса в информационно-телекоммуникационных сетях, включая сеть «Интернет» (Часть 1)

Public danger and criminalization of the creation, placement, maintenance and use of an imitation of an information resource in information and telecommunication networks, including the Internet (Part 1)

Аннотация. *Стабильно высокий рост количества пользователей информационно-телекоммуникационными сетями, особенно сети «Интернет», количества обращений к информационным ресурсам свидетельствует о цифровизации общественных отношений. В первой части публикации раскрыта общественная опасность создания, размещения, обслуживания и использования имитации информационного ресурса в информационно-телекоммуникационных сетях, включая сеть «Интернет», приведены примеры её характеризующие. Обосновывается необходимость криминализации такого рода общественно опасных деяний.*

Ключевые слова: *имитация информационного ресурса, информационная безопасность, санитарно-эпидемиологическое благополучие населения, преступление, криминализация, уголовное право, уголовно-правовая политика, благополучие населения, общественная опасность, создание, размещение, обслуживание и использование.*

Annotation. *A consistently high growth in the number of users of information and telecommunication networks, especially the Internet, the number of appeals to information resources indicates the digitalization of public relations. The first part of the publication reveals the social danger of creating, hosting, maintaining and using an imitation of an information resource in information and telecommunication networks, including the Internet, and examples characterizing it are given. The necessity of criminalization of this kind of socially dangerous acts is substantiated.*

Key words: *imitation of an information resource, information security, sanitary and epidemiological welfare of the population, crime, criminalization, criminal law, criminal law policy, welfare of the population, public danger, creation, placement, maintenance and use.*

Стабильно высокий рост количества пользователей информационно-телекоммуникационными сетями, особенно сети «Интернет», количества обращений к информационным ресурсам (интернет-страницы, интернет-сайты, мобильные приложения смартфонов, планшетов и других мобильных устройств) информационно-телекоммуникационных сетей, а также учитывая, что информационно-телекоммуникационные сети активно используются образовательными, торговыми, финансовыми и иными организациями, учреждениями здравоохранения, органами публичной власти для предоставления государственных и муниципальных услуг свидетельствует о цифровизации общественных отношений. Социально значимые и позитивные достижения, которые мы можем наблюдать в результате научно-технического прогресса и глобальной информатизации социума, имеют и обратный, негативный эффект. Достижения науки и техники используются с целью совершения преступлений и иных, пока уголовно не наказуемых общественно опасных деяний. Технологический прогресс, с одной стороны, порождает новые возможности и эффективные средства противодействия силам деструкции, но, в то же время, наделяет преступников и террористов

инновационными ранее не существовавшими методами и инструментами [1, с. 22].

Соглашаясь с мнением Ю.Е. Пудовочкина, укажем, что новые вызовы, к которым относится и обеспечение информационной безопасности нашего общества, требуют от уголовной политики в целом и уголовного права, в частности, поиска новых решений, которые не возможны без пересмотра многих, если не всех, традиционных начал уголовно-правового регулирования, однако, пересмотра такого, который не сопровождался бы разрушением отрасли, но обеспечил бы ее устойчивое развитие в будущем, ответы на такого рода вызовы, зачастую, сводятся к многочисленным частным корректировкам уголовного закона и уголовной политики, в то время как, сама по себе, новая проблема требует инновационной уголовно-политической идеи, реализация которой может привести к созданию и внедрению нового технологичного продукта – уголовного права эпохи информатизации и поиск которой должен составить основное направление развития современной правовой науки [2, с.91]. Также, отметим верность позиции А.Н. Игнатова, о том, что минимизация криминогенности техногенности человеческого развития обуславливает необходимость выработки эффективных механизмов контроля над ситуацией. Безопасность нашего будущего во многом определяется своевременностью анализа и предвидения перспектив, рисков и криминогенности человеческой рационально-технологической деятельности в условиях техногенного цивилизационного развития и возможностей защиты человека, общества и государства от соответствующих угроз[3, с. 34-40].

В программном документе «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы» отмечается, что «информационные и коммуникационные технологии стали частью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка» [4]. Мы уже живем в цифровом мире, указывает В.С. Овчинский, строим цифровую экономику, но у нас отсутствует какой-либо структурированный взгляд на образ преступности цифрового мира[5].

Указанные обстоятельства требуют соответствующей и своевременной реакции со стороны государства с целью обеспечения правового регулирования и правовой охраны общественных отношений, которые уже объективно существуют в процессе пользования информационными ресурсами информационно-телекоммуникационных сетей.

Изучение способов совершения преступлений, иных противоправных действий с использованием информационно-телекоммуникационных технологий (далее – ИТТ) свидетельствует о том, что у правоприменителя отсутствует правовой инструментарий, дающий возможность обеспечивать уголовно-правовую охрану общественных отношений в сфере информационной безопасности, не криминализированы общественно опасные деяния, связанные с имитацией оригинального информационного

ресурса в информационно-телекоммуникационных сетях, в том числе, в сети «Интернет».

Создание, размещение, обслуживание и использование имитации информационного ресурса в информационно-телекоммуникационных сетях, включая сеть «Интернет», создает угрозу общественным отношениям в сфере информационной безопасности, охрана которых, исходя из вышеизложенного, становится все более актуальной в современных условиях. Кроме того, совершение вышеописанных общественно опасных деяний может способствовать совершению преступлений против:

- собственности, преступлений посягающих на неприкосновенность частной жизни, честь и достоинство личности;
- авторских и смежных прав;
- здоровья населения (в части санитарно-эпидемиологического благополучия населения).

Хрестоматийным является положение, что именно общественная опасность деяния выступает базисом криминализации, который принимается законодателем за основу при внесении изменений либо дополнений в действующий уголовный закон. Раскрывая сущность общественной опасности информационных преступлений, к которым мы относим и противоправное создание имитации информационного ресурса, следует согласиться с мнением о том, что «в XXI веке значимость компьютерной информации сложно преуменьшить, и общественные отношения в сфере безопасности компьютерной информации, конечно же, нуждаются в уголовно-правовой охране. Однако формирование и формулирование уголовно-правовых запретов в данной области не может осуществляться без учета характера и степени общественной опасности деяний» [6].

Мы полагаем, что общественная опасность деяния, связанного с созданием имитатора информационно-телекоммуникационного ресурса, характеризуется такими показателями, как:

- высокие уровни распространенности, повторности (прецедентности) и латентности;
- дистанционный характер деяния (существенная географическая удаленность жертв и виновных лиц);
- использование злоумышленниками инновационных информационно-когнитивных способов совершения преступлений;

Нам представляется, что общественная опасность создания и использования, размещения и обслуживания имитатора информационного ресурса также выражается и в том, что такого рода деяния способствуют иной общественно опасной деятельности, которая выражается, например, в совершении хищения либо в противоправном распространении сведений о частной жизни иного лица. Такого рода общественно опасные деяния обладают, по мнению исследователей, кумулятивной общественной опасностью [7, с. 60], которая характеризуется высоким негативным потенциалом. Этот потенциал направлен на другие общественные отношения, помимо тех, которые были затронуты совершенным

преступлением. Иначе говоря, преступное посягательство на один объект уголовно-правовой охраны потенциально влечет посягательство на другой объект преступлений в иной сфере [6].

Существующие нормы отечественного уголовного законодательства не обеспечивают надлежащую охрану общественных отношений в сфере информационной безопасности и защищенности в связи с чем, возникает необходимость дополнения Уголовного кодекса Российской Федерации (далее – УК РФ) нормой, устанавливающей уголовную ответственность за создание, размещение, обслуживание и использование имитации информационного ресурса в информационно-телекоммуникационных сетях, включая сеть «Интернет». Такого рода норма обеспечит реализацию одной из задач, предусмотренных ч. 1 ст. 2 УК РФ, а именно, предупреждение общественно опасных деяний средствами уголовного законодательства. Кроме того, предлагаемая нами норма обеспечит уголовно-правовое предупреждение иных преступлений на стадии приготовления и покушения.

Предлагаемая нами уголовно-правовая новелла содержит ряд новых для теории уголовного права и правоприменительной практики терминов, которые следует разъяснить, среди них - «имитация информационного ресурса информационно-телекоммуникационных сетей». Под информационным ресурсом информационно-телекоммуникационной сети мы понимаем любую интернет-страницу, их совокупность, объединенные в соответствующие интернет-сайты, а также - мобильные приложения смартфонов, планшетов и других мобильных устройств. Информационные ресурсы обладают определенным дизайном, установленным доменным именем сетевым адресом (открытым – интернет-страница (интернет-сайт) или закрытым – мобильное приложение) и обеспечивают возможность получения и передачи соответствующих сведений исходя из целевой установки информационного ресурса. Оригинальные информационные ресурсы информационно-телекоммуникационных сетей, обеспечивающие:

- сбор и хранение персональных данных (например, персональные страницы пользователей в социальных сетях);

- проведение финансовых, торговых либо иных операций (веб-клиент-менеджеры банков (интернет-банкинг), онлайн-гипермаркеты, маркетплейс, торговые интернет-сервисы);

- дистанционного подтверждения права либо освобождения от обязанностей (сайты и мобильные приложения органов публичной власти (сайт или мобильное приложение «Госуслуги»)).

Все чаще они становятся предметом противоправной имитации в информационно-телекоммуникационных сетях.

Имитация оригинального информационного ресурса информационно-телекоммуникационной сети графически, визуально (дизайнерски) в полной мере соответствует оригинальному информационному ресурсу информационно-телекоммуникационной сети, в нем присутствуют аналогичные изображения, вкладки, однако, имитация создается с целью противоправного получения информации от пользователя либо для передачи

информации не соответствующей действительности. Вместе с тем, имитатор оригинала информационного ресурса информационно-телекоммуникационной сети всегда будет иметь другое доменное имя и IP-адрес.

Оригинальные информационные ресурсы, как уже отмечалось выше, обладают определенным веб-дизайном и соответствующим доменным именем (символьным именем, например, https://www.avito.ru), а также, сетевым адресом (IP-адрес сайта, интернет-адресом, например, https://146.158.48.24 – по состоянию на 18 января 2022 года один из IP-адресов сайта «Авито»). Доменное имя информационного ресурса воспринимается пользователем как совокупность относительно легко читаемых и воспринимаемых; и что главное - свободно воспроизводимых символов, например «mail.ru» или «лдпр.рф» в отличии от сетевого адреса интернет-ресурса, который сложно запомнить и в последующим сложно воспроизвести по памяти.

В специальной литературе отмечается: « … Система DNS (англ. Domain Name System) становится все более уязвимой. Злоумышленники без труда перенаправляют запросы пользователей по символьному имени на подставные серверы и, таким образом, получают доступ к паролям, номерам кредитных карт и другой конфиденциальной информации. Сами пользователи ничего не могут с этим поделать, так как, в большинстве случаев, даже не подозревают о том, что запрос был перенаправлен – запись в строке браузера и сам сайт в точности такие, какими их и ожидает увидеть пользователь» [8].

Указанное обстоятельство свидетельствует о том, что существует техническая возможность перевести пользователя с оригинального информационного ресурса с доменным именем на фейковый информационный ресурс, в котором указан ложный сетевой адрес. Не вдаваясь в технические подробности, отметим, что многие оригинальные информационные ресурсы, обозначенные символьным именем, а также, веб-браузеры имеют программную защиту, направленную на минимизацию возможных атак, путем подлога (подмены) IP-адреса при разрешении доменных имен. Такого рода защита не дает возможность перенаправлять запросы пользователей по доменному имени на подставные серверы с сетевым адресом, а сам пользователь предупреждается о возможной ложной маршрутизации с целью противоправного завладения личной информацией пользователя. Таким образом, нивелируется возможность противоправного доступа к информации, охраняемой законом (пароли, персональные данные, номера банковских карт иная конфиденциальная информация).

Как нам представляется, создание специальной программы, которая блокирует работу оригинального информационного ресурса и меняет маршрут пользователя, выводя его на имитацию (фейк) оригинального информационного ресурса полностью охватывается составом преступления, предусмотренного ст. 273 УК РФ. С технической точки зрения вышеописанный способ совершения преступления возможен, но он сложен в

силу наличия программных и аппаратных средств защиты оригинальных информационных ресурсов.

Отметим, что существенное распространение, создание и использование имитаций информационных ресурсов информационно-телекоммуникационных сетей, в том числе, сети «Интернет» получили после вынужденного введения ограничений посещения объектов социальной инфраструктуры (непродовольственные магазины, транспорт, кинотеатры, театры и иные) с целью предупреждения распространения новой коронавирусной инфекции на территории Российской Федерации (COVID-19). После вынужденного введения ограничений, посещение объектов социальной инфраструктуры возможно только при предъявлении документа (сертификата), подтверждающего факт вакцинации от COVID-19 или факт перенесенного коронавирусного заболевания, либо QR-кода, который обеспечивает доступ к сведениям, подтверждающим вышеуказанные факты, посредствам гиперссылки на информационные ресурсы «immune.mos.ru» или «gosuslugi.ru». Однако QR-код, предъявляемый уполномоченным лицам, документом не является в силу того, что «QR-код для доступа в общественные места Москвы содержит только ссылку на сайт immune.mos.ru или gosuslugi.ru, что не позволяет считать его официальным электронным документом. Соответственно, ни создание, ни использование фейкового QR-кода не должно повлечь ответственность по ст. 327 УК» [9], так как не содержит сведения, позволяющие идентифицировать личность. Приведенное обстоятельство свидетельствует об отсутствии уголовно-правового механизма охраны общественных отношений, связанных с генерацией и использованием QR-кодов в сфере здоровья населения (санитарно-эпидемиологического благополучия населения). Существующие информационные технологии, их широкая распространенность и доступность дают возможность лицам, обладающим определенными знаниями, опытом и навыками в сфере IT-технологий, создавать информационные ресурсы имитаторы визуально и содержательно похожими на информационный ресурс ЕСИА «Госуслуги» https://www.gosuslugi.ru/covid-cert/status/********** и размещать их в информационно-телекоммуникационной сети «Интернет», привязывать к имитатору QR-код, который якобы подтверждает факт вакцинации от COVID-19 или факт перенесенного коронавирусного заболевания [10].

Также, отметим, что в правоприменительной практике известны случаи создания имитатора информационного ресурса фискального органа, когда от имени органа публичной власти (ГИБДД МВД России, судебных приставов, налоговых органов) на электронную почту пользователя приходит уведомление о якобы возникшей задолженности, которую можно оплатить (погасить), перейдя по гиперссылке, размещенной в письме. Перейдя по гиперссылке, потерпевший попадает на имитатор информационного ресурса «Госуслуги», либо фискального органа публичной власти на котором предлагается погасить имеющуюся задолженность.

Негативный потенциал и кумулятивный (мультипликативный) эффект общественной опасности создания имитатора информационного ресурса, о котором говорилось ранее, может также выражаться в воспрепятствовании осуществлению избирательных прав или работе избирательных комиссий. Возможности информационно-телекоммуникационной сетей, в том числе, сети «Интернет» при организации и проведении голосования неоднократно использовались Центральной избирательной комиссии России (далее – ЦИК России). Голосование на выборах депутатов Государственной Думы Российской Федерации 17-19 сентября 2021 года прошли с использованием дистанционного электронного голосования (онлайн-голосования). Согласно данных ЦИК России, онлайн-голосование проводилось с 08:00 17 сентября до 20:00 19 сентября 2021 года, дистанционное электронное голосование прошло без нарушений [11].

Создание имитатора информационного ресурса ЦИК России, иной избирательной комиссии может быть осуществлено с целью повлиять на итоги официального голосования путем срыва проведения такого рода голосования либо устранения нежелательных избирателей посредством направления последним гиперссылок о возможности волеизъявления с использованием дистанционного электронного голосования (онлайн-голосования). Гиперссылка может прийти на электронную почту избирателя либо в персональный кабинет гражданина-пользователя информационного ресурса «Госуслуги».

Литература:

1. Криминология цифрового мира: учебник для магистратуры / В.С. Овчинский. – М.: Норма: ИНФРА-М, 2018. – 352 с., с. 22.

2. Пудовочкин Ю.Е. Закономерности формирования и развития российской уголовной политики в условиях глобализации // Журнал российского права. – 2017. – № 3 (243). – С. 82-91.

3. Игнатов А.Н. Криминогенность техногенности // Общество и право. – 2019. – № 2. – С. 34-40.

4. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы. Указ Президента Российской Федерации от 9 мая 2017 г. № 203. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102431687

5. Овчинский В.С. Преступность и борьба с ней в цифровом мире // Проектирование будущего. Проблемы цифровой реальности: труды 1-й Международной конференции (8-9 февраля 2018 г., Москва). – М.: ИПМ им. М.В.Келдыша, 2018. – С. 136-140. – URL: http://keldysh.ru/future/2018/20.pdf doi:10.20948/future-2018-20

6. Антонов А.Г., Крюков Д.В. К вопросу об общественной опасности неправомерного доступа к компьютерной информации, повлекшего ее блокирование // Ленинградский юридический журнал. – 2021. – № 2(64). – С. 168–179. DOI 10.35231/18136230_2021_2_168

7. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. – М.: Мир, 1999. – 351 с., с. 60.

8. Domain Name System Security Extensions https://www.securitylab.ru/news/tags/DNSSEC/

9. Предъявите документы: риски уголовной ответственности за подделку QR-кода // https://300.pravo.ru/opinion/233146/

10. Вишневецкий К.В., Кашкаров А.А., Кашкаров А.А. О необходимости обеспечения уголовно-правовой охраны генерации, использования и оборота QR-кодов в сфере безопасности и обеспечения благополучия населения // Гуманитарные, социально-экономические и общественные науки. 2022. № 1.С. 90-95.

11. В Российской Федерации завершилось голосование на выборах депутатов Государственной Думы. // http://www.cikrf.ru/news/cec/50559/

Literature:

1. Criminology of the digital world: a textbook for magistracy / V.S. Ovchinsky. - M.: Norma: INFRA-M, 2018. - 352 p.

2. Pudovochkin Yu.E. Patterns of Formation and Development of Russian Criminal Policy in the Context of Globalization // Journal of Russian Law. - 2017. - No. 3 (243). – P. 82-91.

3. Ignatov A.N. Criminogenicity of technogenicity // Society and Law. - 2019. - No. 2. - P. 34-40.

4. Strategy for the development of the information society in the Russian Federation for 2017-2030. Decree of the President of the Russian Federation of May 9, 2017 No. 203. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102431687

5. Ovchinsky V.S. Crime and fight against it in the digital world // Designing the future. Problems of Digital Reality: Proceedings of the 1st International Conference (February 8-9, 2018, Moscow). – M.: IPM im. M.V. Keldysh, 2018. - S. 136-140. – URL: http://keldysh.ru/future/2018/20.pdf doi:10.20948/future-2018-20

6. Antonov A.G., Kryukov D.V. To the question of the public danger of illegal access to computer information, resulting in its blocking // Leningradsky juridical journal. - 2021. - No. 2 (64). – S. 168–179. DOI 10.35231/18136230_2021_2_168

7. Aikov D., Seiger K., Fonstorkh U. Computer crimes. Guide to Combating Computer Crimes. - M.: Mir, 1999. - 351 p.

8. Domain Name System Security Extensions https://www.securitylab.ru/news/tags/DNSSEC/

9. Present documents: risks of criminal liability for forging a QR code // https://300.pravo.ru/opinion/233146/

10. Vishnevetsky K.V., Kashkarov A.A., Kashkarov A.A. On the need to ensure criminal law protection of the generation, use and circulation of QR codes in the field of security and ensuring the well-being of the population // Humanitarian, socio-economic and social sciences. 2022. №. 1.P. 90-95.

11. Voting in the elections of deputies of the State Duma has ended in the Russian Federation. // http://www.cikrf.ru/news/cec/50559/