ЦИФРОВИЗАЦИЯ И НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

https://doi.org/10.33874/2072-9936-2022-0-1-44-49

В статье рассматриваются актуальные вопросы национальной и информационной безопасности в век всеобщей цифровизации. Актуальность работы состоит в том, что за последние годы постоянно растет значимость информационного обмена во всех сферах человеческой деятельности, и нет сомнения, что тенденция цифровизации в ближайшие годы сохранится и даже усилится. Предметом проведенного исследования являются общественные отношения, сложившиеся в процессе цифровизации большинства сфер деятельности общества, а также законодательные акты, регулирующие эти отношения. Целью работы является анализ нормативных актов и сложившихся новых общественных отношений в области цифровизации, определение направлений, в которых необходимо проводить научные исследования, и, следовательно, выделение нормативных правовых актов, нуждающихся в совершенствовании. Методологию исследования составили как общие, так и частнонаучные методы познания, используемые в юридической науке. Новизна работы состоит в том, что в представленной статье выделяются проблемы, возникающие в правоприменительной деятельности в связи с использованием при совершении преступлений новых информационных технологий, телекоммуникационных систем и современного программного обеспечения, что повышает общественную опасность такого рода преступлений и на практике усложняет применение к ним мер противодействия. В статье исследованы проблемы цифровизации с учетом принятых за последние годы нормативных правовых актов в сфере национальной безопасности, а также с учетом изменений, произошедших в политической, экономической и социальной жизни общества. Показано значение цифровизации, которая способствует развитию всех сфер человеческой деятельности, но влечет за собой определенные риски, в том числе в сфере безопасности граждан, общества и государства, национальной безопасности. Рассмотрены направления, в которых следует проводить исследования с целью совершенствования уголовного законодательства. Проанализирована нормативная база, обеспечивающая национальную и общественную безопасность, изучены нормы Уголовного кодекса РФ, нуждающиеся во внесении в них изменений для улучшения борьбы с преступлениями, совершаемыми с использованием информационных технологий и информационно-телекоммуникационных сетей, в том числе сети Интернет. Сделаны выводы и предложения по имеющимся пробелам законодательства по выбранной теме. Внесены предложения по совершенствованию уголовного законодательства.

КОРАБЕЛЬНИКОВ
Сергей Маркович

кандидат юридических наук,
доцент, доцент кафедры уголовного права и криминологии
Всероссийского государственного университета юстиции
(РПА Минюста России) (г. Москва)

smkorabelnikov@mail.ru

Преступление;
цифровизация;
ответственность;
уголовное законодательство;
национальная безопасность;
информационная безопасность;
компьютерная информация;
информационно-телекоммуникационные сети;
Интернет

Sergey M. KORABELNIKOV

Candidate of Legal Sciences,
Associate Professor, Department of Criminal Law and Criminology,
All-Russian State University of Justice (Moscow)

smkorabelnikov@mail.ru

DIGITALIZATION AND NATIONAL SECURITY

The article deals with topical issues of national and information security in the age of universal digitalization. The relevance of the work lies in the fact that in recent years the importance of information exchange in all spheres of human activity has been constantly growing and there is no doubt that the digitalization trend will continue and even increase in the coming years. The subject of the study

Crime; digitalization; responsibility; criminal legislation; national security; information security; computer information; information and telecommunications networks; Internet

is the social relations that have developed in the process of digitalization of most areas of society, as well as the legislative acts regulating these relations. The purpose of the work is to analyze the regulations and the existing new social relations in the field of digitalization, definition of directions in which it is necessary to carry out scientific research and, consequently, the allocation of regulatory legal acts that need to be improved. The research methodology consists of both general and particular scientific methods of cognition used in legal science. The novelty lies in the fact that the presented article highlights the problems that arise in law enforcement activities in connection with the use of new information technologies, telecommunications systems and modern software in the commission of crimes, which increases the social danger of such crimes and in practice complicates the application of countermeasures to them. The article examines the problems of digitalization, taking into account the normative legal acts adopted in recent years in the field of national security, as well as taking into account the changes that have occurred in the political, economic and social life of society. The importance of digitalization is shown, which contributes to the development of all spheres of human activity, but entails certain risks, including in the field of security of citizens, society and the state, and national security. The directions in which research should be carried out in order to improve criminal legislation are considered. The regulatory framework that ensures national and public security is analyzed, the norms of the Criminal Code of the Russian Federation are studied, which need to be amended to improve the fight against crimes committed using information technology and information and telecommunication networks, including the Internet. Conclusions and suggestions are made on the existing gaps in the legislation on the chosen topic of the article under consideration. Proposals have been made to improve the criminal legislation.

Жизнь современного общества трудно представить без цифровой составляющей. Возникновение повышенного научного интереса к цифровизации обусловлено в том числе принятием целого ряда нормативных правовых актов, регулирующих отношения в сфере социально-экономического развития и обеспечивающих национальную безопасность в информационном пространстве. Цифровизация – это бесспорное благо, но она также влечет за собой определенные риски и угрозы. Задача государства – их снимать и обеспечивать безопасность во всех сферах человеческой деятельности, во всех областях жизни страны.

В соответствии со Стратегией национальной безопасности Российской Федерации, утв. указом Президента РФ от 31 декабря 2015 г. № 683, национальная безопасность РФ – это «состояние защищенности личности, общества и государства от внутренних и внешних угроз, при которой обеспечивается реализация конституционных прав и свобод гражданина Российской Федерации, достойное качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности» [1]. Обеспечивая национальную безопасность, государство обеспечивает жизненно-важные интересы, под которыми следует понимать «совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства» [2, с. 360]. Национальная безопасность в информационной (цифровой) сфере является неотъемлемой составной частью национальной безопасности России. Доктрина информационной безопасности Российской Федерации, утв. указом Президента РФ от 5 декабря 2016 г. № 646 (далее – Доктрина), представляет собой систему официальных взглядов на обеспечение национальной безопасности РФ в информационной сфере. Согласно подп. «в» п. 2 Доктрины информационная безопасность – «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечивается реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской

Федерации, оборона и безопасность государства» [3]. В Доктрине определены национальные интересы в информационной сфере, ими являются:

– обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получение и использования информации, неприкосновенности частной жизни;

– обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры;

– развитие отрасли информационных технологий и электронной промышленности;

– содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на защиту суверенитета РФ в информационном пространстве [3].

К сферам обеспечения информационной безопасности относятся:

– интересы личности в части реализации конституционных прав, включая право на доступ к информации, защиту личного пространства, чести и достоинства человека;

– интересы общества, состоящие в развитии демократии, создании и функционировании общественных институтов, духовном развитии общества, а также в формировании и поддержании общественного согласия;

– интересы государства в политической, экономической, военной, международной сферах деятельности, обеспечении суверенитета, территориальной целостности, общественного порядка и социальной стабильности.

В соответствии с постановлением Правительства РФ от 15 апреля 2014 г. № 313 (в ред. от 18 декабря 2021 г.) «Об утверждении государственной программы Российской Федерации «Информационное общество»» приоритеты государственной программы Российской Федерации «Информационное общество»» (далее – Программа) определены указами Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», от 1 декабря 2016 г. № 642 «О Стратегии научно-технологического развития Российской Федерации»; этими и другими документами сформулированы основные направления развития информационного общества в РФ, которыми являются повышение благосостояния, качества жизни и работы граждан, улучшение доступности и качества государственных услуг, повышение степени информированности и цифровой грамотности, развитие экономического потенциала страны с использованием современных информационных, телекоммуникационных и цифровых технологий.

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, утв. указом Президента РФ от 9 мая 2017 г. № 203, задает цели, задачи и меры по осуществлению внутренней и внешней политики РФ в сфере применения информационных и коммуникационных технологий, направленные на совершенствование информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

Информационная безопасность обеспечивается по средствам использования организационных и технических (технологических) и правовых мер.

Защите информации посвящена ст. 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации». В ней, в частности, говорится о том, что защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

– обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования информации;

– соблюдение конфиденциальности информации;

– реализацию права на доступ к информации.

Организационные меры обеспечения информационной безопасности состоят в:

– создании системы обеспечения информационной безопасности в РФ;

– осуществлении правоприменительной деятельности органов государственной власти, направленной на предупреждение и пресечение правонарушений в информационной сфере, а также выявление и привлечение к уголовной ответственности лиц, совершивших указные правонарушения.

Технические меры представляют собой:

– разработку и совершенствование средств и иных мер защиты информации и методов контроля, развитие телекоммуникационных систем и современного программного обеспечения;

– выявление систем, технических устройств, программ, представляющих опасность вмешательства в деятельность защищенных информационных систем;

– создание систем для предотвращения несанкционированного доступа к информации, а также иных технических систем, обеспечивающих информационную безопасность человека, общество и государство.

К числу *правовых мер* относятся: создание нормативной базы в информационной сфере, которая была бы способна регулировать информационные отношения и устанавливать все виды ответственности за нарушение законодательства в сфере распространения и защиты информации в соответствии с положением ч. 4 ст. 29 Конституции РФ, гарантирующей каждому право свободно искать, получать, передавать,

производить и распространять информацию любым законным способом. Эти права также находятся под защитой закона.

В систему ответственности за правонарушения в информационной сфере входят все четыре вида ответственности: дисциплинарная, административная, гражданско-правовая и уголовная. На последней из них мы остановимся более подробно.

Бурное развитие цифровых технологий в последние годы, бесспорно, оказывает влияние на состоянии правового регулирования и на правоприменительную практику. Развитие современных информационных технологий влияет на правовые инструменты в сфере гражданского, уголовного, информационного и других отраслей права. Рассмотрим некоторые уголовно-правовые проблемы, связанные с цифровизацией и представляющие научный интерес.

Высказывалось мнение, что России следует принять нормативные стандарты в сфере цифровизации, чтобы управлять процессом перемен [4, с. 25]. Не очень понятно, о каких стандартах идет речь, но принятие конкретных нормативных актов для упорядочения деятельности в цифровой сфере представляется нам необходимым.

Следует обратить внимание на влияние цифровизации на изменение (совершенствование) уголовного закона и применение уголовно-правовых норм. Обратимся к тем из них, которые совершаются посредством компьютеров, компьютерных систем с использованием соответствующих сетей. Такое деяние может рассматриваться как виновное противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также как иные противоправные общественно опасные действия, совершенные при помощи или посредством компьютеров, компьютерных сетей и программ [5, с. 102].

В системе обеспечения национальной безопасности следует проводить активную, наступательную работу на опережение в отношении возникновения возможных негативных процессов в сфере информационной безопасности. Полагаем, что некоторые нормы Уголовного кодекса РФ (далее – УК РФ) нуждаются в дальнейшем совершенствовании. Это относится в первую очередь к статьям разд. IV о преступлениях против общественной безопасности и общественного порядка, предусматривающим ответственность за преступления террористической направленности, массовые беспорядки, деяния, совершаемые в сфере оборота оружия и оборота наркотических средств, и некоторые другие. Следует согласиться с позицией Н. А. Голованової, А. А. Гравиной, О. А. Зайцева о необходимости дополнения статей о преступлениях террористической направленности квалифицирующим признаком об использовании для совершения преступлений информационно-телекоммуникационных сетей [5, с. 108]. В частности, необходимо внести изменение в ст. 205 УК РФ, дополнив ч. 2 пунктом следующего содержания: «г) совершенные с использованием компьютерных программ, компьютерной информации, информационно-телекоммуникационных сетей, в том числе сети «Интернет», посягающих на критическую информационную инфраструктуру Российской Федерации».

Статью 205-1 УК РФ о содействии террористической деятельности в части склонения, вербовки и иного вовлечения в совершение преступлений террористической направленности, а также совершение некоторых преступлений против основ конституционного строя и безопасности государства следует дополнить ч. 1.2 следующего содержания: «деяния, предусмотренные частью первой или частью первой.1, совершенные с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»».

Практика последних лет показала, что при организации и проведении массовых беспорядков широко используется сеть Интернет, посредством которой осуществляется руководство лицами, участвующими в массовых беспорядках, в результате чего осложняются действия правоохранительных органов по наведению порядка и ликвидации массовых беспорядков. Недавние события начала января 2022 г. в г. Алматы Республики Казахстан показали, какой ущерб безопасности гражданам и государству могут нанести хорошо организованные, в том числе руководимые посредством сети Интернет, массовые беспорядки. В связи с этим полагаем необходимым ст. 212 УК РФ дополнить ч. 1.2 следующего содержания: «деяния, предусмотренные частью первой или частями первой и первой.1, совершенные с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»».

Считаем необходимым также рассмотреть вопрос о специальной ответственности за взлом сайтов государственных органов. Ответственность за такое преступление должна быть включена в главу о преступлениях против конституционного строя и безопасности государства. Отсюда вытекает еще один важный вопрос: в большинстве случаев хакеры все-таки выполняют «свою работу» по заказу, поэтому важно установить самостоятельную ответственность заказчиков (организаторов) преступления по типу ст. 210 УК РФ.

В главе, посвященной преступлениям против конституционного строя и безопасности государства, также необходимо внести изменения в ст. 282-1 об организации экстремистского сообщества и в ст. 282-2 об организации деятельности экстремисткой организации, дополнив нормы о склонении, вербовке или

иного вовлечения лица в деятельность экстремистского сообщества или экстремистской организации соответственно ч. 1.2 следующего содержания: «деяния, предусмотренные частью первой.1, совершенные с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»».

В условиях проникновения информационных технологий в разные сферы жизнедеятельности общества и продолжающейся цифровизации в уголовное законодательство за последние годы уже внесен ряд изменений. Этот процесс идет и, будем надеяться, продолжится в будущем. Можно не сомневаться, что необходимость внесения соответствующих изменений будет отражаться в законодательной практике.

Так, Федеральным законом от 1 марта 2012 г. № 18-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» внесено изменение в п. «б» ч. 2 ст. 228.1 УК РФ и была установлена ответственность за сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием электронных или информационно-телекоммуникационных сетей (включая сеть Интернет).

Целесообразно было бы аналогичные изменения внести в ст. 228.4, 234 и 234.1 УК РФ, также предусматривающие ответственность за сбыт прекурсоров наркотических средств или психотропных веществ, сильнодействующих или ядовитых веществ, не являющихся наркотическими средствами или психотропными веществами, либо оборудования для их изготовления или переработки, новых потенциально опасных психоактивных веществ. Вероятно, подобные нормы в перспективе необходимо будет включать и в статьи других глав Особенной части УК РФ.

Были внесены и другие изменения в УК РФ, связанные с происходящим процессом цифровизации. Можно упомянуть п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110.1, ч. 2 ст. 110.2, ч. 3 ст. 141, ст. 159.6 УК РФ и др. Чем больше появляется в УК РФ составов преступлений, совершаемых посредством использования информационно-телекоммуникационных сетей (включая сеть Интернет), тем острее становится вопрос о конкуренции этих норм со статьями гл. 28, содержащей поступления в сфере компьютерной информации. Если применительно к ст. 272 (неправомерный доступ к компьютерной информации) вопрос конкуренции решается в рамках правил конкуренции общей и специальной норм, то неправомерное воздействие на критическую информационную структуру РФ может являться средством совершения другого преступления, например террористического акта (ст. 205 УК РФ), государственной измены (ст. 275 УК РФ), шпионажа (ст. 276 УК РФ), насильственного захвата власти (ст. 278 УК РФ), вооруженного мятежа (ст. 279 УК). Очевидно, что перечисленные статьи, за исключением ст. 205 УК РФ, не могут содержать квалифицирующие признаки, связанные с использованием информационно-телекоммуникационных сетей (включая сеть Интернет), поскольку санкции этих статей предусматривают максимальное наказание в виде лишения свободы. В указанной ситуации перечисленные преступления должны квалифицироваться по совокупности со ст. 274.1 УК РФ о неправомерном воздействии на критическую информационную структуру РФ. В этом случае посягательство осуществляется в первую очередь на безопасность государства и основным объектом посягательства выступает государственная и национальная безопасность.

В юридической литературе уже высказывалось мнение, что, возможно, не во всех случаях целесообразно включать в статьи УК РФ в качестве квалифицирующего признака использование информационно-телекоммуникационных сетей (включая сеть Интернет) как средство совершение преступления, но в качестве отягчающего наказание обстоятельства в ст. 63 УК РФ его следует включить [5, с. 121].

В заключение необходимо констатировать, что в обеспечение национальной информационной безопасности с учетом существующих реалий цифровизации, а также возможных внутренних и внешних угроз у уголовно-правовых средств имеется определенный потенциал в системе комплекса государственных мер, которые необходимо будет реализовывать в процессе дальнейшего развития цифровизации.

Пристатейный библиографический список

1. Стратегия национальной безопасности Российской Федерации, утв. указом Президента РФ от 31 декабря 2015 г. № 683 // СЗ РФ. 2016. № 1 (ч. 2). Ст. 212.
2. *Рассолов И. М.* Информационное право : учебник для магистров. М. : Юрайт. 2013.
3. Доктрина информационной безопасности Российской Федерации, утв. указом Президента РФ от 5 декабря 2016 г. № 646 // СЗ РФ. 2016. № 50. Ст. 7074.
4. *Трунцевский Ю. В.* О проблемах правового регулирования взаимоотношений государства и бизнеса // Юридический мир. 2011. № 4.
5. Уголовно-юрисдикционная деятельность в условиях цифровизации : монография. М. : ИЗиСП ; КОНТРАКТ, 2019.

References

1. National Security Strategy of the Russian Federation, approved by the Decree of the President of the Russian Federation of 31 December 2015 No. 683. *Collection of the Legislation of the Russian Federation*. 2016. No. 1 (part 2). Art. 212.
2. *Rassolov I. M.* Information Law: Textbook for Masters. Moscow: Iurait, 2013.
3. Doctrine of Information Security of the Russian Federation, approved by the Decree of the President of the Russian Federation of 5 December 2016 No. 646. *Collection of the Legislation of the Russian Federation*. 2016. No. 50. Art. 7074.
4. *Truntsevskii Iu. V.* Problems of Legal Regulation of Relations Between the State and Business. *Legal World*. 2011. No. 4.
5. Criminal Jurisdictional Activity in the Conditions of Digitalization: Monograph. Moscow: Institute of Legislation and Comparative Law under the Government of the Russian Federation; Kontrakt, 2019.