Актуальные проблемы экономики и права. 2019. Т. 13, № 4
Actual Problems of Economics and Law, 2019, vol. 13, No. 4

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

УДК 343.3/.7:004(049.32) **DOI: http://dx.doi.org/10.21202/1993-047X.13.2019.4.1732-1743**

Т. М. ЛОПАТИНА[1]

[1] *Смоленский государственный университет, г. Смоленск, Россия*

РЕЦЕНЗИЯ

на монографию «Бегишев И. Р., Бикеев И. И. Преступления в сфере обращения цифровой информации. Казань: Изд-во „Познание“ Казанского инновационного университета, 2020, 300 с.»

Лопатина Татьяна Михайловна, доктор юридических наук, заведующий кафедрой уголовного права и уголовного процесса факультета истории и права, Смоленский государственный университет (СмолГУ)
Адрес: г. Смоленск, ул. Пржевальского, 4, тел.: +7 (4812) 38-31-57
E-mail: rectorat@smolgu.ru

Цель: проведение всестороннего комплексного анализа монографии И. Р. Бегишева и И. И. Бикеева, которая посвящена исследованию такого сложного и быстро развивающегося института уголовного права, как преступления в сфере обращения цифровой информации.
Методы: диалектический подход к познанию социальных явлений в их развитии и взаимном влиянии, который определил выбор следующих правовых методов исследования: формально-юридический, сравнительно-правовой и др.
Результаты: произведена оценка основных подходов, изложенных в рецензируемой монографии, касающихся юридической природы преступлений и иных общественно опасных деяний в сфере обращения цифровой информации, а также ответственности за их совершение.
Научная новизна: впервые дана оценка уголовно-правовой природы преступлений в сфере обращения цифровой информации; внесены предложения, направленные на совершенствование российского законодательства в сфере регулирования общественных отношений, складывающихся по поводу уголовно-правовой регламентации преступлений и иных общественно опасных деяний в сфере обращения цифровой информации. Сделан вывод о существенном вкладе монографии И. Р. Бегишева, И. И. Бикеева в развитие «цифровых» основ теории уголовного права.
Практическая значимость: рецензентом сделан вывод о том, что монографическое исследование И. Р. Бегишева и И. И. Бикеева может использоваться научными работниками, преподавателями юридических вузов, практикующими юристами, представителями судебной системы, правоохранительных органов, студентами, магистрантами и аспирантами.

Ключевые слова: рецензия; преступления в сфере обращения цифровой информации; противодействие преступлениям в сфере компьютерной информации; безопасность критической информационной инфраструктуры; цифровая информация; цифровые технологии; цифровая инфраструктура; цифровая экономика; преступления; уголовное право и криминология; компьютерные преступления

Конфликт интересов: автором не заявлен.

Как цитировать статью: Лопатина Т. М. Рецензия на монографию «Бегишев И. Р., Бикеев И. И. Преступления в сфере обращения цифровой информации. Казань: Изд-во „Познание“ Казанского инновационного университета, 2020, 300 с.» // Актуальные проблемы экономики и права. 2019. Т. 13, № 4. С. 1732–1743. DOI: http://dx.doi.org/10.21202/1993-047X.13.2019.4.1732-1743

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

T. M. LOPATINA[1]

[1] *Smolensk State University, Smolensk, Russia*

REVIEW

of the monograph "Begishev I. R., Bikeev I. I. Crimes in the sphere of digital information circulation. Kazan: Poznaniye Publishers of Kazan Innovative University, 2020, 300 p."

Tatyana M. Lopatina, Doctor of Law, Head of the Department of Criminal Law and criminal Procedure of the Faculty of History and Law,
Smolensk State University
Address: 4 Przhevalskogo Str., Smolensk, tel.: +7 (4812) 38-31-57
E-mail: rectorat@smolgu.ru

Objective: to assess the completeness and quality of the dissertation research carried out by I. A. Efremova on "Institute of exemption from punishment in the theory of criminal law, legislative and judicial practice".
Methods: dialectical approach to cognition of social phenomena, allowing to analyze them in their historical development and functioning, which contributed to applying the following research methods: logical, formal-legal, system, analytical, comparative-legal, sociological.
Results: the theoretical model of convicts release from criminal punishment formed by the author is analyzed; the assessment is given of the regularities, tendencies and dependences established by the applicant, and of the new knowledge on the institute of release from criminal punishment and its norms.
Scientific novelty: the advantages and disadvantages of the dissertation research are revealed; it is established that the dissertation research is an independent, complete scientific and qualification work, representing an advance in science and making a significant contribution to the development of the criminal policy of the state, including the doctrine of exemption from punishment.
Practical significance: the main provisions and conclusions set out in the review can be used in scientific, pedagogical, law-making, and law-enforcement activities when considering the application and improvement of the institution of exemption of convicts from criminal punishment.

Keywords: Review; Crimes in the sphere of digital information circulation; Counteraction to crimes in the sphere of computer information; Security of critical information infrastructure; Digital information; Digital technologies; Digital infrastructure; Digital economy; Crimes; Criminal law, criminology; Cybercrimes

Conflict of Interest: No conflict of interest is declared by the author.

For citation: Lopatina T. M. Review of the monograph "Begishev I. R., Bikeev I. I. Crimes in the sphere of digital information circulation. Kazan: Poznaniye Publishers of Kazan Innovative University, 2020, 300 p.", *Actual Problems of Economics and Law*, 2019, Vol. 13, No. 4, pp. 1732–1743 (in Russ.). DOI: http://dx.doi.org/10.21202/1993-047X.13.2019.4.1732-1743

Цифровая преступность в течение последних десятилетий превратилась в одну из главных мировых угроз безопасности, что требует пристального внимания к вопросам эффективного противодействия преступлениям в сфере обращения цифровой информации. Монография «Преступления в сфере обращения цифровой информации», подготовленная специалистами Казанского инновационного университета имени В. Г. Тимирясова (ИЭУП) И. Р. Бегишевым и И. И. Бикеевым, расширяет область современной российской науки уголовного права, которая посвящена изучению преступлений в сфере обращения информации [1–47].

В монографии рассмотрены теоретические и прикладные аспекты установления уголовно-правовой природы преступлений в сфере обращения цифровой информации, выработаны обоснованные предложения по совершенствованию и повышению эффективности уголовного законодательства об ответственности за отдельные виды таких деяний и практики их примене-

АПЭП
Актуальные проблемы экономики и права. 2019. Т. 13, № 4
Actual Problems of Economics and Law, 2019, vol. 13, No. 4
ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

ния. Несомненной заслугой авторов монографии является заложенный в ней многоаспектный подход к познанию рассматриваемых видов преступлений в сфере обращения цифровой информации. Внесение научно обоснованных предложений по совершенствованию этого направления деятельности обусловлено потребностью теории и практики в дальнейшем научном поиске наиболее удачных решений в противодействии преступлениям в сфере обращения цифровой информации и является не только важным направлением научной деятельности, но и практически значимым для правоохранительной деятельности.

Научная и практическая значимость результатов любого исследования определяется в том числе массивом проанализированных источников. В данном случае это Конституция Российской Федерации, международные правовые акты, уголовное законодательство зарубежных стран, Уголовный кодекс Российской Федерации (далее – УК РФ), федеральные законы, акты Президента и Правительства Российской Федерации, постановления Конституционного Суда Российской Федерации, постановления Пленума Верховного Суда Российской Федерации, другие отечественные и зарубежные правовые акты.

Несомненным достоинством монографии является широкая эмпирическая база исследования, включающая различные материалы за период с 2010 по 2018 гг.:

– данные опубликованной судебной практики судов общей юрисдикции Российской Федерации по уголовным делам о преступлениях, предусмотренных гл. 28 УК РФ;

– статистические данные МВД России о количестве зарегистрированных преступлений в сфере компьютерной информации в Российской Федерации;

– экспертно-аналитические отчеты российских и зарубежных компаний, специализирующихся на обеспечении информационной безопасности и защиты информации (Positive Technologies, Symantec, Digital Security, InfoWatch, Group-IB, Trustwave, G Data Software, Anti-Malware и др.);

– аналитические материалы ведущих антивирусных компаний (Лаборатория Касперского, Dr.Web, McAfee, Microsoft, Avast, ESET и др.);

– результаты анкетирования 175 респондентов: сотрудников соответствующих профилю монографии подразделений Министерства внутренних дел Российской Федерации, Следственного комитета Российской Федерации, Федеральной службы безопасности Российской Федерации и Федеральной службы охраны Российской Федерации; преподавателей юридических факультетов и вузов; ученых, исследующих различные вопросы обеспечения информационной безопасности; работников организаций, занимающихся практической реализацией мер по защите информации.

Все сказанное выше позволяет говорить о высокой актуальности монографического исследования И. Р. Бегишева и И. И. Бикеева, которое направлено, прежде всего, на совершенствование правового регулирования цифровизации общественных отношений.

Остановимся на структуре рецензируемой монографии и описании основных ее частей. Монография состоит из введения, трех глав, заключения, списка литературы и приложений.

Введение посвящено обоснованию актуальности исследования, значимости нормативного регулирования ответственности за преступления в сфере цифровой информации как неотъемлемой составной части системы цифровизации общественных отношений в сферах экономической и социальной жизни общества.

В первой главе монографии, именуемой «Уголовно-правовая природа преступлений в сфере обращения цифровой информации», рассматриваются актуальные аспекты уголовно-правовой природы исследуемого феномена; раскрывается содержание понятия «цифровая информация», которое рассматривается с трех позиций: филологической, технической и юридической. Значительное внимание уделено соотношению понятий «цифровая информация», «компьютерная информация» и «электронная информация». Понятие «цифровая информация» определяется в качестве родового понятия по отношению к понятиям «компьютерная информация» и «электронная информация».

Многие суждения авторов, изложенные в монографии, заслуживают одобрения и поддержки. Так, авторы, верно утверждают, что компьютерная информация является лишь подвидом цифровой информации, поэтому в действующем уголовном законодательстве следует использовать более широкий по содержанию термин «цифровая информация». Авторы обозначили свое отношение к понятию цифровой информации, под которой понимают сведения (сообщения, данные), обращающиеся в информационно-телекоммуникационных устройствах, их системах и сетях.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

Ретроспективный анализ имеющихся в юридической науке подходов к определению понятия «преступление в сфере обращения цифровой информации», а также его соотношение с такими понятиями, как «преступление в сфере информационных технологий», «преступление в сфере высоких технологий», «компьютерное преступление», «киберпреступление», позволил авторам сформулировать блок преступлений, относящихся, по их мнению, к преступлениям в сфере обращения цифровой информации: это деяния, предусмотренные ст. 138.1, 159.6, 272, 273, 274 и 274.1 УК РФ.

Исследовав специфику рассматриваемых преступлений, авторы приходят к выводу, что под преступлением в сфере обращения цифровой информации предлагается понимать предусмотренное уголовным законом виновно совершенное общественно опасное деяние, направленное на нарушение конфиденциальности, целостности, достоверности и доступности охраняемой законом цифровой информации.

Исследование специфики противодействия преступлениям в сфере обращения цифровой информации позволило авторам предложить современный способ предупреждения данного вида преступлений посредством введения механизма внесудебного ограничения доступа на территории Российской Федерации к интернет-ресурсам, размещающим информацию о формах их совершения, а также блокирования объявлений о предоставлении незаконных услуг в этой сфере.

Особый интерес представляет обоснование необходимости введения в научный оборот термина «феномен безопасной компьютерной атаки». В монографии приводится авторское его определение – «состояние субъектов информационных правоотношений, осознающих опасность нарушения и важность обеспечения безопасности информационной инфраструктуры, но в силу различных причин не обеспечивающих ее, в том числе при проведении в отношении нее компьютерных атак». Авторы раскрывают причины феномена безопасной компьютерной атаки, особенности деятельности субъектов информационных правоотношений в условиях защиты информации. Делается вывод о возможности использования термина «феномен безопасной компьютерной атаки» в качестве оценочного индикатора в системе обеспечения информационной безопасности субъектов информационных правоотношений.

Во второй главе монографии, именуемой «Преступления в сфере компьютерной информации по Уголовному кодексу Российской Федерации как виды преступлений в сфере обращения цифровой информации», обосновываются предложения по совершенствованию уголовной ответственности за данный вид преступлений.

Авторы подробно описывают и аргументируют свои предложения по совершенствованию формулировок диспозиций составов преступлений, предусмотренных в ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», в ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», в ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», в ст. 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

Отмечается несоответствие терминологии ст. 272 УК РФ современному состоянию науки и техники, рассматриваются негативные аспекты пробела уголовной ответственности за перехват охраняемой законом цифровой информации. Формулируется вывод об основном отличии перехвата от неправомерного доступа, которое видится авторам в том, что электромагнитному перехвату подвержена цифровая информация, циркулирующая в пространстве, а неправомерный доступ требует нарушения системы защиты информации информационно-телекоммуникационного устройства.

Учитывая, что ст. 272 УК РФ не включает в себя указания на такое противоправное действие, как перехват цифровой информации, предлагается установить за него уголовную ответственность и внести соответствующие изменения в ст. 272 УК РФ, а в примечании к указанной статье сформулировать определение понятия указанного деяния.

Вместе с тем сложность состава преступления, предусмотренного ст. 272 УК РФ, заключается в том, что он носит техногенный характер. Преступление может быть совершено различными качественными и количественными комбинациями общеизвестных основных способов, алгоритм действий которых может со временем усложняться и модернизироваться. Так, еще Ю. М. Батуриным (1991) к методам перехвата

Актуальные проблемы экономики и права. 2019. Т. 13, № 4
Actual Problems of Economics and Law, 2019, vol. 13, No. 4
ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

были отнесены: непосредственный перехват; электромагнитный перехват; аудиоперехват; видеоперехват; «уборка мусора». В. Б. Веховым (1996) к одному из возможных вариантов противоправного доступа к средствам компьютерной техники также был отнесен перехват информации.

Представляется, что указанные авторы допускают излишнюю конкретизацию способов совершения деяния. Следует обратить внимание на подход, содержащийся в Конвенции о киберпреступности 2001 г.[1], в которой не названы возможные способы совершения компьютерных преступлений, а сформирован лишь их перечень: *Illegal access* (неправомерный доступ) и *Illegal interception* (неправомерный перехват).

Подробному изучению подвергнута ст. 273 УК РФ, что позволило авторам выделить возможные направления совершенствования рассматриваемой уголовно-правовой нормы. Выдвигается положение о том, что действия вредоносных компьютерных программ могут нарушить работу средств защиты компьютерной информации. Оспаривается позиция законодателя, который предусмотрел только нейтрализацию средств защиты компьютерной информации. Авторам представляется не совсем уместным использование данного термина, поскольку он не является устоявшимся понятием в русском языке и не имеет единого смыслового значения. Они оправданно считают более удачным решением замену термина «нейтрализация» на термин «нарушение», который широко используется в российском уголовном законе.

Изучение особенностей формулировки бланкетной диспозиции ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» натолкнуло авторов на мысль, что норма отсылает к большому количеству нормативных правовых актов, устанавливающих правила хранения, обработки и передачи компьютерной информации. Законодатель к средствам хранения, обработки или передачи компьютерной информации относит персональные компьютеры и иные информационно-телекоммуникационные устройства, в которых компьютерная информация обращается. Исходя из этого, предлагается обобщить указанные средства хранения, обработки или передачи компьютерной информации и указать вместо них в названии и в диспозиции ст. 274 УК РФ более широкое по содержанию определение: «информационно-телекоммуникационные устройства, их системы и сети». Ввиду уточнения термина, указывающего на объекты обращения цифровой информации, предложена авторская редакция ст. 274 УК РФ.

Рассмотрены проблемы, связанные с выработкой новых государственных подходов к обеспечению безопасности критической информационной инфраструктуры в условиях проведения систематических компьютерных атак на информационные ресурсы. Раскрыто содержание и сущность понятия «безопасность критической информационной инфраструктуры» с учетом положений Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Обосновано, что обеспечение безопасности критической информационной инфраструктуры должно основываться на принципах и методологии обеспечения национальной безопасности. Выработаны предложения по отнесению части субъектов экономической деятельности к субъектам критической информационной инфраструктуры, предложены некоторые дополнительные механизмы повышения защищенности критической информационной инфраструктуры. Доказано, что уголовно-правовая норма об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации требует совершенствования, и предложены его направления.

Не оставлены без внимания проблемы уголовно-правовой регламентации иных преступлений в сфере обращения цифровой информации. В качестве предложений в новую редакцию Уголовного кодекса РФ включены следующие положения:

– установление уголовной ответственности за незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации;

– установление уголовной ответственности за приобретение или сбыт цифровой информации, заведомо добытой преступным путем.

В третьей главе монографии, именуемой «Иные виды преступлений и опасных деяний в сфере об-

[1] URL: https://base.garant.ru/4089723/ (дата обращения: 20.07.2019).

Актуальные проблемы экономики и права. 2019. Т. 13, № 4
Actual Problems of Economics and Law, 2019, vol. 13, No. 4
ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

ращения цифровой информации, нуждающихся в криминализации», исследуются новые высокотехнологичные составы преступлений рассматриваемой тематики, в частности, мошенничество в сфере компьютерной информации и незаконный оборот специальных технических средств, предназначенных для негласного получения информации.

По результатам проведенного анализа авторами предложены пути совершенствования положений уголовного законодательства об ответственности за такие преступления. Авторами доказано, что деяние, предусмотренное ст. 159.6 УК РФ, относится к преступлениям, совершаемым с использованием цифровой информации. Кроме того, установлено, что мошенничество в сфере компьютерной информации может совершаться как с использованием вредоносных компьютерных программ, так и с нарушением систем защиты цифровой информации. В связи с этим авторами предложено озаглавить статью как «Мошенничество с использованием цифровой информации».

С целью дифференциации ответственности за мошенничество в сфере цифровой информации предложено внести в ч. 2 ст. 159.6 УК РФ соответствующее дополнение. Поскольку сеть Интернет содержит информацию о вредоносных компьютерных программах и программных средствах, предназначенных для нарушения систем защиты цифровой информации информационно-телекоммуникационных устройств, их систем и сетей, предложено в порядке предупреждения этих преступлений ввести механизм внесудебного ограничения доступа на территории Российской Федерации к такой информации.

Критический анализ ст. 138.1 УК РФ позволил авторам установить недостаточность учета общественной опасности неправомерного обращения со специальными техническими средствами, используемыми для негласного получения информации. Констатация факта возможного их использования при получении сведений о частной жизни человека (ст. 137 УК РФ), нарушении тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ), нарушении тайны голосования (ст. 141 УК РФ), получении сведений, составляющих коммерческую или банковскую тайну (ст. 183 УК РФ), послужило основанием формулирования предложения об установлении в качестве квалифицирующего признака ответственности за применение таких средств в ч. 2 ст. 137 УК РФ, ч. 2 ст. 138 УК РФ, ч. 2 ст. 141 УК РФ и ч. 3 ст. 183 УК РФ.

Доказана целесообразность установления в ст. 226.1 УК РФ ответственности за контрабанду специальных технических средств, используемых для негласного получения информации, а также специальных технических средств, предназначенных для нарушения систем защиты цифровой информации. Обосновывается и предлагается авторский вариант уголовно-правового ограничения обращения и применения специальных технических средств, предназначенных для нарушения систем защиты цифровой информации.

Исследование неправомерного воздействия на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов позволило обосновать неоправданность применения понятия «кибертерроризм», предлагаются решения по дополнению ст. 272 и 273 УК РФ.

Думается, что разрушение информационной инфраструктуры критически важных и потенциально опасных объектов Российской Федерации путем неправомерного доступа к цифровой информации или внедрения в них вредоносных компьютерных программ может нанести значительный ущерб национальной безопасности, а также привести к экологической катастрофе, человеческим жертвам и иным тяжким последствиям.

Современные информационно-телекоммуникационные устройства, системы и сети в основном хорошо защищены от атак на цифровую информацию, обращающуюся в них, так как находятся под охраной современных средств защиты цифровой информации. Этап проникновения в информационно-телекоммуникационные устройства с целью, например, копирования информации, наступает только после этапа обхода или нарушения системы защиты цифровой информации, предусмотренной в таких устройствах, иначе заполучить цифровую информацию преступнику просто не удастся. Во многих случаях неправомерные деяния с цифровой информацией невозможны без использования специальных технических средств, предназначенных для нарушения систем защиты цифровой информации. Основное назначение таких специальных технических средств – это взлом или

Актуальные проблемы экономики и права. 2019. Т. 13, № 4
Actual Problems of Economics and Law, 2019, vol. 13, No. 4
ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

обход имеющихся средств защиты цифровой информации в информационно-телекоммуникационных устройствах, их системах и сетях.

Поскольку оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации, имеет повышенную опасность, авторами выдвинуто предложение об установлении в качестве квалифицирующего признака применение таких средств в ч. 3 ст. 272 УК РФ и в ч. 2 ст. 273 УК РФ, а также введение в уголовный кодекс самостоятельной уголовно-правовой нормы, предусматривающей ответственность за незаконные производство, приобретение и (или) сбыт специальных технических средств, предназначенных для нарушения систем защиты цифровой информации. Заслуживает внимания предложение авторов о замене в УК РФ вызывающего неоднозначные трактовки термина «специальные технические средства, предназначенные для негласного получения информации» на более точный и недвусмысленный термин «технические средства негласного получения информации».

Исследование вопросов квалификации деяний, связанных с приобретением или сбытом цифровой информации, заведомо добытой преступным путем, позволило авторам предложить способ восполнения пробела в уголовном законодательстве, связанного с отсутствием нормы, которая устанавливала бы ответственность за приобретение или сбыт цифровой информации, заведомо добытой преступным путем.

Информацию обычно не признают имуществом, и поэтому манипуляции с ней не подпадают под признаки ст. 175 «Приобретение или сбыт имущества, заведомо добытого преступным путем» УК РФ, так как в названной норме под имуществом понимается совокупность вещей и материальных ценностей, находящихся во владении или законном пользовании физического или юридического лица.

Думается, что между цифровой информацией и иными вещами материального мира имеется принципиальное различие. Цифровую информацию, по сравнению, например, с драгоценным металлом или ценной бумагой, являющимися материальными ценностями, невозможно потрогать и ощутить, хотя носитель информации (например, флеш-карта), на котором находится цифровая информация, является материальной ценностью. Учитывая, что ст. 175 «Приобретение или сбыт имущества, заведомо добытого преступным путем» УК РФ не содержит указаний на такой предмет, как цифровая информация, авторами предложено дополнить УК РФ ст. 272.1 и установить ответственность за приобретение или сбыт цифровой информации, заведомо добытой преступным путем.

Заключение содержит итоговые выводы авторов о вопросах и проблемах, поднимаемых в рецензируемой монографии, подчеркивается необходимость дальнейшей проработки высказанных на страницах монографии соображений, выводов и предложений.

Несомненным достоинством монографии И. Р. Бегишева и И. И. Бикеева является обоснование единых подходов к правовой регламентации ответственности за преступления в сфере обращения цифровой информации, основанных на использовании проблематики как Общей, так и Особенной частей уголовного права. Исследование базируется на новейших современных достижениях науки и техники, сближает юридические и неюридические отрасли знания, устраняет разрыв между ними. Разработанные авторами теоретические положения и рекомендации прикладного характера имеют значение для унификации ответственности за общественно опасные деяния в сфере обращения цифровой информации.

Завершая рецензию, необходимо подчеркнуть, что монография И. Р. Бегишева и И. И. Бикеева на тему «Преступления в сфере обращения цифровой информации» вносит существенный вклад в развитие российской юридической доктрины о правовом регулировании ответственности за общественно опасные деяния в сфере обращения цифровой информации. Значительная часть выводов авторов монографии направлена на развитие правоприменительной практики по обеспечению безопасного оборота цифровой информации.

Создание электронного государства предполагает использование комплексного подхода к ускорению технологического развития России путем внедрения цифровых технологий в различные сферы общества. Национальная программа «Цифровая экономика Российской Федерации» предусматривает «создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

и домохозяйств»[2]. При этом присутствует необходимость в разработке комплексных научно-прикладных исследований по рассматриваемой проблематике, формирование единой правовой политики и научно-методической базы цифровой трансформации общества с учетом потребностей в формировании продукта цифровой среды. В связи с этим можно заключить, что рецензируемая монография является первым комплексным исследованием преступлений в сфере обращения цифровой информации, теоретически обосновывающим совершенствование механизма противодействия этому негативному явлению.

Рукопись монографии И. Р. Бегишева и И. И. Бикеева является законченным научным трудом, в котором выдвинут, доказан и практически подтвержден ряд научных положений, заслуживающих законодательной поддержки. Подробное и последовательное изложение «цифровых» теоретических основ в теории уголовного права и широкое их использование для анализа общественных отношений позволяют работать с монографией не только специализирующемуся на данной тематике исследователю, но и читателю, ранее недостаточно знакомому с теорией и практикой уголовного права.

Актуальность темы, профессионализм авторов и широкая юридическая база позволяют высоко оценить вклад этой работы в развитие уголовно-правовой науки и регулирование общественных отношений в сфере цифровой информации. Поднятые в монографии проблемы могут быть подвергнуты дальнейшей научной разработке в целях соблюдения интересов личности в условиях функционирования информационного общества.

Список литературы

1. Study of Russia and the UK legislations in combating digital crimes / A. Y. Bokovnya, Z. I. Khisamova, I. R. Begishev // Helix. 2019. Vol. 9, № 5. Pp. 5458–5461. DOI: 10.29042/2019-5458-5461

2. Experience of Civil Government of Russian Federation Subjects with Institutions of Civil Society in the Sphere of Corruption / I. I. Bikeev, S. G. Nikitin, Z. I. Khisamova, I. R. Begishev, A. Y. Bokovnya // International Journal of Innovative Technology and Exploring Engineering. 2019. Vol. 9, № 1. Pp. 5184–5187. DOI: 10.35940/ijitee.A9227.119119

3. Criminological Risks and Legal Aspects of Artificial Intelligence Implementation / I. I. Bikeev, P. A. Kabanov, I. R. Begishev, Z. I. Khisamova // ACM International Conference on Artificial Intelligence, Information Processing and Cloud Computing (AIIPCC2019). 2019. December. Sanya, China.

4. Information infrastructure of safe computer attack / I. R. Begishev, Z. I. Khisamova, G. I. Mazitova // Helix. 2019. Vol. 9, № 5. Pp. 5639–5642. DOI: 10.29042/2019-5639-5642

5. Criminal legal ensuring of security of critical information infrastructure of the Russian Federation / I. R. Begishev, Z. I. Khisamova, G. I. Mazitova // Revista Gênero & Direito. 2019. Vol. 8, № 6. Pp. 283–292.

6. On Methods to Legal Regulation of Artificial Intelligence in the World / Z. I. Khisamova, I. R. Begishev, R. R. Gaifutdinov // International Journal of Innovative Technology and Exploring Engineering. 2019. Vol. 9, № 1. Pp. 5159–5162. DOI: 10.35940/ijitee.A9220.119119

7. Бегишев И. Р. Понятие и виды преступлений в сфере обращения цифровой информации: автореф. дис. … канд. юрид. наук. Казань, 2017. 31 с.

8. Бегишев И. Р. Понятие и виды преступлений в сфере обращения цифровой информации: дис. … канд. юрид. наук. Казань, 2017. 204 с.

9. Бегишев И. Р. Безопасность критической информационной инфраструктуры Российской Федерации // Безопасность бизнеса. 2019. № 1. С. 27–32.

10. Бегишев И. Р. Синдром безопасной атаки: юридико-психологический феномен // Юридическая психология. 2018. № 2. С. 27–30.

[2] О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: Указ Президента РФ от 7 мая 2018 г. № 204 от 7 мая 2018 г., п. «а» ст. 11 (ред. от 19.07.2018) // Собрание законодательства РФ. 14.05.2018. № 20. Ст. 2817.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

11. Бегишев И. Р., Хисамова З. И. Криминологические риски применения искусственного интеллекта // Всероссийский криминологический журнал. 2018. Т. 12, № 6. С. 767–775. DOI: 10.17150/2500-4255.2018.12(6).767-775

12. Хисамова З. И., Бегишев И. Р. Уголовная ответственность и искусственный интеллект: теоретические и прикладные аспекты // Всероссийский криминологический журнал. 2019. Т. 13, № 4. С. 564-574.

13. Хисамова З. И., Бегишев И. Р. Правовое регулирование искусственного интеллекта // Baikal Research Journal. 2019. Т. 10, № 2.

14. Хисамова З. И., Бегишев И. Р. Сравнительно-правовой анализ законодательства Великобритании и России в области противодействия преступлениям в цифровой сфере // Baikal Research Journal. 2019. Т. 10, № 3.

15. Бегишев И. Р. Федеральная служба информационной безопасности Российской Федерации: миф или реальность? // Information Security / Информационная безопасность. 2016. № 6. С. 14–15.

16. Бегишев И. Р. Изготовление, сбыт и приобретение специальных технических средств, предназначенных для нарушения систем защиты цифровой информации: правовой аспект // Информация и безопасность. 2010. № 2. С. 255–258.

17. Бегишев И. Р. Информационное оружие как средство совершения преступлений // Информационное право. 2010. № 4. С. 23–25.

18. Бегишев И. Р. Информационные войны: предупреждение и предотвращение угроз // Защита информации. Inside. 2010. № 4. С. 34–35.

19. Бегишев И. Р. Меры предупреждения преступлений в сфере обращения цифровой информации // Информация и безопасность. 2011. № 3. С. 433–438.

20. Бегишев И. Р. Новое в ответственности за неправомерный доступ к компьютерной информации по Уголовному кодексу Российской Федерации // Правосудие в Татарстане. 2011. № 4. С. 42–44.

21. Бегишев И. Р. Ответственность за нарушение работы информационно-телекоммуникационных устройств, их систем и сетей // Безопасность информационных технологий. 2011. № 1. С. 73–75.

22. Бегишев И. Р. Открытое ПО: вопросы права, безопасности и последствий // Information Security / Информационная безопасность. 2011. № 4. С. 28–29.

23. Бегишев И. Р. Перехват охраняемой законом цифровой информации: уголовно-правовые аспекты // Информационная безопасность регионов. 2011. № 1. С. 78–81.

24. Бегишев И. Р. Правовые аспекты безопасности информационного общества // Информационное общество. 2011. № 4. С. 54–59.

25. Бегишев И. Р. Преступления в сфере обращения цифровой информации. Результаты научного исследования // Information Security / Информационная безопасность. 2012. № 6. С. 8–10.

26. Бегишев И. Р. Преступления в сфере цифровой информации: состояние, пробелы и пути их решения // Информационное право. 2010. № 2. С. 18–21.

27. Бегишев И. Р. Проблемы противодействия преступным посягательствам на информационные системы критически важных и потенциально опасных объектов // Информационная безопасность регионов. 2010. № 1. С. 9–13.

28. Бегишев И. Р. Противодействие утечкам цифровой информации: вопросы уголовной ответственности // Защита информации. Inside. 2011. № 2. С. 32–34.

29. Бегишев И. Р. Создание, использование и распространение вредоносных компьютерных программ // Проблемы права. 2012. № 3. С. 218–221.

30. Бегишев И. Р. Уголовная ответственность за приобретение или сбыт цифровой и документированной информации, заведомо добытой преступным путем // Актуальные проблемы экономики и права. 2010. № 1. С. 123–126.

31. Бегишев И. Р. Проблемы уголовной ответственности за обращение со специальными техническими средствами, предназначенными для негласного получения информации // Следователь. 2010. № 5. С. 2–4.

32. Бегишев И. Р. Уголовно-правовые аспекты кибертерроризма // Правовые вопросы национальной безопасности. 2010. № 5–6. С. 34–37.

33. Бегишев И. Р. Цифровая информация: понятие и сущность как предмета преступления по российскому уголовному праву // Академический юридический журнал. 2011. № 2. С. 47–55.

34. Бегишев И. Р. Ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей // Вестник УрФО. Безопасность в информационной сфере. 2012. № 1. С. 15–18.

35. Бегишев И. Р. Некоторые вопросы противодействия мошенничеству в сфере компьютерной информации // Вестник Казанского юридического института МВД России. 2016. № 3. С. 112–117.

36. Бегишев И. Р. Проблемы ответственности за незаконные действия с информацией, заведомо добытой преступным путем // Безопасность информационных технологий. 2010. № 1. С. 43–44.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

37. Бегишев И. Р. Уголовная ответственность за перехват цифровой информации // Information Security / Информационная безопасность. 2010. № 4. С. 16–17.

38. Бегишев И. Р. Уголовная ответственность за нарушение работы цифровых устройств, их систем и сетей // Information Security / Информационная безопасность. 2010. № 5. С. 22–23.

39. Бегишев И. Р. Некоторые механизмы совершенствования уголовного законодательства за совершение преступлений в сфере обращения цифровой информации // Information Security / Информационная безопасность. 2017. № 6. С. 40–43.

40. Бегишев И. Р. Уголовно-правовое нововведение в сфере защиты цифровой информации // Information Security / Информационная безопасность. 2011. № 1. С. 18–19.

41. Бегишев И. Р. Новеллы в уголовном законодательстве об ответственности за преступления в сфере компьютерной информации // Information Security / Информационная безопасность. 2012. № 2. С. 52–53.

42. Бегишев И. Р. Новый взгляд на мошенничество в сфере компьютерной информации // Information Security / Информационная безопасность. 2016. № 1. С. 28–29.

43. Некоторые аспекты информационной безопасности технологии блокчейн / А. К. Арюков, И. Р. Бегишев, Н. А. Мальцев // Information Security / Информационная безопасность. 2018. № 6. С. 18–19.

44. Бегишев И. Р. Компьютерные атаки на КИИ России: правовые меры защиты // Information Security / Информационная безопасность. 2019. № 5. С. 8–10.

45. Бегишев И. Р. О некоторых способах совершения противоправных деяний в современных информационно-телекоммуникационных системах обращения цифровой информации // Информация и безопасность. 2009. № 4. С. 607–610.

46. Бегишев И. Р. Современное состояние преступлений в сфере обращения цифровой информации // Информация и безопасность. 2010. № 4. С. 567–572.

47. Бикеев И. И. Материальные объекты повышенной опасности в российском уголовном праве: общие и специальные вопросы. Казань: Познание, 2007. 272 с.

References

1. Bokovnya A. Y., Khisamova Z. I., Begishev I. R. Study of Russia and the UK legislations in combating digital crimes, *Helix*, 2019, Vol. 9, No. 5, pp. 5458–5461. DOI: 10.29042/2019-5458-5461

2. Bikeev I. I., Nikitin S. G., Khisamova Z. I., Begishev I. R., Bokovnya A. Y. Experience of Civil Government of Russian Federation Subjects with Institutions of Civil Society in the Sphere of Corruption, *International Journal of Innovative Technology and Exploring Engineering*, 2019, Vol. 9, No. 1, pp. 5184–5187. DOI: 10.35940/ijitee.A9227.119119

3. Bikeev I. I., Kabanov P. A., Begishev I. R., Khisamova Z. I. Criminological Risks and Legal Aspects of Artificial Intelligence Implementation, *ACM International Conference on Artificial Intelligence, Information Processing and Cloud Computing (AIIPCC2019)*, 2019, December, Sanya, China.

4. Begishev I. R., Khisamova Z. I., Mazitova G. I. Information infrastructure of safe computer attacks, *Helix,* 2019, Vol. 9, No. 5, pp. 5639–5642. DOI: 10.29042/2019-5639-5642

5. Begishev I. R., Khisamova Z. I., Mazitova G. I. Criminal legal ensuring of security of critical information infrastructure of the Russian Federation, *Revista Gênero & Direito*, 2019, Vol. 8, No. 6, pp. 283–292.

6. Khisamova Z. I., Begishev I. R., Gaifutdinov R. R. On Methods to Legal Regulation of Artificial Intelligence in the World, *International Journal of Innovative Technology and Exploring Engineering*, 2019, Vol. 9, No. 1, pp. 5159–5162. DOI: 10.35940/ijitee.A9220.119119

7. Begishev I. R. *Notion and types of crimes in the sphere of digital information circulation,* abstract of PhD (Law) thesis, Kazan, 2017, 31 p. (in Russ.)

8. Begishev I. R. *Notion and types of crimes in the sphere of digital information circulation,* PhD (Law) thesis, Kazan, 2017, 204 p. (in Russ.)

9. Begishev I. R. Safety of critical information infrastructure of the Russian Federation, *Bezopasnost' biznesa*, 2019, No. 1, pp. 27–32 (in Russ.).

10. Begishev I. R. Syndrome of a safe attack: legal-psychological phenomenon, *Yuridicheskaya psikhologiya*, 2018, No. 2, pp. 27–30 (in Russ.).

11. Begishev I. R., Khisamova Z. I. Criminological risks of using artificial intellect, *Vserossiiskii kriminologicheskii zhurnal*, 2018, Vol. 12, No. 6, pp. 767–775 (in Russ.). DOI: 10.17150/2500-4255.2018.12(6).767-775

12. Khisamova Z. I., Begishev I. R. Criminal liability and artificial intellect: theoretical and applied aspects, *Vserossiiskii kriminologicheskii zhurnal*, 2019, Vol. 13, No. 4, pp. 432–450 (in Russ.).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

13. Khisamova Z. I., Begishev I. R. Legal regulation of artificial intellect, *Baikal Research Journal*, 2019, Vol. 10, No. 2 (in Russ.).

14. Khisamova Z. I., Begishev I. R. Comparative-legal analysis of the Great Britain and Russia legislations in the sphere of counteracting digital crimes, *Baikal Research Journal*, 2019, Vol. 10, No. 3 (in Russ.).

15. Begishev I. R. Federal agency of information security of the Russian Federation: myth or reality?, *Information Security / Informatsionnaya bezopasnost'*, 2016, No. 6, pp. 14–15 (in Russ.).

16. Begishev I. R. Manufacturing , marketing and purchasing of special technical means aimed at violating the systems of digital information protection: legal aspect, *Informatsiya i bezopasnost'*, 2010, No. 2, pp. 255–258 (in Russ.).

17. Begishev I. R. Information armaments as a means of committing crimes, *Informatsionnoe pravo*, 2010, No. 4, pp. 23–25 (in Russ.).

18. Begishev I. R. Information wars: prevention and preclusion of threats, *Zashchita informatsii. Inside*, 2010, No. 4, pp. 34–35 (in Russ.).

19. Begishev I. R. Measures to prevent crimes in the sphere of digital information circulation, *Informatsiya i bezopasnost'*, 2011, No. 3, pp. 433–438 (in Russ.).

20. Begishev I. R. Novelties in liability for illegal access to computer information according to the Criminal Code of the Russian Federation, *Pravosudie v Tatarstane*, 2011, No. 4, pp. 42–44 (in Russ.).

21. Begishev I. R. Liability for violating the functioning of information-communication devices, their systems and networks, *Bezopasnost' informatsionnykh tekhnologii*, 2011, No. 1, pp. 73–75 (in Russ.).

22. Begishev I. R. Open software: issues of law, safety and consequences, *Information Security / Informatsionnaya bezopasnost'*, 2011, No. 4, pp. 28–29 (in Russ.).

23. Begishev I. R. Interception of digital information protected by law: criminal-legal aspects, *Informatsionnaya bezopasnost' regionov*, 2011, No. 1, pp. 78–81 (in Russ.).

24. Begishev I. R. Legal aspects of safety of information society, *Informatsionnoe obshchestvo*, 2011, No. 4, pp. 54–59 (in Russ.).

25. Begishev I. R. Crimes in the sphere of digital information circulation. Research results, *Information Security / Informatsionnaya bezopasnost'*, 2012, No. 6, pp. 8–10 (in Russ.).

26. Begishev I. R. Crimes in the sphere of digital information circulation: state, gaps and solutions, *Informatsionnoe pravo*, 2010, No. 2, pp. 18–21 (in Russ.).

27. Begishev I. R. Issues of counteracting the criminal infringements on informational systems of critically important and potentially dangerous objects, *Informatsionnaya bezopasnost' regionov*, 2010, No. 1, pp. 9–13 (in Russ.).

28. Begishev I. R. Counteracting leakages of digital information: issues of criminal liability, *Zashchita informatsii. Inside*, 2011, No. 2, pp. 32–34 (in Russ.).

29. Begishev I. R. Creating, using and distributing harmful computer software, *Problemy prava*, 2012, No. 3, pp. 218–221 (in Russ.).

30. Begishev I. R. Criminal liability for purchasing or marketing of digital and documented information knowingly obtained with criminal means, Actual Problems of Economics and Law, 2010, No. 1, pp. 123–126 (in Russ.).

31. Begishev I. R. Issues of criminal liability for using special technical means intended for undercover obtaining of information, *Sledovatel'*, 2010, No. 5, pp. 2–4 (in Russ.).

32. Begishev I. R. Criminal-legal aspects of cyberterrorism, *Pravovye voprosy natsional'noi bezopasnosti*, 2010, No. 5–6, pp. 34–37 (in Russ.).

33. Begishev I. R. Digital information: notion and essence as an object of crime according to the Russian criminal law, *Akademicheskii yuridicheskii zhurnal*, 2011, No. 2, pp. 47–55 (in Russ.).

34. Begishev I. R. Liability for violating the rules of exploitation of means of storing, processing or transmitting computer information and information-telecommunication networks, *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere*, 2012, No. 1, pp. 15–18 (in Russ.).

35. Begishev I. R. Some issues of counteracting fraud in the sphere of computer information, *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii*, 2016, No. 3, pp. 112–117 (in Russ.).

36. Begishev I. R. Issues of liability for illegal actions with information knowingly obtained with criminal means, *Bezopasnost' informatsionnykh tekhnologii*, 2010, No. 1, pp. 43–44 (in Russ.).

37. Begishev I. R. Legal liability for intercept of digital information, *Information Security / Informatsionnaya bezopasnost'*, 2010, No. 4, pp. 16–17 (in Russ.).

38. Begishev I. R. Legal liability for violating the functioning of digital devices, their systems and networks, *Information Security / Informatsionnaya bezopasnost'*, 2010, No. 5, pp. 22–23 (in Russ.).

39. Begishev I. R. Some mechanisms of improving criminal legislation for crimes in the sphere of digital information circulation, *Information Security / Informatsionnaya bezopasnost'*, 2017, No. 6, pp. 40–43 (in Russ.).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

40. Begishev I. R. Criminal-legal novelties in the sphere of digital information protection, *Information Security / Informatsionnaya bezopasnost'*, 2011, No. 1, pp. 18–19 (in Russ.).

41. Begishev I. R. Novels in the criminal legislation on liability for crimes in the sphere of computer information, *Information Security / Informatsionnaya bezopasnost'*, 2012, No. 2, pp. 52–53 (in Russ.).

42. Begishev I. R. New look at fraud in the sphere of computer information, *Information Security / Informatsionnaya bezopasnost'*, 2016, No. 1, pp. 28–29 (in Russ.).

43. Aryukov A. K., Begishev I. R., Mal'tsev N. A. Some aspects of information security of blockchain technology, *Information Security / Informatsionnaya bezopasnost'*, 2018, No. 6, pp. 18–19 (in Russ.).

44. Begishev I. R. Computer attacks at Critical Information Infrastructure in Russia: legal means of protection, *Information Security / Informatsionnaya bezopasnost'*, 2019, No. 5, pp. 8–10 (in Russ.).

45. Begishev I. R. On some means of committing illegal acts in modern information-telecommunication systems of digital information circulation, *Informatsiya i bezopasnost'*, 2009, No. 4, pp. 607–610 (in Russ.).

46. Begishev I. R. Modern state of crimes in the sphere of digital information circulation, *Informatsiya i bezopasnost'*, 2010, No. 4, pp. 567–572 (in Russ.).

47. Bikeev I. I. *Highly hazardous material objects in the Russian criminal law: general and special issues,* Kazan, Poznanie, 2007, 272 p. (in Russ.).

Дата поступления / Received 27.08.2019
Дата принятия в печать / Accepted 10.10.2019
Дата онлайн-размещения / Available online 25.12.2019

© Лопатина Т. М., 2019
© Lopatina T. M., 2019

ПОЗНАНИЕ

Шаймиева, Э. Ш.

Теория и практика электронного правительства: учеб. пособие / Э. Ш. Шаймиева, Г. И. Гумерова. – Казань: Изд-во «Познание» Казанского инновационного университета, 2019. – 136 с.

В учебном пособии рассмотрены теоретические основы концепции электронного правительства, его научно-практические аспекты на основе международной, российской практики, реализация концепции электронного правительства в России. Вопросы развития концепции электронного правительства в разных странах изучаются во взаимосвязи с программами информатизации в государственном, частном секторах на базе основных подходов к информатизации общества в мировом масштабе. Представлен опыт развития электронного правительства в США, Европе, Японии. В части перспективы развития электронного правительства представлены положения концепции «открытого правительства».

Содержит необходимые теоретические материалы, задания для выполнения практических работ, тесты и вопросы для самоконтроля.

Предназначено для студентов бакалавриата, обучающихся по направлению подготовки 38.03.04 «Государственное и муниципальное управление», профиль подготовки «Региональное и муниципальное управление», лиц, занимающихся повышением квалификации или проходящих переподготовку по данному направлению, а также магистрантов, аспирантов, изучающих вопросы информационного общества, электронного правительства, использования информационно-коммуникационных технологий в государственном управлении в процессе формирования экономики знаний.