DOI 10.17150/2411-6262.2019.10(3).15 http://brj-bguep.ru

УДК 343.34

И.Р. Бегишев
Казанский инновационный университет им. В.Г. Тимирясова (ИЭУП), г. Казань, Российская Федерация

З.И. Хисамова
Краснодарский университет Министерства внутренних дел Российской Федерации, г. Краснодар, Российская Федерация

СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА ВЕЛИКОБРИТАНИИ И РОССИИ В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В ЦИФРОВОЙ СФЕРЕ

АННОТАЦИЯ. В работе приведен компаративный анализ уголовного и информационного законодательства, правовых актов по обеспечению кибербезопасности Великобритании и России. Опыт Великобритании как наиболее «цифровой» страны мира в противодействии преступлениям, совершаемым с использованием цифровых технологий, представляется как никогда востребованным и актуальным. Отмечается, что в России ущерб для граждан и организаций от преступных посягательств в пять раз превышает аналогичный ущерб для поданных Великобритании, между тем общее количество зарегистрированных в Российской Федерации посягательств значительно ниже официальной криминальной статистики Великобритании. Авторами обосновывается тезис о целесообразности создания в российском законодательстве более универсальных норм с определенным «порогом прочности» к новым видам цифровых угроз. Утверждается, что отдельным направлением внутренней уголовной политики всех стран должно стать создание эффективных механизмов применения положений законодательства в цифровой сфере. На основе проведенного исследования предложены некоторые механизмы обеспечения безопасности отношений в цифровой сфере.

КЛЮЧЕВЫЕ СЛОВА. Безопасность, Великобритания, информация, киберпреступления, компьютерные преступления, критическая инфраструктура, несанкционированный доступ, обеспечение кибербезопасности, ответственность, преступление, преступления в сфере компьютерной информации, Россия, уголовная ответственность, уголовное право, цифровая экономика, цифровые преступления, цифровые технологии.

ИНФОРМАЦИЯ О СТАТЬЕ. Дата поступления 20 июня 2019 г.; дата принятия к печати 4 октября 2019 г.; дата онлайн-размещения 31 октября 2019 г.

I.R. Begishev
V.G. Timiryasov Kazan Innovative University (IEML), Kazan, Russian Federation

Z.I. Khisamova
Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, Krasnodar, Russian Federation

COMPARATIVE AND LEGAL ANALYSIS OF LEGISLATIONS OF GREAT BRITAIN AND RUSSIA IN THE FIELD OF PREVENTING CRIMES IN THE DIGITAL SPHERE

ABSTRACT. The paper presents a comparative analysis of criminal and information legislations, legal acts to ensure cybersecurity in the UK and Russia. The experience of

the UK as the most “digital” country in the world in combating crimes committed with the use of digital technologies seems to be more than ever requested and topical. It notes that in Russia the damage to citizens and organizations from criminal attacks is five times higher than the similar damage to the UK citizens, while the total number of attacks registered in the Russian Federation is much lower than that of the official UK criminal statistics. The authors substantiate the thesis about feasibility of creating in the Russian legislation more universal norms with a certain “threshold of strength” to new types of digital threats. They argue that creation of effective mechanisms for application of legislation provisions in the digital sphere should be a separate area of domestic criminal policy of all countries. On the basis of the conducted research, they offer some mechanisms of securing relations in the digital sphere.

KEYWORDS. Security, United Kingdom, information, cybercrime, computer crimes, critical infrastructure, unauthorized access, cybersecurity, liability, crime, computer information crimes, Russia, criminal liability, criminal law, digital economy, digital crimes, digital technology.

ARTICLE INFO. Received June 20, 2019; accepted October 04, 2019; available online October 31, 2019.

Переход от производственной к цифровой модели экономики охватил почти все мировое сообщество. Наблюдается повсеместное внедрение технологий хранения больших данных, цифровизации банковского сектора, систем здравоохранения и образования и других отраслей. Вполне закономерно, что повсеместное внедрение цифровых технологий находится в прямой зависимости со степенью распространенности их использования в противоправных целях. Для предотвращения нарастающей угрозы и минимизации уже имеющихся последствий разрабатываются правовые акты, ставящие некоторые сферы деятельности вне закона. Опыт Великобритании как наиболее «цифровой» страны мира в противодействии преступлениям, совершаемым с использованием цифровых технологий, представляется как никогда востребованным и актуальным. Сегодня страна трансформировалась в ведущую мировую цифровую экономику. Великобритания имеет самую производительную научную базу, и занимает первое место во многих ключевых глобальных показателях качества исследований.

Согласно исследованию международной компании, специализирующейся на управленческом консалтинге The Boston Consulting Group (BCG) Великобритания является лидером по доле цифровой экономики в ВВП страны. Область, которая включает в себя информационные технологии и телекоммуникации, расходы государства, связанные с интернетом, кибербезопасностью занимает второе место в экономике страны — порядка 12,4 %, уступая только недвижимости, и одновременно обгоняя торговлю и производство[1]. Страна входит в ТОП-5 рейтинга стран с развитой цифровой экономикой (Digital Evolution Index 2017)[2], индекса развития инноваций (The Global Innovation Index 2017)[3], международного индекса цифровой экономики и общества (I-DESI) и индекса развития информационно-коммуникационных технологий (The ICT Development Index 2017)[4].

1 марта 2017 г. в Великобритании была принята Стратегия цифровой экономики (UK Digital Strategy 2017)[5]. Основная цель принятия Стратегии — это

[1] The Boston Consulting Group (BCG). URL: https://www.bcg.com/ru-ru/default.aspx.

[2] ТОП 10 стран с наиболее развитой цифровой экономикой. URL: http://web-payment.ru/article/250/top-10-cifrovaya-/.

[3] The Global Innovation Index 2017. URL: https://www.globalinnovationindex.org/Home.

[4] The ICT Development Index 2017. URL: https://gtmarket.ru/ratings/ict-development-index/ict-development-index-info#united-kingdom.

[5] UK Digital Strategy 2017. URL: https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy#a-safe-and-secure-cyberspace-making-the-uk-the-safest-place-in-the-world-to-live-and-work-online.

создание после выхода из Евросоюза экономики, устойчивой к изменениям и пригодной для будущего. Отмечается, что Великобритания всегда была в авангарде цифровых инноваций: с самых первых дней изобретения вычислительной техники до развития всемирной паутины. В Стратегии выделены 7 приоритетных направлений:

– создание цифровой инфраструктуры мирового класса;

– формирование цифровых навыков и инклюзивности;

– создание благоприятных условий для начала и развития цифрового бизнеса;

– создание условий для ведения цифрового бизнеса;

– сохранение правительством мирового лидерства в обслуживании своих граждан в интернете (цифровое правительство);

– создание условий для политики открытых данных и повышение доверия общественности к ее использованию;

– обеспечение безопасности и защищенного киберпространства.

Для достижения указанных целей 27 апреля 2017 г. был принят закон «О цифровой экономике» (Digital Economy Act 2017)[6]. Законом детально регламентировано и раскрыто содержание понятий в сфере обеспечения доступа к цифровым услугам; внесены изменения в нормы, регулирующие работу и развитие цифровой инфраструктуры и цифрового правительства; введены ограничения, направленные на противодействие распространения порнографии с участием несовершеннолетних в Интернете, а также обеспечивающие защиту интеллектуальной собственности.

Аналогом рассматриваемого закона является принятая в России программа «Цифровая экономики Российской Федерации»[7], которая в последствии преобразовалась в одноименную национальную программу[8].

Наиболее значимый вклад в цифровую трансформацию российской экономики страны вносит реализация национальной программы «Цифровая экономика Российской Федерации», включающая 6 приоритетных направлений:

– нормативное регулирование цифровой среды (создание гибкой системы правового регулирования, обеспечивающей цифровую трансформацию отраслей экономики, социальной сферы и управления);

– информационная инфраструктура (создание глобально-конкурентоспособной инфраструктуры передачи, обработки и хранения данных, а также цифровых продуктов для граждан, бизнеса и власти);

– кадры для цифровой экономики (создание условий для формирования рынка труда квалифицированными и конкурентоспособными кадрами цифровой экономики через трансформацию всех уровней систем образования, внедрения программ переобучения в компаниях и ведомствах);

– информационная безопасность (создание безопасной и устойчивой информационной инфраструктуры для граждан, представителей бизнеса и государства в цифровом пространстве);

– цифровые технологии (создание комплексной системы поддержки исследований, проектов по разработке, внедрению цифровых технологий и платформенных решений);

---

[6] Digital Economy Act 2017. URL: https:// http://www.wipo.int/wipolex/ru/text.jsp?file_id=474843 (дата обращения: 15.05.2019).

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

[8] О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года : Указ Президента РФ от 7 мая 2018 г. № 204 // Собрание законодательства РФ. 2018. № 20. Ст. 2817.

– цифровое государственное управление (переход к управлению данными государства на основе цифровых технологий, разработка комплексных суперсервисов для получения гражданами и бизнесом государственных услуг в «один клик»).

Особое внимание в российской национальной программе уделено вопросам безопасности информационной инфраструктуры, и внедрения цифровых технологий, в частности, новых интеллектуальных технологий, поскольку, в настоящее время началось формирование криминологических основ применения искусственного интеллекта, что требует принятия действий и решений по предупреждению возможных негативных проявлений его использования и государственному реагированию на них [1].

Важнейшим для цифровой экономики является вопрос применения и использования цифровых технологий. Так, например, Р. Вудхед, П. Стивенсон и Д. Морри указываю, что развитие цифровых технологий сильно влияет на Стратегию цифровой экономики [2].

Однако, несмотря на предпринимаемые меры, по словам М. Хьюлетта, руководителя операций Британского национального управления по борьбе с киберпреступностью, в 2017 г. «около половины всех зарегистрированных преступлений в Великобритании так или иначе были связаны с кибербезопасностью» (56 % или 1,9 млн)[9]. В то же время около 68 % крупных британских предприятий также выявили нарушения кибербезопасности или попытки атак за последние 12 месяцев[10].

Г. Хорсман отмечает, невзирая на то, что в настоящее время правоохранительные службы противодействуют цифровым преступлениям, все же возникает вопрос относительно того, смогут ли они поддерживать этот уровень в условиях быстрого распространения цифровой преступности [3], в числе прочего в условиях угроз кибербезопасности Великобритании после брексита [4].

По данным Агентства национальной статистики Великобритании, на сентябрь 2018 г. было зафиксировано 367 845 сообщений о мошенничестве в цифровой сфере (прирост 11 % к АППГ), и 13 357 компьютерных преступлений[11]. Для сравнения по данным официальной статистики МВД России, за 2018 г. в Российской Федерации было зарегистрировано 95 876 мошенничеств в цифровой сфере (4,4 % от всех зарегистрированных в России преступлений, прирост к АППГ 37 %) и 2 499 цифровых преступлений[12], при этом ущерб в России составил около 400 млрд р., тогда как в Великобритании он оценивается примерно в 84 млрд р. Таким образом, можно заключить, что в России ущерб для граждан и организаций от преступных посягательств в 5 раз превышает аналогичный ущерб для поданных Великобритании, между тем общее количество зарегистрированных в Российской Федерации посягательств значительно ниже официальной криминальной статистики Великобритании. Указанное обстоятельство можно объяснить высоким уровнем латентности цифровых преступлений в Российской Федерации [5].

В целях становления Великобритании как безопасного и защищенного киберпространства была принята Национальная Стратегия кибербезопасности, опубли-

[9] Crime in England and Wales: Additional tables on fraud and cybercrime. URL: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables.

[10] Cybercrime in the UK. URL: https://www.governmenteuropa.eu/cybercrime-uk/86105/.

[11] National Fraud profile: National Fraud Intelligence Bureau. URL: https://www.gov.uk/government/organisations/national-fraud-authority/about.

[12] Статистика и аналитика / ГИАЦ МВД России // Министерство внутренних дел Российской Федерации. URL: https://мвд.рф/Deljatelnost/statistics.

кованная 1 ноября 2016 г. (National cybersecurity Strategy 2016–2021)[13]. Основная цель Стратегии — достижение Великобританией к 2021 г. статуса безопасной и устойчивой к киберугрозам страны, процветающий и уверенной в цифровом мире.

Примечательно, что в Стратегии выделяются две формы преступной деятельности[14]:

– киберзависимые преступления — преступления, совершаемые только посредством использования цифровых технологий, где устройства используются как инструмент для совершения преступления, а цель преступления — разработка и распространение вредоносных программ для получения финансовой выгоды, взлома для кражи, повреждения, искажения или уничтожения информации и/или сети или деятельности;

– киберпреступления — «традиционные» преступления, последствия и масштабы которых могут быть увеличены путем применения вычислительной техники, компьютерных сетей или других форм ИКТ (например, мошенничества и кражи данных).

Отдельно в Стратегии выделяется криптоджекинг как самостоятельное направление преступной деятельности. Полагаем, что дальнейшее расширение сферы применения цифровых финансовых активов (криптовалют и др.) ознаменует расширение границ указанного направления преступной деятельности.

Аналогичный документ стратегического характера имеется в России — Доктрина информационной безопасности Российской Федерации[15]. В ней определены стратегические цели и основные направления обеспечения информационной безопасности, проанализированы основные информационные угрозы и дана оценка состоянию информационной безопасности. В ней приводятся основные направления обеспечения информационной безопасности в области обороны, государственной и общественной безопасности, в экономической сфере, в области науки, технологий и образования, стратегической стабильности и равноправного стратегического партнерства.

Закон «Computer Misuse Act 1990»[16] — является базовым «цифровым» уголовным актом Великобритании [6] (далее — Закон).

Следует отметить, что проблемы развития законодательства Великобритании в цифровой сфере подробно рассмотрены в специальных источниках информации [7].

Рассмотрим более подробно положения Закона о неправомерном использовании компьютера, положения которого неоднократно подвергались существенным коррективам.

Статья 1 Закона предусмотрено наказание за несанкционированный доступ к компьютерным материалам. Указанную норму можно рассматривать в качестве основного преступления, так как зачастую оно предшествует совершению других, более серьезных преступлений. Преступление считается оконченным с момента, как лицо включило компьютер для получения санкционированных материалов. Насколько ему удалось реализовать свой умысел, значения не имеет. Норма является общей, поэтому умысел злоумышленника не должен быть направлен на какую-либо конкретную информацию, данные или программу, хранящиеся на компьютере.

---

[13] National Cyber Security Strategy 2016 to 2021. URL: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

[14] Авторы придерживаются синонимичного толкования, использованного авторами понятия «преступления в цифровой сфере» и понятия «киберпреступления».

[15] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 5 дек. 2016 г. № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

[16] Computer Misuse. URL: https://www.cps.gov.uk/legal-guidance/computer-misuse.

Доступ является несанкционированным, если лицо не имеет права или не получило согласия на такой доступ. Понимание британским правоприменителем содержания несанкционированного или неавторизованного доступа аналогично тому, что дается в Европейской конвенции по борьбе с киберпреступностью[17].

Необходимо ответить, что под данную норму подпадают и должностные лица, которые превысили пределы своих полномочий по доступу к информации, к которой они не были допущены.

Такая практика сложилась в деле мирового суда на Боу-стрит[18]. Палата лордов сочла, что сотрудник явно подпадает под положения ст. 1 Закона о неправомерном использовании компьютера, поскольку преднамеренно получил доступ, на который не имел права. При этом было установлено, что работник будет виновен в правонарушении только в том случае, если работодатель четко определил пределы полномочий работника на доступ к программе или данным[19].

За несанкционированный доступ с целью совершения или содействия совершению новых преступлений ответственность предусмотрена ст. 2 упомянутого Закона. Такой доступ также является подготовительным этапом при совершении иного (нового) преступления. Лицо может быть признано виновным в совершении преступления, даже если совершение основного преступления невозможно (ч. 4 ст. 2). Человек, признанный невиновным по ст. 2 или 3 Закона судом присяжных, может быть осужден за преступление по ст. 1.

Статьей 3 Закона предусмотрена ответственность за несанкционированные действия в отношении компьютерных систем с целью нанесения ущерба или по неосторожности. Лицо признается виновным в совершении преступления, если совершает любое несанкционированное действие, в том числе и получает доступ к данным. К ответственности по ст. 3 привлекаются также лица, виновные в совершении DDoS-атак.

Статьей 3 ZA Закона предусмотрена ответственность за несанкционированные действия, вызывающие или создающие риск серьезного ущерба.

Указанная норма направлена для пресечения посягательств на объекты критически важной национальной инфраструктуры (в зависимости от мотивов исполнителя также может быть применено антитеррористическое законодательство). Полагаем, что рассматриваемая норма тождественна по своей сути ст. 274.1. «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» Уголовного кодекса Российской Федерации[20] (далее — УК РФ). Более подробно указанные вопросы рассмотрены в предыдущих научных работах авторов [8–10].

Статья 3А Закона устанавливает ответственность за деяния, сопряженные с неправомерным использованием цифровых технологий, то есть преступлений, предусмотренных ст. 1, 3 или 3 ZA.

Указанная норма представляется частично тождественной положениям ст. 187 «Неправомерный оборот средств платежей» и ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ. Кроме того, рассматриваемая статья хорошо коррелируется с предложениями об установлении ответственности за незаконные действия с информацией, заведомо добытой преступным путем [11; 12].

---

[17] Convention on Cybercrime (ETS № 185). URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

[18] Case of R v Bow Street Magistrates' Court and Allison (AP) Ex parte Government Of The United States of America [Allison] [2002] 2 AC 216.

[19] Computer Misuse. URL: https://www.cps.gov.uk/legal-guidance/computer-misuse-act-1990.

[20] Уголовный кодекс Российской Федерации : Федер. закон РФ от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

Так, ответственности подлежат лица, производящие или поставляющие «вредоносные программы». Для привлечения к ответственности по данной норме необходимо обязательное установление умысла на совершение преступления. Сами по себе указанные деяния, без преступного умысла, не криминализированы [13].

Стоит подчеркнуть, что в законодательстве Великобритании также отражены обязательные для инкорпорирования в национальное законодательство положения Европейской Конвенции по борьбе с киберпреступностью[21] и Директивы Европейского парламента и Совета Европейского Союза[22]. В России Конвенция на сегодняшний день не ратифицирована.

Обобщая вышеизложенное, необходимо отметить следующее. В Великобритании сегодня создана достаточно стройная система обеспечения безопасности отношений в цифровой сфере, в стране приняты и успешно применяются нормы уголовного законодательства в указанной сфере. Казуистичность англо-саксонского права и его гибкость, на наш взгляд, обладают особым преимуществом в условиях постоянной трансформации и изменения правоотношений в цифровой сфере. Однако, проведенный компаративный анализ позволяет заключить, что в российском уголовном законодательстве, так же как и в британском, нашли отражение положения, являющиеся адекватной реакцией на возникающие преступные посягательства.

Однако, в условиях постоянного совершенствования цифровых технологий и их быстрой адаптации для преступных целей, полагаем целесообразным создание в российском законодательстве более универсальных норм с определенным «порогом прочности» к новым видам цифровых угроз.

Вместе с тем, в условиях всеобщей глобализации для всех стран становится очевидным, что преступность в IT-сфере — неотъемлемая часть цифровой экономики, ведь, как известно, у любой стороны две медали. И с большей цифровизацией общества ее границы буду расти, постепенно полностью вытесняя традиционную преступность. И реагировать на нее необходимо комплексно и постоянно. Трансграничный характер указанных посягательств в числе основных задач ставит унификацию правовых норм, регулирующих цифровую сферу, создание единого механизма привлечения к ответственности за посягательства в указанной сфере во всем мире, невзирая на геополитические границы. Отдельным направлением внутренней уголовной политики всех стран должно стать создание эффективных механизмов применения положений законодательства в цифровой сфере, так как без необходимого механизма его применения любое законодательство, даже самое прогрессивное, бесполезно и носит лишь декларативный характер. Для привлечения к уголовной ответственности необходимо наличие доказательств о виновности лица. Информационный характер посягательств обусловливает необходимость расширения границ полномочий правоохранительных органов, что неразрывно приводит к проблеме поиска баланса между соблюдением свобод граждан в цифровом пространстве и обеспечением всеобщей кибербезопасности. В Великобритании, как и во всех странах мира, ответ на этот вопрос еще не найден.

---

[21] Convention on Cybercrime (ETS № 185). URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

[22] Об атаках на информационные системы и о замене Рамочного Решения 2005/222/ПВД Совета ЕС : Директива Европейского парламента и Совета Европейского Союза 2013/40/ЕС от 12 авг. 2013 г. URL: https://base.garant.ru/70557982/; Об атаках на информационные системы : Рамочное решение 2005/222/ПВД Совета ЕС от 24 февр. 2005 г. // Official Journal. 2005. № 69. P. 67.

Список использованной литературы

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

2. Woodhead R. Digital construction: From point solutions to IoT ecosystem / R. Woodhead, P. Stephenson, D. Morrey. — DOI 10.1016/j.autcon.2018.05.004 // Automation in Construction. — 2018. — № 93. — P. 35–46.

3 Horsman G. Can we continue to effectively police digital crime? / G. Horsman. — DOI 10.1016/j.scijus.2017.06.001 // Science & Justice. — 2017. — № 6 (57). — P. 448–454.

4. Hert P. Vagelis Papakonstantinou The rich UK contribution to the field of EU data protection: Let's not go for «third country» status after Brexit / P. Hert. — DOI 10.1016/j.clsr.2017.03.008 // Computer Law & Security Review. — 2017. — № 3 (33). — P. 354–360.

5. Воротников В.Л. Уголовно-правовая политика в отношении преступлений в сфере компьютерной информации / В.Л. Воротников // Вестник Тамбовского университета. Серия: Гуманитарные науки. — 2009. — № 4 (72). — С. 280–282.

6. Хисамова З.И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий : дис. ... канд. юрид. наук : 12.00.08 / З.И. Хисамова. — Краснодар, 2016. — 222 с.

7. Kemp R. IT law in the UK: Looking back on 2007 and ahead to 2009 / R. Kemp. — DOI 10.1016/j.clsr.2008.09.004 // Computer Law & Security Review. — 2008. — № 6 (24). — P. 473–474.

8. Бегишев И.Р. Понятие и виды преступлений в сфере обращения цифровой информации : автореф. дис. ... канд. юрид. наук : 12.00.08 / И.Р. Бегишев. — Казань, 2017. — 30 с.

9. Бегишев И.Р. Проблемы противодействия преступным посягательствам на информационные системы критически важных и потенциально опасных объектов / И.Р. Бегишев // Информационная безопасность регионов. — 2010. — №. 1 (6). — С. 9–13.

10. Бегишев И.Р. Ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей / И.Р. Бегишев // Вестник УрФО. Безопасность в информационной сфере. — 2012. — № 1 (3). — С. 15–18.

11. Бегишев И.Р. Проблемы ответственности за незаконные действия с информацией, заведомо добытой преступным путем / И.Р. Бегишев // Безопасность информационных технологий. — 2010. — Т. 17, № 1. — С. 43–44.

12. Бегишев И.Р. Уголовная ответственность за приобретение или сбыт цифровой и документированной информации, заведомо добытой преступным путем / И.Р. Бегишев // Актуальные проблемы экономики и права. — 2010. — № 1 (13). — С. 123–126.

13. Хисамова З.И. Международный опыт уголовно-правового противодействия преступлениям в сфере цифровой экономики / З.И. Хисамова. — Краснодар : Изд-во Краснодар. ун-та МВД России, 2018. — 116 с.

References

1. Begishev I.R., Khisamova Z.I. Criminological Risks of Using Artificial Intelligence. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2018, vol. 12, no. 6, pp. 767–775. DOI: 10.17150/2500-4255.2018.12(6).767-775. (In Russian).

2. Woodhead R., Stephenson P., Morrey D. Digital Construction: From Point Solutions to IoT Ecosystem. *Automation in Construction*, 2018, no. 93, pp. 35–46. DOI: 10.1016/j.autcon.2018.05.004.

3. Horsman G. Can we Continue to Effectively Police Digital Crime? *Science & Justice*, 2017, no. 6 (57), pp. 448–454. DOI: 10.1016/j.scijus.2017.06.001.

4. Hert P. Vagelis Papakonstantinou The rich UK Contribution to the Field of EU Data Protection: Let's not go for «Third Country» Status after Brexit. *Computer Law & Security Review*, 2017, no. 3 (33), pp. 354–360. DOI: 10.1016/j.clsr.2017.03.008.

5. Vorotnikov V.L. The Criminally-Legal Policy Concerning Crimes in the Sphere of the Computer Information. *Vestnik Tambovskogo Universiteta. Serija: Gumanitarnye Nauki = Tambov State University Bulletin. Series: Humanities*, 2009, no. 4 (72), pp. 280–282. (In Russian).

6. Khisamova Z.I. *Ugolovno-pravovye mery protivodeistviya prestupleniyam, sovershaemym v finansovoi sfere s ispol'zovaniem informatsionno-telekommunikatsionnykh tekhnologii. Kand. Diss*. [Criminal and legal measures of counteracting crimes committed in financial sphere with use of information and telecommunication technologies. Cand. Diss.]. Krasnodar, 2016. 222 p.

7. Kemp R. IT law in the UK: Looking Back on 2007 and Ahead to 2009. *Computer Law & Security Review,* 2008, no. 6 (24), pp. 473–474. DOI: 10.1016/j.clsr.2008.09.004.

8. Begishev I.R. *Ponyatie i vidy prestuplenii v sfere obrashcheniya tsifrovoi informatsii. Avtoref. Kand. Diss.* [Concept and types of crimes in the sphere of digital information circulation. Cand. Diss. Thesis]. Kazan, 2017. 30 p.

9. Begishev I.R. Problems of Counter Action to the Criminal Encroachments on the Information Systems of Critical and Potentially Dangerous Objects. *Informatsionnaya bezopasnost' regionov = Information Security of Regions,* 2010, no. 1 (6), pp. 9–13. (In Russian).

10. Begishev I.R. Responsibility for Violating Service Regulations on the Means for Data Storing, Processing and Transferring and Information and Telecommunication Networks. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere = UrFR Newsletter. Information Security,* 2012, no. 1 (3), pp. 15–18. (In Russian).

11. Begishev I.R. The Problem of the Responsibility for Illegal Actions with the Information Obviously Extracted Criminal Way. *Bezopasnost' informatsionnykh tekhnologii = IT Security,* 2010, vol. 17, no. 1, pp. 43–44. (In Russian).

12. Begishev I.R. Criminal responsibility for acquisition or marketing of digital and documented information obtained by deliberately criminal manner. *Aktual'niye problemy ekonomiki i prava = Actual Problems of Economics and Law,* 2010, no. 1 (13), pp. 123–126. (In Russian).

13. Khisamova Z.I. *Mezhdunarodnyi opyt ugolovno-pravovogo protivodeistviya prestupleniyam v sfere tsifrovoi ekonomiki* [International experience of criminal and legal counteractions to crimes in the sphere of digital economy]. Krasnodar University of the Ministry of Internal Affairs of the Russian Federation Publ., 2018. 116 p.

Информация об авторах

Бегишев Ильдар Рустамович — кандидат юридических наук, заслуженный юрист Республики Татарстан, старший научный сотрудник, Казанский инновационный университет им. В.Г. Тимирясова (ИЭУП), Российская Федерация, г. Казань, e-mail: begishev@mail.ru.

Хисамова Зарина Илдузовна — кандидат юридических наук, начальник отделения планирования и координации научной деятельности научно-исследовательского отдела, Краснодарский университет Министерства внутренних дел Российской Федерации, Российская Федерация, г. Краснодар, e-mail: alise89@inbox.ru.

Authors

Ildar R. Begishev — Ph.D. in Law, Honored Lawyer of the Republic of Tatarstan, Senior Researcher, V.G. Timiryasov Kazan Innovative University (IEML), Kazan, Russian Federation, e-mail: begishev@mail.ru.

Zarina I. Khisamova — Ph.D. in Law, Head of Department of Planning and Coordination of Research Department Scientific Activities, Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, Krasnodar, Russian Federation, e-mail: alise89@inbox.ru.

Для цитирования

Бегишев И.Р. Сравнительно-правовой анализ законодательства Великобритании и России в области противодействия преступлениям в цифровой сфере / И.Р. Бегишев, З.И. Хисамова // Baikal Research Journal. — 2019. — Т. 10, № 3. — DOI : 10.17150/2411-6262.2019.10(3).15.

For Citation

Begishev I.R., Khisamova Z.I. Comparative and Legal Analysis of Legislations of Great Britain and Russia in the Field of Preventing Crimes in the Digital Sphere. *Baikal Research Journal*, 2019, vol. 10, no. 3. DOI: 10.17150/2411-6262.2019.10(3).15. (In Russian).