УДК 343.9
DOI 10.17150/2500-4255.2020.14(6).898-913

ГАРМОНИЗАЦИЯ РОССИЙСКОГО УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА О ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПНОСТИ С ПРАВОВЫМИ СТАНДАРТАМИ СОВЕТА ЕВРОПЫ

В.П. Кириленко, Г.В. Алексеев
Северо-Западный институт управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, г. Санкт-Петербург, Российская Федерация

Информация о статье

Дата поступления
20 апреля 2020 г.

Дата принятия в печать
21 декабря 2020 г.

Дата онлайн-размещения
30 декабря 2020 г.

Ключевые слова
Интернет; компьютерные преступления; взлом; мошенничество; вымогательство; фишинг; правоприменение

Аннотация. Преступность в виртуальном пространстве, созданном цифровыми технологиями, причиняет существенный экономический ущерб. Корыстные мотивы преступников в информационном обществе порождают все более изощренные способы злоупотребления доверием пользователей компьютерных сетей. Гармонизация российского законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы неизбежна в силу трансграничного характера преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, и их высокой общественной опасности. Методика исследования киберпреступности основана на сравнительном анализе российской правоприменительной практики по преступлениям в сфере компьютерной информации с наиболее прогрессивными практиками борьбы с киберпреступностью в государствах — участниках Совета Европы. Методы включенного наблюдения и дискурсивного анализа позволяют выявить латентные деликты в современном информационном пространстве. Анализ уголовного законодательства и практик криминального поведения в киберпространстве нацелен на совершенствование мер по противодействию нарушениям фундаментальных прав человека в процессе цифровизации народного хозяйства, где наиболее типичным виртуальным преступлением становится мошенничество в форме злоупотребления доверием пользователей сетей компьютерной связи. Пользователи сети Интернет заинтересованы в том, чтобы сообщать о фактах правонарушений в информационном пространстве при условии защиты государством их фундаментальных свобод. Создание криминальными структурами закрытых социальных сетей, наряду с расширением технических возможностей для осуществления вымогательства, приводит к формированию универсальных схем обогащения преступников, не только заинтересованных в снижении влияния государства на общественные отношения, но и претендующих на свое право доминировать на экономическом поле информационного общества. Эффективная политика борьбы правоохранительных органов с экономической преступностью в глобальном информационном пространстве требует международного консенсуса в вопросах развития государственно-частного партнерства в деле выявления киберпреступлений и пресечения криминальных практик, сопряженных с использованием информационных технологий.

THE HARMONIZATION OF RUSSIAN CRIMINAL LEGISLATION ON COUNTERACTING CYBERCRIME WITH THE LEGAL STANDARDS OF THE COUNCIL OF EUROPE

Viktor P. Kirilenko, Georgy V. Alekseev
North-West Institute of Management of the Russian Presidential Academy of National Economy and Public Administration, Saint Petersburg, the Russian Federation

Article info

Received
2020 April 20

Abstract. Crimes that happen in the virtual environment created by digital technologies inflict considerable economic damage. Mercenary motives of criminals in the information society are giving rise to increasingly more and more sophisticated methods of abusing the trust of computer networks' users. The harmonization of Russian legislation on

ISSN 2500-4255

Accepted
2020 December 21
Available online
2020 December 30

Keywords
Internet; computer crime; hacking; fraud; extortion; phishing; law enforcement

counteracting cybercrimes with the legal standards of the Council of Europe is inevitable due to the trans-border character of crimes committed using information and telecommunication technologies, and to their high public danger. The methodology of researching cybercrime is based on the comparative analysis of Russian law enforcement practice on crimes in the sphere of computer information and the most progressive practices of counteracting cybercrime in the member states of the Council of Europe. The methods of inclusive observation and discursive analysis make it possible to identify latent delicts in contemporary information space. The analysis of criminal legislation and the practices of criminal behavior in cyberspace are aimed at improving the measures of counteracting the violations of fundamental human rights in the process of the digitization of economy, when fraud based on the abuse of network users' trust becomes the most typical virtual crime. Internet users are interested in reporting the facts of offences in the information space on the condition that the state protects their fundamental freedoms. The creation of closed social networks by criminal organizations and the widening technical opportunities for extortion result in the creation of universal schemes that enrich criminals, who are not only interested in reducing the state's influence on public relations, but are also trying to establish their dominance in the economic space of information society. The effective policy of law enforcement bodies on counteracting economic crimes in the global information space requires an international consensus regarding the development of public-private partnership in identifying cybercrimes and suppressing criminal practices connected with the use of information technologies.

Президент Российской Федерации В.В. Путин, признавая значимость цифровых технологий, в своем обращении к участникам Десятого российского форума по управлению Интернетом (RIGF-2019) подчеркнул важность эффективного противодействия «рискам и вызовам киберпреступности, распространению контента, нарушающего закон, представляющего угрозу правам граждан и интересам государства»[1].

Генеральный секретарь Интерпола Ю. Шток (Jürgen Stock), выступая на Восьмой конференции Интерпола и Европола по киберпреступности 6 октября 2020 г., отметил, что «в мире, где более 4,5 млрд человек подключены к сети, более половины человечества в любой момент рискует стать жертвой киберпреступности»[2]. Вице-президент Интерпола А.В. Прокопчук справедливо отмечает, что «противодействие киберпреступности затруднено ее трансграничным характером»[3], и признает общепринятый в Совете Европы тезис о том, что киберпреступность не знает границ[4].

Гармонизация законодательства о противодействии киберпреступности под эгидой Совета Европы осуществляется посредством имплементации Конвенции о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.)[5] в национальное уголовное законодательство. Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем (ETS № 189, Страсбург, 28 января 2003 г.), распространил действие Будапештской конвенции 2001 г. на правонарушения экстремистской направленности.

Программа Совета Европы «Действие против киберпреступности»[6] предполагает разработку Второго дополнительного протокола к Будапештской конвенции, который обеспечит защиту персональных данных и тайну частной жизни. Вместе с тем на практике именно экономические преступления занимают центральное место в структуре киберпреступности и угрожают устойчивому развитию.

Ратификация Будапештской конвенции 2001 г. почти всеми государствами — членами Совета Европы, а также США, Канадой, Японией

[1] Путин заявил о важности противодействия киберпреступности // РИА Новости. URL: https://ria.ru/20190408/1552468651.html.

[2] Interpol-Europol 8th Cybercrime Conference: «Half of humanity at risk» // INTERPOL. URL: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-Europol-8th-Cybercrime-Conference-Half-of-humanity-at-risk.

[3] Глава НЦБ Интерпола МВД РФ: со всеми зарубежными партнерами мы готовы вести диалог // ТАСС. URL: https://tass.ru/interviews/9543411.

[4] Cybercrime: new survey shows Europeans feel better informed but remain concerned // Europska komisija. URL: https://ec.europa.eu/commission/presscorner/detail/hr/ip_20_143.

[5] Convention on Cybercrime : ETS no. 185 (Budapest, 23 Nov. 2001) // Council of Europe. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[6] Protocol negotiations // Ibid. URL: https://www.coe.int/en/web/cybercrime/t-cy-drafting-group.

и многими другими неевропейскими странами демонстрирует широкое международное признание необходимости эффективного противодействия преступности в глобальном информационном пространстве. Однако признание высокой общественной опасности киберпреступности не гарантирует единообразного ее понимания всеми участниками международного общения, и потому гармонизация уголовного законодательства происходит на национальном уровне.

Понятие киберпреступности и противодействие ее проявлениям во многом зависят от национальной политики по применению норм уголовного права в виртуальном пространстве.

В российском уголовном законодательстве не используется термин «киберпреступность», однако, следуя современным тенденциям в европейской криминологии, Министерство внутренних дел Российской Федерации с 2018 г. характеризует киберпреступность как *преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации*. Российское понимание киберпреступности охватывает: преступления в сфере компьютерной информации (ст. 272–274.1 УК РФ), кражи (ст. 158 УК РФ), мошенничества (ст. 159 УК РФ), специальные составы — мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ) и мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), а также другие составы преступлений, при совершении которых задействуются ресурсы компьютерных сетей. В структуре российской киберпреступности, по данным за 2019 г., хищения составляют более 80 %, незаконный сбыт наркотических средств (ст. 228.1 УК РФ) — более 8 %, преступления в сфере компьютерной информации — около 1 %; также МВД РФ в компьютерных сетях выявлено 508 фактов нарушения неприкосновенности частной жизни (ст. 137 УК РФ), 469 преступлений экстремистской направленности (ст. 205.2 и 280 УК РФ), 232 факта нарушения авторских и смежных прав (ст. 146 УК РФ), 25 инцидентов, связанных с самоубийством (ст. 110, 110.1 УК РФ)[7].

Преступность в сфере компьютерной информации теоретически охватывает широкий круг деликтов, что отражается в официальной статистике. Анализируя социальные и технологические аспекты противодействия компьютерным преступлениям, Д.С. Уолл (David S. Wall) отмечает, что киберпреступления являются продуктом функционирования компьютерных сетей [1]. Преступления, связанные с контентом компьютеров — материалами, хранящимися в сетевых компьютерных системах, включают в себя мошенничество, торговлю порнографическими материалами и их распространение, преступления на почве ненависти, публикацию видео со сценами убийств и пыток похищенных граждан и др. [2, p. 4]. Активность неуправляемых компьютерных программ (ботов) неуклонно нарастает, создавая сети зараженных компьютеров, контролируемые злоумышленниками, которые все чаще играют роль в широком спектре киберпреступлений, что приводит к развитию новой концепции — концепции преступности искусственного интеллекта [3]. Неизбежное повышение уровня киберпреступности в условиях цифровой трансформации порождает ряд теоретических, политических и методологических проблем для правоприменительной деятельности.

Во-первых, в теоретическом плане от концептуального осмысления цифровых ценностей, процессов цифровизации и общественных отношений в виртуальном мире зависит правовая оценка степени общественной опасности противоправных деяний в компьютерных сетях и обоснованность криминализации конкретных составов преступлений, связанных с распространением компьютерной информации. Внедрение умных технологий позволяет криминальным элементам разрабатывать и реализовывать на практике новые преступные схемы, рассчитанные на получение дохода. Так, в частности, функционируют фишинговые сайты, виртуальные казино, через ресурсы Интернета реализуются заведомо некачественные и контрафактные товары, Даркнет (Darkweb) позволяет организовать анонимную торговлю наркотиками и другими товарами, изъятыми из хозяйственного оборота, а также оплачивать услуги откровенно криминального содержания [4].

Во-вторых, гармонизация законодательства о противодействии киберпреступности требует политического консенсуса в отношении степени открытости международного информационного пространства и применения норм международного права к общественным отношениям в сети Интернет. Коллизии разнонациональных законов применительно к общим информационным ресурсам не столько влекут юрисдикци-

[7] Единый отчет по преступности. Сборник по России. МВД России. 2019.

онные споры и актуализируют дискурс о защите информационного суверенитета, сколько создают правовую неопределенность в уголовно-правовой квалификации деяний, последствия которых затрагивают интересы всех государств и пользователей глобального информационного пространства.

В-третьих, формализм в методологическом плане значительно усложняет решение задачи по изысканию адекватных мер борьбы с киберпреступностью. С одной стороны, формальный подход к криминализации деяний, свойственный уголовному законодательству большинства государств — членов Совета Европы, призван исключить проблему оценки справедливости наказания за конкретные правонарушения из правоприменительной практики. С другой стороны, правоприменительная практика показывает, что принцип добросовестности (bona fide) нередко оказывается куда более уместной правовой нормой в отношении лиц, обвиняемых в совершении деликтов в постиндустриальном мире в целом [5] и в цифровом пространстве в частности [6], а фактические уголовные дела, связанные с киберпреступностью, редко отражают реальную криминальную активность хакеров [7].

Характеристика киберпреступности дается в большинстве государств — членов Совета Европы на основе полицейской статистики.

По данным российских правоохранительных органов, больше половины всех киберпреступлений совершается с использованием сети Интернет, свыше 42 % — при помощи средств мобильной связи; общее их количество, по статистическим сведениям за 2020 г., может превысить полмиллиона и составит около четверти всех преступлений, совершенных в России (табл. 1). На фоне роста удельного веса киберпреступности статистика по отдельным составам преступлений, таким как мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) и незаконные организация и проведение азартных игр (ст. 171.2 УК РФ), остается неизменной или снижается, что вряд ли отражает действительность, и свидетельствует скорее о проблемах правоприменения, чем о сокращении числа конкретных фактов правонарушений или их низкой общественной опасности.

Прирост киберпреступности в России, как представляется, замедлится, так как исходя из зарубежного опыта удельный вес киберпреступности в 30 % является на настоящее время предельным.

Прогноз динамики киберпреступности определяется обзором доступных опросов по виктимизации, которые показывают, что в период с 2010 по 2020 г. в государствах — членах Совета Европы киберпреступность может составлять от трети до половины преступлений [8], при этом есть все основания полагать, что рост количества компьютерных преступлений способствовал снижению уровня традиционной преступности,

Таблица 1 / Table 1

Динамика состояния и структуры киберпреступлений в России в 2016–2020 гг.*

Dynamics of the condition and structure of cybercrimes in Russia in 2016–2020

Показатель / Indicator	2016	2017	2018	2019	2020**
Число преступлений / Number of crimes	65 949	90 587	174 674	294 409	420 662
Темп прироста, % / Increase rate, %	–	+37,0	+92,0	+68,5	+75,0
Удельный вес, % / Specific weight, %	3,0	4,4	8,7	14,5	25,0
Преступления в сфере компьютерной информации / Crimes in the sphere of computer information	1 748	1 883	2 500	2 883	4 440
Мошенничество / Fraud: ст. 159 УК РФ / Art. 159 of the CC of the RF	–	–	90 368	119 485	173 233
ст. 159.3 УК РФ / Art. 159.3 of the CC of the RF	–	–	4 236	16 119	24 560
ст. 159.6 УК РФ / Art. 159.6 of the CC of the RF	–	–	962	676	398
Кража / Theft	–	–	32 668	98 798	144 808
Вымогательство / Extortion	–	–	1 621	2 090	2 425
Незаконные организация и проведение азартных игр / Illegal organization of gambling	–	–	875	842	668

* Составлена по данным МВД России / Based on the data from Russian Ministry of the Interior. URL: http://crimestat.ru/analytics.

** За десять месяцев 2020 г. / For ten months of 2020.

и в то время как степень общественной опасности киберпреступности неуклонно растет, «наибольшая часть киберпреступлений остается за рамками статистики» [8, с. 69].

В Великобритании действует Закон о неправомерном использовании компьютеров 1990 г.[8], который направлен на борьбу с широким спектром компьютерных преступлений. Достаточно иллюстративна британская динамика *компьютерной преступности и мошенничества* (fraud and computer misuse offences), где в последние два года наблюдается прирост около 10 %, а компьютерные преступления и мошенничество в компьютерных сетях составляют около 12–13 % всех правонарушений (табл. 2).

Британская характеристика компьютерных преступлений и мошенничества (прим. 4, Table E2)[9] относит к киберпреступности (cyber crime) только «случаи, когда действия в Интернете или сетях связи имели отношения к любым элементам состава правонарушения». Британские правоохранительные органы сталкиваются с онлайн-преступностью (online crime) и отдельно выделяют такие составы преступлений в Интернете, как домогательство (harassment and stalking), нецензурные публикации (obscene publications), сексуальные преступления в отношении детей (child sexual offences) и шантаж (blackmail). Показатели онлайн-преступности в Англии за период с 2016 по 2018 г. выросли в 2 раза — с 44 832 до 97 538 расследованных фактов.

В ФРГ компьютерная преступность включает в себя компьютерное мошенничество (computerbetrug (ст. 263а УК ФРГ)) и компьютерные преступления в узком смысле, такие как взлом, распространение вредоносных программ и другой опасной информации через компьютерные сети, которые более чем в 60 % случаев также преследуют цели хищения. По данным полиции ФРГ за 2019 г., прирост компьютерной преступности также отражает изменения в структуре преступности (табл. 3). Однако спад общего уровня преступности в Германии более чем на 14 % (с 6,3 млн до 5,4 млн выявленных правонарушений) в период с 2015 по 2019 г. свидетель-

[8] Computer Misuse Act 1990 // OGL. URL: https://www.legislation.gov.uk/ukpga/1990/18/contents.

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

Таблица 2 / Table 2

Динамика состояния и структуры компьютерных преступлений и мошенничества в Англии и Уэльсе в 2016–2020 гг.*

Dynamics of the condition and structure of computer crimes and fraud in England and Wales in 2016–2020

Показатель / Indicator	2016	2017	2018	2019	2020
Число преступлений / Number of crimes	619 152	652 362	638 358	693 421	774 541
Темп прироста, % / Increase rate, %	–	+5,4	–2,2	+8,6	+11,7
Удельный вес, % / Specific weight, %	13,7	13,1	11,5	11,6	12,7
Доля киберпреступности, % / Share of cybercrimes, %	70	68	63	–	–

* Составлена по данным / Based on: Office for national statistics. Year ending June 2020 // OGL. URL: https://www.ons.gov.uk.

Таблица 3 / Table 3

Динамика состояния и структуры компьютерных преступлений в ФРГ в 2015–2019 гг.*

Dynamics of the condition and structure of computer crimes in the FRG in 2015–2019

Показатель / Indicator	2015	2016	2017	2018	2019
Число преступлений / Number of crimes	70 068	107 751	108 510	110 475	123 006
Темп прироста, % / Increase rate, %		+53,7	+0,7	+1,8	+11,3
Удельный вес, % / Specific weight, %	1,1	1,7	1,9	2,0	2,3
Доля компьютерных преступлений (в узком смысле) / Share of computer crimes (in a narrow sense)	45 793	82 649	85 960	87 106	100 514

* Составлена по данным / Based on: Police Crime Statistics 2015–2019 // Bundeskriminalamt. URL: https://www.bka.de/EN/CurrentInformation/PoliceCrimeStatistics/policecrimestatistics_node.html.

ствует, скорее всего, о существенных проблемах в выявлении киберпреступлений. Представляется весьма вероятным значительный рост показателей статистики по киберпреступности в Германии в ближайшие три-четыре года.

Характеристика киберпреступности в ФРГ оценивает сеть Интернет как «инструмент совершения преступлений», что фактически относит все информационные технологии к средствам совершения преступлений.

Во Франции мероприятия по борьбе с киберпреступностью (cybercriminalité) осуществляет Министерство внутренних дел Французской Республики (Ministère de l'Intérieur), которое выработало собственные подходы к пониманию киберпреступности и принципам формирования статистики по правонарушениям в сфере компьютерной информации. Во-первых, посредством социологических опросов было установлено, что за 2016 г. 55 млн французских пользователей сети Интернет столкнулись более чем с 1,2 млн случаев компьютерного мошенничества, что почти в 2 раза больше, чем в 2011 г., затем число латентных правонарушений стабилизировалось и мало меняется[10]. Во-вторых, во Франции отдельно учитываются жалобы на факты киберделиктов в органы жандармерии и жалобы на вредные и опасные ресурсы сети Интернет на платформе Pharos, в функции которой входит гармонизация подхода к киберпреступности в понимании государства и пользователей сети Интернет, а также блокирование зарубежного криминального контента[11]. В-третьих, характеристика киберпреступности во Франции изначально была ориентирована на широкое понимание кибербезопасности и защиту от компьютерных преступлений посредством воспитания правовой культуры пользователей Интернета.

Структура киберпреступности во Франции прослеживается из заявлений о фактах преступлений в органы жандармерии и жалоб на платформе Pharos (табл. 4). Картина криминального поведения в рамках виртуальной реальности во многом сходна с общеевропейской. В частности, мошенничество (escroquerie) в структуре киберпреступности составляет около 75 %, хищение персональных данных (usurpation d'identité) — около 7 %, электронная диффамация (diffamation par voie électronique) — 4 %, отмечается высокая активность в создании платформ для фишинга[12].

В Испании также отмечается устойчивый рост показателей киберпреступности (cibercriminalidad), увеличивается и удельный вес киберпреступлений (с 2,1 % в 2011 г. до 7,0 % в 2018 г.). Из 84 607 зарегистрированных правоохранительными органами Испании киберделиктов в 2018 г. мошенничество (fraude) составляло 50,2 %, распространение вредоносных программ (malware) — 24,2 %, взлом компьютерных программ (intrusión) — 7,7 %; около 80 % киберпреступлений, так же как практически во всех европейских странах, совершено из корыстных побуждений[13].

Сравнительный анализ динамики киберпреступности в России, Великобритании, Германии и Франции (при известной разнице в правовых системах, общем числе выявленных правонарушений, численности населения и

[10] Les défis de la mesure statistique de la cybercriminalité — Revue de la Gendarmerie Nationale // Ministère de l'Intérieur. URL: https://www.interieur.gouv.fr/Actualites/Communiques/L-etat-de-la-menace-liee-au-numerique-en-2019.

[11] Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements (Pharos) // Ibid. URL: https://www.internet-signalement.gouv.fr.

[12] L'état de la menace liée au numérique en 2019 : La Réponse du Ministère de L'intérieur. La Réponse du Ministère de l'intérieur. Paris, 2019. P. 87–88.

[13] Estudio Sobre La Cibercriminalidad En España. Ministerio del Interior, 2018. P. 20–38.

Таблица 4 / Table 4

Динамика состояния и структуры киберпреступлений во Франции в 2015–2019 гг.*
Dynamics of the condition and structure of cybercrime in France in 2015–2019

Показатель / Indicator	2015	2016	2017	2018	2019
Число преступлений / Number of crimes	21 896	42 934	63 138	67 890	77 000
Темп прироста, % / Increase rate, %	–	+51	+32	+7	+12
Удельный вес, % / Specific weight, %	1,1	1,7	2,1	2,2	2,7
Заявления на Pharos / Reports in Pharos	188 000	170 712	153 586	163 723	228 545

* Составлена по данным / Based on: Rapport — l'état de la menace liée au numérique en 2019 // Ministère de l'intérieur. URL: https://www.interieur.gouv.fr/Actualites/Communiques/L-etat-de-la-menace-liee-au-numerique-en-2019.

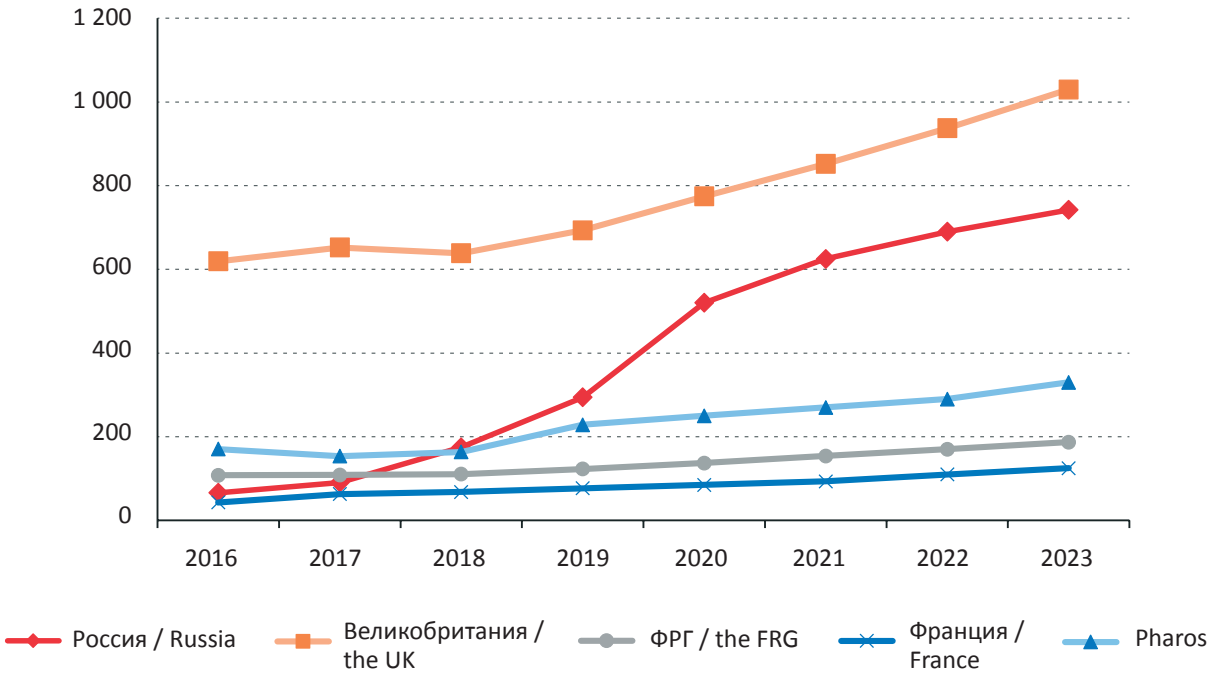
уровне экономического развития) достаточно ясно демонстрирует, что российские правоохранительные органы довольно поздно отреагировали на угрозы киберпреступности, однако в период 2018–2020 гг. вышли на тот уровень выявления и раскрываемости киберпреступлений, который в полной мере соответствует правоприменительной практике в рамках Совета Европы.

При существующем общем уровне преступности в России (около 2 млн преступлений в год) число выявленных киберпреступлений, как представляется, не может превысить 750 тыс. к 2023 г., что предполагает рост числа киберпреступлений на 10–12 % в год. В результате таких изменений в структуре преступности России киберпреступность приобретет максимально возможный удельный вес в 35 %, при этом защищенность пользователей компьютерных систем останется на относительно низком уровне. В 2020 г. 63,5 млн британских пользователей Интернета столкнулись более чем с 770 тыс. выявленных фактов компьютерных преступлений и мошенничества, и, надо полагать, 116,3 млн российских пользователей Интернета ежегодно сталкиваются более чем с 1,4 млн аналогичных правонарушений, а 79 млн немецких пользователей Сети в течение года оказываются жертвами как минимум 950 тыс. потенциально выявляемых компьютерных правонарушений (в широком смысле) различной степени тяжести.

Прогноз динамики киберпреступности на среднесрочную перспективу методом экстраполяции (рис.) актуален только при условии неизменности уголовной политики государств в области цифровых технологий. Гармонизация уголовно-правового подхода к киберделиктам будет способствовать тому, что удельный вес киберпреступности в государствах — членах Совета Европы не будет превышать 25–30 %, что связано с предполагаемым прогрессом в выявлении и пресечении компьютерных преступлений.

Прогноз динамики киберпреступности учитывает актуальное состояние киберпреступности, темпы ее прироста и выявленный уровень латентности. Исходя из современных подходов к прогнозированию динамики преступности, основанных на демографических показателях и сетевой активности [9], есть основания полагать, что в ближайшие три года рост киберпреступности составит 8–12 % в год при сохранении текущего уровня цифровизации в государствах — членах Совета Европы.

Рост киберпреступности связан с широкими возможностями доступа граждан к сети Интернет. Это не только изменило правовую культуру



Динамика киберпреступности в России, Англии, Германии и Франции в 2016–2023 гг., тыс. преступлений

Dynamics of cybercrimes in Russia, the UK, Germany and France in 2016–2023, th. crimes

населения, но и значительно затруднило реализацию традиционных полицейских стратегий предупреждения преступности [10]. Выявление и пресечение киберпреступлений в большей степени зависят от поведения жертв, чем от реального вреда компьютерных преступлений [11]. И поскольку, как справедливо отмечает А.Г. Волеводз, «законодательное регулирование киберпространства в одной отдельно взятой стране вряд ли возможно» [12, с. 19], постольку правовая культура пользователей Интернета, позволяющая им участвовать в международном общении, будет определять характер борьбы с киберпреступностью. Правоприменение, однако, будет по-прежнему сталкиваться с традиционными для трансграничной преступности проблемами доказывания обстоятельств дела и размера причиненного вреда.

Проблемы гармонизации уголовного законодательства государств — членов Совета Европы в области киберпреступности весьма ясно отражают подходы к статистике по киберпреступности, воспринятые на национальном уровне. В Совете Европы сложился лишь относительный консенсус в вопросе признания государствами общественной опасности некоторых материальных составов компьютерных преступлений и мошенничества в Интернете, однако вопросы уголовно-процессуального характера вызывают острые противоречия.

Россия участвует в Совете Европы, однако не участвует в Будапештской конвенции 2001 г. Отмена распоряжения Президента РФ «О подписании Конвенции о киберпреступности» от 15 ноября 2005 г. № 557-рп[14] обусловлена тем, что «положения пункта «b» ст. 32 Конвенции сформулированы таким образом, что… могут нанести ущерб суверенитету и национальной безопасности государств-участников, правам и законным интересам их граждан и юридических лиц»[15].

Спорные положения Будапештской конвенции 2001 г. позволяют государствам «получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их» при определенных обстоятельствах (п. «b» ст. 32), что может быть истолковано как юридическое основание вмешательства в дела, входящие во внутреннюю компетенцию государства — участника соглашения. Частные процессуальные вопросы нередко препятствуют имплементации международных соглашений в национальную правовую систему, и, как следует из политического скандала вокруг иностранного вмешательства в выборы президента США [13; 14], вопросы кибербезопасности определенно могут затрагивать национальные интересы государств.

Неприсоединение России к Будапештской конвенции 2001 г. оставляет открытым вопрос о соответствии норм ее национального уголовного законодательства международным стандартам и предполагает изыскание соответствующих национальным интересам форматов международного противодействия киберпреступности. В этом контексте особое значение имеет участие России в работе Шанхайской организации сотрудничества (ШОС).

Хартия ШОС от 6 июня 2002 г. нацелена на борьбу «с незаконным оборотом наркотиков и оружия, другими видами транснациональной преступной деятельности» (ст. 1), а значит, в полной мере относится к киберпреступности. Секретарь Совета безопасности РФ Н.П. Патрушев по итогам встречи в рамках ШОС 15 сентября 2020 г. заявил, что в рамках организации возможно принятие соглашения по вопросам информационной безопасности. Представляется, что разработка Конвенции ШОС о киберпреступности на основе подвергнутых необходимой корректировке положений Будапештской конвенции 2001 г. будет в наибольшей степени отвечать интересам обеспечения региональной информационной безопасности и поспособствует гармонизации российского уголовного законодательства.

Классификация материальных составов киберпреступлений в документах Совета Европы не вызывает принципиальных разногласий, однако несколько отличается от структуры статистических отчетов правоохранительных органов. Будапештская конвенция 2001 г. выделяет преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (ст. 2–6), правонарушения, связанные с использованием компьютерных средств (ст. 7–8), правонарушения, связанные с содержанием данных (ст. 9), правонарушения, свя-

[14] О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности» : распоряжение Президента РФ от 22 марта 2008 г. № 144-рп. URL: http://www.kremlin.ru/acts/bank/27059.

[15] О подписании Конвенции о киберпреступности : распоряжение Президента РФ от 15 нояб. 2005 г. № 557-рп // Собрание законодательства РФ. 2005. № 47. Ст. 4929.

занные с нарушением авторского права и смежных прав (ст. 10).

Классификация киберпреступлений демонстрирует, что субъекты, не имеющие специальных знаний в области технологий компьютерного программирования, могут быть причастны к совершению тяжких киберпреступлений. Так, в частности, при освоении компьютерных сетей террористическими организациями возникает опасная разновидность компьютерной преступности — кибертерроризм [8, с. 67], при этом очевидно, что кибертерроризм предполагает прежде всего вербовку аудитории социальных сетей и пропаганду насильственного экстремизма [15, p. 238].

Гармонизация российского законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы может позволить устранить ряд проблем российской правоприменительной практики касательно мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ), доля которого, судя по данным российской статистики, постепенно снижается (см. табл. 1).

Во-первых, квалификация хищения по ст. 159.6 УК РФ для преступника, осуществлявшего незаконный взлом ресурсов компьютерной сети (хакера), влечет квалификацию деяния по соответствующему составу гл. 28 УК РФ (идеальная совокупность преступлений [16, с. 151]), хотя такая правовая логика небесспорна [17, с. 90].

Во-вторых, постановление Пленума Верховного Суда РФ «О судебной практике по делам о мошенничестве, присвоении и растрате» от 30 ноября 2017 г. № 48 разъясняет, что по смыслу ст. 159.6 УК РФ вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается «целенаправленное воздействие программных… средств на серверы, средства вычислительной техники (компьютеры)…» (п. 20). Фактически «если хищение чужого имущества… осуществляется путем распространения заведомо ложных сведений… (например, создание поддельных сайтов…), то такое мошенничество следует квалифицировать по статье 159, а не 159.6 УК РФ» (п. 21). Представляется, что создание поддельных сайтов является формой фишинга — типичного modus operandi киберпреступников и по своей сути является мошенничеством в сфере компьютерной информации, что отражает статистика применения общей статьи 159 УК РФ по киберпреступности.

Законодатель и органы судебной власти России трактуют использование компьютерных сетей как квалифицирующий признак по ряду составов преступлений. В частности, постановление Пленума Верховного Суда РФ «О судебной практике по уголовным делам о преступлениях экстремистской направленности» от 28 июня 2011 г. № 11 отмечает возможность привлечения к уголовной ответственности за публичные призывы к осуществлению экстремистской деятельности в Интернете (ч. 2 ст. 280 УК РФ). В других случаях компьютерные сети признаются органами судебной власти средством совершения преступления. Так, постановление Пленума Верховного Суда РФ «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности» от 4 декабря 2014 г. № 16 поясняет, что «развратными могут признаваться и такие действия, при которых непосредственный физический контакт с телом потерпевшего лица отсутствовал, включая действия, совершенные с использованием сети Интернет» (п. 17). По нашему мнению, криминализация *распространения опасной информации в сетях компьютерной связи* представляется перспективным способом гармонизации уголовного законодательства в рамках Совета Европы и ШОС.

Практика борьбы с киберпреступностью в государствах — членах Совета Европы сталкивается с социально-политическими противоречиями между интересами различных групп населения [18–23], а решения этой проблемы отражают специфику национальных правовых систем и не всегда приемлемы для прямой рецепции.

Европейский опыт демонстрирует технологическую зависимость всех законодательных и политических инициатив в виртуальном мире [14; 24; 25]. При реализации законодательной политики ряд стран Совета Европы следует стратегии снижения вреда (в том числе от запретительных мер), основанной на партнерских отношениях между государственным и частным секторами для защиты «цифровой экосистемы» [26, p. 97]. На уровне Европейского союза проводится гармонизация национального уголовного законодательства, устанавливающего ответственность за преступления в компьютерных сетях [27], однако такие «неюридические факторы, как национальная безопасность, политика, экономика и общественное мнение… стимулируют

спонтанное внедрение европейской правовой базы» [28, p. 339]. При этом высокий уровень «теневого мошенничества» свидетельствует о том, что «оценка предупреждения преступности, основанная исключительно на полицейской статистике, может быть неадекватной» [29].

С одной стороны, в России и Великобритании защита компьютерных систем от несанкционированного доступа имеет общий объект преступного посягательства, который связан с использованием компьютерных технологий [30]. С другой стороны, в отличие от гл. 28 УК РФ «Преступления в сфере компьютерной информации», которая защищает компьютерные системы от причинения им вреда, нормы британского права о киберпреступности в большей степени ориентированы на защиту пользователей компьютерных сетей.

Британский законодатель, например, разъясняет, что типичные составы компьютерных преступлений связаны с несанкционированным доступом к компьютерным материалам или несанкционированной модификацией компьютерных программ. Это: 1) взлом, включая получение доступа к аккаунтам в социальных сетях и паролям от электронной почты; 2) фишинг — злоупотребление доверием пользователей с целью получения паролей, информации о безопасности и личных данных; 3) создание вредоносного программного обеспечения, включая программы-вымогатели различного рода [31, p. 1583–1584], распределенные атаки типа «отказ в обслуживании» (DDOS) на веб-сайты, которые также сопровождаются вымогательством[16].

Теоретическое обоснование исследования киберпреступности методом включенного наблюдения предполагает, что нарушение прав и свобод пользователей компьютерных сетей обусловлено экономическими интересами, и большинство киберпреступников действуют из корыстных мотивов, вовлекая потенциальных жертв в сетевое общение.

В силу того что многие сегменты сети Интернет находятся под юрисдикцией США, «решения Верховного суда [США] вызывают отголоски далеко за пределами… судебной системы» [32, p. 137]. Правоприменение в США подтверждает, вывод из статистики по европейской киберпреступности о том, что актуальной проблемой в современном Интернете является мошенничество. Идея расширения возможностей правоохранительных органов США в борьбе с сайтами, зарегистрированными за рубежом, нарушением авторских прав в Интернете и незаконным оборотом контрафактных товаров зашла в тупик после того, как в 2012 г. законодательные инициативы SOPA (Stop Online Piracy Act — Закон о борьбе с пиратством в Интернете) и PIPA (Protect IP Act) были отвергнуты и стало очевидно, что экономические интересы сетевых корпораций подчинены системообразующим принципам виртуальной среды, где доминирует свобода слова и инновации, а всякая интернет-цензура встретит жесткий протест со стороны сетевого сообщества [20; 33].

Борьба с киберпреступностью, по мнению С. де Сильва (Sam De Silva), предполагает противодействие кибератакам [34], однако преступность XXI в. не всегда подчиняется логике банального грабежа и риски причинения вреда правам и свободам человека через злоупотребление корпорациями своим технологическим превосходством в существенной степени недооценены [35]. Еще в начале XXI в. Г. Ластовка (Gregory Lastowka) и Д. Хантер (Dan Hunter), прогнозируя возможности использования искусственного интеллекта в противоправных целях, развивали концепцию виртуальной преступности [36; 37].

Прогрессивные российские исследования подтверждают, что «государство обязано не игнорировать «виртуальные проблемы», а заниматься ими вплотную, в противном случае устанавливать «правила игры» начнут частные компании — производители онлайновых миров» [38, с. 30]. В виртуальном пространстве обман не становится нормой, но способы маскировки мошенничества под творческие решения, как и информационное противоборство, приобретают характер социально-политической международной технологии [39; 40]. С одной стороны, техническое понимание принципиальных отличий «креативного» цифрового терроризма от классических преступлений экстремистского характера отражает необходимость разработки специальных норм для обеспечения законности в глобальном информационном пространстве [41]. С другой стороны, опасность творческих проектов лишь косвенно связана с их технической реализацией, так как виртуальная реальность может нести новые социально-психологические и экономические угрозы [18].

В российской юридической науке признается, что «существующие правовые механизмы

[16] URL: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime.

не всегда реализуемы для интернет-отношений» [42, с. 40] и законодательство недостаточно эффективно защищает права потребителей программного обеспечения компьютеров [43]. Очевидно, что киберпреступность внедряется в самые разные организационные структуры, ориентируясь на получение прибыли за счет нарушения прав широких слоев населения [44; 45]. Обеспечение доступа к потенциальным жертвам преступлений нередко осуществляется за счет создания в Интернете различных социальных сетей, эмпирические данных внутри которых достаточно сложно собрать [46].

В классификация компьютерных преступлений на основе технологических особенностей реализации преступного замысла, предложенной М. Макгвайром (Michael McGuire), выделяется телепреступность и микропреступность [11]. Телепреступность предполагает трансляцию опасного контента через сети цифровой связи и представляет особую опасность в силу того, что число жертв таких правонарушений может исчисляться сотнями тысяч. Некоторые тяжкие телепреступления, которые причинили вред критической информационной инфраструктуре, так и не были раскрыты, несмотря на пристальное внимание мирового сообщества и все усилия правоохранительных органов. Например, создатели вируса WannaCry не были изобличены и привлечены к ответственности [47].

Для выявления фактов телепреступлений за виртуальными системами легче наблюдать при их открытом характере и ограниченном размере, так как именно там мошенники теряют бдительность и рассчитывают на безнаказанность в силу малозначительности правонарушений. Для инициативных научных исследований рационален выбор сетей размером в 3 000–5 000 тыс. пользователей онлайн с анонимной регистрацией и признаками мошенничества со стороны оператора проекта. Признаки мошенничества, как правило, проявляются в обоснованных жалобах пользователей сетевого ресурса. Очевидно, что именно жалобы потерпевших могут позволить выявить мошенничество и охарактеризовать modus operandi виртуального делинквента.

Исследование интерактивного сетевого проекта проводилось в течение 2019 — начала 2020 г. за счет собственных средств методом включенного наблюдения и показало, что некоторые творческие решения в интернет-бизнесе действительно могут представлять существенную общественную опасность и обладают рядом признаков компьютерного мошенничества[17]. В содержательном плане наблюдаемый авторами настоящего исследования игровой интерактивный проект обладал такой особенностью, как создание игровой квазивалюты, курс которой был увязан с реальной валютой (изначально российским рублем, а затем долларом США). Любое действие в виртуальном игровом пространстве неизменно приобретало денежное содержание, и у пользователей интерактивного приложения складывалась иллюзия, что они распоряжаются существенными имущественными активами. Целевая аудитория проекта оказалась многонациональной, активно пользовалась международными денежными переводами.

В юридическом аспекте реализации проекта наблюдались явные признаки состава преступления, предусмотренного ст. 171.2 УК РФ «Незаконные организация и проведение азартных игр». Во-первых, пользователи регулярно осуществляли различные платежные операции, а также приобретали за реальные деньги «внутриигровое имущество», которым распоряжались, делая ставки в игре. Во-вторых, инициативы администрации по изменению правил игры явно стимулировали игроков к приобретению через электронные платежные системы игровой валюты за реальные деньги, при этом платеж объявлялся оператором сайта добровольным пожертвованием и ничего не гарантировал.

В течение шести месяцев наблюдения за сетевыми сообществами внутри проекта у большинства активных игроков проявились признаки игровой зависимости, многие испытывали явный стресс, угрожая расправой через форум проекта друг другу и администрации игрового ресурса. Поскольку пользователи не могли предвидеть характер будущих изменений правил игры оператором проекта, у них возникала обоснованная уверенность в том, что их систематически обманывают. «Пожертвования» со стороны отдельных игроков, как правило, не достигали крупного размера в смысле примеч. 4 к ст. 158 УК РФ, однако доход оператора проекта очевидно превышал крупный размер в смысле примеч. 2 к ст. 171.2 УК РФ.

Основываясь на презумпции невиновности, можно констатировать, что использование пробелов в действующем законодательстве о сборе пожертвований через сетевые ресурсы и реализации интеллектуальных прав на интерактивные

[17] Объект исследования — компания novaArt, проект Xcraft. URL: https://xcraft.ru.

произведения позволяет злоупотреблять доверием пользователей интерактивных приложений, присваивая «пожертвования» вполне легально через электронные переводы денежных средств под удобную национальную юрисдикцию.

Наблюдение за функционированием ресурсов Интернета показывает существование коммерческих проектов, сомнительных в плане законности получения доходов операторами, разработчиками и правообладателями. Виртуальная преступность, приобретая международный характер [48], требует особых подходов к расследованию фактов правонарушений [49] и защите прав пользователей компьютерных сетей [50].

Киберпреступники, совершая экономические преступления в виртуальном мире, маскируют свои действия под реализацию товаров, услуг и интеллектуальных прав, а также под добровольные пожертвования граждан на развитие их проектов, что следует учитывать в процессе гармонизации законодательства о противодействии компьютерной преступности.

Подведем итоги. Итак, уровень гармонизации уголовного законодательства государств — членов Совета Европы определяется их национальными интересами, а состояние киберпреступности характеризуется особенностями уголовного правоприменения на национальном уровне. Положения российского уголовного законодательства в отношении преступлений в сфере компьютерной информации (гл. 28 УК РФ) в процессе их гармонизации с правовыми стандартами Совета Европы необходимо более адресно сориентировать на защиту прав пользователей компьютерных сетей, признав фишинг, вымогательство и организацию азартных игр в компьютерных сетях составами киберпреступлений.

В теоретическом плане представляется правильным рассматривать киберпреступность в понимании, предложенном Будапештской конвенцией 2001 г., согласовав на международном уровне, в форматах ШОС и Совета Европы, совместные усилия по борьбе с мошенничеством в Интернете.

На политическом уровне при гармонизации российского уголовного законодательства следует учитывать членство России в Совете Европы и ШОС. С учетом потребностей в защите государственного суверенитета и организации противодействия организованной преступности в Интернете вполне рациональна перспектива разработки Конвенции ШОС о противодействии киберпреступности, которая создаст эффективный механизм взаимодействия с Интерполом и Европолом (например, аналогичный французской платформе Pharos) для обеспечения международной информационной безопасности.

В методологическом плане гармонизация законодательства о противодействии киберпреступности предполагает выработку государствами совместно с лидерами сетевого сообщества принципов криминализации и выявления фактов нарушения прав пользователей сетевых ресурсов. Энергия виртуальных вещей (Интернет вещей) [51] позволяет злоумышленникам вводить пользователей Интернета в заблуждение посредством интерактивных творческих проектов.

Противодействие компьютерной преступности должно основываться на методе включенного наблюдения за экономическими практиками Интернета, где развивается латентная преступность [10; 29]. При этом знание фактического уровня киберпреступности может, как в случае преступлений против фундаментальных прав человека, не только изменить подход к выявлению скрытых преступлений, повысить их реальный уровень в зарегистрированной части и уровень реального реагирования на них со стороны правоохранительных органов [52], но и способно обеспечить гармонизацию политики в Совете Европы по криминализации или декриминализации киберделиктов.

Гармонизация уголовного законодательства предполагает взаимодействие правоохранительных органов и институтов гражданского общества в виртуальном пространстве при противодействии таким формам криминального поведения, как вербовка экстремистов через социальные сети, фишинг и организация азартных игр, которые носят трансграничный и анонимный характер и могут быть глубоко законспирированы сетевыми ресурсами Даркнета.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing / ed. D.S. Wall, M.L. Williams. — London : Routledge, 2014. — 168 p.

2. Wall D.S. Cybercrime: The Transformation of Crime in the Information Age / D.S. Wall. — Cambridge : Polity, 2007. — 288 p.

3. Wagen W. van der. From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks / W. van der Wagen, W. Pieters. — DOI: 10.1093/bjc/azv009 // British Journal of Criminology. — 2015. — Vol. 55, iss. 3. — P. 578–595.

4. Selling Drugs on Darkweb Cryptomarkets: Differentiated Pathways, Risks and Rewards / J. Martin, R. Munksgaard, R. Coomber [et al.] — DOI: 10.1093/bjc/azz075 // British Journal of Criminology. — 2020. — Vol. 60, iss. 3. — P. 559–578.

5. Aas K.F. «Crimmigrant» bodies and bona fide travelers: Surveillance, citizenship and global governance / K.F. Aas. — DOI: 10.1177/1362480610396643 // Theoretical Criminology. — 2011. — Vol. 15, iss. 3. — P. 331–346.

6. Skinner C.P. Cybercrime in the Securities Market: Is U.C.C. Article 8 Prepared? / C.P. Skinner. — DOI: 10.2139/ssrn.1952955 // North Carolina Law Review Addendum. — 2012. — Vol. 90. — P. 132–157.

7. Mayer J. Cybercrime Litigation / J. Mayer // University of Pennsylvania Law Review. — 2016. — Vol. 164, iss. 6. — P. 1453–1507.

8. Журавленко Н.И. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере / Н.И. Журавленко, Л.Е. Шведова // Общество и право. — 2015. — № 3 (53). — С. 66–70.

9. Once Upon a Crime: Towards Crime Prediction from Demographics and Mobile Data / A. Bogomolov, B. Lepri, J. Staiano [et al.]. — DOI: 10.1145/2663204.2663254 // Computer Science, Physics : Proceedings of the 16th International Conference on Multimodal Interaction. — Istanbul, 2014. — P. 427–434.

10. Caneppele S. Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes / S. Caneppele, M.F. Aebi. — DOI: 10.1093/police/pax055 // Policing: A Journal of Policy and Practice. — 2019. — Vol. 13, iss. 1. — P. 66–79.

11. McGuire M. Technology, Crime, and Justice: The Question Concerning Technomia / M. McGuire. — London : Routledge, 2012. — 284 p.

12. Волеводз А.Г. Конвенция о киберпреступности: новации правового регулирования / А.Г. Волеводз // Правовые вопросы связи. — 2007. — № 2. — С. 17–25.

13. Justice J.W. Hacked: Defining the 2016 Presidential Election in the Liberal Media / J.W. Justice, B.J. Bricker. — DOI: 10.14321/rhetpublaffa.22.3.0389 // Rhetoric and Public Affairs. — 2019. — Vol. 22, iss. 3. — P. 389–420.

14. Brenner S.W. Cyberthreats and the Decline of the Nation-State / S.W. Brenner. — London : Routledge, 2014. — 182 p.

15. Ammar J. Cyber Gremlin: social networking, machine learning and the global war on Al-Qaida-and IS-inspired terrorism / J. Ammar. — DOI: 10.1093/ijlit/eaz006 // International Journal of Law and Information Technology. — 2019. — Vol. 27, iss. 3. — P. 238–265.

16. Черненко Т.Г. Квалификация совокупности преступлений / Т.Г. Черненко // Вестник Омского университета. Сер.: Право. — 2014. — № 1 (38). — С. 148–162.

17. Энгельгардт А.А. О понимании мошенничества в сфере компьютерной информации / А.А. Энгельгардт // Вестник Московского университета МВД России. — 2016. — № 8. — С. 84–90.

18. Противодействие киберпреступности в аспекте обеспечения национальной безопасности / П.В. Агапов, С.В. Борисов, Д.В. Вагурин [и др.]. — Москва : Юнити, 2014. — 512 с.

19. Cyber Criminology: Exploring Internet Crimes and Criminal Behavior / ed. K. Jaishankar. — London : CRC Press, 2011. — 461 p.

20. Hacking Politics: How Geeks, Progressives, the Tea Party, Gamers, Anarchists and Suits Teamed up to Defeat SOPA and Save the Internet / ed. D. Moon, P. Ruffini, D. Segal. — New York : OR Books, 2013. — 316 p.

21. Leman-Langlois S. Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace commercial / S. Leman-Langlois. — DOI: 10.7202/013126ar // Criminologie. — 2006. — Vol. 39, № 1. — P. 63–81.

22. Weber A.M. The Council of Europe's Convention on Cybercrime / A.M. Weber // Berkeley Technology Law Journal. — 2003. — Vol. 18, iss. 1. — P. 425–446.

23. Williams M. Virtually Criminal: Crime, Deviance and Regulation Online / M. Williams. — London : Routledge, 2006. — 208 p.

24. Gercke M. Europe's legal approaches to cybercrime / M. Gercke. — DOI: 10.1007/s12027-009-0132-5 // ERA Forum. — 2009. — Vol. 10, iss. 3. — P. 409–420.

25. Yar M. Cybercrime and Society / M. Yar. — DOI: 10.4135/9781446212196. — London : Sage, 2006. — 232 p.

26. Dupont B. Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime / B. Dupont. — DOI: 10.1007/s10611-016-9649-z // Crime, Law and Social Change. — 2017. — Vol. 67, iss. 1. — P. 97–116.

27. Buono L. Fighting cybercrime between legal challenges and practical difficulties: EU and national approaches / L. Buono. — DOI: 10.1007/s12027-016-0432-5 // ERA Forum. — 2016. — Vol. 17, iss. 3. — P. 343–353.

28. Calderoni F. The European legal framework on cybercrime: striving for an effective implementation / F. Calderoni. — DOI: 10.1007/s10611-010-9261-6 // Crime, Law and Social Change. — 2010. — Vol. 54, iss. 5. — P. 339–357.

29. Kemp S. The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain / S. Kemp, F. Miró-Llinares, A. Moneva. — DOI: 10.1007/s10610-020-09439-2 // European Journal on Criminal Policy and Research. — 2020. — Vol. 26, iss. 3. — P. 293–312.

30. Карамнов А.Ю. Законодательство Великобритании о преступлениях в сфере компьютерной информации / А.Ю. Карамнов, М.Ю. Дворецкий // Социально-экономические явления и процессы. — 2013. — № 8 (54). — С. 164–167.

31. The phenomenon of cyber-crime and fraud victimization in online shop / M.D.T.P. Nasution, A.P.U. Siahaan, Y. Rossanty, S. Aryza // International Journal of Civil Engineering and Technology. — 2018. — Vol. 9, iss. 6. — P. 1583–1592.

32. Fisher J.L. A Clinic's Place in the Supreme Court Bar / J.L. Fisher. — DOI: 10.2139/ssrn.1921430 // Stanford Law Review. — 2013. — Vol. 65, iss. 1. — P. 137–201.

33. Kapczynski A. Intellectual Property's Leviathan / A. Kapczynski // Law and Contemporary Problems. — 2015. — Vol. 77, № 4. — P. 131–145.

34. De Silva S. Cyber Crime and the Law / S. De Silva. — DOI: 10.1093/itnow/bww101 // ITNOW. — 2016. — Vol. 58, iss. 4. — P. 28–29.

35. Cooper M. How Cyber Crime Damages Lives / M. Cooper. — DOI: 10.1093/itnow/bwaa016 // ITNOW. — 2020. — Vol. 62, iss. 1. — P. 36–37.

36. Lastowka G. Virtual Crimes / G. Lastowka, D. Hunter // New York Law School Law Review. — 2004. — Vol. 49, iss. 1. — P. 293–316.

37. Lastowka G. The Laws of the Virtual Worlds / G. Lastowka, D. Hunter. — DOI: 10.15779/Z386H7P // California Law Review. — 2004. — Vol. 92, iss. 1. — P. 1–74.

38. Батурин Ю.М. Что делает виртуальные преступления реальными / Ю.М. Батурин, С.В. Полубинская // Труды Института государства и права РАН. — 2018. — Т. 13, № 2. — С. 9–35.

39. D'Aspremont J. Cyber Operations and International Law: An Interventionist Legal Thought / J. d'Aspremont. — DOI: 10.1093/jcsl/krw022 // Journal of Conflict and Security Law. — 2016. — Vol. 21, iss. 3. — P. 575–593.

40. Кириленко В.П. Политические технологии и международный конфликт в информационном пространстве Балтийского региона / В.П. Кириленко, Г.В. Алексеев. — DOI: 10.5922/2079-8555-2018-4-2 // Балтийский регион. — 2018. — Т. 10, № 4. — С. 20–38.

41. Taylor R.W. Digital Crime and Digital Terrorism / R.W. Taylor, E.J. Fritsch, J. Liederbach. — New York : Prentice Hall Press, 2014. — 416 p.

42. Жарова А.К. Маршрутизация и IP для обеспечения правового регулирования интернет-отношений / А.К. Жарова. — DOI: 10.28995/2686-679X-2019-2-32-42 // Вестник РГГУ. Сер.: Информатика. Информационная безопасность. Математика. — 2019. — № 2. — С. 32–42.

43. Zharova A. Ensuring the Information Security of Information Communication Technology Users in Russia / A. Zharova. — DOI: 10.5281/zenodo.3698141 // International Journal of Cyber Criminology. — 2019. — Vol. 13, iss. 2. — P. 255–269.

44. Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime / R.G. Broadhurst, P. Grabosky, M. Alazab, S. Chon. — DOI: 10.2139/ssrn.2345525 // International Journal of Cyber Criminology. — 2014. — Vol. 8, iss. 1. — P. 1–20.

45. Leukfeldt E.R. Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime / E.R. Leukfeldt, A. Lavorgna, E.R. Kleemans. — DOI: 10.1007/s10610-016-9332-z // European Journal on Criminal Policy and Research. — 2017. — Vol. 23, iss. 3. — P. 287–300.

46. Lavorgna A. Cyber-organised crime. A case of moral panic? / A. Lavorgna. — DOI: 10.1007/s12117-018-9342-y // Trends in Organized Crime. — 2019. — Vol. 22, iss. 4. — P. 357–374.

47. Kettemann M.C. Ensuring Cybersecurity through International Law / M.C. Kettemann // Revista Española de Derecho Internacional. — 2017. — Vol. 69, iss. 2. — P. 281–290.

48. Номоконов В.А. Киберпреступность: прогнозы и проблемы борьбы / В.А. Номоконов, Т.Л. Тропина // Библиотека криминалиста. — 2013. — № 5 (10). — С. 148–160.

49. Walden I. Computer Crimes and Digital Investigations / I. Walden. — Oxford : Oxford Univ. Press, 2016. — 600 p.

50. Reep-van den Bergh C.M.M. Victims of cybercrime in Europe: a review of victim surveys / C.M.M. Reep-van den Bergh, M. Junger. — DOI: 10.1186/s40163-018-0079-3 // Crime Science. — 2018. — Vol. 7, iss. 1. — URL: https://crimesciencejournal.biomedcentral.com/track/pdf/10.1186/s40163-018-0079-3.pdf.

51. Mylrea M. Smart energy-internet-of-things opportunities require smart treatment of legal, privacy and cybersecurity challenges / M. Mylrea. — DOI: 10.1093/jwelb/jwx001 // The Journal of World Energy Law & Business. — 2017. — Vol. 10, iss. 2. — P. 147–158.

52. Репецкая А.Л. Убийства в России: методика определения латентного массива / А.Л. Репецкая. — DOI: 10.17223/22253513/32/5 // Вестник Томского государственного университета. Право. — 2019. — № 32. — С. 55–68.

REFERENCES

1. Wall D.S., Williams M.L. (eds.). *Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing*. London, Routledge, 2014. 168 p.

2. Wall D.S. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, Polity, 2007. 288 p.

3. Wagen W. van der, Pieters W. From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks. *British Journal of Criminology*, 2015, vol. 55, iss. 3, pp. 578–595. DOI: 10.1093/bjc/azv009.

4. Martin J., Munksgaard R., Coomber R., Demant J., Barratt M.J. Selling Drugs on Darkweb Cryptomarkets: Differentiated Pathways, Risks and Rewards. *British Journal of Criminology*, 2020, vol. 60, iss. 3, pp. 559–578. DOI: 10.1093/bjc/azz075.

5. Aas K.F. «Crimmigrant» bodies and bona fide travelers: Surveillance, citizenship and global governance. *Theoretical Criminology*, 2011, vol. 15, iss. 3, pp. 331–346. DOI: 10.1177/1362480610396643.

6. Skinner C.P. Cybercrime in the Securities Market: Is U.C.C. Article 8 Prepared? *North Carolina Law Review Addendum*, 2012, vol. 90, pp. 132–157. DOI: 10.2139/ssrn.1952955.

7. Mayer J. Cybercrime Litigation. *University of Pennsylvania Law Review*, 2016, vol. 164, iss. 6, pp. 1453–1507.

8. Zhuravlevko N.I., Shvedova L.E. Problems of Fight against Cybercrime and Future Directions of International Cooperation in this Field. *Obshchestvo i pravo = Society and Law*, 2015, no. 3 (53), pp. 66–70. (In Russian).

9. Bogomolov A., Lepri B., Staiano J., Oliver N., Pianesi F., Pentland A. Once Upon a Crime: Towards Crime Prediction from Demographics and Mobile Data. *Computer Science, Physics*. Proceedings of the 16th International Conference on Multimodal Interaction. Istanbul, 2014, pp. 427–434. DOI: 10.1145/2663204.2663254.

10. Caneppele S., Aebi M.F. Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes. *Policing: A Journal of Policy and Practice*, 2019, vol. 13, iss. 1, pp. 66–79. DOI: 10.1093/police/pax055.

11. McGuire M. *Technology, Crime, and Justice: The Question Concerning Technomia*. London, Routledge, 2012. 284 p.

12. Volevodz A.G. Cybercrime Convention: Novelties of Legal Regulation. *Pravovye voprosy svyazi = Legal Issues of Communications*, 2007, no. 2, pp. 17–25. (In Russian).

13. Justice J.W., Bricker B.J. Hacked: Defining the 2016 Presidential Election in the Liberal Media. *Rhetoric and Public Affairs*, 2019, vol. 22, iss. 3, pp. 389–420. DOI: 10.14321/rhetpublaffa.22.3.0389.

14. Brenner S.W. *Cyberthreats and the Decline of the Nation-State*. London, Routledge, 2014. 182 p.

15. Ammar J. Cyber Gremlin: social networking, machine learning and the global war on Al-Qaida-and IS-inspired terrorism. *International Journal of Law and Information Technology*, 2019, vol. 27, iss. 3, pp. 238–265. DOI: 10.1093/ijlit/eaz006.

16. Chernenko T.G. Qualification of Crimes Aggregate. *Vestnik Omskogo universiteta. Seriya: Pravo = Herald of Omsk University. Series: Law*, 2014, no. 1 (38), pp. 148–162. (In Russian).

17. Engelgardt A.A. Understanding of Fraud in the Sphere of Computer Information. *Vestnik Moskovskogo universiteta MVD Rossii = Bulletin of Moscow University of the Ministry of Internal Affairs of Russia*, 2016, no. 8, pp. 84–90. (In Russian).

18. Agapov P.V., Borisov S.V., Vagurin D.V., Korenyuk A.L., Merkurev V.V. *Protivodeistvie kiberprestupnosti v aspekte obespecheniya natsional'noi bezopasnosti* [Counteracting Cybercrime in the Light of Ensuring National Security]. Moscow, Yuniti Publ., 2014. 512 p.

19. Jaishankar K. (ed.). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. London, CRC Press, 2011. 461 p.

20. Moon D., Ruffini P., Segal D. (eds.). *Hacking Politics: How Geeks, Progressives, the Tea Party, Gamers, Anarchists and Suits Teamed up to Defeat SOPA and Save the Internet*. New York, OR Books, 2013. 316 p.

21. Leman-Langlois S. Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace commercial. *Criminologie*, 2006, vol. 39, no. 1, pp. 63–81. (In French).

22. Weber A.M. The Council of Europe's Convention on Cybercrime. *Berkeley Technology Law Journal*, 2003, vol. 18, iss. 1, pp. 425–446.

23. Williams M. *Virtually Criminal: Crime, Deviance and Regulation Online*. London, Routledge, 2006. 208 p.

24. Gercke M. Europe's legal approaches to cybercrime. *ERA Forum*, 2009, vol. 10, iss. 3, pp. 409–420. DOI: 10.1007/s12027-009-0132-5.

25. Yar M. *Cybercrime and Society*. London, Sage, 2006. 232 p. DOI: 10.4135/9781446212196.

26. Dupont B. Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change*, 2017, vol. 67, iss. 1, pp. 97–116. DOI: 10.1007/s10611-016-9649-z.

27. Buono L. Fighting cybercrime between legal challenges and practical difficulties: EU and national approaches. *ERA Forum*, 2016, vol. 17, iss. 3, pp. 343–353. DOI: 10.1007/s12027-016-0432-5.

28. Calderoni F. The European legal framework on cybercrime: striving for an effective implementation. *Crime, Law and Social Change*, 2010, vol. 54, iss. 5, pp. 339–357. DOI: 10.1007/s10611-010-9261-6.

29. Kemp S., Miró-Llinares F., Moneva A. The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*, 2020, vol. 26, iss. 3, pp. 293–312. DOI: 10.1007/s10610-020-09439-2.

30. Karamnov A.Yu., Dvoretskii M.Yu. Great Britain Legislation of Crimes in the Sphere of Computer Information. *Sotsial'no-ekonomicheskie yavleniya i protsessy = Socio-Economic Processes and Phenomena*, 2013, no. 8 (54), pp. 164–167. (In Russian).

31. Nasution M.D.T.P., Siahaan A.P.U., Rossanty Y., Aryza S. The phenomenon of cyber-crime and fraud victimization in online shop. *International Journal of Civil Engineering and Technology*, 2018, vol. 9, iss. 6, pp. 1583–1592.

32. Fisher J.L. A Clinic's Place in the Supreme Court Bar. *Stanford Law Review*, 2013, vol. 65, iss. 1, pp. 137–201. DOI: 10.2139/ssrn.1921430.

33. Kapczynski A. Intellectual Property's Leviathan. *Law and Contemporary Problems*, 2015, vol. 77, no. 4, pp. 131–145.

34. De Silva S. Cyber Crime and the Law. *ITNOW*, 2016, vol. 58, iss. 4, pp. 28–29. DOI: 10.1093/itnow/bww101.

35. Cooper M. How Cyber Crime Damages Lives. *ITNOW*, 2020, vol. 62, iss. 1, pp. 36–37. DOI: 10.1093/itnow/bwaa016.

36. Lastowka G., Hunter D. Virtual Crimes. *New York Law School Law Review*, 2004, vol. 49, iss. 1, pp. 293–316.

37. Lastowka G., Hunter D. The Laws of the Virtual Worlds. *California Law Review*, 2004, vol. 92, iss. 1, pp. 1–74. DOI: 10.15779/Z386H7P.

38. Baturin Yu.M., Polubinskaya S.V. What Makes Virtual Crimes to be Real. *Trudy Instituta gosudarstva i prava RAN = Proceedings of the Institute of State and Law of the RAS*, 2018, vol. 13, no. 2, pp. 9–35. (In Russian).

39. D'Aspremont J. Cyber Operations and International Law: An Interventionist Legal Thought. *Journal of Conflict and Security Law*, 2016, vol. 21, iss. 3, pp. 575–593. DOI: 10.1093/jcsl/krw022.

40. Kirilenko V.P., Alexeyev G.V. Political technologies and international conflicts in the information space of the Baltic Sea. *Baltiiskii region = Baltic Region*, 2018, vol. 10, no. 4, pp. 20–38. DOI: 10.5922/2079-8555-2018-4-2. (In Russian).

41. Taylor R.W., Fritsch E.J., Liederbach J. *Digital Crime and Digital Terrorism*. New York, Prentice Hall Press, 2014. 416 p.

42. Zharova A.K. Routing and IP to Ensure Legal Regulation of Relationships in Cyberspace. *Vestnik RGGU. Seriya: Informatika. Informatsionnaya bezopasnost'. Matematika = RSUH Bulletin. Information Science. Information Security. Mathematics*, 2019, no. 2, pp. 32–42. DOI: 10.28995/2686-679X-2019-2-32-42. (In Russian).

43. Zharova A. Ensuring the Information Security of Information Communication Technology Users in Russia. *International Journal of Cyber Criminology*, 2019, vol. 13, iss. 2, pp. 255–269. DOI: 10.5281/zenodo.3698141.

44. Broadhurst R.G., Grabosky P., Alazab M., Chon S. Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*, 2014, vol. 8, iss. 1, pp. 1–20. DOI: 10.2139/ssrn.2345525.

45. Leukfeldt E.R., Lavorgna A., Kleemans E.R. Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*, 2017, vol. 23, iss. 3, pp. 287–300. DOI: 10.1007/s10610-016-9332-z.

46. Lavorgna A. Cyber-organised crime. A case of moral panic? *Trends in Organized Crime*, 2019, vol. 22, iss. 4, pp. 357–374. DOI: 10.1007/s12117-018-9342-y.

47. Kettemann M.C. Ensuring Cybersecurity through International Law. *Revista Española de Derecho Internacional*, 2017, vol. 69, iss. 2, pp. 281–290.

48. Nomokonov V.A., Tropina T.L. Cybercrime: Forecasts and Problems of Fighting. *Biblioteka kriminalista = Library of a Criminalist*, 2013, no. 5 (10), pp. 148–160. (In Russian).

49. Walden I. *Computer Crimes and Digital Investigations*. Oxford University Press, 2016. 600 p.

50. Reep-van den Bergh C.M.M., Junger M. Victims of cybercrime in Europe: a review of victim surveys. *Crime Science*, 2018, vol. 7, iss. 1. DOI: 10.1186/s40163-018-0079-3. Available at: https://crimesciencejournal.biomedcentral.com/track/pdf/10.1186/s40163-018-0079-3.pdf.

51. Mylrea M. Smart energy-internet-of-things opportunities require smart treatment of legal, privacy and cybersecurity challenges. *The Journal of World Energy Law & Business*, 2017, vol. 10, iss. 2, pp. 147–158. DOI: 10.1093/jwelb/jwx001.

52. Repetskaya A.L. Murders in Russia: Method for Determining Latency of an Array. *Vestnik Tomskogo gosudarstvennogo universiteta. Pravo = Tomsk State University Journal of Law*, 2019, no. 32, pp. 55–68. DOI: 10.17223/22253513/32/5. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Кириленко Виктор Петрович — заведующий кафедрой международного и гуманитарного права Северо-Западного института управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, доктор юридических наук, профессор, заслуженный юрист Российской Федерации, г. Санкт-Петербург, Российская Федерация; e-mail: v.vvaas@yandex.ru

Алексеев Георгий Валерьевич — доцент кафедры правоведения Северо-Западного института управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, кандидат юридических наук, доцент, г. Санкт-Петербург, Российская Федерация; e-mail: deltafox1@yandex.ru.

ДЛЯ ЦИТИРОВАНИЯ

Кириленко В.П. Гармонизация российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы / В.П. Кириленко, Г.В. Алексеев. — DOI: 10.17150/2500-4255.2020.14(6).898-913 // Всероссийский криминологический журнал. — 2020. — Т. 14, № 6. — С. 898–913.

INFORMATION ABOUT THE AUTHORS

Kirilenko, Viktor P. — Head, Chair of International and Humanitarian Law, North-West Institute of Management, Russian Presidential Academy of National Economy and Public Administration, Doctor of Law, Professor, Honored Lawyer of the Russian Federation, Saint Petersburg, the Russian Federation; e-mail: v.vvaas@yandex.ru.

Alekseev, Georgy V. — Ass. Professor, Chair of Law, North-West Institute of Management, Russian Presidential Academy of National Economy and Public Administration, Ph.D. in Law, Ass. Professor, Saint Petersburg, the Russian Federation; e-mail: deltafox1@yandex.ru.

FOR CITATION

Kirilenko V.P., Alekseev G.V. The harmonization of Russian criminal legislation on counteracting cybercrime with the legal standards of the Council of Europe. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 6, pp. 898–913. DOI: 10.17150/2500-4255.2020.14(6).898-913. (In Russian).