DOI 10.22394/2686-7834-2021-1-39-53

Киберпреступность и цифровая трансформация

Кириленко Виктор Петрович

доктор юридических наук, профессор, заслуженный юрист Российской Федерации, заведующий кафедрой международного и гуманитарного права Северо-Западного института управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС), Санкт-Петербург, Российская Федерация; kirilenko-vp@ranepa.ru

Алексеев Георгий Валерьевич

кандидат юридических наук, доцент кафедры правоведения Северо-Западного института управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС), Санкт-Петербург, Российская Федерация; deltafox1@yandex.ru

АННОТАЦИЯ

Преступность в киберпространстве является критической угрозой информационной безопасности государства и гражданского общества. Злоупотребление доверием пользователей компьютерных сетей позволяет организованным преступным группам достигать свои экономические и политические цели, совершая правонарушения в международном информационном пространстве. Методы включенного наблюдения, сравнительно-правового и дискурсивного анализа показывают, что цифровая трансформация ослабила влияние государства на развитие культурной сферы жизни общества, а компьютерные технологии стали объектом интересов криминальных структур. Цифровая трансформация создала виртуальную реальность, которая существует на основе законов и правил сетевого сообщества. Сетевые сообщества, отвергая большинство императивных норм, навязываемых гражданскому обществу национальными правительствами в политических целях, становятся жертвами широкого круга киберпреступлений: хищений, распространения вредоносных программ и пропаганды экстремизма. Поскольку цифровая трансформация — универсальное явление, которое неизбежно изменит жизнь всего мирового сообщества, постольку необходимо достижение консенсуса по вопросу выработки и имплементации современных международных соглашений, которые, с одной стороны, гарантируют свободу слова и право каждого человека на доступ к информации, а с другой стороны, защитят граждан, государства и социальные институты от преступных посягательств в активно развивающейся цифровой среде.

Ключевые слова: права человека, преступление, информация, мошенничество, экстремизм, хакер, ответственность, общественная опасность, технологии

Cybercrime and Digital Transformation

Viktor P. Kirilenko

Doctor of Sciences (Jurisprudence), Professor, North-West Institute of Management, Russian Presidential Academy of National Economy and Public Administration (RANEPA), Sankt Petersburg, Russian Federation; kirilenko-vp@ranepa.ru

Georgy V. Alekseev

PhD in Jurisprudence, Associate Professor, North-West Institute of Management, Russian Presidential Academy of National Economy and Public Administration (RANEPA), Sankt Petersburg, Russian Federation; deltafox1@yandex.ru

ABSTRACT

Cyberspace crime is a critical threat to the information security of the state and civil society institutions. Inside global network the abuse of computer user's trust allows organized criminal groups to achieve their economic and political goals by committing offenses in the international information space. The methods of participatory observation, comparative legal and discourse analysis show that digital transformation has weakened the influence of the state on the development of the cultural sphere of society, and computer technologies have become the object of interests of criminal structures. Digital transformation has created virtual reality based on the laws and regulations of the networked community. Civil society by rejecting most of the peremptory norms imposed by national governments for political purposes produce victims of a wide range of cybercrimes: fraud and computer misuse offences and obscene publications. Since digital transformation is a universal phenomenon that will inevitably change the life of the entire world community, it is necessary to reach a consensus on the development and implementation of modern international agreement which, on the one hand, will guarantee freedom of speech and the right of every person to access information, and on the other hand will protect citizens, states and social institutions from criminal encroachments in an actively developing digital environment.

Keywords: human rights, crime, information, fraud, extremism, hacker, responsibility, public danger, technology

Генеральный секретарь Организации Объединенных Наций Антониу Гутерриш в ноябре 2018 г., комментируя работу Управления ООН по наркотикам и преступности (УНП ООН; UNODC), обратил внимание на то, что «новые технологии, включая большие данные, искусственный интеллект и

автоматизацию, вступают в эпоху преобразований, ...и, несмотря на преимущества, которые дает такой прогресс, он также способствует появлению новых форм преступности»[1]. Очевидно, что развитие информационных технологий, создав виртуальную среду для общественных отношений, актуализировало новые преступные схемы с уникальными и недостаточно изученными способами совершения преступлений (modus operandi). В условиях цифровой трансформации, когда встают вопросы об ответственности за решения, принятые искусственным интеллектом, и машинная обработка больших данных практически полностью исключает возможность нормативного ограничения доступа к информации на длительное время, перед законодателем стоит задача создать такие нормы уголовного права, которые будут одновременно способствовать техническому прогрессу и привлечению к ответственности лиц, виновных в совершении преступлений.

Развитие национального законодательства в условиях цифровой трансформации отстает от темпов технического прогресса. Искусственный интеллект, различные элементы которого планомерно разрабатывают и внедряют транснациональные корпорации, призван содействовать достижению целей устойчивого развития[2], а реагирование государственного аппарата на становление трансграничной и саморазвивающейся кибернетической среды предопределяется заинтересованностью социальных институтов в организации международного диалога в масштабах глобального медиапространства. Очевидно, что глобальные системы международного общения не дают права отдельным лицам злоупотреблять свободой слова[3], использовать искусственный интеллект и большие данные в преступных целях[4], создавать криминальные сообщества в виртуальном пространстве[5]. Однако различия в понимании легитимности различных форм протестного поведения ставят на повестку дня вопрос о различии в киберпространстве действий современных преступников и «партизан», которые хотят «держаться в сфере политического» и не хотят «упасть в сферу криминального» в своем стремлении форсировать изменение жизненного порядка[6].

Вице-президент Европейской комиссии Маргаритис Скинас (Margaritis Schinas) на заседании Комиссии 29 января 2020 г. особо подчеркнул, что «борьба с киберпреступностью является ключевой частью работы по созданию Европейского союза, который защищает своих граждан. Киберпреступники не знают границ»[7]. Вместе с тем широкое международное признание угроз и опасности преступной деятельности в виртуальном пространстве компьютерных сетей не приблизило мировое сообщество к консенсусу в разграничении легитимного демократического протеста и преступной пропаганды насильственного экстремизма. Статистика по киберпреступности показывает, что, в то время как около 80% преступников в виртуальном пространстве совершают правонарушения из корыстных побуждений[8], остальные злоумышленники выражают своим поведением деятельный протест в отношении политической системы и современной общественной морали.

Характер влияния цифровой трансформации на динамику киберпреступности определяется рациональностью применения компьютерных технологий, благодаря которым появляются новые объекты правового регулирования, такие как социальные сети, виртуальные вещи и мультимедийные информационные ресурсы. С расширением возможностей цифровых технологий происходит трансформация всех сфер жизни общества, а значит, меняется и преступный мир, где становится меньше грубого насилия и появляется больше высоких технологий. В процессе того как анонимность

---

[1] “Much work to do and no time to waste” in cybercrime fight, says UN chief [Электронный ресурс]. URL: https://news.un.org/en/story/2018/05/1009692 (дата обращения: 25.02.2021).

[2] См.: *Tomašević V., Ilić-Kosanović T., Ilić D.* (2020) Skills Engineering in Sustainable Counter Defense Against Cyber Extremism. In: Al-Masri A., Al-Assaf Y. (eds) Sustainable Development and Social Responsibility. Vol. 2. Advances in Science, Technology & Innovation (IEREK Interdisciplinary Series for Sustainable Development). Springer, Cham. DOI:10.1007/978-3-030-32902-0_25.

[3] См.: *Кириленко В. П., Шамахов В. А., Алексеев Г. В.* Свобода слова и медиабезопасность. СЗИУ РАНХиГС. Санкт-Петербург. 2019. 440 с.

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

[5] См.: *Broadhurst R. G., P. Grabosky, M. Alazab, S. Chon.* 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.

[6] *Кириленко В. П., Алексеев Г. В.* Легитимность демократии в работах Макса Вебера и Карла Шмитта // Правоведение. 2018. Т. 62. № 3. С. 511. DOI: 10.21638/11701/spbu25.2018.305. См. также: *Schmitt Carl.* Theorie des Partisanen. Zwischenbemerkung zum Begriff des Politischen. Duncker & Humblot. 1963.

[7] Cybercrime: New Survey Shows Europeans Feel Better Informed but Remain Concerned [Электронный ресурс]. URL: https://ec.europa.eu/commission/presscorner/detail/hr/ip_20_143 (дата обращения: 01.03.202).

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

пользователей интернета и их физическая удаленность друг от друга способствуют процветанию мошенничества в виртуальном мире, также снижается и уровень доверия к ресурсам интернета. В условиях низкого уровня взаимного доверия и разобщенности пользователей социальных сетей преступные сообщества, делающие ставку на радикализацию и насильственный экстремизм в виртуальном пространстве, как правило, имеют мало шансов на успех. Повестку дня мультимедийных информационных ресурсов диктуют цифровые транснациональные корпорации, которые не заинтересованы в криминализации собственного бизнеса и выступают естественными союзниками правоохранительных органов в противодействии различным проявлениям насильственного экстремизма.

Американский ученый Сидней Таррoy (Sidney Tarrow) характеризует любой активный протест как «власть в движении», где вдохновение у протестующих, которые пережили социальную стигму, полицейских собак, резиновые пули, драки и даже смерть друзей, возникает тогда, когда люди собираются вместе, чтобы коллективно реализовать свои чаяния[9]. При использовании виртуального пространства интернета для выражения политического протеста многие активисты и исследователи социальных движений скептически настроены в отношении потенциальных последствий интернет-активизма, отдавая предпочтение офлайновому протесту как «реальному протесту»[10]. Низкая эффективность виртуального протеста, однако, не исключает усилий экстремистских сообществ по радикализации общественного мнения через «онлайн-протест»[11] с последующей эскалацией радикализации до уровня «реального протеста»[12].

Очевидно, что юридическим средством защиты несовершеннолетних от некоторых проявлений киберпреступности может служить более широкая имплементация Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и нравственному развитию» и ряда соответствующих ему правовых норм[13]. Вместе с тем экспертиза информационной продукции, во-первых, зависит от квалификации экспертов и их моральных и политических взглядов, а во-вторых, ограничивается правовым пространством России. По обоснованному мнению профессора А. И. Бастрыкина, «ответственность за безопасность ребенка, когда он общается в интернете, должны взять на себя его родные. Ведь в отличие от непосредственного контакта с преступником, в социальных сетях ребенку должно быть легче прекратить общение с педофилом»[14].

Виртуальный мир социальных сетей и интерфейс компьютерных программ существенно отличаются от реальных действий и непосредственного общения, так как логика виртуального акта и его последствия зависят от особенностей цифровой среды, внутри которой происходит общение и совершаются юридически значимые действия. В виртуальном пространстве реализуются заведомо некачественные и контрафактные товары, ресурсы Даркнета (Darkweb) позволяют организовать торговлю товарами, изъятыми из хозяйственного оборота, и оплачивать услуги откровенно криминального содержания[15], экстремистские сообщества осуществляют вербовку сторонников через социальные сети[16]. Онлайн-экстремизм, нацеленный на радикализацию общественного

---

[9] *Tarrow S.* Power in Movement: Social Movements, Collective Action and Politics. New York : Cambridge University Press. 1994. 251 p.

[10] См.: *Rucht D.* Movement Allies, Adversaries, and Third Parties. 2007. DOI:10.1002/9780470999103.ch9.

[11] См.: *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; *Awan I.* Cyber-extremism: Isis and the Power of Social Media // Social Science and Public Policy 2017. Vol. 54. Pp. 138–149. DOI: 10.1007/s12115-017-0114-0; *Earl J.* Protest Online: Theorizing the Consequences of Online Engagement. In L. Bosi, M. Giugni & K. Uba (Eds.). The Consequences of Social Movements. Cambridge : Cambridge University Press. 2016. Pp. 363–400. DOI: 10.1017/CBO9781316337790.015.

[12] Supra note 10.

[13] См.: *Одинцова Н. Е., Репецкая А. Л.* Проблемные аспекты отечественного и зарубежного законодательства в противодействии пропаганде педофилии // Международный журнал гуманитарных и естественных наук. 2019. № 11–3 (38). С. 84–89. DOI: 10.24411/2500-1000-2019-11821.

[14] *Бастрыкин А. И.* Преступления против несовершеннолетних в интернет-пространстве: к вопросу о виктимологической профилактике и уголовно-правовой оценке // Всероссийский криминологический журнал. 2017. Т. 11. № 1. С. 7. DOI: 10.17150/2500-4255.2017.11(1).5-12.

[15] См.: *Martin J., Munksgaard R., Coomber R.* & oths. 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.

[16] См.: *Earl J.* Protest Online: Theorizing the Consequences of Online Engagement. In L. Bosi, M. Giugni & K. Uba (Eds.). The Consequences of Social Movements. Cambridge : Cambridge University Press. 2016. Pp. 363–400. DOI: 10.1017/CBO9781316337790.015; *Taylor R. W. Fritsch E. J., Liederbach J.* Digital Crime and Digital Terrorism. New York : Prentice Hall Press, 2014. 416 p.

мнения и вербовку новых сторонников, осуществляется организованными преступными группами[17]. Исследования в области медиабезопасности[18] и насильственного экстремизма[19] демонстрируют иррациональность медиалогики пропаганды насильственного экстремизма, которая отчасти обусловлена заинтересованностью радикальных групп в вербовке индивидов, страдающих психическими расстройствами, в том числе синдромом убийства-самоубийства[20].

Цифровая трансформация настолько изменила восприятие преступности, что жертв временами сложно отличить от соучастников преступлений, а методика научной оценки динамики киберпреступности прогнозирует рост преступности онлайн[21]. Обзор доступных опросов по виктимизации показывает, что в период с 2010 по 2020 гг. в развитых государствах киберпреступность может составлять от одной трети до половины преступлений[22]. В России до смягчения уголовной политики в 2018 г. в отношении экстремистских правонарушений в виртуальном пространстве быстрыми темпами росло количество преступлений террористического характера и экстремистской направленности[23]. Есть все основания полагать, что рост компьютерных преступлений способствовал снижению уровня традиционной преступности, а сами киберпреступления не попали в официальную статистику. В то время как степень общественной опасности киберпреступности неуклонно растет, очевидно, что «наибольшая часть киберпреступлений остается за рамками статистики»[24].

Гармонизация российского уголовного законодательства в области цифровых технологий с нормами уголовного права развитых государств представляется необходимым условием для организации международного полицейского сотрудничества. Необходимость международного сотрудничества в деле противодействия киберпреступности определяется отсутствием в информационном пространстве государственных границ. Разработка под эгидой Совета Европы Конвенции о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) и ратификация этого соглашения большинством государств — членов Совета Европы — важный элемент глобальной кибербезопасности. 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 Конвенции на правонарушения экстремистской направленности.

Российская Федерация не участвует в Конвенции о преступности в сфере компьютерной информации, и вместе с тем большинство положений Будапештской конвенции стали широко признанными нормами обычного международного права. Несмотря на то, что Распоряжением Президента Российской Федерации от 22 марта 2008 г. № 144-рп было отменено Распоряжение Президента Российской Федерации от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности»[25], рациональность большинства положений этой Конвенции не вызывает со-

---

[17] *Broadhurst R. G., P. Grabosky, M. Alazab, S. Chon.* 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. P. 1–20. DOI: 10.2139/ssrn.2345525; *Dalgaard-Nielsen A.* Violent Radicalization in Europe: What We Know and What We Do Not Know // Stud Conflict Terrorism 2010. Vol. 33, iss. 9. P. 797–814. DOI: 10.1080/1057610X.2010.501423; *Walden I.* Computer Crimes and Digital Investigations / I. Walden. Oxford : Oxford University Press. 2016. 600 p.

[18] См., например: *Кириленко В. П., Алексеев Г. В.* Политические технологии и международный конфликт в информационном пространстве Балтийского региона // Балтийский регион. 2018. Т. 10. № 4. С. 20–38. DOI: 10.5922/2079-8555-2018-4-2; *Кириленко В. П., Шамахов В. А., Алексеев Г. В.* Указ. соч.

[19] См., например: *Кириленко В. П., Алексеев Г. В.* Актуальные проблемы противодействия преступлениям экстремистской направленности // Всероссийский криминологический журнал. 2018. Т. 12. № 4. С. 561–571. DOI: 10.17150/2500-4255.2018.12(4).561-571; *Кириленко В. П., Алексеев Г. В.* Противодействие идеологии современного терроризма // Управленческое консультирование. 2018. № 5 (113). С. 8–18. DOI: 10.22394/1726-1139-2018-5-8-18.

[20] *Кириленко В. П., Алексеев Г. В.* Экстремисты: преступники и жертвы радикального насилия // Всероссийский криминологический журнал. 2019. Т. 13. № 4. С. 617–618. DOI: 10.17150/2500-4255.2019.13(4).612-628.

[21] См.: *Номоконов В. А., Тропина Т. Л.* Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. 2013. № 5 (10). С. 148–160; *Кириленко В. П., Алексеев Г. В.* Указ. соч. Supra note 8.

[22] См.: *Reep-van den Bergh C. M. M., Junger M.* Victims of Cybercrime in Europe: A Review of Victim Surveys // Crime Science. 2018. Vol. 7, art No. 5. DOI:10.1186/s40163-018-0079-3.

[23] *Репецкая А. Л.* Современное состояние, структура и тенденции российской преступности // Вестник Омского университета. Серия: Право. 2018. № 1 (54). С. 155. DOI: 10.25513/1990-5173.2018.1.151-156.

[24] *Журавленко Н. И., Шведова Л. Е.* Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере / Н. И. Журавленко // Общество и право. 2015. № 3 (53). С. 69.

[25] Распоряжение Президента Российской Федерации от 22 марта 2008 г. № 144-рп [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/27059 (дата обращения: 22.02.2021).

мнений, так как изначально подчеркивалось, что «Российская Федерация исходит из того, что положения пункта «b» статьи 32 Конвенции сформулированы таким образом, что ...могут нанести ущерб суверенитету и национальной безопасности государств-участников, правам и законным интересам их граждан и юридических лиц»[26]. 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, вопросы кибербезопасности определенно могут затрагивать принципиально значимые национальные интересы государств[27]. Цифровая трансформация, несомненно, требует совершенствования институтов международного информационного права[28].

Спорные положения Конвенции о преступности в сфере компьютерной информации позволяют государствам-участникам «получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему» (п. “b” ст. 32), что при определенных обстоятельствах может быть истолковано как юридическое основание вмешательства в дела входящие во внутреннюю компетенцию государства — участника соглашения. Однако неприсоединение к Будапештской конвенции оставляет открытым вопрос о соответствии норм уголовного законодательства Российской Федерации международным стандартам и современности положений гл. 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной информации» (ст. 272–274.1 УК РФ). Криминализация неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) не в полной мере отражает экономическую сущность современных информационных технологий. Суверенитет России в информационном пространстве защищается в соответствии с Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», однако уголовное законодательство недостаточно точно определяет понятие критической информационной инфраструктуры, что порождает правовую неопределенность в деле борьбы с киберпреступностью.

Классификация материальных составов киберпреступлений не вызывает принципиальных разногласий в документах Совета Европы, однако является неоднозначной проблемой в национальном уголовном праве. Конвенция о преступлениях в сфере компьютерной информации 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, связанные с нарушением авторского права и смежных прав (ст. 10). Правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем, очевидно, относятся к группе преступлений, связанных с содержанием данных. Из конвенционной классификации можно сделать заключение, что компьютерные преступления могут совершаться как субъектами, применяющими специальные знания в области технологий компьютерного программирования в преступных целях, так и лицами, использующими для совершения преступлений легальное программное обеспечение компьютеров. В частности, «все чаще отмечаются факты освоения информационных технологий и компьютерных сетей транснациональными террористическими и экстремистскими организациями, что обусловило появление наиболее опасной разновидности компьютерной преступности — кибертерроризма»[29], при этом очевидно, что кибертерроризм связан не только с модификацией программного обеспечения, но также предполагает вербовку аудитории социальных сетей и пропаганду экстремизма[30]. Для финансирования экстремистской деятельности и международного терроризма активно используются технологии компьютерного мошенничества.

В Российской Федерации квалификация хищения по ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации» для преступника, осуществлявшего незаконные операции в ком-

---

[26] О подписании Конвенции о киберпреступности : распоряжение Президента Российской Федерации от 15 ноября 2005 г. № 557-рп // Собрание законодательства Российской Федерации, 2005, № 47, ст. 4929.

[27] См.: *Brenner S. W.* Cyberthreats and the Decline of the Nation-State. London : Routledge. 2014. 182 p.; *Justice J. W., Bricker B. J.* Hacked: Defining the 2016 Presidential Election in the Liberal Media / J. W. Justice // Rhetoric and Public Affairs. 2019. Vol. 22, iss. 3. Pp. 389–420. DOI: 10.14321/rhetpublaffa.22.3.0389.

[28] См.: *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; *Kettemann M. C.* Ensuring Cybersecurity through International Law // Revista Española de Derecho Internacional. Vol. 69, iss. 2. Pp. 281–290.

[29] Supra note 24. P. 67.

[30] Supra note 11. P. 238.

пьютерной сети (хакера), может повлечь квалификацию деяния по соответствующему составу гл. 28 УК РФ (идеальная совокупность преступлений[31]), однако такая правовая логика не применяется на практике[32]. Поскольку хакерские атаки могут преследовать не только экономические, но и политические мотивы[33], постольку их рассматривают как преступление с материальным составом и квалифицируют по их последствиям.

Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» 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 и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) — ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети...» (п. 20). Фактически «если хищение чужого имущества ... осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть Интернет (например, создание поддельных сайтов...), то такое мошенничество следует квалифицировать по ст. 159, а не 159.6 УК РФ» (п. 21).

Выработанная в рамках борьбы с экономическими киберпреступлениями правовая логика не нашла применения в практике защиты других объектов уголовно-правовой охраны. В Постановлении Пленума Верховного Суда Российской Федерации от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина...» отмечается, что распространение сведений о частной жизни лица заключается в сообщении (разглашении) их одному или нескольким лицам в устной, письменной или иной форме и любым способом (в частности, путем передачи материалов или размещения информации с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет) (п. 3), однако распространение информации ограниченного доступа в компьютерной сети не образует специальный состав преступления. Аналогичны положения Постановления Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности», где отмечается возможность привлечения к уголовной ответственности за публичные призывы к осуществлению экстремистской деятельности в интернете на тех же правовых основаниях, что были разработаны для привлечения к ответственности журналистов, злоупотребляющих свободой слова (ч. 2 ст. 280 УК РФ). Положения Федерального закона от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» толкуются органами судебной власти исходя из того, что сеть Интернет, включая сайты, блоги и форумы, является частным примером публичного пространства.

В Постановлении Пленума Верховного Суда Российской Федерации от 4 декабря 2014 г. № 16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности» отмечается, что «развратными могут признаваться и такие действия, при которых непосредственный физический контакт с телом потерпевшего лица отсутствовал, включая действия, совершенные с использованием сети Интернет, иных информационно-телекоммуникационных сетей» (п. 17).

Постановление Пленума Верховного Суда Российской Федерации от 26 апреля 2007 г. № 14 «О практике рассмотрения судами уголовных дел о нарушении авторских, смежных, изобретательских и патентных прав, а также о незаконном использовании товарного знака» в духе ст. 10 Будапештской конвенции признает возможность совершения преступлений против интеллектуальной собственности в компьютерных сетях (п. 4), однако специальных норм и разъяснений по данному виду компьютерных преступлений не содержит.

Постановление Пленума Верховного Суда Российской Федерации от 15 июня 2006 г. № 14 «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами» (с изменениями и дополнениями от 16 мая 2017 г.) не уделяет должного внимания угрозе распространения наркотических средств

---

[31] *Черненко Т. Г.* Квалификация совокупности преступлений // Вестник Омского университета. Серия: Право. 2014. № 1 (38). С. 151.

[32] *Энгельгардт А. А.* О понимании мошенничества в сфере компьютерной информации // Вестник Московского университета МВД России. 2016. № 8. С. 90.

[33] См.: *Arnold N., Mahoney W., Derrick D., Ligon G.* & Harms M. Feasibility of a Cyber Attack on National Critical Infrastructure by a Non-State Violent Extremist Organization // Journal of Information Warfare. 2015. Vol. 14, iss. 1. Pp. 84–100.

посредством сетей компьютерной связи и пропаганде рекреационного использования психоактивных веществ. Есть все основания полагать, что угрозы, исходящие от киберпреступности, не в полной мере оценены правоохранительными органами и происходит это не только в Российской Федерации, но и в других странах.

Опыт индустриально развитых стран демонстрирует технологическую зависимость всех законодательных инициатив в виртуальном мире[34]. Посредством законодательной политики такие страны, как Япония, Южная Корея, Австралия, Нидерланды и Германия, реализуют стратегии снижения вреда (в том числе от запретительных мер), основанные на партнерских отношениях между государственным и частным секторами для защиты «цифровой экосистемы»[35]. На уровне Европейского союза проводится гармонизация национального уголовного законодательства, устанавливающего ответственность за преступления в компьютерных сетях[36], однако такие «не юридические факторы, как национальная безопасность, политика, экономика и общественное мнение ...стимулируют спонтанное внедрение европейской правовой базы»[37]. Несовершенство европейского законодательства выражается в высоком уровне «теневого мошенничества», свидетельствующем о том, что «оценка предупреждения преступности, основанная исключительно на полицейской статистике, может быть неадекватной»[38].

В Великобритании действует Закон о неправомерном использовании компьютеров 1990 г. (Computer Misuse Act), который направлен на борьбу с киберпреступностью и во многом схож с российским уголовным законодательством, однако имеет определенную специфику. С одной стороны, защита компьютерных систем и технологий от несанкционированного доступа или изменения всегда определяет объект посягательства преступлений, которые связаны с использованием компьютерных технологий[39]. С другой стороны, очевидно, что в отличие от российского уголовного права, которое защищает компьютерные системы от причинения им вреда, британские статуты изначально в большей степени ориентированы на защиту прав пользователей компьютерных сетей. Британский законодатель разъясняет, что наиболее типичные составы компьютерных преступлений связаны с несанкционированным доступом к компьютерным материалам или несанкционированной модификацией компьютерных программ и включают в себя: (1) взлом (hacking), включая доступ к аккаунтам социальных сетей и паролей электронной почты; (2) фишинг (phishing) — злоупотребление доверием пользователей с целью получения паролей, информации о безопасности и личных данных; (3) создание вредоносного программного обеспечения (malware), включая программы-вымогатели различного рода[40], распределенные атаки типа «отказ в обслуживании» (DDOS) на веб-сайты, которые также сопровождаются вымогательством[41].

В Соединенных Штатах Америки на федеральном уровне в наибольшей степени компьютерным преступлениям, в смысле российского уголовного законодательства, соответствуют составы преступлений, связанные с незаконным доступом к коммуникациям и нарушением их нормальной работы (18 U.S.C. § 2701–2703), а также состав причинения вреда линиям связи, станциям или системам (18 U.S.C. § 1362). Специальная уголовно-правовая защита компьютерных сетей в США осуществляется на уровне штатов. Особое значение для международного информационного пространства имеет охранительная норма ст. 502 Уголовного кодекса Калифорнии[42], так как

---

[34] См.: *Gercke M.* Europe's Legal Approaches to Cybercrime // ERA Forum. 2009. Vol. 10. P. 409–420. DOI:10.1007/s12027-009-0132-5.

[35] *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. DOI: 10.1007/s10611-016-9649-z.

[36] См.: *Buono L.* Fighting Cybercrime between Legal Challenges and Practical Difficulties: EU and National Approaches // ERA Forum. 2016. Vol. 17. Pp. 343–353. DOI: 10.1007/s12027-016-0432-5.

[37] *Calderoni F.* The European Legal Framework on Cybercrime: Striving for an Effective Implementation // Crime, Law and Social Change. 2010. Vol. 54, iss. 5. P. 339. DOI: 10.1007/s10611-010-9261-6.

[38] *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. DOI: 10.1007/s10610-020-09439-2.

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

[40] *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. 1584–1585.

[41] The Threat from Cyber Crime [Электронный ресурс]. URL: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime (дата обращения: 22.02.2021).

[42] California Penal Code § 502. [Электронный ресурс]. URL: http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEN&sectionNum=502 (дата обращения: 01.03.2021).

коммерческая инфраструктура интернета находится в Силиконовой долине под юрисдикцией штата[43].

Федеральная правоприменительная практика в США долгое время исходила из высокой общественной опасности киберпреступлений, однако это изначально касалось защиты всех технологических систем электрической связи (The Omnibus Crime Control and Safe Streets Act of 1968 [Wiretap Act] и Berger v. New York, 388 U. S. 41 (1967) Katz v. United States, 389 U. S. 347 (1967)). Из дела United States v. Sutcliffe[44] прямо следует намерение американского правосудия применять для защиты информации в компьютерных сетях логику аналогии закона о торговых сетях и электрической связи, учитывая, что конгресс обладает необходимыми полномочиями по регулированию интернета, равно как и других инструментов и каналов торговли между штатами (United States v. Hornaday, 392 F. 3d 1306, 1311).

Исходя из логики экономической природы интернета, в США наиболее типичным составом компьютерных преступлений является мошенничество, связанное с распространением компьютерной информации различного рода (18 U.S.C. § 1028, § 1028A, § 1029, § 1030, § 1037), особое внимание уделяется вводящим в заблуждение доменным именам (18 U.S.C. § 2252B), а также «словам или цифровым изображениям в интернете» (18 U.S.C. § 2252C). Распространение запрещенной информации через компьютерные сети в США преследуется на общих основаниях (18 U.S.C. § 2252A), той же логике подчинено уголовное преследование за нарушение авторских прав в компьютерных сетях (17 U.S.C. § 506, 18 U.S.C. § 2319). Американский законодатель намеренно защищает физическую инфраструктуру связи теми же законодательными нормами, что и программное обеспечение, обоснованно полагая, что санкция (до десяти лет лишения свободы) связана с попыткой нанесения ущерба тем компьютерным системам на национальном уровне, которые особо значимы для государства (в России такие системы характеризуются как критическая информационная инфраструктура). Подходы к киберпреступности в российском и зарубежном уголовном праве во многом совпадают, однако некоторые принципиальные вопросы разрешаются с учетом особенностей источников национального права.

Дискурсивный анализ законодательства и судебных решений показывает, что в условиях цифровой трансформации необходимо защищать широкий круг интересов высокотехнологических корпораций и их клиентов от преступных посягательств со стороны криминальных структур, находящихся внутри государственного аппарата, бизнес-сообщества и общественных организаций. При этом американская правоприменительная практика демонстрирует, что *распространение информации через сети компьютерной связи,* являясь способом совершения различных преступлений, осуществляется обычно субъектом, имеющим доступ к служебной информации, и должно квалифицироваться с учетом мотивов преступника и реальных последствий правонарушения, без специального внимания к конкретному способу получения доступа к закрытой информации.

Известный американский юрист Джеффри Фишер (Jeffrey L. Fisher), выступая адвокатом Натана Ван Бурена (Nathan Van Buren), бывшего сотрудника полиции штата Джорджия, который предоставил информацию из базы данных полиции знакомому за 6 тыс. долл. США, справедливо отметил, что решение по делу United States v. Van Buren[45] делает из нарушения обычных ограничений на обработку цифровых данных серьезное федеральное преступление. Верховный суд США, рассматривая вопрос о том, необходим ли реальный взлом компьютера для обвинения в совершении компьютерного преступления, пришел к выводу, что действия образуют состав преступления, если был получен незаконный доступ к компьютерной информации, способ получения доступа при этом не имеет существенного значения для квалификации деяния. В свою очередь, дело Riley v. California[46] демонстрирует необходимость уважать интересы граждан в компьютерных сетях со стороны государства и особо защищать тайну частной жизни, учитывая, что все «цифровое отличается от физического»[47]. Прецедентное право США показывает то, как «решения Вер-

---

[43] *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.

[44] United States of America, Plaintiff-Appellee v. Steven William Sutcliffe, Defendant-Appellant, No. 04-50189, Decided: October 11, 2007 [Электронный ресурс]. URL: https://caselaw.findlaw.com/us-9th-circuit/1166432.html (дата обращения: 01.03.2021).

[45] United States v. Van Buren. No. 18-12024 (11th Cir. 2019) [Электронный ресурс]. URL: https://law.justia.com/cases/federal/appellate-courts/ca11/18-12024/18-12024-2019-10-10.html (дата обращения: 01.03.2021).

[46] Supreme Court of the United States Syllabus. Riley v. California [Электронный ресурс]. URL: https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf (дата обращения: 01.03.2021).

[47] Faculty on Point: Prof. Jeffrey Fisher on Digital Privacy and the Riley Decision [Электронный ресурс]. URL: https://law.stanford.edu/directory/jeffrey-l-fisher/#slsnav-featured-video (дата обращения: 01.03.2021).

ховного Суда [США] вызывают отголоски далеко за пределами конкретных вовлеченных сторон, даже за пределами судебной системы»[48].

После того как идея расширения возможности правоохранительных органов США в борьбе с сайтами, зарегистрированными за рубежом, нарушением авторских прав в интернете и незаконным оборотом контрафактных товаров в интернете зашла в тупик в 2012 г., а законодательные инициативы SOPA (Stop Online Piracy Act — Закон о борьбе с пиратством в интернете) и PIPA (Protect IP Act) были отвергнуты, стало очевидно, что экономические интересы корпораций подчинены системообразующим принципам виртуальной среды, где доминируют свобода слова и инновации, а всякая интернет-цензура встретит жесткий протест со стороны сетевого сообщества[49].

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»[50]. В виртуальном пространстве обман не становится нормой, однако способы маскировки технологий мошенничества под творческие решения, как и информационное противоборство, приобретают характер социально-политической международной технологии[51]. С одной стороны, техническое понимание принципиальных отличий акций креативных партизан цифровизации от классических преступлений экстремистского характера отражает необходимость разработки специальных норм для обеспечения законности в глобальном информационном пространстве[52]. С другой стороны, опасность творческих проектов лишь косвенно связана с их технической реализацией, так как виртуальная реальность может нести непредсказуемые социально-психологические и экономические угрозы[53].

Киберпреступность, исходя из технологических особенностей реализации преступного замысла, может охватывать неопределенный круг лиц — адресатов потенциально опасных сообщений[54]. Для высокотехнологичных отраслей общие нормы уголовного права не всегда приемлемы. В российской юридической науке также присутствует понимание того, что «существующие правовые механизмы не всегда реализуемы для интернет-отношений»[55] и, в частности, законодательство недостаточно эффективно защищает права потребителей программного обеспечения компьютеров[56]. Очевидно, что киберпреступность внедряется в самые разные организационные структуры и ориентирована на получение прибыли за счет нарушения прав широких слоев населения[57]. Обеспечение доступа к потенциальным жертвам преступлений нередко осуществляется за счет создания в интернете различных социально-технологических сетей[58], эмпирические данные внутри которых достаточно сложно собрать, а неизвестность, действительно, может порождать панику вокруг незащищенной аудитории интернета[59].

---

[48] *Fisher J. L.* A Clinic’s Place in the Supreme Court Bar // Stanford Law Review. 2013 (2011). Vol. 65, iss. 1. P. 137. DOI: 10.2139/ssrn.1921430.

[49] См.: Hacking Politics: How Geeks, Progressives, the Tea Party, Gamers, Anarchists and Suits Teamed up to Defeat SOPA and Save the Internet / D. Moon, P. Ruffini, D. Segal (eds). OR Books. 2013. 316 p.; *Kapczynski A.* Intellectual Property’s Leviathan // Law and Contemporary Problems. 2015. Vol. 77, iss. 4. Pp. 131–145.

[50] *Батурин Ю. М., Полубинская С. В.* Что делает виртуальные преступления реальными // Труды Института государства и права Российской академии наук 2018. Т. 13. № 2. С. 30.

[51] *Кириленко В. П., Алексеев Г. В.* Указ соч. Supra note 8, 18.

[52] См.: *Taylor R. W., Fritsch E. J., Liederbach J.* Digital Crime and Digital Terrorism. New York : Prentice Hall Press, 2014. 416 p.

[53] *Батурин Ю. М., Полубинская С. В.* Указ. соч. Supra note 50.

[54] См.: *Cooper M.* How Cyber Crime Damages Lives // ITNOW. 2020. Vol. 62, iss. 1. Pp. 36–37. DOI: 10.1093/itnow/bwaa016; *De Silva S.* Cyber Crime and the Law // ITNOW. 2016. Vol. 58, iss. 4. Pp. 28–29. DOI: 10.1093/itnow/bww101; *Dalgaard-Nielsen A.* Supra note 17; *Walden I.* Supra note 17.

[55] *Жарова А. К.* Маршрутизация и IP для обеспечения правового регулирования интернет-отношений // Вестник РГГУ. Серия: Информатика. Информационная безопасность. Математика. 2019. № 2. С. 40. DOI: 10.28995/2686-679X-2019-2-32-42.

[56] См.: *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.

[57] См.: *Leukfeldt E. R., A. Lavorgna, E.R. Kleemans.* 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. P. 287-300. DOI:10.1007/s10610-016-9332-z; Broadhurst R. G., P. Grabosky, M. Alazab. Supra note 5.

[58] См.: *Иванцов С. В., Борисов С. В., Узембаева Г. И.* и др. Актуальные проблемы совершенствования системы мер криминологического предупреждения преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных сетей // Всероссийский криминологический журнал. 2018. Т. 12. № 6. С. 776–784. DOI: 10.17150/2500-4255.2018.12(6).776-784.

[59] См.: *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.

Отдельные громкие киберпреступления не причинили вреда критической информационной инфраструктуре, а некоторые серьезные тяжкие преступления не были раскрыты, так, например, создатели вируса WannaCry так и не были изобличены и привлечены к ответственности, а значит, не были установлены их экономические или политические мотивы. Обоснованная квалификация компьютерных преступлений во многом зависит от объективной стороны их состава. Два аналогичных по объекту посягательства компьютерных преступления может отличать принципиально разная общественная опасность. Так, например, американский студент Варун Сарджа (Varun H. Sarja), взломав несколько компьютеров в учебном заведении, изменил свои оценки и был приговорен к полутора годам лишения свободы условно[60]. В то же время британский хакер Алекс Бесселл (Alex Bessell) был наказан двумя годами лишения свободы за формально аналогичное преступление — систематические кибератаки, осуществляя которые он заработал более 50 тыс. фунтов стерлингов[61]. Оба случая демонстрируют наличие существенных проблем в оценке судом реального ущерба от противоправных действий в компьютерных сетях. Уголовное преследование американского сенатора Энтони Винера (Anthony D. Weiner) за развратные действия в социальных сетях по отношению к несовершеннолетней жертве продемонстрировало, что проблемы со здоровьем, содействие следствию и примерное поведение способны обусловить фактическое наказание в полтора года принудительного лечения с последующими мерами дополнительного наказания[62].

Практика правоприменения подтверждает, что при квалификации компьютерных преступлений и назначении наказания за их совершение осуществляется юридическая оценка последствий правонарушения, то есть виртуальные преступления рассматриваются судом как преступления с материальным составом, при этом степень вины виртуального делинквента может характеризоваться косвенным умыслом, а способы совершения преступлений будут все более подвержены влиянию искусственного интеллекта[63]. Мотивы разрушения виртуальной инфраструктуры могут диктоваться логикой, свойственной международным преступлениям против культурного наследия, и охватывают как комплекс Герострата, так экстремистские убеждения, приводящие к дискриминации[64].

Большое значение в системе оценки общественной опасности киберпреступлений имеет презумпция невиновности всех участников сетевого общения, однако субъектам, совершающим тяжкие преступления в виртуальном мире, свойственно маскировать свои действия под реализацию товаров, услуг и интеллектуальных прав, а также под добровольные пожертвования граждан на развитие их проектов. При выявлении киберделиктов основаниями для сомнений в законности функционирования сайтов интернета могут служить как явные признаки наличия состава правонарушения, так и жалобы пользователей сетевого ресурса на нарушение их субъективных прав. Очевидно, что именно жалобы потерпевших могут позволить выявить мошенничество, пропаганду экстремизма и другие киберпреступления, раскрывая при этом modus operandi виртуального делинквента. Мошеннические сайты, онлайн-казино и группы смерти в социальных сетях нередко используют идентичные приемы для фишинга персональных данных и получения контроля над действиями жертвы преступления. Есть все основания полагать, что действующие из корыстных и экстремистских мотивов организованные преступные сообщества, существующие в виртуальном пространстве, рано или поздно включаются в борьбу за власть и политическое влияние, злоупотребляя доверием пользователей интернета.

Заключение. Цифровая трансформация расширяет возможности активных субъектов правоотношений во всех сферах жизни современного общества, однако внедрение информационных технологий в народное хозяйство на практике нередко вызывает серьезные социальные проблемы. С одной стороны, в процессе цифровизации возникает множество новых возможностей для твор-

---

[60] Former University of Kansas Student Gets Probation for Changing Failing Grades to 'A' Via Hacking [Электронный ресурс]. URL: https://www.indiawest.com/news/global_indian/former-university-of-kansas-student-gets-probation-for-changing-failing/article_07766628-7f0d-11e8-8d2a-3bf0c388ace0.html (дата обращения: 20.02.2021).

[61] Hacker Alex Bessell Jailed for Cyber Crime Offences [Электронный ресурс]. URL: https://www.bbc.com/news/uk-england-42733638 (дата обращения: 20.02.2021).

[62] Anthony Weiner Released from Prison After Serving 18 months for Sexting Teenager [Электронный ресурс]. URL: https://www.nytimes.com/2019/05/14/nyregion/anthony-weiner-prison-release.html (дата обращения: 20.02.2021).

[63] См.: *Бегишев И. Р., Хисамова З. И.* Указ. соч. Supra note 4; *Van der Wagen 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.

[64] См.: *Brosché J., Legnér M., Kreutz J., Ijla A.* Heritage under Attack: Motives for Targeting Cultural Property During Armed Conflict // International Journal of Heritage Studies 2017. Vol. 23, iss. 3. Pp. 248–260. DOI: 10.1080/13527258.2016.1261918.

чества, организации общения, моделирования виртуальной реальности и реализации амбициозных технических проектов. С другой стороны, в результате цифровой трансформации возникают и новые аспекты в деятельности преступных сообществ. Во-первых, преступные сообщества используют информационные сети для вербовки новых членов в свои ряды и мотивации отдельных членов общества к действиям, способствующим достижению преступных целей. Во-вторых, значительная часть доходов от мошенничества в сфере компьютерной информации по разным причинам чисто криминального свойства может направляться на финансирование экстремистской деятельности. В-третьих, возникает угроза криминализации киберпространства, где развивается организованная преступность, процветают криминальные сетевые ресурсы, такие как: информационные системы для поиска исполнителей криминальных услуг и их оплаты, ресурсы по предоставлению доступа к закрытой и контрафактной информации, сайты по продаже поддельных и некачественных товаров, онлайн-казино и различные мошеннические политические проекты, злоупотребляющие доверием граждан.

Материальное уголовное право существенно отстает в своем развитии от тех преступных схем, которые активно разрабатываются и внедряются в жизнь сетевого сообщества. Необходимо введение новых видов дополнительного уголовного наказания, которые могут ограничивать права граждан на участие в сетевом общении, включая запреты: на пользование социальными сетями, на создание сетевых сайтов, на пользование ресурсами нумерации глобальной сети. В тех случаях, когда криминальная активность в информационном пространстве носит трансграничный характер, гармонизация уголовного законодательства и международное полицейское сотрудничество становятся критически важными элементами информационной безопасности.

Система оценки общественной опасности киберпреступлений должна быть основана на учете вреда, причиненного охраняемым законом интересам всех пользователей сетевых ресурсов, а также на своевременности демаскировки преступного замысла правоохранительными органами. Центральным элементом критической информационной инфраструктуры каждого государства остается пользователь компьютерных систем, и именно пользователь наименее защищен уголовным законодательством в процессе цифровой трансформации всех сфер жизни общества.

Учитывая тот факт, что «существует множество теоретических рассуждений о страхе перед санкциями, который мотивирует людей не нарушать юридические обязательства»[65], очевидно, что цифровая трансформация меняет восприятия угрозы наказания большинством пользователей компьютерных сетей. Энергия виртуальных вещей (интернет вещей)[66] и коммодификация компьютерного общения оказывают существенное влияние на активность криминальных структур, которые в новых условиях стремятся решить собственные криминальные и политические задачи при помощи цифровых технологий в виртуальном пространстве компьютерных сетей. Расширяющиеся возможности для использования искусственного интеллекта в интересах преступных сообществ подчеркивают важность корректировки уголовной политики развитых государств в направлении защиты идеалов гуманизма и охрану статуса личности, которая все больше уязвима в конкуренции между человеческим и машинным интеллектом. Нет сомнений, что механизмы уголовного права необходимы для предотвращения цифрового рабства и обесценивания человеческого труда.

Литература

1. *Бастрыкин А. И.* Преступления против несовершеннолетних в интернет-пространстве: к вопросу о виктимологической профилактике и уголовно-правовой оценке // Всероссийский криминологический журнал. 2017. Т. 11. № 1. С. 5–12. DOI: 10.17150/2500-4255.2017.11(1).5–12.
2. *Батурин Ю. М., Полубинская С. В.* Что делает виртуальные преступления реальными // Труды Института государства и права Российской академии наук 2018. Т. 13. № 2. С. 9–35.
3. *Бегишев И. Р., Хисамова З. И.* Криминологические риски применения искусственного интеллекта // Всероссийский криминологический журнал. 2018. Т. 12. № 6. С. 767–775. DOI: 10.17150/2500-4255.2018.12(6).767–775.
4. *Жарова А. К.* Маршрутизация и IP для обеспечения правового регулирования интернет-отношений // Вестник РГГУ. Серия: Информатика. Информационная безопасность. Математика. 2019. № 2. С. 32–42. DOI: 10.28995/2686-679X-2019-2-32–42.

[65] См.: *Nuotio K.* A Legitimacy-Based Approach to EU Criminal Law: Maybe We Are Getting There, After All // New Journal of European Criminal Law. 2020. Vol. 11, iss. 1. P. 24. DOI: 10.1177/2032284420903386.

[66] См.: *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.

5. *Журавленко Н. И., Шведова Л. Е.* Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере / Н. И. Журавленко // Общество и право. 2015. № 3 (53). С. 66–70.
6. *Иванцов С. В., Борисов С. В., Узембаева Г. И.* и др. Актуальные проблемы совершенствования системы мер криминологического предупреждения преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных сетей // Всероссийский криминологический журнал. 2018. Т. 12. № 6. С. 776–784. DOI: 10.17150/2500-4255.2018.12(6).776–784.
7. *Карамнов А. Ю., Дворецкий М. Ю.* Законодательство Великобритании о преступлениях в сфере компьютерной информации // Социально-экономические явления и процессы. 2013. № 8 (54). С. 164–167.
8. *Кириленко В. П., Алексеев Г. В.* Актуальные проблемы противодействия преступлениям экстремистской направленности // Всероссийский криминологический журнал. 2018. Т. 12. № 4. С. 561–571. DOI: 10.17150/2500-4255.2018.12(4).561–571.
9. *Кириленко В. П., Алексеев Г. В.* Гармонизация российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы // Всероссийский криминологический журнал. 2020. Т. 14. № 6. С. 898–913. DOI: 10.17150/2500-4255.2020.14(6).898–913.
10. *Кириленко В. П., Алексеев Г. В.* Легитимность демократии в работах Макса Вебера и Карла Шмитта // Правоведение. 2018. Т. 62. № 3. С. 501–517. DOI: 10.21638/11701/spbu25.2018.305.
11. *Кириленко В. П., Алексеев Г. В.* Политические технологии и международный конфликт в информационном пространстве Балтийского региона // Балтийский регион. 2018. Т. 10. № 4. С. 20–38. DOI: 10.5922/2079-8555-2018-4-2.
12. *Кириленко В. П., Алексеев Г. В.* Противодействие идеологии современного терроризма // Управленческое консультирование. 2018. № 5 (113). С. 8–18. DOI: 10.22394/1726-1139-2018-5-8–18.
13. *Кириленко В. П., Алексеев Г. В.* Экстремисты: преступники и жертвы радикального насилия // Всероссийский криминологический журнал. 2019. Т. 13. № 4. С. 612–628. DOI: 10.17150/2500-4255.2019.13(4).612–628.
14. *Кириленко В. П., Шамахов В. А., Алексеев Г. В.* Свобода слова и медиабезопасность. СЗИУ РАНХиГС. Санкт-Петербург. 2019. 440 с.
15. *Номоконов В. А., Тропина Т. Л.* Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. 2013. № 5 (10). С. 148–160.
16. *Одинцова Н. Е., Репецкая А. Л.* Проблемные аспекты отечественного и зарубежного законодательства в противодействии пропаганде педофилии // Международный журнал гуманитарных и естественных наук. 2019. № 11–3 (38). С. 84–89. DOI: 10.24411/2500-1000-2019-11821.
17. *Репецкая А. Л.* Современное состояние, структура и тенденции российской преступности // Вестник Омского университета. Серия: Право. 2018. № 1 (54). С. 151–156. DOI: 10.25513/1990-5173.2018.1.151–156.
18. *Черненко Т. Г.* Квалификация совокупности преступлений // Вестник Омского университета. Серия: Право. 2014. № 1 (38). С. 14–162.
19. *Энгельгардт А. А.* О понимании мошенничества в сфере компьютерной информации // Вестник Московского университета МВД России. 2016. № 8. С. 84–90.
20. *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.
21. *Arnold N., Mahoney W., Derrick D., Ligon G.* & Harms M. Feasibility of a Cyber Attack on National Critical Infrastructure by a Non-State Violent Extremist Organization // Journal of Information Warfare. 2015. Vol. 14, iss. 1. Pp. 84–100.
22. *Awan I.* Cyber-Extremism: Isis and the Power of Social Media // Social Science and Public Policy. 2017. Vol. 54. Pp. 138–149. DOI: 10.1007/s12115-017-0114-0.
23. *Brenner S. W.* Cyberthreats and the Decline of the Nation-State. London : Routledge. 2014. 182 p.
24. *Broadhurst R. G., P. Grabosky, M. Alazab, S. Chon.* 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.
25. *Brosché J., Legnér M., Kreutz J., Ijla A.* Heritage under Attack: Motives for Targeting Cultural Property During Armed Conflict // International Journal of Heritage Studies 2017. Vol. 23, iss. 3. Pp. 248–260. DOI: 10.1080/13527258.2016.1261918.
26. *Buono L.* Fighting Cybercrime Between Legal Challenges and Practical Difficulties: EU and National Approaches // ERA Forum. 2016. Vol. 17. Pp. 343–353. DOI: 10.1007/s12027-016-0432-5.
27. *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.
28. *Cooper M.* How Cyber Crime Damages Lives // ITNOW. 2020. Vol. 62, iss. 1. Pp. 36–37. DOI: 10.1093/itnow/bwaa016.
29. *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.
30. *Dalgaard-Nielsen A.* Violent Radicalization in Europe: What We Know and What We Do Not Know // Stud Conflict Terrorism 2010. Vol. 33, iss. 9. Pp. 797–814. DOI: 10.1080/1057610X.2010.501423.
31. *De Silva S.* Cyber Crime and the Law // ITNOW. 2016. Vol. 58, iss. 4. Pp. 28–29. DOI: 10.1093/itnow/bww101.
32. *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.

33. *Earl J.* Protest Online: Theorizing the Consequences of Online Engagement. In L. Bosi, M. Giugni & K. Uba (eds.). The Consequences of Social Movements. Cambridge : Cambridge University Press. 2016. Pp. 363–400. DOI: 10.1017/CBO9781316337790.015.
34. *Fisher J. L.* A Clinic's Place in the Supreme Court Bar // Stanford Law Review. 2013 (2011). Vol. 65, iss. 1. Pp. 137–201. DOI: 10.2139/ssrn.1921430.
35. *Gercke M.* Europe's Legal Approaches to Cybercrime // ERA Forum. 2009. Vol. 10. Pp. 409–420. DOI: 10.1007/s12027-009-0132-5.
36. Hacking Politics: How Geeks, Progressives, the Tea Party, Gamers, Anarchists and Suits Teamed up to Defeat SOPA and Save the Internet / D. Moon, P. Ruffini, D. Segal (eds). OR Books. 2013. 316 p.
37. *Justice J. W., Bricker B. J.* Hacked: Defining the 2016 Presidential Election in the Liberal Media / J. W. Justice // Rhetoric and Public Affairs. 2019. Vol. 22, iss. 3. Pp. 389–420. DOI: 10.14321/rhetpublaffa.22.3.0389.
38. *Kapczynski A.* Intellectual Property's Leviathan // Law and Contemporary Problems. 2015. Vol. 77, iss. 4. Pp. 131–145.
39. *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. DOI: 10.1007/s10610-020-09439-2.
40. *Kettemann M. C.* Ensuring Cybersecurity through International Law // Revista Española de Derecho Internacional. Vol. 69, iss. 2. Pp. 281–290.
41. *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.
42. *Leukfeldt E. R., A. Lavorgna, E. R. Kleemans.* 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.
43. *Martin J., Munksgaard R., Coomber R.* & oths. 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.
44. *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.
45. *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.
46. *Nuotio K.* A Legitimacy-Based Approach to EU Criminal Law: Maybe We Are Getting There, after all // New Journal of European Criminal Law. 2020. Vol. 11, iss. 1. Pp. 20–39. DOI:10.1177/2032284420903386.
47. *Reep-van den Bergh C. M. M., Junger M.* Victims of Cybercrime in Europe: A Review of Victim Surveys // Crime Science. 2018. Vol. 7, art No. 5. DOI: 10.1186/s40163-018-0079-3.
48. *Rucht D.* Movement Allies, Adversaries, and Third Parties. 2007. DOI:10.1002/9780470999103.ch9.
49. *Schmitt Carl.* Theorie des Partisanen. Zwischenbemerkung zum Begriff des Politischen. Duncker & Humblot. 1963.
50. *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.
51. *Taylor R. W., Fritsch E. J., Liederbach J.* Digital Crime and Digital Terrorism. New York : Prentice Hall Press, 2014. 416 p.
52. Tarrow S. Power in Movement: Social Movements, Collective Action and Politics. New York : Cambridge University Press. 1994. 251 p.
53. *Tomašević V., Ilić-Kosanović T., Ilić D.* (2020) Skills Engineering in Sustainable Counter Defense Against Cyber Extremism. In: Al-Masri A., Al-Assaf Y. (eds). Sustainable Development and Social Responsibility. Vol. 2. Advances in Science, Technology & Innovation (IEREK Interdisciplinary Series for Sustainable Development). Springer, Cham. DOI: 10.1007/978-3-030-32902-0_25.
54. *Van der Wagen 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.
55. *Walden I.* Computer Crimes and Digital Investigations / I. Walden. Oxford : Oxford University Press. 2016. 600 p.
56. *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.

References

1. 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.
2. Arnold, N., Mahoney, W., Derrick, D., Ligon, G. & Harms, M. Feasibility of a Cyber Attack on National Critical Infrastructure by a Non-State Violent Extremist Organization // Journal of Information Warfare. 2015. Vol. 14, iss. 1. Pp. 84–100.
3. Awan, I. Cyber-Extremism: Isis and the Power of Social Media // Social Science and Public Policy 2017. Vol. 54. Pp. 138–149. DOI: 10.1007/s12115-017-0114-0.
4. Bastrykin, A. I. Crimes Against Minors in the Internet Space: On the Issue of Victimological Prevention and Criminal-Legal Assessment [Prestupleniya protiv nesovershennoletnikh v internet-prostranstve: k voprosu o viktimologicheskoi profilaktike i ugolovno-pravovoi otsenke] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2017. Vol. 11. No. 1. Pp. 5–12. DOI: 10.17150/2500-4255.2017.11 (1).5–12. (in rus)

5. Baturin, Yu. M., Polubinskaya, S. V. What Makes Virtual Crimes Real [Chto delaet virtual'nye prestupleniya real'nymi] // Proceedings of the Institute of State and Law of the Russian Academy of Sciences [Trudy Instituta gosudarstva i prava Rossiiskoi akademii nauk]. 2018. V. 13. No. 2. Pp. 9–35. (in rus)
6. Begishev, I. R. Khisamova, Z. I. Criminological Risks of Using Artificial Intelligence [Kriminologicheskie riski primeneniya iskusstvennogo intellekta] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2018. T. 12, No. 6. Pp. 767–775. DOI: 10.17150 / 2500-4255.2018.12 (6). 767-775. (in rus)
7. Brenner, S. W. Cyberthreats and the Decline of the Nation-State. London : Routledge. 2014. 182 p.
8. Broadhurst, R. G., P. Grabosky, M. Alazab, S. Chon. 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.
9. Brosché, J., Legnér, M., Kreutz, J., Ijla, A. Heritage under Attack: Motives for Targeting Cultural Property During Armed Conflict// International Journal of Heritage Studies 2017. Vol. 23, iss. 3. Pp. 248–260. DOI: 10.1080/13527258.2016.1261918.
10. Buono, L. Fighting Cybercrime Between Legal Challenges and Practical Difficulties: EU and National Approaches // ERA Forum. 2016. Vol. 17. Pp. 343–353. DOI: 10.1007/s12027-016-0432-5.
11. 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.
12. Chernenko, T. G. The Qualification of the Aggregate of Crimes [Kvalifikatsiya sovokupnosti prestuplenii] // Bulletin of Omsk University. Series: Law [Vestnik Omskogo universiteta. Seriya: Pravo.]. 2014. No. 1 (38). Pp. 148–162. (in rus)
13. Cooper, M. How Cyber Crime Damages Lives // ITNOW. 2020. Vol. 62, iss. 1. Pp. 36–37. DOI: 10.1093/itnow/bwaa016.
14. 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.
15. Dalgaard-Nielsen, A. Violent Radicalization in Europe: What We Know and What We Do Not Know // Stud Conflict Terrorism 2010. Vol. 33, iss. 9. Pp. 797–814. DOI: 10.1080/1057610X.2010.501423.
16. De Silva, S. Cyber Crime and the Law // ITNOW 2016. Vol. 58, iss. 4. Pp. 28–29. DOI: 10.1093/itnow/bww101.
17. 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.
18. Earl, J. Protest Online: Theorizing the Consequences of Online Engagement. In L. Bosi, M.Giugni & K. Uba (eds.). The Consequences of Social Movements. Cambridge : Cambridge University Press. 2016. Pp. 363–400. DOI: 10.1017/CBO9781316337790.015.
19. Engelhardt, A. A. On Understanding of Fraud in the Field of Computer Information // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2016. No. 8. Pp. 84–90. (in rus)
20. Fisher, J. L. A Clinic's Place in the Supreme Court Bar // Stanford Law Review. 2013 (2011). Vol. 65, iss. 1. Pp. 137–201. DOI: 10.2139/ssrn.1921430.
21. Gercke, M. Europe's Legal Approaches to Cybercrime // ERA Forum. 2009. Vol. 10. Pp. 409–420. DOI: 10.1007/s12027-009-0132-5.
22. Hacking Politics: How Geeks, Progressives, the Tea Party, Gamers, Anarchists and Suits Teamed up to Defeat SOPA and Save the Internet / D. Moon, P. Ruffini, D. Segal (eds). OR Books. 2013. 316 p.
23. Ivantsov, S. V., Borisov, S. V., Uzembaeva, G. I., Muzychuk, T. L., Tishchenko, Yu. Yu. Actual Problems of Improving the System of Measures for Criminological Prevention of Extremist Crimes Committed Using Information and Telecommunication Networks [Aktual'nye problemy sovershenstvovaniya sistemy mer kriminologicheskogo preduprezhdeniya prestuplenii ekstremistskoi napravlennosti, sovershaemykh s ispol'zovaniem informatsionno-telekommunikatsionnykh setei] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2018. T. 12, No. 6. Pp. 776–784. DOI: 10.17150/2500-4255.2018.12(6).776–784 (in rus)
24. Justice, J. W., Bricker, B. J. Hacked: Defining the 2016 Presidential Election in the Liberal Media / J. W. Justice // Rhetoric and Public Affairs 2019. Vol. 22, iss. 3. Pp. 389–420. DOI: 10.14321/rhetpublaffa.22.3.0389.
25. Kapczynski, A. Intellectual Property's Leviathan // Law and Contemporary Problems. 2015. Vol.77, iss. 4. Pp. 131–145.
26. Karamnov, A. Yu., Dvoretsky, M. Yu. UK Legislation on Crimes in the Field of Computer Information [Zakonodatel'stvo Velikobritanii o prestupleniyakh v sfere komp'yuternoi informatsii] // Socio-Economic Phenomena and Processes [Sotsial'no-ekonomicheskie yavleniya i protsessy]. 2013. № 8 (54). Pp. 164–167. (in rus)
27. 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. DOI: 10.1007/s10610-020-09439-2.
28. Kettemann, M. C. Ensuring Cybersecurity through International Law // Revista Española de Derecho Internacional. Vol. 69, iss. 2. Pp. 281–290.
29. Kirilenko, V. P., Alekseev, G. V. Actual Problems of Countering Extremist Crimes [Aktual'nye problemy protivodeistviya prestupleniyam ekstremistskoi napravlennosti] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2018. Vol. 12. No. 4. Pp. 561–571. DOI: 10.17150/2500-4255.2018.12 (4).561–571. (in rus)
30. Kirilenko, V. P., Alekseev, G. V. Harmonization of Russian Criminal Legislation on Combating Cybercrime with the Legal Standards of the Council of Europe [Garmonizatsiya rossiiskogo ugolovnogo zakonodatel'stva o protivodeistvii kiberprestupnosti s pravovymi standartami Soveta Evropy] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2020. Vol. 14. No. 6. Pp. 898–913. DOI: 10.17150/2500-4255.2020.14(6).898–913. (in rus)

31. Kirilenko, V. P., Alekseev, G. V. The Legitimacy of Democracy in the Works of Max Weber and Karl Schmitt [Legitimnost' demokratii v rabotakh Maksa Vebera i Karla Shmitta] // Jurisprudence [Pravovedenie]. 2018. Vol. 62. No. 3. Pp. 501–517. DOI: 10.21638/11701/spbu25.2018.305. (in rus)
32. Kirilenko, V. P., Alekseev, G. V. Political Technologies and International Conflict in the Information Space of the Baltic Region [Politicheskie tekhnologii i mezhdunarodnyi konflikt v informatsionnom prostranstve Baltiiskogo regiona] // Baltic Region [Baltiiskii region]. 2018. Vol. 10. No. 4. Pp. 20–38. DOI: 10.5922/2079-8555-2018-4-2. (in rus)
33. Kirilenko, V. P., Alekseev, G. V. Counteracting the Ideology of Modern Terrorism [Protivodeistvie ideologii sovremennogo terrorizma] // Administrative Consulting [Upravlencheskoe konsul'tirovanie]. 2018. No. 5 (113). Pp. 8–18. DOI: 10.22394/1726-1139-2018-5-8-18. (in rus)
34. Kirilenko, V. P., Alekseev, G. V. Extremists: Criminals and Victims of Radical Violence [Ekstremisty: prestupniki i zhertvy radikal'nogo nasiliya] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2019. Vol. 13. No. 4. Pp. 612–628. DOI: 10.17150/2500-4255.2019.13(4).612–628. (in rus)
35. Kirilenko, V. P., Shamakhov, V. A., Alekseev G. V. Freedom of Speech and Media Safety [Svoboda slova i mediabezopasnost']. SZIU RANEPA. St. Petersburg. 2019. 440 p. (in rus)
36. 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.
37. Leukfeldt, E. R., A. Lavorgna, E. R. Kleemans. 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.
38. Martin, J., Munksgaard, R., Coomber R. & oths. 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.
39. 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.
40. 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.
41. Nomokonov, V. A., Tropina, T. L. Cybercrime: Forecasts and Problems of Struggle [Kiberprestupnost': prognozy i problemy bor'by] // Criminalist Library [Biblioteka kriminalista]. 2013. № 5 (10). Pp. 148–160. (in rus)
42. Nuotio, K. A Legitimacy-Based Approach to EU Criminal Law: Maybe We Are Getting There, After All // New Journal of European Criminal Law. 2020. Vol. 11, iss. 1. Pp. 20–39. DOI: 10.1177/2032284420903386.
43. Odintsova, N. E., Repetskaya, A. L. Problematic Aspects of Domestic and Foreign Legislation in Countering the Propaganda of Pedophilia [Problemnye aspekty otechestvennogo i zarubezhnogo zakonodatel'stva v protivodeistvii propagande pedofilii] // International Journal of Humanities and Natural Sciences [Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk]. 2019. No. 11–3 (38). Pp. 84–89. DOI: 10.24411/2500-1000-2019-11821. (in rus)
44. Reep-van den Bergh, C. M. M., Junger M. Victims of Cybercrime in Europe: A Review of Victim Surveys // Crime Science. 2018. Vol. 7, art No. 5. DOI: 10.1186/s40163-018-0079-3.
45. Repetskaya, A. L. Current State, Structure and Trends of Russian Crime [Sovremennoe sostoyanie, struktura i tendentsii rossiiskoi prestupnosti] // Bulletin of Omsk University. Series: Law [Vestnik Omskogo universiteta. Seriya: Pravo]. 2018. No. 1 (54). Pp. 151–156. DOI: 10.25513/1990-5173.2018.1.151–156. (in rus)
46. Rucht, D. Movement Allies, Adversaries, and Third Parties. 2007. DOI: 10.1002/9780470999103.ch9.
47. Schmitt, Carl. Theorie des Partisanen. Zwischenbemerkung zum Begriff des Politischen. Duncker & Humblot. 1963.
48. 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.
49. Tarrow, S. Power in Movement: Social Movements, Collective Action and Politics. New York : Cambridge University Press. 1994. 251 p.
50. Taylor, R. W., Fritsch, E. J., Liederbach, J. Digital Crime and Digital Terrorism. New York : Prentice Hall Press, 2014. 416 p.
51. Tomašević, V., Ilić-Kosanović, T., Ilić, D. (2020) Skills Engineering in Sustainable Counter Defense Against Cyber Extremism. In: Al-Masri A., Al-Assaf Y. (eds.) Sustainable Development and Social Responsibility. Vol. 2. Advances in Science, Technology & Innovation (IEREK Interdisciplinary Series for Sustainable Development). Springer, Cham. DOI: 10.1007/978-3-030-32902-0_25.
52. Van der Wagen, 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.
53. Walden, I. Computer Crimes and Digital Investigations / I. Walden. Oxford : Oxford University Press. 2016. 600 p.
54. 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.
55. Zharova, A. K. Routing and IP to Ensure the Legal Regulation of Internet Relations [Marshrutizatsiya i IP dlya obespecheniya pravovogo regulirovaniya internet-otnoshenii] // Bulletin of the Russian State Humanitarian University. Series "Informatics. Information Security. Mathematics" [Vestnik RGGU. Seriya «Informatika. Informatsionnaya bezopasnost'. Matematika»]. 2019. No. 2. Pp. 32–42. DOI: 10.28995/2686-679X-2019-2-32-42. (in rus)
56. Zhuravlenko, N. I., Shvedova, L. E. Problems of Combating Cybercrime and Promising Areas of International Cooperation in this Area [Problemy bor'by s kiberprestupnost'yu i perspektivnye napravleniya mezhdunarodnogo sotrudnichestva v etoi sfere] // Society and Law [Obshchestvo i pravo]. 2015. No. 3 (53). Pp. 66–70. (in rus)