ISSN 2500-4255

Научная статья
УДК 343.9.01
DOI 10.17150/2500-4255.2021.15(6).681-691

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ КРИМИНОЛОГИЧЕСКОЙ НАУКИ И ПРАКТИКИ ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВА

А.Л. Осипенко, В.С. Соловьев
Краснодарский университет МВД России, г. Краснодар, Российская Федерация

Информация о статье

Дата поступления
30 сентября 2021 г.

Дата принятия в печать
29 ноября 2021 г.

Дата онлайн-размещения
28 декабря 2021 г.

Ключевые слова

Криминология; киберпреступность; кибербезопасность; киберпространство; цифровизация; виртуализация; искусственный интеллект; Интернет; национальная безопасность; предупреждение преступности

Аннотация. Процесс цифровизации общества, связанный с масштабным внедрением цифровых технологий во все значимые социальные сферы, наряду с позитивными эффектами оказал мощное влияние на трансформацию преступности и криминогенных факторов. В связи с этим возрастает актуальность исследования перспектив криминологической науки в обновленных условиях, усиления ее роли в обеспечении национальной безопасности, изменения направления совершенствования ее методологии. В статье определены основные криминальные угрозы безопасности цифрового пространства: стремительное нарастание его криминализации из-за наличия привлекательных для преступности качеств (наднациональный характер киберпространства, широкое использование в нем средств анонимизации и шифрования данных, применимость дистанционных способов совершения преступлений и сокрытия их следов и др.); образование и расширение криминогенных зон киберпространства, особое место среди которых занимает DarkNet; применение криминалитетом «цифровых» методов противодействия правоохранительным органам, в том числе использование криптовалют и искусственного интеллекта. Делается вывод о том, что указанные обстоятельства обусловливают потребность в изменении методологии криминологической науки и практики предупреждения преступлений. Сбор и обобщение данных из общедоступных цифровых источников, их анализ с применением технологий больших данных приобретают особый научный потенциал, связанный с возможностью обнаружения неявных закономерностей и получения на этой основе криминологического знания, недостижимого иными методами. В процессе цифровизации общества развиваются условия для внедрения упреждающей модели правоохранительной деятельности, опирающейся на применение методов предиктивной аналитики. Становится возможным оперативное выявление сигналов, свидетельствующих о криминальной активности, требующей как конкретной реакции со стороны правоохранительных органов, так и системных управленческих решений. Широкие перспективы открываются для прогнозирования индивидуального преступного поведения на основе анализа сетевой активности конкретных лиц. С учетом этого авторами выделяются наиболее актуальные направления развития криминологической науки и практики предупреждения преступлений в условиях цифровизации общества.

Original article

MAIN TRENDS IN THE DEVELOPMENT OF CRIMINOLOGICAL THEORY AND CRIME PREVENTION PRACTICE IN THE CONTEXT OF THE DIGITALIZATION OF SOCIETY

Anatoliy L. Osipenko, Vladislav S. Solovev
Krasnodar University of the Ministry of Internal Affairs of Russia, Krasnodar, the Russian Federation

Article info

Received
2021 September 30

Accepted
2021 November 29

Available online
2021 December 28

Abstract. The digitalization of society, associated with a large-scale introduction of digital technologies in all socially relevant spheres, not only brough about positive changes, but also had a powerful effect on the transformation of crime and criminogenic factors. This has created an urgent need for understanding the prospects of criminological science in the new conditions, for strengthening its role in ensuring national security, for improving its methodology in new ways. The authors define key criminal threats to the security of the digital space: a rapid increase of its criminalization

ISSN 2500-4255

Keywords

Criminology; cybercrime; cyber security; cyber space; digitalization; virtualization; artificial intelligence; Internet; national security; crime prevention

due to the features attractive for criminals (trans-national character of cyberspace, widespread anonymization and encryption, digital means of committing crimes and concealing their traces, etc.); the emergence and widening of criminogenic zones of cyberspace, with DarkNet holding a special place; the use of «digital» methods of resisting law enforcement, including cryptocurrencies and artificial intelligence. It is concluded that the abovementioned circumstances make it necessary to change the methodology of criminological research and the practice of law enforcement. The collection and generalization of information from publicly available digital sources, its analysis with the use of big data acquire a special research potential connected with the possibility of finding hidden regularities and obtaining criminological knowledge that cannot be found elsewhere. The digitalization of society creates conditions for the introduction of a preventive model of law enforcement based on predictive analysis methods. It becomes possible to quickly detect signs of criminal activity that require both a specific reaction of law enforcement and systemic managerial decisions. It also opens broad prospects for predicting individual criminal behavior by analyzing the Internet activity of specific individuals. The authors then highlight the most relevant directions for the development of criminological theory and the practice of crime prevention in the conditions of the digitalization of society.

В современных условиях особую роль среди процессов, оказывающих существенное влияние на социальные изменения, играет цифровизация, связанная с масштабным внедрением цифровых технологий во все сферы жизни общества. В качестве главного драйвера ускоренного перехода к информационному обществу она активно поддерживается государством. В то же время наряду с очевидными позитивными социальными эффектами цифровизация получает мощное отражение в трансформации преступности и многих криминогенных факторов, порождая новые вызовы и угрозы.

В утвержденной в июле 2021 г. Стратегии национальной безопасности Российской Федерации[1] (далее — Стратегия) обозначено, что достижение целей обеспечения государственной и общественной безопасности осуществляется путем реализации государственной политики, направленной на решение ряда задач, в числе которых названо предупреждение и пресечение правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе легализации преступных доходов, финансирования терроризма, организации незаконного распространения наркотических средств и психотропных веществ, а также использования в противоправных целях цифровых валют. Здесь же среди негативных явлений выделяются: распространение недостоверной информации, направленной на дестабилизацию общественно-политической ситуации в Российской Федерации, размещение в сети Интернет материалов террористических и экстремистских организаций, призывов к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, совершению самоубийства. В этот список включаются и пропаганда криминального образа жизни, потребления наркотических средств и психотропных веществ, размещение иной противоправной информации.

Перечисление в Стратегии конкретных криминальных угроз, нарастающих в цифровом информационном пространстве, ставит перед криминологической наукой особые задачи по накоплению и обобщению криминологически значимой информации как о видах преступности, способных существовать только в цифровой среде, так и о традиционных преступлениях, получивших в условиях цифровизации новые возможности при подготовке, совершении и сокрытии следов. Важно, чтобы на этой основе разрабатывалась и развивалась эффективная система предупреждения преступлений.

Развитие «цифровой составляющей» криминологической науки и правоохранительной практики должно способствовать достижению обозначенной в Стратегии цели обеспечения информационной безопасности в виде укрепления суверенитета Российской Федерации в информационном пространстве. Это возможно за счет реализации государственной политики, направленной на решение широкого круга задач в области информационной безопасности, одной из которых выступает формирование условий для эффективного предупреждения, выявления

[1] О Стратегии национальной безопасности Российской Федерации : указ Президента РФ от 2 июля 2021 г. № 400 // СПС «КонсультантПлюс».

и пресечения преступлений и иных правонарушений, совершаемых с использованием информационно-коммуникационных технологий.

Ошибкой было бы не использовать и высокий антикриминальный потенциал современных цифровых технологий. В Стратегии к действенным средствам обеспечения информационной безопасности государства причислены квантовые вычисления и технологии искусственного интеллекта. Последние призваны способствовать решению наиболее сложных задач, требующих особых интеллектуальных усилий. Ключевой составляющей их функционирования считается машинное обучение, обеспечивающее последовательное повышение эффективности достижения конкретной цели за счет применения алгоритмов, оценивающих результаты, получаемые на основе множества исходных данных, и выявляющих с применением статистических методов определенные закономерности и оптимальные наборы действий, которые могут быть использованы при последующем решении поставленных задач, в том числе правоохранительной направленности.

Процесс цифровизации сопровождается виртуализацией реальности, оказывающей существенное влияние на многие общественные процессы, в том числе на характер преступности и механизм противодействия ей. Соответствующие процессы резко активизируются на фоне ускоренного развития информационных технологий. Происходит постепенное «размывание» границ, отделяющих виртуальный мир от реального. Погружаясь в цифровое киберпространство, индивид отходит от реального мира, воспринимает в качестве реальности ее искусственную подмену, причем «виртуальная реальность в современной ее форме влияет не только на личность, но и на всю социальную систему, преобразуя последнюю» [1].

В обиходной речи укоренились такие термины, как «виртуальное общение», «виртуальное пространство», «виртуальная валюта», «виртуальное обучение». Социологи уже оперируют понятием «виртуальные ценности». По их мнению, характерная для современного социума виртуализация системы ценностей «тяжело переживается обычным человеком, особенно молодежью, компенсируется различного рода маргинальными, виртуальными или фантастическими формами идентификации: молодежными субкультурами, сектами, религиозным или псевдорелигиозным фундаментализмом, анархизмом» [2].

Виртуализация информационного пространства, сопровождаемая расширением спектра анонимных источников, отсутствием ответственности за достоверность информации, совершенствованием технологий дезинформирования, ведет к утрате доверия к получаемым сведениям и, как следствие, к социальной апатии, основанной на ощущении абсурдности всего происходящего. Несущие высокий криминогенный потенциал *технологии фальсификации информации ложатся в основу конфликтной мобилизации больших групп людей, их применение способно спровоцировать масштабные экстремистские акции и массовые беспорядки*.

Особым объектом криминологического изучения, объединяющим информационное и физическое пространство, стоит признать *киберпространство, проявляющееся как виртуальная среда реализации социальных отношений, возникающая в результате сложных взаимодействий пользователей сети с техническими устройствами ее инфраструктуры при формировании и использовании информационных ресурсов*. Исследователи выделяют его особые качества, существенные с позиций криминологии, поскольку киберпространство «стало новой средой жизнедеятельности человека как субъекта киберсоциализации… обеспечивает отличные от условий реальной жизнедеятельности возможности коммуникации, принадлежности человека к определенным социальным категориям, референтной группе и относительно безопасное экспериментирование с идентичностью» [3]. Это связано главным образом *с возможностью формирования его участниками особых виртуальных образов, которым могут быть присвоены практически любые атрибуты нереальной жизни, причем нередко этот виртуальный образ представляется для индивида гораздо более значимым, нежели образ реальный*. Такая виртуализация самопрезентации во многих случаях сопровождается искажением восприятия реальных событий, стиранием границ между вымыслом и правдой, подменой реальных ценностей мнимыми и, как результат, неприятием важных социальных норм, приводящим к закреплению в социальных сетях условий для склонения к потреблению наркотиков, суициду, вовлечения в антиобщественные движения (экстремизм, АУЕ), террористические организации. Особая опасность воздействия на детей и подростков через искаженные виртуальные образы сетевых «наставников», за которы-

ми скрываются деструктивные личности с букетом психологических комплексов, отмечается на самом высоком уровне[2].

Полагаем, что обобщение названных явлений и процессов (спектр которых продолжает расширяться) с учетом задач, поставленных в Стратегии национальной безопасности, позволяет считать, что для *эффективной системы социально-правового контроля над криминальными процессами в цифровой среде важно выработать особое системное криминологическое представление о новой цифровой и виртуализирующейся реальности, в которой формируются и трансформируются уникальные объекты, подлежащие изучению с позиций криминологии*: «цифровая» преступность, виртуальные образы личности преступника и жертвы, факторы преступности, порождаемые киберсредой. *Необходима и системная адаптация деятельности по предупреждению преступлений, как «высокотехнологичных», так и вполне традиционных, к специфическим условиям цифровой среды*.

Приступая к исследованию направлений криминологического изучения особенностей противодействия преступности в цифровой среде, стоит дать оценку влияния ее специфики на противоправные проявления, которые могут быть выделены в качестве особых криминальных угроз безопасности цифрового пространства.

1. В первую очередь необходимо назвать стремительное нарастание криминализации киберпространства, которое приобрело особые, весьма привлекательные для преступности качества (наднациональный характер, наличие широкого спектра средств анонимизации и шифрования данных, применимость дистанционных, в том числе трансграничных, способов совершения преступлений и сокрытия их следов и др.). Не случайно в опубликованной в апреле 2021 г. Стратегии ЕС по борьбе с организованной преступностью особый акцент сделан на деятельности правоохранительных органов в цифровом пространстве [4]. Специфика киберпространства существенно затрудняет выявление и раскрытие совершаемых в нем преступлений, что влечет увеличение их количества, нарастание масштабов наносимого ущерба и числа жертв. Особенности таких преступлений и специализация многих субъектов на их совершении позволяют выделить особый вид преступности, обозначаемый понятием «киберпреступность». Зарубежные специалисты отмечают сложность оценки роста и масштабов киберпреступности, по которым существующие данные и исследования очень ограниченны [5].

При этом фиксируются два криминальных тренда: во-первых, укрепляется организованность самой киберпреступности, а во-вторых, все чаще для достижения своих криминальных целей ее использует традиционная организованная преступность [6]. И в том и в другом случае происходит расширение применяемых схем преступной деятельности, противодействие которым традиционными средствами невозможно или существенно затруднено. Особое место при этом занимает схема «киберпреступление как услуга», повышающая доступность кибертехнологий для совершения преступлений лицами, не обладающими достаточным уровнем технических знаний, однако способными профинансировать достижение желаемого результата.

Отдельные авторы рассматривают киберпреступность как индустрию с особой организационной инфраструктурой киберпреступлений, направленных на получение прибыли [7].

Обретают новые черты и принципы функционирования криминальных сообществ: хакеры-одиночки, мотивированные любопытством и лозунгами свободного доступа к информации, вытесняются хорошо организованными корыстными преступниками, объединенными в имеющие сетевую структуру группы, совершающие резонансные акции (Cobalt, MoneyTaker, Lazarus и др.). В зарубежной литературе уделяется внимание криминальным сетевым структурам [8], и в частности особенностям их функционирования в DarkNet (теневом Интернете)[3] [9].

2. Криминальные явления в киберпространстве наносят существенный ущерб интересам

[2] Президент России В.В. Путин отметил, что «когда полиция добирается до этих уродов… это совсем другие люди. …Сидит в Интернете такой «крутой Рэмбо», толкает какую-то девчонку или пацана с крыши прыгать, выстраивает целую концепцию, подводя к этому. Как только полиция зашла, в штаны наложил в прямом смысле этого слова» (см.: Встреча с участниками общероссийской акции взаимопомощи «Мы вместе» // Президент России. 2021. URL: http://www.kremlin.ru/events/president/news/65096).

[3] Термином «DarkNet» обозначается сформировавшаяся в сети Интернет подсистема, которая объединяет технологии и коммуникации, призванные обеспечить анонимность их пользователей (в первую очередь — невозможность определения их реального IP-адреса, сведений об их личности и содержания передаваемых пакетов данных).

не только личности, общества, но и государства. Как отмечается в п. 44 Стратегии, деструктивные силы за рубежом и внутри страны предпринимают попытки использования объективных социально-экономических трудностей в Российской Федерации в целях стимулирования негативных социальных процессов, обострения межнациональных и межконфессиональных конфликтов, манипулирования в информационной сфере. Не ослабевает активность разведывательной и иной деятельности специальных служб и организаций иностранных государств, осуществляемой в том числе с использованием подконтрольных им российских общественных объединений и отдельных лиц. Международные террористические и экстремистские организации стремятся усилить пропагандистскую работу и работу по вербовке российских граждан, созданию на территории России своих законспирированных ячеек, вовлечению в противоправную деятельность российской молодежи. Для распространения недостоверной информации, организации незаконных публичных акций широко используются возможности глобальных интернет-компаний.

В киберпространстве в большинстве случаев сложно отличить криминальные действия преступников-одиночек, организованных преступных формирований, в том числе международных, от враждебных акций иностранных государств. Дополнительную остроту проблемам обеспечения национальной безопасности придает наднациональный характер киберпространства, а также отмечаемое в последние годы усиление напряженности между странами по вопросам обеспечения в нем национальных интересов, которое создает дополнительные трудности в реализации процедур взаимной правовой помощи.

3. В киберпространстве образуются и расширяются криминогенные зоны, к которым могут быть причислены сайты противоправной направленности, сегменты социальных сетей. Особое место среди таких зон занимает DarkNet, где имеются почтовые и поисковые системы, места сетевого общения, функционируют торговые площадки, на некоторых из них производится отмывание денег через криптовалютный рынок, торговля оружием, наркотическими веществами, детской порнографией, реквизитами кредитных карт, поддельными документами. По некоторым оценкам, до 57 % сайтов в сети Tor вовлечено в подобную преступную деятельность [10].

4. В киберпространстве происходит концентрация цифровых следов преступной деятельности, которые необходимо использовать в процессе раскрытия и расследования преступлений. Исследование специфики механизмов следообразования в цифровой среде необходимо для грамотной адаптации к ее особенностям применяемых методик выявления и расследования преступлений. С учетом этого в отдельных государствах уже действуют подразделения, специализирующиеся на расследовании киберпреступлений[4]. Есть такие подразделения и в ряде служб центрального аппарата МВД России, и в территориальных органах внутренних дел. Добавим, что недостаточная готовность правоохранительной системы к полноценной работе по предупреждению, выявлению, раскрытию и расследованию преступлений в киберпространстве выступает одним из важнейших факторов, способствующих росту киберпреступности. Для его преодоления важно совершенствовать систему подготовки специалистов, обладающих необходимыми компетенциями, в образовательных организациях МВД России. Кроме того, следует в той или иной мере адаптировать к условиям киберпространства и деятельность большинства подразделений правоохранительных органов, в том числе осуществляющих предупреждение преступлений.

5. Важным обстоятельством, подлежащим изучению с позиций криминологии, является расширение применения криминалитетом «цифровых» методов противодействия правоохранительным органам. По данным обзора Европола за 2020 г., «в таких областях, как DarkNet, преступники усилили сотрудничество и объединили усилия, чтобы дать ответ на общие проблемы. Это означает, что они могут сделать свой криминальный бизнес более устойчивым и, в частности, использовать более совершенные решения в области безопасности с тем, чтобы правоохранительные органы не могли их отслеживать. В целом киберпреступники демонстрируют повышенный уровень операционной безопасности и доказывают, что хорошо осведомлены о том, как скрыть свою личность и преступную деятельность от правоохранитель-

[4] С 2015 г. в Великобритании функционирует спецподразделение по борьбе с преступностью в DarkNet (Joint Operations Cell, JOC). Подобные подразделения созданы в 2018 г. при Европоле и в 2020 г. при Министерстве юстиции США.

ных органов или компаний частного сектора»[5]. С целью затруднения доступа к скрываемой информации и следам преступной активности преступниками применяются криптографические алгоритмы и современные технологии шифрования. Для усложнения отслеживания платежей, связанных с криминальной деятельностью, широко используются криптовалюты[6]. С точки зрения криминологии названные обстоятельства существенно повышают латентность преступлений и служат фактором преступности.

Высокие риски нового качества связаны с использованием преступностью технологий искусственного интеллекта, в результате чего часть криминальной активности может выпасть из поля зрения полиции. На это все чаще обращают внимание зарубежные криминологи [11]. Названные технологии позволяют определять оптимальные стратегии криминальной деятельности[7], осуществлять поиск неизвестных ранее «бизнес-моделей» преступлений, повышающих их прибыльность и уменьшающих вероятность обнаружения полицией. По данным аналитического обзора Центра по противодействию киберпреступности Европола[8], в качестве основных направлений применения искусственного интеллекта в преступной деятельности можно выделить:

– разработку вредоносных программ с усиленными алгоритмами взлома и повышенной скрытностью функционирования;

– дистанционное управление техническими устройствами интернета вещей (например, элементами умного дома) для получения доступа к конфиденциальным данным и создания условий для совершения противоправных действий [12];

– манипулирование системами искусственного интеллекта, управляющими движением транспортных средств и беспилотников, при подготовке и совершении преступлений;

– повышение эффективности алгоритмов подбора паролей к зашифрованным данным и взлом систем компьютерной безопасности;

– усиление устойчивости криптографических систем, используемых для сокрытия следов преступлений;

– формирование «виртуальной личности» в социальных сетях для совершения мошенничеств;

– повышение эффективности методов социальной инженерии с целью выявления потенциальных жертв, сбора конфиденциальной и деловой информации.

Есть сведения об использовании искусственного интеллекта при логистическом планировании маршрутов наркотрафика, основанном на применении беспилотных транспортных средств[9]. В целом использование искусственного интеллекта в противоправных целях является фактором преступности, повлиять на который в настоящее время крайне сложно из-за недостатка криминологической информации в этой области.

Особого внимания заслуживают технологии Deepfakes, которые обеспечивают возможность подменять в обрабатываемом видеофрагменте лица конкретных людей и иные объекты, формировать фальсифицированный видеосюжет, синтезировать фразы, произносимые голосом конкретного человека. Это, например, позволяет:

1. Обходить проверки биометрической аутентификации в системах доступа и платежных системах.

2. Организовывать вымогательство либо преследование конкретных лиц, наносить ущерб их репутации за счет публикации сфаль-

[5] Internet Organised Crime Threat Assessment (IOCTA) // Europol. 2021. URL: https://www.europol.europa.eu/iocta-report.

[6] Показательно, что по результатам интервьюирования проходивших повышение квалификации в Краснодарском университете МВД России сотрудников полиции, занимающихся выявлением и расследованием преступлений, связанных с использованием криптовалют и других виртуальных активов, были получены ответы, что единственными преступлениями, с которыми они сталкиваются, являются мошеннические действия под предлогом покупки криптовалюты. Перспективы раскрытия и расследования преступлений, связанных с реальным использованием криптовалют, по их словам, в настоящее время практически отсутствуют.

[7] По оценкам специалистов, «атаки на основе искусственного интеллекта могут обходить традиционные системы обнаружения более чем в 15 % случаев, в то время как средняя фишинговая атака (без искусственного интеллекта) может быть успешной только в 0,3 % случаев» (см.: Защищаемся от ИИ с помощью ИИ: решения с поддержкой искусственного интеллекта для киберугроз нового поколения // SecurityLab.ru. 2021. URL: https://www.securitylab.ru/analytics/518993.php).

[8] Malicious Uses and Abuses of Artificial Intelligence // Europol. 2021. URL: https://www.europol.europa.eu/publications-documents/malicious-uses-and-abuses-of-artificial-intelligence.

[9] Europol. Serious and organised crime threat assessment. 2017. URL: https://www.europol.europa.eu/socta/2017.

сифицированных материалов. В частности, может использоваться изменение внешности участников порнографического видеоконтента, причем юридические средства защиты граждан от возможности стать «героями» подобных роликов довольно ограниченны из-за практической неприменимости действующих норм Уголовного кодекса в силу слабой изученности соответствующих правовых проблем.

3. Реализовывать мероприятия по дезинформации с целью манипулирования общественным мнением, вмешательства в выборы, провоцирования насилия, общественных беспорядков, экстремистских выступлений.

4. Осуществлять влияние на деятельность финансовых рынков с целью незаконного обогащения за счет изменения котировок или стоимости ценных бумаг.

5. Выполнять незаконные действия в отношении несовершеннолетних за счет вхождения к ним в доверие с использованием виртуальной личности, имитирующей подростка.

Значительную опасность представляет применение названных технологий в манипулировании цифровыми доказательствами в уголовном и гражданском судопроизводстве. Преступники могут умышленно формировать довольно убедительные ложные улики с целью отвлечь следствие от реальных фактов, причем используемые сегодня криминалистические методы проверки подлинности цифровых доказательств недостаточно эффективны при выявлении подобных «подделок». Правоохранительные органы остро заинтересованы в разработке и совершенствовании технологий обнаружения фальсифицированного цифрового контента[10]. В ряде стран распространение поддельных реалистичных аудиовизуальных материалов признано общественно опасным деянием [13].

Таким образом, обобщая изложенное, можно утверждать, что цифровизация оказала существенное влияние на трансформацию криминальных процессов и явлений, породила ряд факторов, которые должны восприниматься как важные вызовы криминологической безопасности. Для их нейтрализации важно не только осуществить поиск новых организационных и тактических подходов к решению задач правоохранительной деятельности в цифровом пространстве, но и в целом произвести обновление направлений развития криминологической науки и практики предупреждения преступлений. При сохранении традиционного предмета криминологии (преступность, ее причины и условия, личность преступника и предупреждение преступлений) важно адаптировать его наполнение к современным условиям, определяемым цифровизацией.

В криминологической науке уже предприняты попытки сформулировать концептуальные основы системного научного знания о технологических инновациях преступности и ее предупреждения под общим термином «киберкриминология» [14]. Существуют и иные точки зрения. Например, А.Н. Игнатов говорит о необходимости развития форсайт-криминологии (от англ. foresight — предвидение, в данном случае в контексте прогнозирования научно-технологического и социального развития) как одной из отраслей криминологии. Научно-технический прогресс обусловливает необходимость формирования в качестве одного из направлений указанной отрасли NBIC-криминологии[11] — криминологии высоких технологий [15]. В научном обороте используется и термин «цифровая криминология» [16].

Киберкриминология должна включать в себя криминологическую информацию о киберпреступности, ее детерминантах, личности киберпреступника и жертвы киберпреступления, системе криминологического предупреждения (киберпредупреждения) и традиционного криминологического предупреждения преступлений в современном и будущем киберпространстве [14]. В то же время, несмотря на очевидную актуальность и своевременность обозначенной сферы криминологического знания, возникла серьезная проблема ее наполнения актуальной криминологической информацией и, как следствие, недостаточно эффективной разработки действенной системы предупреждения преступлений, совершаемых с использованием современных цифровых технологий.

Анализ диссертационных исследований, защищенных в течение последних пяти лет (с сентября 2016 г.) по научной специальности 12.00.08 — уголовное право и криминология; уголовно-исполнительное право, позволяет констатировать, что вопросам противодействия преступлениям, совершаемым с использова-

[10] Например, в 2020 г. выпущен новый программный продукт для выявления сфальсифицированного видео Microsoft Video Authenticator.

[11] Направление, изучающее криминальные риски NBIC-технологий (нано-, био-, информационных и когнитивных технологий).

нием цифровых технологий, было посвящено 18 работ. Из них только одна кандидатская диссертация обладает действительно криминологическим содержанием [17], а в темах трех работ заявлено уголовно-правовое и криминологическое исследование. Таким образом, около 86 % научного материала, содержащегося в диссертационных исследованиях, посвящено уголовно-правовым вопросам. Соответственно, практически все предлагаемые меры противодействия преступлениям, совершаемым с использованием современных цифровых технологий, сводятся к корректировке уголовного законодательства и рекомендациям по его применению. Нельзя назвать достаточно высоким и качество криминологических работ. Исследования базируются на традиционных методах, в большинстве случаев опирающихся на анкетирование разного рода специалистов, а в качестве мер предупреждения преступлений в основном предлагается возложение на сотрудников правоохранительных органов обязанностей по проведению бесед с определенными категориями граждан по вопросам виктимологической профилактики.

Между тем цифровизация должна послужить серьезным стимулом для развития криминологических методов исследования преступности. Ученые отмечают, что широкое повседневное использование инфокоммуникационных технологий организациями и отдельными лицами создает колоссальные объемы данных, которые опосредуют социальные события, действия и опыт. Такие данные являются, в частности, и ресурсами для криминальных манипуляций и управления социальными субъектами. Кроме того, использование технологий анализа больших данных открывает перед криминологией новые возможности [18].

Сбор и обобщение данных из общедоступных цифровых источников, получившие в зарубежной литературе название Open Source Intelligence (OSINT), их анализ с применением технологий больших данных имеют, в частности, существенный научный потенциал, связанный с возможностью обнаружения неявных закономерностей и получения на этой основе ценного криминологического знания, недостижимого иными методами. Обработка доступных сведений с применением цифровых аналитических технологий обеспечивает возможность изучать латентную преступность, устанавливать неявные связи между изучаемыми лицами и явлениями для исследования причинности преступности и механизмов преступного поведения, оценивать эффективность конкретных профилактических мероприятий, получать иную значимую для криминологии информацию. Технологии искусственного интеллекта, обладающие особым прогностическим потенциалом, должны использоваться при принятии эффективных управленческих решений. В совокупности это позволяет обеспечить условия для внедрения упреждающей модели правоохранительной деятельности, которая опирается на применение методов предиктивной аналитики с анализом всей оперативной информации[12].

Обозначенная модель предполагает оперативное выявление сигналов, свидетельствующих о криминальной активности, требующей как конкретной реакции со стороны правоохранительных органов, так и системных управленческих решений (криминализация определенных деяний, обновление нормативно-правовой базы предупреждения преступлений, меры по корректировке общесоциальной профилактики, перераспределение финансовых, кадровых и других ресурсов и т.п.).

Широкие перспективы открываются и для прогнозирования индивидуального преступного поведения на основе анализа сетевой активности конкретных лиц. Особое место занимают методы контроля, предполагающие, в частности, мониторинг поведения отдельных категорий граждан, прогнозирование их индивидуального преступного поведения для нейтрализации потенциальных криминальных угроз. Соответствующие технологии, уже внедряемые в деятельность полиции некоторых государств, опираются на масштабный мониторинг сетевых информационных ресурсов, анализ потребляемого в ходе внутрисетевой активности контента, развитие систем видеонаблюдения с применением искусственного интеллекта, обобщение данных от операторов мобильной связи о перемещениях и коммуникациях граждан; учет персональных данных и сведений о финансовых транзакциях и т.п. Цифровое профилирование преступного поведения, осуществляемое методами математического моделирования и прогнозирования, позволяет структурировать и моделировать

[12] Владимир Колокольцев выступил на пленарном заседании Международного полицейского саммита // Министерство внутренних дел РФ. 2019. URL: https://мвд.рф/news/item/18681665.

цифровой профиль (портрет) преступника [19, с. 427]. В качестве примера реального использования искусственного интеллекта в этой сфере можно привести работу с 2012 по 2018 г. проекта под названием Palantir в Новом Орлеане (США), в рамках которого собиралась информация о жителях города: их круге общения, работе, перемещениях, активности в соцсетях и пр. На основании полученных данных искусственный интеллект анализировал социальную картину и пытался определить будущих преступников и жертв преступлений. Palantir успешно определил около 80 % преступников, использующих огнестрельное оружие [20].

Важно учесть, что для повышения эффективности названной модели, обеспечения ее научного сопровождения необходимо сформировать правовые основы доступа к массивам используемых в ней оперативно значимых данных уполномоченных специалистов, проводящих криминологические исследования и реализующих мероприятия по предупреждению преступлений.

Поводя итоги, попытаемся обобщить основные направления криминологических исследований, которым в условиях цифровизации важно уделить повышенное внимание. К ним, на наш взгляд, относятся:

– разработка и уточнение криминологического наполнения понятия киберпреступности, научная оценка реальной картины этого вида преступности с учетом латентной составляющей, построение научно обоснованных прогнозов ее изменения;

– поиск новых методов криминологических исследований как преступлений, совершаемых с использованием цифровых технологий (криптовалют и других виртуальных финансовых активов, искусственного интеллекта, виртуальной и дополненной реальности и др.), так и традиционных видов преступности;

– определение потенциала криминологической науки с точки зрения оценки общественной опасности и распространенности явлений и процессов, происходящих в сетевой среде, для своевременного и обоснованного решения вопросов их криминализации;

– изучение специфики криминальных процессов и угроз, обусловленных информатизацией общества и виртуализацией реальности, их влияния на изменение характера преступности и выбор оптимальных методов деятельности по ее предупреждению;

– определение влияния на организацию и тактику предупреждения преступлений трансформаций современной преступности и использования новых информационных технологий в криминальной деятельности;

– анализ особенностей сетевого поведения пользователей для своевременного обнаружения потенциальных объектов индивидуальной виктимологической профилактики и профилактики индивидуального преступного поведения;

– познание специфики киберпространства, в первую очередь его теневых сегментов и криминогенных объектов, определение возможности их криминологического исследования;

– выявление особенностей сетевых организованных преступных формирований, специфики их взаимодействия, принципов управления ими и координации их деятельности, определение возможности контроля над связанными с ними сетевыми ресурсами и профилактического воздействия на них;

– проработка оптимальных вариантов адаптации традиционных средств и методов предупреждения преступлений к применению в новой информационной среде и в дополненной реальности;

– совершенствование форм взаимодействия специализированных и неспециализированных субъектов предупреждения преступлений в киберпространстве (в том числе зарубежных), оптимизация доступа к информационным ресурсам и организации обмена значимой информацией;

– выявление форм и методов результативного применения аналитических технологий с учетом возможностей искусственного интеллекта, определение среди них наиболее перспективных, адаптация их к решению задач предупреждения преступлений, внедрение методов предиктивной аналитики;

– формирование с использованием технологий искусственного интеллекта модифицированной системы профилактической деятельности.

Полагаем, что приведенный перечень должен подвергаться уточнению и расширению с учетом дальнейшего развития технологий и их влияния на общественные отношения, определяемые цифровизацией.

В практической плоскости важно обеспечить обновление системы подготовки, переподготовки и повышения квалификации кадров с тем, чтобы субъекты предупреждения преступлений приобрели особые компетенции,

необходимые для эффективного решения профилактических задач в изменившихся условиях. Кроме того, криминологический мониторинг и непосредственная реализация профилактических мероприятий, в том числе направленных на предупреждение традиционных преступлений, должны быть переориентированы на функционирование в условиях цифровой среды. При этом важно не нагружать субъектов предупреждения преступлений, в первую очередь сотрудников правоохранительных органов, дополнительными обязанностями, а разумно перераспределять существующие с поправкой на цифровизацию общественных отношений.

И в завершение еще раз подчеркнем важность своевременного адекватного отклика криминологической науки и практики предупреждения преступлений на явное усложнение проблем противодействия преступности в киберпространстве. Полагаем, что он должен быть не только обоснованным, но и достаточно решительным в выборе новых средств и методов, поскольку, как мы уже неоднократно отмечали, потеря тактической и стратегической инициативы в этой сфере привела бы к утрате принципиальных позиций правоохранительной системы, вернуть которые будет гораздо сложнее, чем удержать.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Смолиговец О.С. Субъектные основы виртуализации социальной реальности в информационном обществе / О.С. Смолиговец. — DOI 10.18500/1819-7671-2019-19-2-166-170 // Известия Саратовского университета. Новая серия. Сер.: Философия. Психология. Педагогика. — 2019. — Т. 19, № 2. — С. 166–170.

2. Емелин В.А. Куда нас приведет болезненная степень бессмысленности: симулякры постнормального мира / В.А. Емелин // Независимая газета. — 2019. — 23 сент. — URL: https://www.ng.ru/scenario/2019-09-23/9_12_7683_simulakr.html.

3. Емелин В.А. Симулякры и технологии виртуализации в информационном обществе / В.А. Емелин. — DOI 10.11621/npj.2016.0312 // Национальный психологический журнал. — 2016. — № 3 (23). — С. 86–97.

4. Овчинский В. Европа спасается от мафии: о Стратегии ЕС по борьбе с организованной преступностью на 2021–2025 гг. / В. Овчинский, Ю. Жданов // Завтра. — 2021. — URL: https://zavtra.ru/blogs/evropa_spasaetsya_ot_mafii.

5. Rosenfeld R. Explaining Recent Crime Trends: Introduction to the Special Issue / R. Rosenfeld, D. Weisburd. — DOI 10.1007/s10940-016-9317-6 // Journal of Quantitative Criminology. — 2016. — Vol. 32, iss. 3. — P. 329–334.

6. Peng Wang. Organized crime in cyberspace / Peng Wang, Mei Su, Jingyi Wang. — DOI 10.1093/bjc/azaa064 // The British Journal of Criminology. — 2021. — Vol. 61, iss. 2. — P. 303–324.

7. Lusthaus J. Industry of Anonymity: Inside the Business of Cybercrime / J. Lusthaus. — Cambridge : Harvard Univ. Press, 2018. — 289 p.

8. Papachristos A.V. The Network Structure of Crime / A.V. Papachristos. — DOI 10.1111/soc4.12147 // Sociology Compass. — 2014. — Vol. 8, iss. 4. — P. 347–357.

9. Duxbury S.W. The Network Structure of Opioid Distribution on a DarknetCryptomarket / S.W. Duxbury, D.L. Haynie. — DOI 10.1007/s10940-017-9359-4 // Journal of Quantitative Criminology. — 2018. — Vol. 34, iss. 1. — P. 921–941.

10. Davies G. Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers / G. Davies. — DOI 10.1177/0022018320952557 // The Journal of Criminal Law. — 2020. — Vol. 84, iss. 5. — P. 407–426.

11. Artificial Intelligence and the Law: Cybercrime and Criminal Liability / ed. D.J. Baker, P.H. Robinson. — London : Routledge, 2021. — 280 p.

12. Cybersecurity Risks in Complex IoT Environments: Threats to Smart Homes, Buildings and Other Structures / S. Hilt, N. Huq, M. Rösler, A. Urano // Trend Micro. — 2019. — URL: https://documents.trendmicro.com/assets/white_papers/wp-cybersecurity-risks-in-complex-iot-environments.pdf.

13. Дремлюга Р.И. Борьба с распространением реалистичных аудиовизуальных поддельных материалов за рубежом (deepfake): уголовно-правовые и криминологические аспекты / Р.И. Дремлюга, А.И. Коробеев. — DOI 10.17150/2500-4255.2021.15(3).372-379 // Всероссийский криминологический журнал. — 2021. — Т. 15, № 3. — С. 372–379.

14. Лебедев С.Я. Цифровой безопасности — цифровой уголовно-правовой ресурс / С.Я. Лебедев // Криминология: вчера, сегодня, завтра. — 2019. — № 4 (55). — С. 17–25.

15. Игнатов А.Н. «Криминология завтра» нужна уже сегодня / А.Н. Игнатов // Общество и право. — 2016. — № 4 (58). — С. 94–99.

16. Цифровая криминология: математические методы прогнозирования (часть 1) / А.П. Суходолов, С.В. Иванцов, Т.В. Молчанова [и др.]. — DOI 10.17150/2500-4255.2018.12(2).230-236 // Всероссийский криминологический журнал. — 2018. — Т. 12, № 2. — С. 230–236.

17. Камко А.С. Предупреждение мошенничества с использованием телекоммуникационных и компьютерных сетей : дис. … канд. юрид наук : 12.00.08 / А.С. Камко. — Владивосток, 2020. — 228 с.

18. Smith G. The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approach / G. Smith, L. Moses, J. Chan. — DOI 10.1093/bjc/azw096 // The British Journal of Criminology. — 2017. — Vol. 57, iss. 2. — P. 259–274.

19. Серебренникова А.В. Криминологические проблемы цифрового мира (цифровая криминология) / А.В. Серебренникова. — DOI 10.17150/2500-4255.2020.14(3).423-430 // Всероссийский криминологический журнал. — 2020. — Т. 14, № 3. — С. 423–430.

20. Степаненко Д.А. Использование систем искусственного интеллекта в правоохранительной деятельности / Д.А. Степаненко, Д.В. Бахтеев, Ю.А. Евстратова. — DOI 10.17150/2500-4255.2020.14(2).206-214 // Всероссийский криминологический журнал. — 2020. — Т. 14, № 2. — С. 212–213.

REFERENCES

1. Smoligovets O.S. Subject Bases of Virtualization of Social Reality in the Information Society. *Izvestiya Saratovskogo universiteta. Novaya seriya. Seriya: Filosofiya. Psikhologiya. Pedagogika = Izvestiya of Saratov University. New Series. Series: Philosophy. Psychology. Pedagogy*, 2019, vol. 19, no. 2, pp. 166–170. (In Russian). DOI: 10.18500/1819-7671-2019-19-2-166-170.
2. Emelin V.A. Where the unhealthy stage of meaninglessness will lead us: simulacra of the post-normal world. *Nezavisimaya Gazeta*, 2019, September 23. Available at: https://www.ng.ru/scenario/2019-09-23/9_12_7683_simulakr.html. (In Russian).
3. Emelin V.A. Simulacra and Virtualization Technologies in Information Society. *Natsional'nyi psikhologicheskii zhurnal = National Psychological Journal*, 2016, no. 3, pp. 86–97. (In Russian). DOI: 10.11621/npj.2016.0312.
4. Ovchinskii V., Zhdanov Yu. Europe is saving itself from mafia: the EU Strategy to Tackle Organized Crime in 2021–2025. *Zavtra*, 2021. Available at: https://zavtra.ru/blogs/evropa_spasaetsya_ot_mafii. (In Russian).
5. Rosenfeld R., Weisburd D. Explaining Recent Crime Trends: Introduction to the Special Issue. *Journal of Quantitative Criminology*, 2016, vol. 32, iss. 3, pp. 329–334. DOI: 10.1007/s10940-016-9317-6.
6. Peng Wang, Mei Su, Jingyi Wang. Organized crime in cyberspace. *The British Journal of Criminology*, 2021, vol. 61, iss. 2, pp. 303–324. DOI: 10.1093/bjc/azaa064.
7. Lusthaus J. *Industry of Anonymity: Inside the Business of Cybercrime*. Cambridge, Harvard University Press, 2018. 289 p.
8. Papachristos A.V. The Network Structure of Crime. *Sociology Compass*, 2014, vol. 8, iss. 4, pp. 347–357. DOI: 10.1111/soc4.12147.
9. Duxbury S.W., Haynie D.L. The Network Structure of Opioid Distribution on a Darknet Cryptomarket. *Journal of Quantitative Criminology*, 2018, vol. 34, iss. 1, pp. 921–941. DOI: 10.1007/s10940-017-9359-4.
10. Davies G. Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers. *The Journal of Criminal Law*, 2020, vol. 84, iss. 5, pp. 407–426. DOI: 10.1177/0022018320952557.
11. Baker D.J., Robinson P.H. (eds.). *Artificial Intelligence and the Law: Cybercrime and Criminal Liability*. London, Routledge, 2021. 280 p.
12. Hilt S., Huq N., Rösler M., Urano A. Cybersecurity Risks in Complex IoT Environments: Threats to Smart Homes, Buildings and Other Structures. *Trend Micro*, 2019. Available at: https://documents.trendmicro.com/assets/white_papers/wp-cybersecurity-risks-in-complex-iot-environments.pdf.
13. Dremliuga R.I., Korobeev A.I. A Fight against the Dissemination of Deepfakes in other Countries: Criminal and Criminological Aspects. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2021, vol. 15, no. 3, pp. 372–379. (In Russian). DOI: 10.17150/2500-4255.2021.15(3).372-379.
14. Lebedev S.Ya. Digital Criminal Law Resource for Digital Security. *Kriminologiya: vchera, segodnya, zavtra = Criminology: Yesterday, Today, Tomorrow*, 2019, no. 4, pp. 17–25. (In Russian).
15. Ignatov A.N. «Criminology Tomorrow» is necessary Today. *Obshchestvo i pravo = Society and Law*, 2016, no. 4, pp. 94–99. (In Russian).
16. Sukhodolov A.P., Ivantsov S.V., Molchanova T.V., Spasennikov B.A., Kaluzhina M.A. Digital Criminology: Mathematical Methods of Prediction (Part 1). *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2018, vol. 12, no. 2, pp. 230–236. (In Russian). DOI: 10.17150/2500-4255.2018.12(2).230-236.
17. Kamko A.S. *Prevention of fraud using telecommunication and computer networks. Cand. Diss*. Vladivostok, 2020. 228 p.
18. Smith G., Moses L., Chan J. The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approach. *The British Journal of Criminology*, 2017, vol. 57, iss. 2, pp. 259–274. DOI: 10.1093/bjc/azw096.
19. Serebrennikova A.V. Criminological Problems of the Digital World (Digital Criminology). *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 3, pp. 423–430. (In Russian). DOI: 10.17150/2500-4255.2020.14(3).423-430.
20. Stepanenko D.A., Bakhteev D.V., Evstratova Yu.A. The Use of Artificial Intelligence Systems in Law Enforcement. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 2, pp. 206–214. (In Russian). DOI: 10.17150/2500-4255.2020.14(2).206-214.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Осипенко Анатолий Леонидович — заместитель начальника Краснодарского университета МВД России, доктор юридических наук, профессор, г. Краснодар, Российская Федерация; e-mail: osipenko_al@mail.ru.

Соловьев Владислав Сергеевич — доцент кафедры уголовного права и криминологии Краснодарского университета МВД России, кандидат юридических наук, г. Краснодар, Российская Федерация; e-mail: vladsolovyev@mail.ru.

ДЛЯ ЦИТИРОВАНИЯ

Осипенко А.Л. Основные направления развития криминологической науки и практики предупреждения преступлений в условиях цифровизации общества / А.Л. Осипенко, В.С. Соловьев. — DOI 10.17150/2500-4255.2021.15(6).681-691 // Всероссийский криминологический журнал. — 2021. — Т. 15, № 6. — С. 681–691.

INFORMATION ABOUT THE AUTHORS

Osipenko, Anatoliy L. — Deputy Head for Research, Krasnodar University of the Ministry of Internal Affairs of Russia, Doctor of Law, Professor, Krasnodar, the Russian Federation; e-mail: osipenko_al@mail.ru.

Solovev, Vladislav S. — Ass. Professor, Chair of Criminal Law and Criminology, Krasnodar University of the Ministry of Internal Affairs of Russia, Ph.D. in Law, Krasnodar, the Russian Federation; e-mail: petrov@mail.ru.

FOR CITATION

Osipenko A.L., Solovev V.S. Main trends in the development of criminological theory and crime prevention practice in the context of the digitalization of society. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2021, vol. 15, no. 6, pp. 681–691. (In Russian). DOI: 10.17150/2500-4255.2021.15(6).681-691.