

О киберполиции в Российской Федерации

Ю.А. Гудков¹, М.А. Нагорная²

^{1,2} Омский государственный университет путей сообщения, г. Омск, Российская Федерация

¹ uelrjd1957@mail.ru

² nagornaya71@mail.ru

Аннотация. В статье рассматриваются вопросы, связанные с необходимостью создания киберполиции в России. Анализ криминальной обстановки в России свидетельствует о возникновении на фоне пандемии COVID-19 проблемы негативных воздействий цифровизации и информационных технологий на качественные и количественные изменения структуры и динамики преступности. В настоящее время необходимо создание единой государственной службы по координации противодействия киберпреступности в стране, киберполиции, которая должна быть предназначена для защиты и охраны прав, свобод и законных интересов граждан Российской Федерации, юридических лиц, общества и государства, а также для противодействия киберпреступности и обеспечения информационной безопасности в киберпространстве. Сделан вывод о том, что киберпреступность является частью общей преступности, ее подсистемой, которая имеет свои специфические качественные характеристики, в том числе и свою структуру, и свою динамику.

Ключевые слова: киберполиция, киберполицейские, преступность, киберпреступление, киберпреступность

Для цитирования: Гудков Ю.А., Нагорная М.А. О киберполиции в Российской Федерации // Юридический вестник ДГУ. 2021. Т. 40, № 4. С. 108–114. DOI: 10.21779/2224-0241-2021-40-4-108-114

Original article

About Cyber police in the Russian Federation

Iurii A. Gudkov¹, Marina A. Nagornaya²

^{1,2} Omsk State Transport University, Omsk, Russian Federation,

¹ uelrjd1957@mail.ru

² nagornaya71@mail.ru

Abstract. The article discusses the issues related to the need to create a cyber police in Russia. The analysis of the criminal situation in Russia indicates the emergence of the problem of negative impacts of digitalization and information technologies on qualitative and quantitative changes in the structure and dynamics of crime against the background of the COVID-19 pandemic. Currently, it is necessary to create a unified state service for coordinating the fight against cybercrime in the country, cyber police, which should be designed to protect and protect the rights, freedoms and legitimate interests of citizens of the Russian Federation, legal entities, society and the state, as well as to counter cybercrime and ensure information security in cyberspace. It is concluded that cybercrime is a part of the general crime, its subsystem, which has its own specific qualitative characteristics, including its structure and its dynamics.

Keywords: cyber police, cyber police, crime, cybercrime, cybercrime

For citation: Gudkov I. A., Nagornaya M. A. About cyber police in the Russian Federation. *Yuridicheskii vestnik DGU = Law Herald of DSU*, 2021, vol. 40, no. 4, pp. 108–114. DOI: 10.21779/2224-0241-2021-40-4-108-114 (In Russ.).

Развитие цифровых технологий как манифестирующего проявления информационного общества и процессов глобализации становится неотъемлемой частью современного мира, проникая во все сферы общественной жизни, превращается в часть привычной повседневности.

Вступление в новую эпоху оказывает определяющее воздействие на структуру внешне- и внутривластной стратегии государств, ин-

тегрируя наращивание цифровых технологий в приоритетные государственные цели. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы определяет применение информационных, коммуникационных технологий, формирование информационного пространства и соответствующей ей инфраструктуры в качестве стратегических национальных приоритетов [1].

Указанные процессы приводят к перемещению части общественных отношений в интернет-пространство. Взаимодействие человека с социальными институтами подвергается процессу цифровизации, о чем свидетельствует система предоставления государственных услуг в электронной форме; дистанционное банковское обслуживание, образование, медицина, сфера культуры, транспорт и торговля активно внедряют информационно-коммуникационные технологии в область своей деятельности.

Воздействию информационных технологий подвергается частная жизнь. Социальные сети, мессенджеры, облачные хранилища аккумулируют информацию о личной жизни, в информационном пространстве посредством электронной почты, платежных систем оказываются копии документов, реквизиты банковских карт, другая конфиденциальная информация, поисковые системы формируют социальный портрет пользователя.

Широкое распространение информационно-коммуникационных технологий оказало воздействие и на состояние преступности, что нашло отражение в структуре и динамике совершаемых преступлений.

Согласно данным Министерства внутренних дел Российской Федерации (далее – МВД России) статистика преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, выглядит следующим образом: в 2017 году было зарегистрировано 90587 преступлений, в 2018 году – 174674, в 2019 году – 294409, в 2020 году – 510396, в январе-июле 2021 года – 315671 преступление, что на 15,7% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес составил 8,8% в 2018 году, 14,5% в 2019 году, 25% в 2020 году, в январе-июле 2021 года удельный вес вырос с 20,95 в январе-июле 2020 года до 26,6% [2]. Статистические данные иллюстрируют опасную, неуклонно возрастающую тенденцию роста преступлений, совершенных с использованием информационно-телекоммуникационных технологий, с одновременным повышением их удельного веса в общей массе зарегистрированных преступлений. При этом эксперты отмечают, что доля латентных преступлений в десятки раз выше официальной статистики.

Фактором, активизировавшим «переструктуризацию» преступности, её активный переход в цифровое пространство, стало распространение пандемии COVID-19. Согласно данным МВД России в 2020 году более половины преступлений (52,4%), совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, относится к категориям тяжких и особо тяжких, большая часть которых совершается с использованием сети Интернет, средств мобильной связи, расчетных

(пластиковых) карт [3]. Исследователи констатируют, что в России киберпреступность достаточно оперативно встроилась в ситуацию пандемии, что привело к формированию специфических видов преступлений, таких как: фальшивые уведомления о штрафах за нарушение самоизоляции со ссылкой на несуществующее постановление ФСИН, продажа фальшивых лекарств от коронавируса, тестов на наличие инфекции, прививочных сертификатов; фейковые интернет-магазины, фишинговые сайты, новые мошеннические схемы хищения денег с банковских счетов с применением приемов социальной инженерии и т.д. [4, с. 76].

Наряду с проблемой роста количества преступлений, совершаемых с использованием информационных технологий, не менее важной является проблема предупреждения такой преступности.

Анонимность в виртуальной реальности, сложность с идентификацией и привлечением к ответственности преступника приводят к совершению цепи правонарушений. Помимо уже имеющих, отработанных приемов, преступники, шагая в ногу с научно-техническим прогрессом, постоянно изобретают все более новые способы совершения преступлений.

В результате обычные пользователи из-за чрезмерного психологического доверия, недостаточной осведомленности и понимания реальности угроз, которые подстерегают их сегодня в мобильном техническом устройстве, все чаще становятся жертвами киберпреступников.

Виртуальное пространство, обеспечивая анонимность пользователей, создает благоприятные возможности для увеличения количества субъектов преступлений в информационной среде и роста количества жертв этих преступлений.

В то же время следует отметить, что уровень раскрываемости преступлений, совершенных с использованием информационно-телекоммуникационных технологий, остается на низком уровне: в 2017 году она составила 24,4%, в 2018 году – 26,6%, в 2019 году – 24%, в 2020 году – 20%, в январе-июле 2021 года – 27%, т.е. в среднем, раскрывается только каждое пятое преступление [5].

Учитывая общественную опасность этой группы преступлений, ущерб, наносимый обществу и государству, тенденцию и прогнозирование дальнейшего роста удельного веса в общей массе преступности, высокую степень адаптивности к изменяющимся условиям, следует констатировать необходимость формирования правовых, организационных, аналитических и иных инструментов для эффективной борьбы с указанными преступными деяниями.

Отметим необходимость терминологического уточнения понятия «киберпреступность», используемого для обозначения преступлений, совершаемых в информационной среде. К проблеме определения сущности киберпреступности и конкретизации её признаков и видов в своих работах

обращаются В.А. Номоконов, Т.Л. Тропина. Сравнивая «компьютерную преступность» и «киберпреступность», часто используемые как синонимичные, авторы, опираясь на англоязычное толкование понятий «cybercrime (киберпреступность) как преступности, связанной с использованием компьютеров, информационных технологий и глобальных сетей», и «computer crime (компьютерная преступность), которая относится только к преступлениям, совершаемым против компьютеров или компьютерных данных», делают вывод о том, что компьютерное преступление является разновидностью киберпреступления [6, с. 47]. Исследователи дают широкое толкование киберпреступности, определяя её как «совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных» [6, с. 48]. Такой подход позволяет существенно расширить границы признаков киберпреступлений, упростив, тем самым, процедуру их квалификации.

Д.Н. Карпова, указывая на интегральные характеристики киберпреступления, определяет его как «акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству посредством любого технического средства с доступом в Интернет» [7, с. 47].

Автор рассматривает киберпреступность как сложное социальное явление глобального характера с транснациональной природой, причиняющее экономические потери, подрывающее деятельность политических институтов, распространяющее опасные идеологические идеи, наносящее моральный и психологический вред обществу.

Многомерность, опасность и широта распространения киберпреступности как социального явления спровоцировала институализацию системы кибербезопасности, в качестве организационного компонента которой выступает особая группа правоохранительных органов.

Формирование особых подразделений в системе МВД России, главная задача которых заключается в борьбе с преступлениями в сфере компьютерной информации, т.е. в сущности киберполиции, началось еще в 90-е годы XX века, что было обусловлено развитием информационно-телекоммуникационных систем и появлением связанных с этим явлением новых видов преступлений.

В 1992 году в составе МВД России было образовано Управление информационного и оперативно-технического обеспечения, главной задачей которого стало сопровождение деятельности криминальной милиции по предупреждению и раскрытию преступлений. В дальнейшем подразделение

претерпело ряд реорганизаций, и в 2005 году было преобразовано в Бюро специальных технических мероприятий, одним из направлений деятельности которого является борьба с преступлениями в сфере компьютерной информации, незаконным распространением радиоэлектронных и специальных технических средств, мошенничествами в области электронных платежей.

В 2001 году было создано специализированное оперативное подразделение Управление «К» МВД России, занимающееся раскрытием преступлений, совершаемых в сфере информационных технологий.

В пределах своей компетенции сотрудники подразделения выявляют и пресекают:

- преступления в сфере компьютерной информации: неправомерный доступ к охраняемой законом компьютерной информации, создание, использование и распространение вредоносных компьютерных программ, нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей, мошенничество в сфере компьютерной информации;

- преступления, совершаемые с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) и направленные против здоровья несовершеннолетних и общественной нравственности: изготовление и распространение материалов или предметов с порнографическими изображениями несовершеннолетних, использование несовершеннолетнего в целях изготовления порнографических материалов или предметов;

- преступления, связанные с незаконным оборотом специальных технических средств, предназначенных для негласного получения информации;

- преступления, связанные с незаконным использованием объектов авторского права или смежных прав [8].

МВД России 1 ноября 2020 года приняло решение о внесении изменений в свою структуру, заявив о создании подразделений, которые будут специализироваться на противодействии преступлениям, совершаемым с использованием IT-технологии. Следует отметить, что данным решением был констатирован очередной этап в формировании киберполиции России.

Наряду с МВД России борьбой с киберпреступлениями в рамках своей компетенции занимаются другие федеральные специализированные государственные службы: Федеральная служба безопасности Российской Федерации в вопросах, затрагивающих национальную безопасность [9]; Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, осуществляющая контроль в области средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, за соответствием обра-

ботки персональных данных требованиям федерального законодательства [10]; Федеральная служба по техническому и экспортному контролю выполняющая, в том числе, специальные и контрольные функции в области государственной безопасности по вопросам обеспечения безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, осуществления экспортного контроля [11].

Эксперты полагают, что организационно-правовой механизм взаимодействия и координации деятельности указанных государственных органов не в полной мере отвечает потребностям практики борьбы с киберпреступностью. «В настоящее время преступность является многогранным явлением, которое по мере развития общества приобретает все новые и новые формы своего проявления. Справиться с этой социальной проблемой усилиями одного или нескольких органов, пусть и наделенных самыми широкими полномочиями, не представляется возможным» [12, с. 74]. Полагаем, что наиболее эффективной мерой в борьбе преступлениями в киберпространстве должно стать формирование единой специализированной службы.

Следует отметить, что история МВД содержит примеры реагирования на развитие технического прогресса и складывающуюся криминальную обстановку. Массовое распространение в стране автотранспорта вызвало необходимость создания в 1936 году специальной службы – ГАИ (Государственная автомобильная инспекция) для борьбы с нарушениями правил дорожного движения и обеспечения общественного порядка на дорогах. Рост экономической преступности в СССР привел к необходимости создания в 1937 году для борьбы с этим видом преступности специальной службы – ОБХСС (отдел по борьбе с хищениями социалистической собственности). Появление организованной преступности в России в 1990-е годы сопровождалось формированием в системе МВД специальных подразделений по борьбе с организованной преступностью – РУБОП (Региональные управления по борьбе с организованной преступностью).

Таким образом, представляется возможным утверждать, что создаваемая в Российской Федерации киберполиция, главной целью которой становится борьба с преступлениями, совершаемыми в цифровом пространстве, должна стать отдельной, специальной федеральной службой, в компетенцию которой входят задачи выявления, предупреждения, пресечения и раскрытия киберпреступлений.

Возрастающая роль информационно-коммуникационных технологий выступает провоцирующим фактором обновления и совершенствования киберпреступности: усиливается организованность и латентизация, усложняются схемы совершения преступлений, изменяются характери-

стики субъектов преступлений, наиболее распространенными становятся преступления в сфере интернет-торговли, обслуживания кредитных карт, вымогательства с использованием мобильных средств связи, действия мошенников распространяются за пределы государства, преступность приобретает транснациональный характер.

На фоне трансформации киберпреступности, с учетом ее общественной опасности и роста реальных масштабов исследователи актуализируют проблему, связанную с действующим законодательством.

Председатель Конституционного Суда Российской Федерации В.Д. Зорькин подчеркивает, что «в условиях новой цифровой реальности прежнее нормативно-правовое регулирование различных сфер социальной жизни нуждается в существенной модернизации» [13].

По мнению представителей юридического сообщества, безнаказанность за совершение киберпреступлений связана с тем, что «в настоящее время уголовное законодательство слабо адаптировано к новым видам преступлений в сфере информационных технологий, оно не содержит достаточную нормативную правовую базу для охраны соответствующих общественных отношений, отсутствуют единые разъяснения высшей судебной инстанции по вопросам уголовно-правовой оценки таких преступлений, сохраняя условия для дальнейшей криминализации виртуального пространства» [14, с. 65]. Эксперты считают, что уголовное законодательство Российской Федерации «не в полной мере содержит достаточной нормативной правовой базы для реализации ответственности за преступления исследуемой группы в соответствии с их реальной общественной опасностью, некоторые деяния, обладающие признаком общественной опасности, не криминализованы в рамках УК РФ, отсутствует нормативное закрепление понятий «преступление, совершаемое с использованием компьютерных технологий», «компьютерные технологии», «использование компьютерных технологий» [15, с. 9].

Одной из отправных точек в решении данной проблемы, как полагают исследователи, должно стать научное осмысление проблем противодействия преступности в цифровом пространстве, разработка научно-обоснованных предложений, «научный старт к созданию новых доктрин, научных теорий и развитию новых направлений в научной деятельности значительного количества отраслей не только знаний, но и технологий» [16, с. 13]. С точки зрения С.Я. Лебедева, «цифровые технологии меняют традиционные формы правового обеспечения, усиливая и ускоряя тенденцию его инновационно-технологического переустройства, инновационная модернизация права и соответствующая ей модернизация правоприменения становятся сегодня самостоятельным и значимым ресурсом нового технологического уклада» [17, с. 19].

А.С. Анисимова, анализируя проблемы правового регулирования в сети Интернет, отмечает, что «на сегодняшний день в нашей стране принимается достаточно большое количество новых норм в отношении упорядочения отношений в Интернете, вносятся изменения в уже действующее законодательство, но первостепенную роль играет правовая политика, направленная на достижение высокого уровня и качества правового регулирования: совершенствование всего комплекса юридических средств, достижение поставленных обществом и государством задач юридическими ресурсами» [18, с. 151].

Мнения специалистов о необходимости формирования новых доктрин, преобразований в законодательстве и правоприменительных практиках в отношении преступлений, совершенных в цифровом пространстве, свидетельствуют о появлении качественно новых характеристик преступности, требующих адаптационных изменений всей правовой системы.

Киберпреступность, являясь частью преступности в целом, демонстрирует особые качественные характеристики: отсутствие места преступления в традиционном его понимании, преступление совершается в виртуальном пространстве, где возникают различные виды общественных отношений, а его правовая природа остается не вполне определенной, целью преступных действий становятся объекты виртуальной собственности, статус которой находится в процессе формирования, организационные и процессуальные сложности определяются высокой латентностью таких преступных деяний, трудностями в их выявлении, определении причастности, процедуре сбора доказательств, задержании подозреваемых и обвиняемых.

Таким образом, постиндустриальное общество принесло новую реальность в сферу преступной деятельности, критическое приращение количественной массы преступлений, совершаемых в циф-

ровом пространстве, привело к изменению качественных характеристик преступности.

Данные положения свидетельствуют о необходимости совершенствования уже имеющихся и разработке новых правовых механизмов противодействия преступности в цифровом пространстве.

Следует отметить, что для эффективной борьбы с киберпреступлениями необходимы особые условия: наличие квалифицированных кадров, обладающих специальными навыками и компетентностью в IT-сфере, высокий уровень технической оснащенности, разработанные методики расследования таких преступлений, связанные с применением новейших цифровых технологий, межведомственное и международное взаимодействие и координация.

Многомерность, опасность, латентный характер, высокий уровень цифровизации киберпреступности актуализируют институализацию системы кибербезопасности. Эффективность института кибербезопасности определяется условиями его формирования, к которым можно отнести разработку новых научных подходов к анализу цифровой преступности, аккумуляцию и трансформацию опыта борьбы с киберпреступлениями в эффективный методический инструментарий, совершенствование действующего законодательства, создание механизма международного взаимодействия в области борьбы с преступными деяниями в цифровом пространстве. Ключевым организационным элементом института кибербезопасности и эффективным инструментом борьбы с преступлениями, совершаемыми в цифровом пространстве, должна стать киберполиция, как отдельная, специальная федеральная служба, обладающая широкими компетенциями и полномочиями в сфере выявления, предупреждения, пресечения и раскрытия киберпреступлений.

Список источников

1. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ президента РФ от 9 мая 2017 г. №203 [Электронный ресурс]. Президент Российской Федерации: [офиц. сайт]. URL: <http://static.kremlin.ru/media/acts/files/0001201705100002.pdf> (дата обращения: 20.07.2021)
2. Состояние преступности в Российской Федерации [Электронный ресурс]. Министерство Внутренних дел Российской Федерации: [офиц. сайт]. URL: <https://мвд.рф/reports/item/> (дата обращения: 22.07.2021).
3. Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2020 года [Электронный ресурс]. Министерство внутренних дел Российской Федерации: [офиц. сайт]. URL: <https://xn--b1aew.xn--p1ai/reports/item/22678184> (дата обращения: 25.07.2021).
4. Симонова С.С. Криминологическая характеристика и особенности предупреждения преступлений, совершаемых с применением информационных технологий в период Covid-19 // Проблемы борьбы с преступностью в условиях цифровизации: теория и практика: сб. ст. XVIII Международной науч.-практ. конф. «Уголовно-процессуальные и криминологические чтения на Алтае». Вып. XVI; отв. ред. С.И. Давыдов, В.В. Поляков. Барнаул: Изд-во Алтайского университета, 2020. С. 74–78.
5. Состояние преступности в Российской Федерации [Электронный ресурс]. Министерство Внутренних дел Российской Федерации: [офиц. сайт]. URL: <https://мвд.рф/reports/item/> (дата обращения: 22.07.2021).
6. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера сегодня завтра. 2012. № 1 (24). С.45–55.
7. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 46–50.

8. Управление «К» МВД России [Электронный ресурс]. Министерство Внутренних Дел Российской Федерации: офиц. сайт. URL: https://мвд.пф/мвд/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (дата обращения: 05.08.2021)
9. О федеральной службе безопасности: федер. закон Рос. Федерации от 3 апр.1995 г. № 40-ФЗ: в ред. от 1 июля 2021 г. [Электронный ресурс]. Президент Российской Федерации: [офиц. сайт]. URL: <http://kremlin.ru/acts/bank/7696> (дата обращения: 07.08.2021).
10. Положение о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций: постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 [Электронный ресурс]. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: [офиц. сайт]. URL: <https://rkn.gov.ru/about/> (дата обращения: 07.08.2021)
11. Сведения о полномочиях ФСТЭК России [Электронный ресурс]. Федеральная служба по техническому и экспортному контролю: [офиц. сайт]. URL: <https://fstec.ru/obshchaya-informatsiya/polnomochiya> (дата обращения: 07.08.2021).
12. Воронцов А.Л., Снегирева Н.И., Снегирева Д.Е. Некоторые проблемы организации координационной деятельности государственных органов в сфере борьбы с преступностью // Юридический вестник ДГУ. 2020. №4. Т.36. С. 74–79.
13. Зорькин В.Д. Право в цифровом мире. Размышление на полях Петербургского международного юридического форума [Электронный ресурс] // Рос. газ. 2018. № 7578 (115). URL: <https://rg.ru/2018/05/29/zorkin-zadacha-gosudarstva-priznavat-i-zashchishchat-cifrovye-prava-grazhdan.html> (дата обращения: 15.09.2021).
14. Комплексный анализ состояния преступности в Российской Федерации и расчетные варианты ее развития: аналитический обзор / Ю.М. Антонян, Д.А. Бражников, М.В. Гончарова и др. М.: ФГКУ «ВНИИ МВД России», 2018. 86 с.
15. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. Ч. 1. / А. В. Аносов и др. М.: Академия управления МВД России, 2019. 208 с.
16. Ищук Я.Г., Пинкевич Т.В., Смольянинов Е.С. Цифровая криминология: учеб. пос. М.: Академия управления МВД России, 2021. 244 с.
17. Лебедев С.Я. Цифровая безопасность – цифровой уголовно-правовой ресурс // Криминология: вчера, сегодня, завтра. 2019. № 4 (55). С. 17–25.
18. Анисимова А.С. Правовое регулирование интернета: основные пробелы и направления деятельности государства // Юридический вестник ДГУ. Т. 33. 2020. №1. С. 149–153.

References

1. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы. Ukaz prezidenta RF от 09.05.2017 №203. [On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030: Decree of the President of the Russian Federation No. 203 of May 9, 2017]. Prezident Rossiiskoi Federatsii: ofits. sait [The President of the Russian Federation: ofic. website]. (In Russ.). Available at: <http://static.kremlin.ru/media/acts/files/0001201705100002.pdf> (accessed 20.07.2021).
2. Sostoyanie prestupnosti v Rossiiskoi Federatsii [The state of crime in the Russian Federation], Ministerstvo Vnutrennikh Del Rossiiskoi Federatsii: ofits. sait [Ministry of Internal Affairs of the Russian Federation: ofic. website]. (In Russ.). Available at: <https://мвд.рф/reports/item/> (accessed 22.07.2021).
3. Kratkaya kharakteristika sostoyaniya prestupnosti v Rossiiskoi Federatsii za yanvar' - dekabr' 2020 goda [Brief description of the state of crime in the Russian Federation for January-December 2020]. Ministerstvo vnutrennikh del Rossiiskoi Federatsii: ofits. sait [Ministry of Internal Affairs of the Russian Federation: ofic. website]. (In Russ.). Available at: <https://xn--b1aew.xn--p1ai/reports/item/22678184> (accessed 25.07.2021).
4. Simonova S.S. Kriminologicheskaya kharakteristika i osobennosti preduprezhdeniya prestuplenii, sovershaemykh s primeneniem informatsionnykh tekhnologii v period Covid-19 [Criminological characteristics and features of the prevention of crimes committed with the use of information technologies during Covid-19], *Problemy bor'by s prestupnost'yu v usloviyakh tsifrovizatsii: teoriya i praktika* [Problems of combating crime in the conditions of digitalization: theory and practice], collection of art. XVIII International Scientific and Practical Conference "Criminal procedural and criminalistic readings in Altai". Issue XVI; ed. S.I. Davydov, V.V. Polyakov. Barnaul: Publishing House of Altai University, 2020, pp. 74–78. (In Russ.).
5. Sostoyanie prestupnosti v Rossiiskoi Federatsii [The state of crime in the Russian Federation]. Ministerstvo Vnutrennikh Del Rossiiskoi Federatsii: ofits. sait [Ministry of Internal Affairs of the Russian Federation: ofic. website]. (In Russ.). Available at: <https://мвд.рф/reports/item/> (accessed 22.07.2021).
6. Nomokonov V.A., Tropina T.L. Kiberprestupnost' kak novaya kriminal'naya ugroza [Cybercrime as a new criminal threat], *Kriminologiya: vchera segodnya zavtra* [Criminology: yesterday today tomorrow], 2012, no. 1 (24), pp. 45–55. (In Russ.).
7. Karpova D.N. Kiberprestupnost': global'naya problema i ee reshenie [Cybercrime: a global problem and its solution], *Vlast' [Power]*, 2014, no. 8, pp. 46–50. (In Russ.).

8. Upravlenie «K» MVD Rossii [Department "K" of the Ministry of Internal Affairs of Russia]. Ministerstvo Vnutrennikh Del Rossiiskoi Federatsii: ofits. sait [Ministry of Internal Affairs of the Russian Federation: ofic. website]. (In Russ.). Available at: https://mvd.rf/mvd/structure1/Upravleniya/Upravlenie_K_MVD_Rossii (accessed 05.08.2021).

9. O federal'noi sluzhbe bezopasnosti: Federal'nyi zakon ot 3 apr.1995 N 40-FZ: red. ot 1 iyulya 2021 [About the Federal Security Service: RF Federal Law of April 3, 1995 No. 40-FZ: as amended. from July 1, 2021]. Prezident Rossiiskoi Federatsii: ofits. Sait [The President of the Russian Federation: ofic. website]. (In Russ.). Available at: <http://kremlin.ru/acts/bank/7696> (accessed 07.08.2021).

10. Polozhenie o Federal'noi sluzhbe po nadzoru v sfere svyazi, informatsionnykh tekhnologii i massovykh kommunikatsii: postanovlenie Pravitel'stva Ros. Federatsii ot 16marta 2009 N 228 [Regulations on the Federal Service for Supervision of Communications, Information Technologies and Mass Communications: Decree of the Government of the Russian Federation No. 228 of March 16, 2009]. Federal'naya sluzhba po nadzoru v sfere svyazi, informatsionnykh tekhnologii i massovykh kommunikatsii: ofits. sait [Federal Service for Supervision of Communications, Information Technology and Mass Communications: ofic. website]. (In Russ.). Available at: <https://rkn.gov.ru/about/> (accessed 07.08.2021)

11. Svedeniya o polnomochiyakh FSTEK Rossii [Information about the powers of the FSTEC of Russia]. Federal'naya sluzhba po tekhnicheskemu i eksportnomu kontrolyu: ofits. sait [Federal Service for Technical and Export Control: ofic. website]. (In Russ.). Available at: <https://fstec.ru/obshchaya-informatsiya/polnomochiya> (accessed 07.08.2021).

12. Vorontsov A.L., Snegireva N.I., Snegireva D.E. Nekotorye problemy organizatsii koordinatsionnoi deyatel'nosti gosudarstvennykh organov v sfere bor'by s prestupnost'yu [Some problems of organization of coordination activities of state bodies in the field of combating crime], *Yuridicheskii vestnik DGU [Law Herald of DSU]*, 2020, no.4, vol. 36, pp. 74–79. (In Russ.).

13. Zor'kin V.D. Pravo v tsifrovom mire. Razmyshlenie na polyakh Peterburgskogo mezhdunarodnogo yuridicheskogo foruma [Law in the digital world. Reflection on the margins of the St. Petersburg International Legal Forum], *Rossiiskaya gazeta [Russian Gazette]*. 2018, no. 7578 (115). 29.05.2018. (In Russ.). Available at: <https://rg.ru/2018/05/29/zorkin-zadacha-gosudarstva-priznavat-i-zashchishchat-cifrovye-prava-grazhdan.html> (accessed 15.09.2021).

14. Kompleksnyi analiz sostoyaniya prestupnosti v Rossiiskoi Federatsii i raschetnye varianty ee razvitiya: analiticheskii obzor [Comprehensive analysis of the state of crime in the Russian Federation and estimated options for its development: analytical review], Yu.M. Antonyan, D.A. Brazhnikov et al., Moscow, FGKU «VNII MVD Rossii» Publ., 2018. 86 p. (In Russ.).

15. Deyatel'nost' organov vnutrennikh del po bor'be s prestupleniyami, sovershennymi s ispol'zovaniem informatsionnykh, kommunikatsionnykh i vysokikh tekhnologii: uchebnoe posobie [Activities of the internal affairs bodies to combat crimes committed with the use of information, communication and high technologies: textbook], at 2 h., h. 1, A.V. Anosov et al., Moscow, Akademiya upravleniya MVD Rossii Publ., 2019, 208 p. (In Russ.).

16. Ishchuk Ya.G., Pinkevich T.V., Smol'yaninov E.S. Tsifrovaya kriminologiya: uchebnoe posobie [Digital criminology: textbook], Moscow, Akademiya upravleniya MVD Rossii Publ., 2021, 244 p. (In Russ.).

17. Lebedev S. Ya. Tsifrovaya bezopasnost' – tsifrovoi ugovovno-pravovoi resurs [Digital security – digital criminal legal resource], *Kriminologiya: vchera, segodnya, zavtra [Criminology: yesterday, today, tomorrow]*, 2019, no. 4 (55), pp. 17–25. (In Russ.).

18. Anisimova A.S. Pravovoe regulirovanie interneta: osnovnye probely i napravleniya deyatel'nosti gosudarstva [Legal regulation of the internet: major spaces and directions of activity of the state], *Yuridicheskii vestnik DGU [Law Herald of DSU]*, 2020, no. 1, vol. 33, pp. 149–153. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Гудков Юрий Александрович, кандидат юридических наук, доцент кафедры «Таможенное дело и право», Омский государственный университет путей сообщения (ОмГУПС), г. Омск, Российская Федерация. E-mail: uelrjd1957@mail.ru

Нагорная Марина Алексеевна, кандидат исторических наук, доцент кафедры «Таможенное дело и право», Омский государственный университет путей сообщения (ОмГУПС), г. Омск, Российская Федерация. E-mail: nagornaya71@mail.ru

Поступила в редакцию 12.10.2021 г. одобрена после рецензирования 11.11.2021 г.; принята к публикации 22.11.2021 г.

INFORMATION ABOUT THE AUTHORS

Gudkov Iurii Aleksandrovich, Ph.D of Legal Sciences, Associate professor at the Department of «Customs matter and Law», Omsk State Transport University (OSTU), Omsk, Russian Federation. E-mail: uelrjd1957@mail.ru

Nagornaya Marina Alekseevna, PhD of Historical Sciences, Associate professor at the Department of «Customs matter and Law», Omsk State Transport University (OSTU), Omsk, Russian Federation. E-mail: nagornaya71@mail.ru

Received 12.10.2021; approved after reviewing 11.11.2021; accepted for publication 22.11.2021.