Вестник Восточно-Сибирского института МВД России. 2023. № 4 (107). С. 292–300.
Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2023. No. 4 (107). P. 292–300.

5.1.4. Уголовно-правовые науки (юридические науки)

Научная статья
УДК 343.98
DOI: 10.55001/2312-3184.2024.61.81.025

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

Тимофеев Сергей Владимирович[1], Абидов Руслан Ризуанович[2]
[1]Восточно-Сибирский институт МВД России, Иркутск, Россия, tsv.1981@mail.ru
[2]Северо-Кавказский институт повышения квалификации (филиал) Краснодарского университета МВД России, Нальчик, Россия, abidov27@mail.ru

Введение. Киберпреступность – это особый феномен современного общества. Выявление, документирование и раскрытие преступлений, совершаемых с использованием цифровых технологий – это результат сложной и комплексной работы всех органов власти Российской Федерации, осуществляемой во взаимодействии с организациями, имеющими различную форму собственности. Принятое руководством страны решение о создании специализированного подразделения по борьбе с противоправным использованием информационно-коммуникационных технологий призвано решить многие проблемы, связанные с высоким уровнем киберпреступности в России. Широкий спектр проблем, обусловлен не только сложным механизмом совершения киберпреступлений, но и имеющимися пробелами в правовым регулированием правоотношений, связанных с обеспечением сохранности персональных данных людей, а также использованием преступниками множество доступных средств анонимизации личности.

Материалы и методы*:* Нормативную базу исследования составили Конституция Российской Федерации; уголовное, уголовно-процессуальное и оперативно-розыскное законодательство; иные федеральные законы; акты официального толкования норм; подзаконные нормативные акты. Кроме того, методологическую основу исследования составили всеобщий диалектический метод научного познания, общенаучные методы познания и некоторые частно-научные методы, среди которых: анкетирование и интервьюирование, опрос, обобщение следственной и судебной практики, литературных и интернет-источников.

Результаты исследования. Одной из основных проблем стало массовое проникновение достижений науки и техники не только в повседневную жизнь людей, но и криминализация многих сфере экономики, где используются информационно-телекоммуникационные технологии (далее – ИТТ). Эти технологии качественно изменили не только мировую экономику, но и повысили доступность получения практической любой информации, детерминировало появление новых форм преступности, средств их совершения и обеспечения мер конспирации преступников. Указанные обстоятельства неизбежно вызвали законную реакцию общества в потребности защиты от новых форм преступных посягательств.

Выводы и заключения. Применение обширных знаний из многих областей естественных и гуманитарных наук оказывают положительное влияние на общую ситуацию в стране и мире и показывает. Учитывая то обстоятельство, что в настоящее время объективно существуют угрозы для динамичного развития цифровой экономики в Российской Федерации, деятельность подразделений по организации борьбы с противоправным использованием информационно-коммуникационных технологий (далее – УБК) способна нивелировать проблему киберпреступности. Подготовка высококвалифицированных сотрудников для УБК, разработка научно-обоснованных методик и программ, способны решить проблему эффективного оперативно-розыскного противодействия киберпреступности.

Ключевые слова: оперативно-розыскная деятельность, информационные технологии, информационно-телекоммуникационные технологии, выявление, документирование и раскрытие киберпреступлений.

Для цитирования: Тимофеев С. В., Абидов Р. Р. Проблемы противодействия киберпреступности: вопросы теории и практики // Вестник Восточно-Сибирского института МВД России : науч.-практ. журнал. Иркутск: Восточно-Сибирский институт МВД России. 2024. № 1 (108). С. 292–300.
DOI: 10.55001/2312-3184.2024.61.81.025

5.1.4. Criminal Law Sciences
(legal sciences)

Original article

PROBLEMS OF COUNTERING CYBERCRIME: THEORY AND PRACTICE QUESTIONS

Sergey V. Timofeev [1], Ruslan R. Abidov [2]
[1] East Siberian Institute of the Ministry of Internal Affairs of Russia, Irkutsk, Russia,
[2] North Caucasus Institute for Advanced Studies (branch) of the Krasnodar University of the Ministry of Internal Affairs of Russia, Nalchik, Russia
[1]tsv.1981@mail.ru.
[2] abidov27@mail.ru

Introduction: Cybercrime is a special phenomenon of modern society. Detection, documentation and detection of offences committed with the use of digital technologies is the result of complex and comprehensive work by all the authorities of the Russian Federation, carried out in co-operation with organisations with different forms of ownership. The decision taken by the country's leadership to create a specialised unit to combat the unlawful use of information and communication technologies is intended to address many of the problems associated with the high level of cybercrime in Russia. A wide range of problems is caused not only by the complex mechanism of committing cybercrime, but also by the existing gaps in the legal regulation of legal relations related to ensuring the safety of people's personal data, as well as the use by criminals of many available means of anonymising individuals.

Materials and Methods: The normative basis of the study was formed by the Constitution of the Russian Federation; criminal, criminal procedural and operative-search legislation; other federal laws; acts of official interpretation of norms; subordinate normative acts. In addition, the methodological basis of the study was formed by the universal dialectical method of scientific knowledge, general scientific methods of knowledge and some private-scientific methods,

including: questionnaires and interviewing, survey, generalisation of investigative and judicial practice, literary and Internet sources.

The Results of the Study: One of the main problems has been the massive penetration of science and technology achievements not only into people's everyday lives, but also the criminalization of many areas of the economy where information and telecommunication technologies are used. (hereinafter referred to as ITT). These technologies have qualitatively changed not only the world economy, but also increased the accessibility of obtaining practically any information, determined the emergence of new forms of crime, means of committing them and ensuring measures of secrecy for criminals. These circumstances inevitably caused a legitimate reaction from society in the need for protection from new forms of criminal attacks.

Findings and Conclusions: The application of extensive knowledge from many areas of the natural and human sciences has a positive impact on the overall situation in the country and the world and shows. Considering the fact that there are currently objective threats to the dynamic development of the digital economy in the Russian Federation, the activities of units to organize the fight against the illegal use of information and communication technologies (hereinafter referred to as UCC) can neutralize the problem of cybercrime. The training of highly qualified employees for the UCD, the development of scientifically based methods and programs can solve the problem of effective operational investigative counteraction to cybercrime.

Keywords: operational investigative activities, information technologies, information and telecommunication technologies, identification, documentation and disclosure of cybercrimes.

For citation: Timofeev S.V., Abidov R. R. Problemy protivodejstvija kiberprestupnosti: voprosy teorii i praktiki. [Problems of countering cybercrime: theory and practice questions]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii - Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. Irkutsk, 2024, no. 1 (108), pp. 292–300.
DOI: 10.55001/2312-3184.2024.61.81.025

Киберпреступность – одна из современных проблем общества развивающихся и развитых стран мира. Массовое проникновение достижений науки и техники во все сферы жизни человечества привело к тому, что информационно-телекоммуникационные технологии (далее – ИТТ) оказали значительное воздействие на все стороны общественных отношений. Эти технологии качественно изменили представления людей о качестве и количестве предоставляемых услуг (в том числе дистанционно), способствовали развитию экономических отношений во всем мире, повысили доступность получения любой информации, независимо от локации, при условии наличия оборудованной точки доступа к сети Интернет. Это неизбежно детерминировало изменение способов и средств (механизмов) совершения преступлений.

Важным для практики противодействия киберпреступности является результативность процесса реализации полномочий уполномоченными оперативными подразделениями органов внутренних дел (далее – ОВД) в сфере оперативно-разыскного противодействия преступлениям, совершаемым с использованием цифровых технологий.

В организации деятельности оперативных подразделений ОВД по выявлению, документированию и раскрытию преступлений, совершаемых с использованием ИТТ, помимо общих тенденций увеличения количества рассматриваемых преступлений, отмечаются некоторые проблемы:

– неосведомленность оперативных сотрудников о новых способах или специфических особенностях преступлений в сфере ИТТ;

– практически полное отсутствие кадров в подразделениях уголовного розыска, имеющих образование в IT-сфере;

– недостаточное оснащение оперативных подразделений ОВД компьютерными устройствами с расширенными функциональными возможностями;

– отсутствие подсобного аппарата, предоставляющего оперативно значимую информацию по преступлениям в сфере ИТТ;

– устаревшие и не имеющие конкретизации методические рекомендации и наставления по раскрытию преступлений, совершаемых с использованием ИТТ.

В решении этой проблемы заслуживающей внимания представляется позиция ученых, считающих необходимым совершенствование оперативно-разыскной тактики осуществления ОРД в части проведения оперативно-разыскных и оперативно-технических мероприятий по выявлению и раскрытию киберпреступлений, а также разработок частных методик, посвященных вопросам организации и тактики эффективного использования методов и средств преодоления использования преступниками современных средств анонимизации личности [1, 2, 3, 4, 5, 6].

Для уяснения смысла, вкладываемого в понятие «киберпреступность», необходимо рассмотреть некоторые точки зрения на это.

Профессор В. А. Номоконов под термином «киберпреступность» предлагает понимать «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» [7, с. 48].

И. В. Романов определяет «киберпреступность» как целый спектр противоправных деяний, охватывающий не только преступления, совершенные в отношении компьютерной информации, но с использованием цифровых технологий, в том числе в киберпространстве [8, с. 107].

Несмотря на кажущуюся простоту приведенных определений, уяснение сущности понятия «киберпреступность» сложнее, чем кажется, поскольку оно имеет широкий смысл и потому не всегда однозначно используется как в законодательстве и литературе, так и в обычной повседневной речи.

Опираясь на труды ученых-правоведов, в той или иной мере исследовавших термин «киберпреступность», а также собственные теоретические поиски, мы под понятием «киберпреступность» предлагаем понимать все уголовно наказуемые деяния, где предметом и (или) средством совершения преступления являются цифровые технологии.

Цифровые технологии значительно трансформировали способы сокрытия различных форм девиантного поведения, а средства анонимизации личности спровоцировали лиц, ведущих преступный образ жизни, к их использованию при совершении уголовно наказуемых деяний.

Формы контакта «преступник – потерпевший» сведен к минимуму. Новые инструменты (приложения, гаджеты и т. д.) и методы сокрытия киберпреступлений облегчили их совершение, повысили меры конспирации преступной деятельности. Следствием чего в XXI в. киберпреступления стали одной из главных угроз для безопасности граждан, общества и нормального функционирования институтов государств. Эти формы преступного поведения довольно разнообразны. К примеру, осуществление кибератак на объекты жизнедеятельности; мошенничество; неправомерный доступ и перехват компьютерной информации и т. д.).

Иллюстрацией данного тезиса является официальная статистика ГИАЦ МВД России, наглядно демонстрирующая негативную динамику ежегодного роста числа

преступлений, совершаемых с использованием ИТТ. Так, за 2018–2022 гг. в Российской Федерации из 10 031 289 зарегистрированных преступлений – 1 965 839 относятся к данной категории (19,59 % от числа зарегистрированных), т. е. каждое пятое преступление совершенно с использованием ИТТ.

Обозначенная динамика увеличения количества преступлений данной категории прослеживается и в 2023 г. За январь–июль рост противоправных деяний в сфере информационно-телекоммуникационных технологий вырос на 27,9 %. Их удельный вес в числе всех преступных посягательств возрос до 32,37 %, а по тяжким и особо тяжким – до 55,65 %. Больше совершено дистанционных краж, совершенных с использованием или применением расчетных (пластиковых) карт, мошенничеств, преступлений, связанных с незаконным оборотом наркотиков и преступлений в сфере компьютерной информации (гл. 28 Уголовного кодекса Российской Федерации[1]). Раскрываемость киберпреступлений составила 32,5 %, в том числе совершенных с использованием сети Интернет – 31,7 %, расчетных (пластиковых) карт – 38,9 %, средств мобильной связи – 19,3 %. Сохраняет актуальность противодействие преступлениям, совершаемым с использованием ИТТ[2].

Как справедливо отметил А. В. Варданян «анализ оперативно-розыскной, следственной и судебной практики показал наличие серьезных проблем в научной обеспеченности цифровых методов предупреждения, раскрытия, расследования дистанционных хищений. В первую очередь, это связано с нехваткой разработок в теории оперативно-розыскной деятельности и, соответственно, науке криминалистики» [9, с. 8].

Фактор угрозы киберпреступности для российского общества не остался без должного внимания руководства страны. Президент Российской Федерации В. В. Путин своим указом от 30.09.2022 № 688 «О внесении изменений в некоторые акты» принял решение о создании в составе структуры Министерства внутренних дел Российской Федерации специализированного оперативного подразделения, призванного комплексно и целенаправленно осуществлять оперативно-розыскное противодействие киберпреступности, – Управление по организации борьбе с противоправным использованием информационно-коммуникационных технологий (далее – УБК).

В целях реализации этого решения приказом Министра внутренних дел Российской Федерации В. А. Колокольцева от 31 марта 2023 г. № 199 «Об утверждении перечня оперативных подразделений органов внутренних дел российской федерации, правомочных осуществлять оперативно-розыскную деятельность» УБК было уполномочено осуществлять ОРД в полном объеме.

Приведенные выше цифры и информация показывают, что в целях совершенствования мер по борьбе с киберпреступлениями остро назрел вопрос о подготовке квалифицированных сотрудников для оперативных подразделений органов внутренних дел по борьбе с противоправным использованием ИТТ[3]. В центре внимания

---

[1] Уголовный кодекс Российской Федерации (УК РФ) от 13.06.1996 N№63-ФЗ (ред. от 04.08.2023) : принят Государственной Думой 24 мая 1996 года : одобрен Советом Федерации 5 июня 1996 года // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_ doc_LAW_10699/ (дата обращения: 24.10.2023). Режим доступа: свободный.

[2] Министерство внутренних дел Российской Федерации : сайт // URL: https://мвд.рф/ dejatelnost/statistics (дата обращения: 22.02.2024)

[3] Приказом Министра внутренних дел Российской Федерации генерала полиции В. А. Колокольцева от 29.12.2022 № 1110 было утверждено Положение об Управлении по организации борьбе с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации.

руководства Министерства внутренних дел – вопросы комплектования профильных подразделений сотрудниками, обладающими глубокими техническими знаниями[4].

В современных условиях необходимо проведение тщательного анализа современных проблем борьбы с киберпреступностью, разрешение которых невозможно без осмысления тенденций развития теоретической юридической науки, законодательства и практики его применения. В этой связи логично обратиться к некоторым из них.

Во-первых, до недавнего времени в правовом регулировании общественных отношений Российской Федерации в сфере кибербезопасности наблюдались противоречивые процессы. С одной стороны, из законодательства, в силу его нормативности, требований юридической техники и формальной определенности, постепенно вымываются нравственные начала. В результате принципы справедливости и гуманности в некоторых случаях носят декларативный характер, все чаще правоохранители вынужденно прибегают к ограничению прав граждан (например, право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений). Это влияет на состояние законности и правопорядка, способствует распространению нигилистических идей в обществе. С другой стороны, в ситуации значительного роста киберпреступлений в Российской Федерации законодатель создает правовые условия для повышения эффективности мер противодействия этому противоправному явлению.

Во-вторых, очевидно наличие проблемы отставания уровня знаний в области функционирования сетей передачи цифровых данных, в том числе в теневом сегменте сети Интернет – DarkNet, и необходимость практической подготовки сотрудников оперативных подразделений к противодействию киберпреступности [10, с. 17]. Зачастую, имея юридическое образование, сотрудники полиции ограничены в возможности своевременного и эффективного принятия соответствующих мер защиты граждан от преступлений, совершаемых с использованием ИТТ.

В-третьих, общественные отношения настолько динамичны, что законодатель не в силах спрогнозировать возможные проблемы в будущем, а также своевременно отреагировать на имеющиеся, что особенно актуально для правоохранительных органов в части борьбы с цифровой преступностью [11, с. 17]. В этой связи возникает острая необходимость в совершенствовании законодательства и правоохранительной деятельности, подготовке профессиональных кадров для правоохранительных органов.

В-четвертых, наличие в оперативно-разыскном законодательстве норм, ограничивающих проведение оперативно-разыскных мероприятий разведывательного характера в сети Интернет без отсутствия формальных оснований, предусмотренных ст. 7 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»[5]. В первую очередь это связано с неготовностью общества ограничить личные права в угоду общественным интересам. Так, в российском правоведении на смену существовавших многие десятилетия методологии и догматизму приходит многообразие научных направлений. Появляются первые научные исследования в области цифровых следов преступлений и их использования в уголовном судопроизводстве. В результате

[4] Обобщенные данные Главного информационного центра МВД России за 2022 г. : офиц. сайт. URL: https://мвд.рф/reports/item/35396677/ (дата обращения: 24.10.2023). Режим доступа: свободный.

[5] Об оперативно-розыскной деятельности : Федеральный закон № 144-ФЗ (в послед. ред.) : принят Государственной Думой 5 июля 1995 года // КонсультантПлюс : сайт. URL: https://www.consultant.ru/ document/cons_doc_LAW_7519/ (дата обращения: 10.09.2023). Режим доступа: свободный.

стало очевидным, что понятийно категориальный аппарат теоретической юридической науки требует дальнейшего развития. При этом многие современные проблемы правовой реальности носят не только объективный, но и субъективный характер.

Деятельность УБК дает основание полагать, что динамика ежегодного роста киберпреступности и сравнительно низкий процент раскрываемости этих преступлений, отмечающийся в последние годы, впоследствии эффективно купируются. Решению этой задачи будут способствовать подготовка квалифицированных сотрудников для данного подразделения, разработка научно-обоснованных методик и программ, способных решить проблему эффективного оперативно-разыскного противодействия киберпреступности.

Учитывая обстоятельство, что в настоящее время объективно существуют угрозы для динамичного развития цифровой экономики в Российской Федерации, деятельность УБК будет способствовать нивелированию обозначенной проблемы, а подготовка высококвалифицированных сотрудников для этого подразделения, разработка научно-обоснованных методик и программ способны решить проблему эффективного оперативно-разыскного противодействия киберпреступности.

СПИСОК ИСТОЧНИКОВ

1. Осипенко, А. Л. Киберугрозы в отношении несовершеннолетних и особенности противодействия им с применением информационных технологий / А. Л. Осипенко, В. С. Соловьев // Общество и право : науч. журн. Краснодар : Краснодарский университет Министерства внутренних дел Российской Федерации. 2019. № 3(69). С. 23–31.

2. Шевко, Н. Р. Мошенничество в киберпространстве: реальный ущерб в виртуальном мире // Вестник Восточно-Сибирского института МВД России. Иркутск : Восточно-Сибирский институт МВД России. 2023. № 3(106). С. 276–284.

3. Теория оперативно-розыскной деятельности / О. А. Вагин, К. К. Горяинов, А. В. Земскова и др. : учебник. Москва : Изд. Дом "Инфра-М", 2018. 762 с.

4. Дерюгин, Р. А. О современных способах совершения мошенничества, связанного с использованием персональных данных пользователей сети Интернет // Криминалистика: вчера, сегодня, завтра : сб. науч. тр. Иркутск : Восточно-Сибирский институт МВД России. 2023. № 1(25). С. 65–74.

5. Куликов, А. В. Обстоятельства, подлежащие установлению и доказыванию при расследовании преступлений, связанных с незаконным оборотом наркотических средств, психотропных веществ и их аналогов / А. В. Куликов, О. А. Шелег // Вестник экономической безопасности : науч. журн. Москва : Московский ун-т Министерства внутренних дел Российской Федерации им. В. Я. Кикотя. 2023. № 1. С. 117–120.

6. Железняк, И. Н. Проблемы цифровизации негласного сотрудничества граждан с органами, осуществляющими оперативно-розыскную деятельность / И. Н. Железняк // Вестник Восточно-Сибирского института МВД России. Иркутск : Восточно-Сибирский институт МВД России. 2022. № 2(101). С. 181–192.

7. Номоконов, В. А., Тропина, Т. Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра : науч. журн. Санкт-Петербург : Санкт-Петербургский международный криминологический клуб. 2012. №. 24. С. 45–55.

8. Романов, И. В. Понятие киберпреступлений и его значение для расследования // Сибирские уголовно-процессуальные и криминалистические чтения : науч.журн. Иркутск : Байкальский государственный университет. 2016. № 5 (13). С. 105–109.

9.Варданян, А. В. Проблема систематизации цифровых методов оперативно-розыскной деятельности, используемых в борьбе с дистанционными хищениями, и их криминалистическое значение // Юристъ-Правоведъ : науч.-теорет. и информ.-метод.

журн. Росто-на-Дону : Ростовский юридический институт Министерства внутренних дел Российской Федерации. 2022. № 2(101). С. 7–13.

10. Железняк, И. Н. Дискреционность полномочий в оперативно-розыскной деятельности органов внутренних дел как маркер "ветхости" профильного закона / И. Н. Железняк // Общество и право : науч. журн. Краснодар : Краснодарский университет Министерства внутренних дел Российской Федерации. 2021. № 4(78). С. 67–71.

11. Тимофеев, С. В. К вопросу добывания оперативно значимой информации в сети Интернет: проблемы и пути их решения // Криминалистика: вчера, сегодня, завтра : сб. науч. тр. Иркутск : Восточно-Сибирский институт МВД России. 2021. № 2(18). С. 111–117.

REFERENCES

1. Osipenko, A. L. Kiberugrozy v otnoshenii nesovershennoletnih i osobennosti protivodejstvija im s primeneniem informacionnyh tehnologij [Cyber threats against minors and features of countering them using information technologies]. Obshhestvo i pravo - Society and Law. 2019, no. 3(69), pp. 23-31.

2. Shevko, N. R. Moshennichestvo v kiberprostranstve: real'nyj ushherb v virtual'nom mire [Fraud in cyberspace: real damage in the virtual world]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii - Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2023, no. 3(106),pp. 276-284. – DOI 10.55001/2312-3184.2023.76.95.024.

3. Vagin O. A., Goryainov K. K., Zemskova A. V. O sovremennyh sposobah sovershenija moshennichestva, svjazannogo s ispol'zovaniem personal'nyh dannyh pol'zovatelej seti Internet [The theory of operational-search activity]. Moscow, 2018, 762 p.

4. Deryugin, R. A. O sovremennyh sposobah sovershenija moshennichestva, svjazannogo s ispol'zovaniem personal'nyh dannyh pol'zovatelej seti Internet [On modern methods of committing fraud associated with the use of personal data of Internet users]. Kriminalistika: vchera, segodnja, zavtra - Forensic science: yesterday, today, tomorrow. 2023, no. 1(25), pp. 65-74, DOI 10.55001/2587-9820.2023.56.41.006.

5. Kulikov, A. V. Obstojatel'stva, podlezhashhie ustanovleniju i dokazyvaniju pri rassledovanii prestuplenij, svjazannyh s nezakonnym oborotom narkoticheskih sredstv, psihotropnyh veshhestv i ih analogov [Circumstances to be established and proven during the investigation of crimes related to the illicit trafficking of narcotic drugs, psychotropic substances and their analogues]. Vestnik jekonomicheskoj bezopasnosti - Vestnik of Economic Security. 2023, no. 1, pp. 117-120. – DOI 10.24412/2414-3995-2023-1-117-120.

6. Zheleznyak, I. N. Problemy cifrovizacii neglasnogo sotrudnichestva grazhdan s organami, osushhestvljajushhimi operativno-rozysknuju dejatel'nost' [Problems of digitalization of secret cooperation of citizens with bodies carrying out operational investigative activities]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii - Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2022, no. 2(101), pp. 181-192. – DOI 10.55001/2312-3184.2022.93.64.016.

7. Nomokonov V. A., Tropina T. L. Kiberprestupnost' kak novaja kriminal'naja ugroza [Cybercrime as a new criminal threat]. Kriminologija: vchera, segodnja, zavtra - Criminology: yesterday, today, tomorrow. 2012, no. 24, pp. 45-55.

8. Romanov I. V. Ponjatie kiberprestuplenij i ego znachenie dlja rassledovanija [The concept of cybercrime and its significance for investigation]. Sibirskie ugolovno-processual'nye i kriminalisticheskie chtenija - Siberian criminal procedural and forensic readings. 2016, no. 5 (13), pp. 105-109.

9. Vardanyan, A. V. Problema sistematizacii cifrovyh metodov operativno-rozysknoj dejatel'nosti, ispol'zuemyh v bor'be s distancionnymi hishhenijami, i ih kriminalisticheskoe znachenie [The problem of systematization of digital methods of operational investigative

activities used in the fight against remote theft, and their forensic significance]. Jurist#-Pravoved# - Yurist-Pravoved. 2022, no. 2(101), pp. 7-13.

10. Zheleznyak, I. N. Diskrecionnost' polnomochij v operativno-rozysknoj dejatel'nosti organov vnutrennih del kak marker "vethosti" profil'nogo zakona [Discretion of powers in the operational investigative activities of internal affairs bodies as a marker of the “dilapidation” of the relevant law]. Obshhestvo i pravo - Society and Law. 2021, no. 4(78), pp. 67-71.

11. Timofeev, S. V. K voprosu dobyvanija operativno znachimoj informacii v seti Internet: problemy i puti ih reshenija [On the issue of obtaining operationally significant information on the Internet: problems and ways to solve them]. Kriminalistika: vchera, segodnja, zavtra - Forensic science: yesterday, today, tomorrow. 2021, no. 2(18), pp. 111-117.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Тимофеев Сергей Владимирович, кандидат юридических наук, доцент кафедры оперативно-разыскной деятельности и специальной техники в органах внутренних дел. Восточно-Сибирский институт МВД России, 664074, Россия, г. Иркутск, ул. Лермонтова, 110.
ORCID: 0000-0002-4172-1571
Абидов Руслан Ризуанович, старший преподаватель кафедры огневой подготовки.
Северо-Кавказский институт повышения квалификации (филиал) Краснодарского университета МВД России. 360016, Россия, г. Нальчик, ул. Мальбахова, 123.

INFORMATION ABOUT THE AUTHOR

Timofeev Sergey Vladimirovich, Candidate of legal sciences, Associate Professor, Associate Professor of the Department of Operational Investigative Activities and Special Equipment in Internal Affairs Bodies. East Siberian Institute of the Ministry of Internal Affairs of Russia, 664074, Russia, Irkutsk, st. Lermontova, 110.
ORCID: 0000-0002-4172-1571
Abidov Ruslan Rizuanovich, senior lecturer of the department of fire training. North Caucasus Institute for Advanced Studies (branch) of the Krasnodar University of the Ministry of Internal Affairs of Russia. 360016, Nalchik, Russia, Malbakhova, 123.

Статья поступила в редакцию 25.10.2023; одобрена после рецензирования 02.11.2023; принята к публикации 01.03.2024.

The article was received by the editors on 25.10.2023; approved after peer review 02.11.2023; accepted for publication 01.03.2024.