УГОЛОВНО-ПРАВОВЫЕ НАУКИ

Научная статья
УДК: 343.102

К ВОПРОСУ О ПОЛУЧЕНИИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ПРИ ВЫЯВЛЕНИИ И РАСКРЫТИИ ПРЕСТУПЛЕНИЙ ДИСТАНЦИОННОГО ХАРАКТЕРА (ОПЫТ РОССИЙСКОЙ ФЕДЕРАЦИИ, ГОСУДАРСТВ ВОСТОЧНОЙ И ЮГО-ВОСТОЧНОЙ АЗИИ)

Виталий Федорович Васюков[1], Эмин Исахан оглы Дамирчиев[2]
[1]Московская академия Следственного комитета Российской Федерации имени А. Я. Сухарева, г. Москва, Российская Федерация, vvf0109@yandex.ru
[2]Московский государственный институт международных отношений МИД России (МГИМО), г. Москва, Российская Федерация, damirchiyev@mail.ru

Аннотация. На основе анализа доктринальных подходов рассматриваются правовая природа, цель и задачи оперативно-розыскного мероприятия «получение компьютерной информации». Отечественная конструкция мероприятия сопоставляется с подходами государств Восточной и Юго-Восточной Азии – Китайской Народной Республики, Японии, Республики Корея, Сингапура и Социалистической Республики Вьетнам – к доступу правоохранительных органов к компьютерной информации при выявлении и раскрытии преступлений дистанционного характера. Сформулированы предложения по совершенствованию российского регулирования.

Ключевые слова оперативно-розыскная деятельность, компьютерная информация, преступления дистанционного характера, электронные доказательства, удалённый доступ, зарубежный опыт

Для цитирования: Васюков В. Ф., Дамирчиев Э. И. К вопросу о получении компьютерной информации при выявлении и раскрытии преступлений дистанционного характера (опыт Российской Федерации, государств Восточной и Юго-Восточной Азии) // Криминалистика: вчера, сегодня, завтра. 2026. Т. 38. № 2. С. 7–17.

ON OBTAINING COMPUTER INFORMATION IN THE DETECTION AND INVESTIGATION OF REMOTE CRIMES (THE EXPERIENCE OF THE RUSSIAN FEDERATION AND EAST AND SOUTHEAST ASIAN STATES)

Vitaly F. Vasyukov[1], Emin Is. oglu Damirchiyev[2]
[1]Moscow Academy of the Investigative Committee of the Russian Federation named after A. Ya. Sukharev, Moscow, Russian Federation, vvf0109@yandex.ru
[2]Moscow State Institute of International Relations of the Ministry of Foreign Affairs of Russia (MGIMO), Moscow, Russian Federation, damirchiyev@mail.ru

Abstract Based on an analysis of doctrinal approaches, the article examines the legal nature, purpose and tasks of the operational-search measure “obtaining computer information”. The Russian construction of the measure is compared with the approaches of East and Southeast Asian states – the People’s Republic of China, Japan, the Republic of Korea, Singapore and the Socialist Republic of Vietnam – to law enforcement access to computer information in the detection and investigation of remote (distance) crimes. Proposals for improving Russian regulation are formulated

Keywords: operational-search activity, obtaining computer information, computer information, remote crimes, electronic evidence, remote access, foreign experience

For citation: Vasyukov V. F., Damirchiyev E. I. K voprosu o poluchenii kompyuternoy informatsii pri vyyavlenii i raskrytii prestupleniy distantsionnogo kharaktera (opyt Rossiyskoy Federatsii, gosudarstv Vostochnoy i Yugo-Vostochnoy Azii) [On obtaining computer information in the detection and investigation of remote crimes (the experience of the Russian Federation and East and Southeast Asian states)]. Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2026, vol. 38, no. 2, pp. 7–17 (in Russ.).

Введение

В условиях стремительного развития цифровых технологий и роста числа преступлений, совершаемых с использованием информационно-коммуникационных технологий, доступ правоохранительных органов к компьютерной информации приобретает ключевое значение для выявления и раскрытия деяний дистанционного характера, то есть совершаемых удалённо, без непосредственного контакта виновного с потерпевшим и местом совершения преступления.

Федеральным законом от 6 июля 2016 г. № 374-ФЗ[1] перечень оперативно-розыскных мероприятий (далее – ОРМ) статьи 6 Федерального закона «Об оперативно-розыскной деятельности»[2] был дополнен новым самостоятельным мероприятием – получением компьютерной информации (далее – ПКИ). Вместе с тем ни легального определения данного мероприятия, ни подзаконного нормативного правового акта, раскрывающего его содержание, субъектов и порядка проведения до настоящего времени не принято, а понятие компьютерной информации закреплено лишь в примечании 1 к статье 272 УК РФ, согласно которому ею признаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств

[1] О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : федеральный закон от 6 июля 2016 г. № 374-ФЗ // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/

[2] Об оперативно-розыскной деятельности : федеральный закон от 12 августа 1995 г. № 144-ФЗ (с послед. изм.) // КонсультантПлюс.

их хранения, обработки и передачи[3]. Изложенное обусловливает необходимость обращения к доктринальным подходам, сложившимся вокруг данного мероприятия, и к зарубежному опыту регулирования доступа к компьютерной информации.

Основная часть

Вопросам получения компьютерной информации как оперативно-розыскного мероприятия посвящены труды С. В. Баженова, С. С. Епифанова, Н. С. Вечкаева, А. Л. Осипенко, В. В. Петрова, И. В. Петрова, Е. И. Фокина, Е. И. Фойгеля, А. Г. Проценко, Л. Е. Щетнёва и С. М. Томилина и других исследователей. Вместе с тем единого подхода к ряду ключевых вопросов в науке не выработано.

Наиболее разработанным является вопрос о понятии и правовой природе мероприятия. Прежде всего заслуживает внимания доктринальное определение, сформулированное С. В. Баженовым, согласно которому под получением компьютерной информации следует понимать негласное оперативно-розыскное мероприятие, осуществляемое с использованием возможностей оперативно-технических подразделений в целях копирования или изъятия сведений, содержащихся на жёстком диске компьютера или на иных электронных носителях, когда для их получения требуется удалённый доступ по информационно-коммуникационным сетям, в том числе с применением заблаговременно внедрённых закладных устройств и (или) программных компонентов [1, с. 31].

Указанный подход опирается на сформулированные ранее выводы А. Л. Осипенко, охарактеризовавшего получение компьютерной информации как технически сложные, требующие специальной подготовки действия по добыванию сведений, хранящихся в компьютерных системах либо передаваемых по каналам связи, и предложившего классификацию источников оперативно значимых компьютерных данных и способов доступа к ним [2, с. 83].

Развитие данная линия получила в работах Л. Е. Щетнёва и С. М. Томилина, предложивших закрепить определение мероприятия непосредственно в нормативных правовых актах, регламентирующих оперативно-розыскную деятельность (далее – ОРД), и понимающих под ним совокупность действий оперативных подразделений по получению доступа к компьютерным данным, представляющим оперативный интерес и циркулирующим в компьютерных сетях [3].

Не получил единообразного разрешения вопрос о соотношении нового мероприятия со снятием информации с технических каналов связи. Так, С. В. Баженов отстаивает самостоятельный характер получения компьютерной информации и проводит принципиальное разграничение – если сведения скачиваются из сети и установить IP-адрес отправителя не представляется возможным, речь идёт о сетевой, а не компьютерной информации, в связи с чем отнесение такого перехвата к рассматриваемому мероприятию автор признаёт неправомерным [1, с. 32].

Иной позиции придерживается В. В. Петров, по мнению которого снятие информации с технических каналов связи и получение компьютерной информации сходны по принципу применения, поскольку осуществляются на единой технической базе – с использованием системы техниче-

[3] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (с послед. изм.) : примечание 1 к статье 272 // КонсультантПлюс.

ских средств для обеспечения оперативно-розыскных мероприятий на сетях документальной электросвязи – и носят негласный характер, что приводит автора к выводу о необходимости единообразного правового толкования организации и порядка их проведения [4, с. 142].

Особо значимым является вопрос о способах реализации мероприятия. Так, И. В. Петров и Е. И. Фокин рассматривают получение компьютерной информации как сложносоставное мероприятие, трудность которого обусловлена областью получения данных, сложностью их формализации и отсутствием нормативного закрепления способов проведения; разрешение названных проблем авторы связывают с мерами государственной политики – формированием единого информационного пространства и применением аналитических средств на основе нейронных сетей с привлечением операторов связи и крупных организаций в сфере информационных технологий [5].

В свою очередь, Е. И. Фойгель и А. Г. Проценко акцентируют внимание на технологической стороне вопроса – расширении круга источников за счёт устройств «интернета вещей», реализации мероприятия с использованием комплексов СОРМ, а также нерешённости вопросов, связанных с предоставлением ключей шифрования и хранением значительных массивов данных [6].

Наконец, в науке формируется направление, рассматривающее получение компьютерной информации как частный случай более широкой проблемы цифровизации оперативно-розыскной деятельности. Так, С. С. Епифанов и Н. С. Вечкаев, анализируя применение цифровых оперативно-розыскных средств, обосновывают вывод о том, что без совершенствования ведомственного нормативного правового регулирования порядка принятия решений на их использование развитие оперативной работы существенно затруднено [7, с. 521].

Следует констатировать, что при наличии расхождений по частным вопросам исследователи единодушны в общем – конструкция мероприятия сохраняет общий характер, а предусмотренный законом подзаконный акт так и не принят.

Поскольку легального определения цели мероприятия законодатель не сформулировал, она может быть выведена из совокупности нормативных предписаний. Назначение Федерального закона № 374-ФЗ состоит в усилении противодействия терроризму и обеспечении общественной безопасности.

Вместе с тем как самостоятельное мероприятие получение компьютерной информации служит достижению всего круга задач оперативно-розыскной деятельности, закреплённых в статье 2 Федерального закона «Об оперативно-розыскной деятельности», – выявлению, предупреждению, пресечению и раскрытию преступлений, а также установлению причастных к ним лиц[4]. Применительно к цифровой среде это означает переориентацию классических задач ОРД на источники, существующие исключительно в форме компьютерной информации.

С учётом изложенного цель рассматриваемого мероприятия может быть определена как негласное получение оперативно значимых сведений, хранящихся в компьютерных системах либо передаваемых по информационно-

[4] Об оперативно-розыскной деятельности : федеральный закон от 12 августа 1995 г. № 144-ФЗ : статья 2 // КонсультантПлюс.

телекоммуникационным сетям, в случаях, когда доступ к ним требует использования возможностей оперативно-технических подразделений [2, с. 84].

Именно указание на такие подразделения в части 4 статьи 6 ФЗ об ОРД отграничивает мероприятие от ознакомления с общедоступными сведениями, осуществимого любым пользователем. Производные от названной цели задачи мероприятия могут быть представлены следующим образом:

1. Обнаружение и фиксация компьютерной информации о лицах, событиях и связях, представляющих оперативный интерес, в том числе хранящейся на серверах, в центрах обработки данных и облачных хранилищах.

2. Копирование либо изъятие такой информации с преодолением, при необходимости, технических и программных средств защиты, осуществление которого, как правило, невозможно без участия специалиста оперативно-технического подразделения.

3. Получение удалённого доступа к компьютеру или серверу по сетям в случаях, когда непосредственный физический доступ исключён либо нецелесообразен.

4. Истребование и использование сведений из массивов, которые операторы связи обязаны накапливать и хранить в силу постановления Правительства Российской Федерации от 12 апреля 2018 г. № 445[5].

5. Закрепление полученных результатов в форме, обеспечивающей их последующую легализацию и использование в доказывании.

Таким образом, нормативная регламентация мероприятия носит двухуровневый характер. Федеральный закон № 374-ФЗ определяет его стратегическое назначение и сам инструмент, тогда как постановление Правительства № 445 обеспечивает его ресурсную основу, гарантируя сохранность искомой информации на территории Российской Федерации.

Сравнительно-правовой анализ показывает, что государства Восточной и Юго-Восточной Азии избрали отличный от российского путь регулирования доступа правоохранительных органов к компьютерной информации при выявлении и раскрытии преступлений дистанционного характера.

Китайская Народная Республика. В отличие от Российской Федерации, доступ к компьютерной информации в Китае не выделен в самостоятельное негласное мероприятие, а инкорпорирован в уголовно-процессуальный механизм и снабжён детальной регламентацией. Основополагающее значение имеют Положения о некоторых вопросах сбора, изъятия, проверки и оценки электронных данных при производстве

[5] Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи : постановление Правительства Российской Федерации от 12 апреля 2018 г. № 445 // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001201804190032 (дата обращения: 03.06.2026).

по уголовным делам, совместно принятые Верховным народным судом, Верховной народной прокуратурой и Министерством общественной безопасности и вступившие в силу 1 октября 2016 г.[6]

Названный акт впервые на системном уровне урегулировал обращение с электронными данными как самостоятельным видом доказательств и прямо допустил сетевое изъятие данных, исходный носитель которых находится на удалённой компьютерной системе, а при необходимости – удалённый осмотр такой системы; применение в этих целях технических следственных мер обусловлено соблюдением строгого порядка их санкционирования. Доступ обставлен процессуальными гарантиями, ориентированными на последующее доказывание, – сбор и изъятие осуществляются не менее чем двумя следователями, ход действий протоколируется и фиксируется видеозаписью, а исходный носитель по общему правилу опечатывается в целях обеспечения целостности данных.

Китайский режим стал предметом ряда зарубежных научных исследований. Так, отмечаются сохраняющиеся дефекты регулирования – уязвимость прав подозреваемых, отсутствие специализированного следственного подразделения и недостаточная определённость отдельных положений [8]. Законодательные усилия, доктринальные дискуссии и практика применения правил об электронных данных подробно проанализированы в новейшей литературе [9], а вопросы построения системы электронных доказательств в уголовном судопроизводстве КНР рассмотрены в специальных работах [10]. Указанный режим был уточнён Правилами Министерства общественной безопасности 2019 г., разграничившими порядок работы с данными внутри страны и за её пределами и ограничившими сетевое изъятие зарубежных данных случаями их нахождения в открытом доступе[7].

Наряду с процессуальным регулированием в Китае действует специальный материально-правовой механизм. Закон о противодействии телекоммуникационному и онлайн-мошенничеству, принятый 2 сентября 2022 г. и вступивший в силу 1 декабря 2022 г., в ст. 2 определяет такое мошенничество как совершаемое удалённым, бесконтактным способом с использованием телекоммуникационных и сетевых технологий, что по существу совпадает с используемым в настоящей работе понятием преступления дистанционного характера. Статья 20 названного закона возлагает на орган общественной безопасности при Государственном совете во взаимодействии с иными ведомствами обязанность создать систему мгновенного запроса, экстренной приостановки платежа и быстро-

[6] Provisions on Several Issues Concerning the Collection, Extraction, Examination, and Judgment of Electronic Data in the Handling of Criminal Cases : приняты Верховным народным судом, Верховной народной прокуратурой и Министерством общественной безопасности КНР, вступили в силу 1 октября 2016 г. : англ. пер. // China Law Translate. URL: https://www.chinalawtranslate.com/en/provision-on-collection-and-review-of-digital-information-in-criminal-cases/ (дата обращения: 03.06.2026).

[7] Rules of Public Security Organs for Collecting Electronic Evidence in Criminal Cases : утв. Министерством общественной безопасности КНР, 2019 г. : статья 33 : англ. пер. // China Law Translate. URL: https://www.chinalawtranslate.com/en/Public-Security-Organs-for-Collecting-Electronic-Evidence-in-Criminal-Cases/

го замораживания средств, содействие которой обязаны оказывать банковские и небанковские платёжные организации[8].

Япония. Японское законодательство, как и китайское, не предусматривает самостоятельного негласного мероприятия по образцу российского – доступ к компьютерной информации включён в уголовно-процессуальный институт обыска и выемки и основан на судебной санкции. Реформа Уголовно-процессуального кодекса 2011 г., приводившая национальное законодательство в соответствие с требованиями Конвенции о преступности в сфере компьютерной информации, ввела два значимых правомочия. Первое из них – выемка с предварительным копированием данных при удалённом доступе. Согласно ст. 99(2) УПК, если изымаемый предмет представляет собой компьютер и имеются разумные основания полагать, что подключённый к нему по телекоммуникационным линиям носитель использовался для хранения записей, созданных или изменённых с помощью этого компьютера, такой компьютер либо носитель может быть изъят после копирования соответствующих записей; аналогичное правомочие применительно к стадии расследования закреплено в ст. 218[9]. Тем самым реформа 2011 г. позволила вместо изъятия самого компьютера или сервера копировать соответствующие данные и изымать носитель информации, в том числе без согласия его владельца.

Существенно, что японская модель прямо определяет пределы принуждения. Лицо, исполняющее выемку, вправе потребовать от субъекта эксплуатации компьютера иного содействия, включая расшифровку зашифрованных записей, однако отказ от такого содействия ответственности не влечёт. Перехват же содержания сообщений вынесен в отдельный закон и допускается лишь по ограниченному кругу тяжких преступлений[10]. Тем самым в японском праве последовательно разграничены доступ к хранящимся компьютерным данным и перехват сообщений.

Республика Корея. Подход Республики Корея основан на Законе о защите тайны связи и характеризуется выраженным конституционно-судебным контролем. Закон разграничивает два режима. Первый из них – меры, ограничивающие связь, то есть перехват содержания сообщений, допускаемый исключительно по судебному разрешению, по ограниченному кругу оснований и на ограниченный срок.

Второй – предоставление данных, подтверждающих факт связи (сведений о соединениях, сеансах доступа и местоположении), регламентированное статьями 13 и 13-3 и также поставленное под судебный контроль[11].

---

[8] Anti-Telecom and Online Fraud Law of the People's Republic of China : принят на 36-й сессии Постоянного комитета ВСНП 13-го созыва 2 сентября 2022 г., вступил в силу 1 декабря 2022 г. : статьи 2, 20 : англ. пер. // The National People's Congress of the PRC. URL: http://en.npc.gov.cn.cdurl.cn/2022-09/02/c_875967.htm/

[9] Code of Criminal Procedure (Act No. 131 of 1948, с изм. Act No. 74 of 2011) : статьи 99(2), 218 : англ. пер. // Japanese Law Translation. URL: https://www.japaneselawtranslation.go.jp/en/laws/view/2056/en/

[10] Government Access to Encrypted Communications: Japan // Library of Congress. URL: https://maint.loc.gov/law/help/encrypted-communications/japan.php (дата обращения: 03.06.2026).

[11] Protection of Communications Secrets Act: статьи 12-2, 13, 13-3 : англ. пер. // Korea

Показательно, что после признания Конституционным судом в 2018 г. не соответствующим Конституции прежнего порядка так называемого пакетного перехвата интернет-соединений законодатель ввёл статью 12-2, установившую самостоятельный режим обращения с материалами, полученными такими мерами при расследовании преступлений. Тем самым расширение негласных полномочий заменяется их детализацией и обеспечением процессуальными гарантиями под судебным надзором.

Сингапур. Сингапурское законодательство закрепляет доступ к компьютерной информации непосредственно в Уголовно-процессуальном кодексе 2010 г. Согласно статье 39 («Полномочие на доступ к компьютеру») сотрудник полиции или уполномоченное лицо при расследовании преступления, влекущего арест, вправе получить доступ к компьютеру, произвести поиск и копирование данных, а также воспрепятствовать доступу к нему иных лиц; в отношении компьютеров, находящихся за пределами страны, такие полномочия осуществляются лишь с согласия владельца либо на ином законном основании.

Статья 40 («Полномочие на доступ к информации для расшифровки») дополнительно, по приказу Генерального прокурора, наделяет правом получить доступ к средствам расшифровки и потребовать от причастных лиц содействия в дешифровании данных[12]. Тем самым сингапурская модель сочетает широкие полномочия по доступу к компьютеру с дифференцированным порядком санкционирования – от полицейского усмотрения до прокурорского приказа.

Социалистическая Республика Вьетнам. Во Вьетнаме доступ к компьютерной информации опирается на Уголовно-процессуальный кодекс 2015 г., впервые признавший электронные данные самостоятельным источником доказательств и закрепивший в статьях 223-228 специальные следственные меры – негласную аудио- и видеозапись, прослушивание телефонных переговоров и негласный сбор электронных данных. Их применение допускается лишь по делам о преступлениях против национальной безопасности, о наркопреступлениях, коррупции, терроризме, отмывании денежных средств и иных особо тяжких деяниях и только после санкционирования компетентным должностным лицом[13].

Дополнительно Закон о кибербезопасности 2018 г. возлагает на поставщиков услуг, в том числе зарубежных, обязанности по хранению данных и содействию органам, что сближает вьетнамский подход с китайским в части инфраструктуры доступа к данным.

Legislation Research Institute. URL: https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=59856&type=part&key=43/

[12] Criminal Procedure Code 2010 (Act 15 of 2010, Cap. 68) : sections 39, 40 // Singapore Statutes Online. URL: https://sso.agc.gov.sg/Act/CPC2010 (дата обращения: 03.06.2026).

[13] Уголовно-процессуальный кодекс Социалистической Республики Вьетнам 2015 г. (Закон № 101/2015/QH13) : статьи 223–228 (специальные следственные меры, включая негласный сбор электронных данных); Закон о кибербезопасности 2018 г. (Закон № 24/2018/QH14) // Vietnam Law and Legal Forum. URL: https://vietnamlawmagazine.vn/special-procedural-investigation-measures-under-criminal-procedure-code-73947.html (дата обращения: 03.06.2026).

Выводы и заключение

Проведённое сопоставление позволяет выявить единый для всех рассмотренных правовых систем вызов – необходимость законного доступа к сведениям, существующим исключительно в форме компьютерной информации, при выявлении и раскрытии преступлений дистанционного характера, – и различные варианты ответа на него.

Российская Федерация ответила на данный вызов введением самостоятельного негласного оперативно-розыскного мероприятия в рамках Закона об ОРД. Между тем, отдельные азиатские государства избрали путь процессуальной детализации. Особую сложность во всех рассмотренных государствах сохраняет трансграничный доступ к данным, размещённым за пределами национальной юрисдикции. В зарубежной литературе детально проанализированы национальные подходы к такому доступу [11], а также механизмы прямого взаимодействия правоохранительных органов с поставщиками облачных услуг [12].

Изложенное позволяет сформулировать три ориентира для совершенствования отечественного регулирования. Во-первых, представляется обоснованным перенос акцента с декларации мероприятия на детальную регламентацию порядка его проведения по примеру китайских Положений об электронных данных. Во-вторых, требует прямого разрешения вопрос о доказательственной пригодности полученных результатов – о порядке их фиксации, опечатывания носителей и удостоверения процесса, – то есть та проблема легализации, на которую указывает отечественная доктрина. В-третьих, заслуживает внимания последовательное разграничение доступа к хранящимся компьютерным данным и перехвата сообщений, реализованное в японском и корейском законодательстве. Сформулированные ориентиры не предполагают механического заимствования, однако позволяют наметить направление, в котором рамочная конструкция получения компьютерной информации может быть преобразована в действенный правовой институт.

СПИСОК ИСТОЧНИКОВ

1. *Баженов, С. В.* Оперативно-розыскное мероприятие «Получение компьютерной информации» // Научный вестник Омской академии МВД России. 2017. № 2(65). С. 31–34.

2. *Осипенко, А. Л.* Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления // Вестник Воронежского института МВД России. 2016. № 3. С. 83–90. URL: https://cyberleninka.ru/article/n/novoe-operativno-rozysknoe-meropriyatie-poluchenie-kompyuternoy-informatsii-soderzhanie-i-osnovy-osuschestvleniya (дата обращения: 03.06.2026).

3. *Щетнёв, Л. Е., Томилин, С. М.* Оперативно-розыскное мероприятие «получение компьютерной информации»: содержание, структура, технические аспекты проведения // Вестник Владимирского юридического института. 2019. № 4(53). С. 116–119.

4. *Петров, В. В.* Особенности и правовые аспекты проведения оперативно-розыскных мероприятий «снятие информации с технических каналов связи» и «получение компьютерной информации» // Вестник Уфимского юридического института МВД России. 2025. № 1(107). С. 132–145.

5. *Петров, И. В., Фокин, Е. И.* К вопросу о способах реализации оперативно-разыскного мероприятия «получение компьютерной информации» // Военное право. 2019. № 6(58). С. 186–193.

6. *Фойгель, Е. И., Проценко, А. Г.* К вопросу о проблемах практической реализации нового оперативно-розыскного мероприятия «получение компьютерной информации» при раскрытии преступлений в сфере компьютерной информации. С. 73–82.

7. *Епифанов, С. С., Вечкаев, Н. С.* Правовое обеспечение применения цифровых оперативно-розыскных средств при осуществлении оперативно-розыскной деятельности: понятие, состояние и перспективы // Право и государство: теория и практика. 2025. № 5. С. 521–523. DOI: 10.47643/1815-1337_2025_5_521.

8. Yang, F., Feng, J. Rules of electronic data in criminal cases in China // International Journal of Law, Crime and Justice. 2021. Vol. 64. Article 100453. URL: https://www.sciencedirect.com/science/article/abs/pii/S1756061620304882.

9. Guo, Z. Regulating the use of electronic evidence in Chinese courts: legislative efforts, academic debates and practical applications // Computer Law & Security Review. 2022. Vol. 48. Article 105774. DOI: 10.1016/j.clsr.2022.105774.

10. Du, J., Ding, L., Chen, G. Research on the Rules of Electronic Evidence in Chinese Criminal Proceedings // International Journal of Digital Crime and Forensics. 2020. Vol. 12, № 3. P. 111–121. DOI: 10.4018/IJDCF.2020070108.

11. Abraha, H. H. Regulating law enforcement access to electronic evidence across borders: the United States approach // Information & Communications Technology Law. 2020. Vol. 29, iss. 3. P. 324–353. DOI: 10.1080/13600834.2020.1794617.

12. Svantesson, D. J. B., van Zwieten, L. Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution // Computer Law & Security Review. 2016. Vol. 32, iss. 5. P. 671–682. DOI: 10.1016/j.clsr.2016.07.011.

REFERENCES

1. *Bazhenov, S. V.* Operativno-rozysknoe meropriyatie «Poluchenie komp'yuternoj informacii» [The operational-search measure "Obtaining computer information"]. Nauchnyj vestnik Omskoj akademii MVD Rossii – Scientific Bulletin of the Omsk Academy of the MIA of Russia. 2017, no. 2(65), pp. 31–34. (in Russian).

2. *Osipenko, A. L.* Novoe operativno-rozysknoe meropriyatie «poluchenie komp'yuternoj informacii»: soderzhanie i osnovy osushchestvleniya [The new operational-search measure "obtaining computer information": content and bases of implementation]. Vestnik Voronezhskogo instituta MVD Rossii – Bulletin of the Voronezh Institute of the MIA of Russia. 2016, no. 3, pp. 83–90. (in Russian).

3. *Shchetnev, L. E., Tomilin, S. M.* Operativno-rozysknoe meropriyatie «poluchenie komp'yuternoj informacii»: soderzhanie, struktura, tekhnicheskie aspekty provedeniya. Vestnik Vladimirskogo yuridicheskogo instituta. 2019, no. 4(53), pp. 116–119. (in Russian).

4. *Petrov, V. V.* Osobennosti i pravovye aspekty provedeniya operativno-rozysknyh meropriyatij «snyatie informacii s tekhnicheskih kanalov svyazi» i «poluchenie komp'yuternoj informacii». Vestnik Ufimskogo yuridicheskogo instituta MVD Rossii. 2025, no. 1(107), pp. 132–145. (in Russian).

5. *Petrov, I. V., Fokin, E. I.* K voprosu o sposobah realizacii operativno-razysknogo meropriyatiya «poluchenie komp'yuternoj informacii». Voennoe pravo – Military Law. 2019, no. 6(58), pp. 186–193. (in Russian).

6. *Foigel, E. I., Procenko, A. G.* K voprosu o problemah prakticheskoj realizacii novogo operativno-rozysknogo meropriyatiya «poluchenie komp'yuternoj informacii» pri raskrytii prestuplenij v sfere komp'yuternoj informacii. Pp. 73–82. (in Russian).

7. *Epifanov, S. S., Vechkaev, N. S.* Pravovoe obespechenie primeneniya cifrovyh operativno-rozysknyh sredstv pri osushchestvlenii operativno-rozysknoj deyatel'nosti: ponyatie, sostoyanie i perspektivy. Pravo i gosudarstvo: teoriya i praktika. 2025, no. 5, pp. 521–523. (in Russian).

8. *Yang, F., Feng, J.* Rules of electronic data in criminal cases in China. International Journal of Law, Crime and Justice. 2021, vol. 64, article 100453.

9. *Guo, Z.* Regulating the use of electronic evidence in Chinese courts: legislative efforts, academic debates and practical applications. Computer Law & Security Review. 2022, vol. 48, article 105774. (in Russian).

10. *Du, J., Ding, L., Chen, G.* Research on the Rules of Electronic Evidence in Chinese Criminal Proceedings. International Journal of Digital Crime and Forensics. 2020, vol. 12, no. 3, pp. 111–121. (in Russian).

11. *Abraha, H. H.* Regulating law enforcement access to electronic evidence across borders: the United States approach. Information & Communications Technology Law. 2020, vol. 29, iss. 3, pp. 324–353. (in Russian).

12. *Svantesson, D. J. B., van Zwieten, L.* Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution. Computer Law & Security Review. 2016, vol. 32, iss. 5, pp. 671–682.. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Васюков Виталий Федорович, доктор юридических наук, профессор, главный научный сотрудник научно-исследовательского отдела. Московская академия Следственного комитета Российской Федерации имени А. Я. Сухарева. 125080, Российская Федерация, г. Москва, ул. Врубеля, 12.

Дамирчиев Эмин Исахан оглы, кандидат юридических наук, кандидат политических наук, доцент кафедры уголовного права, уголовного процесса и криминалистики. Московский государственный институт международных отношений МИД России (МГИМО). 119454, Российская Федерация, г. Москва, проспект Вернадского, 76б.

INFORMATION ABOUT THE AUTHORS

Vitaly F. Vasyukov, Doctor of Law, Professor, Chief Researcher of the Research Department of the Moscow Academy of the Investigative Committee of the Russian Federation named after A. Ya. Sukharev. 12, Vrubel st., Moscow, Russian Federation, 125080.

Emin Is. oglu Damirchiev, Candidate of Legal Sciences, Candidate of Political Sciences, Associate Professor of the Department of Criminal Law, Criminal Procedure and Forensic Science. Moscow State Institute of International Relations of the Ministry of Foreign Affairs of Russia (MGIMO), 76 b, Vernadsky Avenue, Moscow, Russian Federation, 119454.