МРНТИ 10.85.51 DOI: https://doi.org/10.62687/VLJ.3.2.2026.68

КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ

Е.П. Шульгин*
Карагандинская академия МВД Республики Казахстан им. Б. Бейсенова, Караганда, Республика Казахстан
*e-mail: shulgin_e@internet.ru

Е.П. Шульгин – кандидат юридических наук, ассоциированный профессор (доцент), начальник кафедры кибербезопасности и информационных технологий Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова; Караганда, Республика Казахстан; e-mail: shulgin_e@internet.ru; ORCID ID: https://orcid.org/0000-0003-3478-0052

Аннотация. Статья посвящена криминалистическому обеспечению деятельности органов внутренних дел по противодействию киберпреступности. Актуальность исследования определяется тем, что цифровая среда изменяет механизм следообразования, способы получения криминалистически значимой информации и организацию взаимодействия между оперативными, следственными и криминалистическими подразделениями. Цель исследования состоит в систематизации научно обоснованных направлений криминалистического обеспечения такой деятельности и определении их взаимосвязи. Применены методы анализа, синтеза, сравнительного и системно-структурного исследования, а также научного обобщения. Установлено, что рассматриваемое обеспечение целесообразно выстраивать как взаимосвязанную систему, включающую своевременное выявление и сохранение цифровой информации, методически корректную работу с цифровыми следами, участие компетентных специалистов, стандартизацию криминалистической регистрации, информационное взаимодействие и постоянное обновление профессиональной подготовки. Показано, что изолированное развитие отдельных технических средств не заменяет организационной согласованности этих элементов. Сделан вывод о практической значимости единых требований к компетентности, процедурам фиксации и учету цифровых следов, а также устойчивым каналам межподразделенческого и международного информационного обмена.

Ключевые слова: киберпреступность; органы внутренних дел; цифровые следы; цифровая криминалистика; криминалистическая регистрация; информационное взаимодействие; специальные знания.

ІШКІ ІСТЕР ОРГАНДАРЫНЫҢ КИБЕРҚЫЛМЫСҚА ҚАРСЫ ІС-ҚИМЫЛЫН КРИМИНАЛИСТИКАЛЫҚ ҚАМТАМАСЫЗ ЕТУ

Е.П. Шульгин*
Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясы, Қарағанды, Қазақстан Республикасы
*e-mail: shulgin_e@internet.ru

Е.П. Шульгин – заң ғылымдарының кандидаты, қауымдастырылған профессор (доцент), Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясының киберқауіпсіздік және ақпараттық технологиялар кафедрасының бастығы; Қарағанды, Қазақстан Республикасы; e-mail: shulgin_e@internet.ru; ORCID ID: https://orcid.org/0000-0003-3478-0052

Аңдатпа. Мақала ішкі істер органдарының киберқылмысқа қарсы іс-қимыл жөніндегі қызметін криминалистикалық қамтамасыз ету мәселесіне арналған. Зерттеудің өзектілігі цифрлық ортаның іздердің қалыптасу тетігін, криминалистикалық маңызы бар ақпаратты

алу тәсілдерін және жедел, тергеу мен жедел-криминалистикалық бөлімшелер арасындағы өзара іс-қимылды ұйымдастыруды өзгертуімен айқындалады. Зерттеудің мақсаты -- аталған қызметті криминалистикалық қамтамасыз етудің ғылыми негізделген бағыттарын жүйелеу және олардың өзара байланысын анықтау. Талдау, синтез, салыстырмалы және жүйелік-құрылымдық зерттеу, сондай-ақ ғылыми қорытындылау әдістері қолданылды. Зерттеу нәтижесінде криминалистикалық қамтамасыз етуді цифрлық ақпаратты уақтылы анықтау мен сақтауды, цифрлық іздермен әдістемелік тұрғыдан дұрыс жұмыс істеуді, құзыретті мамандардың қатысуын, криминалистикалық тіркеуді стандарттауды, ақпараттық өзара іс-қимылды және кәсіби даярлықты тұрақты жаңартуды қамтитын өзара байланысты жүйе ретінде құру орынды екені анықталды. Жекелеген техникалық құралдарды оқшау дамыту осы элементтердің ұйымдастырушылық үйлесімділігін алмастырмайтыны көрсетілді. Қорытындыда құзыреттілікке, цифрлық іздерді бекіту мен есепке алу рәсімдеріне бірыңғай талаптар, сондай-ақ бөлімшелер арасындағы және халықаралық ақпарат алмасудың тұрақты арналары практикалық маңызға ие екені негізделді.

Түйін сөздер: киберқылмыс; ішкі істер органдары; цифрлық іздер; цифрлық криминалистика; криминалистикалық тіркеу; ақпараттық өзара іс-қимыл; арнайы білім.

FORENSIC SUPPORT FOR COUNTERING CYBERCRIME BY INTERNAL AFFAIRS BODIES

E.P. Shulgin*
B. Beisenov Karaganda Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan, Karaganda, Republic of Kazakhstan
*e-mail: shulgin_e@internet.ru

E.P. Shulgin – Candidate of Legal Sciences, Associate Professor, Head of the Department of Cybersecurity and Information Technologies at the B. Beisenov Karaganda Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan; Karaganda, Republic of Kazakhstan; e-mail: shulgin_e@internet.ru; ORCID ID: https://orcid.org/0000-0003-3478-0052

Abstract. The article examines forensic support for the activities of internal affairs bodies in countering cybercrime. The relevance of the study stems from the fact that the digital environment changes trace formation mechanisms, the ways in which forensically significant information is obtained, and the organization of cooperation among operational, investigative and forensic units. The purpose of the study is to systematize scientifically grounded areas of forensic support for such activities and to determine their interrelationship. The study uses analysis, synthesis, comparative and system-structural methods, as well as scientific generalization. The results show that forensic support should be organized as an interconnected system comprising timely detection and preservation of digital information, methodologically sound handling of digital traces, participation of competent specialists, standardization of forensic registration, information exchange, and continuous updating of professional training. The analysis demonstrates that isolated development of individual technical tools cannot substitute for organizational consistency among these elements. The article concludes that unified competence requirements, standardized procedures for recording and registering digital traces, and stable channels of inter-unit and international information exchange have practical significance for internal affairs bodies.

Keywords: cybercrime; internal affairs bodies; digital traces; digital forensics; forensic registration; information exchange; specialized knowledge.

Введение. Цифровая трансформация общественных отношений существенно влияет не только на способы совершения преступлений, но и на содержание криминалистической деятельности. Для органов внутренних дел это проявляется прежде всего в том, что значимая для раскрытия и расследования информация все чаще имеет цифровую форму, находится в информационно-телекоммуникационной среде и требует специальных методов обнаружения,

фиксации, сохранения, исследования и последующего использования. При этом само понятие киберпреступности в научной литературе не является терминологически бесспорным. Б.Э. Шавалеев, анализируя понятийный аппарат, указывает на отсутствие полного единства в его применении и связывает классификацию киберпреступлений с функциями информационных технологий в механизме преступления (Шавалеев, 2022: 93–96). Поэтому в настоящей статье термин «киберпреступность» используется как обобщающий для обозначения исследуемой сферы противодействия, а выводы формулируются применительно к тем организационным и криминалистическим проблемам, которые непосредственно подтверждаются рассмотренными научными работами.

Специфика цифровой среды делает особенно значимым информационное обеспечение первоначального этапа расследования. Р.Н. Подольный показывает, что расследование преступлений, совершенных с применением цифровых технологий, требует быстрого получения и закрепления информации, а связь деятельности по выявлению преступления с последующим расследованием имеет самостоятельное криминалистическое значение. Автор особо отмечает роль достоверных данных, в том числе получаемых в результате оперативно-розыскной деятельности, для определения направления и тактики первоначальных действий (Подольный, 2025: 127–133). Этот вывод принципиален для деятельности органов внутренних дел, поскольку позволяет рассматривать выявление, оперативное сопровождение и расследование не как изолированные процессы, а как последовательные элементы единой информационной работы.

Одновременно научные публикации фиксируют несколько взаимосвязанных проблем: методическую сложность работы с цифровыми следами, необходимость специальных знаний, требования к их сохранности и целостности, недостаточную стандартизацию отдельных информационно-учетных процессов, а также потребность в устойчивом взаимодействии между правоохранительными органами и иными участниками информационного обмена. Так, Е.Р. Россинская и Т.А. Сааков связывают собирание цифровых следов из социальных сетей и мессенджеров с необходимостью специальных методологических подходов и участия специалиста (Россинская, Сааков, 2020: 109–121). В.О. Давыдов и И.В. Тишутина акцентируют требования к компетентности специалистов, подготовке кадров и накоплению криминалистически значимой цифровой информации (Давыдов, Тишутина, 2020: 22–27). А.Б. Кокушев обосновывает значение стандартизации учетно-регистрационной деятельности оперативно-криминалистических подразделений МВД Республики Казахстан для упорядочения формирования, обработки и предоставления криминалистически значимой информации (Кокушев, 2023: 233–235).

Вместе с тем перечисленные направления в научной литературе преимущественно исследуются раздельно: одни работы посвящены методике собирания цифровых следов, другие – специальным знаниям, криминалистической регистрации, стандартизации, оперативной деятельности либо международному сотрудничеству, что создает основание для постановки исследовательского вопроса: какие из подтвержденных научными публикациями направлений образуют взаимосвязанную систему криминалистического обеспечения деятельности органов внутренних дел по противодействию киберпреступности и каким образом они должны соотноситься между собой?

Объектом исследования является деятельность органов внутренних дел по противодействию преступлениям, связанным с использованием цифровых технологий. Предмет исследования составляют научно обоснованные организационные и криминалистические положения о выявлении, сохранении, исследовании, регистрации и информационном использовании цифровых следов, применении специальных знаний и организации взаимодействия. Цель статьи состоит в систематизации указанных положений и обосновании их взаимосвязи в рамках единого криминалистического обеспечения. Для достижения цели поставлены задачи: определить значение своевременного получения цифровой информации; раскрыть роль методически корректной фиксации и сохранения цифровых следов; сопоставить позиции о компетентности специалистов;

оценить возможности криминалистической регистрации и стандартизации; установить значение внутриведомственного, межведомственного и международного информационного взаимодействия; сформулировать практические направления, непосредственно вытекающие из рассмотренных научных результатов. Рабочий тезис исследования состоит в том, что результативность криминалистического обеспечения зависит не от наличия отдельного технического решения, а от согласованности информационных, методических, кадровых, учетных и организационных элементов.

Материалы и методы исследования. Материальную основу исследования составили научные публикации. Отбор проводился по содержательному критерию: в исследовательский массив включались работы, непосредственно посвященные киберпреступности, преступлениям с применением цифровых технологий, цифровым следам, цифровой криминалистике, криминалистической регистрации, деятельности оперативных и криминалистических подразделений, а также взаимодействию правоохранительных органов. Для выполнения требования о включении зарубежной англоязычной научной позиции использована работа B. Khamidov, опубликованная на английском языке и посвященная общетеоретическим и методическим вопросам обращения с цифровыми доказательствами (Khamidov, 2021: 8–16).

Исследование не претендует на исчерпывающий библиометрический обзор всех публикаций о киберпреступности. Его границы определены поставленной целью: выявить устойчиво повторяющиеся и взаимодополняющие положения, имеющие непосредственное значение для криминалистического обеспечения органов внутренних дел. В связи с этим из анализа исключались статистические сведения, если для целей статьи не требовалось их воспроизведение, а также практические утверждения, которые не могли быть проверены по использованным научным работам. Такой подход позволяет отделить собственно результат систематизации научных положений от оценок, не обеспеченных источниковой базой.

Методологическую основу составили анализ и синтез, сравнительный и системно-структурный методы, а также научное обобщение. На первом этапе были выделены положения о цифровом следообразовании, своевременности выявления информации и ее сохранении. На втором этапе сопоставлены исследования об участии специалиста и требованиях к профессиональной компетентности. На третьем этапе проанализированы научные предложения по криминалистической регистрации цифровых следов и стандартизации учетно-регистрационной деятельности. На четвертом этапе рассмотрены работы о координации, информационном обмене и международном сотрудничестве. Итоговым этапом стало системно-структурное сопоставление этих блоков и формулирование выводов о характере их взаимосвязи.

Научная новизна исследования ограничивается именно систематизирующим результатом: отдельные элементы криминалистического обеспечения ранее исследованы соответствующими авторами самостоятельно, тогда как в настоящей статье они сопоставлены как взаимозависимые направления деятельности органов внутренних дел, что не означает приписывания источникам выводов, которых в них нет. Предлагаемая система является результатом научного обобщения подтвержденных положений и потому далее разграничивается с конкретными авторскими предложениями, содержащимися в рассмотренных публикациях.

Результаты исследования и их обсуждение. Первым системообразующим элементом выступает своевременное получение криминалистически значимой информации и обеспечение преемственности между выявлением преступления и его расследованием. Р.Н. Подольный обращает внимание на временную чувствительность цифровых следов и на необходимость уже на начальном этапе располагать достаточным объемом достоверной информации для определения направления дальнейшей деятельности. В его исследовании выявление рассматривается как информационная основа расследования, а взаимодействие следователя с органами, осуществляющими оперативно-розыскную деятельность, сохраняет значение и на последующих этапах (Подольный, 2025: 130–135). Следовательно, применительно

к органам внутренних дел криминалистическое обеспечение должно начинаться не с момента назначения исследования цифрового устройства, а раньше – с организационно и методически выстроенного получения, закрепления и передачи информации между субъектами, участвующими в выявлении и расследовании.

Такой подход согласуется с исследованиями цифровых следов в оперативной деятельности. С.В. Тимофеев и Р.Х. Кочесоков рассматривают цифровые следы как значимый инструмент деятельности оперативных подразделений, одновременно отмечая проблемы отсутствия стандартизированных подходов к обработке данных, вопросы конфиденциальности и необходимость совершенствования взаимодействия (Тимофеев, Кочесоков, 2024: 262–276). Сопоставление этой позиции с выводами Р.Н. Подольного показывает, что информационная преемственность должна обеспечивать два условия: данные должны быть получены своевременно и в таком виде, который позволяет в дальнейшем корректно использовать их при решении следственных, оперативных и криминалистических задач. В противном случае технически обнаруженная информация может не реализовать своего криминалистического потенциала.

Вторым элементом является методически корректная работа с цифровыми следами. Е.Р. Россинская и Т.А. Сааков на материале социальных сетей и мессенджеров исследуют подходы к обнаружению, фиксации и изъятию цифровых следов и специально выделяют роль специалиста в действиях, связанных с собиранием цифровой информации (Россинская, Сааков, 2020: 109–121). Для рассматриваемой темы существенен не конкретный вид цифрового сервиса, а более общий вывод: цифровая информация требует соблюдения особых методических условий, поскольку ее получение связано с технической средой, способом доступа и необходимостью достоверной фиксации результата.

Работа B. Khamidov дополняет этот вывод требованиями к обращению с цифровыми доказательствами. Автор рассматривает вопросы их сбора, хранения, проверки, транспортировки и оценки, уделяя внимание целостности цифровых данных, их идентификации и аутентификации; в числе технических средств проверки целостности анализируется применение хэш-функций (Khamidov, 2021: 11–14). Для органов внутренних дел данная позиция важна как подтверждение того, что работа с цифровой информацией не исчерпывается ее копированием либо визуальной фиксацией. Методическое обеспечение должно позволять подтвердить, что исследуемые данные соотносятся с первоначально полученной информацией и не утратили значимых свойств в ходе последующих действий. При этом конкретный набор технических процедур зависит от объекта и задачи, поэтому научно обоснованным является требование к проверяемости целостности и происхождения данных, а не универсализация одной технической операции для всех ситуаций.

Третий элемент связан со специальными знаниями и профессиональной компетентностью. В.О. Давыдов и И.В. Тишутина показывают, что цифровые следы изменяют требования к компетенции судебных экспертов и специалистов-криминалистов. Авторы связывают решение выявленных проблем с подготовкой и переподготовкой кадров, стандартизацией квалификации и накоплением криминалистически значимой информации (Давыдов, Тишутина, 2020: 22–27). Д.Д. Архипов, Ю.Ю. Гарцева и В.Ю. Миллер также рассматривают нехватку специалистов и экспертов как одну из проблем применения цифровой криминалистики (Архипов и др., 2024: 158–163). Эти исследования позволяют сделать вывод, что участие специалиста должно оцениваться не формально, по самому факту его привлечения, а через соответствие знаний и навыков конкретной цифровой задаче.

Из этого следует практический принцип дифференцированной компетентности. Для одних действий сотруднику достаточно базовой подготовки по обнаружению и первоначальной фиксации цифровой информации; для других требуется участие специалиста, обладающего специальными знаниями и средствами исследования. Научные источники не дают оснований устанавливать универсальный перечень должностей или единый количественный норматив кадрового обеспечения для всех подразделений. Однако они подтверждают необходимость стандартизировать требования к компетентности и систематически обновлять подготовку с

учетом изменения цифровых технологий (Давыдов, Тишутина, 2020: 24–27; Кокушев, 2023: 233–235). Поэтому обоснованным направлением является не произвольное увеличение числа технических специалистов, а организационное закрепление проверяемых квалификационных требований применительно к выполняемым функциям.

Четвертым элементом выступает криминалистическая регистрация цифровых следов. Н.И. Валькирия рассматривает цифровые следы как источник криминалистически значимой информации об устанавливаемом лице и связывает дальнейшее повышение возможностей их использования с развитием криминалистических учетов и поисковых инструментов (Валькирия, 2023: 61–64). А.А. Курин и В.А. Гаужаева анализируют возможность специализированного учета электронно-цифровых следов и предлагают использовать метапоисковый подход к обработке данных из разнородных, но логически связанных источников. Авторы подчеркивают, что смысл формирования новых информационных массивов заключается в получении достоверной и актуальной информации, необходимой для принятия процессуальных, тактических и организационных решений (Курин, Гаужаева, 2023: 143–146).

Принципиальное значение этих работ состоит в переходе от эпизодического использования цифрового следа в рамках отдельного материала к его возможному информационно-поисковому значению. Вместе с тем такое направление требует осторожного организационного оформления. Сам факт технической возможности накапливать цифровые сведения не является достаточным основанием для расширения массивов данных. Научно подтвержденными условиями являются целевая криминалистическая значимость информации, ее достоверность, актуальность и возможность системного поиска. Вопросы конфиденциальности и правовых ограничений при работе с цифровыми следами отдельно отмечаются в исследовании С.В. Тимофеева и Р.Х. Кочесокова (Тимофеев, Кочесоков, 2024: 262–264). Следовательно, учетный компонент должен развиваться одновременно с требованиями к качеству данных и режиму их правомерного использования.

Для органов внутренних дел Республики Казахстан непосредственное значение имеет исследование А.Б. Кокушева. Автор анализирует учетно-регистрационную деятельность оперативно-криминалистических подразделений МВД Республики Казахстан и рассматривает стандартизацию как средство упорядочивания процессов формирования, кодирования, систематизации и предоставления криминалистически значимой информации. В числе элементов стандартизации им рассматриваются единообразие организационно-методической работы, технического обеспечения и подготовки специалистов (Кокушев, 2023: 233–235), что позволяет уточнить содержание учетного элемента: криминалистическая регистрация цифровой информации должна быть не только технически доступной, но и организационно сопоставимой между подразделениями, иначе единый информационный массив не гарантирует единообразного качества включаемых в него сведений.

Пятым элементом является информационное взаимодействие. Ю.Г. Наумов, П.В. Самолысов и Е.А. Тришкина, рассматривая инструменты противодействия киберпреступности, делают акцент на необходимости комплексного подхода и сотрудничества между правоохранительными органами, государственными структурами, частным сектором и международными партнерами (Наумов и др., 2024: 59–64). Для криминалистического обеспечения этот вывод имеет прикладной смысл: значимая информация может находиться за пределами подразделения, непосредственно ведущего проверку или расследование, а потому качество противодействия зависит от способности своевременно инициировать и поддерживать обмен данными в пределах предусмотренной компетенции.

Внутри системы органов внутренних дел такое взаимодействие должно обеспечивать прежде всего непрерывность движения информации между оперативными, следственными и криминалистическими направлениями. Данный вывод не требует создания новой организационной структуры: он вытекает из уже рассмотренной взаимозависимости выявления, исследования и криминалистической регистрации. Оперативно полученные сведения определяют направления поиска и первоначальных действий; корректно

зафиксированные цифровые следы становятся объектом дальнейшего исследования; результаты исследования при наличии соответствующих оснований могут приобретать информационно-поисковое значение; сведения из учетов, в свою очередь, способны ориентировать дальнейшую оперативную и следственную работу. Так формируется не линейная передача документа, а повторяющийся информационный обмен между функционально различными участниками.

Особое место занимает международное сотрудничество. А.Г. Кузнецов обосновывает необходимость усиления взаимодействия органов внутренних дел (полиции) государств – участников СНГ в сфере предотвращения и раскрытия киберпреступлений и связывает развитие такого сотрудничества с общими стандартами и устойчивыми механизмами информационного обмена (Кузнецов, 2023: 131–135). Для настоящего исследования важно ограничить вывод пределами источника: речь идет не о том, что любой факт киберпреступности автоматически требует международного механизма, а о том, что трансграничный характер отдельных цифровых данных объективно делает международный информационный канал самостоятельным элементом организационного обеспечения в тех случаях, когда сведения или соответствующие субъекты находятся в разных юрисдикциях.

Шестым элементом является постоянное методическое и образовательное обновление. Этот элемент напрямую связан с компетентностью, но имеет самостоятельное организационное значение. В.О. Давыдов и И.В. Тишутина связывают эффективное использование цифровых следов с образовательными программами, повышением квалификации и накоплением информации (Давыдов, Тишутина, 2020: 23–27). Д.Д. Архипов, Ю.Ю. Гарцева и В.Ю. Миллер указывают на кадровую проблему цифровой криминалистики (Архипов и др., 2024: 158–163), а А.Б. Кокушев включает унификацию подготовки специалистов в содержание стандартизации учетно-регистрационной деятельности (Кокушев, 2023: 233–235). Следовательно, профессиональная подготовка должна быть встроена в систему криминалистического обеспечения как постоянный механизм актуализации практики, а не как разовое освоение конкретного программного продукта.

Сопоставление рассмотренных работ позволяет сформулировать основной результат исследования. Криминалистическое обеспечение противодействия киберпреступности органами внутренних дел целесообразно представлять как систему шести взаимосвязанных направлений:

1. своевременное выявление и информационная преемственность между оперативной и следственной деятельностью;
2. методически корректное обнаружение, фиксация, сохранение и проверка целостности цифровой информации;
3. участие специалистов с компетентностью, соответствующей конкретной задаче;
4. стандартизированная криминалистическая регистрация и аналитический поиск по достоверным и актуальным данным;
5. внутриведомственное, межведомственное и при необходимости международное информационное взаимодействие;
6. постоянное обновление профессиональной подготовки и методических рекомендаций.

Каждый из этих элементов подтверждается самостоятельным массивом научных публикаций, а системный результат состоит в установлении их функциональной взаимозависимости.

Взаимозависимость проявляется следующим образом. Своевременное выявление без корректного сохранения цифровых данных создает риск утраты их последующей информационной ценности. Технически безупречное копирование данных без компетентного определения объекта и задачи не обеспечивает их содержательной интерпретации. Исследование без надлежащей передачи результатов в информационную систему ограничивает повторное использование выявленных закономерностей. Криминалистический учет без стандартизации требований к исходным данным может накапливать неоднородную

информацию. Информационный обмен без единых методических ориентиров не устраняет различий в качестве получаемых сведений. Наконец, все перечисленные элементы зависят от профессиональной подготовки сотрудников, поскольку цифровые технологии и способы работы с ними изменяются. Эти связи выводятся из сопоставления позиций Р.Н. Подольного, Е.Р. Россинской и Т.А. Саакова, В.О. Давыдова и И.В. Тишутиной, А.Б. Кокушева, А.А. Курина и В.А. Гаужаевой (Подольный, 2025: 130–135; Россинская, Сааков, 2020: 109–121; Давыдов, Тишутина, 2020: 22–27; Кокушев, 2023: 233–235; Курин, Гаужаева, 2023: 143–146).

Системное понимание позволяет также разграничить технологическое и криминалистическое обеспечение. Использование современного программного или аппаратного средства относится к технологии выполнения конкретной задачи. Криминалистическое обеспечение шире: оно должно отвечать на вопросы о том, кто и при каких условиях работает с цифровой информацией, каким образом подтверждается ее сохранность, где и в каком стандартизированном виде фиксируется результат, кому он передается и как полученная информация может быть использована в дальнейшем. Именно поэтому наличие цифровых инструментов само по себе не устраняет кадровых, методических, учетных и организационных проблем, на которые указывают рассмотренные авторы (Архипов и др., 2024: 158–163; Тимофеев, Кочесоков, 2024: 262–276).

В практическом плане из проведенного анализа вытекают несколько направлений, не выходящих за пределы подтвержденной источниками аргументации. Во-первых, при разработке ведомственных методических материалов целесообразно обеспечивать преемственность между действиями по первоначальному выявлению цифровой информации и ее последующим исследованием, поскольку информационный разрыв на раннем этапе снижает возможность рационального планирования дальнейших действий (Подольный, 2025: 130–135). Во-вторых, требования к привлечению специалиста следует связывать с фактической сложностью цифровой задачи и проверяемой компетентностью лица, а подготовку – с постоянным обновлением знаний (Давыдов, Тишутина, 2020: 24–27; Архипов и др., 2024: 158–163).

В-третьих, развитие криминалистических учетов цифровых следов целесообразно сопрягать со стандартизацией качества исходных данных и поисковых процедур. Предложения Н.И. Валькирии о развитии криминалистической регистрации и А.А. Курина, В.А. Гаужаевой о специализированном учете и метапоиске приобретают практическую устойчивость именно при учете подхода А.Б. Кокушева к единообразию организационных, технических и кадровых условий учетно-регистрационной деятельности (Валькирия, 2023: 61–64; Курин, Гаужаева, 2023: 143–146; Кокушев, 2023: 233–235). Иными словами, развитие учета цифровых следов должно происходить одновременно по содержательному и организационному направлениям: определяется, какие сведения имеют криминалистическое значение, и устанавливается, каким образом обеспечивается сопоставимое качество их формирования и использования.

В-четвертых, информационное взаимодействие должно рассматриваться как часть криминалистического обеспечения, а не только как внешний административный процесс. Научные выводы о комплексном сотрудничестве правоохранительных органов, государственных структур, частного сектора и международных партнеров указывают на необходимость заранее определенных каналов и правил обмена в пределах соответствующей компетенции (Наумов и др., 2024: 59–64). Для трансграничных ситуаций данный вывод дополняется положениями А.Г. Кузнецова о развитии международного взаимодействия полиции и общих стандартов сотрудничества в борьбе с киберпреступностью (Кузнецов, 2023: 131–135).

Наконец, в систему оценки качества криминалистического обеспечения следует включать не только наличие технических средств, но и организационные признаки: своевременность передачи информации, соответствие компетентности сотрудника задаче, соблюдение методики фиксации и сохранения цифровых следов, единообразие учетных процедур и возможность последующего поиска релевантной информации. В рассмотренных источниках нет единой универсальной системы количественных показателей, поэтому

настоящая статья не предлагает искусственных нормативов. Однако качественные критерии прямо вытекают из проанализированных работ и могут служить основанием для дальнейшей эмпирической проверки в конкретных подразделениях органов внутренних дел.

Заключение. Проведенное исследование позволило систематизировать научные положения о криминалистическом обеспечении деятельности органов внутренних дел по противодействию киберпреступности без обращения к неподтвержденным статистическим данным и без экстраполяции выводов за пределы использованных публикаций.

Основной результат состоит в обосновании взаимосвязи шести направлений: своевременного выявления и информационной преемственности; методически корректной работы с цифровыми следами и обеспечения проверяемости их целостности; участия компетентных специалистов; стандартизированной криминалистической регистрации; внутриведомственного, межведомственного и международного информационного взаимодействия; постоянного обновления профессиональной подготовки. Научные работы, посвященные каждому из этих направлений, показывают, что цифровая криминалистика не может быть сведена к применению отдельного программного продукта или технического устройства. Ее организационная эффективность зависит от того, насколько согласованы действия субъектов, методические процедуры и информационные массивы.

Для деятельности органов внутренних дел практическое значение имеют следующие выводы. Требования к работе с цифровыми следами должны обеспечивать не только возможность извлечения информации, но и ее достоверную фиксацию, сохранность и последующую проверяемость. Участие специалиста должно основываться на соответствующей задаче компетентности, а подготовка кадров – регулярно обновляться. Развитие криминалистической регистрации цифровых следов требует стандартизации качества исходной информации, порядка ее систематизации и поиска. Информационный обмен между оперативными, следственными и криминалистическими подразделениями должен сохранять преемственность от стадии выявления до использования результатов исследования и учета. В случаях, имеющих трансграничный информационный компонент, самостоятельное значение приобретает международное сотрудничество.

Перспективой дальнейшего исследования является эмпирическая проверка предложенной систематизации на материалах конкретных подразделений органов внутренних дел. Научно значимыми представляются разработка проверяемых критериев компетентности для различных видов работы с цифровой информацией, изучение качества и совместимости учетно-регистрационных процессов, а также оценка того, какие организационные формы взаимодействия обеспечивают наименьшие потери значимой информации между выявлением, расследованием и исследованием. Такие исследования требуют самостоятельной эмпирической базы; поэтому количественные показатели и выводы об их фактической результативности в настоящей статье намеренно не формулируются.

Литература

Архипов, Гарцева, Миллер, 2024 — Архипов Д.Д., Гарцева Ю.Ю., Миллер В.Ю. К вопросу применения цифровой криминалистики в современных условиях // Азиатско-Тихоокеанский регион: экономика, политика, право. — 2024. — Т. 26. — № 3. — С. 158–168. [Russ.]

Валькирия, 2023 — Валькирия Н.И. Использование цифровых следов в деятельности по установлению лица, совершившего преступление // Криминалистика: вчера, сегодня, завтра. — 2023. — Т. 28. — № 4. — С. 56–66. [Russ.]

Давыдов, Тишутина, 2020 — Давыдов В.О., Тишутина И.В. Цифровые следы в расследовании дистанционного мошенничества // Известия Тульского государственного университета. Экономические и юридические науки. — 2020. — № 3. — С. 20–27. [Russ.]

Кокушев, 2023 — Кокушев А.Б. Стандартизация учетно-регистрационной деятельности оперативно-криминалистических подразделений МВД Республики Казахстан как инструмент повышения эффективности информационного обеспечения // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. — 2023. — № 1 (94). — С. 229–236. [Russ.]

Кузнецов, 2023 — Кузнецов А.Г. Международное сотрудничество в борьбе с киберпреступностью // Научный портал МВД России. — 2023. — № 1 (61). — С. 131–136. [Russ.]

Курин, Гаужаева, 2023 — Курин А.А., Гаужаева В.А. Электронно-цифровые следы как объекты криминалистической регистрации // Право и управление. — 2023. — № 7. — С. 141–147. [Russ.]

Наумов, Самолысов, Тришкина, 2024 — Наумов Ю.Г., Самолысов П.В., Тришкина Е.А. Правовые и экономические инструменты противодействия киберпреступности в Российской Федерации // Труды Академии управления МВД России. — 2024. — № 3 (71). — С. 58–65. [Russ.]

Подольный, 2025 — Подольный Р.Н. Выявление как система действий, формирующих информационную основу расследования

преступлений, совершенных с применением цифровых технологий // Известия высших учебных заведений. Поволжский регион. Общественные науки. — 2025. — № 2. — С. 127–137. [Russ.]
Россинская, Сааков, 2020 — Россинская Е.Р., Сааков Т.А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. — 2020. — № 3 (15). — С. 106–123. [Russ.]
Тимофеев, Кочесоков, 2024 — Тимофеев С.В., Кочесоков Р.Х. Перспективы совершенствования российского законодательства в области использования цифровых следов преступления // Вестник Восточно-Сибирского института МВД России. — 2024. — № 4 (111). — С. 262–277. [Russ.]
Шавалеев, 2022 — Шавалеев Б.Э. Классификация киберпреступлений // Вестник Казанского юридического института МВД России. — 2022. — Т. 13. — № 3 (49). — С. 93–97. [Russ.]
Khamidov, 2021 — Khamidov B. General-theoretical issues related to digital evidence: problem and solution // Norwegian Journal of Development of the International Science. — 2021. — No. 63-2. — P. 8–16. [Eng.]

References

Arkhipov, Gartseva, Miller, 2024 — Arkhipov D.D., Gartseva Yu.Yu., Miller V.Yu. K voprosu primeneniya tsifrovoi kriminalistiki v sovremennykh usloviyakh [On the issue of application of digital forensics in modern conditions] // Aziatsko-Tikhookeanskii region: ekonomika, politika, pravo. — 2024. — Vol. 26. — No. 3. — P. 158–168. [in Russ.]
Davydov, Tishutina, 2020 — Davydov V.O., Tishutina I.V. Tsifrovye sledy v rassledovanii distantsionnogo moshennichestva [Digital traces in remote fraud investigations] // Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki. — 2020. — No. 3. — P. 20–27. [in Russ.]
Khamidov, 2021 — Khamidov B. General-theoretical issues related to digital evidence: problem and solution // Norwegian Journal of Development of the International Science. — 2021. — No. 63-2. — P. 8–16. [in Eng.]
Kokushev, 2023 — Kokushev A.B. Standartizatsiya uchetno-registratsionnoi deyatel'nosti operativno-kriminalisticheskikh podrazdelenii MVD Respubliki Kazakhstan kak instrument povysheniya effektivnosti informatsionnogo obespecheniya [Standardization of accounting and registration activities of operational forensic units of the Ministry of Internal Affairs of the Republic of Kazakhstan as a tool for improving the efficiency of information support] // Nauchnyi vestnik Orlovskogo yuridicheskogo instituta MVD Rossii imeni V.V. Luk'yanova. — 2023. — No. 1 (94). — P. 229–236. [in Russ.]
Kurin, Gauzhaeva, 2023 — Kurin A.A., Gauzhaeva V.A. Elektronno-tsifrovye sledy kak ob"ekty kriminalisticheskoi registratsii [Electronic-digital traces as objects of forensic registration] // Pravo i upravlenie. — 2023. — No. 7. — P. 141–147. [in Russ.]
Kuznetsov, 2023 — Kuznetsov A.G. Mezhdunarodnoe sotrudnichestvo v bor'be s kiberprestupnost'yu [International cooperation in the fight against cybercrime] // Nauchnyi portal MVD Rossii. — 2023. — No. 1 (61). — P. 131–136. [in Russ.]
Naumov, Samolysov, Trishkina, 2024 — Naumov Yu.G., Samolysov P.V., Trishkina E.A. Pravovye i ekonomicheskie instrumenty protivodeistviya kiberprestupnosti v Rossiiskoi Federatsii [Legal and economic instruments for countering cybercrime in the Russian Federation] // Trudy Akademii upravleniya MVD Rossii. — 2024. — No. 3 (71). — P. 58–65. [in Russ.]
Podolnyy, 2025 — Podolnyy R.N. Vyyavlenie kak sistema deistvii, formiruyushchikh informatsionnuyu osnovu rassledovaniya prestuplenii, sovershennykh s primeneniem tsifrovykh tekhnologii [Identification as a system of actions that form the information basis for the investigation of crimes committed using digital technologies] // Izvestiya vysshikh uchebnykh zavedenii. Povolzhskii region. Obshchestvennye nauki. — 2025. — No. 2. — P. 127–137. [in Russ.]
Rossinskaya, Saakov, 2020 — Rossinskaya E.R., Saakov T.A. Problemy sobiraniya tsifrovykh sledov prestuplenii iz sotsial'nykh setei i messendzherov [Problems of collecting digital traces of crimes from social networks and messengers] // Kriminalistika: vchera, segodnya, zavtra. — 2020. — No. 3 (15). — P. 106–123. [in Russ.]
Shavaleyev, 2022 — Shavaleyev B.E. Klassifikatsiya kiberprestuplenii [Classification of cybercrimes] // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. — 2022. — Vol. 13. — No. 3 (49). — P. 93–97. [in Russ.]
Timofeev, Kochesokov, 2024 — Timofeev S.V., Kochesokov R.Kh. Perspektivy sovershenstvovaniya rossiiskogo zakonodatel'stva v oblasti ispol'zovaniya tsifrovykh sledov prestupleniya [Prospects for improving Russian legislation in the field of using digital traces of crime] // Vestnik Vostochno-Sibirskogo instituta MVD Rossii. — 2024. — No. 4 (111). — P. 262–277. [in Russ.]
Valkiriya, 2023 — Valkiriya N.I. Ispol'zovanie tsifrovykh sledov v deyatel'nosti po ustanovleniyu litsa, sovershivshego prestuplenie [Use of digital traces in the activity of identification of the person who committed the crime] // Kriminalistika: vchera, segodnya, zavtra. — 2023. — Vol. 28. — No. 4. — P. 56–66. [in Russ.]