Научная статья
УДК 343.101
DOI: 10.47475/2311-696X-2024-41-2-48-54

IT-СЛЕДОВАТЕЛЬ В ЦИФРОВОЙ СРЕДЕ УГОЛОВНОГО СУДОПРОИЗВОДСТВА

Сергей Васильевич Зуев[1], **Анатолий Игоревич Зазулин**[2]
[1] *Южно-Уральский государственный университет (НИУ), Челябинск, Россия*
zuevsergej@inbox.ru
[2] *Юридическая фирма «ИНТЕЛЛЕКТ», Екатеринбург, Россия*
a.zazulin@intellect.law

Аннотация. Данная работа посвящена вопросам расследования преступлений, отличающихся сложностью и широким применением цифровых технологий. Авторы утверждают, что уголовное судопроизводство в настоящее время нуждается в модернизации за счет привлечения технологий, а также в обеспечении высококвалифицированными следователями, способными использовать знания межотраслевых наук для решения техногенных задач уголовного процесса.

Многие преступления совершаются с использованием современных технологий. При этом преступления становятся все более изощренными, технологичными. Расследование их могут осуществлять IT-следователи. Представляется, что уровень компетенции последних может определяться категорией преступлений, определяемой по способу совершения преступлений. Высококвалифицированные следователи должны также заниматься расследованием преступлений, связанных с цифровыми финансовыми активами и цифровой валютой.

Авторами обосновывается, что IT-следователь должен уметь работать с большими данными, читать экспертные заключения по результатам проведения компьютерно-технических экспертиз любой сложности, широко применять электронные документы, в перспективе использовать электронного помощника. Цифровая видеотека, аудиозаписи и фотографии могут накапливаться в облачных пространствах, относительно которых на сегодня имеются различные предложения по применению программного обеспечения, моделированию, алгоритмизации процессов.

Ключевые слова: следователь, расследование, уголовное дело, информационные технологии, уголовное дело

Для цитирования: Зуев С. В., Зазулин А. И. IT-следователь в цифровой среде уголовного судопроизводства // Правопорядок: история, теория, практика. 2024. № 2 (41). С. 48–54. DOI: 10.47475/2311-696X-2024-41-2-48-54

Research article

IT-INVESTIGATOR IN THE DIGITAL ENVIRONMENT OF CRIMINAL PROCEEDINGS

Sergey V. Zuev[1], **Anatoly I. Zazulin**[2]
[1] *South Ural State University (NRU), Chelyabinsk, Russia*
zuevsergej@inbox.ru
[2] *INTELLECT Law Firm, Yekaterinburg, Russia*
a.zazulin@intellect.law

Abstract. This paper is devoted to the issues of investigation of crimes characterized by complexity and extensive use of digital technologies. The authors argue that criminal proceedings nowadays need modernization through the involvement of technology, as well as the provision of highly qualified investigators who are able to use the knowledge of interdisciplinary sciences to solve technogenic problems of criminal proceedings.

Many crimes are committed with the use of modern technologies. At the same time, crimes are becoming more and more sophisticated and technological. They can be investigated by IT-investigators. It seems that the level of competence of the latter can be determined by the category of crimes, defined by the method of committing crimes. Highly qualified investigators should also investigate crimes related to digital financial assets and digital currency.

The authors substantiate that an IT investigator should be able to work with big data, read expert opinions on the results of computer-technical examinations of any complexity, widely use electronic documents, and in the future use an electronic assistant. Digital video library, audio recordings and photos can be accumulated in cloud spaces, regarding which today there are various proposals for the application of software, modeling, algorithmization of processes.

Keywords: investigator, investigation, criminal case, information technology, criminal case

For citation: Zuev SV, Zazulin AI. IT-investigator in the digital environment of criminal proceedings. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2024;(2):48-54. DOI: 10.47475/2311-696X-2024-41-2-48-54 (In Russ.)

Введение

В настоящее время наблюдается все больший разрыв между знающими людьми и теми, кто существенно отстает от первых. Развитие науки и техники делает одних увлеченными в поисках новых знаний, других — довольствующимися малым, достаточным и простым. Сложные технологии пугают и отталкивают последних, однако кого-то они увлекают поисками истины в хорошо запутанных лабиринтах правды.

Описание проводимого исследования

Информационные технологии обретают цифровую среду и вместе с этим требуют правового регулирования осуществления деятельности в новых условиях. Уголовное судопроизводство нуждается в модернизации за счет привлечения технологий, а также в обеспечении высококвалифицированными следователями, способными использовать знания межотраслевых наук для решения техногенных задач уголовного процесса.

Прежде всего, это касается следователей, от которых зависит результат расследования преступлений и окончательный итог досудебного производства по уголовным делам. Существующая специализация следователей происходит с учетом подследственности без учета особенностей расследования отдельных видов преступлений, сложности в установлении некоторых обстоятельств преступлений. Известные критерии (правила) не позволяют выделить спектр преступлений, расследование по которым требует применения соответствующих информационных технологий. Последние являются неким ответом на изощренность, высокотехнологичность самих преступлений.

Результаты проводимого исследования, обсуждение

Многие преступления совершаются с использованием современных технологий. При этом преступления становятся все более изощренными, технологичными. Расследование их могут осуществлять IT-следователи. Представляется, что уровень компетенции последних будет определяться, прежде всего, категорией преступлений, по которым предстоит проводить расследование. Возможно, что речь идет о новой подследственности, определяемой по способу совершения преступлений.

Представляется, что такими способами совершения преступлений могут быть, например, использование сетевых атак, использование вредоносного ПО, использование незаконно полученных идентификаторов (логин, пароль, PIN-код, и др.) и другой конфиденциальной информации, использование уязвимостей в программном обеспечении локального или удаленного устройства, аудиоперехват, электромагнитный перехват и т. п.

Так, преступления могут совершаться с использованием «бот-сети». Бот-сети — это сети взаимосвязанных компьютеров с удаленным управлением, как правило, зараженных вредоносными программами, которые преобразуют зараженную систему в так называемые «боты», «роботы» или «зомби». Пользователь сети Интернет не подозревает о заражении его устройства. Тем временем бот-сети устанавливают устойчивое соединение с компьютером злоумышленника («сервером управления и контроля») или другими ботами для получения инструкций, загрузки дополнительного программного обеспечения и передачи информации, собранной в зараженной системе. Бот-сети в таких деяниях будут являться орудием преступления, посредством которого осуществляются DDoS-атаки, хищение данных личного характера, незаконный доступ, перехват или получение цифровой информации, хостинг вредоносных сайтов и доставка «полезной нагрузки» других вредоносных программ, рассылка спама, что может рассматриваться как незаконный доступ к компьютерной информации, создание, использование и распространение вредоносных компьютерных программ. Кроме того, бот-сети могут использоваться в целях незаконного получения прибыли, например, при мошенничестве [8, с. 55].

Схожим является способ рассылки электронных писем, иных сообщений с вредоносными вложениями от той или иной организации или лица. Порой письмо, иное сообщение содержит эксплойт[1] (подвид вредоносной программы, который содержит данные или исполняемый код, использующий уязвимости в программном обеспечении на локальном или удаленном компьютере[2]) или сразу вредоносную программу.

С помощью удаленного управления или автоматических переводов через системы бухгалтерского учета 1С может происходить хищения средств со счетов юридических лиц.

Распространенным способом хищений является веб-фишинг[3] — атаки, основанные на массовой рассылке сообщений. Причем, для повышения таких атак могут использоваться домашние роутеры, перенаправляющие пользователей на соответствующие сайты.

[1] Эксплойт — от англ. exploit — использовать.

[2] Что такое эксплойты и почему их все так боятся? // Блог Касперского. URL: https://www.kaspersky.ru/blog/exploits-problem-explanation/8459/ (дата обращения: 25.02.2024).

[3] Веб-фишинг — вид мошенничества в сети Интернет, построенный на принципах социальной инженерии, посредством реализации которого злоумышленники получают доступ к конфиденциальным данным и личной информации пользователей.

Не стоит также недооценивать возможную пользу от IT-следователей в борьбе с организованной преступностью, которая в последнее время все больше переходит на «цифровые рельсы». Преступники организовывают свою деятельность посредством использования Даркнета, специальных или обычных мессенджеров и цифровых устройств. Один из таких примеров — полукриминальная сеть Encrochat. Компания с одноименным названием гарантировала своим пользователям полную конфиденциальность, продавая модифицированные смартфоны без USB-портов и прочих модулей аппаратной связи с собственной операционной системой. Связь между телефонами осуществлялась с помощью нескольких уровней шифрования через собственные серверы компании. Таким образом, «Encrochat» обеспечивала обособленный и зашифрованный от остального интернета трафик, использовавшийся преступниками для координации своей деятельности. Хотя сеть Encrochat не была полностью изолирована от интернета, но фактически ее инфраструктура не позволяла установить точное местонахождение мобильных устройств пользователей. Взлом и последующее раскрытие криминальной сети Европолом стали возможны только после установления местонахождения выделенных серверов компании во Франции [11, с. 452].

Если в ходе расследования преступлений появляются данные, указывающие на то, что преступная группа использует для организации своей деятельности цифровые технологии, то к расследованию должен подключаться IT-следователь — например, посредством участия в составе следственной группы (ст. 163 УПК РФ).

IT-следователь должен также заниматься расследованием преступлений, связанных с цифровыми финансовыми активами и цифровой валютой. Сложности в расследовании таких преступлений очевидны. Следователю требуются знания в экономике и цифровых технологиях в этой сфере.

Особенности расследования такого рода преступлений раскрываются через задачи с учетом требований уголовно-процессуального закона и существующих методик расследования.

Основной задачей предварительного расследования как стадии уголовного процесса является раскрытие преступления. Законодатель не определяет понятия «раскрытие преступления». В Уголовно-процессуальном кодексе Российской Федерации (далее — УПК РФ) такое словосочетание встречается в статье 317.1 применительно к вопросу о заключении досудебного соглашения о сотрудничестве. То, что раскрытие преступлений является задачей досудебного производства не вызывает никаких сомнений. В теории оперативно-розыскной деятельности отношение к данному понятию неоднозначно.

Раскрытие преступлений понимается как задержание лица, совершившего преступление, с поличным; установление лица, его совершившего, изобличение, доставление к следователю; факт подтверждения виновности лица в совершении преступления, который отражается в предъявлении ему обвинения следователем; обеспечение доказательственной базой в виновности всех участников преступления, которое достигается к концу расследования, когда следователь направляет уголовное дело в суд; привлечение виновных лиц к уголовной ответственности, которое выражается в обвинительном приговоре [4, с. 13].

В любом случае просматривается обеспечительная роль оперативно-розыскной деятельности по отношению предварительному расследованию. В этом видится ее главное предназначение, результативность и эффективность.

Решение рассматриваемой задачи предполагает установление наличия уголовно наказуемого деяния, обнаружение всех его проявлений (эпизодов, квалифицирующих признаков), выявление и изобличении лиц его совершивших [6, с. 188]. Задача является сложной, требующей высокого профессионализма от следователя и решается прежде всего благодаря взаимодействию с сотрудниками органов, осуществляющих оперативно-розыскную деятельность. При этом должны соблюдаться *принципы недопустимости разглашения планов и полученных результатов совместной работы (конспирация), непрерывности и динамичности взаимодействия.*

В ходе проведения гласных и негласных оперативно-розыскных мероприятий могут применяться цифровые технологии. Правовой основой этого выступают статьи 38, 144, 152, 157 и 210 УПК РФ. При организации и проведении таких мероприятий следует также руководствоваться Федеральным законом от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»[1] и подзаконными нормативными правовыми актами.

IT-следователь должен иметь представление о цифровых следах, которые представляют собой результат действий человека или автоматизированной системы, воплощённые, как правило, в текстовой или мультимедийной форме, и пригодные к трансформации в доказательства по уголовным делам в электронном виде.

«Обычный следователь» также сталкивается с обнаружением и фиксацией цифровых следов. Так, например, при расследовании факта получения взятки следователю предстоит фиксировать цифровые следы, указывающие на подготовительные действия злоумышленника (возможно была предварительная договоренность о встречах взяткодателя с взяткополучателем, решался вопрос об участии посредника при передаче-получении взятки). Часто общение между взяткодателем и взяткополучателем происходит не при встречах, а с помощью средств компьютерной техники, мобильных устройств, когда информационный обмен осуществлялся с помощью SMS-сообщений,

[1] СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 25.02.2024).

сообщений в мессенджерах, электронных писем и фиксация факта передачи-получения взятки также была на электронных информационных носителях [8, с. 71].

Однако IT-следователь должен уметь работать с большими данными, читать экспертные заключения по результатам проведения компьютерно-технических экспертиз любой сложности, широко применять электронные документы и в перспективе использовать электронного помощника. Цифровая видеотека, аудиозаписи и фотографии могут накапливаться в облачных пространствах, относительно которых на сегодня имеются различные предложения по применения программного обеспечения, моделирования, алгоритмизации процессов.

Для этого, в первую очередь, предполагается, что обучение (повышение квалификации) таких следователей будет производиться в особом порядке, посредством привлечения не только теоретиков уголовно-процессуального права, но и экспертов в области цифровых технологий и компьютерной безопасности.

Следует отметить, что эффективное применение цифровых технологий при расследовании уголовных дел возможно только в случае согласованной работы трех групп: исследователей, правоприменителей и экспертов-программистов. Исследователи подготавливают теоретическую основу и методики для последующего применения на практике. Однако эти конструкции нуждаются в шлифовке и реализации через участие экспертов, корректирующих полученные результаты с позиции информатики, и правоприменителей, которые знают все многообразие проблем и подводных камней, свойственных практике [7, с. 387–395].

Таким образом, подготовка IT-следователей должна осуществляться по специальным образовательным программам, сочетающим как теоретические курсы, подготовленные ведущими учеными в сфере цифровизации уголовного процесса, так и практические занятия с экспертами-программистами, объясняющими, как работают и как могут применяться те или иные цифровые технологии. Создание таких программ обучения и подготовки кадров, основанных на триединстве теории, практики и экспертизы, является важной предпосылкой не только введения института IT-следователей, но и его последующего эффективного функционирования.

В ходе производства экспертизы при исследовании цифровых следов, цифровых носителей информации эксперт применяет специальные приемы и методики, которые, в свою очередь, основаны на применении цифровых технологий. В заключении эксперт указывает содержание и результаты исследования с указанием примененных методик, с которыми должен быть хорошо знаком следователь. При необходимости следователь может назначить дополнительную и повторную экспертизу (ст. 207 УПК РФ).

Многие ученые пишут о различных вариантах применения электронного помощника следователя [1; 2; 5], который мог бы быть использован для обработки процессуально значимой цифровой информации, включая видеоизображения, а также анализа правовой информации, выбора методических рекомендаций. Важным аспектом является реконструкция криминального события. Цифровой ассистент следователя, используя математические методы, моделирование и автоматическую проверку информации мог бы оказать в этом существенную помощь.

Изобличение виновных в совершении преступления — другая, не менее важная задача предварительного расследования, которая вытекает из задачи раскрытия преступлений. Решение данной задачи направлено на реализацию принципа неотвратимости наказания за совершенное преступление. Осуществляя уголовное преследование, орган предварительного расследования доказывает виновность всех лиц, причастных к совершению преступления, для обеспечения применения к ним наказания или иных мер уголовно-правового воздействия.

Преступления, совершаемые с использованием цифровых технологий, могут быть разные. На первоначальном этапе расследования следователь, как правило, действует в условиях информационной неопределенности. Информация о событии преступления может быть и в цифровом виде. Для ее получения необходимо провести следственные действия — обыск, осмотр, выемку. С целью обнаружения цифровых следов следователь обязан привлечь специалиста, который будет применять различные программы. С учетом ст. 58 УПК РФ специалистом в данном случае будет лицо, обладающее специальными познаниями в цифровых технологиях, оказывающее следователю содействие в обнаружении, фиксации и изъятии цифровых следов и вещественных доказательств, с применением специфических технических средств, приемов и методик. IT-следователь мог бы приглашать специалиста для участия в следственных действиях по своему усмотрению. При работе с цифровыми следами следователь такого уровня должен определять степень сложности изъятия или копирования данным. Такое усмотрение следовало бы закрепить в законе.

Еще более актуальной станет роль IT-следователя в случае введения в уголовный процесс дополнительных цифровых следственных действий, таких как компьютерное моделирование с помощью нейросетей или онлайн-обыск. Уже сейчас нейросети позволяют обычным пользователям не только генерировать различные изображения, но и моделировать самые разные ситуации. Поэтому в рамках множества исследований идет работа над применением алгоритмов нейросетей в моделировании и предсказании преступлений (т. н. *algorithmic crime control*) [9, с. 273–296].

В эффективном применении таких алгоритмических моделей огромную роль играет навык пользователя по правильному составлению запросов и введению исходных данных (*промптинг*, *промтинжиниринг*). От следователя при применении таких методов расследования требуется давать программе

четкие инструкции и вводные данные, позволяющие получить объективный результат генерации. Для этого не требуется специальных знаний, т. к. интерфейс современных нейросетевых инструментов позволяет задавать вводные данные на естественных языках (а не языках программирования). Между тем, использование нейросетей потребует от пользователя обладать соответствующим навыком промптинга, который должен быть развит у IT-следователя.

Аналогичных специальных навыков потребует и осуществление онлайн-обыска, представляющего собой удаленный взлом цифрового устройства подозреваемого с помощью специального компьютерного следственного вируса. Программа устанавливается на компьютер обвиняемого (или иных лиц в случаях, предусмотренных законом), после чего может записывать видеозвонки, сохранять введенные пароли, самостоятельно включать микрофон устройства и вебкамеру для записи переговоров [10, с. 55–75].

Переход на цифровой формат ведения уголовного судопроизводства позволит отказаться от бумажных носителей информации, широко использовать электронные документы и дистанционные формы коммуникаций, обеспечить экономию материальных средств и времени, упрощение и защиту данных (А. Ф. Абдулвалиев, М. С. Колосович, М. В. Пальчикова, Е. Г. Ларин, Л. Н. Симанович, П. В. Козловский, Ю. Н. Познанский, Н. Н. Штыкова и др.). В связи с этим возможности сторон будут значительно увеличены. Актуализируется задача по *обеспечению участия обвиняемого и других лиц в производстве по делу.*

Прежде всего, это касается стороны защиты и взаимодействия с ней следователя. После перехода на формат «Электронное уголовное дело» у стороны защиты появятся новые возможности, в том числе возможность в автономном режиме прикреплять полученные доказательства в электронном виде, используя единую цифровую площадку осуществления производства по уголовным делам [3, с. 132–135].

Электронная форма подачи заявления станет обычным делом. При производстве следственных действий широко будет использоваться видеозапись, стороне защиты будет предоставлено право на получение копии технической записи и доступа к ее оригиналу неограниченное время.

Применение технических средств фиксации (видеопротоколирование) позволяет сократить сроки рассмотрения путем исключения времени на ознакомление с протоколом в бумажном виде, исключить ошибки и различное толкование, дисциплинировать участков судебного процесса, автоматизировать регистрацию и дальнейшую публикацию протоколов на сайтах судов, создавать архивы, что также обеспечит быстрый поиск документов по заданным параметрам.

Электронное уголовное дело предполагает широкое использование электронных документов. Поэтому понадобится обеспечить всех участников следственных или судебных действий электронной подписью, что придаст легитимность документам и обеспечит выполнение требований закона. Цифровая система уголовного судопроизводства позволит любому участнику уголовно-процессуальных отношений самостоятельно прикреплять документы в электронном виде. Для стороны защиты — это возможность реализовать в какой-то степени так называемое адвокатское расследование, так как откроются дополнительные возможности по сбору и прикреплению к делу доказательств. Лицо, производящее расследование, должно лишь получить уведомление об этом и контролировать ситуацию.

Для стороны защиты представляется важным обеспечить цифровую конфиденциальную видеоконференцсвязь адвоката с подзащитным. Такой канал может иметь самостоятельную функцию, но обязательно анонсироваться (фиксироваться, отражаться) в общем электронном деле. Интерфейс может предусматривать специальную вкладку для подключения данных лиц к видеосвязи[1].

Расширение возможностей сторон по использованию цифровых технологий не должно повлечь сокращения объема процессуальных гарантий и предполагает по возможности сохранение существующих стандартов и принципов уголовного судопроизводства. Производством по уголовным делам в электронном виде, как минимум на первое время после внедрения цифровой платформы, должны заниматься IT-следователи.

Принятие мер к установлению вреда, причиненного преступлением, и его возмещению является еще одной задачей предварительного расследования. В развитии положения ст. 6 УПК РФ, закон предусматривает обеспечение уполномоченными должностными лицами и государственными органами возмещения потерпевшему вреда, причиненного преступлением (ч. 3 ст. 42 УПК РФ). Характер и размер вреда, причиненного преступлением, выступает в качестве одного из обстоятельств, подлежащих доказыванию по уголовным делам (п. 4 ч. 1 ст. 73 УПК РФ).

При подготовке к совершению преступления или позже субъекты преступления, используя цифровые технологии, как правило, применяют меры к его сокрытию. Их действия направлены на сокрытие как материальных, так и цифровых следов, что может также быть связано с сокрытием объема причиненного ущерба.

При этом могут быть использованы такие способы, как маскировка или сокрытие исходного IP-адреса системы, создание срытых файлов и каналов, использование методов шифрования, использование самоуничтожающихся программ, изменение интернет-протоколов и др.

Сложности в установлении причиненного ущерба преступлением также могло бы служить одним

[1] В СИЗО внедряются онлайн-встречи с адвокатами // Адвокатское бюро «Антонов и партнеры» : [сайт]. URL: https://pravo163.ru/v-sizo-vnedryayutsya-onlajn-vstrechi-s-advokatami/ (дата обращения: 25.02.2024).

из критериев передачи IT-следователю дела для проведения расследования.

Участие IT-следователя в досудебном производстве по уголовным делам могло бы иметь *профилактическое и воспитательного воздействия на граждан*. Как известно, правовое воспитание на стадии предварительного расследования включает в себя: ознакомление участников уголовного процесса с предписаниями закона и формирование у них уважения к праву; предоставление возможности применять нормы права в конкретных случаях; разъяснение необходимости и потребности исполнения требований закона; демонстрация отрицательного отношения к преступлениям и лицам, их совершающим; предоставление возможности отстаивать свои, а также представляемые права и законные интересы. Правовое воспитание — это эффективное средство профилактики совершения преступлений.

Уровень IT-следователи будет способствовать повышению авторитета правоохранительных органов и в какой-то мере сдерживать лиц от совершения противоправных действий, понимая, что неотвратимость наказания неизбежна. Высокая квалификация IT-следователей позволит эффективно бороться с новыми вызовами — и, что не менее важно, их работа должна будет сопровождаться постоянным повышением квалификации, позволяющим всегда опережать преступность в гонке за сохранение правопорядка и безопасности общества. IT-следователи и программы их обучения только начинают появляться в некоторых странах (например, Германии[1]), что обуславливает все большую актуальность данного вопроса.

Результат исследования и выводы

Подводя итог, следует отметить, что выделение IT-следователей в отдельную группу позволит сосредоточить внимание правоохранительных органов и высших учебных заведений на подготовку соответствующих кадров и грамотному планированию, организации работы органов предварительного расследования. При этом массовая распространенность цифровых технологий в общественной жизни дает иллюзию их постижимости специалистом в любой области знаний. Только высококвалифицированные специалисты в области уголовно-процессуального права и цифровых технологий будут решать задачи повышенной сложности, что позволит иметь равное, а то и преимущественное положение в борьбе с преступностью.

[1] Computer Hacking Forensic Investigator (CHFI) / TÜV Rheinland. URL: https://akademie.tuv.com/weiterbildungen/computer-hacking-forensic-investigator-chfi-ilearn-14821813 (дата обращения: 25.02.2024).

Список литературы

1. Буглаева Е. А. Перспективы внедрения технологий искусственного интеллекта в деятельность правоохранительных органов по составлению процессуальных документов // Вестник Южно-Уральского государственного университета. Серия: Право. 2022. Т. 22, № 1. С. 7–12;

2. Власова С. В. К вопросу о приспосабливании уголовно-процессуального механизма к цифровой реальности // Библиотека криминалиста. 2018. № 1 (36). С. 9–18.

3. Зуев С. В., Каменев А. С. Собирание и проверка электронной доказательственной информации стороной защиты в уголовном судопроизводстве : монография. Москва : Юрлитинформ, 2024. 160 с.

4. Зуев С. В. Основы оперативно-розыскной деятельности : учебное пособие для вузов. Москва : Юрайт, 2020. 191 с.

5. Смушкин А. Б. Цифровая трансформация процесса расследования как объективная реальность // Вестник СПбГУ. Право. 2023. Т. 14, вып. 1 С. 90–106.

6. Уголовный процесс : учебник / С. В. Зуев, К. И. Сутягин. Челябинск : Издательский центр ЮУрГУ, 2016. 463 с.

7. Цветкова А. Д. Проблема рассогласованности при цифровизации правоохранительной деятельности // Цифровые технологии и право : сборник научных трудов II Международной научно-практической конференции (Казань, 22 сентября 2023 года) : в 6 т., Т. 3. Казань : Познание, 2023. С. 387–395.

8. Цифровая криминалистика : учебник для вузов / В. Б. Вехов [и др.] ; под ред. В. Б. Вехова, С. В. Зуева. Москва : Юрайт, 2023. 417 с.

9. Sommerer L., § 9 Algorithmic crime control bet weenrisk, objectivity, and power // The Law between Objectivity and Power (ed. Philip M. Bender). P. 273–296. DOI: 10.5771/9783748927211-273

10. Ramalo D. S. The use of malware as a means of obtaining evidence in Portuguese criminal proceedings // Digital Evidence and Electronic Signature Law Review. 2014. Vol. 11. P. 55–75.

11. Wahl Th. Verwertung von im Ausland überwachter Chatnachrichten im Strafverfahren Zugleich Besprechung der EncroChat-Beschlüsse des OLG Bremen v. 18.12.2020 — 1 Ws 166/20, und OLG Hamburg v. 29.1.2021 — 1 Ws 2/21 // ZIS. 2021. № 7-8. P. 452–461.

КОНФЛИКТ ИНТЕРЕСОВ
Конфликт интересов отсутствует.

CONFLICT OF INTEREST
There is no conflict of interest.

ВКЛАД АВТОРОВ
Вклад авторов равноценный.

CONTRIBUTION OF THE AUTHORS
The contribution of the authors is equivalent.

Дата поступления статьи / Received: 29.02.2024.
Дата рецензирования статьи / Revised: 25.03.2024.
Дата принятия статьи к публикации / Accepted: 25.04.2024.