УДК 343.1 **DOI: 10.34670/AR.2023.51.45.058**

Роль электронных доказательств в расследовании отдельных категорий преступлений

Рябова Оксана Васильевна

Следователь по расследованию экономических преступлений
и проявлений организованной преступности
Следственного отдела Отдела МВД России «Шатковский»;
Адъюнкт,
Нижегородская академия МВД России,
603950, Российская Федерация, Нижний Новгород,
Анкудиновское шоссе, 3;
e-mail: ataeva.2013@inbox.ru

Аннотация

Одно из центральных мест в системе стадий отечественного уголовного судопроизводства по праву принадлежит стадии предварительного расследования, которая, к тому же, является одни из этапов досудебного производства. Именно на стадии предварительного расследования выполняются действия по собиранию, проверке и оценке доказательств. Настоящая статья посвящена исследованию значимости института «электронных доказательств» в контексте их использования в процессе раскрытия и расследования отдельных категорий преступления. Отмечается первостепенность явления «электронно-цифрового следа преступления», его двойственный характер и степень его влияние, оказываемого на процесс установления лица, виновного в совершении противоправного деяния. Раскрывается содержание форм, в рамках которых предстает электронное доказательство при осуществлении досудебного производства по уголовным делам, возбужденным по экономическим преступления и по преступления общеуголовной направленности. Освещается практический аспект процессуального оформления обнаруженных и изъятых следов преступлений, пребывающих и функционирующих в цифровом пространстве. Автор призывает обратить внимание на сформированные уголовно-правовой и уголовно-процессуальной доктриной тенденции необходимости регулирования института «электронных доказательств» на законодательном уровне в целях эффективного раскрытия преступлений и улучшения качества расследования уголовных дел.

Для цитирования в научных исследованиях

Рябова О.В. Роль электронных доказательств в расследовании отдельных категорий преступлений // Вопросы российского и международного права. 2023. Том 13. № 6А. С. 382-391. DOI: 10.34670/AR.2023.51.45.058

Ключевые слова

Уголовный процесс, электронное доказательство, уголовно-процессуальное право, уголовное право, категория преступлений, киберпреступления, электронно-цифровой след преступления, экономические преступления, электронный документ, общеуголовные преступления.

Введение

Одно из центральных мест в системе стадий отечественного уголовного судопроизводства по праву принадлежит стадии предварительного расследования, которая, к тому же, является одни из этапов досудебного производства. Именно на стадии предварительного расследования выполняются действия по собиранию, проверке и оценке доказательств, соотносящиеся с утвержденным действующим Уголовно-процессуальным Кодексом Российской Федерации (далее – УПК РФ) перечнем обстоятельств, подлежащих доказыванию, и, представляющих значимость для разрешения уголовного дела по существу. Их наличие подтверждает факт совершения преступления, способствует изобличению виновного лица его совершившего, а также формирует основу обвинения, после которого определяется дальнейший ход расследования уголовного дела, его движение в соответствующих инстанциях, и, соответственно, принятия итогового судебного решения.

Будучи частью уголовно-процессуального права, которая содержит в себе совокупность уголовно-процессуальных норм, регламентирующих цель доказывания, порядок собирания, проверки, оценки доказательств и их использования для обоснования выводов по расследуемому делу, доказательственное право в теоретическом аспекте трактуется как часть науки уголовного процесса, которая изучает методологические и правовые основы доказывания [Григорьев, Победкин, Яшин, 2008, 159; Лазарева, 2014, 10]. Отечественному доказательственному праву, как с точки зрения единой взаимосвязанной системы, так и в контексте рассмотрения отдельных его институтов, уделяется достаточное внимание в уголовно-процессуальном праве. Ввиду того, что императивными для исполнения правоприменителями являются нормы уголовно-процессуального закона, представляется необходимым остановиться на них более подробно.

Основная часть

Не останавливаясь на анализе положений действующего УПК РФ, регулирующих систему доказательственного права, в качестве одного из имеющихся видов доказательств законодатель называет вещественные доказательства, уникальность которых определяется наличием физических свойств и исключительности обладаемой правовой природой.

В последнее время в научных кругах ведутся дискуссии о целесообразности законодательного закрепления института «электронных доказательств» двумя способами: посредством его включения в систему вещественных доказательств, поскольку содержание электронного доказательства может находится только на определенном материальном носителе, или официальным регулированием последнего в качестве самостоятельного института уголовного процесса. В силу высокого уровня информатизации современного общества, наблюдаемого в последнее время, институт «электронных доказательств» доказал свою потребность. Вопреки отсутствию официального регулирования в отечественном уголовно-процессуальном законе, его существование убедило ряд исследователей в своей значимости и надобности использования в ходе раскрытия и расследования как отдельной категории преступлений, непосредственно связанных с использованием компьютерных и иных информационно-телекоммуникационных технологий, так и иных противоправных деяний.

Вследствие чего, представляется логичным начать с исследования той категории

преступлений, которые совершаются в сфере цифрового пространства и которые непосредственно связаны с использованием информационно-телекоммуникационных технологий. Так, теория уголовного права называет такие противоправные деяния «киберпреступлениями», которые регламентируются в законе главой 28 Уголовного кодекса Российской Федерации (далее – УК РФ) – «Преступления в сфере компьютерной информации». В контексте их анализа, особое внимание следует уделить двойственности природы виртуальных следов, которая характеризуется двумя основополагающими критериями: наличием у объекта, содержащего в себе электронную информацию, физического свойства, и, наличием у лица, ее анализирующего, специальных познаний в области информационно-телекоммуникационных технологий [Вершищкая, 2022].

Нет сомнений относительно достоверности высказанной позиции, поскольку, учитывая специфический характер сведений, пребывающих в цифровом пространстве, а также их сохранность и способность к воспроизведению, копированию или иному действию, которые невыполнимы без их нахождения на соответствующем электронном носителе. Вместе с тем, нуждается в уточнении то обстоятельство, что вид предмета, содержимое которого будет включать в себя соответствующие данные, не имеет значения, так как в каждом отдельном случае выбор материального носителя индивидуален, и определяется должностным лицом, осуществляющим предварительное расследование. На практике, в случае, когда исследуемая информация обладает большим объемом, или, ее перенос на бумажный носитель не представляется возможным, то, по окончании осмотра, принимается решение о помещении сведений на соответствующий электронный носитель (к примеру, на жесткий диск), после чего, при наличии оснований полагать, что полученные сведения представляют значимость для расследования уголовного дела, последние признаются и приобщаются к материалам уголовного дела в качестве вещественных доказательств. В качестве доказательства признается информация, полученная из цифрового пространства, и, помещенная на электронный носитель. В действительности, указанные данные обозначают не столько вещественное, сколько электронное доказательство, однако, ввиду отсутствия его нормативно-правовой регламентации в отечественном уголовно-процессуальном законе, остается лишь воспринимать его как вещественное, дабы не утратить ценность его содержания.

Рассуждая на тему значимости электронных доказательств в процессе расследования киберпреступлений, имеет смысл проанализировать категорию «виртуальных», «электронно-цифровых», «информационных» и «компьютерных» следов преступлений, которые, фактически, отождествляются с сущностью электронного доказательства, и которые, имеют первостепенную важность при расследовании преступлений такого рода.

При изучении данного вопроса следует обратиться к предложенной Колычевой А.Н. дефиниции, которая относит рассматриваемый след преступления к невидимому материальному следу, именует его «электронно-цифровым» и определяет его как «криминалистически значимую информацию, выраженную посредством электромагнитных взаимодействий или сигналов в форме, пригодной для обработки с использованием компьютерной техники, в результате создания определенного набора двоичного машинного кода либо его преобразования, выразившегося в модификации, копировании, удалении или блокировании, зафиксированную на материальном носителе, без которого не может существовать» [Колычева, 2019, 25].

Формулировка вышеприведенного термина весьма удачна, поскольку детально отражает

сущность рассматриваемого следа, его структурные компоненты и назначение. Но, вместе с тем, представляется возможным частично видоизменить ее в некоторых аспектах, предложив тем самым иную редакцию рассматриваемого понятия. Так, использование словосочетания «с использованием информационно-телекоммуникационных технологий» будет более удачным, так как предложенный термин более многогранен, и с учетом его структурного содержания, уже включает в себя упомянутую ранее «компьютерную технику».

Выделяя из вышеприведенного понятия основные характеристики, необходимо расставить акценты на следующих признаках. Во-первых, это вид информации, которая отличается узконаправленным характером, в силу чего, охватывает определенный спектр воздействия. Во-вторых, сфера ее пребывания, которой принято информационное поле, электронное пространство или виртуальную среду пребывания. В-третьих, особый порядок функционирования, выражающийся в особенностях ее изъятия и хранения. В-четвертых, использование специальных познаний в процессе изучения данных, сопровождаемое участием специалиста, которое может быть как обязательным, ввиду необходимости особенных познаний; так и нет, когда субъект уголовно-процессуальной деятельности может обойтись без привлечения какой-либо помощи извне.

Что касается построения плана расследования таких преступлений, необходимо отметить многообразие подходов в теории уголовно-процессуального права относительно их раскрытия и расследования. В научном кругу исследователями предлагается двухуровневый алгоритм работы с выявленными преступлениями, где первый этап включает в себя деятельность по обнаружению местоположения устройства посредством вычисления его ip-адреса, имеющегося у любого технического средства, с использованием которой было совершено противоправное деяние, и, соответственно, лица его применяющего в процессе совершения преступления. Второй этап охватывает процесс анализа обнаруженного цифрового следа: изучение его сущности и содержания, места его пребывания, процесса его считывания и иных характеристик, с помощью которых представляется возможным выявить искомую информацию [Тарасов, Санников, 2022]. Однако, предложенные алгоритмы являются весьма условными, так как на практике субъект доказывания зачастую сталкивается с ситуацией, когда выследить ip-адрес устройства, с использованием которого было совершено преступление, не представляется возможным, к примеру, из-за его нахождения за пределами Российской Федерации. Так, детальному изучению электронно-цифровых следов предшествует производство ряда следственных действий, выполнение осуществляется как в ходе проведения проверочных мероприятий, так и после вынесения постановления о возбуждении уголовного дела. Среди обязательно проводимых следует выделить осмотр (места происшествия, предметов и документов) и проведение судебной экспертизы.

Разрабатывая методику расследования киберпреступлений, учеными отмечается рациональность незамедлительного назначения компьютерно-технической экспертизы в целях сохранения сведений, содержащихся на изъятом предмете [Егерева, Коломинов, Сизова, 2018]. Проведение экспертизы по уголовном делу представляет собой один из важнейших этапов в ходе расследования уголовного дела, поскольку в процессе ее осуществления подтверждается подлинность обнаруженных и изъятых следов преступления, а также устанавливается степень их значимости для изобличения лица, виновного в совершении инкриминируемого ему деяния.

В данный момент и возникает острая потребность в привлечении к процессу расследования специалистов, обладающих соответствующими специфическими познаниями в изучаемой

сфере. Процессуальное оформление его участия осуществляется следователем, однако, к сожалению, законодательно, данный вопрос подробно не регламентируется. На сегодняшний уголовно-процессуальные нормы не называют строго определенную процедуру привлечения специалиста, организацию его деятельности, а также процесс построения работы в зависимости от специфики следа преступления, представленного для проведения исследования. С учетом прав, предоставленных эксперту буквой закона, его главная задача заключается в изучении и детальном анализе механизма взаимодействия следов и его осуществлении в конкретных ситуациях. Соответственно, именно в ходе проведения компьютерно-технической экспертизы становится возможным определить цифровые (виртуальные) следы криминальной деятельности, реализуемой конкретным лицом в сети Интернет [Сысенко, Смирнова, Тимошенко, 2020].

С учетом уникальности цифрового пространства, в рамках которой формируются и функционируют уголовно-процессуальные отношения, только электронно-цифровой след преступления, признанный в последующем электронным доказательством по уголовному делу, будет являться прямым и одним из основополагающих доказательств, подтверждающих виновность лица, совершившего киберпреступление. В силу своих исключительных качеств, электронное доказательство имеет потенциальное преимущество по сравнению с другими доказательствами, поэтому доказательства может оказать реальное содействие в борьбе с распространяющимися формами преступности и способами, применяемыми при совершении преступлений. И, если бы, киберпреступления являлись бы единственной категорией преступлений, в процессе работы с которыми возникали проблемные вопросы как относительно нормативно-правовой регламентации, так и практики их применения, отечественному уголовно-процессуальному праву было бы намного легче.

Затронувшие все сферы жизни современного общества результаты технологического прогресса наложили свой отпечаток и на процедуру раскрытия и расследования иных категорий преступлений. На данный момент, наиболее часто совершаемыми и, к сожалению, в большинстве случаев, остающимися в статусе «расследуемых в условиях неочевидности», являются преступления, совершенные против собственности. Из закрепленных действующим УК РФ, наиболее подходящими для использования в качестве примеров являются определенные виды мошенничеств, в частности, мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ) и мошенничество в сфере компьютерной информации (ст. 169.6 УК РФ). Кроме озвученных преступных деяний к представленному списку также следует отнести кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ).

Диспозиции вышеназванных статей тем или иным образом содержат в себе термины «электронный», «компьютерный», что, само собой, указывает на специфику совершения указанных преступлений. Не углубляясь в изучение объективной стороны каждого из названных составов, обращается внимание что помимо того, что их объекты и предметы являются смежными, также они в той или иной степени неразрывно существуют с информационным пространством или электронной средой, что в очередной раз подтверждает особый порядок обнаружения, фиксации и исследования полученных в ходе расследования сведений, признанных впоследствии доказательствами по уголовному делу.

В отличие от преступлений, совершенных с использованием компьютерных технологий, рассматриваемая категория преступлений соотносится с терминами «банковский счет»,

«банковская карта» и «платежная система». Банковский счет и платежная система являются по своей природе виртуальными системами, которые пребывают и функционируют в цифровом пространстве. В то время как законодательной конструкции «банковского счета» посвящен целый параграф Гражданского кодекса Российской Федерации, ни одна из представленных диспозиций не разъясняет значение рассматриваемого термина, в отличие от доктрины, которая вполне обоснованно объясняет его содержание. Так, под банковским счетом принято понимать документ (лицевой счет), оформление которого кредитной организацией на определенное лицо (клиента, владельца счета) является составной частью предмета заключенного между ними договора банковского счета, который предназначен для отражения денежных обязательств кредитной организации перед этим лицом [Курбатов, 2007]. При этом, банковский лицевой счет существует, как и в электронном формате, так как располагается в соответствующей цифровой базе, так и представлен в бумажном формате, поскольку является результатом заключения договора. Однако, принимая во внимание, что договор банковского счета содержит в себе конфиденциальную информацию о личных персональных данных его держателя, и в качестве предмета преступного посягательства банковский счет отождествляется с электронной формой, исследуется посредством применения цифровых технологий, в связи с чем, его по праву можно считать полноценным электронным доказательством.

С платежной системой ситуация обстоит куда сложнее. Действующее российское законодательство определяет национальную платежную систему как совокупность операторов по переводу денежных средств (включая операторов электронных денежных средств), банковских платежных агентов (субагентов), платежных агентов, организаций федеральной почтовой связи при оказании ими платежных услуг в соответствии с законодательством Российской Федерации, операторов платежных систем, операторов услуг платежной инфраструктуры (субъекты национальной платежной системы). Всевозможные виды эксплуатируемых в настоящее время платежных систем стали реальностью по причине непрерывного совершенствования в сфере информационно-телекоммуникационных технологий, что, обусловило своевременность и эффективность их применения. Поэтому, нет ничего удивительного в том, что некоторые используют просторы информационного поля и продукты цифровых технологий не во благо, а для достижения преступных целей. В связи с чем, при расследовании преступлений, совершенных с использованием банковского счета и платежной системы, априори, следует говорить о наличии и детальном исследовании электронных доказательств как основополагающих следов преступления, подтверждающих преступное воздействие на чью-либо собственность.

В отличие от банковского счета и платежной системы, банковская карта признается и приобщается к материалам уголовного дела в качестве вещественного доказательства, поскольку, будучи, платежным инструментом, представлена в виде предмета, обладающего физическими характеристиками, который представляется возможным изучить наглядно. Это подразумевает под собой его изъятие, осмотр, принятие мер к обеспечению его целостности и сохранности, а также последующее решение вопроса о месте хранения, что, в свою очередь, приравнивает банковскую карту к статусу привычного «вещественного доказательства».

Безусловно, организация работы по исследованию предоставляемых предметов для субъектов доказывания (следователя или дознавателя) не представляет труда в контексте получения искомой информации, которая содержится в анализируемых системах в виду отсутствия необходимости в привлечении специалистов для их анализа, поскольку сведения

изложены в стандартном виде (данные, которые содержатся на бумажном носителе; таблицы в формате docx, exel, хранящиеся на цифровом диске), и не представляют сложности для восприятия и последующего анализа. Примером таких сведений могут служить как выписка о движении денежных средств по банковскому счету банковской карты лица, в отношении которого были совершены преступные мошеннические действия, подтверждающая факт несанкционированного списания денежных средств потерпевшего, так и телефонные соединения абонентского устройства, представленные в виде детализации абонентского номера, которая свидетельствует о контакте, произошедшем между потерпевшим и лицом, подозреваемым в совершении конкретного преступления.

При рассмотрении вопроса об использовании электронных доказательств в расследовании экономических преступлений принято говорить о такой их разновидности как электронный документ [Яковлев, 2005]. В конкретном случае, именно электронный документ демонстрирует сосредоточение в одном файле больших объемов конкретной информации финансового характера, которая содержит в себе соответствующие сведения, имеющие значение для расследования преступления. К числу таких сведений следует отнести данные об открытых расчетных счетах, принадлежащих физическим и юридическим лицам, данные о движении по ним денежных средств, а также всевозможные электронные базы данных [Жуланов, Ищенко, 2007].

Относительно процессуального порядка признания последних доказательствами по уголовному делу, следует отметить, что на начальном этапе, процедура обнаружения, фиксации и последующего исследования выявленных электронно-цифровых следов преступлений аналогична анализу следов, изучаемых при раскрытии иных общественно-опасных деяний, поскольку зачастую они предоставляются по окончании проведения оперативно-розыскных мероприятий, осуществляемых в рамках первоначальной проверки, и, уже в последующем, на стадии предварительного расследования, решается вопрос об их пригодности и легитимности в качестве подтверждения виновности субъекта преступления [Переверзева , Комов, 2022]. Эта разновидность преступлений была выбрана неслучайно, так как особо-сложные по способу совершения преступления, большинство из них совершается с обязательным использованием электронных доказательств, которые, либо являются средствами совершения преступления, либо осуществляют вспомогательную процессуальную функцию в процессе их расследования.

Кратко изучив и проанализировав основные аспекты, раскрывающие порядок применения электронных доказательств при раскрытии киберпреступлений, преступлений против собственности, а также экономических преступлений, нельзя не отметить их предопределяющую роль, которую они играют в процессе доказывания на различных этапах уголовного процесса. Озвученные противоправные деяния объединяет то, что в целях реализации полноценного, всестороннего и эффективного расследования преступлений возникла необходимость в активном применении электронно-цифровых следов, формирующих полноценную доказательственную базу, обеспечивающую не только выполнение функции разрешения уголовного дела по существу, но и реализацию поставленных перед уголовным судопроизводством задач. Существующее в настоящее время многообразие их побуждает общество к их дальнейшему изучению, а также к поиску и созданию новых информационно-телекоммуникационных технологий, отвечающих последним стремлениям социума.

Заключение

Любое анализируемое явление многогранно, и, подобно медали, имеет противоположные друг другу стороны. Также и результаты, получаемые в процессе его применения, могут быть использованы, как со злым умыслом, так и во благо человечества. И, рассматривая право, как одну из важных сфер его жизнедеятельности, перед нами как исследователями стоит задача, суть которой заключается в преобразовании результатов информационного прогресса в инструменты, которые будут являться либо полноправными и полноценными институтами своих отраслей или же играть роль вспомогательных средств, направленных на содействие в достижении намеченных целей в рамках осуществления уголовно-процессуальной деятельности. В качестве такого института и может быть представлен феномен «электронных доказательств», призванный в сложившихся условиях облегчить реализацию процесса доказывания по уголовным делам различных категорий на конкретных этапах уголовного судопроизводства. Только законодательное подспорье в виде регламентации процессуального порядка оформления, изъятия, исследования и последующего определения судьбы доказательства такого рода будет способствовать стремительному раскрытию преступления, эффективному расследованию уголовного дела и постановлению соответствующего судебного решения. Вследствие чего, законодателю лишь остается внять веяниями доктрины и принять верное и аргументированное решение о включении в действующий УПК РФ понятия «электронных доказательств», воплотив при этом в жизнь замысел теоретиков, и, тем самым, существенно облегчив практическую деятельность правоприменителей.

Библиография

1. Вершицкая Г.В. Возможности использования виртуальных следов в ходе расследования киберпреступлений // Вестник Поволжского института управления. 2022. Том 22. № 2. С. 17-23.
2. Григорьев В.Н., Победкин А.В., Яшин В.Н. Уголовный процесс. М.: Эксмо, 2008. 832 с.
3. Егерева О.А., Коломинов В.В., Сизова М.С. Некоторые вопросы методики расследования киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2018. Выпуск 4 (22). С. 24-32.
4. Жуланов В., Ищенко Е. Использование баз данных в расследовании экономических преступлений // Законность. 2007. № 10. С. 25-28.
5. Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети «Интернет»: дис. … канд. юрид. наук. М., 2019. 199 с.
6. Курбатов А.Я. Разграничение банковских счетов со смежными понятиями: критерии и значение // Банковское право. 2007. № 4. С. 5-13.
7. Лазарева В.А. Доказывание в уголовном процессе. М.: Юрайт, 2014. 359 с.
8. Переверзева Е.С., Комов А.В. Особенности предоставления результатов оперативно-розыскной деятельности в виде компьютерных следов органу предварительного расследования по экономическим преступлениям // Вестник Санкт-Петербургского университета МВД России. 2022. № 3 (95). С. 98-104.
9. Сысенко А.Р., Смирнова И.С., Тимошенко С.Е. Проблемы назначения и производства судебной компьютерно-технической экспертизы // Сибирское юридическое обозрение. 2020. Том 17. № 4. С. 524-533.
10. Тарасов А.В., Санников Д.И. Криминалистические аспекты использования следов киберпреступлений как доказательства в суде при рассмотрении уголовных дел // Молодой ученый. 2022. № 33 (428). С. 104-106.
11. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 года № 174-ФЗ (в ред. от 25 марта 2022 г.) (с изм. и доп., вступил в силу с 19.05.2022).
12. Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ (в ред. от 12 ноября 2018) (с изм. и доп., вступил в силу с 18.03.2023).
13. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (редакция от 03.07.2019).
14. Яковлев А.Н. Электронные документы как доказательства при расследовании экономических и налоговых преступлений // Вестник МВД России. 2005. № 4 (80). URL: https://www.lawnow.ru/articles/law/430-2009-12-26-14-03-56/

The role of electronic evidence in the investigation of certain categories of crimes

Oksana V. Ryabova

Investigator for the Investigation of Economic Crimes
and Manifestations of Organized Crime,
Shatkovsky Investigative Department
of the Ministry of Internal Affairs of Russia;
Adjunct,
Nizhniy Novgorod Academy of the Ministry of Interior of Russia,
603950, 3, Ankudinovskoe highway, Nizhniy Novgorod, Russian Federation;
e-mail: ataeva.2013@inbox.ru

Abstract

One of the central places in the system of stages of domestic criminal proceedings rightfully belongs to the stage of preliminary investigation, which, moreover, is one of the stages of pre-trial proceedings. It is at the stage of preliminary investigation that actions are taken to collect, verify and evaluate evidence. This article is devoted to the study of the significance of the institution of "electronic evidence" in the context of their use in the process of disclosure and investigation of certain categories of crime. The primacy of the phenomenon of "electronic-digital trace of a crime", its dual nature and the degree of its influence on the process of identifying a person guilty of an unlawful act are noted. The content of the forms within which electronic evidence is presented in the course of pre-trial proceedings in criminal cases initiated for economic crimes and general criminal offenses is disclosed. The practical aspect of the procedural registration of the detected and seized traces of crimes that reside and function in the digital space is consecrated. The author calls to pay attention to the trends formed by the criminal law and criminal procedure doctrine of the need to regulate the institution of "electronic evidence" at the legislative level in order to effectively solve crimes and improve the quality of the investigation of criminal cases.

For citation

Ryabova O.V. (2023) Rol' elektronnykh dokazatel'stv v rassledovanii otdel'nykh kategorii prestuplenii [The role of electronic evidence in the investigation of certain categories of crimes]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 13 (6A), pp. 382-391. DOI: 10.34670/AR.2023.51.45.058

Keywords

Criminal process, electronic evidence, criminal procedural law, criminal law, category of crimes, cybercrimes, electronic digital trace of a crime, economic crimes, electronic document, ordinary crimes.

References

1. Egereva O.A., Kolominov V.V., Sizova M.S. (2018) Nekotorye voprosy metodiki rassledovaniya kiberprestuplenii [Some questions of the methodology for investigating cybercrimes]. *Sibirskie ugolovno-protsessual'nye i*

kriminalisticheskie chteniya [Siberian Criminal Procedure and Forensic Readings], 4 (22), pp. 24-32.
2. *Federal'nyi zakon ot 27.06.2011 № 161-FZ «O natsional'noi platezhnoi sisteme» (redaktsiya ot 03.07.2019)* [Federal Law No. 161-FZ of June 27, 2011 "On the National Payment System" (as amended on July 3, 2019)].
3. Grigor'ev V.N., Pobedkin A.V., Yashin V.N. (2008) *Ugolovnyi protsess* [Criminal process]. Moscow: Eksmo Publ.
4. Kolycheva A.N. (2019) *Fiksatsiya dokazatel'stvennoi informatsii, khranyashcheisya na resursakh seti «Internet». Doct. Dis.* [Fixing evidentiary information stored on the resources of the Internet. Doct. Dis.]. Moscow.
5. Kurbatov A.Ya. (2007) Razgranichenie bankovskikh schetov so smezhnymi ponyatiyami: kriterii i znachenie [Differentiation of bank accounts with related concepts: criteria and meaning]. *Bankovskoe pravo* [Banking law], 4, pp. 5-13.
6. Lazareva V.A. (2014) *Dokazyvanie v ugolovnom protsesse* [Evidence in criminal proceedings]. Moscow: Yurait Publ.
7. Pereverzeva E.S., Komov A.V. (2022) Osobennosti predostavleniya rezul'tatov operativno-rozysknoi deyatel'nosti v vide komp'yuternykh sledov organu predvaritel'nogo rassledovaniya po ekonomicheskim prestupleniyam [Features of presenting the results of operational-search activity in the form of computer traces to the body of preliminary investigation on economic crimes]. *Vestnik Sankt-Peterburgskogo universiteta MVD Rossii* [Bulletin of the St. Petersburg University of the Ministry of Internal Affairs of Russia], 3 (95), pp. 98-104.
8. Sysenko A.R., Smirnova I.S., Timoshenko S.E. (2020) Problemy naznacheniya i proizvodstva sudebnoi komp'yuterno-tekhnicheskoi ekspertizy [Problems of Appointment and Production of Forensic Computer-Technical Expertise]. *Sibirskoe yuridicheskoe obozrenie* [Siberian Legal Review], 17, 4, pp. 524-533.
9. Tarasov A.V., Sannikov D.I. (2022) Kriminalisticheskie aspekty ispol'zovaniya sledov kiberprestuplenii kak dokazatel'stva v sude pri rassmotrenii ugolovnykh del [Forensic aspects of using traces of cybercrime as evidence in court when considering criminal cases]. *Molodoi uchenyi* [Young scientist], 33 (428), pp. 104-106.
10. *Ugolovno-protsessual'nyi kodeks Rossiiskoi Federatsii ot 18 dekabrya 2001 goda № 174-FZ (v red. ot 25 marta 2022 g.) (s izm. i dop., vstupil v silu s 19.05.2022)* [Code of Criminal Procedure of the Russian Federation of December 18, 2001 No. 174-FZ (as amended on March 25, 2022) (as amended and supplemented, entered into force on May 19, 2022)].
11. *Ugolovnyi kodeks Rossiiskoi Federatsii ot 13 iyunya 1996 goda № 63-FZ (v red. ot 12 noyabrya 2018) (s izm. i dop., vstupil v silu s 18.03.2023)* [Criminal Code of the Russian Federation of June 13, 1996 No. 63-FZ (as amended on November 12, 2018) (as amended and supplemented, entered into force on March 18, 2023)].
12. Vershishchkaya G.V. (2022) Vozmozhnosti ispol'zovaniya virtual'nykh sledov v khode rassledovaniya kiberprestuplenii [Possibilities of using virtual traces in the course of investigating cybercrime]. *Vestnik Povolzhskogo instituta upravleniya* [Bulletin of the Volga Institute of Management], 22, 2, pp. 17-23.
13. Yakovlev A.N. (2005) Elektronnye dokumenty kak dokazatel'stva pri rassledovanii ekonomicheskikh i nalogovykh prestuplenii [Electronic documents as evidence in the investigation of economic and tax crimes]. *Vestnik MVD Rossii* [Bulletin of the Ministry of Internal Affairs of Russia], 4 (80). Available at: https://www.lawnow.ru/articles/law/430-2009-12-26-14-03-56/ [Accessed 06/06/2023]
14. Zhulanov V., Ishchenko E. (2007) Ispol'zovanie baz dannykh v rassledovanii ekonomicheskikh prestuplenii [The use of databases in the investigation of economic crimes]. *Zakonnost'* [Lagality], 10, pp. 25-28.