КОМПАРАТИВИСТСКИЕ ИССЛЕДОВАНИЯ УГОЛОВНОГО ПРАВА, КРИМИНОЛОГИИ И УГОЛОВНО-ИСПОЛНИТЕЛЬНОГО ПРАВА

DOI: 10.12737/jflcl.2019.4.4

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ В КАЧЕСТВЕ ДОКАЗАТЕЛЬСТВ ПО УГОЛОВНОМУ ДЕЛУ: СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ ЗАРУБЕЖНОГО ЗАКОНОДАТЕЛЬСТВА

ЗАЙЦЕВ Олег Александрович, и. о. заведующего отделом уголовного и уголовно-процессуального законодательства, судоустройства Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, доктор юридических наук, профессор, заслуженный деятель науки Российской Федерации, почетный работник высшего профессионального образования Российской Федерации

Россия, 117218, г. Москва, ул. Большая Черемушkinsкая, 34

E-mail: oleg010663@mail.ru

Цифровизация активно проникает в уголовно-процессуальные отношения, оказывает существенное воздействие на формирование доказательств по уголовному делу. Особую актуальность приобретают исследования, связанные с развитием электронной формы фиксации, передачи и использования информации. Возникает потребность в разработке новых методов обнаружения, фиксации и оценки доказательств при совершении противоправных деяний, в первую очередь связанных с использованием средств компьютерной техники.

Цель исследования — выявить особую роль электронных доказательств в сфере уголовного судопроизводства и разработать предложения по совершенствованию действующего законодательства. Задачи исследования: а) определить особенности зарубежного уголовно-процессуального законодательства, регламентирующего отдельные процедуры и правила работы с электронными доказательствами; б) показать позиции зарубежных и российских ученых-процессуалистов относительно понятия и содержания электронных доказательств; в) обосновать рекомендации по дальнейшему развитию российского законодательства в рассматриваемой сфере деятельности.

Методологической основой исследования послужил диалектический метод познания, общенаучные методы абстрагирования, анализа и синтеза, а также специальные юридические методы (сравнительно-правовой, логико-юридический и др.).

Автор приходит к выводу, что на законодательном уровне необходимы: закрепление ключевых принципов применения цифровых технологий; расширение пределов допустимости доказательств; фиксация новых источников фактических данных; применение цифровых технологий при принятии процессуально значимых решений по уголовному делу. В УПК РФ целесообразно предусмотреть применение электронно-цифровых документов, составляемых сторонами защиты и обвинения в ходе фиксации процесса и результата следственных и судебных действий, направленных на получение необходимой доказательственной информации по уголовному делу. Должно быть допустимым предоставление информации любым способом, обеспечивающим надежность ее сохранения и передачи в электронном виде в надлежащий правоохранительный орган или уполномоченному должностному лицу. В перспективе следует перейти на исключительно электронный документооборот в уголовном судопроизводстве.

Ключевые слова: цифровизация, уголовное судопроизводство, электронные доказательства, доказывание, электронное уголовное дело, использование электронной информации.

Для цитирования: Зайцев О. А. Особенности использования электронной информации в качестве доказательств по уголовному делу: сравнительно-правовой анализ зарубежного законодательства // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 4. С. 42—57. DOI: 10.12737/jflcl.2019.4.4

FEATURES OF THE USE OF ELECTRONIC INFORMATION AS CRIMINAL EVIDENCE: A COMPARATIVE-LEGAL ANALYSIS OF FOREIGN LEGISLATION

O. A. ZAITSEV, Institute of Legislation and Comparative Law under the Government of the Russian Federation, Moscow 117218, Russian Federation

E-mail: oleg010663@mail.ru

Digitization actively penetrates criminal procedure relations, has a significant impact on the formation of evidence in a criminal case. Of particular relevance are researches related to the development of the electronic form of recording, transmission and use of information. There is a need to develop new methods for detecting, fixing and evaluating evidence when committing unlawful acts, primarily involving the use of computer technology.

The purpose of this study is to identify the special role of electronic evidence in the field of criminal proceedings and to develop proposals for improving the current legislation. The objectives of the research are: a) to determine the peculiarities of foreign criminal procedure legislation, which regulates certain procedures and rules for working with electronic evidence; b) to show the position of foreign and Russian procedural scientists regarding the concept and content of electronic evidence; c) to substantiate recommendations for the further development of Russian legislation in the considered field of activity.

The methodological basis of the study was the dialectical method of cognition, the general scientific methods of abstraction, analysis and synthesis, as well as special legal methods (comparative legal, logical and legal, etc.).

The author comes to the conclusion that, at the legislative level, the key principles of the use of digital technologies need to be fixed, expanding the limits of admissibility of evidence; fixing new sources of evidence; the use of digital technologies in making procedurally significant decisions in a criminal case. In the Code of Criminal Procedure, it is advisable to provide for the use of electronic digital documents drawn up by the parties to the defense and the prosecution during the recording of the progress and result of investigative and judicial actions aimed at obtaining the necessary evidentiary information in a criminal case. It should be permissible to provide information in any way that ensures the reliability of its preservation and transmission in electronic form to the appropriate law enforcement agency or an authorized official. In the future, it is necessary to switch to exclusively electronic document circulation in criminal proceedings.

Keywords: digitalization, criminal justice, electronic evidence, proof, electronic criminal case, the use of electronic information.

For citation: Zaitsev O.A. Features of the Use of Electronic Information as Criminal Evidence: A Comparative-Legal Analysis of Foreign Legislation. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya* = *Journal of Foreign Legislation and Comparative Law*, 2019, no. 4, pp. 42—57. (In Russ.) DOI: 10.12737/jfcl.2019.4.4

Стремительное внедрение информационно-цифровых технологий и возникающих в процессе их использования новых общественных отношений существенным образом изменяют нашу жизнь. Информационное пространство вокруг меняется с такой скоростью, что человечество не успевает в полной мере освоить появившиеся технологии и их возможности. Цифровизация превращается в одну из приоритетных задач развития государства и общества¹.

Так, 20 февраля 2019 г. в ежегодном Послании Федеральному Собранию Президент РФ В. В. Путин отметил необходимость оперативного принятия законов, приоритетных для создания правовой среды цифровой экономики. Законодательство нашей страны должно соответствовать новой технологической реальности и помогать развитию перспективных отраслей². Принятие в последние годы на государственном уровне различного рода документов свидетельствует о серьезности намерений в данном направлении и грядущих масштабных преобразованиях во всех сферах деятельности³.

Перед юридической наукой стоят фундаментальные и прикладные задачи в части доктринального освоения имеющихся закономерностей развития и дальнейшего функционирования права и государственно-правовой сферы жизни нашего общества в условиях цифровой реальности и определения путей их решения. Разработка научно обоснованных инструментов и моделей правового регулирования различных сфер общественной жизни позволит государству более эффективно реагировать на вызовы цифровой реальности, управлять происходящими трансформациями, регулировать новые, а также видоизменяющиеся общественные отношения⁴.

Внедрение информационно-цифровых технологий затронуло практически все направления судебной и правоохранительной деятельности, включая производство по уголовным, гражданским, арбитражным делам, а также по делам об административных правонарушениях. Об этом свидетельствуют и осуществляемые научные исследования в данном направлении, изучение опыта зарубежных стран по цифровизации правосудия⁵.

¹ См.: Правовое пространство и человек: монография / отв. ред. Ю. А. Тихомиров, Е. В. Пуляева, Н. И. Хлуденева. М., 2012. С. 177.

² См.: Российская газета. 2019. 21 февр.

³ См., например, Стратегию развития информационного общества в Российской Федерации на 2017—2030 годы, утв. Указом Президента РФ от 9 мая 2017 г. № 203; Указ Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»; Основные направления деятельности

Правительства Российской Федерации на период до 2024 года, утв. Правительством РФ 29 сентября 2018 г.

⁴ См.: Хабриева Т. Я. Право перед вызовами цифровой реальности // Журнал российского права. 2018. № 9. С. 5—16; Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 85—102.

⁵ См., например: Дремлюга Р. И. Компьютерная информация как предмет посягательства при неправомерном доступе: сравнительный анализ законодательства США и России // Журнал зарубежного и сравнительного правоведения. 2018.

В 2012 г. Правительство РФ утвердило государственную программу «Развитие судебной системы России на 2013—2020 годы», которая направлена на повышение качества правосудия и эффективности рассмотрения судебных споров, обеспечения его доступности и открытости. Реализация данной программы предусматривает процесс внедрения и использования информационных технологий как внутри судебной системы, так и во взаимоотношениях с внешними субъектами⁶. Кроме того, формируется правовая база с принятием специальных норм, регулирующих процессуальные аспекты осуществления правосудия с помощью электронных средств.

Во исполнение указанной программы принят Федеральный закон от 23 июня 2016 г. № 220-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти». Благодаря этому участники судебных производств получили доступ к системам электронной подачи заявлений, обращений, ходатайств и доказательств.

В ходе осуществления производства по делу одной из основных целей является доказывание факта совершения противоправного деяния. При этом любое решение принимается на основе собранных, исследованных и оцененных доказательств. Развитие информационно-цифровых технологий, перевод функций государства в электронную сферу, создание и деятельность электронного правительства настоятельно требуют деформализации всего процесса доказывания. В связи с этим возникает необходимость перехода в цифровую (электронную) сферу с заменой ряда традиционных источников доказывания на совершенно новые источники.

Появление электронной формы фиксации, передачи и использования информации диктует потребность в разработке новых методов обнаружения, фиксации и оценки доказательств при совершении противоправных деяний, в первую очередь связанных с использованием средств компьютерной техники. Об этом свидетельствуют как опубликованные результаты масштабной работы ученых⁷, так и проведенные в

последний период времени диссертационные исследования по данному направлению⁸.

Под цифровыми технологиями в уголовном процессе понимается определенная совокупность средств, приемов и методов собирания (поиска, обнаружения, фиксации, изъятия), обработки (в том числе с использованием искусственного интеллекта), передачи и представления информации о расследуемом событии для получения уголовно-процессуальных доказательств. Данные доказательства позволяют в ходе производства по уголовному делу устанавливать наличие или отсутствие обстоятельств, подлежащих доказыванию, а также иных обстоятельств, имеющих значение для расследования конкретного преступления. При этом следует осознавать важность правового регулирования уголовно-процессуальной формы цифровых технологий. Ненадлежащий характер такого регулирования влечет определенные правовые последствия, в том числе признание доказательств недопустимыми, что, как известно, может привести к вынесению оправдательного приговора, основанного не на установленной невинности подсудимого, а на недоказанности его вины вследствие исключения признанных недопустимыми доказательств обвинения из списка доказательств по уголовному делу.

В связи с этим повышенный интерес вызывает зарубежный опыт, где на законодательном уровне закреплена возможность производства уголовного дела в электронном формате⁹ и использования в качестве

2019. 264 с.; Развитие информационных технологий в уголовном судопроизводстве: монография / под ред. С. В. Зуева. М., 2018. 248 с.; Боннер А. Т. Традиционные и нетрадиционные средства доказывания в гражданском и арбитражном процессе. М., 2015. 624 с.; Пастухов П. С. Доктринальная модель совершенствования уголовно-процессуального доказывания в условиях информационного общества: монография. М., 2015. 352 с.

⁸ См., например: Булгаков А. Н. Административное расследование правонарушений в области обеспечения безопасности дорожного движения: дис. ... канд. юрид. наук. Краснодар, 2017. 187 с.; Ворожебит С. П. Электронные средства доказывания в гражданском и арбитражном процессе: дис. ... канд. юрид. наук. СПб., 2011. 235 с.; Зазулин А. И. Правовые и методологические основы использования цифровой информации в доказывании по уголовным делам: дис. ... канд. юрид. наук. Екатеринбург, 2018. 251 с.; Овсянников Д. В. Копирование электронной информации как средство уголовно-процессуального доказывания: дис. ... канд. юрид. наук. Челябинск, 2015. 192 с.; Оконенко Р. И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: автореф. дис. ... канд. юрид. наук. М., 2016. 23 с.

⁹ Практика производства по уголовному делу в электронном формате достаточно широко распространена в рамках

№ 6. С. 129—133; Талалина Э. В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2. С. 5—17; Жилкин В. А. Цифровые технологии и применение искусственного интеллекта в Финляндии и России: сравнительно-правовое исследование // Журнал зарубежного и сравнительного правоведения. 2018. № 6. С. 129—133.

⁶ См.: Бурдина Е. В. Развитие судебной системы в условиях информационного общества // Российское правосудие. 2018. № 7. С. 19—33.

⁷ См., например: Муратова Н. Г., Сергеев М. С. Правовое регулирование применения электронной информации и электронных носителей информации в уголовном судопроизводстве: отечественный и зарубежный опыт: монография. М.,

доказательств электронной информации. При этом следует учитывать, что правовые системы, а также уровень развития информационно-цифровых технологий в каждой стране имеет свои особенности.

Прежде всего следует обратить внимание на имеющиеся межгосударственные усилия по внедрению электронных доказательств в уголовное судопроизводство. Это связано с развитием высокотехнологичной транснациональной преступности в киберпространстве, появлением новых видов общественно опасных деяний в сфере электронной торговли и цифровой экономики. Происходящие тенденции потребовали разработки новых подходов к деятельности судебных и правоохранительных органов, процедур сбора электронных доказательств и механизмов международного сотрудничества по уголовным делам. Не случайно в рамках Организации Объединенных Наций, Совета Европы, ряда других универсальных организаций приняты основополагающие документы, содержащие международно-правовые принципы и стандарты применения электронных форм фиксации, передачи и использования информации о преступлении.

Одним из первых документов в данном направлении является Декларация принципов и программа действий ООН в области предупреждения преступности и уголовного правосудия 1991 г., в которой были рекомендованы меры, направленные на борьбу с общественно опасными деяниями, связанными с использованием высоких технологий и компьютеров. В частности, государствам предложено:

- на национальном уровне разработать и применить нормы и процедуры для выявления и расследования вышеуказанных преступлений;

- обеспечить правоохранительные органы необходимым оборудованием и обучить сотрудников для эффективного расследования транснациональных преступлений;

- разработать телекоммуникационное оборудование, сетевое программное обеспечение и другие соответствующие продукты и услуги для предупреждения преступлений, облегчения их выявления, расследования и уголовного преследования.

Прямым развитием идей Декларации ООН, в том числе тех, которые касаются использования при расследовании преступлений высоких технологий, явилась разработка Конвенции о преступности в сфере компьютерной информации 2001 г. Данный документ является всеобъемлющей основой для разработки национального законодательства, в том числе и относительно сбора доказательств в электронной форме уголовного преступления (ст. 14 (2)). В частности, в нем содержатся конкретные положения:

- о разработке процессуальных законодательных мер для того, чтобы правоохранительные органы смогли сохранить легко изменяемые электронные доказательства наиболее эффективно, включая оперативное обеспечение сохранности данных, обыск и выемку хранимых компьютерных данных, перехват данных и т. д.;

- о международном сотрудничестве через общие (выдача, взаимная правовая помощь и др.) и специальные процессуальные меры (оперативное обеспечение данных, доступ к хранящимся данным, перехват телекоммуникационных сообщений, создание контактных центров, работающих круглосуточно, и др.).

В докладе Генерального секретаря ООН, сделанном в апреле 2013 г. в г. Вене, особо отмечено, что для расследования преступлений правоохранительным органам необходимо использовать как традиционные, так и новые методы работы полиции. Повышенное внимание уделено электронным доказательствам, под которыми понимаются существующие в электронной (или цифровой) форме средства, при помощи которых в ходе судебного разбирательства устанавливаются факты, касающиеся виновности или невиновности лица. Они могут представлять собой хранимые или временные данные, существовать в виде компьютерных файлов, электронных журналов, метаданных или сетевых данных.

Указывается, что некоторые следственные действия, в основе которых лежит пространственный, ориентированный на предметы подход, трудно применять в ситуациях, связанных с хранением электронных данных и потоками данных в режиме реального времени. В связи с этим следует развивать возможности получения доказательств с помощью таких специализированных методов, как: обыск компьютерного аппаратного обеспечения или компьютерных данных; выемка компьютерного аппаратного обеспечения или компьютерных данных; распоряжение о предоставлении информации о подписчиках; распоряжение о предоставлении хранимых данных о потоках информации; распоряжение о предоставлении хранимых данных о содержании; сбор в режиме реального времени данных о потоках информации; сбор в режиме реального времени информации о содержании данных; оперативное обеспечение сохранности компьютерных данных; использование удаленной компьютерно-технической экспертизы; трансграничный доступ к компьютерной системе или данным.

Возникают трудности в осуществлении взаимодействия между правоохранительными органами и поставщиками услуг Интернета, располагающими информацией об абонентах, счетами-фактурами, некоторыми журналами связи, информацией о местоположении (например, поставщики услуг мобильной связи имеют информацию с антенн сотовой связи) и содержании данных. Все это может представлять со-

правовых систем таких зарубежных стран, как Австрия, Германия, Дания, Италия, Канада, Нидерланды, Саудовская Аравия, США, Швеция, Южная Корея и др.

бой важнейшие электронные доказательства совершения того или иного преступления.

Отмечена возрастающая роль судебной цифровой экспертизы, целью которой является восстановление нередко неустойчивой и легко подверженной искажению информации, имеющей особую доказательную ценность. В ходе производства подобного рода экспертных исследований применяются новые методы по созданию копий хранимой и удаленной информации по принципу «бит в бит», «блокировке записи» для предотвращения внесения изменений в исходные данные, использованию криптографических хэш-кодов или цифровых подписей, показывающих наличие изменений в информации.

Сделаны выводы, что применение традиционных средств официального международного сотрудничества в вопросах противодействия преступности в настоящее время не позволяет обеспечить своевременное и эффективное реагирование, необходимое для получения неустойчивых электронных доказательств. Расследование все чаще связано с обнаружением и сбором подобного рода доказательств, имеющих не только в конкретном государстве, но и далеко за его пределами. В мире облачных вычислений и центров данных следует по-новому подойти к пониманию «местонахождения» электронных и иных доказательств, других вопросов, связанных с необходимостью получения прямого доступа правоохранных органов к экстерриториальным данным о совершенном общественно опасном деянии¹⁰.

Значительную деятельность в консолидации межгосударственных усилий по внедрению электронных доказательств в уголовное судопроизводство осуществляет Совет Европы. В его документах определены базовые стандарты и принципы повышения эффективности взаимной правовой помощи в рассматриваемом направлении, которые эта универсальная организация требует эффективно применять на национальном уровне.

В частности, Европейским парламентом в октябре 2017 г. принята Резолюция о борьбе с киберпреступностью¹¹, в которой особо выделяются проблемы доступа правоохранных органов к электронным доказательствам через границы. Указана необходимость разработки европейской правовой основы для сохранения, предоставления и получения элек-

тронных доказательств. Предложено гармонизировать правила для определения статуса иностранного и внутреннего поставщика услуг, наложить на него обязанность отвечать на запросы государств-членов, основанные на надлежащей правовой процедуре.

В рассматриваемой сфере деятельности следует выделить утвержденный в 2018 г. Европейским парламентом Регламент по получению электронных доказательств в ходе расследования и судебного преследования преступников на территории Европейского Союза¹². Данный документ закрепляет конкретные механизмы сотрудничества судебных и правоохранительных органов в эпоху цифровых технологий. В нем предусмотрены определенные инструменты, позволяющие противостоять современным формам преступности, а также ускорять процесс защиты и получения электронных доказательств.

Среди ключевых новелл, предусмотренных в указанном Регламенте, можно выделить:

- введение европейских ордеров на предоставление электронных доказательств независимо от местонахождения данных;

- использование запрашиваемых данных только для тех целей, для которых они были получены (исключение составляет необходимость предотвращения непосредственной и серьезной угрозы общественной безопасности государства-эмитента или его основным интересам);

- установление 10-дневного предельного срока для выполнения запроса. В экстренных случаях данный срок может быть ограничен до шести часов. В случае если европейский ордер на предоставление электронных доказательств касается данных об абонентах и доступе к ним, он может быть отправлен без предварительной проверки компетентным судебным органом;

- закрепление ответственности за неисполнение европейского ордера на предоставление электронных доказательств в виде применения денежных санкций в размере до 2% от общемирового годового оборота предыдущего финансового года;

- разработка системы специальных уведомлений относительно защиты запрашиваемой информации определенными иммунитетами и привилегиями, подчинения правилам ограничения уголовной ответственности, связанной со свободой слова (прессы) и др.

Обращается внимание, что в странах Европейского Союза имеются разнообразные подходы в отношении электронных доказательств по уголовным делам. В связи с этим была принята Директива, обязывающая назначать своего законного представителя

¹⁰ См.: Содействие деятельности по борьбе с киберпреступностью, включая оказание технической помощи и наращивание потенциала: доклад Генерального секретаря ООН. Вена, 22—26 апреля 2013 г. URL: http://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2017/other_relevant_documentation/E_CN_15_2013_24_R.pdf.

¹¹ European Parliament Resolution of 3 October 2017 on the Fight Against Cybercrime (2017/2068(INI)). URL: <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2017-0366&format=XML&language=EN>.

¹² См.: Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters. Strasbourg 17.04.2018. URL: <http://eur-lex.europa.eu/legal-content/EN/TXT/DOC>.

в Союзе для получения, соблюдения и обеспечения исполнения решений, направленных на сбор доказательств компетентными национальными органами в рамках уголовного судопроизводства¹³.

Предусмотренные в Директиве положения направлены на определение четкого адресата запросов, нацеленных на сбор электронных доказательств в уголовном процессе. Это, в свою очередь, облегчит выполнение европейских ордеров, поскольку законный представитель несет персональную ответственность за неисполнение имеющихся в запросе требований о предоставлении электронных доказательств. Например, в Федеративной Республике Германия уже принят нормативный акт, предусматривающий конкретные штрафные санкции¹⁴.

Рассматривая вопросы использования электронной информации в качестве доказательств по уголовному делу, нельзя не затронуть международные документы, разрабатываемые на региональном уровне Содружеством Независимых Государств. В связи с развалом единой правовой структуры СССР возникла масса проблем в расследовании и судебном разбирательстве уголовных дел. Прозрачность государственных границ между бывшими республиками Советского Союза позволяет преступникам активно объединяться и совершать общественно опасные деяния на международном уровне.

Отметим, что определенную роль при решении возникающих проблем уголовного судопроизводства и доказывания обстоятельств преступления играют двусторонние и многосторонние межведомственные соглашения и договоренности. Но эти документы, как правило, носят временный характер и призваны обеспечить взаимодействие и сотрудничество между правоохранительными органами различных стран на период подготовки и принятия межгосударственных договоров об оказании взаимной правовой помощи в сфере применения уголовного законодательства.

В рамках проводимого исследования необходимо выделить Соглашение о сотрудничестве государств — участников СНГ в борьбе с преступлениями в сфере компьютерной информации, подписанное в июне 2001 г. в г. Минске. Данным документом определены основные формы сотрудничества в рассматриваемой сфере деятельности, в частности:

создание информационных систем, направленных на эффективное обеспечение выполнения задач по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере компьютерной информации;

проведение совместных научных исследований по представляющим взаимный интерес проблемам борьбы с преступлениями в данном направлении;

обмен соответствующими нормативными правовыми актами, научно-технической литературой по проблемам борьбы с преступлениями в сфере компьютерной информации.

Программой сотрудничества государств — участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий, на 2016—2020 гг.¹⁵ предусмотрен комплекс различного рода мероприятий, направленных прежде всего на совершенствование международно-правовой базы взаимодействия в рассматриваемой области.

Так, одной из организационно-правовых мер сотрудничества является рассмотрение вопроса о целесообразности присоединения к основным договорам, заключенным в рамках ООН, СНГ и других международных организаций в сфере борьбы с преступлениями, совершаемыми с использованием информационных технологий. Следует регулярно осуществлять анализ национального законодательства в целях выработки рекомендаций по его дальнейшему совершенствованию.

Среди организационно-практических мероприятий выделена необходимость развития сотрудничества в области разработки, производства, поставки и оказания помощи правоохранительным органам по внедрению специальных программно-технических средств, необходимых для обнаружения, фиксации, изъятия и исследования следов преступлений, совершаемых с использованием информационных технологий.

Особый акцент сделан на информационном и научном обеспечении сотрудничества между странами СНГ путем обмена передовыми технологиями, проведения совместных научных исследований по вопросам борьбы с преступлениями, совершаемыми с использованием информационных технологий. Указанные и иные мероприятия призваны выявить новые формы электронных доказательств; усовершенствовать механизм обмена информацией в методике и тактике выявления, раскрытия, расследования и судебной практике рассмотрения различных категорий уголовных дел.

Практический пример взаимодействия правоохранительных органов разных стран по борьбе с преступлениями в области высоких технологий можно

¹³ См.: Proposal for a Directive of the European Parliament and of the Council laying down harmonised Rules on the Appointment of legal Representatives for the Purpose of gathering Evidence in criminal proceedings. Strasbourg. 01.07.2018. URL: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:226:FIN>.

¹⁴ См.: Network Enforcement Act. Regulatory Fining Guidelines. Guidelines on Setting Regulatory Fines within the Scope of the Network Enforcement Act (Netzwerkdurchsetzungsgesetz — NetzDG) of 22.03.2018. URL: http://www.bmjjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/NetzDG_Bu%C3%9Fgeldleitlinien_engl.pdf.

¹⁵ Утв. Советом глав государств 15 сентября 2016 г. URL: <http://cis.minsk.by/reestr/ru/index.html#reestr/view/text?doc=5476>.

проиллюстрировать положениями Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола¹⁶. В частности, взаимодействующие стороны в процессе расследования преступлений по соответствующим запросам могут получить информацию: о сетевых адресах, именах доменов и серверов организаций и пользователей; содержании протоколов, трейсингов, логических файлов; об электронной информации, заблокированной в порядке оперативного взаимодействия правоохранительных органов при пресечении трансграничных правонарушений; о провайдерах и дистрибьюторах сетевых и телекоммуникационных услуг; физических и юридических лицах, имеющих отношение к преступлениям в сфере высоких технологий; специализированном программном обеспечении, методиках и тактике борьбы с компьютерными и телекоммуникационными преступлениями.

Повышенное внимание уделяется особенностям использования электронной информации в качестве доказательств в уголовном судопроизводстве ряда стран, в которых сделаны значительные шаги по разработке и совершенствованию законодательства в рассматриваемом направлении.

Среди развитых зарубежных стран США имеют уникальный опыт по формированию цифровых доказательств, что является одним из основных прикладных направлений использования информационно-цифровых технологий в уголовном судопроизводстве¹⁷. В этой стране под электронными (цифровыми) доказательствами понимается любая информация, которая хранится или передается в цифровой форме и которую сторона уголовного процесса может использовать в качестве доказательства в судебном разбирательстве¹⁸. Цифровые доказательства, такие как, например, прослушивание или мониторинг сетевого трафика или изготовление цифровых копий (криминалистические изображения, копии файлов и т. д.), могут быть получены путем поиска, задержаний и проверок, путем принудительного или добровольного их изъятия.

Под цифровой информацией подразумевается любая информация в цифровой форме, которая может быть разделена на контент (например, текстовый документ, рисунок или фотографию, базу дан-

ных и т. д.) и информацию об этом контенте (метаданные). Часто невозможно обрабатывать цифровую информацию, не получая сведений о конкретном наборе данных или цифровом документе, которые описывают, как, когда и кем информация была представлена, создан или осуществлен доступ к набору данных или цифровому документу или в документ внесены изменения¹⁹.

Отметим, что в США процедуры доказывания с использованием цифровых доказательств по уголовному делу более подробно регламентируются в Руководстве по поиску и собиранию электронных доказательств²⁰. В соответствии с данным нормативным актом электронные доказательства классифицируются на прямые и косвенные.

К прямым доказательствам относятся те, которые сгенерированы ЭВМ без участия человека и подразделяются на две категории: 1) записи, созданные компьютером; 2) записи, хранящиеся в памяти ЭВМ.

Косвенные доказательства содержат результат деятельности человека (письма, памятки, документы бухгалтерского учета и т. д., созданные людьми), к ним применяются правила исследования косвенных доказательств.

С учетом происхождения выделяются две группы компьютерных доказательств: 1) результаты деятельности человека, хранящиеся на электронном носителе (жестком диске, флоппи-диске, компакт-диске, стримере) и содержащие информацию, внесенную пользователем; 2) доказательства, созданные компьютером в соответствии с заложенной программой и представляющие собой результат обработки тех или иных начальных данных.

Также в данном документе содержатся иные классификации электронных доказательств, где критерием разграничения является их сущность, форма представления.

В Руководстве по поиску и собиранию электронных доказательств определен ряд требований к электронному документу как процессуальному доказательству.

В частности, участник уголовного судопроизводства обязан доказать аутентичность электронного документа при помощи стандартной процедуры его аутентификации, как и любой другой записи, в соответствии с неполным списком Федеральных правил доказывания. В целях демонстрации аутентификации записей, сгенерированных компьютером, сторона уголовного судопроизводства должна представить описание процесса или систему, используемую

¹⁶ См. приказ МВД России, Минюста России, ФСБ России, ФСО России, ФСКН России и ФТС России от 6 октября 2006 г. № 786/310/470/454/333/971 «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола».

¹⁷ См.: *Сергеев М. С.* Электронные доказательства в уголовном судопроизводстве. Опыт США // *Вестник экономики, права и социологии*. 2016. № 2. С. 206—212.

¹⁸ См.: *Casey E.* Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet. 3rd ed. Baltimore, 2011. P. 7.

¹⁹ См.: Chapter on Digital Evidence Gathering. 2014. URL: <http://www.internationalcompetitionnetwork.org/uploads/library/doc1006.pdf>.

²⁰ См.: Searching and Obtaining Electronic Evidence Manual. 2009 // United States Department of Justice. URL: <http://cybercrime.Gov/ssmanual/05ssma.html>.

для получения результата, и показать, что процесс или система производят точный результат.

Если компьютерная программа используется не на постоянной основе, сторона обвинения или защиты обязана раскрыть, какие именно операции было поручено выполнять компьютеру, а также точные инструкции, которые были даны ЭВМ.

Определяя подлинность записей ЭВМ, законодательство США опирается: на постулат о том, что в отсутствие конкретных доказательств произошедшего вмешательства сама возможность такого вмешательства не влияет на достоверность компьютерной записи; правило о лучшем доказательстве, не требующем представления оригинала записи в суд²¹; ограничение предоставления в суд «сборников» компьютерных распечаток²².

В отношении электронного документа, являющегося косвенным доказательством, закреплены положения: о неприменении правил о косвенных доказательствах к электронным документам, сгенерированным ЭВМ; о применении правил о косвенных доказательствах в отношении записей, хранящихся в ЭВМ.

Отдельное место в Руководстве по поиску и собиранию электронных доказательств уделено освещению правовых и практических вопросов, связанных с оформлением документов для получения разрешения на извлечение информации из компьютеров и компьютерных устройств; установления оснований и порядка получения доказательственной информации из компьютерных сетей, от провайдеров, а также из электронной почты.

Особо устанавливается, что сотрудники органов расследования вправе: осуществлять электронное наблюдение в режиме реального времени в целях установления «клонированных» учетных записей, определения местонахождения сотового телефона или компьютера подозреваемого; прослушать телефон подозреваемого или узнать, кому звонил данный участник уголовного судопроизводства.

В Великобритании сотрудник полиции, осуществляющий расследование преступления, должен иметь возможность фиксировать доказательства в цифровом виде на месте преступления (в частности, показания потерпевших и свидетелей), принимать заявления и загружать информацию по делу с помощью мобильных устройств. Впоследствии данная цифровая информация передается в Королевскую прокурорскую службу для принятия решения о предъявлении подозреваемому лицу обвинения. Собранные по делу электронные доказательства без их дублирования на бумажном носителе в дальнейшем исследу-

ются в суде и используются им для принятия итогового решения по уголовному делу.

Отметим, что в Шотландии также предполагается полный отказ от бумажного формата уголовного дела и использование Системы хранения цифровых доказательств²³. Данная Система предназначена для работы с различного вида доказательствами, получения к ним доступа со стороны уполномоченных на то участников уголовного судопроизводства.

Сотрудники полиции Англии, Уэльса и Северной Ирландии в своей деятельности при расследовании преступлений опираются на Руководство по работе с цифровыми доказательствами²⁴. Данным документом устанавливаются определенные требования к лицам, участвующим в собирании электронных доказательств, а также в идентификации цифровой информации, необходимой для расследования преступлений.

Основными принципами работы с цифровыми доказательствами по делу являются: неизменяемость полученных данных, которые впоследствии могут быть использованы в суде; компетентность должностных лиц относительно изъятых доказательств, последствий и содержания своих действий; ведение записей всех процессов, применяемых к цифровым доказательствам; ответственность должностных лиц, осуществляющих расследование, за реализацию принципов работы с цифровыми доказательствами.

В Руководстве по работе с цифровыми доказательствами содержится общая характеристика компьютерных средств и других телекоммуникационных устройств как потенциальных источников цифровой доказательственной информации. Особое место в данном документе уделено регламентации правового порядка обнаружения, фиксации и изъятия цифровых устройств на месте происшествия и в ходе производства иных следственных действий. В частности, сотрудникам полиции предлагаются алгоритмы действий по подготовке, использованию различного рода технических устройств, предназначенных для закрепления вещественных цифровых доказательств на месте происшествия. Содержатся положения относительно получения в ходе расследования цифровых доказательств в режиме онлайн (например, связанных с веб-сайтами, форумами и блогами). Имеются рекомендации, связанные с фиксацией данных и направленные на недопустимость разглашения деятельности органов полиции в данном направлении перед владельцем веб-сайта.

²³ URL: http://www.publiccontractsscotland.gov.uk/Search/show/Search_View.aspx?ID=FEB310609.

²⁴ См.: Good Practice Guide for Digital Evidence. Version 5 (October 2011) // Association of Chief Police Officers of England, Wales & Northern Ireland. URL: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.

²¹ См.: Federal Rules of Evidence. 2017 ed. Art. 1002. URL: <http://judiciary.house.gov/wp-content/uploads/2013/07/Evidence2016.pdf>.

²² См.: Federal Rules of Evidence. Art. 1006.

В рассматриваемом документе также содержится анализ ряда дополнительных документов, регламентирующих процедуру изъятия компьютерных устройств и цифровой информации²⁵. Раскрываются процессы, связанные с надлежащим оформлением полицейских протоколов и позволяющие должным образом обеспечить допустимость цифровых доказательств.

В большинстве европейских стран, представляющих романо-германскую правовую семью, допустимость электронных доказательств в ходе предварительного расследования и судебного разбирательства уголовного дела, как правило, регулируется общими положениями уголовно-процессуального законодательства о традиционных доказательствах.

Например, в уголовно-процессуальном законодательстве ФРГ среди процессуальных действий, направленных на получение доказательств обстоятельств совершенного общественно опасного деяния, предусмотрены контроль телекоммуникации, прослушивание и запись высказываний, сделанных непублично, применение технических средств и др.

В частности, УПК Германии позволяет производство контроля и записи телекоммуникации в отношении обвиняемого и других лиц, если имеются основания полагать, что они передают или принимают сообщения, предназначенные для виновного в совершении преступления, а также исходящие от него (§ 100a абз. 3). При этом положения законодательства распространяются на любой вид телекоммуникации: передача информации по телефону, факсу, посредством телеграфии, с помощью компьютерной техники.

Также в УПК ФРГ предусмотрен технический контроль телекоммуникационного оборота, позволяющий получить информацию о связи. Это может быть номер абонентской карты, идентификационный номер мобильного телефона и динамические IP-адреса компьютеров, время начала и окончания соединения и др. Указанное процессуальное действие допускается по делам о преступлениях, совершенных при помощи средств коммуникации (§ 100a абз. 2).

Согласно § 100i УПК ФРГ допускается применение пеленгатора IMSI в целях установления идентификационного номера прибора (IMEI), идентификатора абонента (IMSI), а также местонахождения мобильного телефона.

Информация, содержащаяся на компьютере обвиняемого, включая полученные или отправленные им

электронные письма, может быть изъята в соответствии с общими положениями процессуального законодательства о выемке, установленными в § 94—98 УПК ФРГ. Аналогично может быть получена информация, содержащаяся на сим-карте мобильного телефона обвиняемого (об исходящих и входящих звонках, времени разговора и телефонном номере собеседника и др.).

Уголовно-процессуальное законодательство Германии допускает проведение автоматического сравнения и передачу личных данных лиц, соответствующих определенным признакам, которыми предположительно обладает обвиняемый. Данное сравнение осуществляется прежде всего с целью исключения лиц, которые не подозреваются в совершении преступления, а также установления лиц, обладающих определенными признаками, имеющими существенное значение для расследуемого дела (§ 98a УПК ФРГ).

В соответствии с § 100f УПК ФРГ допускается прослушивание и запись высказываний, сделанных непублично. Данная мера может применяться при совершении тяжких и особо тяжких преступлений при наличии указанных в законе оснований к обвиняемому и иным лицам, в отношении которых существует предположение, что они состоят в контакте с лицом, виновным в совершении общественно опасного деяния. Отметим, что прослушивание и запись высказываний, сделанных непублично, может быть осуществляться только в том случае, если не будут зафиксированы такие высказывания, которые относятся к внутренней сфере частной жизни (§ 100с абз. 4 УПК ФРГ). Если же в процессе применения указанной меры это все-таки произойдет, то прослушивание незамедлительно прерывается, а уже сделанные записи уничтожаются (§ 100с абз. 5 УПК ФРГ).

Кроме того, согласно § 100h УПК ФРГ возможно применение технических средств при наличии простого первичного подозрения лица в совершении преступления, если установление обстоятельств дела или местонахождение виновного иным способом установить невозможно. К таким техническим средствам относятся фото-, кино- и видеосъемка, приборы ночного видения, пеленгаторы, передатчики GPS и др.

Также уголовно-процессуальное законодательство Германии содержит положения относительно защиты данных в ходе расследования уголовного дела и применимые к электронным доказательствам. В них содержатся предписания относительно соблюдения определенных мер по сохранению личных данных, полученных из различных баз. При этом подробно регламентируются условия для уничтожения электронных данных, не относящихся к делу (§ 101 УПК ФРГ)²⁶.

²⁵ См.: Forensic Science Providers: Codes of Practice and Conduct. URL: <http://www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct>; Digital Imaging Procedure. URL: <http://www.bwvsg.com/wp-content/uploads/2013/07/Home-Office-Digital-Imaging-Procedure-Nov-07.pdf>; Storage, Replay and Disposal of Digital Evidential Images. URL: <http://library.college.police.uk/docs/APPref/storage-replay-and-disposal.pdf>.

²⁶ См.: Головинков П., Спича Н. Уголовно-процессуальный кодекс Федеративной Республики Германия —

В Законе об уголовном процессе Испании предусмотрены такие электронные доказательства, как средства воспроизведения слов, звуков и изображения, а также инструменты, разрешающие или воспроизводящие слова, цифры и математические операции, выполняемые для целей бухгалтерского учета или других целей, относящихся к судебному разбирательству.

Согласно Уголовному кодексу Италии под электронным документом понимается любой компьютерный инструмент, который содержит информацию с доказательственной значимостью или любым указанным программным обеспечением для обработки такой информации.

Допустимость в качестве доказательств цифровых документов предусмотрена по законодательству Бельгии, Голландии, Португалии, Румынии, Финляндии и ряда других стран.

Таким образом, в законодательстве стран Европы отсутствуют конкретное определение электронных доказательств по уголовным делам, а также правила их допустимости в ходе расследования и судебного разбирательства уголовного дела. Как правило, электронные документы сопоставляются с бумажными документами для придания им ценности в качестве доказательств.

Представляют интерес результаты проведенного опроса европейских судей относительно возможностей использования электронных доказательств по уголовному делу. Так, подавляющее большинство опрошенных признают электронные доказательства как эквивалент традиционных доказательств. Относительно их надежности высказываются противоположные мнения. Одни судьи полагают, что электронные доказательства более надежные в силу их объективности и точности, так как содержащаяся в них информация исходит из электронного документа, в котором отсутствует какая-либо субъективность по сравнению с такими доказательствами, как, например, показания потерпевших и свидетелей. Другие судьи считают электронные доказательства более уязвимыми по сравнению с традиционными ввиду отсутствия эффективных средств для проверки подлинности электронного документа. При этом отмечаются сложности в установлении юридической ценности электронных доказательств из-за отсутствия ясного правового регулирования данных правоотношений, трудности их хранения, а также возможность манипулирования такими доказательствами, что вызывает определенные проблемы в случае установления их подлинности.

Особого внимания требуют предлагаемые европейскими учеными и практиками меры, связанные с допустимостью электронных доказательств в хо-

де расследования и судебного разбирательства уголовного дела. В частности, обосновывается необходимость на законодательном уровне предусмотреть положения, позволяющие: уменьшить степень незащищенности электронных документов; собирать, сохранять и предоставлять в суде электронные доказательства, наделенные надлежащими юридическими гарантиями²⁷.

Среди государств постсоветского пространства повышенный интерес вызывает уголовно-процессуальное законодательство Грузии, которое содержит положения, предусматривающие производство следственных действий по собиранию и проверке электронных доказательств.

В частности, согласно ч. 1 ст. 136 УПК Грузии допускается истребование документа или информации в случае наличия обоснованного предположения о том, что в компьютерной системе или средстве хранения компьютерных данных содержится информация или документ, имеющие значение для уголовного дела. Также при наличии оснований полагать, что лицо осуществляет преступное деяние с использованием компьютерной системы, у поставщика услуг может быть истребована информация о пользователе. Это может быть любая информация, которая хранится в форме компьютерных данных или любой иной форме, связанная с пользователями поставщика услуг, отличается от данных интернет-трафика и содержательных данных. Благодаря такой информации можно определить: тип используемого коммуникационного обслуживания, используемые технические средства и время оказания услуги; личность, почтовый адрес или адрес места жительства, номер телефона и другие контактные номера пользователя, информацию о счетах и налогах, доступную на основании договора или соглашения об оказании услуг; любую другую информацию о местонахождении установленного коммуникационного оборудования, доступную на основании договора или соглашения об оказании услуг (ч. 2 и ч. 3 ст. 136 УПК Грузии).

Другим следственным действием, связанным с получением компьютерной информации по уголовному делу, является текущий сбор данных интернет-трафика, который допускается при наличии обоснованного предположения, что лицо осуществляет преступное деяние с использованием компьютерной системы. При этом на поставщика услуг возлагается обязанность по сотрудничеству с органами предварительного расследования и оказанию им помощи в сборе или записи в текущем режиме данных интернет-трафика, которые связаны с конкретными коммуникациями, осуществляемыми на территории Грузии и передаваемыми посредством компьютерной системы (ст. 137 УПК Грузии). При наличии преду-

Strafprozessordnung (StPO): науч.-практ. комментарий и перевод текста закона. Potsdam, 2012. С. 53—60.

²⁷ См.: Основы теории электронных доказательств / под ред. С. В. Зуева. М., 2019. С. 256—260.

смотренных в законе оснований также допускается текущий сбор содержательных данных, связанных с конкретными коммуникациями, осуществляемыми на территории Грузии и передаваемыми посредством компьютерной системы (ст. 138 УПК Грузии).

Кроме того, в августе 2014 г. УПК Грузии был дополнен новой ст. 143.1, в которой предусмотрена возможность производства следующих тайных следственных действий с использованием современных технических и электронных средств: а) скрытое прослушивание и запись телефонных переговоров; б) снятие и фиксация информации с канала связи (путем подсоединения к средствам связи, компьютерным сетям, линейным коммуникациям и станционной аппаратуре), с компьютерной системы (как непосредственно, так и дистанционно) и инсталляция в компьютерную систему с указанной целью соответствующих средств программного обеспечения; в) контроль почтовых отправлений и телеграфных сообщений (кроме дипломатической почты); г) скрытая видео- и аудиозапись, кино- и фотосъемка; д) электронное слежение при помощи технических средств, использование которых не причиняет вреда жизни, здоровью людей и окружающей среде.

При этом поиск и обнаружение необходимой по делу электронной или иной информации еще не превращает ее в доказательство по уголовному делу. Законодатель требует выполнения ряда требований по процессуальному оформлению и фиксации получаемой информации для ее трансформации в доказательство²⁸.

В другом государстве постсоветского пространства — Республике Казахстан — в 2014 г. принят новый Уголовно-процессуальный кодекс, в котором отражен предыдущий опыт развития уголовно-процессуального права страны, а также разумное восприятие и соотношение либеральных и радикальных начал, сложившихся в мировой правовой системе в ее классических исторических типах применительно к уголовному судопроизводству²⁹.

Одними из значимых новелл УПК РК являются нормы об использовании в ходе производства по уголовному делу цифровых доказательств. В частности, защитник или представитель потерпевшего вправе проводить опрос лиц, предположительно владеющих информацией по делу, с использованием научно-технических средств. Ход и результаты такого опроса могут быть отражены на электронном носителе, которые подлежат приобщению к уголовному делу и приобретают статус доказательства после их исследования и оценки органом, ведущим уголовный про-

цесс (п. 5 ч. 3 ст. 122 УПК РК). Законодатель разрешает целому ряду участников уголовного судопроизводства (подозреваемому, обвиняемому, защитнику, частному обвинителю, потерпевшему, гражданскому истцу, гражданскому ответчику и их представителям), а также любым гражданам и организациям предоставлять сведения в форме электронного документа для приобщения их в качестве доказательств к уголовному делу (ч. 4 ст. 122 УПК РК). Также допускается возможность производства дистанционного допроса потерпевшего и свидетеля в режиме видеосвязи (ст. 213 УПК РК).

В декабре 2017 г. в УПК РК был внесен ряд изменений и дополнений, направленных на цифровизацию производства по уголовному делу³⁰. В частности, закреплено положение, согласно которому судопроизводство допускается как в бумажном, так и в электронном формате. Решение об этом принимает должностное лицо, которому поручено осуществление досудебного расследования, при принятии дела к своему производству. Если отсутствует возможность дальнейшего ведения уголовного судопроизводства в электронном формате, то осуществляется переход на бумажный вариант (ст. 42-1 УПК РК).

Реализовать вышеуказанные положения закона позволяет информационная система «Электронное уголовное дело (е-УД)», разработанная в 2017 г. межведомственной рабочей группой Верховного Суда, Генеральной прокуратуры, Министерства финансов, Министерства внутренних дел, Агентства по делам государственной службы и противодействия коррупции. Электронное уголовное дело представляет собой обособленное производство, ведущееся органом уголовного преследования по поводу одного или нескольких уголовных правонарушений посредством функционала специального модуля е-УД в рамках общей электронной системы ведения досудебного расследования с момента регистрации до исполнения наказания.

Законодатель также наделил Генерального прокурора Республики Казахстан правом принятия нормативных правовых актов в пределах своей компетенции по вопросам ведения уголовного судопроизводства в электронном формате (п. 6 ст. 58 УПК РК). С учетом этого 3 января 2018 г. Генеральный прокурор РК утвердил Инструкцию, определяющую порядок ведения уголовного судопроизводства в электронном формате на стадии досудебного расследования (далее — Инструкция)³¹.

²⁸ См.: Уголовно-процессуальный кодекс Грузии. URL: <http://www.matsne.gov.ge>.

²⁹ См.: Когамов М. Ч. Что такое уголовно-процессуальное право и уголовный процесс Республики Казахстан. Алматы, 2013. С. 6—7.

³⁰ Закон Республики Казахстан от 21 декабря 2017 г. № 118-VI ЗРК «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам модернизации процессуальных основ правоохранительной деятельности».

³¹ См. приказ Генерального прокурора Республики Казахстан от 3 января 2018 г. № 2 «Об утверждении Инструкции о ведении уголовного судопроизводства в электронном формате».

Согласно данному документу производство по уголовному делу на стадии досудебного расследования в электронном формате осуществляется в модуле «Электронное уголовное дело» посредством: внесения необходимых учетных сведений и реквизитов электронных форм в информационную систему; создания электронных документов с помощью имеющихся шаблонов и документов в формате PDF; подписания участниками уголовного процесса электронных документов посредством электронной цифровой подписи или планшета подписи; электронного взаимодействия с судом для осуществления необходимых процедур, связанных с рассмотрением уголовных дел и материалов в электронном формате; электронного взаимодействия с экспертами и специалистами в целях получения заключений в электронном формате или в случае необходимости осуществления перевода бумажных материалов в такой формат и др.

Производство по уголовному делу ведется с использованием специальных электронных шаблонов документов, которые содержатся в информационной системе или автоматически формируются и вкладываются данной системой (сопроводительные письма, рапорты, уведомления и т. п.). Также к электронному уголовному делу по решению должностного лица, осуществляющего производство, приобщаются медиа-файлы (видео-, фото- и аудиоматериалы), процессуальные документы в формате PDF, оформленные ранее в бумажном формате (например, протокол осмотра места происшествия, протокол эксгумации), материалы проведенных негласных следственных действий.

Казахстанские ученые-процессуалисты отмечают несомненные преимущества перехода на электронный формат ведения уголовного судопроизводства, а также обращают внимание на следующие его недостатки:

отсутствие в действующем уголовно-процессуальном законодательстве специальных норм, регламентирующих процедуру ведения электронного уголовного дела;

недостаточность ведомственных нормативных актов, конкретизирующих правила пользователя электронного уголовного дела;

слабая техническая оснащенность рабочих мест должностных лиц, осуществляющих уголовное преследование;

отсутствие осведомленности у населения о возможности ведения электронного формата досудебного расследования и др.³²

³² См.: Сокурова Э. Ж., Аширбекова К. Б. Уголовное дело в электронном формате // Конституция: воплощение ценностей верховенства права, гражданского общества и современного государства: матер. междунар. науч.-практ. конф. Астана, 2018. С. 349.

В настоящее время Верховный суд Республики Казахстан решил вопрос о создании «Электронного зала судебного заседания», где предполагается отказ от бумажных носителей при проведении судебного разбирательства уголовного дела и перевод всех процессуальных документов в электронный формат. Одновременно проводятся мероприятия по внедрению в эту модель автоматизированных рабочих мест судей, прокуроров, адвокатов, потерпевших³³.

Необходимо отметить, что и в других государствах постсоветского пространства осуществляется переход на ведение уголовных дел в электронном формате. Например, в Республике Молдова с 1 июля 2017 г. сотрудники прокуратуры применяют автоматизированную информационную систему «Уголовное преследование: Е-дело». В данную систему вносится вся информация о предпринятых процессуальных действиях и мерах в рамках процедурных материалов и уголовных дел. Разработанная автоматизированная информационная система охватывает все этапы уголовного преследования, выполняемые или руководимые прокурором, который имеет доступ к уголовному процессу в реальном времени, сокращая тем самым задержки в принятии решений по тому или иному делу.

В ближайшее время система «Уголовное преследование: Е-дело» будет интегрироваться с модулями информационных систем МВД, Национального центра по борьбе с коррупцией, Таможенной службы, Министерства юстиции, Министерства информационных технологий и связи и других государственных структур Молдовы. Это также позволит вести унифицированный учет и информационное взаимодействие органов уголовного преследования, прокуратуры, судебных инстанций и органов исполнения наказания в виде лишения свободы. По мнению представителей правоприменительной практики, предстоящий переход от бумажного документооборота в ведении уголовных дел к электронному будет способствовать модернизации уголовного судопроизводства, а также улучшит доступ к процессуальной информации для всех участников процесса, создаст дополнительные возможности для их взаимодействия³⁴.

В Республике Узбекистан в соответствии с Указом Президента этой страны от 30 ноября 2017 г. № УП-5268 «О дополнительных мерах по усилению гарантий прав и свобод граждан в судебно-следственной деятельности» предполагается разработка и внесение предложений по дальнейшему совершенствованию законодательства и методологии расследования и рассмотрения уголовных дел; расширению использования современных информационно-комму-

³³ См.: Сокурова Э. Ж., Аширбекова К. Б. Указ. соч. С. 350.

³⁴ См.: Молдавская прокуратура начала вести уголовные дела в электронном виде. URL: <http://www.digital.report>.

никационных технологий в судебно-следственной деятельности, оптимизации и упрощению делопроизводства по уголовным делам, в том числе путем внедрения системы «Электронное уголовное дело». Указанные меры направлены прежде всего на модернизацию уголовного судопроизводства (пересмотр его принципов, разработку новой модели досудебного и судебного производства, усиление гарантий прав участников уголовного процесса, повышение открытости, доступности и оперативности правосудия, а также устранение избыточного формализма). В результате предполагается полный отказ от бумажного уголовного судопроизводства с переходом к электронному уголовному делу.

В Узбекистане ожидается, что это позволит: сократить сроки уголовного судопроизводства; улучшить доступ к процессуальной информации всех участников судопроизводства; создать дополнительные возможности обеспечения права на защиту соответствующих участников уголовного процесса; сократить процессуальные издержки; улучшить систематизацию и структурирование материалов уголовного дела; снизить риски фальсификации материалов уголовного дела; повысить транспарентность правосудия по уголовным делам³⁵.

Информационные автоматизированные системы, связанные с производством уголовного дела в электронном формате, уже внедрены или еще внедряются в ряде государств постсоветского пространства: Грузии, Украине, Эстонии и др.

Подводя итог, отметим повышенное внимание международного сообщества к выработке и закреплению в соответствующих актах нормативных положений, предусматривающих различные возможности использования электронной информации в качестве доказательств по уголовному делу. С учетом этого появился ряд крупных международных инициатив и документов, направленных на повышение эффективности сотрудничества в сфере расследования преступлений, имеющих транснациональный и трансграничный характер. Взаимодействие правоохранительных органов различных государств в данном направлении возможно только на основе совершенствования национального законодательства с учетом экстерриториальной локализации электронных доказательств, необходимости цифровизации уголовно-процессуальной и криминалистической деятельности.

Исследование правовых, организационных и иных проблем, связанных с применением электронных доказательств в современных системах права, показало, что до сих пор не решен вопрос о трансграничном доступе к ним. Среди универсальных

международных организаций следует выделить Совет Европы, который предпринимает определенные меры в данном направлении, в частности с помощью разработки и функционирования согласованной правовой основы, позволяющей направлять судебные приказы непосредственно внешним и внутренним поставщикам услуг. Новизна сотрудничества правоохранительных органов по получению электронных доказательств заключается в создании эффективно действующего механизма взамен старого, основанного на взаимной правовой помощи государств, который исполнялся несколько месяцев или вообще не исполнялся ввиду различного рода ограничений.

Перед международным сообществом стоит задача по поиску разумного компромисса между неприкосновенностью частной жизни и публичным интересом при расследовании преступлений при использовании электронной информации в качестве доказательств по уголовному делу. В национальном уголовно-процессуальном законодательстве должны быть закреплены основные правовые гарантии, разработанные и закрепленные в международных документах, удовлетворяющие представлениям о справедливом правосудии. Среди них — более четкое изложение обстоятельств, при которых органы предварительного расследования и судебного разбирательства вправе производить процессуальные действия, направленные на обнаружение и сбор электронных доказательств. При этом следует учитывать необходимость соблюдения основных положений неприкосновенности частной жизни граждан, недопущения злоупотреблений в сфере защиты охраняемой законом информации.

Законодательство зарубежных государств по мере развития научно-технического прогресса, совершенствования компьютерной техники, появления новых видов коммуникаций между людьми включает все новые виды правовых средств, направленных на использование современных технологий для собирания доказательственной цифровой информации в ходе производства по уголовному делу. В большей степени это проявляется в сфере развития телефонной связи, электронного наблюдения, деятельности по изъятию информации в компьютерных сетях, созданию электронного документооборота, в конечном счете — формированию доказательств.

Электронные доказательства характеризуются особым объемом, источниками образования и хранения, трудностями выявления, фиксации, изъятия, легкой изменчивостью и др. Учитывая данные обстоятельства в зарубежных странах, наряду с уголовно-процессуальными нормами имеются различные рода документы (руководства, инструкции, положения, рекомендации), в которых конкретизируются процедуры работы с доказательствами подобного рода.

³⁵ См.: Тухташева У. А. Модернизация уголовного судопроизводства и усиление гарантий прав человека. URL: <http://www.napostu.uz/xabarlar/370>.

В США, Великобритании и ряде других стран, которым свойствен состязательный тип уголовного процесса, понятие доказательства более широкое (без указания на конкретный источник его получения), что позволяет правоохранительным органам более свободно использовать электронные доказательства в доказывании по уголовным делам.

Изучение зарубежной практической уголовно-процессуальной деятельности свидетельствует, что современные объемы и виды различной цифровой доказательственной информации побуждают законодателя активнее внедрять в уголовное судопроизводство электронный документооборот.

Повышенное внимание в зарубежном законодательстве при использовании информационных технологий и собирании цифровых доказательств уделяется компетентности должностных лиц, осуществляющих предварительное расследование и судебное разбирательство уголовного дела. Данные лица должны обладать специальными знаниями и пройти соответствующую подготовку.

Возможность использования электронного документа в качестве доказательства в нашей стране осложняется рядом проблем: а) в настоящее время определены условия только равнозначности электронного документа (подписанного электронной подписью) и документа на бумажном носителе при отсутствии собственно равенства между электронным документом и документом на бумажном носителе; б) при использовании электронного документа в качестве доказательства по уголовным делам основной акцент делается на материальную составляющую информационного объекта, но никак не на его информационную компоненту; в) не определены место и роль электронного документа в качестве доказательства по уголовным делам; г) не предпринимаются меры по интеграции подходов в данном вопросе с существующими международными соглашениями и практическими наработками в данной сфере в других государствах³⁶.

С учетом имеющегося в Российской Федерации несоответствия фактического и нормативно обусловленного использования цифровых технологий в уголовном судопроизводстве возникает необходимость в совершенствовании уголовно-процессуального законодательства при использовании электронных до-

казательств. Имеются все основания для определения основных направлений его развития:

закрепление принципов применения цифровых технологий, более подробной регламентации уголовно-процессуальной формы следственных и судебных действий, производимых с их использованием;

расширение пределов допустимости доказательств и появление новых источников фактических данных; увеличение количества следственных и судебных действий;

применение цифровых технологий при принятии процессуально значимых решений по уголовному делу.

В дальнейшей разработке нуждаются определение «цифровые доказательства», основные критерии их допустимости, относимости и достоверности. Перечень доказательств, содержащийся в ч. 2 ст. 74 УПК РФ, подлежит расширению за счет допуска: показаний (подозреваемого, обвиняемого, потерпевшего, свидетеля, эксперта, специалиста) в электронно-цифровой форме; заключений (эксперта, специалиста) в электронно-цифровой форме; электронных вещественных доказательств; электронных следственных и судебных действий.

На законодательном уровне следует закрепить применение электронно-цифровых документов, составляемых сторонами защиты и обвинения в ходе фиксации хода и результата следственных и судебных действий, направленных на получение необходимой доказательственной информации по уголовному делу. Должно быть допустимым предоставление информации любым способом, обеспечивающим надежность ее сохранения и передачи в электронном виде в надлежащий правоохранительный орган или уполномоченному должностному лицу. В перспективе следует перейти на исключительно электронный документооборот в уголовном судопроизводстве³⁷.

³⁷ См.: Развитие информационных технологий в уголовном судопроизводстве. С. 162—175; Кувычков С. И. Использование в доказывании по уголовным делам информации, представленной в электронном виде: дис. ... канд. юрид. наук. Н. Новгород, 2016. С. 188; Андреева О. И., Зайцев О. А. Перспективы ведения российского уголовного судопроизводства в электронном формате // Уголовная юстиция. 2018. № 12. С. 57—62; Андреева О. И., Зайцев О. А. Проблемы использования в уголовном судопроизводстве электронных доказательств // Правовые проблемы укрепления российской государственности: сб. ст. Томск, 2018. Ч. 79. С. 4—16.

³⁶ См.: Развитие информационных технологий в уголовном судопроизводстве. С. 57.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

- Casey E. Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet. 3rd ed. Baltimore, 2011.
- Андреева О. И., Зайцев О. А. Перспективы ведения российского уголовного судопроизводства в электронном формате // Уголовная юстиция. 2018. № 12.
- Андреева О. И., Зайцев О. А. Проблемы использования в уголовном судопроизводстве электронных доказательств // Правовые проблемы укрепления российской государственности: сб. ст. Томск, 2018. Ч. 79.
- Боннер А. Т. Традиционные и нетрадиционные средства доказывания в гражданском и арбитражном процессе. М., 2015. 624 с.

- Булгаков А. Н. Административное расследование правонарушений в области обеспечения безопасности дорожного движения: дис. ... канд. юрид. наук. Краснодар, 2017. 187 с.
- Бурдина Е. В. Развитие судебной системы в условиях информационного общества // Российское правосудие. 2018. № 7.
- Ворожбит С. П. Электронные средства доказывания в гражданском и арбитражном процессе: дис. ... канд. юрид. наук. СПб, 2011. 235 с.
- Головненков П., Спица Н. Уголовно-процессуальный кодекс Федеративной Республики Германия — *Strafprozessordnung* (StPO): науч.-практ. комментарий и перевод текста закона. Potsdam, 2012.
- Дремлюга Р. И. Компьютерная информация как предмет посягательства при неправомерном доступе: сравнительный анализ законодательства США и России // Журнал зарубежного и сравнительного правоведения. 2018. № 6.
- Жилкин В. А. Цифровые технологии и применение искусственного интеллекта в Финляндии и России: сравнительно-правовое исследование // Журнал зарубежного и сравнительного правоведения. 2018. № 6.
- Зазулин А. И. Правовые и методологические основы использования цифровой информации в доказывании по уголовным делам: дис. ... канд. юрид. наук. Екатеринбург, 2018. 251 с.
- Когамов М. Ч. Что такое уголовно-процессуальное право и уголовный процесс Республики Казахстан. Алматы, 2013.
- Кувычков С. И. Использование в доказывании по уголовным делам информации, представленной в электронном виде: дис. ... канд. юрид. наук. Н. Новгород, 2016.
- Молдавская прокуратура начала вести уголовные дела в электронном виде. URL: <http://www.digital.report>.
- Муратова Н. Г., Сергеев М. С. Правовое регулирование применения электронной информации и электронных носителей информации в уголовном судопроизводстве: отечественный и зарубежный опыт: монография. М., 2019. 264 с.
- Овсянников Д. В. Копирование электронной информации как средство уголовно-процессуального доказывания: дис. ... канд. юрид. наук. Челябинск, 2015. 192 с.
- Оконенко Р. И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: автореф. дис. ... канд. юрид. наук. М., 2016.
- Основы теории электронных доказательств / под ред. С. В. Зуева. М., 2019.
- Пастухов П. С. Доктринальная модель совершенствования уголовно-процессуального доказывания в условиях информационного общества: монография. М., 2015. 352 с.
- Правовое пространство и человек: монография / отв. ред. Ю. А. Тихомиров, Е. В. Пуляева, Н. И. Хлуденева. М., 2012.
- Развитие информационных технологий в уголовном судопроизводстве: монография / под ред. С. В. Зуева. М., 2018. 248 с.
- Сергеев М. С. Электронные доказательства в уголовном судопроизводстве. Опыт США // Вестник экономики, права и социологии. 2016. № 2.
- Содействие деятельности по борьбе с киберпреступностью, включая оказание технической помощи и наращивание потенциала: доклад Генерального секретаря ООН. Вена, 22—26 апреля 2013 г. URL: http://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2017/other_relevant_documentation/E_CN_15_2013_24_R.pdf.
- Сокурова Э. Ж., Аширбекова К. Б. Уголовное дело в электронном формате // Конституция: воплощение ценностей верховенства права, гражданского общества и современного государства: матер. междунар. науч.-практ. конф. Астана, 2018.
- Талапина Э. В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2.
- Тухташева У. А. Модернизация уголовного судопроизводства и усиление гарантий прав человека. URL: <http://www.napostu.uz/xabarlar/370>.
- Хабриева Т. Я. Право перед вызовами цифровой реальности // Журнал российского права. 2018. № 9.
- Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1.

REFERENCES

- Andreeva O. I., Zaytsev O. A. Problems of use of electronic documents in criminal proceedings. *Legal problems of strengthening Russian statehood*. Tomsk, 2018. Part 79. Pp. 4-17 (In Russ.)
- Andreeva O. I., Zaytsev O. A. Prospects for conducting Russian criminal proceedings in electronic format. *Ugolovnaya yustitsiya*, 2018, no. 12, pp. 57—61. (In Russ.)
- Bonner A. T. Traditional and non-traditional means of proof in civil and arbitration proceedings. Moscow, 2015. 624 p. (In Russ.)
- Bulgakov A. N. Administrative investigation of offences in the field of road safety. Cand. diss. Krasnodar, 2017. 187 p. (In Russ.)
- Burdina Ye. V. Development of Judicial System in Conditions of Information Society. *Rossiyskoe pravosudie*, 2018, no. 7, pp. 19—33. (In Russ.)
- Casey E. Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet. 3rd ed. Baltimore, 2011.
- Development of information technologies in criminal proceedings. Ed. by S. V. Zuev. Moscow, 2018. 248 p. (In Russ.)
- Dremlyuga R. I. Computer Information as an Target for Illegal Access: Comparative Analysis of the USA and Russian Legislation. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya* = *Journal of Foreign Legislation and Comparative Law*, 2018, no. 6, pp. 129—133. (In Russ.)
- Fundamentals of the theory of electronic evidence. Ed. by S. V. Zuev. Moscow, 2019. 400 p. (In Russ.)

- Golovnenkov P., Spitsa N. Code of criminal procedure of the Federal Republic of Germany — Code Of Criminal Procedure (CCP): scientific and practical commentary and translation of the law. Potsdam, 2012. 404 p.
- Jilkine V. A. Digital Technologies and the Application of Artificial Intelligence in Finland and in Russia: Comparative Legal Research. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya = Journal of Foreign Legislation and Comparative Law*, 2018, no. 6, pp. 74—78. (In Russ.)
- Khabrieva T. Y. Law Facing the Challenges of Digital Reality. *Zhurnal rossijskogo prava = Journal of Russian Law*, 2018, no. 9, pp. 5—16. (In Russ.)
- Khabrieva T. Y., Chernogor N. N. The Law in the Conditions of Digital Reality. *Zhurnal rossijskogo prava = Journal of Russian Law*, 2018, no. 1, pp. 85—102. (In Russ.)
- Kogamov M. Ch. What is the criminal procedure law and criminal procedure of the Republic of Kazakhstan. Almaty, 2013. 44 p. (In Russ.)
- Kuvychkov S. I. Use of information provided in electronic form in criminal cases in evidence. Cand. diss. Nizhny Novgorod, 2016. 273 p. (In Russ.)
- Legal space and a person. Ed. by Yu. A. Tikhomirov, E. V. Pulyaeva, N. I. Khludeneva. Moscow, 2012. 240 p. (In Russ.)
- Moldovan Prosecutor's office began to conduct criminal cases in electronic form. Available at: <http://www.digital.report>. (In Russ.)
- Muratova N. G., Sergeev M. S. Legal regulation of the use of electronic information and electronic media in criminal proceedings: domestic and foreign experience. Moscow, 2019. 264 p. (In Russ.)
- Okonenko R. I. Electronic evidence and problems of ensuring the rights of citizens to protection of privacy in criminal proceedings: comparative analysis of the legislation of the United States of America and the Russian Federation. Cand. diss. thesis. Moscow, 2016. 158 p. (In Russ.)
- Ovsyannikov D. V. Copying of electronic information as a means of criminal procedure evidence. Cand. diss. Chelyabinsk, 2015. 192 p. (In Russ.)
- Pastukhov P. S. Doctrinal model of improvement of criminal procedural evidence in the information society. Moscow, 2015. 352 p. (In Russ.)
- Promotion of activities to combat cybercrime, including technical assistance and capacity-building: report of the UN Secretary General. Vienna, 22—26 April 2013. Available at: http://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2017/other_relevant_documentation/E_CN_15_2013_24_R.pdf. (In Russ.)
- Sergeev M. S. The aim of the research is comparative legal analysis of regulation of applying digital evidences in the US criminal procedure. *Vestnik ekonomiki, prava i sotsiologii*, 2016, no. 2, pp. 206—212 (In Russ.)
- Sokurova E. Zh., Ashirbekova K. B. Criminal case in electronic format. *A Constitution: the Embodiment of the Values of the Rule of Law, Civil Society and Modern State: materials of the International Scientific and Practical Conference*. Astana, 2018. Pp. 346—350.
- Talapina E. V. Law and Digitalization: New Challenges and Prospects. *Zhurnal rossijskogo prava = Journal of Russian Law*, 2018, no. 2, pp. 5—17. (In Russ.)
- Tukhtasheva U. A. Modernization of criminal proceedings and strengthening of human rights guarantees. Available at: <http://www.napostu.uz/xabarlar/370>. (In Russ.)
- Vorozhbit S. P. Electronic evidence in civil and arbitration proceedings. Cand. diss. St. Petersburg, 2011. 235 p. (In Russ.)
- Zazulin A. I. Legal and methodological basis for the use of digital information in criminal evidence. Cand. diss. Yekaterinburg, 2018. 251 p. (In Russ.).