

EDN: RBGZJO
УДК 343(1–924.2/.3)

Assessment of Digital Evidence in Criminal Proceedings: Roman-German and Anglo-Saxon Approaches

Fahil A. Abdulkareem^{*a} and Andrei I. Semenovskii^b

^a*Duhok Polytechnic University
Duhok, Republic of Iraq*

^b*Siberian Federal University
Krasnoyarsk, Russian Federation*

Received 09.08.2024, received in revised form 20.03.2025, accepted 19.04.2025

Abstract. The information systems emergence has led to new challenges for criminal proceedings, digital evidences. They have a number of features: these evidences require special technical knowledge; they are relatively difficult to destroy and relatively easy to reproduce.

The study of approaches to assessing evidence of the Roman-German and Anglo-Saxon types showed that in order for digital evidence to be accepted in court, three conditions should be met: they have to be recognized as credible, the court has to be internally convinced of their reliability, and they have to be examined with the parties' participation. The court's assessment of the credibility of digital evidence depends on the current legal system. Two main approaches to assessing digital evidence can be distinguished: the approach of the continental legal family, known for the principle of freedom of evidence assessment, and the approach of the common law family, known for the desire to formalize the evidence assessment.

Keywords: criminal proceedings, digital criminology, digital evidence, evidence examination, evidence assessment.

Research area: Social Structure, Social Institutions and Processes; Criminal Law.

Citation: Abdulkareem F.A., Semenovskii A.I. Assessment of Digital Evidence in Criminal Proceedings: Roman-German and Anglo-Saxon Approaches. In: *J. Sib. Fed. Univ. Humanit. soc. sci.*, 2025, 18(5), 906–915. EDN: RBGZJO



Оценка цифровых доказательств в уголовном судопроизводстве: романо-германский и англосаксонский подходы

Ф.А. Абдулкарим^а, А.И. Семеновский^б

^аДахукский политехнический университет
Республика, Ирак Дахук

^бСибирский федеральный университет
Российская Федерация, Красноярск

Аннотация. Появление информационных систем привело к возникновению новых вызовов для уголовного судопроизводства, цифровых доказательств. Они обладают рядом особенностей – это доказательства, требующие специальных технических познаний; их относительно трудно уничтожить и относительно легко воспроизвести. Проведенное исследование подходов к оценке доказательств романо-германского и англосаксонского типа показало, чтобы цифровые доказательства были приняты в суде, должны быть соблюдены три условия: они должны быть признаны допустимыми, суд должен быть внутренне убежден в их достоверности, и они должны быть исследованы с участием сторон. Оценка судом допустимости цифровых доказательств зависит от действующей правовой системы. Можно выделить два основных подхода к оценке цифровых доказательств: подход континентальной правовой семьи, известный принципом свободы оценки доказательств, и подход семьи общего права, известный стремлением к формализации оценки доказательств.

Ключевые слова: уголовное судопроизводство, цифровая криминалистика, цифровые доказательства, исследование доказательств, оценка доказательств.

Научная специальность: 5.1.4. Социальная структура, социальные институты и процессы; уголовное право.

Цитирование: Абдулкарим Ф. А., Семеновский А. И. Оценка цифровых доказательств в уголовном судопроизводстве: романо-германский и англосаксонский подходы. *Журн. Сиб. федер. ун-та. Гуманитарные науки*, 2025, 18(5), 906–915. EDN: RBGZJO

Введение

Основным средством познания обстоятельств преступления и установления вины обвиняемого в уголовном судопроизводстве, несомненно, являются доказательства. Доказательства способствуют установлению достоверных сведений о расследуемом событии. Получаемая из них информация имеет значение на всех стадиях уголовного процесса. Доказательства в правовых процедурах играют решающую роль в установлении юридических фактов, имеющих значение для дела, подлежат собиранию

и оценке уполномоченными на то субъектами права по правилам и методам, предписанным той или иной отраслью процессуального права.

Научно-технический прогресс порождает так называемую информационную среду с ее техническими и программными средствами хранения, обработки и передачи информации, процессами информатизации общества, охватившими значительную часть населения Земли информационными системами, улучшающими жизнь человека в разных сферах –

культуре, науке, политике. С другой стороны, развитие информационной среды стало почвой для новых вызовов обществу, поскольку сама информационная среда оказалась местом и средством совершения киберпреступлений.

В целом, чтобы доказательства были приняты судом в качестве допустимых (имеются в виду не цифровые доказательства, так называемые традиционные), в мировой практике к ним предъявляется ряд требований. В частности, такие доказательства должны содержать конкретные, относимые к предмету доказывания сведения о подлежащих доказыванию обстоятельствах («специфичность доказательств»), должны всегда быть собраны из первоисточника («прямота доказательств»), и сведения из них должны быть пригодными для аргументации обвиняющего или оправдывающего тезиса (не следует путать с допустимостью и относимостью, в данном случае важна пригодность доказательств к аргументации позиции в плане их познавательной ценности).

Чтобы быть принятыми в качестве допустимых, цифровые доказательства также должны соответствовать определенным критериям. В свете настоящего исследования возникает вопрос: что понимать под цифровыми доказательствами и как они оцениваются органами уголовной юстиции в семьях континентального и общего права?

Понятие цифровых доказательств

Понятие цифровых доказательств имеет как широкий, так и узкий подходы в мировой практике.

На Конференции координаторов исследований организаций системы Организации Объединенных Наций и многосторонних финансовых учреждений (Рим, 2021) цифровые доказательства были определены в качестве информации, имеющей потенциальную ценность для расследования, которая хранится или передается в цифровой форме.

Цифровые доказательства, как было обсуждено в ходе данной конференции, от-

личаются от иных видов доказательств следующими особенностями:

1. Они носят комплексный характер, то есть зачастую распределены по различным физическим и цифровым локациям, их собирание требует экспертных знаний и специального инструментария.

2. Цифровые доказательства легко подвергаются изменению в силу случайного или намеренного на них воздействия, при этом потенциально может не оставаться следов такого воздействия.

3. Цифровые доказательства легко могут быть продублированы и переданы другим лицам, что затрудняет сохранение их в тайне.

4. По своему характеру они не устойчивы: сетевые журналы, история посещений Интернета, публикации в социальных сетях, мгновенные сообщения, кэшированные и удаленные данные могут быть утеряны, если они вовремя не были должным образом сохранены¹.

В более узком смысле в зарубежных источниках цифровые доказательства подразделяются на собственно цифровые и так называемые электронные доказательства. Под электронными доказательствами следует понимать сведения, полученные из электронно-вычислительных машин в качестве магнитных или электрических полей, а также импульсов. Такие данные возможно собрать и исследовать с помощью специализированного программного обеспечения, пользовательских приложений и технических средств. В свою очередь, полученные таким образом сведения могут быть представлены в качестве приемлемых в суде доказательств – могущих быть исследованными самим судом непосредственно. Сведения, имеющиеся в цифровом пространстве в виде отмеченных импульсов и полей, представленные в суд в виде документов, которые может воспринимать сам человек, именуются за рубежом цифровыми доказательствами (Horsman, 2023).

¹ См.: Конференция международных следователей (СП 2021), «Общие принципы цифровых доказательств», 2021 г., URL: <https://www.ciinvestigators.org>.

Особенности цифровых доказательств

Цифровые доказательства имеют особенности, позитивно отличающие их от иных личных и вещественных доказательств в контексте доказывания по уголовным делам.

В настоящее время признается, что полностью уничтожить цифровые доказательства не так просто, как иные. Они не воспринимаются человеком непосредственно с помощью его органов чувств, а потому часто остаются как бы незаметными для лица, что и предопределяет трудности как при их обнаружении, так и уничтожении. Это также предопределяет необходимость проведения экспертного исследования их источников для их обнаружения, а значит, подобные доказательства должны оказывать большее влияние на внутреннее убеждение суда, так как получают экспертом. След в цифровой среде меньше всего подвержен изменениям, следовательно, цифровые доказательства потенциально содержат наиболее точные сведения о расследуемом событии (Stoykova, 2023).

Помимо указанных характеристик цифровые доказательства также обладают следующими особенностями:

1. Это «невидимые доказательства», они не воспринимаются непосредственно человеком, относятся к массиву данных и информации, существующей в нематериальной электронной форме, которая им придается с использованием электронно-вычислительных машин и специальных программных систем для такого оборудования (Morelato et al., 2023).

2. Цифровые доказательства признаются доказательствами, получаемыми с помощью специалиста, специальных экспертных знаний. В контексте сравнительного правоведения в правовых системах познание обстоятельств преступного события с привлечением специальных знаний подразумевает наиболее точное соответствие действительности собираемых сведений.

3. Цифровые доказательства связаны с техническими средствами, способными создавать, считывать, воспроизводить, копировать, транслировать и передавать

по сверхскоростным каналам импульсы и сигналы, в форме которых существуют данные доказательства. Соответственно, цифровые доказательства потенциально обладают способностью передаваться на большие расстояния в короткий промежуток времени.

4. Цифровые доказательства могут быть скопированы без потери содержащейся в них доказательственной информации, что нивелирует опасность уничтожения оригинала такого доказательства (Choi & Yang, 2021). Копирование информации в электронно-цифровой среде идентично ее созданию, что обуславливает эффективную гарантию сохранения доказательств от утраты и повреждения за счет использования их точных копий.

5. В настоящее время цифровые доказательства трудно уничтожаемы, так как современное программное обеспечение способно восстанавливать цифровые данные даже после их удаления. Вопрос стоит лишь в технической способности восстановить данные в зависимости от метода удаления цифровой информации.

Наиболее распространенные виды цифровых доказательств

Цифровые сообщения

Письменные сообщения между двумя или более лицами в цифровой среде считаются одними из самых надежных доказательств в истории права. Такое общение не только помогает следователям получить новую информацию о преступлении, но также определить отношения между подозреваемыми, подтвердить показания и установить хронологию событий (Sokol et al., 2023). Следователи не могут игнорировать источник цифрового сообщения, несмотря на их основной интерес к его содержанию. В нашем веке цифровые сообщения разнообразны, включают текстовые сообщения, которые можно отправлять через смартфоны, платформы социальных сетей, программы для обмена мгновенными сообщениями и электронную почту. Кроме того, цифровые заметки и документы также можно использовать в целях общения.

Браузер и история поиска

Известно, что люди в среднем проводят в Интернете более шести часов в день². Это делает браузеры ценным источником цифровых доказательств. Каждый поиск и посещение веб-сайта оставляет след, по которому можно проследить цепочку посещаемых лицом веб-страниц, а анализ истории просмотров в браузере обычно является самым простым способом, обеспечивающим установление такой цепочки. Некоторые люди могут очистить историю браузера, чтобы скрыть историю поиска соответствующих веб-страниц, но способы получить эту информацию все же есть. Например, некоторые веб-сайты и платформы, такие как Google, хранят данные истории поиска каждого пользователя под их персональной учетной записью. В результате запроса или выемки таких сведений могут быть собраны данные, которые потенциально предоставят значительный объем криминалистической информации для расследования уголовного дела или будут использованы в качестве доказательств в суде.

Цифровые Фотографии и Видеоматериалы

Цифровые изображения и видео являются важными доказательствами по уголовным делам. Однако содержание таких доказательств, увы, легко подвергается изменению, и люди, обращающиеся с ними, могут даже не осознать, как это произойдет. Простые действия, такие как воспроизведение видео с помощью неподходящего под формат файла программного обеспечения, сжатие, например, видео для совместного использования или преобразование фото- и видеофайлов в воспроизводимый формат, удобный для того или иного лица, могут изменить содержимое таких фотографий и видеоматериалов (Pedapudi & Vadlamani, 2023). Поэтому необходимо соблюдать правильные процедуры получения, хранения и представления таких доказательств. Так, необходимо получить и изучить оригинальные, немодифицированные цифровые

файлы (фотографии, видеозаписи) в качестве доказательств. В настоящее время обеспечить получение данных доказательств такого качества возможно путем изъятия, руководствуясь соответствующими криминалистическими рекомендациями, технических средств, с помощью которых данные доказательства были созданы (Holt & Dolliver, 2021; Dolliver et al., 2017).

Лог-файлы («журналы активности»)

Программное обеспечение современных электронно-вычислительных машин обычно создает так называемые журналы активности (лог-файлы), в которых отражаются различные процессы использования данного программного обеспечения и ошибки в его работе, например, характеристики операционной системы, с помощью которой осуществлялось взаимодействие пользователя с данным программным обеспечением, вплоть до сбоев в видеоиграх.

Хотя эти журналы в первую очередь предназначены для целей технического обслуживания (Dolliver et al., 2017), они также могут служить доказательством для подтверждения деятельности конкретных лиц или раскрывать дополнительную информацию для следователей. Содержание и расположение в операционной системе каждого журнала активности могут различаться в зависимости от программного обеспечения (Cheng et al., 2021). Распространенные примеры используемых в качестве цифровых доказательств журналов активности включают следующие:

1. Журналы телефонных звонков. Телефоны-смартфоны хранят подробные записи о повседневной деятельности пользователя, включая частоту звонков и данные о местоположении пользователя во время звонка. Иногда такие журналы используются даже для доказывания времени съемки того или иного фото или видео (Domingues et al., 2021).

2. Журналы интернет-протоколов: используются в электронной цифровой среде для управления IP-адресами устройств некоторой сети. IP-адреса использу-

² Среднесуточное использование Интернета онлайн-пользователями по странам и регионам по состоянию на второй квартал 2023 г. URL: <https://www.statista.com/statistics/1258232/daily-time-spent-online-worldwide/>

ются для идентификации электронно-вычислительных машин и их пользователей, заходящих на веб-сайт, а их физическое местоположение можно определить с помощью журналов IP-адресов (Sokol et al., 2020).

3. Журналы транзакций. Эти журналы используются для отслеживания изменений, внесенных в файлы электронной цифровой среды, что позволяет администраторам файла вернуться к предыдущему его состоянию. Эти журналы обычно используются серверами, базами данных и облачными хранилищами документов, например таким, как Google Документы (Choi & Lee, 2023).

4. Журналы событий. Программное обеспечение электронно-вычислительных машин и их операционные системы ведут журналы событий для отслеживания активности, выявления ошибок в своей работе и диагностики сбоев. Эти журналы также помогают определить, вызвано ли конкретное событие человеком или компьютерным процессом (Khan et al., 2023).

5. Журналы сообщений. Большинство программ электронных сообщений (электронная почта, мессенджеры) сохраняют содержание электронной переписки для последующего использования (Forte, 2004).

Выделяемые в мировой практике условия для признания цифровых доказательств допустимыми

Суду в рамках рассмотрения уголовного дела, в котором имеются цифровые доказательства, следует руководствоваться следующими тремя условиями, обеспечивающими признание имеющихся цифровых доказательств в качестве допустимых.

Первым условием, обеспечивающим допустимость полученных цифровых доказательств, является их получение в рамках предусмотренной системой уголовной юстиции правовой формы, закрепленной соответствующим уголовно-процессуальным законодательством. В ином случае суд признает недопустимой форму, в которой были получены такие «доказательства», а также сами подобные «доказательства». Например, применение таких незаконных мер, как

физическое или психическое принуждения или обман в отношении подозреваемого с целью установления кода доступа в операционную систему принадлежащей ему электронно-вычислительной машины, влечет в конечном счете признание полученных цифровых доказательств недопустимыми. В Рекомендации № 18 Пятнадцатой Международной конференции Международной ассоциации уголовного права, состоявшейся в Бразилии в сентябре 1994 года, отмечается, что нарушение законности при собирании доказательств влечет недопустимость таких доказательств, в том числе недопустимость любых производных от них доказательств, распространяющуюся на все стадии производства по уголовному делу³.

Принцип законности имеет решающее значение при исследовании цифровых доказательств в ходе расследования как киберпреступлений, так и «традиционных» преступлений, в том числе гибридных – совершаемых с использованием электронно-цифровой среды. Любое нарушение этого принципа влечет признание недопустимой форму получения таких доказательств, соответственно, недопустимы и сами эти доказательства. Кроме того, этот принцип подразумевает наступление предусмотренной законом ответственности для следователя, который допустил собирание доказательств вне законной процессуальной формы.

Вторым условием признания цифровых доказательств допустимыми является уровень уверенности судьи при осуждении обвиняемого, что характерно для Республики Ирак – страны, на правовую систему которой оказало сильное влияние мусульманское право в смещении с романо-германской и англо-саксонской правовой традиций. По Основному закону Ирака, для судьи крайне важно иметь высокий уровень внутреннего убеждения в виновности обвиняемого, независимо от того, явля-

³ Пятнадцатый международный конгресс по уголовному праву (Рио-де-Жанейро, 4–10 сентября 1994 г.), *Revue Internationale de droit penal*, 2015/1–2 (Том 86), стр. 369–390. DOI: 10.3917/ridp.861.0369. URL: <https://www.cairn.info/revue-internationale-de-droitipenal-2015-1-page-369.htm>.

ются ли доказательства традиционными, цифровыми или комбинацией тех и других. Согласно пункту 5 статьи 19 Конституции Республики Ирак 2005 года⁴, в случае возникновения каких-либо сомнений по уголовному делу они всегда должны толковаться в пользу обвиняемого.

Чтобы достичь состояния внутреннего убеждения в виновности обвиняемого при рассмотрении уголовных дел по «традиционным преступлениям», то есть где нет цифровых следов, судья должен тщательно изучить доказательства, проанализировать их и, соответственно, уже сделать вывод о виновности или невиновности обвиняемого. Однако когда дело доходит до киберпреступлений, судья должен обладать техническими познаниями в вопросах существования информации в электронно-цифровой среде, чтобы определить достоверность собранных цифровых доказательств. Без достаточных технических знаний у судьи могут возникнуть сомнения относительно достоверности таких доказательств, что может привести к оправданию действительно виновного лица.

Между тем, по мнению большинства экспертов по сравнительному уголовному праву, данные о преступном событии, получаемые из электронно-цифровой среды, имеют высокий уровень достоверности. В отдельных правовых системах, например в США, копии данных, извлеченных из электронно-вычислительных машин, признаются доказательствами, имеющими приоритетную доказательную силу над другими.

Третье условие, обеспечивающее признание цифровых доказательств допустимыми: они должны быть исследованы с участием сторон, которым должна быть представлена возможность ознакомиться с доказательствами и возможность выска-

заться по существу их содержания и допустимости в целом. В отдельных правовых порядках это обеспечивается только в ходе судебного разбирательства по уголовному делу. Что касается правовой системы Республики Ирак, то такой подход не отличает цифровые доказательства от всех других видов доказательств, закреплен в статье 212 Уголовно-процессуального кодекса Республики Ирак № 23 от 1971 года⁵. Обсуждение цифровых доказательств осуществляется по двум основным правилам. Во-первых, стороны имеют право на ознакомление с цифровыми доказательствами и право выразить свое отношение к ним до тех пор, пока не будет принято решение по уголовному делу, предусмотренное статьями 123 и 124 Уголовно-процессуального кодекса Республики Ирак № 23 1971 года⁶. В этом положении подчеркивается важность предоставления отдельным лицам возможности защищать себя и противостоять доказательствам, представленным против них. Во-вторых, чтобы приговор по существу рассмотрения уголовного дела

⁵ Статья 212 Уголовно-процессуального кодекса Республики Ирак № 23 от 1971 года гласит: «Недопускается, чтобы суд обосновывал свое решение на доказательствах, которые не были исследованы в ходе судебного заседания или были основаны на документе, представленном одной из сторон процесса, без возможности ознакомления с этим документом процессуальными оппонентами. Судья не может выносить решение, основываясь только лишь на своих личных знаниях». URL: https://pureportal.spbu.ru/files/96272162/i_741978.pdf.

⁶ В статьях 123 и 124 Уголовно-процессуального кодекса Республики Ирак № 23 от 1971 года описываются процедуры, которые необходимо соблюдать при допросе обвиняемого. Согласно статье 123(а): «Следственный судья (или следователь) должны допросить обвиняемого в течение двадцати четырех часов с момента доставления после проверки личности обвиняемого и информирования его о совершенном им преступлении. Обвиняемый может собственноручно написать показания, а также опровергнуть доказательства. Показания обвиняемого должны быть записаны с изложением доказательств в его пользу. Обвиняемый должен быть допрошен снова, если это необходимо для установления истины». Статья 124 «Обвиняемый имеет право выступить с заявлением в любое время после заслушивания показаний любого свидетеля и обсудить эти показания (дать по ним свои показания) или потребовать, чтобы между ним и свидетелем была проведена очная ставка». URL: https://pureportal.spbu.ru/files/96272162/i_741978.pdf.

⁴ Пункт 5 статьи 19 Конституции Республики Ирак 2005 года гласит: «Обвиняемый невиновен, пока его вина не будет доказана в ходе справедливого судебного разбирательства. Обвиняемый не может быть привлечен к суду за одно и то же преступление повторно после оправдания, если не будут представлены новые доказательства». URL: <https://iq.parliament.iq/en/wp-content/uploads/2022/01/Iraqi-Constitution.pdf>.

имел юридическую силу, доказательства должны быть закреплены в предусмотренных законом материалах уголовного дела.

Судебное усмотрение при оценке допустимости цифровых доказательств

Допустимость цифровых доказательств остается на усмотрение судьи и зависит от преобладающей системы доказательств (Prashant Bhadu, 2021). Эти системы включают романо-германский и англосаксонский подходы к доказательствам.

1. Романо-германский подход представляет собой правовое явление, в котором законодатель не предопределяет доказательства и средства доказывания в рамках рассмотрения уголовного дела по конкретным видам преступлений, а скорее оставляет судье свободу выносить свое решение по своему усмотрению, не навязывая ему каких-либо конкретных доказательств, не предопределяя их силу. С развитием судебной экспертизы и цифровых доказательств судьям в этой системе приходится иметь дело с новыми видами доказательств для раскрытия преступлений. В указанном подходе судья не связан доказательствами, представленными сторонами дела (Tatulych, 2020). Чтобы получить цифровые доказательства, ответственное лицо суда, обычно им выступает сам судья, может вынести особое постановление интернет-провайдеру. Подобное постановление может требовать представления провайдером информации, касающейся веб-сайтов, например, которые посещал подсудимый, содержание онлайн-переговоров, в которых он участвовал, а также текстовых электронных сообщений, которые он отправлял и получал. Кроме того, такое ответственное лицо может обязать оператора интернет-ресурса предоставить суду необходимые данные для доступа к ресурсу, что может включать раскрытие паролей и кодов для доступа к различным закрытым частям этого ресурса. Уполномоченное лицо суда может в постановлении обязать провести осмотр операционной системы электронно-вычислительной машины. Однако судья должен убедиться, что любые

доказательства, которые предоставляются суду, достоверны и допустимы в соответствии с соответствующим законом, прежде чем признавать за ними юридическую силу доказательств. Такой подход закреплен в законодательстве Алжира и Египта, а также во французском законодательстве (Oparnica, 2016).

2. Англосаксонский подход известен своей системой формализации оценки доказательств. В этой системе законодатель заранее определяет перечень доказательств (их конкретные виды), оценка доказательств может быть в известной степени предопределена действующим правом (доказательства могут различаться по юридической силе, только определенными доказательствами может быть предопределено выяснять конкретные обстоятельства по делу), и судья не имеет права отклоняться от заданной траектории оценки доказательств. Соответственно, в ситуации, когда у судьи не сформировалось внутреннего убеждения относительно существования определенного юридического факта, но в деле имеются доказательства, которые по закону должны подтверждать данный факт, суд обязан признать факт доказанным.

Процесс доказывания в этом подходе подчинен двум основным принципам: первый – это правило запрета свидетельствования по слуху, а второй – правило наилучшего доказательства (Bierekoven et al., 2014).

1. Запрет свидетельствовать по слуху гласит, что показания, сформированные свидетелем только со слов третьих лиц, не могут быть использованы в доказывании по делу, если сообщающий их свидетель сам не воспринимал своими органами чувств сведения из таких показаний. Такие «показания» формируются вне производства по делу, в классическом их понимании, их источник невозможно определить, соответственно, допросить в рамках установленных процедур, что исключает их использование. Однако из данного принципа есть ряд исключений, что относится и к сведениям, о которых сообщает свидетель, полученным из электронно-цифровой среды. Английская судебная система неоднократно принимала

показания такого типа. Например, в деле R. v. Wood (1983) (Harvey, 2019) установлено, что показания, сформированные на основе воспринятых сведений, представленных электронно-вычислительной машиной, не подпадают под правило запрета свидетельствовать по слуху и считаются первоначальными доказательствами.

2. Правило наилучшего доказательства предусматривает, что зачастую для подтверждения содержания доказательства требуется оригинал письма, записи или фотографии. В обобщенном виде правило наилучшего доказательства подразумевает неоспоримое превосходство по доказательственной силе оригинала над копией доказательства. В США это правило содержится в Законе о доказательствах. Согласно «Правилу 1002. Требование оригинала» указанного Закона, электронно-цифровые материалы должны оцениваться так же, как и любой другой вид доказательств. Текстовая информация, содержащаяся на электронно-цифровом носителе информации, в любом случае приравнивается по юридической силе к оригинальному документу. Копия такого текстового файла в электронно-цифровой среде, дословная распечатка данного файла на бумаге, в доказательственном плане приравнивается к оригинальному документу («Правило 1003. Допустимость дубликатов» Закона).

Заключение

Цифровые доказательства обладают рядом преимуществ перед «традиционными» видами доказательств, в отдельных правовых системах даже имеют преиму-

щества по юридической силе при их оценивании, несмотря на свою нематериальную природу. Однако в ситуациях международного сотрудничества в рамках уголовного судопроизводства использование цифровых доказательств может осложняться отсутствием унифицированных подходов в их оценке, осложненных традициями уголовно-процессуального права стран разных правовых систем. Развитие цифровизации, что неминуемо касается и сферы уголовного судопроизводства, требует повышение технической грамотности следователей и судей. В отдельных правовых порядках отсутствуют правовые институты, регулирующие использование цифровых доказательств в сфере уголовного судопроизводства. Например, такая ситуация имеется в Республике Ирак, однако правоприменительная практика уже складывается таким образом, что использование цифровых доказательств в Ираке следует романо-германской традиции в оценке доказательств. Романо-германский подход в оценке доказательств предусматривает широкую свободу в их оценке, не предусматривает конкретные виды цифровых доказательств. Противоположностью ему выступает подход стран общего права, устанавливающий конкретные виды доказательств и правила их оценки. Подобный подход нам кажется более приемлемым, во всяком случае для Республики Ирак, так как предполагает критерии оценивания, заранее заданные, что видится обоснованным в контексте оценки цифровых доказательств, требующих специальных познаний в области информационных технологий.

Список литературы \ References

- Bierekoven C., Bazin P. & Kozlowski T. Electronic Signatures in German, French and Polish Law Perspective. *Digital Evidence and Electronic Signature Law Review*, 2014, 1(0). <https://doi.org/10.14296/deeslr.v1i0.1719>
- Cheng C. C.-C., Shi C., Gong N. Z. & Guan Y. LogExtractor: Extracting digital evidence from android log messages via string and taint analysis. *Forensic Science International: Digital Investigation*, 2021, 37, 301193. <https://doi.org/10.1016/j.fsidi.2021.301193>
- Choi H., Lee S. Forensic analysis of SQL server transaction log in unallocated area of file system. *Forensic Science International: Digital Investigation*, 2023, 46, 301605. <https://doi.org/10.1016/j.fsidi.2023.301605>
- Choi J. P. & Yang S. Investigative journalism and media capture in the digital age. *Information Economics and Policy*, 2021, 57, 100942. <https://doi.org/10.1016/j.infoecopol.2021.100942>

- Dolliver D.S., Collins C. & Sams B. Hybrid approaches to digital forensic investigations: A comparative analysis in an institutional context. *Digital Investigation*, 2017, 23, 124–137. <https://doi.org/10.1016/j.diin.2017.10.005>
- Domingues P., Andrade L. M. & Frade, M. Microsoft's Your Phone environment from a digital forensic perspective. *Forensic Science International: Digital Investigation*, 2021, 38, 301177. <https://doi.org/10.1016/j.fsidi.2021.301177>
- Forte D. Principles of digital evidence collection. *Network Security*, 2003, 2003(12), 6–7. [https://doi.org/10.1016/s1353-4858\(03\)00006-0](https://doi.org/10.1016/s1353-4858(03)00006-0)
- Forte D. The importance of text searches in digital forensics. *Network Security*, 2004, 2004(4), 13–15. [https://doi.org/10.1016/s1353-4858\(04\)00067-4](https://doi.org/10.1016/s1353-4858(04)00067-4)
- Franco D. The Importance of Research in Forensic Sciences and Digital Forensics in Contemporary Society. *International Journal of Forensic Sciences*, 2023, 8(4), 1–2. <https://doi.org/10.23880/ijfsc-16000336>
- Harvey D.J. Digital Evidence Admissibility: Some Issues. *SSRN Electronic Journal*. 2019. Published. <https://doi.org/10.2139/ssrn.3505611>
- Holt T. & Dolliver, D. S. Exploring digital evidence recognition among front-line law enforcement officers at fatal crash scenes. *Forensic Science International: Digital Investigation*, 2021, 37, 301167. <https://doi.org/10.1016/j.fsidi.2021.301167>
- Horsman G. Digital evidence strategies for digital forensic science examinations. *Science & Justice*, 2023, 63(1), 116–126. <https://doi.org/10.1016/j.scijus.2022.11.004>
- Khan S., Parkinson S. & Murphy, C. Context-based irregular activity detection in event logs for forensic investigations: An itemset mining approach. *Expert Systems with Applications*, 2023, 233, 120991. <https://doi.org/10.1016/j.eswa.2023.120991>
- Makulilo A. B. The admissibility of electronic evidence in Tanzania: new rules and case law. *Digital Evidence and Electronic Signature Law Review*, 2016, 13(0). <https://doi.org/10.14296/deeslr.v13i0.2302>
- Morelato M., Cadola L., Bérubé M., Ribaux O. & Baechler, S. Forensic intelligence teaching and learning in higher education: An international approach. *Forensic Science International*, 2023, 344, 111575. <https://doi.org/10.1016/j.forsciint.2023.111575>
- Oparnica G. Digital evidence and digital forensic education. *Digital Evidence and Electronic Signature Law Review*, 2016, 13(0). <https://doi.org/10.14296/deeslr.v13i0.2305>
- Pedapudi S. M. & Vadlamani, N. Digital forensics approach for handling audio and video files. *Measurement: Sensors*, 2023, 29, 100860. <https://doi.org/10.1016/j.measen.2023.100860>
- Prashant Bhadu. Admissibility And Perplexity Of Digital Evidence: An Overview. *Legal Research Development*, 2021, 5(IV), 10–20. <https://doi.org/10.53724/lrd/v5n4.03>
- Rule 1002. Requirement of the Original. (n.d.). LII / Legal Information Institute. https://www.law.cornell.edu/rules/fre/rule_1002
- Rule 1003. Admissibility of Duplicates. (n.d.). LII / Legal Information Institute. https://www.law.cornell.edu/rules/fre/rule_1003
- Scanlon M., Breiting F., Hargreaves C., Hilgert J.-N. & Sheppard, J. ChatGPT for digital forensic investigation: The good, the bad, and the unknown. *Forensic Science International: Digital Investigation*, 2023, 46, 301609. <https://doi.org/10.1016/j.fsidi.2023.301609>
- Sokol P., Antoni L., Křídlo O., Marková E., Kováčová K. & Krajčí, S. Formal concept analysis approach to understand digital evidence relationships. *International Journal of Approximate Reasoning*, 2023, 159, 108940. <https://doi.org/10.1016/j.ijar.2023.108940>
- Sokol P., Rózenfeldová L., Lučivjanská K. & Harašta J. IP Addresses in the Context of Digital Evidence in the Criminal and Civil Case Law of the Slovak Republic. *Forensic Science International: Digital Investigation*, 2020, 32, 300918. <https://doi.org/10.1016/j.fsidi.2020.300918>
- Stoykova R. The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, 2023, 49, 105801. <https://doi.org/10.1016/j.clsr.2023.105801>
- Tatulych I. Electronic evidence as a means of evidence in civil proceedings. *Law Review of Kyiv University of Law*, 2020, 1, 215–219. <https://doi.org/10.36695/2219-5521.1.2020.43>