

## ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ (ЭЛЕКТРОННЫХ) ТЕХНОЛОГИЙ В ПРОЦЕССЕ ДОКАЗЫВАНИЯ ПО УГОЛОВНЫМ ДЕЛАМ О ПРЕСТУПЛЕНИЯХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

**Яковлев Д.С.**

Алтайский государственный университет, г. Барнаул, Россия

**Аннотация.** Статья посвящена исследованию основных аспектов использования цифровых (электронных) технологий в процессе доказывания по уголовным делам о преступлениях в сфере компьютерной информации. Рассматриваются и систематизируются основные научные подходы к пониманию роли цифровых технологий, предлагается авторское определение данного понятия, освещаются ключевые направления применения цифровых технологий на стадиях собирания и исследования доказательств. На примерах судебной практики выявляются проблемные аспекты, возникающие в процессе использования таких технологий в процессе доказывания по уголовным делам о преступлениях в сфере компьютерной информации, включая отсутствие единой методики применения таких технологий, а также несоблюдение сроков предварительного расследования при проведении компьютерной экспертизы как последующей проблемы. В заключение предлагаются конкретные пути решения выявленных проблем, направленные на совершенствование уголовно-процессуального законодательства и оптимизацию процесса доказывания.

**Ключевые слова:** доказывание, цифровые технологии, компьютерная информация, компьютерная экспертиза, следственные действия.

## USE OF DIGITAL (ELECTRONIC) TECHNOLOGIES IN THE PROCEDURE OF EVIDENCE IN CRIMINAL CASES ON COMPUTER INFORMATION CRIMES

**Yakovlev D.S.**

Altai State University, Barnaul, Russia

**Abstract.** The article is devoted to the study of the main aspects of the use of digital (electronic) technologies in the process of proving criminal cases on crimes

*in the field of computer information. The main scientific approaches to understanding the role of digital technologies are considered and systematized, the author's definition of this concept is proposed, the key areas of application of digital technologies at the stages of collecting and examining evidence are highlighted, and the problematic aspects arising in the process of using such technologies in the process of proving criminal cases on crimes in the field of computer information are identified using examples from judicial practice, including the lack of a unified methodology for applying such technologies, as well as the non-compliance with the terms of preliminary investigation during computer examination as a subsequent problem. In conclusion, the article proposes specific solutions to the identified problems aimed at improving criminal procedure legislation and optimizing.*

**Keywords:** *evidence, digital technologies, computer information, computer expertise, investigative actions.*

Актуальность темы исследования обусловлена стремительной цифровизацией всех сфер общественной жизни, что, в свою очередь, порождает новую, высокотехнологичную компьютерную преступность. Безусловно, преступления в сфере компьютерной информации, предусмотренные гл. 28 Уголовного кодекса Российской Федерации (далее – УК РФ) [1], сегодня представляют значительную угрозу для охраняемых законом интересов личности, общества и государства.

Исходя из прим. 1 к ст. 272 УК РФ, под компьютерной информацией понимаются любые сведения (сообщения, данные), представленные в виде электрических сигналов, независимо от средств их хранения, обработки и передачи. Такие сведения могут находиться в запоминающем устройстве электронно-вычислительных машин и в других компьютерных устройствах [2], а также на любых внешних электронных носителях (дисках, в т.ч. жёстких дисках – накопителях, флеш-картах и т. п.) в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электрической связи. В соответствии с разъяснениями, содержащимися в Постановлении Пленума Верховного Суда Российской Федерации от 15.12.2022 года № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»», к числу преступлений в сфере компьютерной информации следует относить уничтожение, блокирование, модификацию, копирование компьютерной информации и нейтрализацию средств её защиты [2]. Эффективное расследование и рассмотрение таких уголовных дел невозможно без

адаптации традиционного процесса доказывания к цифровой среде, что требует активного внедрения и использования специальных цифровых технологий. Значимость данного вопроса подчёркивается и в Стратегии национальной безопасности Российской Федерации, где указано, что цель обеспечения информационной безопасности – укрепление суверенитета Российской Федерации в информационном пространстве [3].

Анализ научных трудов, посвящённых проблемам уголовно-процессуального доказывания в условиях цифровой трансформации всего общества и в том числе уголовного судопроизводства, позволяет выделить несколько основных подходов к пониманию роли цифровых технологий в уголовном процессе. Большинство существующих точек зрения можно условно разделить на следующие группы:

1. Цифровые технологии как новый инструмент для работы с новыми видами доказательств (П. С. Пастухов [4], О. А. Зайцев [5] и др.). Сторонники этого подхода акцентируют внимание на том, что цифровые технологии изменили способы накопления и использования цифровой доказательственной информации, вследствие чего появление электронной формы работы с такой информацией диктует потребность в разработке новых методов собирания, исследования и оценки доказательств при совершении преступлений, в большей степени в сфере компьютерной информации.

2. Цифровые технологии как средство процессуальной оптимизации (Д. А. Гришин [6], М. А. Малина [7] и др.). Данная позиция заключается в том, что цифровые технологии ускоряют и упрощают совершение отдельных процессуальных действий, не меняя при этом их сущности, а, наоборот, повышая оперативность уголовно-процессуальной деятельности и прокурорского надзора.

Последняя точка зрения, по нашему мнению, является наиболее верной и перспективной, поскольку цифровые технологии интегрируются в уголовный процесс не только как вспомогательный инструмент, но и как элемент, трансформирующий традиционные процедуры доказывания в целях повышения их эффективности в условиях вызовов современного высокотехнологичного общества.

Относительно сущности использования цифровых (электронных) технологий в ходе осуществления уголовно-процессуального доказывания можно её определить как основанную на законе деятельность властных субъектов такого доказывания (дознателя, следователя, прокурора, суда). Её содержание заключается в применении названными субъектами специализированных технических средств, программно-аппаратных комплексов и информационных систем для собирания, проверки и оценки цифровых (электронных) доказательств, а также для совершения иных

процессуальных действий, направленных на установление обстоятельств, подлежащих доказыванию по конкретному уголовному делу. При этом, исходя из специфики данной деятельности, наиболее ярким примером преступлений, при расследовании которых осуществляется данная деятельность, являются преступления, совершенные в сфере компьютерной информации.

Обозначим и раскроем два вида таких технологий, которые наиболее ярко выделяются в практике доказывания по указанным выше делам:

1. Экспертиза компьютерной техники. Данная технология включает в себя технологии анализа аппаратного и программного обеспечения, используемого подозреваемым, восстановления удалённых файлов, расшифровку файлов или установление личности интернет-пользователя путём анализа данных посещаемых сайтов [8, с. 28].

Например, применение аппаратно-программного комплекса «Мобильный криминалист Эксперт Плюс» делает возможным проведение комплексной цифровой экспертизы, при которой извлекаются данные из мобильных устройств, персональных компьютеров и облачных сервисов. А в случае совершения преступления с использованием средств анонимизации, позволяет даже удалённо извлекать необходимые данные [9, с. 409].

2. Искусственный интеллект. Криминалистический аспект применения таких технологий может быть разноплановым. Он может касаться как ориентирующей информации и специфических учётов, так и частных криминалистических методик [10, с. 38]. Базы данных, созданные при помощи искусственного интеллекта, позволили бы в короткие сроки получить необходимые данные в отношении участников уголовного судопроизводства, например, принадлежность и регистрация компьютерного устройства, с использованием которого было совершено конкретное преступление в сфере компьютерной информации, фиксация IP-адресов в случае копирования компьютерной информации посредством её электронного отправления за пределы государственной границы Российской Федерации.

В частности, существуют базы данных «Палантир», «Осирис», «Шерлок», «Псков», которые позволяют раскрывать преступления в интернет-пространстве [10, с. 37].

В целом, в уголовном судопроизводстве в ходе доказывания и многих других видов преступлений можно выделить два ключевых направления использования цифровых технологий, а именно:

1. Собираение цифровых доказательств: применение комплексов для изъятия и копирования информации с электронных носителей, использование программ для проверки целостности данных, создание цифровых слепков

(образов) жёстких дисков, протоколирование действий с помощью специализированного программного обеспечения.

2. Исследование цифровых доказательств: проведение судебных экспертиз и исследований с использованием программных пакетов для анализа данных, восстановления удалённой информации, исследования журналов событий, сетевого трафика и метаданных.

Правовой основой для использования таких технологий в процессе доказывания по уголовным делам служат, в частности, Уголовно-процессуальный кодекс Российской Федерации (далее по тексту – УПК РФ) (ст. ст. 74, 164.1 УПК РФ) [11], а также Федеральный закон от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [12] и др.

Однако на пути внедрения и применения цифровых технологий в уголовно-процессуальном доказывании возникает ряд проблем. Так, нами в ходе исследования установлено, что одной из основных проблем является отсутствие единой методики процессуального закрепления (легитимации) цифровых доказательств. Нашу позицию подтверждают многочисленные споры, которые возникают на практике о том, в каком именно порядке должно происходить изъятие электронного носителя и (или) данных из сети «Интернет».

Так, Апелляционным постановлением Приморского краевого суда № 22-1119/2025 22К-1119/2025 от 10.03.2025 года по делу № 3/10-1/25 суд оставил без удовлетворения апелляционную жалобу заявителя и его адвоката, в которой они просили признать незаконными действия следователя органа внутренних дел Российской Федерации касаясь того, что в нарушение ст. 164.1 УПК РФ электронные носители информации изъяты в нарушение, в отсутствие специалиста, сим-карта на экспертизу не направлялась, в качестве вещественного доказательства не признавалась. Суд указал, что, исходя из представленных данных по делу, были назначены компьютерные экспертизы, изъятые в ходе обыска предметы фактически переданы на экспертизу, при этом следователем разъяснены причины, по которым экспертизы длительное время не проведены, оснований ставить под сомнение представление в распоряжение экспертов конкретных предметов не имеется, а то обстоятельство, что изъятая в ходе обыска сим-карта на экспертизу не направлялась и не возвращена, не свидетельствует о незаконности действий должностного лица в целом [13].

В этой связи можно согласиться с А. Б. Сергеевым, который справедливо отмечает, что сведения об обстоятельствах совершенного преступления будут допустимыми (до судебного их исследования), если:



а) сведения (доказательства) получены из одного из источников, указанных в ч. 2 ст. 74 УПК РФ;

б) сведения (доказательства) получены уполномоченным, в том числе на уголовно-процессуальное закрепление, должностным лицом (следователем, дознавателем);

в) сведения получены законным способом;

г) при проведении следственного действия (законный способ) порядок производства (процедура, алгоритм, последовательность этапов) выдержан и не нарушен.

В итоге, следует согласиться с А. Б. Сергеевым в том, что «Соблюдение перечисленных требований обеспечивает достаточно высокий уровень качества досудебного производства и в целом отправление правосудия по уголовным делам в сфере компьютерной информации» [14, с. 70].

В качестве другой проблемы, связанной с использованием цифровых технологий в уголовно-процессуальном доказывании преступлений, совершенных в сфере компьютерной информации, можно выделить проблему соблюдения сроков проведения следственных действий, осложненных необходимостью применения таких технологий. Действительно, как свидетельствует практика, процессы копирования и анализа больших массивов данных могут занимать недели и даже месяцы, что не всегда укладывается в общие сроки предварительного расследования, установленные ст. 162 УПК РФ, особенно в сроки меры пресечения, применяемой в отношении обвиняемого. Существование такой проблемы подтверждается и результатами исследования А. Г. Холевчука и А. В. Савченко, которые установили, что из-за большого количественного роста запоминающих устройств привлекаемые в процесс доказывания по уголовным делам специалисты сталкиваются с нехваткой времени для создания криминалистического изображения предметного устройства или обработки всех обнаруженных данных [15, с. 149]. Безусловно, такие ситуации создают риски как для защиты прав обвиняемого на разумный срок уголовного судопроизводства в отношении него, так и для обеспечения полноты и всесторонности расследования уголовного дела.

Подтверждением такому выводу служит Апелляционное постановление Московского областного суда № 22К-4591/2017 от 14.06.2017 года по делу № 22К-4591/2017, которым было оставлено без удовлетворения апелляционное представление помощника Раменского городского прокурора К. об отмене постановления суда об избрании обвиняемому в совершении преступлений, предусмотренных ч. 3 ст. 159.6, ч. 2 ст. 273 УК РФ, меры пресечения в виде залога в размере 1 500 000 руб. и направлении ходатайства следователя на новое судебное рассмотрение. В обоснование своих требований К. указала,

что обвиняемый обвиняется в совершении тяжких преступлений, связанных с обманом граждан в сфере компьютерной информации, вину не признал, до задержания не работал и не имел постоянных источников дохода, имея заграничный паспорт, может скрыться от следствия и суда, по делу не выполнены в полном объеме следственные и процессуальные действия, находясь на свободе, обвиняемый может помешать следствию, в т. ч. вступить в преступный сговор с находящимися на свободе лицами, причастными к совершению указанных преступлений, скрывающимися от следствия и продолжить заниматься преступной деятельностью в сфере компьютерной информации, связанной с телекоммуникационной сетью «Интернет». По мнению следователя, оснований для изменения меры пресечения обвиняемому не имеется. Заявленное ходатайство следователь обосновала необходимостью проведения следственных действий, направленных на сбор доказательств, иных следственных действий, в частности, получить заключения по двум ранее назначенным судебным компьютерно-техническим экспертизам, ознакомить заинтересованных лиц с заключениями экспертов, получить ответы на ранее направленные запросы и поручения, собрать в полном объеме характеризующий материал на обвиняемых, установить иных лиц, причастных к совершению преступлений по настоящему делу, выполнить иные следственные действия, направленные на окончание расследования, выполнить требования ст. ст. 215-220 УПК РФ, на что потребуется дополнительное время не менее 2 месяцев. Суд первой инстанции, исходя из предоставленного следствием и защитой материалов, в т. ч., характеризующих личность обвиняемого, пришёл к правильному выводу о необходимости изменения обвиняемому меры пресечения с домашнего ареста на залог. Суд апелляционной инстанции приходит к выводу, что постановление суда первой инстанции соответствует требованиям ст. 7 УПК РФ, вынесено с соблюдением норм уголовно-процессуального законодательства, регламентирующих решение судом данного вопроса, и поэтому оснований для отмены постановления суда по доводам апелляционного представления помощника прокурора об изменении меры пресечения на более строгую (домашний арест) суд апелляционной инстанции не находит [16].

Для оптимизации процесса доказывания по уголовным делам о преступлениях в сфере компьютерной информации, следуя результатам авторского исследования и существующим позициям учёных-правоведов в теории уголовного процесса, можно предложить следующие пути решения выявленных проблем:

1. Закрепить в ст. 5 УПК РФ «Основные понятия» такие определения, как «цифровые технологии», «аппаратно-программный комплекс»,

«цифровые доказательства», что унифицирует терминологию и снизит почву для правовых споров между участниками уголовного судопроизводства.

2. Разработать и внедрить в УПК РФ отдельную главу или регламентировать в ст. 164.1 УПК РФ детальный порядок производства следственных действий с использованием цифровых технологий, включая типовые формы протоколов и требования к используемому программному обеспечению.

3. Внести изменения в ст. 162 УПК РФ, предусмотрев специальные основания и порядок продления сроков предварительного следствия по делам, связанным с необходимостью анализа значительных объёмов компьютерной информации.

4. Создать и законодательно утвердить национальные стандарты для программного обеспечения и ведомственные методики, которые бы использовались при работе с цифровыми доказательствами, что обеспечило бы единообразие и проверяемость проводимых действий.

В завершение можно сделать общий вывод о том, что использование цифровых технологий в доказывании по делам о компьютерных преступлениях является объективной необходимостью. Преодоление существующих правовых и организационных пробелов требует комплексного подхода, включающего совершенствование уголовно-процессуального законодательства, развитие специальных (цифровых) знаний у правоприменителей и формирование единой судебно-следственной практики.

### Литература

1. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 года № 63-ФЗ (ред. от 15.10.2025 года) // СПС «КонсультантПлюс».

2. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: Постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 года № 37 // СПС «КонсультантПлюс».

3. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 02.07.2021 года № 400 // СПС «КонсультантПлюс».

4. Пастухов П. С. Основные направления цифровизации уголовно-процессуальной деятельности // Пенитенциарная система и общество: опыт взаимодействия: сборник материалов VIII Международной научно-практической конференции, Пермь, 6-8 апреля 2021 года. Том 1. Пермь:



Пермский институт Федеральной службы исполнения наказаний, 2021. С. 21-24. EDN: [UJRUFA](#).

5. 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 (77). С. 42-57. DOI: [10.12737/jflcl.2019.4.4](#).

6. Гришин Д. А. Цифровизация досудебного уголовного судопроизводства // Вестник Томского государственного университета. 2020. № 455. С. 208-215. DOI: [10.17223/15617793/455/28](#).

7. Малина М. А. Цифровизация российского уголовного процесса: искусственный интеллект для следователя или вместо следователя // Российский следователь. 2021. № 2. С. 29-32. DOI: [10.18572/1812-3783-2021-2-29-32](#).

8. Попова Ю. С. Использование цифровых доказательств в расследовании киберпреступлений // Технологии, образование, наука: современные теории и прикладные исследования: Сборник научных трудов по материалам Международной научно-практической конференции, Белгород, 14 ноября 2023 года. Белгород: ООО «Агентство перспективных научных исследований», 2023. С. 27-30. EDN: [LFNAKR](#).

9. Войтович Х. И. К вопросу о цифровизации российского уголовного судопроизводства // Вестник науки. 2023. № 6 (63). С. 403-413. EDN: [CWMION](#).

10. Палиева О. Н., Семенцова И. А. Использование искусственного интеллекта и информационных технологий в ходе расследования уголовных дел // Вестник Московского университета им. С.Ю. Витте. Серия 2. Юридические науки. 2021. № 2 (28). С. 35-40.

11. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 года № 174-ФЗ (ред. от 31.07.2025 года) (с изм. и доп., вступ. в силу с 01.09.2025 года) // СПС «КонсультантПлюс».

12. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 года № 149-ФЗ (ред. от 24.06.2025 года) (с изм. и доп., вступ. в силу с 01.09.2025 года) // СПС «КонсультантПлюс».

13. Апелляционное постановление Приморского краевого суда № 22-1119/2025 22К-1119/2025 от 10.03.2025 года по делу № 3/10-1/25 // Судебные и нормативные акты Российской Федерации: сайт. URL: <https://sudact.ru/regular/doc/M93Fiy2lGIJj/?ysclid=mh7v9nv3sh668013895> (дата обращения: 21.10.2025 года).

14. Сергеев А. Б. «Цифровое» доказательственное право при производстве по уголовным делам о преступлениях в сфере компьютерной информации: вопросы целесообразности // Юридическая наука и правоохранительная практика. 2022. № 3 (61). С. 66-72.

15. Холевчук А. Г., Савченко А. В. Проблемы использования цифровых средств доказывания при расследовании преступлений в сфере компьютерной информации // Вестник Нижегородского университета им. Н.И. Лобачевского. 2021. № 5. С. 149-154. DOI: [10.52452/19931778\\_2021\\_5\\_149](https://doi.org/10.52452/19931778_2021_5_149).

16. Апелляционное постановление Московского областного суда № 22К-4591/2017 от 14.06.2017 года по делу № 22К-4591/2017 // Судебные и нормативные акты Российской Федерации: сайт. URL: <https://sudact.ru/regular/doc/fRwxtlg3CDQY/?ysclid=mh7vam69pzl47284094> (дата обращения: 23.10.2025 года).

### References

1. The Criminal Code of the Russian Federation: Federal Law No. 63-FZ of 13.06.1996 (as amended on 15.10.2025). *ConsultantPlus Legal Reference System*. (In Russ.).

2. On some issues of judicial practice in criminal cases of crimes in the field of computer information, as well as other crimes committed using electronic or information and telecommunication networks, including the Internet: Resolution of the Plenum of the Supreme Court of the Russian Federation dated 12/15/2022 No. 37. *ConsultantPlus Legal Reference System*. (In Russ.).

3. On the National Security Strategy of the Russian Federation: Decree of the President of the Russian Federation dated 07/02/2021 No. 400. *ConsultantPlus Legal Reference System*. (In Russ.).

4. Pastukhov P. S. The main directions of digitalization of criminal procedural activities. *The Penitentiary System and Society: The Experience of Interaction*. Proceedings of the VIII International Scientific and Practical Conference, Perm, April 6-8, 2021. Volume 1. Perm: Perm Institute of the Federal Penitentiary Service Publ.; 2021: 21-24. (In Russ.).

5. Zaitsev O. A. Features of using electronic information as evidence in a criminal case: comparative legal analysis of foreign legislation. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya*. 2019; 4 (77): 42-57. (In Russ.).

6. Grishin D. A. Digitalization of pre-trial criminal proceedings. *Bulletin of Tomsk State University*. 2020; 455: 208-215. (In Russ.).

7. Malina M. A. Digitalization of the Russian criminal process: artificial intelligence for the investigator or instead of the investigator. *Rossiiskij sledovatel'*. 2021; 2: 29-32. (In Russ.).

8. Popova Yu. S. The use of digital evidence in the investigation of cybercrimes. *Technology, education, science: modern theories and applied research*. A collection of scientific papers based on the materials of the International Scientific and Practical Conference, Belgorod, November 14, 2023. Belgorod: Agency for Advanced Scientific Research Publ.; 2023: 27-30. (In Russ.).
9. Voitovich H. I. On the issue of digitalization of Russian criminal proceedings. *Vestnik nauki*. 2023; 6 (63): 403-413. (In Russ.).
10. Palieva O. N., Sementsova I. A. The use of artificial intelligence and information technologies during the investigation of criminal cases. *Bulletin of the Witte Moscow University. Series 2. Legal Sciences*. 2021; 2 (28): 35-40. (In Russ.).
11. The Criminal Procedure Code of the Russian Federation: Federal Law No. 174-FZ of December 18, 2001 (as amended on July 31, 2025) (as amended and supplemented, intro. effective from 01.09.2025) *ConsultantPlus Legal Reference System*. (In Russ.).
12. On Information, Information Technologies and Information Protection: Federal Law No. 149-FZ of 27.07.2006 (as amended on 24.06.2025) (as amended and supplemented, intro. effective from 09/01/2025) *ConsultantPlus Legal Reference System*. (In Russ.).
13. Appeal resolution of the Primorsky Regional Court No. 22-1119/2025 22K-1119/2025 dated 10.03.2025 in case No. 3/10-1/25. *Judicial and regulatory acts of the Russian Federation*. Available at: <https://sudact.ru/regular/doc/M93Fiy2lGIJj/?ysclid=mh7v9nv3sh668013895> (accessed: 10/21/2025). (In Russ.).
14. Sergeev A. B. "Digital" evidentiary law in criminal proceedings on crimes in the field of computer information: issues of expediency. *Yuridicheskaya nauka i pravookhranitel'naya praktika*. 2022; 3 (61): 66-72. (In Russ.).
15. Kholevchuk A. G., Savchenko A.V. Problems of using digital means of evidence in the investigation of crimes in the field of computer information. *Bulletin of the Nizhny Novgorod University named after N.I. Lobachevsky*. 2021; 5: 149-154.
16. Moscow Regional Court Appeal Resolution No. 22K-4591/2017 of 14.06.2017 in case No. 22K-4591/2017. *Judicial and Regulatory Acts of the Russian Federation*. Available at: <https://sudact.ru/regular/doc/fRwxtlg3CDQY/?ysclid=mh7vam69pz147284094> (accessed: 23.10.2025). (In Russ.).

***Информация об авторах***

**Яковлев Даниил Сергеевич** - ассистент кафедры уголовного процесса и криминалистики, Алтайский государственный университет, г. Барнаул, Россия.

e-mail: [sega708-1980@mail.ru](mailto:sega708-1980@mail.ru)

***Information about the authors***

**Yakovlev, Daniil S.** - Assistant of the Department of Criminal Procedure and Criminalistics, Altai State University, Barnaul, Russia.

e-mail: [sega708-1980@mail.ru](mailto:sega708-1980@mail.ru)

***Для цитирования***

Яковлев Д. С. Использование цифровых (электронных) технологий в процессе доказывания по уголовным делам о преступлениях в сфере компьютерной информации // Журнал Высокотехнологичное право. – 2025. Т. 1, № 2. – С. 103-114.

***For citation***

Yakovlev D. S. Use of digital (electronic) technologies in the procedure of evidence in criminal cases on computer information crimes // Journal of High-tech Law. – 2025. Vol. 1, No. 2. – Pp. 103-114.

Поступила в редакцию / Received 25.11.2025

Поступила после рецензирования / Received after review 12.12.2025

Принята к публикации / Accepted 15.12.2025