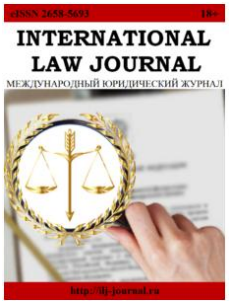
ISSN 2658-5693
https://ilj-journal.ru



Научно-исследовательский журнал «International Law Journal»
https://ilj-journal.ru
2025, Том 8, № 8 / 2025, Vol. 8, Iss. 8 https://ilj-journal.ru/archives/category/publications
Научная статья / Original article
Шифр научной специальности: 5.1.4. Уголовно-правовые науки (юридические науки)
УДК 343.985

Сравнительный анализ следственных тактик зарубежных стран в отношении цифровых данных

[1] Эзейбэ П.Э.,
[1] Кубанский государственный университет

Аннотация: *целью статьи является проведение сравнительного анализа следственных тактик зарубежных стран, определение возможности их адаптации к условиям российского уголовного процесса. Аавтором рассматриваются правовые и организационно-технические основы сбора, фиксации, хранения, анализа и использования цифровых данных в уголовном процессе на примере США, Великобритании и Франции. Анализ показал, что общими для всех трёх юрисдикций являются: приоритет судебного контроля, документирование процедур и экспертная верификация цифровых данных. При этом подходы различаются по степени процессуальной формализации, где американская модель основана на конституционных гарантиях частной жизни и строгих стандартах аутентификации, британская – профессиональной стандартизации и независимом аудите, французская – высокой формализации и институциональной централизации. Внедрение в российскую правовую систему института аутентификации цифровых доказательств, сертификации экспертов и судебного контроля за доступом к зашифрованной информации будет способствовать повышению достоверности и процессуальной защищённости цифровых доказательств.*

Ключевые слова*: цифровые доказательства, следственная тактика, криминалистика, уголовный процесс, аутентификация, цепочка хранения*

Для цитирования: Эзейбэ П.Э. Сравнительный анализ следственных тактик зарубежных стран в отношении цифровых данных // International Law Journal. 2025. Том 8. № 8. С. 59 – 64.

Поступила в редакцию: 22 августа 2025 г.; Одобрена после рецензирования: 19 октября 2025 г.; Принята к публикации: 16 декабря 2025 г.

Comparative analysis of investigative tactics of foreign countries in relation to digital data

[1] Ezeibe P.E.,
[1] Kuban State University

Abstract: *the purpose of the article is to conduct a comparative analysis of investigative tactics of foreign countries, to determine the possibility of their adaptation to the conditions of the Russian criminal process. The author examines the legal and organizational and technical foundations of the collection, recording, storage, analysis and use of digital data in criminal proceedings using the example of the United States, Great Britain and France. The analysis showed that the priority of judicial control, documentation of procedures and expert verification of digital data are common to all three jurisdictions. At the same time, approaches differ in the degree of procedural formalization: the American model is based on constitutional guarantees of privacy and strict authentication standards, the British model is based on professional standardization and independent audit, the French model is based on high formalization and institutional centralization. The introduction of the institute of digital evidence authentication, expert certification and judicial control over access to encrypted information into the Russian legal system will help to increase the reliability and procedural security of digital evidence.*

ISSN 2658-5693
https://ilj-journal.ru

Keywords: *digital evidence, investigative tactics, criminalistics, criminal procedure, authentication, storage chain*

For citation: Ezeibe P.E. Comparative analysis of investigative tactics of foreign countries in relation to digital data. International Law Journal. 2025. 8 (8). P. 59 – 64.

The article was submitted: August 22, 2025; Approved after reviewing: October 19, 2025; Accepted for publication: December 16, 2025.

Введение

Цифровая революция «индустриализировала» масштаб известных ранее видов преступлений, таких как мошенничество, и стимулировала появление новых цифровых форм преступности. Согласно оценкам CompTIA, мировые убытки от киберпреступности в 2025 году увеличатся на 10% по сравнению с 2024, достигнув показателя в 10,5 триллионов [14]. Цифровые данные и цифровые следы становятся ключевыми источниками доказательственной информации, однако их использование связано с особыми требованиями к процессуальной допустимости, достоверности и сохранности [1, 2]. Практика показывает, что традиционные криминалистические подходы не всегда обеспечивают достаточный уровень защиты и воспроизводимости цифровых следов [12]. Таким образом, актуальность настоящего исследования обусловлена необходимостью адаптации зарубежных следственных тактик к российской правовой системе, выработки единых стандартов цифровой криминалистики и повышения уровня процессуальной защищённости цифровых доказательств в условиях цифровизации уголовного судопроизводства.

Цель исследования – проведение сравнительного анализа следственных тактик зарубежных стран, определение возможности их адаптации к условиям российского уголовного процесса.

Задачи – проанализировать нормативно-правовые основы обращения с цифровыми доказательствами в США, Великобритании и Франции; выявить ключевые элементы зарубежных моделей цифровой криминалистики.

Гипотеза – комплексная адаптация зарубежных следственных тактик обращения с цифровыми доказательствами способна обеспечить повышение достоверности и процессуальной защищённости цифровых доказательств в российском уголовном процессе за счёт формирования унифицированных и воспроизводимых процедур их получения, обработки и оценки.

Материалы и методы исследований

В исследовании применены следующие общенаучные и специальные юридические методы: сравнительно-правовой метод, системно-структурный анализ, формально-юридический метод, логический и сравнительно-исторический методы.

Эмпирическая база исследования: нормативные правовые акты, информация по судебным делам, научная литература, материалы средств массовой информации.

Результаты и обсуждения

В уголовном процессе под следственной тактикой понимают систему научно обоснованных приёмов и методов организации расследования, направленных на получение и использование доказательственной информации [3]. В сфере цифровых данных следственная тактика объединяет процессуальные, криминалистические и технические приёмы, обеспечивающие законность и обоснованность действий правоохранительных органов, сохранение целостности и неизменности информации, воспроизводимость экспертных процедур, допустимость и надёжность представленных данных в суде [4].

Следственная тактика США при работе с цифровыми доказательствами строится на принципах судебного контроля, технической верификации и полной прозрачности действий следователя; тактика сочетает строгие правовые гарантии защиты частной жизни с высоким уровнем стандартизации криминалистических процедур. Нормативное регулирование обращения с цифровыми доказательствами формируется на основе комплекса конституционных, законодательных и судебных норм, закрепляющих баланс между интересами уголовного правосудия и конституционными правами граждан на неприкосновенность частной жизни и тайну переписки. Центральное значение имеет Четвёртая поправка к Конституции США, провозглашающая недопустимость необоснованных обысков и выемок [7], согласно которой изъятие информации, хранящейся на электронных устройствах, допустимо лишь при наличии судебного ордера, выданного на основании достаточных оснований для подозрения [5].

Криминалистические исследования цифровых носителей осуществляются исключительно сертифицированными экспертами, деятельность которых регулируется стандартами [13]. Практическая реализация принципов сохранности и достоверности цифровых доказательств обеспечивается системой «цепочки вла-

ISSN 2658-5693
https://ilj-journal.ru

дения» (chain of custody), включающей строгий учёт всех этапов обращения с цифровыми носителями – от момента их изъятия до представления в суде. Каждое действие документируется, носители опечатываются, маркируются и хранятся в условиях, исключающих несанкционированный доступ или модификацию данных [5].

На судебной стадии ключевое значение имеют нормы Federal Rules of Evidence (FRE), регулирующие порядок признания цифровых данных доказательствами. Правила FRE 901–902 устанавливают требования к аутентификации и допускают использование электронных доказательств при условии надлежащего подтверждения их происхождения и достоверности. Особое внимание заслуживают положения FRE 902(13) и FRE 902(14), введённые в 2017 году, которые допускают возможность самоаутентификации электронных данных, если они сопровождаются цифровыми сертификатами подлинности и экспертными заключениями, подтверждающими отсутствие изменений в ходе анализа [5].

Основу нормативного регулирования обращения с цифровыми доказательствами в Великобритании составляют Police and Criminal Evidence Act (PACE), Regulation of Investigatory Powers Act (RIPA) и Investigatory Powers Act (IPA) [10], которые определяют правовой режим сбора, хранения и использования цифровой информации в уголовном процессе, устанавливая баланс между эффективностью расследования и защитой прав личности. В частности, PACE регулирует полномочия полиции при проведении обысков и выемок, включая изъятие электронных носителей информации. Согласно положениям данного акта, любое изъятие цифровых устройств или копирование их содержимого должно осуществляться на основании судебного ордера, выданного компетентным органом, при наличии достаточных оснований для подозрения. Дополнительное регулирование обеспечивают акты RIPA и IPA, касающиеся получения метаданных, а также доступа к зашифрованной информации. RIPA устанавливает систему разрешений на оперативно-розыскные мероприятия, включая электронное наблюдение, с обязательным судебным контролем. Investigatory Powers Act, который стал реакцией на угрозы в сфере цифровых коммуникаций и законодательно закрепил механизмы взаимодействия следственных органов с интернет-провайдерами и операторами связи [8].

Особое место в практике Великобритании занимает внедрение и применение профессиональных стандартов, разработанных Ассоциацией начальников полиции (ACPO, ныне NPCC) и Регулятором судебной экспертизы (Forensic Science Regulator, FSR). Руководство ACPO Good Practice Guide for Digital Evidence установило четыре фундаментальных принципа цифровой криминалистики, ставших эталоном не только в Великобритании, но и в международной практике: неприкосновенность данных, полная фиксация, воспроизводимость, ответственность эксперта (рис. 1). Дальнейшее развитие британская система получила с введением обязательных стандартов Forensic Science Regulator Codes of Practice and Conduct, которые распространяются на весь цикл цифрового анализа, от конфискации и хранения до интерпретации результатов экспертизы. Кодексы предписывают использование сертифицированных инструментов и проведение процедур в лабораториях, аккредитованных по стандарту ISO/IEC 17025. Регулятор судебной экспертизы обладает правом приостанавливать деятельность лабораторий, нарушающих стандарты качества, что обеспечивает высокий уровень доверия судов к цифровым доказательствам [9].

Рис. 1. Фундаментальные принципы цифровой криминалистики [10].
Fig. 1. Fundamental principles of digital forensics [10].

ISSN 2658-5693
https://ilj-journal.ru

Британская система обращения с цифровыми доказательствами отличается высокой степенью нормативной детализации и профессиональной стандартизации. Система сочетает строгий судебный контроль с технической дисциплиной, в рамках которой минимизирован риск недопустимости доказательств в суде и одновременно обеспечена защита прав граждан от произвольного вмешательства в частную жизнь.

Французская система обращения с цифровыми доказательствами опирается на принципы континентального права и характеризуется высокой степенью процессуальной формализации действий следственных органов. Центральным нормативным источником является Уголовно-процессуальный кодекс Франции (CPP), который содержит специальные нормы, регулирующие порядок обыска, изъятия, хранения и анализа цифровых данных. К числу ключевых положений относятся статьи 56, 94, 97, 706-95-1 и 706-102-1 CPP, формирующие систему процедур обращения с электронными доказательствами в ходе уголовного расследования [6].

Согласно статье 56 CPP, следователь или уполномоченный прокурор вправе изымать любые предметы и документы, имеющие значение для расследования, включая компьютерные устройства, цифровые носители и сетевое оборудование. На законодательном уровне предусмотрена возможность не только физического изъятия, но и создания цифровой копии данных непосредственно на месте проведения следственного действия [6]. Доступ к данным, хранимым у провайдеров или операторов связи, регулируется статьями 706-95-1 и 706-95-2 CPP, которые устанавливают механизм получения логов, электронных сообщений и иной цифровой информации на основании мотивированного постановления прокурора или следственного судьи.

Французская правоприменительная практика исходит из принципа «свободы доказательств», согласно которому суд может принять во внимание любые законно полученные сведения, независимо от их формы, если они обладают признаками достоверности и не нарушают права сторон. Суд самостоятельно оценивает допустимость цифровых данных, исходя из совокупности обстоятельств получения, хранения и представления доказательств [11]. Во французской системе экспертное исследование цифровых доказательств проводится исключительно специалистами, аккредитованными при судебных органах. При проведении экспертизы используются специализированные программные средства, прошедшие сертификацию, а результаты оформляются в виде отчёта, который имеет доказательственную силу в суде.

Французская модель характеризуется процессуальным контролем, институциональной централизацией и акцентом на судебную ответственность при обращении с цифровыми доказательствами. Гибкость принципа свободы доказательств с высокой степенью формализации процедур их получения и анализа обеспечивает не только доказательственную надёжность цифровых данных, но и баланс между интересами уголовного преследования и защитой фундаментальных прав личности.

Сравнительный анализ показал, что общим для всех трёх юрисдикций является приоритет судебного контроля, документирования процедур и экспертной верификации данных. Вместе с тем подходы различаются по степени процессуальной формализации и акцентам регулирования. Американская модель основана на конституционных гарантиях частной жизни и сочетает правовую регламентацию с жёсткими техническими стандартами аутентификации. Британская система сочетает профессиональную стандартизацию и независимый аудит криминалистических процедур. Французская модель характеризуется институциональной централизацией, высокой степенью формализации и судебной ответственностью эксперта, а принцип «свободы доказательств» обеспечивает суду дискреционные полномочия в оценке цифровых материалов.

Опыт США показывает, что ключевым элементом следственных действий является аутентификация цифровых данных, закреплённая в правилах FRE 901-902. Отсутствие аналогичных норм в российском праве осложняет оценку достоверности электронных материалов. Перспективным направлением является введение в УПК РФ положений, устанавливающих критерии аутентификации и требования к документированию технологического процесса извлечения данных. Британская практика подтверждает необходимость сертификации экспертов и лабораторий как условия допустимости цифровых доказательств. В России аналогичная система аккредитации позволила бы обеспечить единый уровень качества экспертных исследований и повысить доверие судов к результатам цифровых экспертиз. Кроме того, зарубежный опыт позволяет судить о необходимости судебного контроля за доступом к зашифрованной информации.

Выводы

Адаптация зарубежного опыта в российскую правовую систему должна основываться на институциональном внедрении наиболее эффективных элементов зарубежных моделей, прежде всего, процедур аутентификации цифровых данных, сертификации экспертов и аккредитации криминалистических лабораторий. Важно закрепить на законодательном уровне требования к документированию технологического процесса извлечения и анализа данных, а также установить обязательный судебный контроль за доступом к зашифрованной информации.

ISSN 2658-5693
https://ilj-journal.ru

Список источников

1. Ищенко П.П. Следственные действия в условиях цифровизации уголовного судопроизводства // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. № 1. С. 30 – 42.
2. Овчинникова О.В. Производство дистанционных следственных действий: опыт зарубежных стран // Правопорядок: история, теория, практика. 2023. №3 (38). С. 87 – 91.
3. Приказ СК России от 08.08.2013 N 53 "Об организации работы следователей-криминалистов в Следственном комитете Российской Федерации" // СПС Консультант Плюс. URL: https://www.consultant.ru/document/cons_doc_LAW_219616/ (дата обращения: 19.07.2025)
4. Фокин А.Д., Принципы и тактика проведения следственного осмотра интернет-ресурса при расследовании дистанционного мошенничества в сфере недвижимости // Российский следователь. 2025. № 3. С. 2 – 7.
5. Aitchison S. Comment, Privacy in the Cloud: The Fourth Amendment Fog // Washington Law Review. 2018. Vol. 93. № 2. P. 1019 – 1055.
6. Code de procédure pénale. URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154/ (дата обращения: 30.09.2025)
7. Constitution of the United States. Fourth Amendment. URL: https://constitution.congress.gov/constitution/amendment-4/ (дата обращения: 17.07.2025)
8. Digital Forensics and Crime. URL: https://researchbriefings.files.parliament.uk/documents/POST-PN-0520/POST-PN-0520.pdf (дата обращения: 25.07.2025)
9. Forensic science providers: codes of practice and conduct. URL: https://www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct (дата обращения: 26.07.2025)
10. Fussey P., Sandhu A.. Surveillance arbitration in the era of digital policing // Theoretical Criminology. 2020. Vol. 26(1). P. 3 – 22.
11. Meissonnier A., Banat-Berger F. French legal framework of digital evidence // Records Management Journal. 2015. Vol. 25. P. 96 – 106.
12. Noland A. Current Challenges of Digital Forensics // Themis: Research Journal of Justice Studies and Forensic Science. 2024. Vol. 12. Iss. 1. Article 1.
13. Special Publication 800-101 Revision 1, Guidelines on Mobile Device Forensics. URL: https://csrc.nist.gov/news/2014/sp-800-101-revision-1,-guidelines-on-mobile-device (дата обращения: 22.07.2025)
14. The cost of cybercrime statistics is projected to be $10.5 trillion annually by 2025. URL: https://deepstrike.io/blog/cybercrime-statistics-2025 (дата обращения: 11.07.2025)

References

1. Ishchenko P.P. Investigative actions in the context of digitalization of criminal proceedings. Siberian criminal procedural and forensic readings. 2022. No. 1. P. 30 – 42.
2. Ovchinnikova O.V. Remote investigative actions: experience of foreign countries. Law and order: history, theory, practice. 2023. No. 3 (38). P. 87 – 91.
3. Order of the Investigative Committee of Russia dated 08.08.2013 N 53 "On the organization of the work of forensic investigators in the Investigative Committee of the Russian Federation". SPS Consultant Plus. URL: https://www.consultant.ru/document/cons_doc_LAW_219616/ (date of access: 19.07.2025)
4. Fokin A.D., Principles and tactics of conducting an investigative inspection of an online resource during the investigation of remote fraud in the real estate sector. Russian investigator. 2025. No. 3. P. 2 – 7.
5. Aitchison S. Comment, Privacy in the Cloud: The Fourth Amendment Fog. Washington Law Review. 2018. Vol. 93. No. 2. P. 1019 – 1055.
6. Code de procédure pénale. URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154/ (date of access: 30.09.2025)
7. Constitution of the United States. Fourth Amendment. URL: https://constitution.congress.gov/constitution/amendment-4/ (date of access: 07.17.2025)
8. Digital Forensics and Crime. URL: https://researchbriefings.files.parliament.uk/documents/POST-PN-0520/POST-PN-0520.pdf (date of access: 07.25.2025)
9. Forensic science providers: codes of practice and conduct. URL: https://www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct (date of access: 07.26.2025)

ISSN 2658-5693
https://ilj-journal.ru

10. Fussey P., Sandhu A.. Surveillance arbitration in the era of digital policing. Theoretical Criminology. 2020. Vol. 26(1). P. 3 – 22.
11. Meissonnier A., Banat-Berger F. French legal framework of digital evidence. Records Management Journal. 2015. Vol. 25. P. 96 – 106.
12. Noland A. Current Challenges of Digital Forensics. Themis: Research Journal of Justice Studies and Forensic Science. 2024. Vol. 12. Iss. 1. Article 1.
13. Special Publication 800-101 Revision 1, Guidelines on Mobile Device Forensics. URL: https://csrc.nist.gov/news/2014/sp-800-101-revision-1,-guidelines-on-mobile-device (date of access: 07.22.2025)
14. The cost of cybercrime statistics is projected to be $10.5 trillion annually by 2025. URL: https://deepstrike.io/blog/cybercrime-statistics-2025 (date of access: 07.11.2025)

Информация об авторе

Эзейбэ П.Э., аспирант, Кубанский государственный университет