DOI 10.37882/2223-2966.2026.03.18

БЕЗОПАСНОСТЬ ЦИФРОВЫХ КОММУНИКАЦИЙ АДВОКАТА: ПРАВОВЫЕ И ТЕХНИЧЕСКИЕ АСПЕКТЫ ВЫБОРА НАДЕЖНЫХ КАНАЛОВ СВЯЗИ

LAWYER'S DIGITAL COMMUNICATIONS SECURITY: LEGAL AND TECHNICAL ASPECTS OF CHOOSING RELIABLE COMMUNICATION CHANNELS

I. Korotkiy

Summary. The article focuses on current issues related to the protection of confidential data by lawyers when using digital communications. The study pays particular attention to key global trends in information security in the activities of attorneys in different countries around the world. A comparative analysis of the regulatory framework and standards for ensuring cyber security of legal services is also conducted, using Russia, the United States, the United Kingdom, and the European Union as examples. Based on the analysis, technical criteria for selecting and verifying secure digital communication channels in legal practice are systematised.

Keywords: lawyer, digital communications, protection, confidentiality, data.

Короткий Игорь Игоревич
Аспирант, ФГАОУ ВО Российский государственный гуманитарный университет, г. Москва
i.korotkiy@bk.ru

Аннотация. Статья посвящена актуальным вопросам, связанным с защитой адвокатами конфиденциальных данных при использовании цифровых коммуникаций. Отдельное внимание в процессе исследования уделено ключевым глобальным трендам информационной безопасности в деятельности адвокатов в разных странах мира. Также проведен сравнительный анализ нормативно-правовой базы и стандартов обеспечения киберзащиты в адвокатской практике на примере России, США, Великобритании и Европейского Союза. На основании проведенного анализа систематизированы технические критерии выбора и верификации защищенных каналов цифровой коммуникации в адвокатской деятельности.

Ключевые слова: адвокат, цифровые коммуникации, защита, конфиденциальность, данные.

Адвокаты выступают ключевыми институтами доверия и правовой добросовестности в сфере оказания квалифицированной юридической помощи и защиты законных интересов доверителей. Их профессиональная деятельность включает проведение комплексной юридической проверки (due diligence), в том числе идентификацию доверителей и их полномочий, оценку правомерности планируемых действий, а также минимизацию правовых рисков и подтверждение юридической чистоты сопровождаемых процедур [1]. Одной из фундаментальных обязанностей адвоката является формирование и соблюдение эффективной политики защиты конфиденциальной информации и персональных данных клиентов, включая предотвращение несанкционированного доступа, утечек и неправомерного использования сведений.

В данном контексте необходимо отметить, что профессия адвоката, ее процессы и практика претерпели стремительные изменения с ростом глобализации и новыми требованиями к доступности юридической помощи в цифровом формате, что также привело к появлению новых правил, защищающих эти фундаментальные юридические процессы от киберрисков. В условиях цифровизации адвокатской деятельности и расширения электронных сервисов вопросы конфиденциальности, информационной безопасности и защиты сведений, отнесенных к охраняемым законом видом тайн, приобретают особую актуальность, поскольку адвокаты все чаще взаимодействуют с электронными реестрами, цифровыми документами и удалёнными каналами коммуникации, что требует внедрения дополнительных организационных и технологических мер защиты информации [2].

Наглядно о сложившейся ситуации свидетельствуют количественные показатели, характеризующие состояние информационной безопасности цифровых каналов связи в нотариальной и юридической деятельности (см. табл. 1). Данные, представленные в таблице 1, отражают корреляцию между развитием технологических векторов атак и эффективностью существующих систем защиты информации в различных странах за период 2024–2025 годов.

Итак, принимая во внимание сведения, представленные в таблице 1, очевидна потребность в разработке практических рекомендаций, контрольных списков, а также общеправовых обязанностей для адвокатов принимать компетентные и разумные меры, связанные с защитой информации, усовершенствованием систем

Таблица 1.

Глобальные технологические тренды информационной безопасности цифровых каналов связи в адвокатской деятельности (2024–2025 гг.).

Параметр анализа	РФ	США	ЕС	Глобальный технологический тренд
Интенсивность кибератак (единиц инцидентов)	118–135	> 31 000	> 4 800	Автоматизация эксплуатации уязвимостей: масштабное сканирование и реализация деструктивного воздействия на сетевые шлюзы.
Объем утечек (миллионов уникальных записей)	710	142,9	110	Интеллектуальная агрегация данных: формирование комплексных векторов угроз путем синтеза данных из гетерогенных источников.
Отраслевая концентрация (процент от общего числа атак)	12 %	14 %	11 %	Эксплуатация доверенного доступа: компрометация привилегированного узла для несанкционированного входа в государственные реестры.
Экономический ущерб (миллионов долларов США)	0,06	10,22	4,4	Рост издержек на репозицию системы: ресурсные затраты на криптографическую регенерацию и аудит информационной инфраструктуры.
Доля применения генеративного ИИ (процент от векторов атаки)	12,50 %	16,00 %	14,50 %	Синтетическая когнитивная атака: применение нейросетевых моделей для имитации биометрических и текстовых признаков идентификации.
Длительность скрытого присутствия (суток)	185	292	215	Латентная эксфильтрация данных: сохранение несанкционированного доступа к трафику каналов связи без прерывания штатных бизнес-процессов.
Уязвимость цепочек поставок (процент успешных проникновений)	24 %	30 %	22 %	Декомпозиция доверенной среды: внедрение вредоносного кода через легитимные механизмы обновления специализированного программного обеспечения.

Составлено автором по данным отчетов «Cost of a Data Breach Report» (IBM Security), «Data Breach Investigations Report» (Verizon), «ENISA Threat Landscape» (Агентство Европейского Союза по кибербезопасности) и аналитических обзоров ПАО «Сбербанк» и ГК «InfoWatch» (2024–2025 гг.)

кибербезопасности и поддержкой эффективных политик, направленных на снижение потенциальных рисков утечки данных.

Таким образом, актуальность и практическая значимость рассматриваемых вопросов предопределили выбор темы данной статьи.

Детальный анализ угроз для данных в компьютерах, мобильных устройствах и информационных системах, используемых адвокатами, описывают в своих трудах Бегичев А.В., Рисовская С.С., Захаркина А.В., Новоселова М.Д., M. Robles-Carrillo, P. García-Teodoro, Özgür Arikan.

Нормативно-правовые аспекты и проблемы, связанные с внедрением цифровых средств в адвокатскую деятельность, а также методы защиты цифровых коммуникаций адвоката рассматривают Фадеев А.В., Воронина П.А., Советкина А.С., Лошкарёв А.В., Коган М.И., Магдеева Д.И.

Технические аспекты использования в цифровых коммуникациях адвокатов стандартизированных сертификатов ИТ-безопасности, таких как ISO 27001, программа Cloud Security Alliance STAR или EuroCloud изучают

Yong Ding, Weiguo Huang, Hai Liang, John Zeleznikow, Hugo Mentzingen, Nuno António, Li Ge, Peng Yan Li.

Высоко оценивая имеющиеся на сегодняшний день труды и наработки, необходимо отметить, что еще широкий спектр вопросов защиты цифровых коммуникаций в адвокатском деле остается нерешенным. Так, например, отдельного внимания заслуживают задачи комплексной оценки устойчивости цифровых каналов к целенаправленным атакам, а также практической интеграции криптографических механизмов с требованиями соблюдения адвокатской тайны и процессуального законодательства. Дополнительную сложность представляет отсутствие единых методик выбора и верификации коммуникационных решений с учётом одновременно технических рисков, правовой ответственности и человеческого фактора.

Таким образом, цель статьи заключается в проведении анализа правовых и технических аспектов выбора надежных каналов связи для обеспечения безопасности цифровых коммуникаций адвоката.

Прежде всего, отметим, что цифровые коммуникации адвоката — это совокупность защищенных высокотехнологичных протоколов, программно-аппаратных средств и инфраструктурных решений, обеспечивающих обмен юридически значимой информацией между адвокатом и субъектами правоотношений (доверителями, судами, государственными органами) [3, 4].

Архитектурные компоненты цифровых коммуникаций включают в себя:

- среды передачи данных: каналы связи, защищенные с помощью криптографических протоколов (TLS/SSL, VPN-туннелирование, ГОСТ-шифрование);
- системы юридически значимого документооборота: платформы для обмена файлами, поддерживающие использование усиленной квалифицированной электронной подписи;
- интерфейсы взаимодействия с государственными ГИС: интеграция с сервисами типа «Электронное правосудие» (ГАС «Правосудие»), «Мой арбитр» и системами Федеральной палаты адвокатов (ККИС ФПА);
- виртуальные переговорные среды: системы видео-конференц-связи, развернутые внутри защищенного контура, исключающие утечку данных на сторонние серверы [5].

Соответственно, учитывая сложность и комплексность цифровых коммуникаций адвоката, а также их критическую значимость для защиты адвокатской тайны и иных охраняемых законом видов тайн, например, персональных данных доверителя, данных предварительного расследования, обеспечение информационной безопасности в деятельности адвокатуры представляет собой сложную междисциплинарную задачу. С точки зрения информационных технологий, адвокатская деятельность характеризуется высокой степенью конфиденциальности обрабатываемых данных и необходимостью обеспечения целостности и доступности юридически значимой информации.

Кратко рассмотрим правовые основы, регламентирующие данные вопросы в разных странах мира.

Российская Федерация. Правовой фундамент данной предметной сферы основан на Федеральном законе «Об адвокатской деятельности и адвокатуре в Российской Федерации», Кодексе профессиональной этики адвоката и Федеральном законе «О персональных данных».

Также в России адвокат обязан следовать рекомендациям, установленным Советом Федеральной палаты адвокатов Российской Федерации (Совет ФПА РФ). Советы адвокатских палат субъектов РФ также могут утверждать рекомендации, обязательные для всех адвокатов, состоящих в палате соответствующего субъекта.

Так 30 ноября 2009 г. Советом ФПА РФ утверждены Рекомендации по обеспечению адвокатской тайны и гарантий независимости адвоката при осуществлении адвокатами профессиональной деятельности.

Ключевой проблемой является отсутствие специализированных отраслевых технических регламентов. Текущая модель предполагает, что адвокат самостоятельно определяет уровень технической защиты, ориентируясь на общие требования законодательства и рекомендации ФПА РФ, что в условиях современных киберугроз создает риски компрометации профессиональной тайны [6].

США. Американская модель отличается высокой степенью детализации через систему прецедентов и нормативных актов Американской ассоциации юристов. На практике широко используется концепция «технологической компетентности», согласно которой адвокат обязан не только знать право, но и понимать риски используемых информационных систем. Основным техническим ориентиром выступают стандарты Национального института стандартов и технологий (NIST) [7].

Великобритания и Европейский Союз. В Великобритании акцент смещен на риск-ориентированный подход и обязательную сертификацию базовых уровней защиты. В ЕС определяющим фактором является Общий регламент по защите данных (GDPR), который накладывает на адвокатские образования обязанности по внедрению организационных и технических мер (шифрование, псевдонимизация), соответствующих актуальному уровню развития науки и техники [8].

Обобщая изученный опыт, в таблице 2 представлена сравнительная характеристика стандартов и норм, действующих в сфере защиты цифровых коммуникаций адвокатов и нотариусов.

Данные, приведенные в таблице 2, позволяют сделать вывод о глобальном переходе от добровольного соблюдения этических норм к императивной стандартизации технических средств защиты информации в деятельности адвокатуры. В отличие от российской модели, ориентированной на организационные меры и локализацию данных, международная практика накладывает на лиц, оказывающих юридическую помощь, прямую обязанность по внедрению сквозного шифрования и прохождению регулярного внешнего аудита киберустойчивости. Итоговые различия в правовых режимах подтверждают необходимость гармонизации отечественных стандартов с международными риск-ориентированными протоколами для обеспечения технологической независимости и соблюдения адвокатской тайны.

На следующем этапе рассмотрим более подробно технические аспекты выбора надежных цифровых каналов связи для обеспечения сохранности и защиты данных в деятельности адвоката.

На практике существует очень широкий спектр критериев и показателей, определяющих безопасность платформы или каналов цифровой коммуникации, используемых адвокатами, вследствие чего их достаточно

Таблица 2.

Сравнительная характеристика стандартов обеспечения информационной безопасности нотариусов в разных странах мира

Параметр сравнения	Российская Федерация	США	Великобритания	Европейский Союз
Нормативная база	Федеральный закон № 63-ФЗ, Кодекс профессиональной этики адвоката	Типовые правила профессиональной этики, Акты ассоциаций штатов	Правила поведения Управления по регулированию деятельности нотариусов	Общий регламент по защите данных (GDPR)
Регламентирующие технические стандарты	Государственные стандарты (ГОСТ) серии 57580 (носят рекомендательный характер)	Специальные публикации Национального института стандартов и технологий (NIST SP 800–53)	Программа «Основы кибербезопасности» (Cyber Essentials)	Международные стандарты ИСО/МЭК 27001 (ISO/IEC 27001)
Требования к криптографической защите	Обязательны для государственных информационных систем; для адвокатов — в рамках защиты персональных данных	Обязательное применение сквозного шифрования при передаче конфиденциальных сведений	Обязательное использование сертифицированных средств криптографии для регулируемых организаций	Строгие требования к шифрованию данных при хранении и передаче согласно принципам минимизации рисков
Регулирование использования облачных вычислений	Требование об обязательном размещении баз данных на территории Российской Федерации	Разрешено при условии проведения всесторонней проверки поставщика услуг на соответствие безопасности	Допускается при наличии детального руководства по управлению рисками в облачной среде	Регламентировано правилами трансграничной передачи данных и стандартами защиты частной жизни
Процедура подтверждения соответствия (сертификация)	В добровольном порядке для адвокатских образований	Требуется для крупных юридических организаций в рамках аудита контроля систем и организаций	Официальная государственная сертификация уровня «Плюс» для работы с государственным сектором	Обязательное подтверждение ответственности контролера данных через механизмы сертификации
Мониторинг и аудит безопасности	Преимущественно внутренний самоконтроль профессионального сообщества	Регулярный внешний аудит в соответствии с требованиями законодательства отдельных штатов	Систематический аудит в рамках общей системы управления правовыми рисками	Обязательная оценка воздействия на защиту данных при использовании новых технологий

(*составлено автором)*

проблематично перечислить, даже в отношении одного конкретного приложения или продукта. Также существует много скрытых опасностей, начиная от вредоносного кода или вирусов в драйверах до кражи идентификационных данных пользователей и уязвимостей межсайтового скриптинга. Кроме того, к сожалению, в большинстве случаев поставщики цифровых коммуникационных услуг предоставляют маркетинговую, а не техническую информацию о том, насколько безопасны их системы или как они обеспечивают сохранность данных. Отдельная проблема связана с тем, что провайдеры услуг не представляют адвокатам и адвокатским образованиям предварительного разрешения на проведение независимых тестов на проникновение в их системы.

Учитывая текущие угрозы и вызовы цифровой среды, не подлежит сомнению тот факт, что выбор и верификация защищенных каналов связи в деятельности адвоката требуют комплексного подхода, основанного на интеграции современных криптографических стандартов и строгом контроле аппаратной среды. С учетом данных требований, в таблице 3 выделены ключевые параметры выбора защищенных каналов и сред, которые базируются на технических регламентах международных институтов стандартизации и позволяют минимизировать риски компрометации профессиональной тайны адвокатов на всех уровнях передачи данных. Систематизация данных характеристик направлена на создание устойчивой ИТ-инфраструктуры, способной противодействовать как типовым сетевым угрозам, так и высокотехнологичным методам анализа трафика.

Технический анализ параметров, представленных в таблице 3, позволяет сделать вывод, что обеспечение надежности цифровых коммуникаций адвоката в современных условиях невозможно без перехода к архитектуре «нулевого доверия», предполагающей непрерывную динамическую верификацию каждого субъекта и устройства в сети. Совокупность использования протоколов с совершенной прямой секретностью и аппаратной изоляцией криптографических ключей формирует эшелонированную систему защиты, нивелирующую угрозы со стороны как внешних злоумышленников, так и администраторов облачных инфраструктур.

Таблица 3.

Технические критерии выбора и верификации защищенных каналов цифровой коммуникации в адвокатской деятельности

Технический параметр	Регламентируемая спецификация (на основе стандартов NIST/ISO)	Научно-техническое обоснование выбора
Протокол транспортного уровня	TLS 1.3 (RFC 8446) / IPsec (IKEv2)	Исключение векторов атак, основанных на принудительном понижении версии протокола, и обеспечение совершенной прямой секретности
Алгоритм асимметричного шифрования	ECDSA / EdDSA (эллиптические кривые P-384, Curve25519)	Повышение вычислительной стойкости при оптимизации длины ключа по сравнению с классическими алгоритмами факторизации целых чисел.
Алгоритм симметричного шифрования	AES-GCM (256 бит)	Реализация режима блочного шифрования с аутентификацией для одновременного обеспечения конфиденциальности и защиты данных.
Архитектура криптографической защиты	Сквозное шифрование (E2EE) / архитектура с «нулевым знанием» (Zero-Knowledge)	Техническое исключение возможности дешифрации контента на промежуточных узлах и стороне поставщика облачных услуг.
Механизмы аутентификации субъектов	Многофакторная аутентификация (стандарты FIDO2 / WebAuthn)	Минимизация вероятности компрометации канала вследствие несанкционированного использования учетных данных и методов социальной инженерии.
Контроль целостности и хеширование	SHA-3 (Keccak)	Обеспечение криптографической неизменности передаваемых массивов данных и устойчивости к поиску коллизий первого и второго рода.
Инфраструктура хранения ключей	Аппаратные модули безопасности (HSM) / Доверенный платформенный модуль (TPM 2.0)	Физическая изоляция секретных ключей от программной среды общего назначения и предотвращение их экстракции вредоносным ПО.

(составлено автором)

Таким образом, резюмируя результаты проведенного анализа, отметим, что в ответ на актуальные вызовы информационной революции и потребности сегодняшнего дня адвокаты в своей практике расширяют использование цифровых коммуникаций, которые позволяют им повышать эффективность своей работы и оказывать доверителям более квалифицированную юридическую помощь с использованием актуальных технологий. Однако эти удобства и новации сопровождаются повышенными рисками кибербезопасности, сохранности данных и защиты конфиденциальных сведений клиентов.

В статье рассмотрены вопросы, связанные с правовыми и техническими аспектами выбора надежных каналов связи. Отмечено, что актуальной является императивная тенденция к технологической стандартизации адвокатской деятельности. Это в свою очередь диктует необходимость внедрения в отечественную практику регламентов сквозного шифрования и многофакторной верификации субъектов. Сформулированные в работе требования к архитектуре каналов связи и протоколам шифрования закладывают основу для формирования единой методики верификации коммуникационных решений, минимизирующей влияние человеческого фактора и уязвимостей стороннего программного обеспечения на адвокатскую деятельность.

ЛИТЕРАТУРА

1. Фадеев А.В., Воронина П.А. Цифровизация адвокатской деятельности // Международный журнал гуманитарных и естественных наук. 2023. №11–4, с. 234–242.
2. Советкина А.С., Лошкарёв А.В. Развитие цифровизации в сфере адвокатуры и адвокатской деятельности: преимущества и возможные недостатки // Международный журнал гуманитарных и естественных наук. 2020. №9–2. С. 195–199.
3. Yong Ding, Weiguo Huang, Hai Liang, A Fast Cross-Chain Protocol Based on Trusted Notary Group for Metaverse // International Journal of Network Management. 2024. Volume 35, Issue 1. P. 19–22.
4. John Zeleznikow, The benefits and dangers of using machine learning to support making legal predictions // Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 2023. Volume 13, Issue 4. P. 71–78.
5. Коган М.И., Обеспечение сохранения адвокатской тайны при использовании адвокатом современных технологий и электронных девайсов // Вестник Университета имени О.Е. Кутафина. 2020. №11 (75). С. 218–223.
6. Hugo Mentzingen, Nuno António, Fernando Bacao Automation of Legal Precedents Retrieval: Findings from a Literature Review // International Journal of Intelligent Systems. 2023. Volume 3, Issue 17. P. 45–51.
7. Li Ge, Peng Yan Li Research on Network Data Monitoring and Legal Evidence Integration Based on Cloud Computing // Mobile Information Systems. 2022. Volume 9, Issue 1. P. 102–106.
8. Магдеева Д.И., Адвокатская тайна в цифровую эпоху: вызовы и способы защиты // Вестник Пензенского государственного университета. 2025. №2(50). С. 22–26.

Журнал «Современная наука: актуальные проблемы теории и практики»