DOI 10.37882/2223-2966.2026.03.17

УЯЗВИМОСТИ ПРОЦЕССОВ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В АДВОКАТСКОЙ ДЕЯТЕЛЬНОСТИ: ТЕХНИЧЕСКИЕ И ЮРИДИЧЕСКИЕ АСПЕКТЫ

VULNERABILITIES OF ELECTRONIC DOCUMENT MANAGEMENT PROCESSES IN ADVOCACY: TECHNICAL AND LEGAL ASPECTS

I. Korotkiy

Summary. The article examines the technical and legal aspects of ensuring the security of electronic document management systems in the activities of lawyers. As a result of analysing statistical data and technical decomposition of architectural solutions, the authors have identified a gap between regulatory requirements and the actual security of digital channels used by lawyers. Using the examples of the Kontur and Goskey platforms, critical vulnerabilities in electronic document management systems in the context of protecting attorney-client privilege have been identified. Particular attention is paid to the risks of data compromise at intermediate nodes of cloud services and the problem of unprotected execution environments on mobile devices.

Keywords: electronic document management, risk, data, leak, lawyer.

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

Аннотация. В статье проанализированы технические и юридические аспекты обеспечения безопасности систем электронного документооборота в деятельности адвокатов. В результате анализа статистических данных и технической декомпозиции архитектурных решений выявлен разрыв между нормативными требованиями и фактической защищенностью цифровых каналов адвокатуры. На примере платформ «Контур» и «Госключ» обозначены критические уязвимости систем электронного документооборота в контексте защиты адвокатской тайны. Особое внимание уделено рискам компрометации данных на промежуточных узлах облачных сервисов и проблеме незащищенности среды исполнения на мобильных устройствах.

Ключевые слова: электронный документооборот, риск, данные, адвокат.

Для современной адвокатской практики в быстро меняющемся мире права эффективность является ключевой детерминантой. Это предопределяет тот факт, что юридические фирмы постоянно ищут способы оптимизации своей деятельности, и программное обеспечение для электронного документооборота (ЭДО) предлагает современное решение этой задачи [1]. Данная технология позволяет адвокатам выполнять свои обязанности в режиме онлайн. Кроме того, она в некоторых случаях устраняет необходимость в личных встречах с доверителями.

В целом можно отметить, что облачная система управления документами с интегрированной технологией электронной подписи — важный инструмент контроля за затратами и повышения качества и скорости оказываемой юридической помощи, которые становится конкурентным факторами в современной отрасли юридических услуг [2]. Многие адвокатские образования уже получили практическую отдачу от использования систем ЭДО, которая проявляется в обеспечении бесшовного взаимодействия, оптимизации юридических процессов и внедрении усиленных механизмов безопасности, направленных на минимизацию рисков, включая снижение рисков утечки информации, связанной с бумажными документами. Кроме того, современные платформы способствуют ускоренному получению подписей клиентов, а также обеспечивают возможность использования цифровых аудиторских следов в целях повышения прозрачности и подтверждения соответствия установленным нормативным требованиям [3, 4].

Однако внедрение систем ЭДО в адвокатскую практику, наряду с ростом операционной эффективности, создает новые векторы угроз, такие как риски атак на цепочки поставок и превышение полномочий поставщиком услуг [5]. На рис. 1 отображены количественные показатели рисков информационной безопасности (ИБ), которые демонстрируют уязвимость адвокатской деятельности перед современными векторами атак на системы ЭДО.

Статистические данные, представленные на рис. 1, отражают критический рост инцидентов, где объектом посягательства является адвокатская тайна, передаваемая через незащищенные каналы связи или скомпрометированные платформы ЭДО. Отдельно следует отметить устойчивую тенденцию к эскалации киберугроз, при этом темпы роста инцидентов в РФ демонстрируют опережающую динамику относительно среднемировых

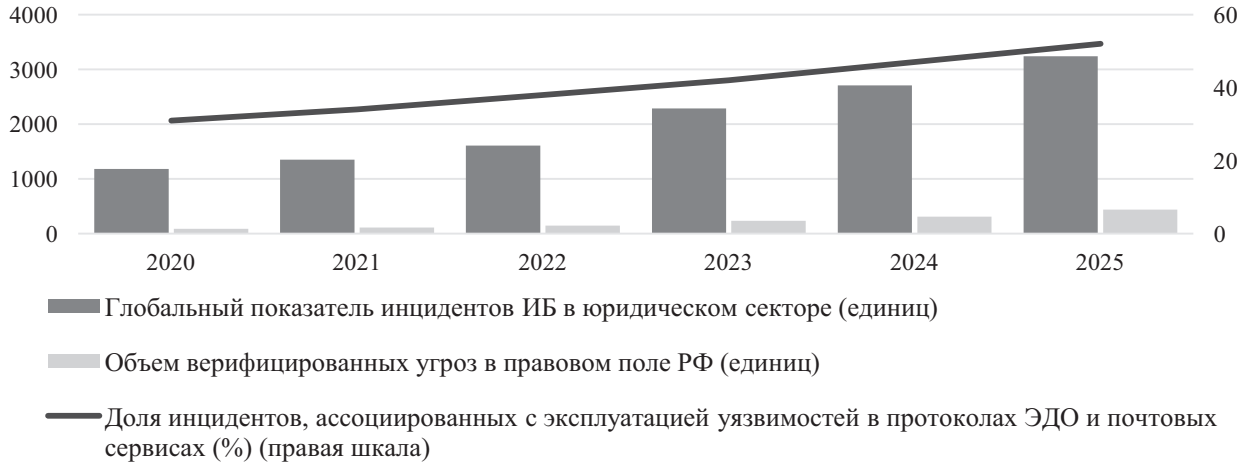

Рис. 1. Динамический анализ количественных показателей киберрисков в инфраструктуре ЭДО адвокатских организаций

Составлено автором на основе агрегированных данных отчетов IBM «Cost of a Data Breach Report» (2020–2024), аналитических обзоров Positive Technologies «Киберугрозы в РФ» и статистики Solicitors Regulation Authority.

показателей. Кроме того, необходимо обратить внимание на прогрессирующее увеличение коэффициента влияния уязвимостей систем электронного документооборота, который в 2025 году превысил критический порог в 50 %, что фактически определяет ЭДО как доминирующий вектор атаки на адвокатскую тайну.

Таким образом, защита систем ЭДО и их безопасное использование в адвокатской деятельности является комплексной задачей, охватывающей правовые, технические, организационные, инфраструктурные, институциональные, профессиональные аспекты, детальное раскрытие которых составляет актуальное направление научного поиска.

Технические аспекты трансформации управления юридическими документами посредством автоматизации и использования цифровых систем, рассматривают в своих публикациях Морозова М.Ю., Фомина П.С., Челак С.В., Филимонова В.А., Junhua Wu, Tiantian Wang, Guangshun Li, Kan Yu.

Проблемы защиты электронной подписи адвоката, а также риски и уязвимости ЭДО, использующих облачные сервисы, описывают Какорина О.А., Юрцев А.Н., Ткачева М.В., Уточкина Л.А., Michael D. Anestis, Allison E. Bond, Malik Mustafa, Marwan Alshare, Deepshikha Bhargava.

Требования к сертификации систем ЭДО в России, практические аспекты соблюдения регламентов хранения и передачи электронных документов адвокатскими образованиями, а также вопросы соответствия систем киберзащиты отраслевым и государственным нормативным актам, нашли свое отражение в работах Даниленко А.Ю., Акимовой Г.П., Черкасовой Е.Н., Сибикиной И.В., Лазаревой Н.А., Цветковой К.В., Эргашевой Р.С.

Несмотря на широкое внимание со стороны научно-экспертных кругов к рассматриваемой проблематике, ряд вопросов нуждается в более углубленном изучении. Так, например, требует дальнейшей проработки проблема соотнесения технических механизмов кибербезопасности с процессуальными гарантиями конфиденциальности и допустимости доказательств. Кроме того, нерешенной остается задача выработки единых стандартов ответственности и реагирования на инциденты информационной безопасности в условиях цифровой трансформации юридической практики.

Таким образом, цель статьи заключается в изучении через призму технических и юридических аспектов уязвимости процессов электронного документооборота в адвокатской деятельности.

Детальное изучение отечественной нормативно-правовой базы (см. табл. 1) позволяет констатировать доминирование организационных мер над жесткими технологическими стандартами в сфере обеспечения информационной безопасности адвокатской деятельности. Отсутствие детальных технических регламентов создает условия для возникновения критических уязвимостей в процессах ЭДО [6]. Данные, представленные в таблице 1, позволяют верифицировать разрыв между требованиями законодательства и фактической защищенностью цифровых каналов коммуникации в деятельности адвокатов.

Сведения, приведенные в таблице 1, позволяют заключить, что в работе адвокатов в России уровень киберрисков и уязвимостей в значительной степени зависит от субъективных решений руководителей адвокатских образований или личных наработок адвокатов, а не от требований стандартов, установленных Феде-

Таблица 1.

Риски нормативной неопределенности в архитектуре цифрового документооборота адвоката

Стадия процесса ЭДО	Нормативное обоснование (акты РФ)	Техническое содержание уязвимости	Риск в области информационной безопасности
Формирование и подготовка документов	Кодекс профессиональной этики адвоката; Федеральный закон № 149-ФЗ	Отсутствие стандартов обязательной очистки метаданных (скрытых атрибутов файла)	Несанкционированное раскрытие истории изменений, структуры локальных каталогов и данных об авторе документа
Транспортировка данных по сетям связи	Федеральный закон № 63-ФЗ «Об электронной подписи»	Отсутствие норм об обязательном применении сквозного шифрования (шифрование от отправителя до получателя)	Перехват и дешифрация информации на промежуточных узлах сетевого оборудования провайдеров связи
Долговременное архивное хранение	ГОСТ Р 7.0.8 (Правила делопроизводства и архивации)	Отсутствие регламентов по обеспечению долговременной достоверности электронного документа	Утрата возможности подтверждения подлинности документа после завершения срока действия сертификата ключа подписи
Управление правами доступа	Приказы ФСТЭК (носящие рекомендательный характер для адвокатов)	Отсутствие требований к реализации архитектуры «нулевого доверия» (непрерывная проверка прав доступа)	Несанкционированный доступ технического персонала или администраторов к адвокатским досье без фиксации в журнале событий
Гарантированное уничтожение	Стандарты профессиональной деятельности (общие положения)	Отсутствие сертифицированных методик безвозвратного удаления данных с физических носителей и из облачных сред	Возможность восстановления конфиденциальных сведений из временных файлов, системных записей и резервных копий

Составлено автором

ральной палатой адвокатов РФ. Выявленные проблемные моменты, начиная от избыточных данных в структуре файлов и заканчивая рисками восстановления удаленной информации, указывают на необходимость доработки рекомендаций ФПА РФ и разработки технического регламента. Внедрение таких механизмов, как аппаратная изоляция ключей шифрования и многофакторная верификация пользователей, позволит минимизировать влияние человеческого фактора и обеспечит защиту адвокатской тайны на всех этапах электронного документооборота [7].

Далее рассмотрим более подробно техническую сторону вопроса уязвимости процессов электронного документооборота в адвокатской деятельности.

В современной отечественной практике наиболее востребованными инструментами цифрового взаимодействия выступают системы «Контур» и «Госключ». Детальный технический анализ данных платформ позволит выявить фундаментальные векторы реализации технологических угроз и сопоставить системные уязвимости процессов информационного обмена с потенциальными рисками для сохранности адвокатской тайны. Составленная автором матрица рисков для систем ЭДО, при использовании анализируемых платформ, представлена в таблице 2.

Проведенное исследование показывает, что эксплуатация систем ЭДО в практике российской адвокатуры сопряжена с рисками, масштаб которых определяется архитектурными особенностями используемых платформ и спецификой отечественного правового регулирования. Техническая верификация процессов в системах «Контур» и «Госключ» позволяет выделить следующие ключевые риски.

1. Проблема делегированного доверия: при использовании централизованных систем (например, «Контур») адвокат фактически делегирует функции контроля над конфиденциальностью оператору ЭДО. Отсутствие возможности проведения независимого аудита и тестов на проникновение со стороны пользователя создает ситуацию «латентной уязвимости», где безопасность адвокатской тайны зависит от добросовестности и киберустойчивости третьей стороны.
2. Уязвимость среды функционирования: в случае с системой «Госключ» основным вектором атаки становится не сам алгоритм электронной подписи, а среда его реализации — мобильное устройство. При отсутствии аппаратной изоляции криптографических ключей (использование доверенных платформ типа TPM/HSM) риск несанкционированной экстракции данных вредоносным программным обеспечением остается критически высоким.
3. Инфраструктурная зависимость: анализ каналов связи и механизмов дистрибуции обновлений подтверждает, что даже легитимное программное обеспечение может стать инструментом компрометации (атаки на цепочки поставок). Без внедрения протоколов с совершенной прямой секретностью и систем многофакторной верифика-

Таблица 2.

Декомпозиция технологических рисков при эксплуатации систем «Контур» и «Госключ» в адвокатской практике

Объект и среда функционирования	Технический вектор реализации риска	Системная уязвимость процесса ЭДО	Последствие для адвокатской тайны
Облачные платформы («Контур»)	Компрометация промежуточного узла: несанкционированный доступ к серверной части оператора.	Отсутствие сквозного шифрования (E2EE) на уровне бизнес-логики поставщика услуг.	Полная эксфильтрация содержимого юридических досье администраторами или внешними злоумышленниками.
	Межсайтовый скриптинг и инъекции: внедрение вредоносного кода в веб-интерфейс системы.	Недостаточная верификация исполняемого кода в клиентском браузере адвоката.	Кража активных сессий и идентификационных данных без нарушения целостности ключей электронной подписи.
Мобильная криптография («Госключ»)	Декомпозиция доверенной среды: эксплуатация уязвимостей операционной системы смартфона.	Хранение секретных ключей в программной среде общего назначения без аппаратной изоляции.	Возможность экстракции закрытого ключа вредоносным программным обеспечением.
	Имитация биометрических признаков: применение нейросетевых моделей для обхода идентификации.	Синтетическая когнитивная атака на механизмы подтверждения личности в мобильном приложении.	Формирование юридически значимой подписи от имени адвоката неуполномоченным лицом.
Каналы передачи данных	Принудительное понижение версии протокола: атака на транспортный уровень соединения.	Использование устаревших стандартов связи (TLS ниже 1.3), допускающих перехват трафика.	Прослушивание канала связи и накопление зашифрованных данных для последующего подбора ключа.
Инфраструктура обновления	Атака на цепочку поставок: внедрение деструктивного кода через легитимные обновления ПО.	Отсутствие независимого аудита и тестов на проникновение перед выпуском патчей операторами.	Скрытое внедрение функций удаленного управления в специализированное ПО адвоката.

Составлено автором

ции, цифровая коммуникация адвоката не может считаться полностью защищенной от перехвата на промежуточных узлах сетевой инфраструктуры.

Вышеизложенное позволяет отметить, что риски, возникающие при эксплуатации адвокатами платформ «Контур» и «Госключ», обусловлены фундаментальным противоречием между централизованной архитектурой сервисов и необходимостью исключения несанкционированного доступа к содержанию адвокатского делопроизводства со стороны операторов и регуляторов. Для обеспечения защищенности систем ЭДО адвокатских образований, а также устранения уязвимостей рассматриваемых систем представляется целесообразным сформулировать рекомендации, которые нацелены на формирование доверенной технической среды, позволяющей нивелировать системные уязвимости за счет внедрения методов аппаратной изоляции и сквозного криптографического сопровождения данных.

Во-первых, модернизация архитектуры взаимодействия с платформой «Контур». Для нивелирования рисков, связанных с компрометацией промежуточных узлов и отсутствием сквозного шифрования в системе «Контур», необходимо предпринять следующие шаги:

— реализация протокола предварительного шифрования, что предполагает обязательное применение программных средств криптографической защиты информации на стороне адвоката для шифрования вложений до их загрузки в облачную инфраструктуру оператора. Данная мера позволит обеспечить функциональную изоляцию облачной инфраструктуры «Контур» от семантического содержания документов [8]. Таким образом роль платформы будет заключаться исключительно в трансляции зашифрованных пакетов данных и управлении метаданными процесса обмена без возможностидешифрацииконтентатретьимилицами;
— изоляция среды веб-доступа путем использования выделенных виртуальных контейнеров или специализированных браузеров с жестко ограниченным набором исполняемых скриптов для работы с веб-интерфейсом системы, что исключает возможность реализации атак типа «межсайтовый скриптинг».

Во-вторых, повышение устойчивости среды функционирования системы «Госключ». Принимая во внимание высокий риск экстракции закрытых ключей из программной среды смартфонов, следует осуществить следующие меры:

— переход на аппаратную токенизацию с помощью внедрения обязательного требования по хранению ключей электронной подписи на внешних аппаратных носителях (смарт-карты, токены с поддержкой NFC), совместимых с мобильным

приложением «Госключ». Это даст возможность исключить нахождение секретного ключа в оперативной памяти мобильного устройства общего назначения;
— программная блокировка работы приложения «Госключ» на устройствах с нарушенной целостностью ядра и отсутствием активированного доверенного модуля, что минимизирует вероятность успеха вредоносного программного обеспечения.

В-третьих, внедрение усиленного механизма верификации субъектности и методов защиты от нейросетевых подмен. Для предотвращения формирования подписи от имени адвоката неуполномоченными лицами через механизмы «Госключа» необходима:
— мультимодальная биометрическая идентификация, а именно дополнение статической биометрии алгоритмами динамической проверки, требующими от пользователя выполнения случайной последовательности действий в реальном времени, что делает невозможным использование синтетических видеопотоков [9];
— внедрение криптографической привязки биометрического шаблона к уникальному идентификатору доверенного аппаратного модуля конкретного устройства.

Подводя итоги проведенному исследованию, можно сделать следующие выводы. Текущая инфраструктура ЭДО в российской адвокатской практике характеризуется высокой степенью уязвимости перед современными векторами кибератак, что обусловлено доминированием организационных мер над технологическими стандартами. Установлено, что централизованная архитектура платформы «Контур» и программная реализация мобильной криптографии «Госключ» создают риски несанкционированной эксфильтрации данных администраторами систем или вредоносным программным обеспечением. Фундаментальным решением обозначенных проблем является переход к парадигме технологически гарантированной конфиденциальности, исключающей зависимость адвокатской тайны от добросовестности третьих лиц.

ЛИТЕРАТУРА

1. Жучков С.В. Цифровая трансформация совершения нотариальных действий в России // Вестник РГГУ. Серия: Экономика. Управление. Право. 2022. № 3–2. С. 253–261.
2. Чертков Н.Н. Квалифицированная электронная подпись как ключевой атрибут электронного юридического документа: проблемы правоприменения // Юридическая наука. 2025. № 11. С. 293–298.
3. Jiaqi Ju, Qi Wang, Wei Wang, Ming Ni Resilience enhancement strategy for cyber–physical distribution systems that considers cross-space propagation of information risk // IET Renewable Power Generation. 2023. Volume 18, Issue 7. P. 12–19.
4. Рытова Е.И. Кибербезопасность государственных информационных систем. Актуальные вопросы безопасности ИС в судебной системе // Оригинальные исследования. 2025. Т. 15. № 8. С. 83–88.
5. Gauri Shankar, Liwa H. Ai-Farhani Improved Multisignature Scheme for Authenticity of Digital Document in Digital Forensics Using Edward-Curve Digital Signature Algorithm // Security and Communication Networks. 2023. Volume 20, Issue 1. P. 13–17.
6. Мезенцев А.В. Анализ уязвимостей электронных подписей на мобильных платформах с использованием VOSVIEWER // Славянский форум. 2025. № 4 (50). С. 45–69.
7. Bagus Tri Atmaja, Jiann-Liang Chen Integrating Large Language Model for Common Criteria Security Document Generation Based on PySide6 // Software: Practice and Experience. 2025. Volume 55, Issue 10. P. 29–34.
8. Романенко К.С. Обзор проблем безопасности систем электронного документооборота // Информатизация и связь. 2023. № 2. С. 76–79.
9. Дудник И.А., Ульянова Е.В. Современные инструменты обеспечения безопасности систем электронного документооборота // Тенденции развития науки и образования. 2023. № 97–12. С. 67–70.

Журнал «Современная наука: актуальные проблемы теории и практики»