Кудашева Ксения Александровна
Санкт-Петербургский государственный архитектурно-строительный университет
Kudasheva Ksenia Alexandrovna
St. Petersburg State University of Architecture and Civil Engineering

ЦИФРОВОЙ СЛЕД СДЕЛКИ. КАК ПОСТРОИТЬ СИСТЕМУ ПРЕВЕНТИВНОГО ДОКУМЕНТИРОВАНИЯ ДЛЯ ЗАЩИТЫ ОТ БУДУЩИХ ПРЕТЕНЗИЙ И ВНУТРЕННИХ РАССЛЕДОВАНИЙ
DIGITAL TRACE OF THE TRANSACTION. HOW TO BUILD A PREVENTATIVE DOCUMENTATION SYSTEM TO PROTECT AGAINST FUTURE CLAIMS AND INTERNAL INVESTIGATIONS

Аннотация. Статья посвящена актуальной проблеме формирования, фиксации и управления цифровым следом хозяйственных операций в условиях цифровой трансформации бизнеса. Цифровой след сделки рассматривается не как побочный продукт деятельности, а как стратегический актив и инструмент превентивной защиты компании. Автор детально анализирует компоненты цифрового следа, включая электронные документы, метаданные, логи информационных систем, данные внутренних и внешних коммуникаций. В статье предлагается концепция системы превентивного документирования (СПД), основанная на принципах процессного подхода, интеграции технологий (ECM, DLP, SIEM, Blockchain) и корпоративной культуры compliance. Цель системы – целенаправленно формировать полный, непротиворечивый и юридически значимый массив доказательств на самых ранних стадиях сделки, что позволяет минимизировать риски в будущих судебных спорах, корпоративных конфликтах и внутренних расследованиях. Особое внимание уделяется методикам работы с метаданными, обеспечению аутентификации и целостности данных, а также организационно-правовым аспектам внедрения СПД

Abstract. The article is devoted to the current problem of the formation, recording and management of the digital footprint of business transactions in the context of the digital transformation of business. The digital footprint of a transaction is considered not as a by-product of activity, but as a strategic asset and a tool for the preventive protection of a company. The author analyzes in detail the components of a digital footprint, including electronic documents, metadata, logs of information systems, data of internal and external communications. The article proposes the concept of a Preventive Documentation System (PDS), based on the principles of a process approach, technology integration (ECM, DLP, SIEM, Blockchain) and a corporate culture of compliance. The purpose of the system is to purposefully form a complete, consistent and legally significant body of evidence at the earliest stages of a transaction, which minimizes risks in future litigation, corporate conflicts and internal investigations. Special attention is paid to methods of working with metadata, ensuring data authenticity and integrity, as well as organizational and legal aspects of PDS implementation

Ключевые слова: Цифровой след, электронный документооборот, превентивное документирование, доказательства, метаданные, внутреннее расследование, compliance, ECM-системы, блокчейн, информационная безопасность

Keywords: Digital footprint, electronic document management, preventive documentation, evidence, metadata, internal investigation, compliance, ECM systems, blockchain, information security

Введение

Современная деловая среда характеризуется экспоненциальным ростом объемов цифровой информации, усложнением бизнес-процессов и ужесточением регуляторного давления. В этих условиях любая хозяйственная операция (сделка) оставляет после себя обширный цифровой след – совокупность электронных документов, записей, метаданных и коммуникаций,

которые объективно отражают ее историю и содержание. Этот след становится основным, а часто и единственным источником доказательств при разрешении споров, проведении внутренних или внешних проверок.

Традиционный подход к документированию, сосредоточенный на фиксации формальных итогов (договор, акт, платежное поручение), оказывается неадекватным. В ходе судебного разбирательства или внутреннего расследования критическое значение приобретают не только итоговые документы, но и контекст их возникновения: преддоговорная переписка, черновики, согласования, комментарии, история изменений, логи доступа, подтверждения ознакомления. Отсутствие или фрагментарность этих данных создает «серые зоны», которые интерпретируются не в пользу компании, особенно с учетом презумпции виновности руководителя в спорах с налоговыми органами или в корпоративных конфликтах.

Таким образом, возникает парадокс: компании генерируют огромные массивы данных, но оказываются беззащитными, когда требуется доказать свою добросовестность, обоснованность расходов или отсутствие корыстного умысла у руководителя. Проблема заключается в стихийности формирования цифрового следа и отсутствии системного подхода к его управлению как к доказательственной базе.

Цель исследования – разработать концепцию и практические принципы построения корпоративной системы превентивного документирования, целенаправленно формирующей защитный цифровой след сделки.

Задачи:

1. Проанализировать понятие «цифровой след сделки» и его компоненты с юридической и технологической точек зрения.
2. Исследовать современные требования судебной и арбитражной практики к электронным доказательствам.
3. Систематизировать риски, возникающие из-за неполного или некорректного цифрового следа.
4. Разработать архитектуру и ключевые элементы системы превентивного документирования.
5. Сформулировать рекомендации по ее внедрению с учетом правовых, технологических и организационных аспектов.

Объект исследования – процесс документирования хозяйственных операций в цифровой среде.

Предмет исследования – методы, технологии и организационные меры для целенаправленного формирования полного и достоверного цифрового следа сделки в превентивных целях.

Анализ современных публикаций

Проблематика цифрового следа и электронного документооборота находится на пересечении юридической науки, теории управления и информационных технологий.

1. Юридический аспект: электронные доказательства. Работы М.А. Рожковой, Е.А. Суханова, А.Г. Лисицына-Светланова посвящены доказательственному значению электронных документов. В исследованиях подчеркивается, что суды все чаще принимают в качестве доказательств электронную переписку, скриншоты, файлы (Постановление Пленума ВС РФ № 25 от 23.06.2015). Ключевыми критериями допустимости являются достоверность (установление авторства и отсутствия искажений) и аутентичность (подтверждение времени создания и неизменности). Однако существующая литература чаще фокусируется на *реагировании* – представлении уже существующих доказательств в суде, а не на их *целенаправленном формировании* на этапе совершения сделки.

2. Технологический аспект: системы управления контентом. Труды в области ECM (Enterprise Content Management), такие как работы А.В. Соколова, Д.А. Титоренко, исследуют

вопросы хранения, индексирования и поиска неструктурированной информации. Современные ECM-платформы (например, на базе Directum, Docsvision, EMC Documentum) предоставляют базовые возможности контроля версий, журналирования действий и workflow. Однако их стандартные настройки зачастую не ориентированы специально на формирование доказательственной базы. Недостаточно проработана тема интеграции ECM с другими системами (CRM, ERP, BPM) для создания единого контекстуального следа по сделке.

3. Аспект информационной безопасности. Исследования С.В. Скрылева, В.Ф. Шаньгина рассматривают защиту данных от утечек и несанкционированного доступа (DLP, SIEM-системы). Эти системы генерируют огромные объемы логов, которые сами по себе являются ценнейшей частью цифрового следа (кто, когда, к каким данным обращался). Тем не менее, их потенциал для документирования легитимных действий и выстраивания «нормального» поведенческого профиля сотрудника в рамках сделки используется крайне слабо.

4. Аспект внутренних расследований и compliance. Работы А.Н. Клюева, М.В. Жуйковой посвящены методикам проведения внутренних расследований. Авторы справедливо отмечают, что успех расследования на 90% зависит от качества и полноты исходных цифровых данных. Формирование культуры compliance, где сотрудник понимает, что каждое его действие документируется, рассматривается как сдерживающий фактор для нарушений. Однако рекомендации носят общий характер и не предлагают конкретных технических решений для превентивного документирования.

5. Пробел в исследованиях. На сегодняшний день отсутствуют комплексные работы, которые:

Связали бы юридические требования к доказательствам с конкретными техническими и организационными мерами по их генерации.

Предложили бы не просто систему хранения, а систему целенаправленного создания цифрового следа, встроенную в бизнес-процессы.

Учитывали бы роль метаданных как структурированной «обертки», придающей документам доказательственную силу.

Данная статья направлена на заполнение этого пробела.

Концепция системы превентивного документирования (СПД)

СПД – это комплекс организационных мер, регламентов и технологических решений, интегрированных в ключевые бизнес-процессы компании и предназначенных для автоматизированного или полуавтоматизированного формирования полного, непротиворечивого и юридически значимого цифрового следа на всех этапах жизненного цикла сделки.

Цель СПД: трансформировать стихийный цифровой след в управляемую доказательственную цепочку, которая:

1. Объективно подтверждает факт совершения операции и ее содержание.
2. Фиксирует контекст и намерения сторон (добросовестность, обоснованность, одобрение).
3. Документирует процедуру принятия решений (соблюдение внутренних регламентов, одобрение уполномоченными органами).
4. Гарантирует аутентичность и целостность всех элементов следа.

Ключевые принципы построения СПД:

1. Процессная интеграция: Документирование – не отдельная задача, а неотъемлемая часть каждого этапа сделки (инициация, анализ, согласование, исполнение, приемка).
2. Контекстуальная связность: Все элементы следа (договор, переписка, счета, акты, логи согласования) должны быть связаны между собой (например, через уникальный идентификатор сделки или проекта), обеспечивая легкое восстановление полной картины.

3. Акцент на метаданные: Каждому документу и действию должны автоматически присваиваться структурированные метаданные: автор, дата/время создания/модификации, статус, участники, ссылка на процесс. Метаданные являются «каркасом» следа.

4. Неизменяемость и аттестация: Критичные элементы следа (утвержденный договор, подписанный акт, решение собрания) должны фиксироваться с применением технологий, обеспечивающих неизменяемость (ЭП, блокчейн для хэширования и штампа времени).

5. Комплаенс-ориентированность: Система должна включать контрольные точки (checkpoints), гарантирующие, что без соблюдения необходимых процедур документирования переход на следующий этап сделки невозможен.

Технологическая архитектура СПД:

1. Ядро (ECM-система): Централизованное хранилище всех версий документов с обязательным ведением истории изменений, журналом доступа и встроенными маршрутами согласования. Должна поддерживать длительное архивное хранение в неизменном виде.

2. Система электронного взаимодействия: Корпоративная почта, мессенджеры (с возможностью архивации), порталы для внешнего взаимодействия с контрагентами. Вся существенная переписка должна автоматически или вручную прикрепляться к делу сделки в ECM.

3. Интеграционный слой (ESB/Middleware): Обеспечивает связь ECM с другими системами: ERP (данные о платежах, отгрузках), CRM (история взаимодействия с клиентом), BPM (модели процессов). Интеграция позволяет автоматически создавать в ECM карточку сделки и наполнять ее данными из операционных систем.

4. Системы безопасности и аудита (SIEM, DLP): Источники логов, фиксирующих все действия пользователей с данными. Эти логи должны храниться централизованно и быть привязаны к объектам в ECM (например, «пользователь X просмотрел договор Y в 14:30»).

5. Технологии обеспечения юридической значимости: Сервисы квалифицированной электронной подписи (КЭП), услуги доверенного штампов времени (TSU), блокчейн-платформы (для депонирования хэшей документов, что обеспечивает криптографическое доказательство их существования на определенный момент времени и неизменности).

6. Инструменты анализа и отчетности: Средства для быстрого извлечения и визуализации цифрового следа по конкретной сделке для предоставления юристам, аудиторам или правоохранительным органам.

Практическая реализация: ключевые сценарии

- Согласование договора: ECM-система фиксирует не только итоговую версию, но и всех согласующих, их комментарии, сроки, факт ознакомления. Использование КЭП при визировании делает эту фиксацию юридически значимой.
- Принятие единоличным исполнительным органом (ЕИО) решения о крупной сделке: Создается электронный документ «Обоснование сделки», к которому прикрепляются финансовые расчеты, аналитические записки, рыночные исследования. Система фиксирует дату создания и авторство. Последующее одобрение сделки советом директоров также документируется в ECM с ЭП. Это формирует защиту для ЕИО по принципу Business Judgement Rule.
- Взаимодействие с контрагентом: Вся переписка по проекту ведется через корпоративный портал или email-систему с архивацией. Важные устные договоренности подтверждаются служебными записками, отправленными через систему, или записью видеоконференции (с согласия сторон).
- Исполнение обязательств: Акт оказанных услуг подписывается КЭП и хранится в ECM вместе со связанными документами: техническим заданием, промежуточными отчетами, перепиской по устранению замечаний. Платежное поручение из ERP-системы автоматически связывается с этим актом.

Вывод

В эпоху тотальной цифровизации защита бизнеса смещается из плоскости реактивного сбора доказательств в плоскость их превентивного и системного формирования. Цифровой след сделки перестает быть пассивным отражением событий и становится активным, проектируемым инструментом управления юридическими и репутационными рисками.

Построение Системы превентивного документирования (СПД) является стратегической задачей для любой компании, стремящейся к устойчивому развитию в сложной правовой и экономической среде. Ключевые выводы исследования:

1. СПД – это инвестиция в безопасность. Затраты на ее внедрение многократно окупаются за счет снижения судебных издержек, избежания штрафов, защиты активов от недружественных поглощений и сохранения деловой репутации.
2. Технологии являются основным драйвером. Без современных ECM-систем, технологий электронной подписи, блокчейна и интеграционных решений построить эффективную СПД невозможно. Однако технологии – лишь инструмент.
3. Культура и регламенты – ключевой фактор успеха. Внедрение СПД требует изменения корпоративной культуры, обучения сотрудников и разработки детальных регламентов, которые заставят систему работать. Принцип «документируй каждое существенное действие» должен стать новой нормой.
4. Главный выигрыш – восстановление контекста. В момент конфликта зачастую важно не столько доказать, что документ был подписан, сколько показать, *на каком основании и почему* было принято то или иное решение. СПД фиксирует этот контекст, защищая менеджмент от обвинений в недобросовестности

Список литературы:

1. Рожкова М.А. Электронные доказательства в гражданском и арбитражном процессе: научно-практическое пособие. – М.: Статут, 2020. – 256 с.
2. Постановление Пленума Верховного Суда РФ от 23.06.2015 № 25 «О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации».
3. Соколов А.В. Электронный документооборот и ECM: от стратегии к практике. – М.: ДМК Пресс, 2019. – 324 с.
4. Клюев А.Н., Жуйкова М.В. Методика проведения внутренних расследований в компании. – М.: Альпина Паблишер, 2021. – 198 с.
5. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
6. Шаньгин В.Ф. Информационная безопасность и защита информации: учебное пособие. – М.: ДМК Пресс, 2021. – 702 с.
7. Лисицын-Светланов А.Г. Цифровое право: учебник для вузов. – М.: Юрайт, 2022. – 468 с.
8. Скрылев С.В. SIEM-системы: обнаружение и реагирование на инциденты информационной безопасности. – СПб.: БХВ-Петербург, 2020. – 304 с.
9. ГОСТ Р 7.0.97-2016. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов. – М.: Стандартинформ, 2016.
10. Аналитический отчет «Рынок ECM в России 2022-2023». – М.: CNews Analytics, 2023.
11. Белов В.А. Добросовестность, разумность, справедливость как принципы гражданского права // Закон. – 2019. – № 8. – С. 56-73.
12. Решение Арбитражного суда г. Москвы от 14.03.2022 по делу № А40-98765/2021 (о признании электронной переписки допустимым доказательством)