Марченко Сергей Сергеевич,
студент юридического института, 4 курс,
ФГАОУ ВО «Белгородский государственный национальный исследовательский университет»

Фандюшин Иван Николаевич,
студент юридического института, 4 курс,
ФГАОУ ВО «Белгородский государственный национальный исследовательский университет»

Научный руководитель:
Гриневич Кристина Валерьевна,
ассистент кафедры теории и истории государства и права,
ФГАОУ ВО «Белгородский государственный национальный исследовательский университет»

ПРОБЛЕМЫ ВНЕДРЕНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА (ЭДО) В ОРГАНИЗАЦИЯХ С ОСОБЫМ РЕЖИМОМ СЕКРЕТНОСТИ

Аннотация. Актуальность темы обусловлена фундаментальным противоречием между курсом государства на всеобъемлющую цифровизацию управленческих процессов и жесткими нормативными требованиями по защите сведений, составляющих государственную тайну. Традиционные методы организации секретного делопроизводства, основанные на физической изоляции носителей и исключительно бумажном документообороте, вступают в прямой конфликт с требованиями федерального проекта «Цифровое государственное управление», что создает объективную необходимость поиска компромиссных организационно-технических решений. Дополнительную остроту проблеме придает нарастающий цифровой разрыв между организациями с особым режимом секретности и иными участниками межведомственного взаимодействия, что снижает эффективность их функционирования в едином контуре государственного управления и требует пересмотра устоявшихся подходов к организации защищенного документооборота.

Ключевые слова: Электронный документооборот, информационная безопасность, режим секретности, гибридный документооборот, государственная тайна, цифровизация управления.

Цифровая трансформация государственного управления выступает одним из приоритетных направлений развития Российской Федерации. С 2018 года в стране действует федеральный проект «Цифровое государственное управление», предусматривающий масштабное внедрение цифровых технологий во все сферы государственного управления. Значительная доля усилий по построению «цифрового правительства» сводится к переходу на электронные безбумажные формы учета и обмена информацией.

Однако повсеместная цифровизация документооборота сталкивается с серьезным барьером в виде требований по защите сведений, составляющих государственную тайну. Как отмечает Р. Г. Диниус, «основной проблемой при применении систем электронного документооборота (СЭД) является обеспечение информационной безопасности, а также риски, связанные с несанкционированным доступом к системе» [1, с. 72]. По оценкам специалистов, фактическая работа СЭД поднимает вопросы внедрения новых систем обеспечения безопасности, действующих в информационном поле [2, с. 74].

Цель настоящей статьи – выявить системные противоречия между требованиями к юридически значимому электронному документообороту и режимом секретности на уровне анализа конкретных норм права, а также предложить систематизированные пути их разрешения.

Для понимания причин возникновения системного конфликта необходимо обратиться к анализу конкретных норм федерального законодательства и подзаконных актов.

Первая коллизия возникает между Федеральным законом «Об электронной подписи» [3] и Законом РФ «О государственной тайне» [4]. Статья 6 ФЗ № 63 признаёт электронную подпись равнозначной собственноручной при соблюдении установленных требований, что создаёт правовую основу для юридически значимого электронного документооборота. Однако статья 24 Закона о гостайне прямо предписывает использование только таких носителей сведений, составляющих государственную тайну, которые исключают несанкционированный доступ. Бумажный носитель в физически изолированном помещении формально удовлетворяет этому требованию, тогда как любая цифровая система потенциально уязвима. Таким образом, ст. 6 ФЗ № 63 и ст. 24 Закона о гостайне вступают в прямое противоречие: первая легализует цифровой документооборот, вторая – фактически запрещает его для секретных сведений. Вторая коллизия касается требований к информационным системам. Приказ ФСТЭК России от 11.02.2013 № 17 устанавливает требования о защите информации, не составляющей гостайну, содержащейся в государственных информационных системах [5]. Для систем, обрабатывающих сведения, составляющие гостайну, действуют отдельные, значительно более жёсткие требования (приказ ФСТЭК № 55), предполагающие физическую изоляцию, отсутствие подключения к открытым сетям и специальную аттестацию.

В результате система ЭДО, соответствующая приказу № 17, не может быть использована для секретного документооборота, а создание отдельной системы под требования приказа № 55 сопряжено с экономическими и техническими трудностями. Третья коллизия имеет межведомственный характер. Система МЭДО создавалась в рамках приказа ФСТЭК № 17 для информации несекретного характера. Передача сведений «Для служебного пользования» (ДСП) через МЭДО во многих регионах не аттестована, а передача секретных сведений через неё невозможна в принципе. Это создаёт разрыв между открытым и закрытым сегментами государственного управления.

На основе анализа приведённых норм можно выделить четыре группы системных проблем. Организации с особым режимом секретности не могут использовать облачные сервисы ЭДО для режимно-секретных подразделений (прямое следствие ст. 24 Закона о гостайне). Как указывает Р. Г. Диниус, «необходимость поддержания двух параллельных контуров документооборота – открытого и закрытого – существенно увеличивает затраты на ИТ-инфраструктуру» [1, с. 75].

Однако помимо финансовых издержек эта техническая вынужденность порождает не менее серьёзную проблему на уровне персонала. Поскольку единая система документооборота отсутствует, сотрудник оказывается перед необходимостью работать в двух средах одновременно: использовать государственные информационные системы в открытой сети и вести секретное делопроизводство на бумажном носителе или в специализированном ПО на изолированном АРМ. Как подчёркивают А. В. Ивкин с соавторами, «подобная двойственность ведет к росту когнитивной нагрузки и повышает риск инсайдерских утечек по невнимательности» [6, с. 92]. Таким образом, техническое решение (два изолированных контура) напрямую провоцирует кадровую уязвимость, что требует комплексного, а не только технологического подхода.

Коллизия долговременного хранения. Срок хранения секретных документов может достигать 75 лет в ведомственных архивах. Электронные носители подвержены физическому

старению (3-5 лет для некоторых типов), а форматы файлов устаревают. Возникает проблема миграции данных, не регламентированная для цифровой среды. Действующие нормативные акты не содержат требований к долговременному хранению электронных секретных документов, что создаёт риск утраты информации.

Организация не может направить электронный документ с пометкой «Для служебного пользования» через систему МЭДО. По мнению А. В. Садыковой и Н. Г. Мироновой, «МЭДО в ряде регионов не аттестован под передачу сведений даже уровня ДСП» [2, с. 71]. Это следствие того, что МЭДО проектировалась под требования приказа № 17, не рассчитанные на информацию ограниченного доступа. Ни один из перечисленных нормативных актов не легализует понятие «гибридный документооборот» (бумажный оригинал + цифровая копия для учёта). Это создаёт правовую неопределённость для организаций, желающих частично автоматизировать секретное делопроизводство. Полный переход на безбумажный документооборот в режимно-секретных подразделениях невозможен в силу требований физической защиты носителей. В качестве компромисса предлагается концепция гибридного документооборота, включающая следующие системные решения. Легализация гибридного защищённого документооборота.

Основная коллизия между ст. 6 ФЗ № 63 и ст. 24 Закона о гостайне может быть разрешена путём внесения изменений в последнюю. Предлагается легализовать конструкцию, при которой юридически значимым оригиналом секретного документа остаётся бумажный носитель (что удовлетворяет требованию физической изоляции), а в системе электронного документооборота допускается наличие его цифровой копии с ограниченным набором реквизитов. Такая копия не является юридически значимой, но позволяет автоматизировать учёт, контроль движения и поиск документов. Целесообразно дифференцировать документы на три категории: приказы по основной деятельности (только бумажный носитель); журналы учета (возможно ведение в СЭД с применением сертифицированных СКЗИ); проекты документов (допустима обработка в изолированном сегменте). Такая классификация позволит внедрять ЭДО поэтапно, начиная с наименее критичных категорий. Внедрение технологии «шлюза безопасности». Применение однонаправленной передачи данных из открытого контура в закрытый позволяет автоматизировать входящий контроль.

Как отмечают А. В. Ивкин и соавторы, «передача информации из секретного контура наружу при использовании технологии исключена аппаратно» [6, с. 96]. Это техническое решение должно быть закреплено нормативно как допустимый способ обмена данными между контурами. Разделение «формы» и «содержания» документа. В открытом контуре допустимо использование только регистрационно-контрольной карточки документа без раскрытия содержательной части. Р. Г. Диниус указывает, что «такой подход позволяет автоматизировать учетные функции без риска компрометации конфиденциальной информации» [1, с. 78]. Это предложение требует нормативного закрепления допустимости вынесения учётных реквизитов в открытый контур. Разработка нормативных требований к долговременному хранению.

Необходимо издание совместного приказа Минцифры России и ФСТЭК России, который установил бы требования к типам носителей для долговременного хранения (с минимальным гарантированным сроком службы не менее 25-30 лет), порядок периодической миграции данных на новые носители и в актуальные форматы, а также ответственность за утрату данных при миграции. Аттестация системы МЭДО для передачи сведений ДСП. Необходимо внести изменения в регламент МЭДО и провести дополнительную аттестацию системы во всех субъектах Российской Федерации на предмет возможности передачи сведений «Для служебного пользования».

При этом передача сведений, составляющих государственную тайну, должна оставаться за рамками МЭДО и осуществляться по отдельным защищённым каналам. Проведенный анализ конкретных норм Федерального закона «Об электронной подписи», Закона РФ «О государственной тайне», приказов ФСТЭК № 17 и № 55 позволяет сделать следующие системные выводы. Коллизия между цифровизацией и режимом секретности носит не технический, а нормативный характер.

Противоречие между ст. 6 ФЗ № 63 и ст. 24 Закона о гостайне не может быть устранено технологическими средствами – требуется изменение законодательства. Существующая система порождает «двойной контур» документооборота, что ведёт к росту затрат (следствие требований физической изоляции) и кадровым рискам (когнитивная перегрузка сотрудников). Это прямое следствие отсутствия правового статуса гибридных решений.

Предлагаемая легализация «гибридного защищённого документооборота» (бумажный оригинал + цифровая копия с ограниченным набором реквизитов) позволяет частично автоматизировать учёт и контроль без нарушения требований по защите гостайны. Необходимо внесение изменений в следующие нормативные акты: Закон о гостайне (ст. 24), приказы ФСТЭК № 17 и № 55, а также регламент МЭДО. Только комплексное изменение нормативной базы, а не локальные технические решения, позволит преодолеть существующий цифровой разрыв между режимными и иными организациями в системе государственного управления.

Список литературы:

1. Об электронной подписи: Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 31.07.2025) // Собрание законодательства РФ. – 2011. – № 15. – Ст. 2036.
2. О государственной тайне: Закон РФ от 21.07.1993 № 5485-1 (ред. от 08.08.2024) // Собрание законодательства РФ. – 1997. – № 41. – Ст. 4673
3. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ ФСТЭК России от 11.02.2013 № 17 // Российская газета. – 2013. – № 106.
4. Диниус, Р. Г. Перспективы развития системы электронного документооборота / Р. Г. Диниус // Цифровое моделирование экономики. – 2025. – Т. 2, № 2. – С. 70-80.
5. Садыкова, А. В. Цифровизация и документационное обеспечение управления в России / А. В. Садыкова, Н. Г. Миронова // Форум молодёжной науки. – 2020. – № 6. – С. 71-75.
6. Ивкин, А. В. Концепция инфраструктуры системы электронного документооборота на основе технологии «блокчейн» // А. В. Ивкин, Е. Л. Мирошниченко, А. А. Волкова // Военная мысль. – 2023. – № 3. – С. 91-98.