

Медведев Владимир Александрович

канд. юрид. наук, доцент

Гаврилов Роман Евгеньевич

студент

ФГБОУ ВО «Чувашский государственный

университет им. И.Н. Ульянова»

г. Чебоксары, Чувашская Республика

АДВОКАТСКАЯ ТАЙНА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: НОВЫЕ УГРОЗЫ И ПРАВОВЫЕ СРЕДСТВА ИХ ПРЕОДОЛЕНИЯ

Аннотация: в статье рассматриваются проблемы обеспечения сохранности адвокатской тайны в условиях стремительного развития цифровых технологий. Анализируются основные угрозы: кибератаки, утечки данных, использование незащищённых каналов связи, облачные хранилища, а также риски, связанные с внедрением видео-конференц-связи в уголовное судопроизводство и удалённым доступом правоохранительных органов к перепискам в мессенджерах. Отмечается недостаточная правовая регламентация соответствующих отношений. Предлагаются меры технического, организационного и законодательного характера, направленные на укрепление гарантий адвокатской тайны в цифровую эпоху.

Ключевые слова: адвокатская тайна, цифровизация, кибербезопасность, конфиденциальность, информационные технологии, правовое регулирование, адвокатская деятельность, защита данных.

Право на квалифицированную юридическую помощь, закреплённое в ст. 48 Конституции РФ, по своей природе не может быть реализовано формально. Его действительность напрямую зависит от того, насколько доверитель уверен в безопасности передаваемой адвокату информации. Именно поэтому законодатель придаёт сведениям, связанным с оказанием юридической помощи, особый правовой режим – режим адвокатской тайны. Согласно ч. 1 ст. 8 Федерального

закона от 31.05.2002 №63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации», к ней относятся любые сведения, полученные адвокатом в связи с оказанием помощи своему доверителю. Такая широкая формулировка не случайна, она подчёркивает, что охране подлежит не только содержание консультации, но и сам факт обращения к адвокату, а также любые сопутствующие обстоятельства. Данный институт имеет глубокие исторические корни, восходящие ещё к эпохе Римской империи, и на протяжении веков остаётся важнейшей гарантией независимости адвоката и доверия между ним и клиентом. Однако сегодня угрозы, с которыми сталкивается адвокатская тайна, выглядят принципиально иначе. Если ещё 10–15 лет назад основными рисками для адвокатской тайны были незаконные допросы, обыски и изъятие документов [5, с. 31], то сегодня на первый план выходят угрозы, порождённые цифровизацией всех сфер жизнедеятельности, включая уголовное судопроизводство. Цель настоящей работы – систематизировать новые вызовы и предложить комплексные меры по обеспечению сохранности адвокатской тайны в цифровую эпоху.

Адвокатская тайна традиционно рассматривается как обязанность адвоката не разглашать сведения, полученные от доверителя. Кодекс профессиональной этики адвоката (ст. 5) устанавливает, что информация сохраняет статус тайны с момента обращения клиента к адвокату и до момента окончательного расчёта, причём под охрану подпадают любые сведения, связанные с участием адвоката в деле [3]. Рекомендации по обеспечению адвокатской тайны и гарантий независимости адвоката, разработанные адвокатским сообществом, конкретизируют отдельные аспекты, однако в условиях цифровизации этих разъяснений становится недостаточно.

Развитие информационных технологий породило целый спектр новых опасностей для адвокатской тайны. Рассмотрим ключевые из них.

Во-первых, это кибератаки и утечки данных. Юридические фирмы и отдельные адвокаты всё чаще становятся мишенями хакеров, поскольку в их распоряжении находятся ценные сведения: договоры, переписка, стратегии ведения дел. Фишинг, вредоносные скрипты, программы-вымогатели, атаки на облачные

хранилища – всё это создаёт реальную угрозу конфиденциальности. Показательны случаи 2022 г., когда в результате атак на крупные юридические компании США были похищены данные о тысячах судебных процессов [4, с. 24].

Во-вторых, широкое использование незащищённых каналов связи. Мессенджеры, электронная почта, видео-конференц-связь, все эти инструменты, ставшие повседневными в работе адвоката, далеко не всегда обеспечивают должный уровень шифрования. Кроме того, адвокаты нередко применяют одни и те же устройства для работы и личных целей, что повышает риск утечки.

Третья проблема – облачные хранилища. Удобство доступа к документам из любой точки мира оборачивается необходимостью тщательной настройки прав доступа и двухфакторной аутентификации. В противном случае конфиденциальная информация окажется в руках злоумышленников [4, с. 25].

В-четвёртых, хотелось бы указать, что специфические риски также возникают в уголовном судопроизводстве. Внедрение видео-конференц-связи (ВКС) для проведения следственных действий и свиданий защитника с подзащитным, с одной стороны, упрощает процесс, но с другой – создаёт возможность записи и последующего доступа третьих лиц к конфиденциальной беседе. Аналогичные проблемы возникают при удалённом доступе правоохранительных органов к перепискам в мессенджерах: даже после удаления сообщений они могут храниться на серверах операторов связи в течение трёх лет и быть предоставлены по запросу. Наконец, обязанность владельцев сетей связи предоставлять уполномоченным органам информацию, необходимая для оперативно-разыскной деятельности, также создаёт предпосылки для нарушения адвокатской тайны.

Действующее законодательство об адвокатуре и адвокатской деятельности формировалось в эпоху, когда цифровые инструменты были не так сильно распространены. Как следствие, многие аспекты защиты адвокатской тайны в цифровой среде остаются неурегулированными. Отсутствуют чёткие нормы, обязывающие адвокатов использовать шифрование, устанавливающие ответственность за утечки, определяющие стандарты безопасности для юридических

компаний. Рекомендации адвокатского сообщества носят общий характер и не подкреплены механизмами принуждения.

Для эффективного противодействия угрозам необходим комплексный подход, сочетающий технические, организационные и правовые меры.

На техническом уровне целесообразно применять обязательное шифрование всех данных, включая переписку, документы и записи видеоконференций; использование защищённых каналов связи и мессенджеров с оконечным шифрованием; применение двухфакторной аутентификации; регулярное резервное копирование с хранением копий на отдельных носителях; привлечение квалифицированных IT-специалистов для аудита безопасности.

На организационном уровне важно повышение квалификации адвокатов в области кибербезопасности [2]; проведение регулярных проверок защищённости информационной среды; создание при адвокатских палатах субъектов РФ центров обнаружения и предупреждения нарушений, связанных с использованием цифровых технологий. Такие центры могли бы информировать адвокатов о новых способах кибератак, консультировать по вопросам безопасного обмена документами, помогать в реагировании на инциденты.

Также представляется, что решение проблемы лежит не в точечных поправках, а в смене подхода к регулированию. Действующий Федеральный закон №63-ФЗ рассматривает адвокатскую тайну преимущественно как этическую обязанность, тогда как в цифровой среде она всё чаще становится объектом технического и процессуального регулирования. Назрела необходимость введения в закон специальной главы, которая бы не просто дублировала существующие нормы, а устанавливала механизм гарантий: от требований к каналам связи, используемым для передачи конфиденциальных сведений, до порядка действий адвоката при обнаружении попытки несанкционированного доступа. Кроме того, целесообразно законодательно закрепить минимальные стандарты информационной безопасности для адвокатских образований и предусмотреть процессуальные барьеры, исключающие попадание сведений, составляющих тайну, в материалы дела при использовании цифровых технологий. Отдельного внимания

требует вопрос об ответственности операторов связи и облачных сервисов, поскольку именно они становятся «точками утечки», находящимися вне контроля адвоката.

Цифровая трансформация юридической сферы – необратимый процесс. Внедрение новых технологий, безусловно, несёт положительные моменты, однако одновременно создаёт беспрецедентные вызовы для адвокатской тайны. Ни действующее законодательство, ни корпоративные рекомендации пока не обеспечивают надёжных гарантий сохранности конфиденциальной информации. Представляется, что цифровизация и развитие правовых гарантий адвокатской тайны должны идти параллельно. Только системный подход, объединяющий технические решения, организационные меры и совершенствование нормативной базы, позволит сохранить доверие клиентов и обеспечить реальную защиту их интересов в цифровую эпоху.

Список литературы

1. Блажеев, В. В. Цифровое право : учебник / В. В. Блажеев, М. А. Егорова. – Москва, 2020. – 623 с.
2. Исаев, С. В. Анализ киберугроз и их источников для корпоративной сети Красноярского научного центра СО РАН / С. В. Исаев // Информационные и математические технологии в науке и управлении. – 2016. – № 4–1.
3. Кириллова, Н. П. Проблемы осуществления уголовного преследования по делам о преступлениях, совершаемых в сфере высоких информационных технологий / Н. П. Кириллова, С. П. Кушниренко // Правоведение. – 2013. – № 3 (308). – С. 74–90.
4. Мchedlishvili, P. P. Кибербезопасность в юридической сфере: угрозы и защита данных / Р. Р. Мchedlishvili, В. Р. Чакрян // Инновационная наука. – 2023. – № 12–1. – С. 45–49.
5. Соловьева, Ю. И. Проблема обеспечения сохранения адвокатской тайны в условиях цифровизации / Ю. И. Соловьева // Евразийская адвокатура. – 2019. – № 6(43). – URL: <https://cyberleninka.ru/article/n/problema-obespecheniya->

sohraneniya-advokatskoy-tayny-v-usloviyah-tsifrovizatsii (дата обращения:
27.10.2026). – Текст : электронный.