

Купирова Чулпан Шеукатовна

канд. юрид. наук, доцент

Алексеева Карина Геннадьевна

студентка

ФГБОУ ВО «Чувашский государственный

университет им. И.Н. Ульянова»

г. Чебоксары, Чувашская Республика

ОБЕСПЕЧЕНИЕ АДВОКАТСКОЙ ТАЙНЫ В ЦИФРОВЫХ КАНАЛАХ КОММУНИКАЦИИ

Аннотация: *обеспечение адвокатской тайны в цифровой среде требует комплексного подхода, сочетающего технические меры защиты с осознанным выбором инструментов и соблюдением профессиональных стандартов. В статье предлагаются меры по защите конфиденциальной информации для обеспечения адвокатской тайны. Адвокат должен постоянно следить за новыми угрозами и применять защитные меры.*

Ключевые слова: *адвокатская тайна, адвокатская деятельность, цифровизация, информационная безопасность, персональные данные.*

Соблюдение адвокатской тайны является обязательным условием реализации права граждан на квалифицированную юридическую помощь, закрепленное Конституцией РФ (ст. 48). Данный термин законодательно закреплен Федеральным законом от 31 мая 2002 г. №63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» (ст. 8). Согласно статье 8 данного закона, адвокатская тайна включает любые сведения, связанные с оказанием юридической помощи, в том числе содержание консультаций, переписку и иные документы, полученные адвокатом от доверителя.

Современный уровень цифровизации существенно повлиял как в целом на юридическую профессию, так и адвокатскую практику, что также привело к появлению новых рисков в сфере обеспечения конфиденциальности.

В статье авторами рассмотрены основные угрозы и способы защиты информации, составляющей адвокатскую тайну.

В настоящее время профессиональная деятельность адвоката имеет преимущественно «удаленный» характер. При проведении судебных заседаний широко используются возможности видеоконференцсвязи, подачу и получение документов из суда возможно осуществлять электронно, а работу с доверителем и его документами организовать в облачном пространстве. Однако, за определенным на первый взгляд упрощением взаимодействия между сторонами, возникают и определенные риски, связанные с обеспечением информационной безопасности. Рассмотрим самые распространенные.

1. Утечка через облачные сервисы. Публичные облачные платформы (Яндекс Диск, Google Drive и т. п.) удобны для совместной работы, но их серверы могут физически находиться за границей. Это создаёт риск несанкционированного доступа к данным со стороны иностранных органов или из-за уязвимостей сервиса.

2. Незащищённые каналы связи. Пересылка сканов документов через мессенджеры, электронную почту или соцсети (например, ВКонтакте, Телеграмм) – самая частая ошибка. Даже популярные сервисы не гарантируют абсолютную безопасность: их могут взломать, а метаданные (информация о том, когда и кому отправили файл) – собирать.

3. Риски с устройств. Смартфоны, ноутбуки, планшеты – всё это хранит конфиденциальную информацию. Если устройство потеряно или украдено, данные могут попасть к третьим лицам. Сюда же относится использование публичных Wi-Fi сетей: данные легко перехватить.

4. Безответственные (халатные) действия самих участников: передача материалов через личные аккаунты, использование слабых паролей, несанкционированный доступ помощников к данным.

5. Влияние госорганов и IT-корпораций. Законодательство (например, обязанность операторов связи хранить переписку) может создавать зависимость адвоката от третьих лиц, что ставит под угрозу конфиденциальность.

6. Цифровой след. Сам факт поиска информации в интернете (изучение судебной практики, новостей по теме дела) формирует пассивный цифровой след, который может быть проанализирован.

Разглашение адвокатской тайны способно привести к неблагоприятному для доверителя исходу рассмотрения судом того или иного дела, поэтому первостепенная задача при совместной работе адвоката с доверителем – это сохранность и недопущение утечки третьим лицам конфиденциальной информации. Следовательно, актуальным представляется проблема какими способами можно защитить конфиденциальные сведения в сети.

Среди технических мер защиты шифрование данных – ключевой способ защиты при передаче и хранении информации. Как при хранении, так и при пересылки такой информации крайне рекомендуется использовать различные средства шифрования, которые могут быть уже встроенными в операционную систему, либо носить характер стороннего решения. В настройках мобильных устройств также должно быть активировано шифрование содержимого памяти.

Следующий способ защиты информации – использование безопасных каналов связи. Если это мессенджеры, то необходимо выбирать платформы со сквозным шифрованием (например, секретные чаты в Telegram, Signal, Wickr), активировать функцию автоматического удаления сообщений по истечении заданного времени. Если это электронная почта, то будет безопаснее использовать корпоративные почтовые ящики или сервисы с двухфакторной аутентификацией. Ни в коем случае нельзя пересылать конфиденциальные файлы через уязвимые сервисы. При осуществлении звонков для конфиденциальных разговоров также можно использовать мессенджеры со сквозным шифрованием.

Мобильное устройство, компьютер и сервис (электронная почта, облачное хранилище, мессенджер) адвоката и доверителя должны быть защищены надежным уникальным паролем: более 12 символов, включая спецсимволы, цифры, строчные и заглавные буквы [2].

При работе с облачными хранилищами не рекомендуется использовать публичные облачные сервисы, серверы которых могут располагаться за пределами

РФ, так как это повышает риск несанкционированного доступа третьих лиц; также данные разных доверителей необходимо хранить отдельно.

Передачу ссылок на файлы и пароли для доступа к ним полезно осуществлять по разным каналам связи (например, ссылку – по email, пароль – в мессенджере).

Необходимо своевременно обновлять программное обеспечение на всех устройствах, чтобы закрывать уязвимости, а также для защиты от компьютерных вирусов и кибератак нужно использовать постоянное функционирование антивирусных средств защиты.

Кроме того, должны соблюдаться базовые правила безопасной работы в сети «Интернет».

Таким образом, адвокату в процессе своей профессиональной деятельности необходимо обучаться и совершенствовать свои знания в сфере кибербезопасности.

Институт адвокатской тайны защищён комплексом норм: Конституцией РФ, Федеральным законом «Об адвокатской деятельности и адвокатуре в Российской Федерации», процессуальным законодательством и международными актами.

В качестве проблемы, требующей законодательного решения, стоит отметить, что нормы права, «регламентирующие институт адвокатуры, созданы до того момента, когда технология и цифровые инструменты стали полноценной частью профессиональной деятельности адвоката. Таким образом, многие аспекты защиты адвокатской тайны и конфиденциальной информации – пробельны» [4]. Необходима разработка и внедрение единых корпоративных стандартов цифровой безопасности для адвокатских палат, включающих в себя комплекс обязательных требований к защите информации в адвокатской деятельности.

В экспертной среде звучат такого рода предложения, вопрос как гарантировать сохранность адвокатской тайны является актуальным. Требуется внесение изменений в действующие законы либо разработка дополнительных подзаконных актов, с чётко прописанными техническими и организационными мерами

защиты адвокатской тайны и регламентацией электронного взаимодействия с судами и доверителем.

Кроме того, Федеральная палата адвокатов и региональные палаты должны направить усилия на выявление практических инструментов, позволяющих обеспечить требования безопасности в цифровой среде, разработать соответствующие методические рекомендации для адвокатов и доверителей, рассмотреть возможность создания консультационных центров для обмена положительным опытом, проведения регулярных обучающих семинаров, тренингов по информационной безопасности.

Список литературы

1. Жукова, Е. В. Адвокатская тайна и цифровые технологии: проблемы конфиденциальности в электронном документообороте / Е. В. Жукова // Наука сегодня: актуальные вопросы теории и практики : сборник статей VI Международной научно-практической конференции. В 2 ч. Ч. 2 (Пенза, 30 мая 2025 г.). – Пенза : Наука и Просвещение, 2025. – С. 104–106.

2. Правила цифровой безопасности. – URL: <https://www.advgazeta.ru/mneniya/pravila-tsifrovoy-bezopasnosti> (дата обращения: 13.10.2026). – Текст : электронный.

3. Чистяков, Н. С. Влияния процессов цифровизации на институт адвокатской тайны / Н. С. Чистяков // Научные высказывания. – 2024. – № 10 (57). – С. 60–63.

4. Магдеева, Д. И. Адвокатская тайна в цифровую эпоху: вызовы и способы защиты / Д. И. Магдеева // Вестник Пензенского государственного университета. – 2025. – № 2 (50). – С. 22–26.