

К ВОПРОСУ ОБ ОБЕСПЕЧЕНИИ СОБЛЮДЕНИЯ АДВОКАТСКОЙ ТАЙНЫ В ПРОЦЕССЕ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ СРЕДСТВ КОММУНИКАЦИИ И ПЕРЕДАЧИ ДАННЫХ

О минимальных необходимых мерах по защите данных и конфиденциальной информации, используемых в деятельности адвокатов при осуществлении ими профессиональной деятельности.

СМИРНОВ Владимир Владимирович

LL.M. (Munster), старший преподаватель кафедры уголовно-правовых дисциплин
ФГБОУ ВО «Государственный университет по землеустройству»
г. Москва, Россия

В статье анализируются угрозы безопасности хранимой и передаваемой информации в юридическом обороте и предлагаются на рассмотрение некоторые рекомендации по защите данных и информации, прежде всего составляющей адвокатскую тайну.

Ключевые слова: адвокатура, электронный документооборот, электронная коммуникация, обмен данными между адвокатами, а также их доверителями, адвокатская тайна.

Сохранение адвокатской тайны – это одно из основных правил и важнейших обязанностей адвоката, прямо закрепленных в Федеральном законе от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации». Согласно статье 8 Федерального закона № 63-ФЗ, адвокат не имеет права разглашать информацию, полученную от своего клиента, если она относится к делу, по которому он его защищает. Эта информация остается конфиденциальной и не может быть использована в уголовном или гражданском процессах без согласия клиента. Соблюдение этого правила позволяет установить доверительный отношение между адвокатом и клиентом, что является важным условием качественной защиты прав и интересов доверителя.

Развитие современных информационных технологий сопровождается в том числе переформатированием всех документов в электронный (цифровой) вид. При этом информация не только хранится, но и передается с помощью цифровых технологий и электронных устройств.

Важнейшей обязанностью адвоката при использовании электронных средств коммуникации является обеспечение сохранности конфиденциальной информации, которую доверитель может сообщить в ходе оказания юридической помощи.

Адвокаты должны быть осведомлены о

том, как правильно использовать современные технологии и как сохранять конфиденциальность своих клиентов. Существует множество рекомендаций и инструментов для защиты конфиденциальной информации, таких как безопасные электронные почтовые сервисы, зашифрованные каналы связи, а также обучение сотрудников о соблюдении правил безопасности при работе с информацией. Нарушение адвокатской тайны может иметь серьезные последствия для профессиональной репутации и даже стать преступлением, поэтому важно соблюдать все меры безопасности для защиты конфиденциальной информации.

Представляется, что использование электронных средств коммуникации в адвокатской деятельности, и вообще в юридической практике может повлечь за собой следующие риски:

1. Нарушение адвокатской тайны: при передаче конфиденциальной информации через электронные средства коммуникации существует риск ее утечки, что может привести к нарушению адвокатской тайны и нарушению закона.

2. Несанкционированный доступ к информации: если электронные средства коммуникации не безопасны, то существует риск несанкционированного доступа к конфиденциальным данным.

3. Сохранение информации: вопрос сохранения информации является ключевым, поскольку, если данные не будут сохранены

должным образом, то это может привести к утечкам и потере информации.

4. Ошибки при передаче информации: при передаче информации через электронные средства коммуникации могут возникнуть технические сбои, которые могут привести к ошибкам при передаче информации, что, в свою очередь, может повлечь за собой нежелательные юридические последствия.

5. Несоответствие требованиям законодательства: использование электронных средств коммуникации может столкнуться с техническими ограничениями и требованиями законодательства, которые нужно учитывать для обеспечения безопасности конфиденциальной информации и соблюдения закона.

Таким образом, Основные требования к информационной безопасности в юридической практике включают в себя следующие аспекты:

1. Защита адвокатской тайны: необходимо обеспечить сохранность и конфиденциальность информации, содержащей адвокатскую тайну. Для этого используются средства криптографической защиты информации, методы аутентификации, контроль доступа, защита от несанкционированного доступа и т. д.

2. Надежность программного обеспечения: для обеспечения информационной безопасности в юридической практике необходимо использовать программное обеспечение, которое соответствует требованиям законодательства, обеспечивает защиту от вирусов и атак злоумышленников.

3. Безопасность хранения информации: для обеспечения сохранности и конфиденциальности информации необходимо использовать специализированные складские помещения, оборудованные системами контроля доступа. Также важно регулярно создавать резервные копии данных, чтобы восстановить информацию в случае потери или повреждения.

4. Контроль за доступом: необходимо обеспечить контроль доступа к информации путем определения параметров доступа. Необходимо использовать системы аутентификации и авторизации, контроль доступа к сети Интернет и системе электронной почты.

5. Контроль изменений: изменения в документах, связанных с юридической практи-

кой, необходимо контролировать и регистрировать, чтобы не допустить несанкционированных изменений.

б. Обучение: важно проводить обучение юристов и персонала, занятого в юридической практике, правилам информационной безопасности. Обучение может проводиться с использованием как офлайн-курсов, так и онлайн-платформ. Информационная безопасность в юридической практике является ключевым аспектом, который должен быть основой при использовании электронных средств коммуникации и передаче данных.

Разработка единых рекомендаций по работе адвоката с электронными устройствами, подготовленных на основании анализа практической адвокатской деятельности, а также взаимодействия с техническими специалистами в сфере цифровых технологий, является необходимой и важной задачей. В настоящее время использование электронных устройств и цифровых технологий неизбежно при выполнении адвокатских задач, поэтому нужны четкие правила и рекомендации для обеспечения безопасного и эффективного использования таких устройств, а также защиты конфиденциальной информации клиента в электронном виде.

По нашему мнению, поскольку обмен информацией с доверителем через интернет, особенно посредством электронной почты, является потенциально опасным с точки зрения безопасности информации, чтобы снизить риски несанкционированного доступа к информации, обеспечить безопасность электронных коммуникаций и защитить сведения, составляющие адвокатскую тайну, необходимо следовать определенным мерам предосторожности:

1. Использовать надежные пароли и системы аутентификации для защиты доступа к устройствам и информации, для электронной почты и других онлайн-аккаунтов.

2. Использовать только установленные и авторизованные программы для работы с электронной почтой и обмена информацией.

3. Использовать защищенные подключения к Интернету, виртуальные частные сети (VPN) для безопасной передачи данных через Интернет.

4. Использовать специальное программное обеспечение для защиты электронной почты, такое как антивирусы и антишпионы.

5. Шифровать важную информацию, передаваемую через интернет, с помощью соответствующих инструментов, таких как сертификаты цифровой подписи или программное обеспечение для шифрования и дешифрования сообщений.

6. Использование сертификатов для проверки подлинности отправителя и защиты от подделки электронной почты.

7. Производить регулярное обновление программного обеспечения и антивирусных программ для защиты от вирусов и кибератак.

8. Всегда проверять достоверность отправителя и получателя сообщений, чтобы избежать фишинговых атак.

9. В условиях работы офисов адвокатских образований ограничивать доступ к информации только уполномоченным лицам с применением правил доступа и механизмов контроля доступа.

10. Стараться не отправлять чувствительную информацию через электронную почту, особенно без предварительного шифрования. Лучше выбрать более безопасные способы передачи информации, например, защищенные онлайн-сервисы.

С современными технологиями защищать конфиденциальную информацию на электронных гаджетах стало значительно проще и надежнее.

Проблема защиты конфиденциальной информации, составляющей адвокатскую тайну при использовании электронных гаджетов, в целом уже решена в техническом плане. Смартфоны практически любой марки и производителя, независимо от используемой операционной среды (Android, iOS) обладают встроенной функцией блокировки, снятие которой производится по антропометрическим данным человека (папиллярный узор, сканирование и распознавание лица). Ноутбуки, широко используемые адвокатами в практической деятельности, имеют сканер отпечатка пальца, причем это оборудование производители стали устанавливать достаточно давно, и за это время пользователи уже имели возможность убедиться в его высокой надежности и простоте использования.

Кроме того, существует шифрование файлов и дисков, что делает еще более сложной возможность несанкционированного доступа к информации. Важно, что адвокаты должны использовать законные средства защиты конфиденциальной информации, чтобы защитить своих клиентов.

ЛИТЕРАТУРА

1. Адвокатская палата города Москвы. Регламентирующие документы. – URL:<https://www.advokatymoscow.ru/appointment/documents/>.
2. Гусятников П.П., Гусятникова П.П. Информационная безопасность адвоката // *Achievements to high school: материалы 11-й международной научно-практической конференции*. – София, 2015. – Т. 5: Закон.
3. Иванова И.Г. Проблемы правового регулирования адвокатской тайны в свете цифровизации адвокатской деятельности / И.Г. Иванова, А.О. Орешникова. – Текст: непосредственный // *Молодой ученый*. – 2022. – № 49(444). – С. 363-365. – URL:<https://moluch.ru/archive/444/97337/> (дата обращения: 10.04.2023).
4. Коган М.И. Обеспечение сохранения адвокатской тайны при использовании адвокатом современных технологий и электронных девайсов. Трибуна молодого ученого // *Вестник университета имени О.Е. Кутафина (МГЮА)*. – URL:<https://cyberleninka.ru/article/n/obespechenie-sohraneniya-advokatskoy-tayny-pri-ispolzovanii-advokatom-sovremennyh-tehnologiy-i-elektronnyh-devaysov/viewer>.
5. Смирнов В.В. Инструменты дальнейшего развития электронного правосудия в России // *Научный потенциал*. – 2022. – № 1(36). – С. 26-29.
6. Указ Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» (ред. от 19.07.2018) Справочно-правовая система (СПС) «Консультант Плюс: Высшая школа. – URL: <http://www.consultant.ru> (дата обращения: 17.03.2023).

TO THE OAPR ON THE ENFORCEMENT OF ATTORNEY-CLIENT PRIVILEGE IN THE USE OF ELECTRONIC MEANS OF COMMUNICATION AND DATA TRANSMISSION

On the minimum necessary measures to protect data and confidential information used in the activities of lawyers in the exercise of their professional activities.

SMIRNOV Vladimir Vladimirovich

LL.M. (MÜNSTER), Senior Lecturer of the Department of Public Law
State University of Land Use Planning
Moscow, Russia

The article analyzes threats to the security of stored and transmitted information in legal circulation and are proposed for consideration by some recommendations for data protection and information, primarily constituting a lawyer secret.

Keywords: advocacy, electronic document flow, electronic communication with courts, data exchange between lawyers, as well as their principals, lawyer institution.

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА СБЫТА НАРКОТИКОВ ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

СОШНИКОВА Ирина Владимировна

кандидат социологических наук, доцент, доцент кафедры публичного права
ФГБОУ ВО «Уральский государственный экономический университет»

БОГДАНОВ Александр Серафимович

магистрант

Уральский институт управления – филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте РФ»
г. Екатеринбург, Россия

В статье проведено исследование уголовно-правовой характеристики сбыта наркотиков посредством использования информационно-телекоммуникационных сетей.

Ключевые слова: уголовно-правовая характеристика, наркотические средства, психотропные вещества, информационно-телекоммуникационные сети.

Преступления, связанные с незаконным оборотом наркотиков, являются чрезвычайно опасными, поскольку порождают вредные последствия для здоровья людей и представляют серьезную общественную угрозу. Наркотическая преступность выступает актуальной проблемой практически для любой страны мира.

Обеспокоенное отношение общества к проблеме распространения данного вида преступлений подтверждает статистика, которая регулярно ведется государственными органами в целях учета преступлений.

Рассмотрим статистику зарегистрированных преступлений в указанной сфере и проанализируем показатель прироста преступлений. В 2018 г. зарегистрировано 200306 преступлений, по сравнению с 2017 г. прирост преступлений составил – 4.0%. В 2019 – 190197, по сравнению с предыдущим годом прирост составил – 5.0%. В 2020 – 189905, по сравнению с предыдущим годом прирост составил – 0.2%. В 2021 – 179732, по сравнению с предыдущим годом прирост составил – 5.4%. В 2022 – 177741, по сравнению с предыдущим годом прирост составил – 1.1%.