Рекомендуемые практические меры по обеспечению информационной безопасности адвокатской деятельности (включая меры по защите информации, составляющей предмет адвокатской тайны)

Данный документ носит неофициальный характер и никоим образом не противоречит положениям, изложенным в Рекомендациях по обеспечению адвокатской тайны и гарантий независимости адвоката при осуществлении адвокатами профессиональной деятельности (Утверждены решением Совета ФПА РФ, 30.11.2009, Протокол №3).

Вместе с тем, авторами предпринята попытка дополнить практические рекомендации по обеспечению адвокатской тайны, принимая во внимание растущую информатизацию современного общества и учитывая международный опыт в данной сфере.

Отметим также, что именно адвокат обязан принимать меры, направленные на защиту доверителя от ситуаций, когда несанкционированный доступ к тайне становится возможным по оплошности (неосторожности) адвоката или полученная третьими лицами информация незаконно используется для формирования доказательственной базы обвинения или исковых требований.

Содержание документа

1. Передача информации в устной форме

1. Общаться с доверителем следует в помещениях, позволяющих обеспечить конфиденциальность общения, что имеет особое значение для адвокатов, осуществляющих адвокатскую деятельность в форме адвокатского кабинета и использующих для этих целей жилые помещения.

2. В телефонных и иных голосовых разговорах (например, через WhatsApp, Viber и др.) с доверителем не рекомендуется касаться вопросов, в которые не должны быть посвящены посторонние, не использовать «громкую» телефонную связь.

3. При общении с доверителем, как лично, так и по телефону (или иным голосовым способом) адвокат должен отдавать себе отчет, что его разговор может записываться доверителем, а также прослушиваться или записываться третьими лицами.

4. В случае необходимости для защиты от прослушивания адвокату рекомендуется использовать разные SIM-карты или телефонные аппараты, а при обсуждении особо важных дел выключать мобильный телефон и вынимать из него батарею питания.

2. Обращение с информацией, содержащейся в физических документах

Примечание. Под физическими документами понимаются материальные носители, на которых информация хранится не в электронном (цифровом) виде, т.е. любые письменные документы, печатные документы, фотографии, аналоговые аудиозаписи, вещественные доказательства и т.д., включая физические документы, переданные доверителем и адвокатское производство.

1. Физические документы не должны храниться или находиться в местах, где с ними смогут ознакомиться, скопировать, повредить или похитить лица, которые не должны быть посвящены в содержание этих документов, в том числе адвокаты, помощники и стажеры адвоката, иные сотрудники адвокатского образования и посетители.

2. Физические документы не должны храниться или находиться в местах, где их могут случайно увидеть или прочесть их содержание лица, входящие в помещение.

3. Не допускается работа с физическими документами (в том числе их чтение, изучение, копирование) в общественных и других местах, в условиях, при которых их содержание может стать известно посторонним лицам.

4. Физические документы должны храниться в служебных помещениях, используемых адвокатом для осуществления адвокатской деятельности или в другом надежном месте, куда адвокат имеет беспрепятственный доступ.

Адвокат может работать с физическими документами в иных помещениях при условии осторожного обращения с ними. При этом рекомендуется брать с собой только минимальное количество документов, необходимое для осуществления профессиональной деятельности.

5. Адвокат должен убрать физические документы в место постоянного хранения сразу после завершения непосредственной работы с ними.

6. Физические документы, содержащие адвокатские производства, в отношении каждого доверителя должны храниться отдельно (а при необходимости и для удобства — должны храниться отдельно документы, содержащие адвокатские производства по каждому делу). При этом физические документы, содержащие правовую аналитику (изложение правовой позиции, тактику, рекомендации и др.), должны храниться отдельно от документов, представленных доверителем.

Физические документы, содержащие адвокатские производства, необходимо хранить в папках, имеющих наклейку или надпись: «Адвокатское производство. Содержащиеся в адвокатском производстве сведения составляют охраняемую законом адвокатскую тайну и не могут использоваться в качестве доказательств обвинения».

7. Физические документы (папки с адвокатскими производствами) необходимо хранить в сейфах или шкафах, имеющих прочно удерживаемую наклейку или надпись: «В сейфе (шкафу) содержатся сведения, составляющие охраняемую законом адвокатскую тайну».

8. Необходимо обеспечить сохранность и безопасность физических документов при их перемещении вне жилых и служебных помещений, используемых для осуществления адвокатской деятельности. Не рекомендуется переносить или перевозить физические документы без необходимости.

В случае необходимости, рекомендуется перемещать только минимальное количество документов, необходимое для осуществления профессиональной деятельности. Перемещение физических документов необходимо производить в папках с такой же надписью, как и при хранении.

9. При перемещении физических документов пешком или на общественном транспорте, документы не должны быть на виду и должны быть убраны в сумку или портфель, который должен постоянно находиться в руках или, как минимум, в поле зрения и не оставаться без присмотра до тех пор пока документы не будут доставлены в место назначения с целью предотвращения их утери, повреждения или хищения.

Таким же образом должно производиться перемещение физических документов на личном транспорте (автомобиле). Физические документы не должны оставаться в автомобиле без присмотра, за исключением случаев, когда это потенциально безопаснее, чем взять их с собой. Запрещается оставлять документы в автомобиле на ночь или более длительный срок.

10. При копировании, сканировании или распечатке документов необходимо знать о том, что современная техника (принтеры, сканеры, копиры) может сохранять копии документов в своей оперативной памяти или на встроенном жестком диске.

11. Во избежание возникновения конфликтов и споров по поводу возможной утраты оригинальных документов рекомендуется по возможности не хранить оригиналы предоставленных доверителями документов, а снимать с них копии. Оригиналы документов целесообразно затребовать у доверителя только по мере необходимости, когда они должны быть представлены в суд или иные органы. Рекомендуется письменно фиксировать передачу таких документов от доверителя адвокату и наоборот.

3. Обращение с электронной информацией, содержащейся на электронных приборах и иных цифровых носителях

Примечание. Под электронными приборами понимается компьютеры, ноутбуки, планшеты, смартфоны и иные приборы, предназначенные для хранения, обработки и передачи информации, представленной в электронном виде. Под цифровым носителем в данном разделе понимаются материальные носители, на которых информация хранится в электронном (цифровом) виде, т.е. съемные носители информации, флеш-карты памяти, жесткие диски, дискеты и др. Цифровой носитель может быть составной частью электронного прибора, например, жесткий диск компьютера или ноутбука.

1. К электронным приборам и цифровым носителям, в силу того, что они являются материальными предметами, применимы все общие правила раздела 2, только лишь с некоторыми поправками на то, что информация на них хранится в электронном виде. Необходимо принимать все перечисленные в разделе 2 меры по предотвращению утери, повреждения или хищения электронных приборов и цифровых носителей при их хранении, работе с ними и перемещении.

2. Электронные приборы, имеющие экран (ноутбуки, планшеты и др.), не должны размещаться так, чтобы содержание экрана могли случайно увидеть или прочесть посторонние лица, особенно при работе с ними в общественных местах.

В общественных местах и при общении с доверителем не рекомендуется класть планшет или смартфон на стол или иную поверхность экраном вверх. Рекомендуется убрать его в сумку или карман или же положить экраном вниз.

3. Электронные приборы и цифровые носители должны иметь прочно удерживаемую наклейку или надпись: «Адвокатское производство. Содержащиеся в адвокатском производстве сведения составляют охраняемую законом адвокатскую тайну и не могут использоваться в качестве доказательств обвинения». В случае малых физических размеров цифрового носителя надпись может быть сокращена до «Адвокатское производство. Содержит адвокатскую тайну».

4. Особую осторожность нужно проявлять в обращении с электронными приборами и цифровыми носителями, содержащими большие объемы информации, относящейся к адвокатскому производству по делам большого количества доверителей за длительный период времени (например, ноутбук адвоката, на котором хранятся материалы по всем делам за несколько лет). Утеря или распространение информации, содержащейся на данном цифровом носителе, может повлечь за собой серьезные последствия.

5. Крайне желательно для осуществления профессиональной деятельности использовать отдельные электронные приборы, содержащие только информацию, связанную с адвокатской деятельностью. Если это невозможно, личную информацию и документы необходимо хранить отдельно от адвокатского производства.

Электронные приборы, используемые для профессиональной деятельности, не рекомендуется выносить без необходимости за пределы жилых и служебных помещений, используемых для осуществления адвокатской деятельности.

6. Рекомендуется хранить всю электронную информацию в зашифрованном виде, для чего использовать специальное программное обеспечение для шифрования отдельных файлов, дисковых разделов или приборов целиком. Рекомендуется использовать шифрование дисковых разделов или приборов целиком, в том числе шифрование системного раздела компьютеров и ноутбуков.

Резервный пароль или диск для аварийного дешифрования информации необходимо хранить отдельно в надежном месте, куда адвокат имеет беспрепятственный доступ.

7. При наличии технической возможности, необходимо активировать в электронных приборах встроенную функцию дистанционного удаления всей информации (Find-my-iPhone и др.) на случай их утери или кражи (или установить на прибор соответствующее программное обеспечение, реализующее данную функцию). В случае утери электронного прибора необходимо дистанционно удалить все его содержимое.

8. Для мобильных электронных приборов и цифровых носителей необходимо максимально уменьшить количество информации, хранящейся непосредственно на них. Рекомендуется хранить на мобильных устройствах только информацию за последние несколько дней (недель). Прочая информация должна храниться на стационарных приборах и носителях.

9. Следует крайне осторожно относиться к использованию цифровых носителей, не принадлежащих адвокату (в том числе, принадлежащих доверителю), так как указанные носители могут содержать вирусы или вредоносное/шпионское программное обеспечение.

10. Необходимо составить и поддерживать актуальный перечень всех электронных приборов, используемых для осуществления адвокатской деятельности с указанием серийного номера.

4. Электронные приборы и доступ в Интернет

1. Доступ ко всем электронным приборам должен быть защищен паролем или сканером отпечатков пальцев (допускается использование иных биометрических технологий). Рекомендуется использование паролей, состоящих не менее чем из 8 символов, включающих в себя буквы, строчные и прописные, цифры и специальные символы. Использование примитивных паролей (1-1-1-1, 1-2-3-4 и др.) не допускается. Не допускается использование одинаковых паролей для доступа к различным электронным приборам.

2. На всех электронных приборах необходимо настроить режим автоматической блокировки в случае неиспользования прибора в течение ограниченного времени (не более нескольких минут); для вывода из режима блокировки должен требоваться ввод пароля или отпечатка пальца.

3. Все используемые электронные приборы: серверы, компьютеры, планшеты, смартфоны должны быть защищены регулярно обновляемым антивирусным программным обеспечением и сетевым экраном. Операционная система на каждом электронном приборе должна своевременно обновляться, обновления связанные с безопасностью, должны устанавливаться максимально оперативно. Должна проводиться регулярная проверка всех электронных приборов на наличие вирусов.

Особую осторожность необходимо проявить при скачивании файлов из Интернета или при получении их по электронной почте. Необходимо проверять достоверность источника (сайта), с которого скачивается файл. Запрещается открывать или запускать файлы, полученные из неизвестного или недоверенного источника (например, с незнакомого адреса e-mail).

4. Доступ в Интернет (в том числе, в жилом помещении) должен быть организован через сетевой экран, установленный либо непосредственно на электронном приборе либо на маршрутизаторе, обеспечивающем выход в Интернет всем электронным приборам в локальной сети. Для локальных wi-fi сетей рекомендуется разрешить подключение к сети только определенному перечню электронных приборов (на уровне MAC-адресов).

5. Не рекомендуется без крайней необходимости использовать общественные сети для доступа в Интернет, в том числе бесплатный или платный wi-fi доступ в общественных местах (кафе, ресторанах, гостиницах, аэропортах и т.д.). Особо опасным является использование общественных компьютеров, расположенных в компьютерных клубах и интернет-кафе. Не рекомендуется разрешать электронным приборам автоматическое подключение к общественным сетям.

5. Передача информации через Интернет (электронные коммуникации)

1. При передаче информации через Интернет адвокат должен отдавать себе отчет, что передаваемая информация при определенном стечении обстоятельств может стать доступной третьим лицам.

2. Рекомендуется передавать электронную информацию по электронной почте в зашифрованном виде, для чего использовать специальное программное обеспечение. Пароль для дешифрования информации никогда не должен передаваться в том же письме.

3. При использовании электронной почты крайне осторожно стоит относиться к системам автоматических подсказок при выборе адресата для того, чтобы исключить отправку сообщения на чужой адрес. Также необходимо с осторожностью использовать поля адресов копии и скрытой копии в сообщениях электронной почты.

4. При использовании электронной почты на планшете или смартфоне необходимо защитить его паролем, также рекомендуется использовать шифрование всего содержимого планшета или смартфона, если это возможно.

5. Рекомендуется отключить на экранах планшетов и смартфонов сообщения, всплывающие автоматически при их получении (уведомления SMS, сообщения WhatsApp, Viber, Facebook Messenger и др.).

6. Облачные и иные публичные Интернет-сервисы

1. При использовании учетных записей публичных сервисов Яндекс, Google и других рекомендуется включить двухфакторную авторизацию (дополнительное подтверждение пароля по SMS).

Не допускается использование одинаковых паролей для доступа к различным публичным Интернет-сервисам.

2. Крайне нежелательно использовать облачные сервисы для хранения и передачи файлов, такие как Яндекс.Диск, Google Drive, Dropbox и др. ввиду того, что неизвестно, доступны ли файлы, хранящиеся в них, третьим лицам, удаляются ли файлы фактически при их удалении в сервисе и т.д.

Использование таких сервисов допускается только если файлы зашифрованы с использованием специального программного обеспечения для того, чтобы полностью исключить возможность несанкционированного доступа к информации, составляющей предмет адвокатской тайны.

7. Резервное копирование электронной информации.

1. Необходимо организовать регулярное резервное копирование электронной информации для того, чтобы обеспечить незамедлительное восстановление информации, модифицированной или уничтоженной вследствие технического сбоя или несанкционированного доступа к ней третьих лиц.

Резервные копии информации не должны храниться на носителе, доступ к которому (как логический, так и физический) имеют лица, которые не должны иметь доступ к данной информации. Рекомендуется использовать шифрование резервных копий с использованием специального программного обеспечения.

2. Рекомендуется иметь дополнительные резервные копии на носителях вне помещений адвокатского образования и иных помещений, используемых адвокатом для осуществления адвокатской деятельности или в облачных сервисах.

При этом резервные копии должны быть зашифрованы с использованием специального программного обеспечения для того, чтобы полностью исключить возможность несанкционированного доступа к информации, составляющей предмет адвокатской тайны.

8. Архивирование, возвращение и уничтожение информации и носителей

1. После завершения выполнения условий соглашения с доверителем физические документы необходимо поместить в архив, место расположения которого и порядок хранения документов в котором также определяются с учетом требований раздела 2. Электронная информация должна быть помещена в электронный архив с учетом требований раздела 3.

Оригиналы физических документов, переданных доверителем, должны быть ему возвращены, факт передачи должен быть зафиксирован письменно.

Адвокатское производство следует хранить не менее трех лет с момента выполнения условий соглашения.

2. Документы и информация, в хранении которых нет необходимости, должны уничтожаться. Физические документы (за исключением оригиналов документов, переданных доверителем) должны уничтожаться в специальном устройстве.

Электронная информация должна удаляться, в том числе и из «корзины». Настоятельно рекомендуется использование специального программного обеспечения для надежного удаления файлов, исключающего возможность их восстановления.

3. Крайне не рекомендуется отдавать (или продавать) кому-либо цифровые носители, использовавшиеся для осуществления адвокатской деятельности, так как даже удаленная информация потенциально может быть восстановлена. Перед утилизацией такие цифровые носители следует уничтожать или повреждать физически, чтобы исключить восстановление содержавшейся на них информации.

9. Взаимодействие с другими адвокатами и персоналом

1. При совещании с другими адвокатами относительно ведения дела запрещается сообщать информацию, составляющую предмет адвокатской тайны, без письменного согласия доверителя.

2. Все сотрудники адвокатского образования при принятии их на работу должны быть предупреждены о недопустимости разглашения адвокатской тайны и до них должно быть доведено содержание настоящих рекомендаций.

3. Все сотрудники адвокатского образования должны быть проинформированы о том, что истребование от них, так же как и от адвоката, информации, связанной с оказанием юридической помощи, не допускается.

4. Сотрудники адвокатского образования должны сразу же сообщить руководителю адвокатского образования о ставших им известным случаях нарушения информационной безопасности, в том числе краже или утере физических документов, электронных приборов и цифровых носителей, попытках несанкционированного доступа к информации и т.д.

5. Особое внимание необходимо уделить защите информации, доступной системному администратору и бухгалтеру.

6. При увольнении сотрудника адвокатского образования, необходимо сразу же принять технические меры по запрещению ему доступа к локальной сети адвокатского образования,

электронной почте и иной информации, ставшей ему доступной вследствие выполнения своих обязанностей.

Контакты авторов:

Петр Гусятников, p.gusyatnikov@gmail.com, +7 (903) 798-34-05
Полина Гусятникова, p.gusyatnikova@gmail.com, +7 (926) 592-69-76