# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕЯТЕЛЬНОСТИ АДВОКАТА: ОСНОВНЫЕ ПОНЯТИЯ

***Гусятников Петр Петрович, кандидат физико-математических наук, магистрант юридического факультета.***

***Место учебы: Негосударственное образовательное учреждение организация высшего образования «Российская академия адвокатуры и нотариата»***

***p.gusyatnikov@gmail.com***
***+7 (903) 798-34-05***

***Гусятникова Полина Петровна, магистрант юридического факультета.***

***Место учебы: Негосударственное образовательное учреждение организация высшего образования «Российская академия адвокатуры и нотариата»***

***p.gusyatnikova@gmail.com***
***+7 (926) 592-69-76***

*Аннотация: В настоящей статье дается единый целостный понятийный аппарат для проведения дальнейших научных исследований в сфере информационной безопасности деятельности адвоката и изучения основных угроз информационной безопасности применительно к оказанию адвокатом квалифицированной юридической помощи доверителю.*

***Ключевые слова: адвокат, адвокатская деятельность, информация, безопасность информации, информационная безопасность деятельности адвоката, угрозы информационной безопасности деятельности адвоката, политика информационной безопасности адвоката.***

# INFORMATION SECURITY OF ADVOCATE'S ACTIVITY: THE MAIN NOTIONS

***Gusyatnikov Petr, candidate of physico-mathematical sciences, masters degree student***

***Study place: Russian Academy of Advocacy and Notary***

***p.gusyatnikov@gmail.com***
***+7 (903) 798-34-05***

***Gusyatnikova Polina, masters degree student***

***Study place: Russian Academy of Advocacy and Notary***

***p.gusyatnikova@gmail.com***
***+7 (926) 592-69-76***

*Abstract: A unified consistent set of notions is given in this paper for further scientific research in the field of advocate's information security and examination of the main threats of information security applicable to rendering qualified legal assistance to the principal.*

***Keywords: advocate, advocate's activity, information, information security, information security of advocate's activity, threats of information security of advocate's activity, advocate's information security policy.***

Адвокатская деятельность — это квалифицированная юридическая помощь, оказываемая на профессиональной основе доверителям в целях

защиты их прав, свобод и интересов. При этом взаимодействие с информацией, т.е. ее хранение, обработка, получение и передача — неотъемлемая часть профессиональной деятельности адвоката и занимает значительную долю его рабочего времени.

Легко видеть, что все основные полномочия адвоката, перечисленные в статье 6 Федерального закона «Об адвокатской деятельности и адвокатуре в Российской Федерации»[1] (далее — Закон об адвокатуре) тесно связаны с работой адвоката с информацией.

Адвокат получает или истребует информацию когда собирает сведения, необходимые для оказания юридической помощи, когда опрашивает с их согласия лиц, предположительно владеющих информацией, относящейся к делу, когда привлекает специалистов для разъяснения вопросов, связанных с оказанием юридической помощи. Адвокат передает информацию или обменивается ей, когда встречается со своим доверителем наедине, в условиях, обеспечивающих конфиденциальность, когда собирает и представляет предметы и документы, которые могут быть признаны вещественными и иными доказательствами и т.д.

Взаимодействие адвоката с информацией и основные его права в этой сфере закреплены и в процессуальном законодательстве. Например, в соответствии с положениями статьи 53 УПК РФ, защитник вправе собирать и представлять доказательства, необходимые для оказания юридической помощи, участвовать в допросе подозреваемого, обвиняемого, а также в иных следственных действиях, знакомиться с протоколом задержания, постановлением о применении меры пресечения, протоколами следственных действий, произведенных с участием подозреваемого, обвиняемого, по

[1] Федеральный закон от 31.05.2002 N 63-ФЗ (ред. от 13.07.2015) «Об адвокатской деятельности и адвокатуре в Российской Федерации»

окончании предварительного расследования знакомиться со всеми материалами уголовного дела и т.д.[2]

Во всех перечисленных случаях деятельность адвоката так или иначе связана с оперированием информацией, существенная доля которой является конфиденциальной и составляет предмет адвокатской тайны, поэтому можно сделать вывод, что профессиональная деятельность адвоката невозможна без обеспечения ее информационной безопасности.

Как явление, информационная безопасность деятельности адвоката появилось одновременно с появлением адвокатуры. Ей уделяется большое внимание со стороны адвокатского сообщества, как в России, так и за рубежом.

Федеральной палатой адвокатов РФ разработаны и утверждены Рекомендации по обеспечению адвокатской тайны и гарантий независимости адвоката при осуществлении адвокатами профессиональной деятельности[3], которые содержат довольно много положений, связанных с не только с обеспечением адвокатской тайны, но и с обеспечением информационной безопасности деятельности адвоката.

В зарубежной адвокатуре этому вопросу также уделяется серьезное внимание: например, в Великобритании палатой барристеров Линкольнс-Инн разработаны детальные рекомендации по обеспечению информационной безопасности, которые касаются всех ее практикующих членов[4].

Вместе с тем, теоретические аспекты информационной безопасности в юридической деятельности в целом, и применительно к адвокатуре в частности, на данный момент, проработаны довольно слабо. Также востребована разработка современных подходов к обеспечению адвокатской тайны и информационной безопасности деятельности адвоката с учетом повсеместного

---

[2] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ

[3] Рекомендации по обеспечению адвокатской тайны и гарантий независимости адвоката при осуществлении адвокатами профессиональной деятельности ы// ФПА РФ, 30.11.2009, Протокол №3

[4] UK Bar Council Guidelines on Information Security, January 2016 http://www.barcouncil.org.uk/media/414748/information_security.pdf

использования информационных технологий, хранения, получения и передачи адвокатами и доверителями сведений и документов в электронном виде.

К сожалению, общепринятая научная терминология в области информационной безопасности деятельности адвоката пока отсутствует. Поэтому для целей настоящей статьи необходимо для начала дать определения основных используемых понятий и терминов.

Часть дефиниций уже присутствует в различных отдельных источниках, но авторы в настоящей статье ставят перед собой задачу сформировать единый целостный понятийный аппарат для дальнейших исследований информационной безопасности применительно именно к оказанию адвокатом квалифицированной юридической помощи доверителю[5].

В статье 2 Федерального закона «Об информации, информационных технологиях и о защите информации»[6] (далее — Закон об информации) содержатся несколько базовых определений, раскрывающих само понятие информации, а также основные понятия, связанные с ним.

Центральным определением, несомненно, является само определение информации: *информация* — сведения (сообщения, данные) независимо от формы их представления.

Также в Законе об информации даются такие достаточно важные определения как «электронный документ» и «электронное сообщение».

*Электронный документ* — это документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах. В большинстве случаев электронный

[5] Романова В.Е., Понятие оказания квалифицированной юридической помощи адвокатом // Бизнес в законе, 2014, №2, С. 216-221.

[6] Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»

документ представляет собой компьютерный файл формата одной из основных используемых компьютерных программ (Microsoft Word, Adobe PDF и т.д.).

*Электронное сообщение* — информация, переданная или полученная пользователем информационно-телекоммуникационной сети. Электронные сообщения по своей сути являются электронными документами, передаваемыми или получаемыми при помощи информационно-телекоммуникационной сети (например, сообщение электронной почты, SMS-сообщение, сообщение Viber или WhatsApp и др).

В дальнейшем мы предлагаем ввести такое авторское определение как *электронная информация* или *информация, представленная в электронном виде*, которого нет в Законе об информации, понимая под этим произвольную совокупность электронных документов.

Стоит отметить, что в статье 272 УК РФ содержится определение сходного понятия «компьютерная информация». Под *компьютерной информацией* понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи[7].

На наш взгляд, речь идет об очень похожем понятии и, возможно, стоит предпринять меры по унификации законодательства и ввести единый термин «электронная информация», так как Закон об информации оперирует терминами «электронный документ» и «электронное сообщение», но не «компьютерный документ» или «компьютерное сообщение». В дальнейших исследованиях мы будем использовать именно авторский термин «электронная информация».

Также интересным, но не относящимся к предмету данной статьи является вопрос о том, можно ли отнести компьютерную информацию к одному из видов доказательств, указанных в части 2 статьи 74 УПК РФ,

[7] «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ

например, к «иные документы», т.е. является ли компьютерная информация документом, или же необходимо выделение ее в качестве отдельного вида доказательств[8].

Говоря об информационно-телекоммуникационной сети, определение которой также дается в статье 2 Закона об информации (*информационно-телекоммуникационная сеть* — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники), мы, в первую очередь, имеем в виду всемирную глобальную сеть Интернет, так как основной объем обмена информацией в настоящее время в мире приходится именно на нее.

Закон об информации также содержит такие определения, как *доступ к информации* (возможность получения информации и ее использования), *обладатель информации*, *конфиденциальность информации* и др.

Статья 16 Закона об информации посвящена непосредственно защите информации. При этом, к сожалению, в ней не дается легальная дефиниция такого важного понятия как безопасность информации.

Если обратиться к чисто техническим определениям, то *безопасность информации* (англ. information security) — состояние защищённости информации (данных), при котором обеспечиваются её (их) конфиденциальность, целостность и доступность[9].

Понятие информационной безопасности применительно к правой сфере уже формулировалось авторами ранее[10]. Под *информационной безопасностью гражданина* мы будем понимать состояние защищенности его прав и законных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

---

[8] Зазулин А.И., Компьютерная информация в уголовном процессе: сущность и способы закрепления в качестве доказательства по уголовному делу // Бизнес в законе, 2015, №4, С. 130-133.

[9] Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).

[10] Гусятников П.П., Гусятникова П.П. — Информационная безопасность адвоката. Материалы 11-й международной научно-практической конференции, «Achievement of high school», София, 2015. Том 5. Закон.

Под *информационной безопасностью деятельности адвоката* в широком смысле мы будем понимать состояние защищенности его прав и законных интересов при осуществлении им профессиональной деятельности, а также прав и законных интересов его доверителей, гарантированных Законом об адвокатура в информационной сфере.

Под *информационной безопасностью деятельности адвоката* в более узком смысле мы будем понимать конфиденциальность, целостность и доступность, то есть именно безопасность информации, которой владеет адвокат. Иными словами, это безопасность личной информации адвоката и информации, составляющей предмет адвокатской тайны в силу статьи 8 Закона об адвокатуре.

Безопасность личной информации адвоката и возможные негативные последствия для доверителя, в том числе, правовые, связанные с ее утратой или разглашением является отдельной достаточно интересной темой для научных исследований. Однако авторы полагают, что на текущий момент гораздо более важным является в первую очередь исследование безопасности информации, составляющей предмет адвокатской тайны.

Поэтому, если не оговорено иное, в дальнейшем под *информационной безопасностью деятельности адвоката* мы будем понимать безопасность только той информации, которая составляет предмет адвокатской тайны в силу статьи 8 Закона об адвокатуре.

Таким образом, для обеспечения информационной безопасности деятельности адвоката, то есть для обеспечения состояния защищенности информации, все имеющиеся у адвоката сведения, составляющие предмет адвокатской тайны, а также методы их хранения, обработки, получения, передачи и доступа к ним должны отвечать трем основным требованиям,

составляющим содержание информационной безопасности: требованиям конфиденциальности, целостности и доступности[11].

Под *конфиденциальностью информации* мы будем понимать обеспечение доступа к информации только субъектам, имеющим на это право (авторизованным пользователям).

Под *целостностью информации* понимается состояние, при котором ее изменение осуществляется только преднамеренно и только субъектами (авторизованными пользователями), имеющими на это право.

Под *доступностью информации* — состояние, при котором субъекты, имеющие право доступа к информации, могут реализовать его беспрепятственно, то есть беспрепятственное обеспечение доступа к информации авторизованных пользователей[12].

Обязательно стоит отметить, что состояния целостности и доступности информации тесно связаны с состоянием *носителя информации*, на котором она содержится. Далее мы будем рассматривать, в первую очередь, носители электронной информации (информации, представленной в электронном виде).

В качестве носителя информации может выступать как физически доступный материальный носитель — жесткий диск компьютера, компакт-диск, флеш-накопитель, так и виртуально доступный носитель — электронная почта адвоката, в которой хранятся файлы (почта Mail.ru, Яндекс и др.), облачные сервисы для хранения файлов (Яндекс Диск, Dropbox и т.д.), файловый сервер адвокатского образования и др.

В случае утраты доступа к носителю информации или его физического повреждения, утрачивается и доступ к информации. Если утрата доступа к носителю имеет временный характер (утеря пароля к электронной почте), то и доступ к информации утрачивается лишь на время. В случае полной утраты

---

[11] ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

[12] Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).

доступа к носителю (физическое повреждение жесткого диска), полностью утрачивается и вся информация, содержащаяся на нем.

*Угроза информационной безопасности деятельности адвоката* — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или) целостности информации, составляющей предмет адвокатской тайны.

Соответственно, в зависимости от *аспекта информационной безопасности*, на который направлена угроза, стоит выделить следующие три основных вида угроз информационной безопасности деятельности адвоката:

1) *угрозы нарушения конфиденциальности информации*, т.е. угрозы несанкционированного доступа третьих лиц к информации, содержащей адвокатскую тайну и последующего использования третьими лицами информации, содержащей адвокатскую тайну;
2) *угрозы нарушения целостности информации*, т.е. угрозы несанкционированной модификации или повреждения (уничтожения) информации, содержащей адвокатскую тайну, или носителя, на котором она содержится;
3) *угрозы нарушения доступности информации*, т.е. угрозы невозможности доступа авторизованных пользователей к информации или к носителю, на котором она содержится.

Угрозы информационной безопасности деятельности адвоката неразрывно связаны с их источниками, а также с их возможными негативными последствиями их реализации. Под *источником угрозы информационной безопасности адвоката* понимается субъект, материальный объект или физическое явление, являющиеся причиной возникновения угрозы его информационной безопасности.

Главным негативным последствием реализации угрозы информационной безопасности адвоката является нарушение адвокатской тайны, т.е. получение,

разглашение, распространение или использование третьими лицами информации, составляющей предмет адвокатской тайны. Прочие второстепенные последствия, которые повлекло за собой указанное нарушение, являются дополнительными. При этом в отношении адвоката может быть возбуждено дисциплинарное производство[13].

Угрозы информационной безопасности деятельности адвоката могут быть классифицированы и по другим признакам[14].

По признаку наличия умысла в действиях угрозы информационной безопасности можно разделить на:

- *случайные* (например, технические сбои в работе информационных систем вследствие стихийных бедствий);
- *неумышленные* (например, отправка электронного письма на ошибочный адрес электронной почты, не принадлежащий доверителю или утеря документов по делу вследствие их небрежного хранения);
- *умышленные* (например, корпоративный шпионаж, подслушивание, визуальное наблюдение, хищение документов и носителей информации, подкуп и шантаж лиц, имеющих доступ к информации).

По расположению источника угрозы:

- *внутренние* (источник угрозы располагается внутри защищаемой информационной системы, например, сотрудник адвокатского образования);
- *внешние* (источник угрозы находится вне защищаемой системы, например, взлом сервера адвокатского образования или хищение

[13] Раудин В.В., Изменение процедурных основ дисциплинарного производства в отношении адвокатов. // Пробелы в российском законодательстве, 2014, №3, С. 217-220.
[14] Гатчин Ю. А., Сухостат В. В. Теория информационной безопасности и методология защиты информации. — СПб.: СПбГУ ИТМО, 2010

производственных отходов: распечаток, записей, списанных носителей информации).

По размеру наносимого ущерба:

- *общие* (нанесение ущерба объекту информационной безопасности в целом, причинение значительного ущерба, например, утрата значимых доказательств, определяющих исход дела);
- *локальные* (причинение вреда отдельным частям объекта информационной безопасности, например, утрата доступа адвоката к электронной почте);
- *частные* (причинение вреда отдельным элементам, например, утрата документа, копию которого можно восстановить).

По степени воздействия на защищаемую информацию:

- *пассивные* (структура и содержание информации не изменяются, например, угроза копирования файлов, содержание которых составляет адвокатскую тайну);
- *активные* (структура и содержание системы подвергается изменениям, например, целенаправленный взлом электронной почты адвоката и удаление всех сообщений).

Можно классифицировать угрозы информационной безопасности деятельности адвоката и по прочим признакам, таким как, например, природа возникновения угрозы (естественные, техногенные и искусственные) или по способу доступа к защищаемой информации (использование стандартного или нестандартного доступа к информации).

*Инцидент информационной безопасности* — это реализованная в действительности угроза информационной безопасности, то есть совокупность фактов, указывающих на нарушение информационной безопасности.

Для обеспечения информационной безопасности адвоката, то есть для обеспечения состояния защищенности информации (сведений), которой

владеет адвокат, необходимо не только классифицировать возможные угрозы информационной безопасности.

Необходимо выстроить *политику информационной безопасности адвоката*, то есть совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности информации, которыми руководствуется адвокат в своей деятельности[15].

Крайне важно привлечь к проблеме теоретического исследования и практического обеспечения информационной безопасности деятельности адвоката внимание адвокатского сообщества, Федеральную палату адвокатов Российской Федерации, адвокатские палаты субъектов Российской Федерации.

Видится разумным разработать единые рекомендации по формированию политики информационной безопасности для адвокатов и адвокатских образований и утвердить их на уровне Совета ФПА РФ, например, в виде приложения к Рекомендациям по обеспечению адвокатской тайны и гарантий независимости адвоката при осуществлении адвокатами профессиональной деятельности[16]. В последующих работах авторы планируют подготовить для этого теоретическую базу и научно обоснованные предложения.

В заключение стоит сказать несколько слов о концепции «Адвокат 2.0», разрабатываемой авторами. Под концепцией «Адвокат 2.0» мы понимаем такую систему организации работы адвоката с информацией, при которой хранение, обработка, получение и передача информации адвокатом происходит *только в электронном виде*, отвечая при этом всем необходимым требованиям информационной безопасности, сформулированным в настоящей статье.

*Список литературы:*

[15] Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).

[16] Рекомендации по обеспечению адвокатской тайны и гарантий независимости адвоката при осуществлении адвокатами профессиональной деятельности ы// ФПА РФ, 30.11.2009, Протокол №3

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ

2. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ

3. Федеральный закон от 31.05.2002 N 63-ФЗ (ред. от 13.07.2015) «Об адвокатской деятельности и адвокатуре в Российской Федерации»

4. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»

5. Рекомендации по обеспечению адвокатской тайны и гарантий независимости адвоката при осуществлении адвокатами профессиональной деятельности ы// ФПА РФ, 30.11.2009, Протокол №3

6. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

7. Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).

8. Гатчин Ю. А., Сухостат В. В. Теория информационной безопасности и методология защиты информации. — СПб.: СПбГУ ИТМО, 2010

9. Гусятников П.П., Гусятникова П.П. — Информационная безопасность адвоката. Материалы 11-й международной научно-практической конференции, «Achievement of high school», София, 2015. Том 5. Закон.

10. Зазулин А.И., Компьютерная информация в уголовном процессе: сущность и способы закрепления в качестве доказательства по уголовному делу // Бизнес в законе, 2015, №4, С. 130-133.

11. Раудин В.В., Изменение процедурных основ дисциплинарного производства в отношении адвокатов // Пробелы в российском законодательстве, 2014, №3, С. 217-220.

12. Романова В.Е., Понятие оказания квалифицированной юридической помощи адвокатом // Бизнес в законе, 2014, №2, С. 216-221.

13. UK Bar Council Guidelines on Information Security, January 2016 http://www.barcouncil.org.uk/media/414748/information_security.pdf