В. А. Канашевский*

БАНКОВСКАЯ ТАЙНА И ИСПОЛЬЗОВАНИЕ БАНКАМИ УСЛУГ АУТСОРСИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *Автор исследует юридические аспекты сохранения режима банковской тайны при предоставлении услуг аутсорсинга информационной безопасности. В статье делается вывод, что сведения, относящиеся к банковской тайне, могут быть переданы третьему лицу, в том числе лицу, оказывающему услуги аутсорсинга информационной безопасности, при условии, что кредитная организация сохраняет контроль за соответствующей инфраструктурой поставщика, и у провайдера аутсорсинговых услуг отсутствует возможность доступа к соответствующим сведениям.*

Автором проанализированы нормы российских законов о банковской и коммерческой тайне — о банках и банковской деятельности, о национальной платежной системе, о коммерческой тайне и др., а также положения Стандарта Банка России СТО БР ИББС-1.4-2018, посвященного вопросам управления риском нарушения информационной безопасности при аутсорсинге. В процессе исследования установлено, что Стандарт СТО БР ИББС-1.4-2018 де-факто позволяет передавать на аутсорсинг поставщикам услуг (т.е. третьим лицам) информацию, относящуюся к банковской тайне, что противоречит действующему законодательству. Для устранения противоречий в российские законы необходимо внести соответствующие изменения.

Ключевые слова: *банковская тайна, коммерческая тайна, конфиденциальная информация, аутсорсинг, информационная безопасность, провайдер услуг, локализация, персональные данные, база данных, кредитная организация, финансовая организация, платежная система.*

DOI: 10.17803/1729-5920.2018.140.7.092-097

В настоящее время многие кредитные организации в России стремятся сократить расходы на обеспечение своей информационной безопасности (далее — ИБ), в том числе за счет обращения к сторонним организациям, оказывающим услуги аутсорсинга. Под аутсорсингом понимается передача банком поставщику услуг выполнения бизнес-функций банка. При этом допускается передача на аутсорсинг существенных функций в части ИБ, т.е. таких, при выполнении которых осуществляется обработка информации, защищаемой в соответствии с требованиями законодательства РФ[1]. При этом к «защищаемой информа-

[1] См.: Стандарт Банка России «СТО БР ИББС-1.4-2018. Обеспечение информационной безопасности организаций банковской системы РФ. Управление риском нарушения информационной безопасности при аутсорсинге. Разд. 3 «Термины и определения» (принят приказом Банка России от 06.03.2018 № ОД-568; вводится в действие с 01.07.2018) // СПС «КонсультантПлюс».

Канашевский Владимир Александрович, доктор юридических наук, профессор, профессор кафедры международного частного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
vakanashevsky@msal.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

ции» относится информация ограниченного доступа, в том числе персональные данные, информация, составляющая банковскую и коммерческую тайну, инсайдерская и другая информация[2].

Использование услуг аутсорсинга существенных функции в части ИБ (далее также — аутсорсинг ИБ) позволяет кредитным организациям существенно экономить на соответствующем программном обеспечении, инфраструктуре, а также специалистах, ответственных за соответствующую работу. Однако при аутсорсинге ИБ ставится на повестку дня вопрос о защите конфиденциальной информации, в том числе вопрос об обеспечении режима коммерческой и банковской тайны[3].

Примерный список защищаемой информации (конфиденциальной информации), приводится, в частности, в рекомендациях Банка России и включает финансовую информацию, информацию о технической и информационной безопасности, внутренние корпоративные документы, банковскую тайну, персональные данные, информацию о кредитной истории, налоговую информацию, тайну страхования и тайну ломбарда, а также иную информацию, признанную финансовой организацией в качестве конфиденциальной[4]. По общему правилу передача третьим лицам (в том числе провайдерам аутсорсинговых услуг) конфиденциальной информации допускается при условии соблюдения ряда требований и ограничений, предусмотренных действующим законодательством и внутренними актами владельцев конфиденциальной информации. Следует также учитывать и требования законодательства РФ о локализации персональных данных и локализации электронных баз данных банков[5].

При передаче кредитной организацией на аутсорсинг существенных функций в части ИБ особое значение приобретает вопрос о соблюдении требований законодательства РФ о защите банковской тайны. Согласно ст. 857 ГК РФ[6] и ст. 26 ФЗ «О банках и банковской деятельности» 1990 г. (в ред. от 31.12.2017)[7] банковская тайна включает в себя следующие категории сведений:

1) сведения о счетах и вкладах клиентов и корреспондентов;
2) информация об операциях по счетам и вкладам клиентов;
3) сведения о самих клиентах;
4) иные сведения, устанавливаемые кредитной организацией.

При этом сведения, составляющие банковскую тайну, могут быть предоставлены:

1) самим клиентам или их представителям;
2) в бюро кредитных историй;
3) государственным органам по их запросам;
4) головным кредитным организациям и банковским холдингам, расположенным на территориях иностранных государств.

Отметим, что обязанность гарантировать банковскую тайну возложена также на операторов по переводу денежных средств, операторов платежных систем, операторов услуг платежной инфраструктуры и банковских платежных агентов (субагентов) (ст. 26 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе», в ред. от 18.07.2017[8]). Кроме того, согласно п. 12 ст. 16 Закона «О национальной платежной системе» начиная с 1 июля 2016 г. банки и другие финансовые организации не вправе передавать на территорию иностранного государства информацию по любому внутреннему переводу денежных средств (а эта информация также относится к банковской тайне).

---

2 См.: СТО БР ИББС-1.4-2018. Разд. «Введение».

3 См.: *Хорват О., Севастьянова Ю.* Аутсорсинг и аутстаффинг в банке — экономический эффект или социальные и налоговые риски? // СПС «КонсультантПлюс».

4 Примерный состав категорий информации, рекомендуемых для включения в класс «информация конфиденциального характера», содержится, в частности, в Приложении А (справочное) к Рекомендациям Банка России в области стандартизации РС БР ИББС-2.9-2016 «Обеспечение информационной безопасности организаций банковской системы РФ. Предотвращение утечек информации» // СПС «КонсультантПлюс».

5 См.: *Канашевский В. А.* Об обязательном хранении информации на территории России (требование локализации) // Международное публичное и частное право. 2017. № 6.

6 СЗ РФ. 1996. № 5. Ст. 410.

7 СЗ РФ. 1996. № 6. Ст. 492.

8 СЗ РФ. 2011. № 27. Ст. 3872.

Законодательство предусматривает административную[9], уголовную[10] и гражданско-правовую ответственность за разглашение банковской тайны. Так, согласно ст. 857 ГК РФ за разглашение банком сведений, составляющих банковскую тайну, клиент вправе потребовать от банка возмещения причиненных убытков.

Отметим, что под термином «банковская тайна» (ст. 857 ГК РФ, ст. 26 Закона «О банках и банковской деятельности», ст. 26 Закона «О национальной платежной системе») по аналогии с Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (в ред. от 12.03.2014)[11] следует понимать не сами сведения (информацию), но определенный режим конфиденциальности информации, который должен быть установлен финансовой организацией. В частности, согласно ст. 10 Закона «О коммерческой тайне» обладатель конфиденциальной информации должен предпринять следующие меры по обеспечению конфиденциальности сведений: определить перечень конфиденциальной информации; установить порядок обращения с этой информацией (принять внутреннее положение о защите такой информации); определить лиц, допущенных к информации, и закрепить соответствующие обязательства в трудовых договорах и договорах с контрагентами; маркировать материальные носители (документы) грифом «коммерческая тайна». Сложность указанных процедур приводит к их несоблюдению на практике, в результате чего соответствующая информация не приобретает статус «информации, составляющей коммерческую тайну» и не получает предусмотренных российским законодательством гарантий защиты (например, не позволяет взыскать убытки с контрагента по договору за разглашение такой информации)[12]. Сложности также заключаются в процедуре доказывания как самого факта распространения конфиденциальной информации конкретным лицом (лицами), так и размера причиненных таким распространением убытков. Этими очевидными обстоятельствами объясняется практически полное отсутствие в российской судебной практике решений о присуждении убытков по данной категории дел.

Отдельно стоит высказаться по вопросу о соотношении банковской тайны и коммерческой тайны. В соответствии с Федеральным законом «О коммерческой тайне» к информации, составляющей коммерческую тайну, относятся сведения, которые имеют действительную или потенциальную коммерческую ценность в силу их неизвестности третьим лицам, в отношении которых обладателем введен режим коммерческой тайны, а именно — сведения о результатах интеллектуальной деятельности в научно-технической сфере, сведения о способах осуществления профессиональной деятельности, иные сведения (ст. 3). Таким образом, сведения, относящиеся к коммерческой тайне, шире, чем те, которые составляют банковскую тайну. Кроме того, как верно отмечается в литературе, «банковская тайна возникает в силу закона вне зависимости от волеизъявления субъектов отношений по поводу ее охраны. Напротив, информация приобретает статус коммерческой тайны после одностороннего объявления ее коммерческой тайной. В отношении банковской тайны закон устанавливает ее содержание, субъектов, порядок предоставления. В то же время… объем информации, относящейся к коммерческой тайне, устанавливается организацией самостоятельно, так же, как и круг лиц, обладающих доступом к охраняемым сведениям». И далее: «Для лица, осуществляющего охрану (коммерческой. — *В. К.*) тайны, существует позитивный экономический стимул. Для банка осуществление охраны банковской тайны имеет лишь негативный стимул в виде ответственности за ее разглашение»[13].

---

[9] Разглашение информации, доступ к которой ограничен федеральным законом, наказывается штрафом — на граждан до 1 тыс. руб.; на должностных лиц — до 5 тыс. руб. (ст. 13.14 КоАП РФ).

[10] Незаконное разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, наказывается штрафом в размере до 1 млн руб., либо исправительными работами на срок до 2 лет, либо лишением свободы до 3 лет (п. 3 ст. 183 УК РФ).

[11] СЗ РФ. 2004. № 32. Ст. 3283.

[12] См., например: постановление Седьмого арбитражного апелляционного суда от 25.04.2012 № 07АП-2839/12 по делу № А27-12862/2011 // СПС «КонсультантПлюс».

[13] *Селивановский А. С.* Банковская тайна: состояние и проблемы // URL: http://www.selivanovsky.ru/pages/bankovskaya_tajna/.

Относительно возможности передачи сведений, относящихся к банковской тайне, на аутсорсинг существуют два противоположных мнения. Согласно распространенной точке зрения такие сведения не могут быть переданы третьему лицу (в том числе лицу, оказывающему услуги аутсорсинга ИБ), поскольку формально нарушаются требования ст. 857 ГК РФ. Однако существует другая, более обоснованная позиция: сведения, относящиеся к банковской тайне, могут быть переданы на аутсорсинг, если: 1) кредитная организация сохраняет контроль за соответствующей инфраструктурой поставщика[14] и 2) у провайдера аутсорсинговых услуг отсутствует возможность доступа к соответствующим сведениям. Таким образом, в результате такой передачи «разглашения» банковской тайны «третьему лицу» не происходит.

Подтверждением последней точки зрения являются следующие аргументы:

1) согласно Стандарту СТО БР ИББС-1.4-2018 передача на аутсорсинг существенных функций ИБ не рассматривается как раскрытие банковской тайны третьим лицам;
2) существующая практика передачи банками на аутсорсинг АБС[15], которые обрабатывают информацию, составляющую банковскую тайну, в сочетании с отсутствием фактов привлечения банков и (или) их сотрудников к ответственности по ст. 183 УК РФ и ст. 857 ГК РФ (возмещение убытков) за разглашение банковской тайны при ее передаче провайдерам аутсорсинговых услуг (т.е. третьим лицам).

Более того, согласно Стандарту СТО БР ИББС-1.4-2018 допускается передача на аутсорсинг функций, связанных с хранением и обработкой информации, в том числе на внешних центрах обработки данных и облачных сервисах (облачных служб). Указанный Стандарт прямо допускает возможность аутсорсинга бизнес-функций, при выполнении которых осуществляется обработка защищаемой информации[16] (в том числе сведений, относящихся к банковской тайне).

Таким образом, Стандарт Банка России СТО БР ИББС-1.4-2018 де-факто позволяет передавать на аутсорсинг поставщикам услуг (т.е. третьим лицам) информацию, относящуюся к банковской тайне. При этом в самом стандарте указывается, что при аутсорсинге возникает риск бесконтрольного несанкционированного доступа к защищаемой информации лиц, не являющихся работниками банка, а также риск несоблюдения требований законодательства РФ в части обеспечения режима защиты банковской тайны[17]. Подчеркнем, что практика передачи банками на аутсорсинг сведений, относящихся к банковской тайне, противоречит действующему законодательству (ст. 857 ГК РФ и ст. 26 Закона «О банках и банковской деятельности», ст. 26 Закона «О национальной платежной системе»). Указанный Стандарт выходит за пределы зоны компетенции Банка России, определенной законодательством России. Для устранения противоречий в соответствующие российские законы необходимо внести изменения, позволяющие финансовым организациям передавать на аутсорсинг в том числе сведения, относящиеся к банковской тайне.

Более того, как указывается в литературе, конструкция самой ст. 26 Закона «О банках и банковской деятельности» допускает указание на недопустимость разглашения сведений и ответственность лиц, которые напрямую не поименованы в качестве субъектов банковской тайны, — аудиторских и иных организаций, операторов платежных систем, операционных центров, платежных клиринговых центров, что косвенно указывает на право таких лиц на доступ к соответствующей информации, порядок доступа к которой не определен[18].

---

[14] Правда, при этом такая передача не охватывается понятием «аутсорсинг ИБ» согласно Стандарту СТО БР ИББС-1.4-2018. Указанный Стандарт под аутсорсингом ИБ понимает «передачу полностью выполнения бизнес-функций поставщику услуг, без участия в реализации указанных бизнес-функций работников организации банковского сектора» (разд. 3 «Термины и определения»).

[15] АБС — автоматизированная банковская система. О практике передачи на полный или частичный аутсорсинг АБС см., например: Аутсорсинг инфраструктуры банковских систем и информационная безопасность: опыт ЦФТ // URL: http://kbrbank.ru/autsorsing-infrastruktury-bankovskih-sistem-i/.

[16] См.: Стандарт СТО БР ИББС-1.4-2018. Введение и п. 6.2.

[17] См.: Стандарт СТО БР ИББС-1.4-2018. Введение.

[18] См.: *Гронин Д. П.* От банковской тайны к финансовой тайне // URL: http://xn----7sbbaj7auwnffhk.xn--p1ai/article/2482.

В этих условиях нелогичным выглядит положение Стандарта СТО БР ИББС-1.4-2018, предусматривающее «возможность аутсорсинга только в случае соблюдения требований законодательства РФ в области… информации, составляющей банковскую тайну…»[19]. Статья 857 ГК РФ устанавливает круг лиц, которым могут быть переданы сведения, относящиеся к банковской тайне, к каковым не относятся поставщики услуг аутсорсинга. Соответственно, согласно российским законам информация, относящаяся к банковской тайне, не может быть передана на аутсорсинг в принципе, что противоречит смыслу стандарта.

Стандарт СТО БР ИББС-1.4-2018 рекомендует финансовым организациям применять организационные меры и технические средства, реализующие контроль доступа работников поставщика услуг и иных лиц к защищаемой информации, а также информационным (автоматизированным) системам, ее обрабатывающим. Для поставщиков облачных услуг важным является следующая рекомендация: обязательное сохранение за финансовой организацией функций управления предоставлением доступа к защищаемой информации, а при технической невозможности (например, при использовании облачных вычислений по модели SaaS[20]) контроль выполнения функций по управлению предоставлением доступа к защищаемой информации поставщиком услуг[21]. Таким образом, если будут предприняты меры, делающие доступ поставщика услуг к сведениям, составляющим банковскую тайну, технически и организационно невозможным, «передача» таких сведений поставщику не происходит.

Согласно Стандарту организация банковской системы РФ должна определить критерии, в том числе основанные на законодательстве РФ о лицензировании отдельных видов деятельности, которые должны использоваться для оценки способности и потенциала поставщика услуг эффективно и качественно обеспечить ИБ при предоставлении услуги по аутсорсингу существенных функций, в том числе обеспечить защиту информации в соответствии с требованиями законодательства РФ. В случае несоответствия поставщика услуг определенным критериям ему не могут передаваться на выполнение существенные функции[22]. Представляется, что наличие лицензий у поставщика услуг в качестве предпосылки для осуществления аутсорсинга ИБ должно быть исключено из требований Стандарта с тем, чтобы позволить зарубежным поставщикам оказывать соответствующие услуги аутсорсинга российским банкам. Такой подход будет способствовать внедрению лучших зарубежных практик и повышению конкурентоспособности отечественной банковской системы. Учитывая рекомендательный характер Стандарта, мы не склонны рассматривать требование наличия лицензий у поставщиков в качестве императивного запрета для российских банков использовать аутсорсинговые услуги зарубежных провайдеров, не имеющих соответствующие лицензии.

Согласно Стандарту «трансграничная передача информации, составляющей банковскую тайну, допускается в обезличенной обобщенной (агрегированной) форме, за исключением случаев, установленных законодательством РФ»[23]. С формально юридической точки зрения это правило Стандарта противоречит законодательству России: в частности, п. 12 ст. 16 Закона «О национальной платежной системе» не допускает передачи информации по любому внутреннему переводу денежных средств на территорию иностранного государства, тогда как к банковской тайне относится в том числе информация об операциях по счетам и вкладам клиентов. Однако сто́ит приветствовать закрепление данного правила в Стандарте как разумного и практически ориентированного. Кроме того, данное положение Стандарта может рассматриваться в качестве косвенного разрешения банкам использовать услуги аутсорсинга зарубежных поставщиков.

Широкое внедрение услуг аутсорсинга ИБ в банковском секторе позволит повысить обеспечение конфиденциальности информации (в том числе сведений, относящихся к банковской тайне), поскольку оказанием соответствующих услуг смогут заниматься специализированные организации, имеющие необходимый опыт. Кроме того, данная практика позволит

[19] См.: Стандарт СТО БР ИББС-1.4-2018. П. 6.2.

[20] Одним из традиционных способов организации предоставления облачных услуг является «программное обеспечение как услуга» (SaaS, Software-as-a-Service).

[21] См.: Стандарт СТО БР ИББС-1.4-2018. П. 6.4.

[22] См.: Стандарт СТО БР ИББС-1.4-2018. П. 6.5.

[23] См.: Стандарт СТО БР ИББС-1.4-2018. П. 6.9.

банкам (особенно небольшим) существенно сэкономить на обеспечении ИБ. Несомненно, что принятие и введение в действие Стандарта СТО БР ИББС-1.4-2018 позволит упорядочить процесс оказания банкам услуг аутсорсинга ИБ. Вместе с тем для полноценной имплементации указанного Стандарта требуется внести изменения в законодательство о банковской тайне и разрешить передачу соответствующих сведений провайдерам услуг аутсорсинга ИБ.

БИБЛИОГРАФИЯ

1. *Гронин Д. П.* От банковской тайны к финансовой тайне // URL: http://xn——7sbbaj7auwnffhk.xn—p1ai/article/2482.
2. *Канашевский В. А.* Об обязательном хранении информации на территории России (требование локализации) // Международное публичное и частное право. — 2017. — № 6.
3. *Селивановский А. С.* Банковская тайна: состояние и проблемы // URL: http://www.selivanovsky.ru/pages/bankovskaya_tajna/.
4. *Хорват О.*, *Севастьянова Ю.* Аутсорсинг и аутстаффинг в банке — экономический эффект или социальные и налоговые риски? // СПС «КонсультантПлюс».

Материал поступил в редакцию 18 февраля 2018 г.

BANK SECRECY AND EMPLOYMENT OF DATA SECURITY OUTSOURCING

KANASHEVSKIY Vladimir Aleksandrovich — Doctor of Law, Professor, Professor of the Department of Private International Law of the Kutafin Moscow State Law University (MSAL)
vakanashevsky@msal.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *The author explores the legal aspects of the preservation of the bank secrecy regime in the provision of outsourcing services for data security. The article concludes that the information pertaining to banking secrecy, may be transferred to a third party, including the party that provides outsourcing services for information security, provided that the credit institution maintains control over the relevant provider's infrastructure and the provider of outsourcing services lacks possibility of access the relevant information.*
The author analyzes the norms of the Russian laws on banking and commercial secrecy, i.e. on banks and banking activities, on the national payment system, on commercial secrets, etc., and also provisions of the Standard of the Bank of Russia STO BR IBBS-1.4-2018, and focuses on managing risks to data security when outsourcing. During the research it is established that the Standard STO BR IBBS-1.4-2018 de facto allows you to outsource data relating to bank secrecy to service providers (i.e. third parties), which contradicts the current legislation. To address inconsistencies in Russian laws it is necessary to make appropriate changes.

Keywords: *bank secrecy, trade secrets, confidential information, outsourcing, IT security, service provider, location, personal data, database, credit institution, financial institution, payment system.*

REFERENCES

1. Gronin D. P. O*t bankovskoy tayny k finansovoy tayne* [From banking secrecy to the financial secret]. URL: http://xn——7sbbaj7auwnffhk.xn—p1ai/article/2482.
2. Kanashevskiy V. A. *Ob obyazatelnom khranenii informatsii na territorii Rossii (trebovanie lokalizatsii)* [The compulsory storage of information on the territory of Russia (the localization requirement)]. *Mezhdunarodnoe publichnoe i chastnoe parvo* [International public and private law. 2017]. No. 6.
3. Selivanovskiy S. A. *Bankovskaya tayna: sostoyanie i problem*y [Bank secrecy: the state and problems]. URL: http://www.selivanovsky.ru/pages/bankovskaya_tajna/
4. Khorvat O., Sevastyanova Yu. *Autsorsing i autstaffing v banke — ekonomicheskiy effekt ili sotsialnye i nalogovye riski* [Outsourcing and outstaffing in a bank — the economic effect or social and tax risks?]. Legal reference system "Konsultant Plus:" [Electronic resource]. «KonsultantPlus»., 2014.