ЗАЩИТА БАНКОВСКОЙ И КОММЕРЧЕСКОЙ ТАЙНЫ ПРИ ПРОИЗВОДСТВЕ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ В ОТНОШЕНИИ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

В.С. Черкасов
Дальневосточный юридический институт МВД России
email: viktor.kmsx@gmail.com

Аннотация. В условиях повсеместной цифровизации различных процессов жизнедеятельности человека, одним из вопросов является степень соблюдения режима банковской и коммерческой тайны при производстве следственных действий в отношении электронных носителей информации. В работе выявляются проблемы и предлагаются механизмы совершенствования защиты банковской и коммерческой тайны при производстве следственного осмотра и назначения компьютерно-технической экспертизы.

Ключевые слова: банковская тайна, коммерческая тайна, следственные действия, электронный носитель информации, цифровые технологии.

Современные информационные технологии многократно увеличили оборот частной информации между людьми. Электронные устройства и интернет-сервисы позволяют мгновенно отправлять сообщения, управлять банковским счетом, бизнесом, получать государственные услуги и т.п. Оборот подобной информации происходит при помощи оконечных устройств (телефонов, ноутбуков и других электронных носителей информации) и интернет-серверов. Для получения электронной информации о частной жизни лица в рамках производства предварительного расследования производится осмотр предмета или назначает компьютерно-техническая экспертиза электронного носителя информации. При этом «проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения» [3].

Соглашаясь с мнением В.Ф. Васюкова, необходимо отметить, что сейчас действует следующее правило: «Правоотношения, регулируемые федеральными законами, касаются только принципов сохранения в тайне данных, которые были доверены гражданином только определенной организации или должностному лицу. Если информация выбыла из сферы ответственности организации (должностного лица) путем фиксации ее в памяти мобильного компьютерного устройства, она как таковая уже не подлежит защите с помощью судебного контроля» [4, С. 67].

Современные криминалистические устройства, которые могут быть использованы при производстве осмотра электронных носителей информации специалистом, позволяют обходить пароли защиты самого носителя и установленных приложений, что значительно расширяет объем информации. К таким устройствам С.Ю. Скобелин относит: универсальное устройство извлечения судебной информации (UFED–Universal Forensic Extraction Devise), «Мобильный криминалист», XRY, MOBILedit, «Тарантул» и другие. Так, посредством комплекса UFED «можно получить информацию о паролях, журналах вызовов, текстовых сообщениях, контактах в электронной почте, мессенджерах, записях в календаре, медиафайлах, геотегах, приложениях, служебных данных (список IMSI, данные последней сим-карты, коды блокировки); данных журнала «Lifeblog», содержащего список действий с телефоном; о переписке в различных социальных сетях («ВКонтакте», «Одноклассники», «Twitter», «Facebook») с помощью таких приложений, как «Skype» и др.» [7, С. 31-32].

В создавшихся условиях представляется важным рассмотреть вопрос о распространении режима «коммерческой» и «банковской» тайны на информацию, к которой можно получить доступ при производстве осмотра и компьютерно-технической экспертизы электронного носителя информации.

Так, в соответствии с п. 2 ст. 3 Закона «О коммерческой тайне»[1], информация, составляющая коммерческую тайну – это «сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны».

Очевидно, что указанные сведения могут быть распространены с помощью различных интернет-сервисов между заинтересованными лицами (между учредителями юридического лица, контрагентами договора коммерческой концессии «франчайзинг» и т.д.). Так, ч. 3 ст. 6 закона «О коммерческой тайне» предусматривает для обладателя информации, составляющей коммерческую тайну, а также для органа государственной власти, местного самоуправления, получившего такую информацию, обязанность предоставлять названную информацию по запросу органа предварительного расследования по делам, находящимся в их производстве.

Необходимо отметить, что ч. 2 ст. 6 закона «О коммерческой тайне», предусматривает для обладателя подобной информации механизм самозащиты. Как указывает К.В. Пронин: «Во всех случаях, когда обладатель коммерческой тайны считает требования государственного органа (органа местного самоуправления) о предоставлении ему тех или иных конфиденциальных сведений незаконными и отказывается исполнить запрос, инициатор запроса, согласно части 2 статьи 6 Закона «О коммерческой тайне», наделяется правом затребовать эту информацию в судебном порядке».

Рассмотрение дела в суде дает обеим сторонам спора равные процессуальные возможности для отстаивания своей позиции, что является дополнительной правовой гарантией от злоупотреблений со стороны чиновников. Кроме того, обладатель коммерческой тайны также наделен правом на обращение в суд - он может подать иск о признании соответствующего предписания государственного органа (органа местного самоуправления) не соответствующим закону, иному нормативному правовому акту» [5, С. 54]. Доступ к электронной информации, составляющей коммерческую тайну, через электронный носитель фактически лишает обладателя данной информации, механизма судебной самозащиты.

Выше уже указывалось, что в настоящее время существуют специальные приложения (программы), которые позволяют управлять банковским счетом (производить транзакции, оплачивать счета, брать кредит, осуществлять вклады, наблюдать информацию по счету и т.д.) через электронный носитель информации. Исходя из этого, через электронный носитель информации можно получить доступ к банковской тайне. Согласно ст. 26 Федерального закона «О банках и банковской деятельности» [2], справки по операциям и счетам юридических лиц, граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, а также физических лиц выдаются кредитной организацией, при наличии согласия руководителя следственного органа, по делам, находящимся в их производстве. При этом, согласно п. 3 ч. 2 ст. 38 УПК РФ, следователь уполномочен самостоятельно направлять ход расследования, принимать решение о производстве следственных и иных процессуальных действий, за исключением случаев, когда в

соответствии с УПК РФ требуется получение судебного решения или согласия руководителя следственного органа.

Взаимосвязанные положения п. 3 ч. 2 ст. 38 УПК РФ и ст. 26 Федерального закона «О банках и банковской деятельности» накладывают на следователя ведомственный контроль со стороны руководителя следственного органа. Исходя из этого, следователь вправе получать сведения, попадающие под режим банковской тайны, только при наличии согласия руководителя следственного органа по возбужденному уголовному делу. Очевидно, что осмотр электронного носителя информации, который может быть произведен до возбуждения уголовного дела, и соответственного «банковского» приложения, согласия руководителя следственного органа не требует, что фактически необоснованно исключает ведомственный контроль и содержит предпосылки для нарушения режима банковской тайны.

Таким образом, существующий механизм получения информации с электронных носителей не обеспечивает соблюдения режима «коммерческой» и «банковской» тайны. Проблема регулирования названных правоотношений видится в том, что сотрудник органа предварительного расследования не может предсказать с каким режимом тайны предстоит столкнуться при производстве следственного действия в отношении электронного носителя информации. Одним из возможных направлений обеспечения действия различных режимов является введение универсального судебного контроля по производству следственных действий в отношении электронных носителей информации, позволяющих направлять, принимать и воспроизводить электронные сообщения с помощью телематической связи.

Библиографический список.

1. Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 20.03.2021) «О коммерческой тайне» // URL: https://base.garant.ru/12136454/ (дата обращения: 20.07.2022 г.).
2. Федеральный закон от 02.12.1990 № 395-1 (ред. от 02.07.2021) «О банках и банковской деятельности» // URL: https://base.garant.ru/10105800/ (дата обращения: 13.07.2022 г.).
3. Определение Конституционного суда РФ от 25 января 2018 № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации // СПС «Консультант плюс» // URL: https://legalacts.ru/sud/opredelenie-konstitutsionnogo-suda-rf-ot-25012018-n- 189-o/ (дата обращения: 12.09.2022).
4. Васюков В.Ф. Осмотр, выемка электронных сообщений и получение компьютерной информации // Уголовный процесс. – 2016. – № 10. – С. 67.
5. Пронин К.В. Защита коммерческой тайны. – М.: Издательство: Гросс-Медиа, 2006. – С. 54.
6. Скобелин С. Н. Использование специальных знаний при работе с электронными следами // Российский следователь. 2014. № 20.

PROTECTION OF BANKING AND COMMERCIAL SECRETS IN THE COURSE OF INVESTIGATIVE ACTIONS IN RELATION TO ELECTRONIC MEDIA

V.S. Cherkasov
Far Eastern Law Institute of the Ministry of Internal Affairs of Russia
email: viktor.kmsx@gmail.com

Abstract. In the conditions of widespread digitalization of various processes of human activity, one of the issues is the degree of compliance with the regime of banking and commercial secrecy in the production of investigative actions against electronic media.

The paper identifies problems and suggests mechanisms for improving the protection of banking and commercial secrets during the investigative examination and the appointment of computer-technical expertise.

Keywords: banking secrecy, commercial secrecy, investigative actions, electronic media, digital technologies.