Статья в журнале
«Защита информации - Инсайд», №2, 2012 год

Александр Катаржнов

к.т.н., доцент, НОУ ДО Учебный центр «ЭВРИКА»

Лицензирование деятельности по технической защите конфиденциальной информации.

За последние годы подзаконная база в области информационной безопасности сформировала затратные, запутанные, противоречивые механизмы, не учитывающие ни особенности обработки конфиденциальной информации в различных сферах деятельности, ни возможности операторов по выполнению установленных требований. Кроме того, требования к операторам информационных систем, обрабатывающих конфиденциальную информации, включая и персональные данные, со стороны ФСТЭК России включают такой механизм государственного регулирования, как лицензирование деятельности по технической защите конфиденциальной информации, для реализации которого у большинства операторов нет достаточных материальных и трудовых ресурсов. Особенно это касается бюджетных организаций в сфере образования, медицинского обслуживания, жилищно-коммунального комплекса. Проблемы правового характера возникли в связи с отсутствием в федеральном законодательстве законов по защите конфиденциальной информации, например, служебной тайны, профессиональных тайн, неоднозначностью положений, а также неоднократными изменениями и дополнениями, внесенными в ФЗ №152 «О персональных данных», другие нормативные правовые акты. При этом федеральные законы требуют дальнейшей конкретизации и разъяснений постановлениями Правительства РФ и методическими документами ФСТЭК и ФСБ России.

Принятие Правительством РФ постановления от 3 февраля 2012 г. №79 «О лицензировании деятельности по технической защите конфиденциальной информации» с утверждением «Положения о лицензировании деятельности по технической защите конфиденциальной информации» (далее – Положение) и отменой ранее действовавшего постановления от 15 августа 2006 г. №504, в очередной раз поднимает вопрос, а что нового в указанном Положении и нужна ли лицензия ФСТЭК России, если организация защищает конфиденциальную информацию «для собственных нужд», а не оказывает услуги за деньги?

В соответствии с п. 1 Положение определяет порядок лицензирования деятельности по технической защите конфиденциальной информации (не содержащей сведения, составляющие государственную тайну, но защищаемой в соответствии с законодательством Российской Федерации), осуществляемой юридическими лицами и индивидуальными предпринимателями.

И сразу встает вопрос с термином "конфиденциальная информация", который дан в Положении и используется в документах ФСТЭК России, но отсутствует в федеральном законодательстве. ФЗ №149 от 27.07. 2006 г.» Об информации, информационных технологиях и о защите информации» в п.7 ст. 2 дает только определение конфиденциальности информации, как обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. Конфиденциальность в переводе с латинского означает "доверие" (т.е. передавая такую информацию мы надеемся на ее сохранность и нераспространение, так как ее разглашение может нанести сторонам определенный ущерб). Отметим, что отсутствие четкости отдельных терминов, а также подчас необоснованные изменения определений и понятий информационного законодательства не способствуют улучшению правового регулирования в информационной сфере. При этом

ФСТЭК России продолжает использовать термин "конфиденциальная информация", от которого законодатели уже отказались.

Согласно законодательству РФ обязательными признаками информации с ограниченным доступом должны быть:

- информация имеет действительную или потенциальную ценность для обладателя в силу неизвестности ее третьим лицам. Такими лицами могут быть государство, юридические или физические лица;

- к информации нет свободного доступа на законном основании. Возможность сохранения ее неизвестной для третьих лиц установлена федеральным законом;

- обладатель информации принимает меры по ее защите.

6 марта 1997 г. Президентом РФ был издан Указ N 188, которым утвержден «Перечень сведений конфиденциального характера», в соответствии с которым к конфиденциальной информации были отнесены следующие сведения:

- о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

- составляющие тайну следствия и судопроизводства;

- доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (служебная тайна);

- связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.);

- связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами (коммерческая тайна);

- о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

В новом Постановлении уточнен и термин «техническая защита конфиденциальной информации» (далее - ТЗКИ), под которой в соответствии с п.2 Положения понимается:

- выполнение работ и (или) оказание услуг по ее защите от несанкционированного доступа, от утечки по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Таким образом речь идет либо о выполнении работ по ТЗКИ, либо об оказании услуг по ТЗКИ, либо о совместных видах деятельности.

При осуществлении деятельности по технической защите конфиденциальной информации лицензированию подлежат следующие виды работ и услуг:

а) контроль защищенности конфиденциальной информации от утечки по техническим каналам в:

- средствах и системах информатизации;

- технических средствах (системах), не обрабатывающих конфиденциальную

информацию, но размещенных в помещениях, где она обрабатывается;

- помещениях со средствами (системами), подлежащими защите;

- помещениях, предназначенных для ведения конфиденциальных переговоров (далее - защищаемые помещения);

б) контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

в) сертификационные испытания на соответствие требованиям по безопасности информации продукции, используемой в целях защиты конфиденциальной информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации (далее – СЗИ), защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации);

г) аттестационные испытания и аттестация на соответствие требованиям по защите информации:

- средств и систем информатизации;

- помещений со средствами (системами) информатизации, подлежащими защите;

- защищаемых помещений;

д) проектирование в защищенном исполнении:

- средств и систем информатизации;

- помещений со средствами (системами) информатизации, подлежащими защите;

- защищаемых помещений;

е) установка, монтаж, испытания, ремонт средств защиты информации (технических СЗИ, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты

информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

При этом эксплуатация СЗИ, в отличии от эксплуатации средств криптографической защиты, где лицензирующим органом является ФСБ России, к лицензируемому виду деятельности не относится. Эта позиция ФСТЭК России вызывает вопросы. Почему лицензируется только первые этапы в создании системы защиты - проектирование системы защиты и установка средств защиты? Почему ежедневная работа специалистов и служб информационной безопасности по эксплуатации и контролю эффективности СЗИ не подпадает под лицензирование? Ведь она не менее важна, чем создание системы защиты, так как задачами лицензирования отдельных видов деятельности являются предупреждение, выявление и пресечение нарушений юридическим лицом, его руководителем и иными должностными лицами требований, которые установлены ФЗ от 4.5.2011г. №99-ФЗ «О лицензировании отдельных видов деятельности», другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации.

В силу п. 1 ст. 49 ГК РФ отдельными видами деятельности, перечень которых определяется законом, юридическое лицо может заниматься только на основании специального разрешения (лицензии). Виды деятельности, на осуществление которых необходимо получить лицензию, указаны в ФЗ от 4.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности", п. 5 ст. 12 которого включает в число этих видов и деятельность по ТЗКИ.

Понятие "услуги" подразумевает под собой определенный вид договора (глава 39, ст.ст. 779-783 ГК РФ), то есть многосторонней сделки, в которой обязательно должна быть и другая сторона (п. 1 ст. 154 ГК РФ). А вот

понятие " работа" в законе не определено и может определяться только исходя из многих значений в русском языке: "занятие, труд, деятельность».

Таким образом, из приведенной формулировки можно сделать вывод, что лицензированию подлежит деятельность по ТЗКИ как третьих лиц ("услуги"), так и для собственных нужд ("работ").

Соответственно, если организация в рамках защиты внутренней конфиденциальной информации осуществляет работы по ее технической защите, она обязана получить соответствующую лицензию. Например, применительно к защите персональных данных у оператора не существует «собственных нужд» по их защите, и существовать не может в силу закона. Единственной целью ФЗ №152 «О персональных данных» является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных. Иных целей (в том числе и удовлетворения нужд операторов) закон не указывает. Кроме этого ФЗ 99-ФЗ «О лицензировании отдельных видов деятельности» к лицензируемым видам деятельности отнесены виды деятельности, осуществление которых может повлечь за собой нанесение ущерба правам, законным интересам, здоровью граждан. Закон не делает различий между интересами субъекта персональных данных (работника) и субъекта персональных данных (стороннего лица) о конституционном праве гражданина на личную тайну. Законодатель же (через институт лицензирования) защищает любого субъекта персональных данных от последствий некачественного выполнения работ по ТЗКИ.

Административным регламентом ФСТЭК России по исполнению государственной функции по лицензированию деятельности по ТЗКИ (далее – Административный регламент), утвержденным приказом от 28.08.07г. №181 с последними изменениями от 30.09.2011 г. в соответствии с приказом №515, определены сроки и последовательность действий (административных процедур) ФСТЭК России при осуществлении полномочий по лицензированию деятельности по ТЗКИ. Лицензированию подлежит

деятельность по ТЗКИ, осуществляемая юридическими лицами и индивидуальными предпринимателями.

Анализ положений Административного регламента показывает, что процедура получения лицензии по ТЗКИ отнимает много времени, сил и средств. Для получения лицензии на деятельность по ТЗКИ необходимо подтвердить возможность выполнения лицензионных требований и условий, определенных Положением.

Лицензионными требованиями, предъявляемыми к соискателю лицензии на осуществление деятельности по ТЗКИ, являются (п.5 Регламента):

а) наличие у соискателя лицензии юридического лица - специалистов, находящихся в штате соискателя лицензии, имеющих высшее профессиональное образование в области технической защиты информации либо высшее техническое или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации.

б) наличие у соискателя лицензии (лицензиата) помещений для осуществления лицензируемой деятельности, соответствующих техническим нормам и требованиям по технической защите информации, установленным нормативными правовыми актами Российской Федерации, и принадлежащих ему на праве собственности или на ином законном основании;

в) наличие на любом законном основании производственного, испытательного и контрольно-измерительного оборудования, прошедшего в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку), маркирование и сертификацию;

г) использование автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших процедуру оценки соответствия (аттестованных и

(или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством Российской Федерации;

д) использование предназначенных для осуществления лицензируемой деятельности программ для электронно-вычислительных машин и баз данных на основании договора с их правообладателем;

е) наличие нормативных правовых актов, нормативно-методических и методических документов по вопросам технической защиты информации в соответствии с перечнем, установленным ФСТЭК России.

Как видно, для выполнения вышеназванных требования в организации необходимо иметь не менее 2 специалистов, что, в ряде случаев (при отсутствии профильного высшего образования) потребует их обучения на курсах повышения квалификации по учебным программам согласованным со ФСТЭК России в объеме не менее чем 72 часа. Кроме этого потребуются нормативные документы, в том числе ограниченного доступа, а также наличие на любом законном основании (в собственности или в аренде на срок не менее срока действия лицензии) производственного, испытательного и контрольно-измерительного оборудования, прошедшего в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку), маркирование и сертификацию. Кроме вышесказанного придется провести проектирование, создание и аттестацию объектов информатизации (автоматизированной системы и защищенного помещения), предназначенных для обработки конфиденциальной информации. При этом возникает проблема приобретения на любом законном основании контрольно-измерительного оборудования, которое не потребуется лицензиату для оказания услуг по ТЗКИ. Причем большинство указанных требований являются достаточно затратными в экономическом плане, в первую очередь, для бюджетных организаций в сфере образования, медицинского обслуживания, жилищно-коммунального комплекса.

Исполнение государственной функции по лицензированию деятельности по ТЗКИ в соответствии с п.п.12-14 Регламента включает в себя следующие административные процедуры (рис.1):

- информирование и консультирование о порядке исполнения государственной функции;

- рассмотрение заявления о предоставлении лицензии;

- проверка возможности выполнения соискателем лицензии лицензионных требований и условий;

- принятие решения о предоставлении лицензии;

- выдача документа, подтверждающего наличие лицензии;

- выдача дубликата и копий документа, подтверждающего наличие лицензии;

- продление срока действия лицензии;

- переоформление документа, подтверждающего наличие лицензии;

- контроль за соблюдением лицензиатом лицензионных требований и условий;

- приостановление, возобновление действия лицензии и аннулирование лицензии;

- ведение реестра лицензий;

- предоставление информации из реестра лицензий.

Должностное лицо ФСТЭК России принимает решение о предоставлении или об отказе в предоставлении лицензии в срок, не превышающий 45 дней со дня поступления заявления о предоставлении лицензии и прилагаемых к нему документов (п.14.1 Регламента).

Основаниями для отказа в предоставлении лицензии являются (п.14.3 Регламента):

наличие в документах, представленных соискателем лицензии, недостоверной или искаженной информации;

несоответствие соискателя лицензии, принадлежащих ему или используемых им объектов лицензионным требованиям и условиям.

Лицензия на осуществление деятельности по технической защите конфиденциальной информации предоставляется сроком на 5 лет (п.14.4 Регламента). При этом с 30 января 2011 г. изменены размеры государственных пошлин: за предоставление лицензии – 2600 рублей и за продление срока действия лицензии – 200 рублей.

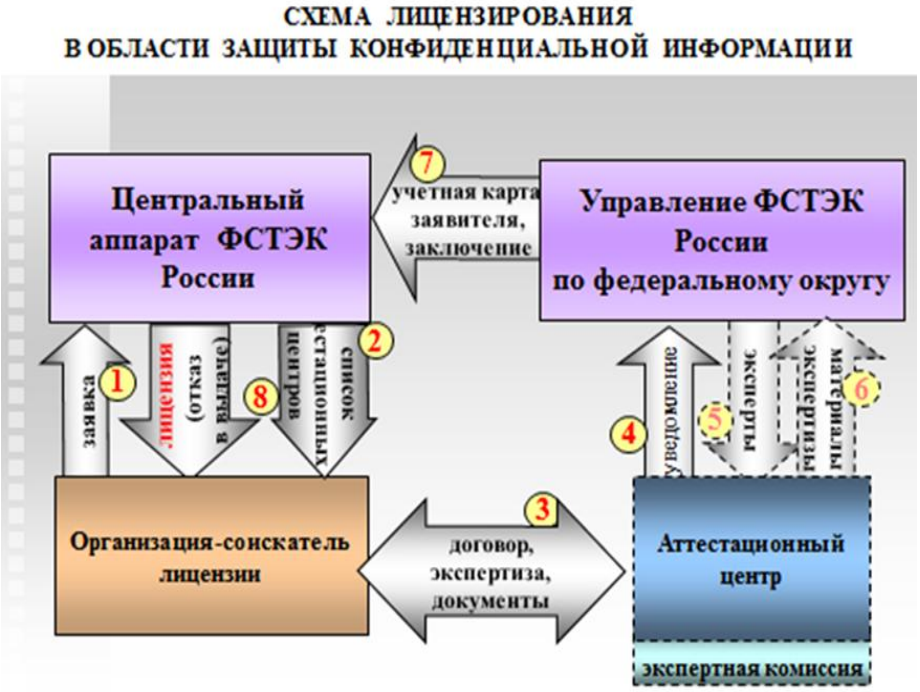

Рис.1

Как видно из схемы и процедур (рис.1) лицензированием ТЗКИ занимается центральный аппарат ФСТЭК России с привлечением управлений ФСТЭК России по федеральным округам в отличие от процедур лицензирования ФСБ России, где лицензированием в своей сфере ответственности занимаются территориальные управления ФСБ России. Продолжительность процесса лицензирования ТЗКИ по времени может занять от двух до шести месяцев и повлечь за собой значительные финансовые затраты, особенно в случае приобретения контрольно-измерительного оборудования в собственность.

Можно ли уйти от необходимости лицензирования деятельности организаций и предприятий по ТЗКИ? Рекомендации ФСТЭК России сводятся к необходимости заключения договора с организацией имеющей лицензию по ТЗКИ, при этом наличие указанной лицензии у оператора обязательным требованием не является.

Вместе с тем, в соответствии с пунктом 10 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781, безопасность персональных данных при их обработке в информационной системе может обеспечивать уполномоченное лицо, которому на основании договора оператор поручает обработку персональных данных. При этом указанное уполномоченное лицо должно иметь лицензию на деятельность по технической защите конфиденциальной информации, а наличие указанной лицензии у оператора обязательным требованием не является.

С уважением,

Начальник 2 управления А.Куц

Рекомендации ФСТЭК России заключать договора с лицензиатами, которых в реестре менее 2000, не позволяют решить проблему защиты конфиденциальной информации. Только операторов персональных данных по экспертным оценкам в России 5-7 миллионов, не считая операторов,

которые обрабатывают другие виды информации ограниченного доступа, подлежащей защите в соответствии с федеральным законодательством. Кроме этого, договор с лицензиатом обычно заключается только на определенный объем работ и услуг, как правило, только на создание системы защиты конфиденциальной информации.

Какие же риски возникают у большинства организаций, которые не имеют и не планируют получать лицензии по ТЗКИ или получать услуги организаций имеющих такую лицензию при неизменности государственной политики и позиции ФСТЭК России? Каждая организация должна для себя принять решение о необходимости получения такой лицензии. Административных наказаний за выполнение работ без лицензии на деятельность по ТЗКИ со стороны ФСТЭК России нет и в сложившейся ситуации маловероятно, что эти наказания появятся, так как в условиях несовершенства нашего законодательства по защите конфиденциальной информации суды по разному трактуют нормы федеральных законов и ответственность за их невыполнение. В результате строгость Постановления компенсируется необязательностью его исполнения. Например, статьей 14.1 Административного Кодекса РФ предусмотрена ответственность за "Осуществление предпринимательской деятельности без государственной регистрации или без специального разрешения (лицензии)". Согласно ст.2 ГК РФ "предпринимательской является самостоятельная, осуществляемая на свой риск деятельность, направленная на систематическое получение прибыли от пользования имуществом, продажи товаров, выполнения работ или оказания услуг лицами, зарегистрированными в этом качестве в установленном законом порядке". Уже одно это говорит о том, что ст.14.1 может применяться только к тем, кто оказывает услуги и зарабатывает на обеспечении безопасности информации, т.е. лицензиаты ФСТЭК и ФСБ России. К подавляющему большинству организаций обрабатывающих конфиденциальную информацию (информации ограниченного доступа, не составляющей государственную тайну) эта статья отношения не имеет. По

мнению многих специалистов по защите информации для большинства негосударственных организаций, не связанных с защитой государственной тайны, реально возможны только формы управления защитой конфиденциальной информации путем рекомендательного использования нормативных правовых актов, руководящих и методических документов регуляторов, организационно-распорядительных документов организаций, применение разработанных и испытанных в интересах органов государственной власти и подведомственных им предприятий систем и СЗИ. Основой функционирования систем защиты конфиденциальной информации в этом случае является личный выбор обладателем информации степени ее защищенности и механизмов защиты. При этом, по опыту стран с развитым законодательством в сфере информационной безопасности, определяющими факторами являются риск участников информационных отношений и их личная ответственность за принятые меры по защите конфиденциальной информации. В России этот подход, например, реализован при введении Стандартов Банка России в организации БС РФ, когда требования по получению лицензий на деятельность по технической защите конфиденциальной информации и требования аттестации информационных систем персональных данных не являются обязательными (в соответствии с пунктом 9.6 СТО БР ИББС-1.0-2010).