ЛИЦЕНЗИРОВАНИЕ ДЕЯТЕЛЬНОСТИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Шахалов Игорь Юрьевич

В статье проводится анализ и сравнение лицензионных требований для получения лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации, которые были до февраля 2012 года и на сегодняшний день. Автор объясняет особенности подготовки заявочного комплекта документов и указывает на ряд особенностей, которые на первый взгляд, не видны соискателю лицензии.

Ключевые слова: *лицензирование, техническая защита конфиденциальной информации, ФСТЭК России, ТЗКИ*

LICENSING IN INFORMATION SECURITY

Igor Shahalov

The new requirements for obtaining the FSTEC Russia license for confidential information technical security are analyzed.

The features of preparation and pitfalls of application documents are explained.

Keywords: *licensing, confidential information technical security, FSTEC Russia*

Актуальность.

Любое государство не просто имеет право, но и обязано (если хочет остаться независимым государством) обеспечить безопасность информации, влияющей на утрату интересов или безопасность государства [2,3].

Для этого необходимо разработать и внедрить систему защиты информации ограниченного распространения на государственном уровне. Важной частью такой системы является процесс выдачи специального разрешения на осуществление деятельности по защите информации, то есть *лицензирование* [1,5-8]. При этом, как правило, существует разграничение на защиту информации, составляющей гостайну и информации, носящей конфиденциальный характер. В настоящей статье будут рассмотрены вопросы лицензирования деятельности по технической защите конфиденциальной информации (ТЗКИ).

В Российской Федерации перечень лицензируемых видов деятельности установлен федеральным законом от 4 мая 2011 года N 99-ФЗ «О лицензировании отдельных видов деятельности». Он пришел на смену действующему ранее одноименному федеральному закону N 128-ФЗ от 8 августа 2001 года. Постановления правительства, регламентирующие выполнение 99-ФЗ в области защиты информации были приняты в первой половине 2012 года.

С принятием этих нормативно-правовых актов кардинально изменился подход к лицензированию деятельности в области информационной безопасности – вместо одного вида деятельности появился целый ряд видов работ и услуг, для занятия которыми требуется лицензия. Сами лицензии стали бессрочными, правда, при этом ужесточились условия, необходимые для проведения проверок лицензиатов.

Существенно изменился и набор лицензионных требований к соискателю лицензии. Стало, с одной стороны, проще, а с другой сложнее – теперь соискателю лицензии или лицензиату (при продлении лицензии) надо научиться правильно выбрать необходимый для осуществления деятельности набор видов работ и услуг, а, следовательно, от этого зависит и объем подготовительных мероприятий по выполнению лицензионных требований.

Среди 49 видов деятельности, указанных в 99-ФЗ, есть несколько, относящихся к вопросам защиты конфиденциальной информации, в том числе есть и такой вид деятельности, как «деятельность по технической защите конфиденциальной информации» (ТКЗИ). Конкретно этот вид деятельности интересен тем, что он наиболее распространен в современных условиях. Защита персональных данных [8], ком-

Таблица 1
Виды работ и услуг

№ п/п	Вид работ и услуг	Уточнение и разделение
1	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);
2	б) контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;	Отсутствуют
3	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, прог раммных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации);	Отсутствуют
4	г) аттестационные испытания и аттестация на соответствие требованиям по защите информации:	средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений;
5	д) проектирование в защищенном исполнении:	средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений;
6	е) установка, монтаж, испытания, ремонт средств защиты информации	технических средств защиты информации, 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

мерческой тайны и других «служебных» тайн[1] подразумевают под собой, в первую очередь, техническую защиту информации. Положение о лицензировании деятельности по ТЗКИ было введено в действие постановлением Правительства Российской Федерации N 79 от 3 февраля 2012 года.

Сотни предприятий и организаций, получивших лицензии на деятельность по ТЗКИ раньше, до вступления в силу указанных выше 99-ФЗ и 79-ПП, в настоящее время встают перед проблемой продления и переоформления лицензий на ТЗКИ. Проблемой потому, что в силу изменившихся лицензионных требований, надо очень внимательно отнестись к формированию заявочного комплекта. В первую очередь потому, что специфика рассмотрения и выдачи лицензии на ТЗКИ во ФСТЭК России подразумевает только рассмотрение представленного соискателем комплекта документов. Выезд сотрудников ФСТЭК России к соискателю в 79-ПП не предусмотрен.

Актуальность данной статьи в этом и заключается – автор постарался показать, что именно изменилось с момента получения предыдущей лицензии, до февраля 2012 года и как правильно подготовиться и оформить заявочный комплект на лицензию по ТЗКИ сейчас.

Сравнение лицензионных требований.

Процесс регулирования процедуры лицензирования в области технической защиты конфиденциальной информации, как было сказано выше, значительно изменился с выходом Постановления Правительства № 79 от 3 февраля 2012 года взамен Постановления Правительства № 504 от 15 августа 2006 года.

[1] Согласно [2], в российском законодательстве всего насчитывается около 50 различных тайн

Таблица 2

Сравнение лицензионных требований по ТЗКИ

ПП № 504 от 15.08.2006 г	ПП № 79 от 03.02.2012 г.
а) наличие в штате соискателя лицензии (лицензиата) специалистов, имеющих высшее профессиональное образование в области технической защиты информации либо высшее или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации;	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 - индивидуального предпринимателя - высшего профессионального образования в области технической защиты информации либо высшего технического или среднего профессионального (технического) образования при условии прохождения им переподготовки или повышения 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;	б) наличие помещений для осуществления лицензируемого вида деятельности, соответствующих установленным законодательством Российской Федерации техническим нормам и требованиям по технической защите информации и принадлежащих соискателю лицензии на праве собственности или на ином законном основании;
	г) наличие на праве собственности или на ином законном основании средств контроля защищенности информации от несанкционированного доступа, сертифицированных по требованиям безопасности информации, в соответствии с перечнем, утверждаемым Федеральной службой по техническому и экспортному контролю (при выполнении работ и (или) оказании услуг, предусмотренных подпунктами «б», «в» и «г» пункта 4 настоящего Положения);
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) наличие автоматизированных систем, предназначенных для обработки конфиденциальной информации, 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 предназначенных для осуществления лицензируемого вида деятельности программ для электронно-вычислительных машин и баз данных, принадлежащих соискателю лицензии на праве собственности или на ином законном основании;
е) наличие нормативных правовых актов, нормативно-методических и методических документов по вопросам технической защиты информации в соответствии с перечнем, установленным Федеральной службой по техническому и экспортному контролю;	ж) наличие технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и (или) оказания услуг, предусмотренных пунктом 4 настоящего Положения, в соответствии с утверждаемым Федеральной службой по техническому и экспортному контролю перечнем и принадлежащих соискателю лицензии на праве собственности или на ином законном основании;
Отсутствует	з) наличие системы производственного контроля в соответствии с установленными стандартами (при выполнении работ, указанных в подпункте «в» пункта 4 настоящего Положения);

Основное отличие нового «Положения…» от предыдущего - это разделение одного вида деятельности на шесть отдельных видов работ и услуг (табл. 1).

Данное разделение значительно облегчило, во-первых, бремя выбора как соискателям лицензий и, во-вторых, так и самому регулирующему органу организацию деятельности лицензиатов.

Теперь, например, невозможно неподготовленному лицензиату проводить аттестацию объектов информатизации (чем зачастую раньше грешили лицензиаты) или сертификационные испытания. При этом у соискателя появилась возможность уйти от больших финансовых затрат, неизбежных ранее при покупке контрольно-измерительной аппаратуры. Достаточно просто ис-

ключить из заявленных видов работ и услуг те работы и услуги, которые подразумевают проведение работ с помощью дорогостоящих аппаратно-программных комплексов по поиску технических каналов утечки информации, оставляя только возможность осуществления своей деятельности в области защиты информации от несанкционированного доступа.

В развитие указанной выше градации работ и услуг несколько изменились и лицензионные требования к соискателям лицензии. Сравнительный анализ лицензионных требований из обоих «Положений…» приведен в табл. 2.

Следует отметить, что некоторые требования остались практически без изменений, очевидно по той причине, что изначально были предельно просты и не позволяли двоякого толкования. В первую очередь это касается требований к специалистам (по их количеству и образованию), наличию помещений для осуществления лицензируемого вида деятельности, легально приобретённого программного обеспечения и аттестованных по требованиям безопасности информации автоматизированных систем.

Если рассматривать эти требования подробнее, то можно выделить ряд особенностей по их выполнению.

По поводу образования, например, надо чётко понимать, что у заявленного специалиста должно быть, если не профессиональное образование в области технической защиты информации, то *обязательно высшее или среднее профессиональное (**техническое**) образование* и переподготовка или повышение квалификации по вопросам технической защиты информации.

Для выполнения требования по наличию помещений, в первую очередь необходимо обратить внимание на фразу: *«…принадлежащих соискателю лицензии на праве собственности или на ином законном основании»*, так как именно недочёты в оформлении договоров аренды помещений являются наиболее частыми причинами отказов в выдачи лицензии. Повторная подача заявления возможна только после устранения замечаний.

Легальность приобретения программного обеспечения подтверждается копиями лицензий на него и соответствующими бухгалтерскими документами.

Что касается аттестации автоматизированных систем – здесь не надо придумывать ничего лишнего, надо просто *чётко* следовать требованиям нормативно-методических документов ФСТЭК России.

Существенно изменились требования по наличию производственного, испытательного и контрольно-измерительного оборудования. В новом «Положении…» (79-ПП) данный вид требований поделен на *пункты **«в»** и **«г»***, что связано с разделением вида деятельности по технической защите конфиденциальной информации на несколько видов работ и услуг, как уже было сказано выше.

Появилось два различных требования:

- по *«контролю защищенности конфиденциальной информации от утечки по техническим каналам»*;

- по *«контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации»*.

При этом если при выполнении первого требования необходимо соответствующее контрольно-измерительное оборудование (стоимостью более одного миллиона рублей), то при выполнении второго достаточно только нескольких программных средств контроля защищенности информации, минимальный набор которых стоит не более пятнадцати тысяч рублей.

Выгода для обычного, рядового соискателя лицензии, очевидна.

Кроме того, появилось новое требование, заключающееся в наличии системы производственного контроля в соответствии с действующими стандартами в области качества. Это требование обязательно для тех соискателей, которые собираются заниматься проектированием объектов информатизации.

Особенности подготовки заявочного комплекта.

Процесс лицензирования является довольно трудоемким в связи с необходимостью сбора большого числа документов для формирования заявочного комплекта, составляющие которого чётко определены в «Положении…». Связано это с тем, что, как уже было сказано в начале настоящей статьи, ФСТЭК Росси проводит проверку только присланных с заявлением документов без проведения выездной проверки соискателя.

Как правильно подготовить заявочный комплект?

Первой составляющей является наличие в штате специалистов, удовлетворяющих лицензионным требованиям. Так как в этом требовании применено множественное число, ФСТЭК России требует наличие не менее двух специали-

стов. Организация должна подтвердить наличие у них высшего технического или профильного образования, факт трудоустройства на штатную должность в компании соискателя, а также факт повышения квалификации или переподготовки, если с момента получения высшего образования прошло более пяти лет. Программы повышения квалификации или переподготовки должны быть согласованы с регулятором. Перечень учебных центров, в которых проводится обучение, указан на сайте ФСТЭК России.

Следующим шагом является сбор документов, подтверждающих наличие помещений для осуществления лицензируемого вида деятельности. Здесь следует выделить два важных момента. Во-первых, как уже упоминалось, помещения должны быть у соискателя на законном основании, это подразумевает подтверждение права собственности, прямой аренды или субаренды соискателем с предоставлением документов, описывающих расположение и состав заявляемых помещений. Во-вторых, помещения должны соответствовать техническим нормам и требованиям по технической защите информации, что указывает на необходимость проведения аттестации на соответствие требованиям по безопасности информации выбранных помещений. Важно работы по аттестации провести с привлечением организации, имеющей лицензию на право оказания таких услуг.

Следующее требование заключается в предоставлении документов, подтверждающих наличие на законном основании у соискателя контрольно-измерительного, производственного и испытательного оборудования для осуществления выбранных пунктов лицензии. Все оборудование должно иметь действующие сертификаты соответствия ФСТЭК России и свидетельства о поверке или калибровке в зависимости от назначения (при необходимости).

Для подтверждения такого вида деятельности, как *контроль защищенности конфиденциальной информации от несанкционированного доступа*, необходимо представить в лицензирующий орган документы, подтверждающие наличие на законном основании средств контроля защищенности, имеющих действующие сертификаты ФСТЭК России. Перечень сертифицированных средств защиты информации представлен на сайте ФСТЭК России.

Далее требуется провести работы по аттестации автоматизированной системы для обработки конфиденциальной информации, если у соискателя такой системы не было ранее. Важно, что, как и в случае с защищаемым помещением, должна быть привлечена организация, имеющая не только разрешение (лицензию) на право проводить такие работы, но и грамотных специалистов, которые проведут установку и настройку средств защиты и разработают организационно-распорядительные документы, которые будут необходимы для организации режима обработки конфиденциальной информации.

Для осуществления лицензируемых видов деятельности необходимо наличие у соискателя на законном основании лицензионного программного обеспечения. В перечень программного обеспечения (в зависимости от заявляемых видов работ и услуг) входят: операционные системы, средства разработки документов, программы антивирусной защиты, базы данных и др.

Осуществление лицензируемых видов деятельности регламентируется нормативно-технической документацией, включающей национальные стандарты, методические и технические документы, которые должны принадлежать соискателю на законном основании. Соискатель должен изучить перечень на сайте ФСТЭК России и приобрести указанные нормативные документы. Большая часть технических документов является открытой, но часть имеет гриф «для служебного пользования» и подлежит приобретению установленным порядком.

Заключительным лицензионным требованием является наличие системы производственного контроля или системы менеджмента качества, включающей заявляемые области деятельности [4]. Подтверждением наличие системы производственного контроля является наличие сертификата соответствия национальным стандартам (при наличии) и/или предоставление внутренних документов по обеспечению качества выполнения работ по заявленным видам работ и услуг (Руководство по качеству, рабочие процедуры и т.п.).

При оформлении документов необходимо учесть требования по подтверждению верности представленных копий документов (Копии документов должны быть прошиты, с указанием на последней странице общего количества листов (не страниц), указанием «копия верна», названия должности 1-го лица предприятия и его фамилии, имени и отчества, подтверждающего верность копии, его личной подписи и даты, скрепленной печатью предприятия. Документы также могут быть заверены нотариально (но не обязательно). Неправильно оформленные документы рассмотрению не подлежат.

Заключение

В современных условиях, для получения лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации необходимо очень тщательно подготовить документы, которые должны быть приложены к заявлению – так называемый «заявочный комплект».

На этом пути соискателя лицензии подстерегает масса «подводных камней», которые надо знать, учитывать и готовить комплект документов так, чтобы эти «подводные камни» не стали препятствием для получения лицензии.

У соискателя есть выбор – либо самому идти тернистым путём проб и ошибок, либо обратиться к организациям, которые специализируются на консалтинге по подготовке соискателей к получению лицензий.

Литература

1. Белгородцева Н.Г., Певцова Е.А. Об особенностях правового регулирования в области защиты информации персонального характера // Современное право. 2011. № 2. С. 76-77.
2. Волчинская Е.К. Роль государства в обеспечении информационной безопасности // Информационное право. -2008. -№ 4. С. 9-16.
3. Козориз Н.Л. О предмете правового регулирования информационной безопасности // Информационное право. 2013. № 4. С. 8-10.
4. Дорофеев А.В., Шахалов И.Ю. Основы управления информационной безопасностью современной организации // Правовая информатика. 2013. №3. С.4-14.
5. Рыжов Р.С. Правовое регулирование отношений, связанных с информационными технологиями и защитой информации // Административное и муниципальное право. 2011. № 9. С. 64-68.
6. Федосин А.С. О лицензировании деятельности в сфере защиты информации. Юридическая наука и практика // Вестник Нижегородской академии МВД России. 2011. № 3. С. 215-218.
7. Шапошников В.И. Некоторые проблемы правового регулирования отношений по лицензированию в области защиты информации // Актуальные проблемы российского права. 2007. № 2. С. 77-81.
8. Шахалов И.Ю. Лицензия как продукт осознанной необходимости // Защита информации. Инсайд. 2010. №2. С. 53-55.

References

1. Belgorodtseva N.G., Pevtsova E.A. Ob osobennostyakh pravovogo regulirovaniya v oblasti zashchity informatsii personal'nogo kharaktera (The peculiarities of legal regulation in the field of the personal data security), Sovremennoe pravo, 2011, No. 2, pp. 76-77.
2. Volchinskaya E.K. Rol' gosudarstva v obespechenii informatsionnoi bezopasnosti (The state's role in providing information security), Informatsionnoe pravo, 2008, No. 4, pp. 9-16.
3. Kozoriz N.L. O predmete pravovogo regulirovaniya informatsionnoi bezopasnosti (Subject of legal regulation of information security), Informatsionnoe pravo, 2013, No. 4, pp. 8-10.
4. Dorofeev A.V., Shakhalov I.Yu. Osnovy upravleniya informatsionnoi bezopasnost'yu sovremennoi organizatsii (The basics of information security management in a modern organizations), Pravovaya informatika, 2013, No. 3, pp. 4-14.
5. Ryzhov R.S. Pravovoe regulirovanie otnoshenii, svyazannykh s informatsionnymi tekhnologiyami i zashchitoi informatsii (Legal regulation of relations connected with information technology and information security), Administrativnoe i munitsipal'noe pravo, 2011, No. 9, pp. 64-68.
6. Fedosin A.S. O litsenzirovanii deyatel'nosti v sfere zashchity informatsii. Yuridicheskaya nauka i praktika: (About licensing of activities in the field of information security. Legal Science and Practice), Vestnik Nizhegorodskoi akademii MVD Rossii, 2011, No. 3, pp. 215-218.
7. Shaposhnikov V.I. Nekotorye problemy pravovogo regulirovaniya otnoshenii po litsenzirovaniyu v oblasti zashchity informatsii (Some problems of legal licensing regulation in the field of information security), Aktual'nye problemy rossiiskogo prava, 2007, No. 2, pp. 77-81.
8. Shakhalov I.Yu. Litsenziya kak produkt osoznannoi neobkhodimosti (License as a product perceived need), Zashchita informatsii. Insaid, 2010, No. 2, pp. 53-55.