

О лицензировании и сертификации в области защиты информации

О.А. Беззубцев А.Н. Ковалев

I

Данная работа представляет собой сокращенный, актуализированный с учетом ряда происшедших за последний период изменений, вариант изданной в качестве учебного пособия книги "Лицензирование и сертификация в области защиты информации", опубликованной в прошедшем году в МИФИ. Не проходящий и не снижающийся интерес к этой проблематике, несмотря на относительно большой объем публикаций по данному вопросу, объясняется тем, что происходящие в стране процессы существенно затронули проблему организации системы защиты информации во всех ее сферах - разработки, производства, реализации, эксплуатации средств защиты, подготовки соответствующих кадров. Прежние традиционные подходы в современных условиях уже не в состоянии обеспечить требуемый уровень безопасности государственно значимой и частной конфиденциальной информации, циркулирующей в информационно-телекоммуникационных системах страны.

Существенным фактором, до настоящего времени оказывающим значительное влияние на положение дел в области защиты информации, является то, что до начала 90-х годов нормативное регулирование в данной области оставляло желать лучшего. Система защиты информации в нашей стране в то время определялась существовавшей политической обстановкой и действовала в основном в интересах Специальных служб государства, Министерства обороны и Военно-промышленного комплекса. Цели защиты информации достигались главным образом за счет реализации принципа "максимальной секретности", в соответствии с которым доступ ко многим видам информации был просто ограничен. Никаких законодательных и иных государственных нормативных актов, определяющих защиту информационных прав негосударственных организаций и отдельных граждан, не существовало. Средства криптографической защиты информации использовались только в интересах государственных органов, а их разработка была прерогативой исключительно специальных служб и немногих специализированных

государственных предприятий. Указанные предприятия строго отбирались и категорировались по уровню допуска к разработке и производству этих средств. Сами изделия тщательно проверялись компетентными государственными органами и допускались к эксплуатации исключительно на основании специальных заключений этих органов. Любые работы в области криптографической защиты информации проводилась на основании утвержденных Правительством страны специальных секретных нормативных актов, полностью регламентировавших порядок заказа, разработки, производства и эксплуатации шифровальных средств. Сведения о этих средствах, их разработке, производстве, и использовании как в стране, так и за рубежом были строго засекречены, а их распространение предельно ограничено. Даже простое упоминание о криптографических средствах в открытых публикациях было запрещено.

В настоящее время можно отметить, что правовое поле в области защиты информации получило весомое заполнение. Конечно нельзя сказать, что процесс построения цивилизованных правовых отношений успешно завершен и задача правового обеспечения деятельности в этой области уже решена. Важно другое - на наш взгляд, можно констатировать, что уже имеется неплохая законодательная база, вполне позволяющая, с одной стороны, предприятиям осуществлять свою деятельность по защите информации в соответствии требованиями действующих нормативных актов, а с другой - уполномоченным государственным органам на законной основе регулировать рынок соответствующих товаров и услуг, обеспечивая необходимый баланс интересов отдельных граждан, общества в целом и государства.

В последнее время в различных публикациях муссируется вопрос о том, что созданный механизм государственного регулирования в области защиты информации используется государственными органами, уполномоченными на ведение лицензионной деятельности, для зажима конкуренции и не соответствует ни мировому опыту, ни законодательству страны. В этой связи, во-первых, хотели бы отметить, что по состоянию на декабрь месяц 1996 года Федеральным агентством правительственной связи и информации при Президенте Российской Федерации оформлена 71 лицензия на деятельность в области защиты информации. Официально в выдаче лицензии отказано только одной фирме. Еще одному предприятию, кстати, государственному отказано в продлении лицензии

за нарушения условий ее действия. Среди лицензиатов - предприятия различных форм собственности и ведомственной принадлежности, включая такие частные фирмы, как: "Авиателеком", "Аргонавт", "Анкей", "КомФАКС", "Инфотекс" и другие. Полный список лицензий, выданных ФАПСИ публикуется в печати, в том числе и в изданиях фирмы "Гротек".

Кроме того, чтобы остудить бушующие вокруг данной проблемы страсти, считаем полезным подробнее ознакомить читателей с имеющимся опытом зарубежного законодательства и требованиями российских нормативных актов в области защиты информации, в первую очередь, криптографическими методами.

II

Законодательные и административные меры для регулирования вопросов защиты информации на государственном уровне применяются в большинстве научно-технически развитых стран мира. Компьютерные преступления приобрели в странах с развитой информационно-телекоммуникационной инфраструктурой такое широкое распространение, что для борьбы с ними в уголовное законодательство введены специальные статьи.

Первый закон о защите информации был принят в Соединенных Штатах Америки в 1906 году. В настоящее время в США имеется около 500 законодательных актов по защите информации, ответственности за ее разглашение и компьютерные преступления. Проблемы информационной безопасности рассматриваются американской администрацией как один из ключевых элементов национальной безопасности. Национальная политика США в области защиты информации формируется Агентством национальной безопасности (АНБ). При этом наиболее важные стратегические вопросы, определяющие национальную политику в данной сфере, как правило, решаются на уровне Совета национальной безопасности, а решения оформляются в виде директив Президента США. Среди таких директив следует отметить следующие:

директива PD/NSC-24 "Политика в области защиты систем связи"

(1977 год, Д. Картер), в которой впервые подчеркивается необходимость защиты важной несекретной информации в обеспечении национальной безопасности;

директива SDD-145 "Национальная политика США в области безопасности систем связи автоматизированных информационных систем" (1984 год, Р. Рейган), которая стала юридической основой для возложения на АНБ функции по

защите информации и контролю за безопасностью не только в каналах связи, но и в вычислительных и сложных информационно-телекоммуникационных системах. Эта же директива возлагала на АНБ ответственность за сертификацию технологий, систем и оборудования в части защиты информации в информационно-телекоммуникационных системах страны, а также по лицензированию деятельности в области защиты информации.

В период с 1967 года по настоящее время в США принят целый ряд федеральных законов, создавших правовую основу для формирования и проведения единой государственной политики в области информатизации и защиты информации с учетом интересов национальной безопасности страны. Это законы

"О свободе информации" (1967 год), "О секретности" (1974 год), "О праве на финансовую секретность" (1978 год), "О доступе к информации о деятельности ЦРУ" (1984 год), "О компьютерных злоупотреблениях и мошенничестве" (1986 год), "О безопасности компьютерных систем" (1987 год) и некоторые другие.

Правительство США при реализации своей политики в области защиты информации исходит из того, что перехват иностранными государствами конфиденциальной государственной и частной информации, а также больших объемов открытой информации, передаваемых по правительственным и коммерческим сетям телекоммуникаций, после их обработки, сопоставления и объединения разрозненных сведений приведет к раскрытию государственных секретов. Поэтому, начиная с середины 80-х годов, защита линий связи и автоматизированных систем становится важной задачей компетентных государственных органов США.

Закон Соединенных Штатов "Об обеспечении безопасности ЭВМ"

№ HR 145, принятый Конгрессом в мае 1987 года, устанавливает приоритет национальных интересов при решении вопросов безопасности информации (в том числе и частной). Например, данный акт декларирует, что требования государственных органов по обеспечению необходимого уровня защиты информации могут быть распространены на любую "важную информацию". При этом закон устанавливает, что "важной" является такая информация, "потеря которой, неправильное использование, несанкционированное изменение которой или доступ к которой могут привести к нежелательным воздействиям на национальные интересы".

Установлена новая категория информации ограниченного доступа - "несекретная, но важная с точки зрения национальной безопасности". К данной категории отнесена практически вся несекретная информация правительственных ведомств, а также большая часть сведений, циркулирующих или обрабатываемых в информационно-телекоммуникационных системах частных фирм и корпораций, работающих по правительственным заказам.

Национальная инструкция об обеспечении безопасности связи США

№ 6002, принятая в июне 1984 года, устанавливает, что потребности в обеспечении безопасности связи государственных подрядчиков определяются компетентными государственными органами. Эти же органы обеспечивают контроль за соблюдением требований по безопасности связи. Инструкция разрешает использовать государственным подрядчикам шифровальную технику, либо изготовленную по заказу Агентства национальной безопасности, либо прошедшую сертификацию в этом агентстве. Фирмы-изготовители средств шифрования не должны находиться в иностранном владении или под иностранным влиянием. Кроме того, эти фирмы должны быть допущены к работе с секретной информацией установленным порядком. Вывоз любых криптографических устройств из Соединенных Штатов возможен только с разрешения АНБ. При этом директива Президента страны "Об управлении шифрованием в обществе" ("Public Encryption Management") однозначно устанавливает, что вывозимые криптографические средства не должны служить препятствием для органов электронной разведки США при добывании ими информации.

Во Франции государственному контролю подлежат изготовление, экспорт и использование шифровального оборудования. Экспорт возможен только с разрешения Премьер-министра страны, выдаваемого после консультаций со специальным комитетом по военному оборудованию. Импорт шифровальных средств на территорию Французской республики вообще запрещен. Закон объявляет экспорт и снабжение криптографическими средствами без специального разрешения преступлением, которое наказывается штрафом в размере до 500 000 франков или тюремным заключением на срок от 1 до 3 месяцев.

Нормы и требования российского законодательства в области лицензирования и сертификации включают в себя положения ряда нормативных актов Российской Федерации различного уровня. Первым по времени открытым правовым нормативным актом, который бы регулировал вопросы оборота средств криптографической защиты информации, является принятое *28 мая 1991 года постановление Верховного Совета СССР № 2195-1 "О видах деятельности, которыми предприятия вправе заниматься только на основании специальных разрешений (лицензий)".* Этим документом был утвержден перечень отдельных видов деятельности, которыми предприятия на территории страны вправе заниматься только при наличии у них специального разрешения или лицензии. В частности, к таким видам деятельности данное постановление относит и производство, ремонт, реализацию и эксплуатацию шифровальной техники.

19 февраля 1993 года Верховным Советом Российской Федерации был принят закон "О федеральных органах правительственной связи и информации" № 4524-1. Статья 11 данного закона предоставила Федеральному агентству права по определению порядка разработки, производства, реализации, эксплуатации шифровальных средств, предоставления услуг в области шифрования информации, а также порядка проведения работ по выявлению электронных устройств перехвата информации в технических средствах и помещениях государственных структур. Одновременно Федеральному агентству этой статьей дано право осуществлять лицензирование указанных видов деятельности и сертификацию соответствующих товаров и услуг. Пунктом м) той же статьи 11 данного закона Федеральному агентству предоставлено право осуществлять лицензирование и сертификацию телекоммуникационных систем и комплексов высших органов государственной власти Российской Федерации и закрытых (защищенных) с помощью шифровальных средств, систем и комплексов телекоммуникаций органов государственной власти субъектов Российской Федерации, федеральных органов исполнительной власти, а также организаций, предприятий, банков и иных учреждений, расположенных на территории России, независимо от их ведомственной принадлежности и форм собственности. Таким образом, закон Российской Федерации "О федеральных органах правительственной связи и информации" является первым собственно российским правовым нормативным актом, который вводит лицензирование деятельности и сертификацию в области защиты информации и дата его

принятия - 19 февраля 1996г. - является исходной точкой от которой необходимо вести отсчет ограничения прав на занятие предпринимательской деятельностью.

Полномочия по лицензированию деятельности в области защиты информации, содержащей сведения, составляющие государственную тайну, а также по сертификации средств ее защиты предоставлены Федеральному агентству *законом Российской Федерации от 21.07.93 "О государственной тайне" № 5485-1*. Статья 20 этого закона определила государственные органы, ответственные за защиту такой информации. Статья 27 предписывает осуществлять допуск предприятий, учреждений и организаций к работам по созданию средств защиты секретной информации и оказанию услуг по защите сведений, составляющих государственную тайну, путем получения ими лицензий на данную деятельность. Статья 28 устанавливает обязательность сертификации технических средств, предназначенных для защиты секретных сведений, и определяет государственные органы, ответственные за проведение сертификации указанных средств (ФАПСИ, Министерство обороны, Гостехкомиссия и Министерство безопасности, правопреемником которого является ФСБ).

Во исполнение этих законов в августе 1993 года Правительством Российской Федерации принято специальное постановление, которое полностью определяет порядок создания и использования криптографических (шифровальных) средств, предназначенных для защиты информации, содержащей сведения, составляющие государственную тайну, начиная от стадии подготовки технического задания на проведение научно-исследовательских работ до серийного производства и установки шифровальной техники в сложные закрытые (защищенные) системы и комплексы обработки, хранения и передачи информации.

Кроме того, в соответствии с упомянутыми законами, а также на основании *закона Российской Федерации от 10.06.93 "О сертификации продукции и услуг"*

№ 5151-1 ФАПСИ 15 ноября 1993 года зарегистрировало в Госстандарте России *"Систему сертификации средств криптографической защиты информации" РОСС.RU.0001.030001*. Данный документ определил организационную структуру системы сертификации шифровальных средств ФАПСИ, а также установил основные правила проведения сертификационных исследований и испытаний

криптографических средств защиты информации и закрытых с их помощью систем и комплексов обработки, хранения и передачи информации.

В начале 1994 года Президентом и Правительством был принят пакет нормативных актов, определивших порядок импорта и экспорта шифровальных средств и нормативно-технической документации к ним на территории Российской Федерации. В первую очередь, это *распоряжение Президента России от 11 февраля 1994 г. № 74-П "О контроле за экспортом из Российской Федерации отдельных видов сырья, материалов, оборудования, технологий и научно-технической информации, которые могут быть применены при создании вооружения и военной техники"*. Данным распоряжением утвержден соответствующий перечень, в котором, в частности, указывается, что аппаратура, узлы, компоненты, программное обеспечение и технология производства, специально разработанные или модифицированные для использования в криптографии или выполнения криптоаналитических функций, подлежат экспортному контролю. Во-вторых, *постановление Правительства от 15.04.94 № 331 "О внесении дополнений и изменений в постановления Правительства Российской Федерации от 06.11.92 № 854 "О лицензировании и квотировании экспорта и импорта товаров (работ, услуг) на территории Российской Федерации" и от 10.12.92 № 959 "О поставках продукции и отходов производства, свободная реализация которых запрещена"*. И, наконец, - *постановление от 01.07.94 № 758 "О мерах по совершенствованию государственного регулирования экспорта товаров и услуг"*. 31 октября 1996г. этот перечень был дополнен *постановлением Правительства N 1299*, которым утверждено Положение "О порядке лицензирования экспорта и импорта товаров (работ, услуг) в Российской Федерации".

Перечисленные документы установили в том числе, что ввоз и вывоз средств криптографической защиты информации (шифровальной техники) и нормативно-технической документации к ней в стране может осуществляться **исключительно** на основании лицензии Министерства внешних экономических связей Российской Федерации, выдаваемой на основании решения ФАПСИ о выдаче лицензии. Кроме того, данные документы определили общий порядок выдачи экспортных лицензий на шифровальные средства, направленный на предотвращение утечки секретных сведений и технологий при вывозе из страны средств защиты информации.

Предоставленные Федеральному агентству законами "О федеральных органах правительственной связи и информации" и "О государственной тайне" права по определению порядка осуществления и лицензированию деятельности в области защиты информации нашли свое отражение в *"Положении о государственном лицензировании деятельности в области защиты информации"*, которое утверждено 27 апреля 1994 года совместным решением № 10 ФАПСИ и Гостехкомиссии России, разграничившим сферы компетенции двух этих ведомств и определившим механизм практического лицензирования, действующий по настоящее время.

Обязательное государственное лицензирование деятельности в области защиты информации криптографическими методами, а также в области выявления электронных устройств перехвата информации в технических средствах и помещениях государственных структур введено *постановлением Правительства от 24.12.94 № 1418 "О лицензировании отдельных видов деятельности"*. Данное постановление распространяет механизм обязательного лицензирования на все виды деятельности в области криптографической защиты информации, независимо от ее характера и степени секретности, на все субъекты этой деятельности, независимо от их организационно-правовой формы, включая и физических лиц.

Новым шагом в деле правового обеспечения деятельности в области защиты информации явилось принятие Федеральным собранием России *Федерального закона "Об информации, информатизации и защите информации" от 20.02.95 № 24-ФЗ*. Данный закон впервые официально вводит понятие "конфиденциальной информации", которая рассматривается как документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, и устанавливает общие правовые требования к организации защиты такой информации в процессе ее обработки, хранения и циркуляции в технических устройствах и информационных и телекоммуникационных системах и комплексах и организации контроля за осуществлением мероприятий по защите конфиденциальной информации. При этом следует подчеркнуть, что Закон не разделяет государственную и частную информацию как объект защиты в том случае, если доступ к ней ограничивается.

Кроме того, закон определяет на государственно-правовом уровне электронную цифровую подпись как средство защиты информации от

несанкционированного искажения, подмены (имитозащиты) и подтверждения подлинности отправителя и получателя информации (аутентификации сторон). В соответствии со статьей 5 "юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью". При этом "юридическая сила электронной цифровой подписи признается при наличии в автоматизированной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования". Далее закон раскрывает требования, предъявляемые к специализированным программно-техническим средствам, реализующим электронную цифровую подпись, и порядку их использования в информационно-телекоммуникационных системах.

Так, статья 19 закона "Об информации, информатизации и защите информации" устанавливает обязательность сертификации средств обработки и защиты документированной информации с ограниченным доступом, предназначенных для обслуживания граждан и организаций, а также обязательность получения лицензий для организаций, осуществляющих проектирование и производство средств защиты информации.

Статья 20 определяет основные цели защиты информации. В соответствии с этой статьей таковыми, в частности, являются: предотвращение утечки, хищения, утраты, искажения и подделки информации; предотвращение угроз безопасности личности, общества и государства; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных сведений; сохранение государственной тайны и конфиденциальности информации.

Пункт 3 статьи 21 возлагает контроль за соблюдением требований к защите информации, за эксплуатацией специальных средств защиты информации, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом, в негосударственных структурах на органы государственной власти.

Очень важна статья 22, которая определяет права и обязанности субъектов в области защиты информации. В частности, пункты 2 и 5 обязывают владельца информационной системы обеспечивать необходимый уровень защиты

конфиденциальной информации и оповещать собственников информационных ресурсов о фактах нарушения режима защиты информации. Пунктом 3 риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения и защиты, возлагается на собственника (владельца) систем и средств. Риск, связанный с использованием информации, полученной из таких систем, относится на потребителя информации. Пункт 4 устанавливает право собственника документов или информационной системы обращаться в организации, осуществляющие сертификацию средств защиты таких систем, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций

Статья 23 Закона "Об информации, информатизации и защите информации" посвящена защите прав субъектов в сфере информационных процессов и информатизации. Статья устанавливает, что защита прав субъектов в данной сфере осуществляется судом, арбитражным судом и третейскими судами, которые могут создаваться на постоянной или временной основе.

Подписанный 3 апреля 1995 года *Указ Президента Российской Федерации № 334 "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации"* запрещает любую деятельность, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных средств, предоставлением услуг в области шифрования информации, без лицензии ФАПСИ. Пункты 2, 3 данного документа устанавливают обязательное использование исключительно сертифицированных средств защиты информации во всех государственных структурах, в том числе и в государственных банках Российской Федерации, на предприятиях, работающих по государственному заказу, а также на предприятиях и в организациях при их информационном взаимодействии с Центральным банком России и его структурными подразделениями. Таким образом, обязательность сертификации распространяется теперь не только на средства защиты информации, содержащей сведения, составляющие государственную тайну, но и на средства защиты любой государственно значимой информации независимо от грифа ее секретности. Кроме того, Указ формирует механизм реализации перечисленных выше законодательных актов, возлагая ответственность за их выполнение на ФАПСИ, а также правоохранительные, таможенные и налоговые органы страны.

В течение первой половины 1995 года Правительством Российской Федерации во исполнение закона "О государственной тайне" приняты постановление от 15 апреля 1995 года № 333 "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны" и постановление от 26.06.95 № 608 "О сертификации средств защиты информации".

Указанные постановления формируют механизм получения предприятиями и организациями, независимо от их организационно-правовой формы, лицензии на право осуществления любой деятельности, связанной с информацией, составляющей государственную тайну, а также общий порядок сертификации средств защиты, предназначенных для защиты секретной информации.

В частности, пункт 2 Положения, утвержденного постановлением

№ 333, устанавливает органы, уполномоченные на ведение лицензионной деятельности, связанной с проведением работ со сведениями, составляющими государственную тайну. Таковыми являются Федеральная служба безопасности России и ее территориальные органы, ФАПСИ, Гостехкомиссия и Служба внешней разведки. Тем же пунктом определяются полномочия перечисленных ведомств:

выдача лицензий по допуску предприятий и организаций к проведению работ, связанных с использованием секретных сведений, на территории Российской Федерации возлагается на органы ФСБ, а за границей - СВР России;

выдача лицензий на право создания средств защиты информации возлагается на Гостехкомиссию и ФАПСИ;

выдача лицензий на право осуществления мероприятий и(или) оказания услуг в области защиты государственной тайны возлагается на ФСБ и ее территориальные органы, Гостехкомиссию, ФАПСИ и СВР.

Постановление от 15.04.95 № 333 устанавливает, что лицензия на право деятельности по проведению работ, связанных с использованием сведений, составляющих государственную тайну, с созданием средств защиты информации и оказанием услуг по защите государственной тайны, может быть выдана предприятию или организации, независимо от формы его собственности, исключительно на основании результатов специальной экспертизы заявителя, в

ходе которой будет установлено наличие на данном предприятии всех необходимых условий для сохранения доверенных ему секретных сведений, и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну.

Постановление от 26 июня 1995 года № 608 устанавливает общие принципы организации систем сертификации средств защиты информации, содержащей сведения, составляющие государственную тайну, всеми ведомствами Российской Федерации, наделенными законом правом проводить подобную сертификацию. Статьи Положения определяют участников системы сертификации средств защиты информации, их права и обязанности; схемы проведения сертификационных испытаний; порядок выдачи, приостановления и аннулирования сертификатов; порядок оплаты услуг по сертификации, контроля за качеством сертифицированных изделий, а также ответственность сторон за выполнение ими своих обязательств в системе сертификации. Кроме того, данным Положением к средствам защиты информации отнесены и средства контроля эффективности защиты информации.

Принятый Государственной Думой *Федеральный закон "Об участии в международном информационном обмене"* от 5 июня 1996 года N 85-ФЗ определяет необходимость сертификации средств международного информационного обмена и необходимость лицензирования деятельности в области международного информационного обмена при работе с конфиденциальной информацией. Закон предоставляет ФАПСИ право участвовать в определении перечней документированной информации, вывоз которой из Российской Федерации, и иностранных информационных продуктов, ввоз которых в Российскую Федерацию, ограничен, определять порядок лицензирования деятельности в области международного информационного обмена при работе с конфиденциальной информацией, а также определять порядок сертификации средств и аттестования систем международного информационного обмена.

Перечисленные нормативные акты определили полномочия и компетенцию ФАПСИ в сфере лицензирования деятельности в области защиты и сертификации средств защиты информации.

Лицензированию Федеральным агентством в соответствии с его компетенцией подлежит деятельность по следующим направлениям:

создание средств защиты информации;

осуществление мероприятий и оказание услуг по защите государственной тайны;

деятельность, связанная с шифровальными средствами;

предоставление услуг в области шифрования информации;

выявление технических устройств скрытого съема информации, электронных закладных устройств и программных закладок в технических средствах и помещениях государственных структур;

создание систем и комплексов телекоммуникаций органов государственной власти Российской Федерации;

создание закрытых (защищенных) с использованием шифровальных средств систем и комплексов телекоммуникаций;

создание и реализация средств выявления технических устройств скрытого съема информации, электронных закладных устройств и программных закладок.

Указанные направления включают определенное множество отдельных видов деятельности к которым относятся разработка, производство, реализация (продажа), эксплуатация, монтаж, установка (инсталляция), наладка, сертификационные испытания, ввоз в страну, вывоз из страны и другие..

Сертификации Федеральным агентством в соответствии с его компетенцией подлежат:

средства (системы, комплексы) криптографической защиты информации;

средства выявления закладных устройств и программных закладок;

защищенные технические средства обработки информации;

закрытые (защищенные) информационные системы и комплексы телекоммуникаций.

В своей деятельности по лицензированию и сертификации ФАПСИ руководствуется положениями указанных выше нормативных актов и строго придерживается предоставленными ему ими правами и полномочиями.

III

Лицензирование и сертификация относятся к таким предметным областям, где отсутствуют необходимый набор формальных правил и критериев регулирования и оценки протекающих процессов и происходящих явлений.

Рассмотрение и анализ в таких случаях осуществляют на качественном уровне. В качестве критерия используется смысловое содержание понятий, а выводы во многом определяются правильностью понимания этих терминов и однозначностью их трактовки.

В этой связи необходимо отметить, что на данный момент времени в рассматриваемой нами области отсутствует единый, принятый во всей стране, понятийный аппарат (т.е. четкая система взаимоувязанных терминов и понятий). Многие понятия и термины, вводимые принимаемыми законами и иными нормативными актами, используемые различными органами, работающими в сфере защиты информации, или отдельными авторами, публикующими материалы по данной тематике, носят неоднозначный, противоречивый характер. В одни и те же термины часто вкладывается различное смысловое содержание. Манипулирование, а в отдельных случаях прямое спекулирование терминами и понятиями происходит зачастую из конъюнктурных соображений. Можно привести множество примеров, иллюстрирующих сказанное, однако авторы не ставят себе такой задачи. Наша цель заключается довести до широкого круга специалистов суть и определение понятий в данной области так, как это отражено в нормативных актах ФАПСИ или официально трактуется Федеральным агентством (в случае наличия четких и ясных формулировок).

Сложность положения с определением понятийного аппарата усугублялась тем обстоятельством, что многие основополагающие понятия и термины, используемые в сфере защиты информации, носили до последнего времени закрытый характер и пока не введены или не определены на общегосударственном уровне в открытом виде. Это относится и к таким, например, понятиям, как "*шифрование*", "*защищенные технические средства*". Не имеют общепринятого определения, например, и такой основополагающий термин как "*вид деятельности*".

Приводимые ниже определения основных понятий может быть, не лишены известных недостатков, но сложились таковыми в результате многолетней практической деятельности подразделений Федерального агентства как собственно в сфере защиты информации, так и в области определения качества соответствующих товаров и услуг. Вообще говоря, вопросы лицензирования деятельности в области защиты информации и сертификации качества соответствующих товаров и услуг не являются совсем новыми для Федерального

агентства. Компетентные подразделения ФАПСИ фактически всегда осуществляли лицензирование деятельности и сертификацию средств защиты информации, составляющей государственную тайну, правда, в несколько иной форме. Эта работа проводилась путем категорирования и строгого отбора разработчиков и производителей средств защиты информации, а также путем экспертизы результатов их работы и выдачи заключений на основании утверждаемых правительством специальных Положений. Однако термины *лицензирование* и *сертификация* при этом не использовались и не упоминались.

Учитывая, что предметом данной работы являются не просто *лицензирование* и *сертификация* сами по себе, а *лицензирование* и *сертификация* в области защиты информации, начнем с определения ряда основных понятий данной сферы деятельности.

Защита информации - комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.

Средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты информации, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Эффективность защиты информации - степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты.

Контроль эффективности защиты информации - проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты.

Безопасность информации (информационная безопасность) - состояние информации, информационных ресурсов и информационных и телекоммуникационных систем, при котором с требуемой вероятностью обеспечивается защита информации.

Требования по безопасности информации - руководящие документы ФАПСИ, регламентирующие качественные и количественные критерии безопасности информации и нормы эффективности ее защиты.

Криптографическая защита - защита данных при помощи криптографического преобразования преобразования данных.

Криптографическое преобразование - преобразование данных при помощи шифрования и (или) выработки имитовставки.

Шифрование - процесс зашифрования или расшифрования.

Зашифрование данных - процесс преобразования открытых данных в зашифрованные при помощи шифра.

Расшифрование данных - процесс преобразования зашифрованных данных в открытые при помощи шифра.

Шифр - совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей.

Имитовставка - отрезок информации фиксированной длины, полученной по определенному правилу из открытых данных и ключа.

Ключ - конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

Приведенные определения, связанные с понятиями криптографического преобразования и шифрования, даны в строгом соответствии с широкоизвестным ГОСТ 28147-89. Анализ этих определений позволяет сформулировать три критерия, которые в первом приближении могут быть использованы в большинстве практических приложений для отнесения средств защиты информации к классу криптографических:

Первый - наличие некоторого математического преобразования данных.

Второй - наличие секретного параметра этого преобразования - ключа, с мощностью ключевого множества большего или равного двум.

Третий - обратимость используемого математического преобразования данных.

При этом подчеркнем еще раз - математическое преобразование и реализованное на его базе средство защиты может быть отнесено или не отнесено к классу криптографических только на основании результатов экспертизы ФАПСИ.

Шифровальные средства (средства криптографической защиты информации):

реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для защиты информации (в том числе и входящие в системы и комплексы защиты информации от несанкционированного доступа), циркулирующей в технических средствах, при ее обработке, хранении и передаче по каналам связи, включая шифровальную технику;

реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и электронной цифровой подписи;

аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для изготовления и распределения ключевых документов, используемых в шифровальных средствах, независимо от вида носителя ключевой информации;

ручные шифры, документы кодирования и другие носители ключевой информации.

Скремблер - шифровальное средство, предназначенное для защиты информации только от непосредственного прослушивания, просмотра или прочтения.

Маскиратор - средство защиты информации, реализующее математический алгоритм преобразования информации, не использующее секретного ключа или передающее (хранящее) его вместе с сообщением.

Техническое средство обработки информации - техническое средство, предназначенное для приема, накопления, хранения, поиска, преобразования, отображения и передачи информации по каналам связи.

Защищенные (закрытые) системы и комплексы телекоммуникаций - системы и комплексы телекоммуникаций, в которых обеспечивается защита информации с использованием шифровальных средств, защищенного оборудования и организационных мер.

Особо прокомментируем определение шифровального средства. Во-первых, любое средство, в котором реализован криптографический алгоритм, работающий под управлением некоторого тайного элемента, называемого ключом, является шифровальным средством, и, следовательно, термины "шифровальные средства" и "криптографические средства защиты" (средства

криптографической защиты) являются синонимами. Во-вторых, средство относится к категории шифровальных независимо от его назначения и способа реализации. Таким образом, реализующие криптографические алгоритмы средства, используемые для закрытия информации в канале связи, имитозащиты сообщения, аутентификации пользователей, средства электронной цифровой подписи, средства закрытия таблицы паролей и т.д. являются шифрсредствами. В-третьих, приведенное определение охватывает не только технические шифрсредства, но и ручные шифры, а также ключевую информацию, предназначенную для шифрования.

Переходя теперь к определению таких понятий как "*лицензирование*" и "*сертификация*" в области защиты информации, отметим, что зачастую эти термины просто путают (не говоря уже об их ошибочном понимании или трактовке). Путают и объекты, к которым они относятся, и, как следствие, нормы, относящиеся к одному понятию, приписываются другому.

Лицензирование - это процесс, осуществляемый в отношении таких категорий, как "*деятельность*" (направления, виды деятельности) и "*субъект*" (физическое лицо, предприятие, организация или иное юридическое лицо), когда некоторый субъект в результате проведения комплекса мероприятий, состав, правила и порядок осуществления которых предписываются законодательными и нормативными актами, получает право на осуществление определенного вида деятельности. Это право закрепляется и оформляется в виде официальных документов, состав, виды и статус которых также предписываются нормативными актами. При за органом, уполномоченном на проведение лицензионной деятельности, закрепляется право на осуществление контроля за деятельностью лицензиата. Здесь термины "деятельность", "право", "правило", "мероприятие", "статус" имеют общепризнанный смысл, и их определения можно почерпнуть в любом толковом словаре. Важно подчеркнуть, и это вытекает из описанной нами формулы, что активную роль в процессе лицензирования играют обе стороны: орган, наделяющий (передающий) кого-либо правом деятельности, и субъект, получающий указанное право. Получить право на осуществление деятельности, подлежащей лицензированию, может не каждый (иначе процесс лицензирования вообще теряет смысл), а лишь субъект, отвечающий определенным критериям, которые заранее определяются правилами проведения лицензирования и

являющимися их неотъемлемой частью требованиями к предприятию-заявителю. Таким образом, субъектом лицензирования становится лишь то физическое или юридическое лицо, которое представляет все необходимые и правильно оформленные документы и удовлетворяет соответствующим критериям. В данной области мы оперируем следующими основными терминами (здесь и далее приводятся термины, определенные в соответствии с приведенными выше Положениями о лицензировании).

Лицензирование в области защиты информации - деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации, и осуществлении контроля за лицензиатом.

Лицензия ФАПСИ - надлежащим образом оформленный официальный документ, который дает право на осуществление указанного в нем вида деятельности в области защиты информации в течение установленного срока, а также определяет условия его осуществления.

Решение ФАПСИ о выдаче лицензии - надлежащим образом оформленный официальный документ, который дает возможность оформления лицензии на указанный в нем вид деятельности с учетом оговоренных в нем условий.

Заявитель в области защиты информации - предприятие, представившее документы, необходимые для получения лицензии или решения о выдаче лицензии.

Требования к заявителю - комплекс определенных Правительством Российской Федерации или ФАПСИ условий, норм и критериев, регламентирующих возможности и деятельность лицензиата, уровень производственной, испытательной, технологической, нормативно-методической базы предприятия, научный и инженерно-технический уровень персонала, а также мероприятия по обеспечению сохранности доверяемой конфиденциальной информации, соответствие которым проверяется в ходе специальной экспертизы заявителя.

Лицензиат - сторона, получившая право на проведение работ в области защиты информации.

Сертификация - это процесс, осуществляемый в отношении такой категории, как "изделие" (товар, средство), когда в результате выполнения комплекса мероприятий, определенных правилами и порядком ее проведения, устанавливается, удостоверяется или подтверждается качество изделия. Таким

образом, *сертификация* есть деятельность некоторой третьей стороны, независимой от изготовителя (продавца) и потребителя продукции или услуг, по подтверждению соответствия этих продукции или услуг установленным требованиям.

В рассматриваемой области - это подтверждение соответствия средства защиты информации как определенной конкретной технической реализации некоторого алгоритма заданным стандартам на этот алгоритм или описанию алгоритма, а также удовлетворения этим средством установленным требованиям по безопасности. Особо при этом следует подчеркнуть три момента. Во-первых, процедура сертификации осуществляется в отношении только технических средств или технической части системы защиты, включающей в обязательном порядке и организационно-технические и организационные средства и меры. Во-вторых, сертификации может подвергаться только готовое, законченное изделие. В-третьих, требования по безопасности включают количественные критерии и нормы, и поэтому, в отличие от других процедур, входящих в процесс лицензирования и сертификации, процедуры сертификационных испытаний базируются на формальных методах и развитой метрологической базе.

Многие термины, используемые в области сертификации, определены законом Российской Федерации "*О сертификации продукции и услуг*". Учитывая это, в данной работе представляется целесообразным дать определения понятий, связанных с рассматриваемой проблематикой.

Сертификация средств защиты информации - деятельность по подтверждению соответствия средств защиты информации требованиям государственных стандартов и требованиям по безопасности информации, предъявляемым

ФАПСИ.

Сертификат на средство защиты информации - надлежащим образом оформленный документ, выданный по правилам системы сертификации и подтверждающий соответствие средства защиты информации требованиям по безопасности информации, предъявляемым ФАПСИ.

Из изложенного выше видно, что *лицензирование* и *сертификация* представляют собой совершенно различные процессы с точки зрения их объектов и используемых методов. Однако с точки зрения технологии их осуществления эти процессы во многом идентичны: и в том и другом случае проверяется

соответствие (удовлетворение) определенным требованиям, и в том и другом случае выходные документы оформляются и выдаются на основании заключений экспертных организаций, специально уполномоченных на проведение подобных экспертиз. Более того, в ряде случаев эти процессы тесно переплетаются, поскольку для выдачи лицензии на некоторые виды деятельности или для принятия решения о выдаче лицензии на ввоз или вывоз шифрсредств, требуется проведение технической экспертизы собственно заявляемых к ввозу(вывозу) изделий.

Необходимо отметить, что наряду с процессами лицензирования и сертификации в области защиты информации достаточно широкое распространение получил процесс *аттестации (аттестования)*.

Понятие "*аттестация (аттестование)*" близко по своей сути к понятию "*сертификация*", и поэтому часто происходит подмена одного из этих понятий другим.

Аттестация - это процесс, осуществляемый в отношении такой категории, как "*объект информатики*", в результате которого удостоверяется возможность обработки на данном конкретном объекте информатики информации с ограниченным доступом определенной категории (необходимая категория определяется собственником, владельцем, пользователем информации в соответствии с действующим законодательством). Схожесть процессов сертификации и аттестации заключается в том, что в обоих случаях используются одни и те же требования и нормы и объектом этих процессов зачастую выступают технические средства обработки информации. Однако различия, и существенные, состоят в том, что при *аттестации* оцениваются в совокупности все средства защиты информации, включая принятые организационно-технические и организационные меры, а также конкретные условия эксплуатации рассматриваемого объекта. При этом *объектом аттестации* выступает *объект информатики*, понимаемый в широком смысле как совокупность помещений с расположенными в них конкретными техническими средствами, которые обслуживаются данным персоналом в соответствии с порядком, предписанным нормативно-технической документацией. В узком смысле под *объектом информатики* может пониматься конкретное, единственное (с конкретными заводскими номерами) техническое средство. Подчеркнем, что данное техническое средство защиты может выступать как в качестве объекта

сертификации, так и в качестве объекта аттестации, поскольку именно это в ряде случаев вызывает непонимание и приводит к путанице и ошибкам. В первом случае, при сертификации, речь идет о типовом образце изделия или типовых испытаниях. Во втором, при аттестации, речь идет о конкретном образце, предназначенном для эксплуатации в определенных условиях с заданным конкретным расположением относительно других технических средств в определенном помещении. Техническое средство обработки, имеющее *аттестат на соответствие некоторой категории, является защищенным*.

Данный блок понятий включает следующие определения:

аттестация объекта в защищенном исполнении - официальное подтверждение наличия на объекте информатики условий, обеспечивающих выполнение установленных требований по безопасности информации;

объекты информатики - автоматизированные системы различного назначения, системы телекоммуникаций, отображения и размножения вместе с помещениями, в которых они установлены, а также отдельные технические средства обработки информации и помещения, предназначенные для ведения конфиденциальных переговоров;

аттестат соответствия - документ, оформленный по правилам системы аттестации, подтверждающий, что объект информатики соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации;

защищенное техническое средство обработки информации - техническое средство обработки информации, удовлетворяющее требованиям нормативно-технических документов по безопасности информации.

Важным моментом, на который необходимо обратить внимание в последнем определении, является то, что *защищенным* считается не *только техническое средство обработки информации*, в которое внедрены дополнительные средства защиты, но и средство, *техническое исполнение* которого удовлетворяет действующим нормам.

В определении понятия "*аттестат соответствия*" используется термин "иные нормативно-технические документы по безопасности информации", под которыми, кроме требований по безопасности информации, понимаются предписания на экранирование помещений, предписания на размещение технических средств, правила их эксплуатации и другие документы аналогичного характера.

В заключение данного раздела отметим, что системы лицензирования и сертификации являются составной частью государственной системы защиты информации, под которой понимается совокупность федеральных и иных органов управления и взаимоувязанных правовых, организационных и технических мер, осуществляемых на различных уровнях управления и реализации информационных отношений и направленных на обеспечение безопасности информации.

IV

Данный раздел посвящен изложению основных принципов и правил функционирования системы лицензирования ФАПСИ, общего порядка и особенностей осуществления лицензирования заявителей в области защиты информации в рамках компетенции ФАПСИ, а также рассмотрению подлежащих лицензированию видов деятельности и требований, предъявляемых к предприятиям-заявителям.

В основе любой системы лежит определенный набор аксиом и постулатов, на которых эта система базируется. Жизнеспособность системы и ее эффективность определяются тем, насколько адекватно этот набор аксиом и постулатов отражает сложившиеся реалии и учитывает потребности той сферы жизнедеятельности, в которой эта система функционирует. Другим необходимым условием, которым необходимо руководствоваться при выборе этих аксиом, является взаимоувязанность и непротиворечивость их между собой. Третьим условием, определяющим соответствующий выбор базовых постулатов, являются их возможности способствовать достижению целей, стоящих перед системой. И, наконец, четвертым условием является учет специфики и особенностей предметной области, в которой функционирует данная система лицензирования, по отношению к другим, аналогичного характера системам.

Приводимые ниже совокупности правил и принципов, положенных в основу своей деятельности ФАПСИ по лицензированию в области защиты информации и построения соответствующей системы, отвечают, на наш взгляд, указанным критериям.

Рассмотрим правила построения и функционирования системы лицензирования ФАПСИ, вытекающие из приведенных выше нормативных актов и

основанные на правах и полномочиях, предоставленных ими Федеральному агентству.

1. Лицензирование в области защиты информации является обязательным.

Данное правило устанавливает, что для занятия деятельностью в области защиты информации одного желания мало и необходимо получение права на ее осуществление. Причем распространяется это требование на все без исключения направления и отдельные виды деятельности. Поскольку не существует определений понятий "*направление*" и "*отдельный вид деятельности*", они вводятся в виде перечисления в соответствующих нормативных актах.

2. Деятельность в области защиты информации физических и юридических лиц, не прошедших лицензирование, запрещена.

Из содержания данного правила вытекает, что субъекты, не получившие право на осуществление деятельности в области защиты информации и продолжающие ее осуществлять, нарушая установленный порядок, занимаются тем самым *противоправной деятельностью*. В отношении таких субъектов могут быть применены санкции, предусмотренные действующим Гражданским кодексом и законодательством об административной и уголовной ответственности.

3. Лицензии ФАПСИ и решения ФАПСИ о выдаче лицензии на право осуществления деятельности в области защиты информации, лицензирование которой относится к компетенции Федерального агентства, выдаются, в основном, юридическим лицам - предприятиям, организациям и учреждениям, независимо от их организационно-правовой формы (далее - предприятия).

Данное правило, однако, лишь на первый взгляд ущемляет интересы физических лиц, которым не предоставляются права на промышленную, коммерческую деятельность, связанную с шифровальными средствами. Включение данного постулата обусловлено рядом факторов. Во-первых, разработка (производство, монтаж, наладка и т.д.) шифровальных средств требует участия высококлассных специалистов разного профиля. Во-вторых, требованиям, предъявляемым ФАПСИ к заявителю, физическое лицо удовлетворить не в состоянии. В-третьих, для проведения работ в этой области необходимо, зачастую, обеспечение выполнения режимных требований и (для ознакомления, например, с нормами требований по безопасности) наличия допуска к сведениям, составляющим государственную тайну. *Лицензии выдаются конкретным юридическим лицам - предприятиям, а не министерствам, ведомствам*

или ассоциациям в целом. Если разрешаемая в лицензии деятельность не является для лицензиата основной, то в лицензии указывается структурное подразделение, которому предоставляется право осуществления указанного в лицензии вида деятельности.

4. *Лицензии ФАПСИ и решения ФАПСИ о выдаче лицензии выдаются только предприятиям, зарегистрированным на территории Российской Федерации.*

5. *Лицензия ФАПСИ выдается только на основании результатов специальной экспертизы заявителя на соответствие требованиям к предприятию на право деятельности в области защиты информации по заявленному направлению работ и аттестации руководителя предприятия или лиц, уполномоченных им для руководства лицензируемой деятельностью.*

Данное положение устанавливает одну из основных норм, определяющих сущностные и процедурные аспекты системы лицензирования ФАПСИ: *лицензия может быть выдана не каждому заявителю, то есть предприятию, подавшему все необходимые и правильно оформленные документы, а только предприятию, обладающему соответствующими возможностями, достаточными для осуществления заявленных видов деятельности. Проверка возможностей предприятия и осуществляется в ходе специальной экспертизы путем экспертных оценок специалистами специально создаваемых, с учетом профиля заявляемых видов деятельности, комиссий факта удовлетворения требованиям, предъявляемым к предприятиям. С данными требованиями заявитель может быть ознакомлен в Лицензионном центре ФАПСИ. Кроме того, по результатам специальной экспертизы заявителя определяются состав и конкретная формулировка разрешенных видов деятельности, а также условия их осуществления. Уточнение формулировок для различных видов деятельности и заявителей может быть проведено с учетом следующих факторов:*

уровня конфиденциальности защищаемой информации;

уровня секретности сведений, используемых при осуществлении заявляемой деятельности;

типа используемого криптографического алгоритма;

способа технической реализации изделия;

уровня квалификации персонала;

назначения изделия, наличия или отсутствия сертификата на него;

страны - производителя изделия;

категории помещений и технических средств.

6. Решение ФАПСИ о выдаче лицензии дается предприятию, подавшему заявление на его получение, на основании результатов технической экспертизы изделия и(или) специальной экспертизы заявителя.

Основными задачами технической экспертизы являются установление соответствия предъявляемого изделия заявляемым характеристикам (классу, типу шифровальных средств) и проверка возможного использования в коммерческих шифрсредствах алгоритмов и способов их реализации, составляющих государственную тайну.

7. Лицензия, выданная ФАПСИ, действует на всей территории Российской Федерации, если иное не оговорено в ней особо.

Могут, например, налагаться следующие ограничения:

для региональных представителей, работающих по договорам на реализацию шифрсредств, - в рамках сферы их деятельности;

для фирм-разработчиков - разработка криптографических средств защиты и защищенных средств и систем в интересах региональных государственных и коммерческих структур.

8. Лицензии ФАПСИ и решения ФАПСИ о выдаче лицензии подписываются генеральным директором Федерального агентства или лица, его замещающего, и заверяются гербовой печатью ФАПСИ.

9. Передача лицензии другим юридическим лицам запрещена.

10. Лицензия имеет ограниченный срок действия, по истечении которого осуществляется переоформление лицензии в порядке, предусмотренном для ее выдачи.

Данные нормы определены постановлением Правительства Российской Федерации от 24.12.94 № 1418 для всех систем лицензирования.

11. Лицензирование осуществляется на платной основе.

Размер платы за рассмотрение заявления и за выдачу лицензии фиксирован. Размер платы за специальную экспертизу определяется договором на ее проведение.

12. Для получения лицензии или решения о выдаче лицензии предприятие обязано представить определенный перечень документов, состав которых определяется нормативными актами Правительства Российской Федерации и ФАПСИ.

Представляемые заявителем документы регистрируются в уполномоченном подразделении Федерального агентства по мере их поступления. *Заявление регистрируется только при наличии всех требуемых для оформления лицензии документов.*

13. *Рассмотрение заявления и специальная экспертиза должны проводиться в сроки, ограниченные соответствующими нормативными актами.*

На настоящий момент продолжительность рассмотрения заявления установлена сроком 30 суток с момента поступления всех необходимых документов (с возможностью увеличения этого срока в отдельных случаях еще максимум на 60 суток). Специальная экспертиза имеет аналогичную продолжительность с момента заключения договора на ее проведение.

14. *Отказ заявителю в выдаче лицензии должен быть мотивирован.*

Заявителю может быть отказано в получении лицензии в следующих случаях:

при наличии в документах, представленных заявителем, недостоверной или искаженной информации;

отрицательного заключения по результатам специальных экспертиз, установивших несоответствие условиям, необходимым для осуществления заявленного вида деятельности и условиям безопасности;

отрицательного заключения по результатам аттестации руководителя предприятия или лица, уполномоченного им на ведение лицензируемой деятельности;

отрицательного заключения по результатам технических экспертиз.

15. *При ликвидации предприятия выданная лицензия теряет юридическую силу.*

В случае реорганизации предприятия, изменения его дислокации или наименования юридического лица, утраты лицензии осуществляется ее переоформление.

Переоформление лицензии в указанных случаях, за исключением изменения наименования юридического лица, осуществляется в порядке, предусмотренным для ее выдачи.

16. *Выданная лицензия может быть приостановлена или аннулирована.*

Приостановление или аннулирование лицензии осуществляется в случаях: представления лицензиатом соответствующего заявления;

обнаружения недостоверных данных в документах, представленных для получения лицензии;

нарушения лицензиатом условий действия лицензии;

невыполнения лицензиатом предписаний или распоряжений государственных органов или приостановления ими деятельности предприятия в соответствии с законодательством Российской Федерации;

ликвидации предприятия.

Приостановление действия лицензии влечет за собой прекращение деятельности лицензиата по виду деятельности (работ, услуг), указанному в лицензии, до устранения выявленных нарушений.

17. Решение ФАПСИ о выдаче лицензии на ввоз(вывоз) шифровальных средств выдается только на конкретную партию изделий. Наличие заключенных договоров не является основанием для выдачи положительного решения о возможности ввоза(вывоза) шифровальных средств.

Данные нормы соответствуют установленному порядку внешнеэкономической деятельности. Заключаемые договора, как правило, содержат статью, учитывающую форс-мажорные обстоятельства, предусматривающие возможный отказ уполномоченных государственных органов в выдаче лицензии на ввоз(вывоз) шифровальных средств. Конкретная партия товара определяется объемом, этапностью и сроками поставок, оговоренных конкретным договором.

Деятельность по лицензированию в области защиты информации осуществляется на основании следующих принципов:

1. Соответствия действующим российским законодательным и нормативным актам.

2. Системного и комплексного подхода к решению вопросов лицензирования и сертификации.

3. Обеспечения надежной защиты информации, составляющей государственную тайну или иной конфиденциальной информации.

4. Дифференцированного подхода к отдельным видам деятельности и средствам защиты.

5. Наложения на лицензиата обязательств по выполнению требований Российского законодательства и иных нормативных актов в области защиты информации.

6. Соответствия заявителей и лицензиатов требованиям по профессиональной подготовке, нормативно-методической, технической и технологической оснащенности, режимным требованиям, проверяемом в ходе проведения обязательной экспертизы заявителей и постоянного контроля за деятельностью лицензиатов.

7. Четкой регламентации предоставляемых лицензиату прав и полномочий, а также механизма его взаимодействия с ФАПСИ.

8. Централизованности выдачи, учета, приостановления и отзыва лицензий и сертификатов.

9. Доступности и открытости систем лицензирования и сертификации в рамках вышеперечисленных принципов.

Собственно лицензирование деятельности предприятий в области защиты информации включает следующие действия:

выдачу лицензий (решений о выдаче лицензий) - подачу, рассмотрение заявления на лицензирование, оформление и выдачу лицензий (решений о выдаче лицензий), переоформление лицензий;

проведение специальной экспертизы заявителя;

проведение аттестации руководителя предприятия или лиц, уполномоченных им для руководства лицензируемой деятельностью;

проведение технической экспертизы изделий.

Типовая схема процесса лицензирования представлена на рис. 1. Рассмотрим подробнее отдельные его фазы.

А.. Рассмотрение заявления и выдача лицензий

Для получения лицензии заявитель представляет заявление по форме, представленной в Приложении, с указанием:

наименования и организационно-правовой формы, юридического адреса, номера расчетного счета и реквизитов соответствующего банка;

вида (видов) деятельности с формулировкой видов в соответствии с "Положением о государственном лицензировании в области защиты информации";

срока действия лицензии.

Заявление подписывается руководителем предприятия (либо лицом его замещающим) с расшифровкой подписи и заверяется основной печатью предприятия. Заявление на лицензирование подается на имя генерального директора Федерального агентства и направляется только почтой по адресу:

103031, г. Москва 31, Большой Кисельный переулок, ФАПСИ.

Переписка по рабочим материалам и конкретным вопросам, возникающим в ходе процесса лицензирования, в том числе представление дополнительных или ранее не представленных материалов, осуществляется с уполномоченным подразделением Лицензионного центра ФАПСИ:

121351, г. Москва 351, а/я 59, Отдел лицензирования и сертификации ФАПСИ.

Заявление о выдаче лицензии принимается к рассмотрению только при наличии всех необходимых, определенных нормативными актами, документов, включающих, в первую очередь, заключение по результатам специальной экспертизы, подтверждающее наличие на предприятии необходимых условий для проведения работ по заявленным видам деятельности и соответствие их предъявляемым ФАПСИ требованиям, а также копию документа, подтверждающего прохождение аттестации руководителем предприятия. Заявитель несет ответственность за достоверность представленных сведений. В ходе рассмотрения заявления ФАПСИ вправе произвести проверку достоверности представляемых сведений.

К заявлению на получение лицензии прилагаются:

копия свидетельства о государственной регистрации предприятия;

копии учредительных документов (устава, договора и т.д.) с предъявлением оригиналов, если копии не заверены нотариусом;

копии документов, подтверждающих право собственности, право полного хозяйственного ведения, и (или) договора аренды на имущество, необходимое на ведение заявленной деятельности;

справка налогового органа о постановке на учет;

представление органов государственной власти Российской Федерации с рекомендацией или ходатайством о выдаче лицензии;

документ, подтверждающий оплату рассмотрения заявления.

Проведение специальной экспертизы осуществляется экспертными комиссиями, формируемыми либо Лицензионным центром ФАПСИ, либо аттестационными центрами в рамках определенных этим центрам полномочий.

В настоящее время Федеральным агентством аккредитованы на проведение специальных экспертиз предприятий-заявителей три аттестационных центра на базе следующих организаций и предприятий:

НТЦ ФАПСИ, аттестат аккредитации от 13.08.96

№ АТФ/001-02.005;

ЗАО "МО ПНИЭИ", аттестат аккредитации от 13.08.96

№ АТФ/057-04.002;

"Общественное объединение "Ассоциация документальной электросвязи", аттестат аккредитации от 04.12.96 №АТФ/057-05.002.

В принципе возможны два варианта проведения лицензирования:

1. Предприятие подает заявление на получение лицензии со всеми перечисленными выше документами, считая его одновременно и заявкой на проведение специальной экспертизы, результаты которой затем прилагаются к поданному заявлению. Датой принятия заявления к рассмотрению в этом случае считается дата утверждения экспертного заключения.

2. Предприятие заранее, на основании отдельной заявки, получает экспертное заключение в Лицензионном центре ФАПСИ или в рекомендованном ему аттестационном центре и вместе с другими требуемыми документами направляет его с заявлением. Датой принятия заявления к рассмотрению в этом случае считается дата регистрации в ФАПСИ полного пакета всех необходимых правильно оформленных документов.

Первый вариант является основным, и дальнейшее изложение будет вестись применительно к нему. Второй вариант целесообразно применять в тех случаях, когда остро не стоит вопрос первичной предварительной оценки документов лицензиата, например, при лицензировании эксплуатации шифровальных средств.

Решение о выдаче или отказе в выдаче лицензии принимается в течение 30 дней со дня принятия заявления к рассмотрению. Выдача лицензий или мотивированных отказов в выдаче лицензий, принятие решений о приостановлении или аннулировании лицензий является прерогативой

генерального директора ФАПСИ. Оформленная надлежащим образом лицензия (подписанная генеральным директором ФАПСИ, удостоверенная гербовой печатью Агентства, имеющая уникальный номер, проставленный срок действия и дату регистрации ее в Государственном реестре лицензий ФАПСИ) вручается лицензиату установленным порядком. Копия лицензии хранится в Лицензионном центре Федерального агентства.

Лицензионный центр ФАПСИ вправе на этапе предварительного рассмотрения заявления согласовать с предприятием вопрос о снятии заявления или изменения запрашиваемого объема работ. Если заявление оформлено правильно и в приложении имеются все необходимые документы, то Лицензионный центр ФАПСИ регистрирует поступившие документы и направляет заявителю уточненные для него требования по конкретным видам деятельности, а также указывает аттестационный центр, который будет проводить специальную экспертизу.

Подготовленное на основании требований обоснование необходимых условий для осуществления работ по заявленным видам деятельности заявитель представляет в определенный для него аттестационный центр, после чего заключается договор на проведение специальной экспертизы. Если представленная документация или сведения не полны, ФАПСИ не принимает такое заявление к рассмотрению.

Б. Специальная экспертиза предприятий

Организация и проведение специальных экспертиз предприятий, в целом, возлагается на Лицензионный центр ФАПСИ или уполномоченный аттестационный центр.

Специальная экспертиза заявителя осуществляется на основании заявки предприятия, содержащей лицензируемые виды деятельности и перечни необходимых для их обеспечения производственного и испытательного оборудования, нормативной и методической документации, имеющихся на предприятии, краткой характеристики состава и квалификации персонала предприятия.

Как указывалось в подразделе А., специальная экспертиза заявителя может быть проведена как до подачи заявления на лицензирование, так и в ходе его рассмотрения. В последнем случае просьба о проведении специальной

экспертизы заявителя должна фигурировать в заявлении на лицензирование, к которому в дополнение к документам, перечисленным выше, должна быть приложена справка с указанием сведений, перечисленных в предыдущем абзаце. Время на проведение специальной экспертизы заявителя в этом случае в отведенный на рассмотрение заявления на лицензирование срок не включается.

Специальная экспертиза заявителя осуществляется экспертной комиссией, состав которой и примерные сроки работы доводятся до заявителя официальным порядком.

В случае необходимости аттестация руководителей предприятий или лиц, уполномоченных ими на руководство лицензируемой деятельностью, может быть проведена Лицензионным центром ФАПСи или аттестационным центром в ходе проведения специальной экспертизы предприятия. Экспертная комиссия вправе засчитать в качестве документа об аттестации руководителя предприятия официальный документ о прохождении переподготовки по соответствующему профилю на курсах, имеющих лицензию на осуществление учебной деятельности и право квалифицировать уровень полученных знаний.

Расходы на специальную экспертизу, а также на аттестацию руководителя предприятия полностью относятся на счет заявителя. Экспертиза проводится на основе хозяйственного договора между Лицензионным центром ФАПСи или аттестационным центром и предприятием-заявителем. Оплата работы членов экспертной комиссии производится исключительно центром, осуществлявшим экспертизу, за счет средств, получаемых в соответствии с указанным договором.

Конкретный порядок проведения специальных экспертиз заявителей, методические рекомендации по организации и проведению аттестации руководителей предприятий или лиц, уполномоченных ими на руководство лицензируемой деятельностью, определяются ведомственной инструкцией, разрабатываемой

Лицензионным центром ФАПСи, которая раскрывает и уточняет рассмотренные в настоящей работе аспекты.

В. Техническая экспертиза изделий

. От результатов этой экспертизы зависит решение таких вопросов, как:
необходимость лицензирования своей деятельности тем или иным предприятием;

необходимость и возможность получение разрешения на ввоз в страну или вывоз из нее конкретных средств защиты информации;

и т. д.

Целями такой экспертизы являются:

обоснованное отнесение какого-либо аппаратного, аппаратно-программного или программного средства или его функциональной части, встроенного блока, программного модуля к категориям средств защиты информации, средств криптографической защиты информации (шифровальных средств) и(или) защищенного оборудования;

обоснованное отнесение научно-технической и(или) нормативно-технической документации или технологии к категориям информации и технологии двойного применения, которые могут быть использованы при создании военной техники;

определение уровня защищенности конфиденциальной информации при ее обработке, хранении и передаче по линиям связи, а также эффективности контроля ее защиты в конкретных защищенных системах и комплексах телекоммуникаций, объектах информатики и информационно-телекоммуникационных системах и комплексах;

определение уровня эффективности обнаружения закладных электронных устройств перехвата информации техническими средствами;

контроль за деятельностью лицензиатов в области защиты информации.

Техническая экспертиза проводится на основании решения Федерального агентства или Лицензионного центра ФАПСИ либо самим Лицензионным центром, либо, по его поручению, аккредитованными аттестационными или испытательными сертификационными центрами (лабораториями), а также в предусмотренных законодательными или иными нормативными актами Российской Федерации случаях на основании обращений судебных, правоохранительных, таможенных, налоговых органов или отдельных предприятий, по заявлениям субъектов лицензионной и внешнеторговой деятельности в области защиты информации.

Примером такой экспертизы может служить определение правильности отнесения ввозимого или вывозимого товара к категории шифровальных средств и, следовательно, его классификации по группе 8473 кодов товарной номенклатуры внешней экономической деятельности (кодов ТН ВЭД). В качестве

другого примера приведем оценку стойкости телефонного шифратора с целью его правильной классификации как скремблера.

V

Данный раздел посвящен более подробному рассмотрению вопросов лицензирования деятельности банков, предприятий, организаций и учреждений в области эксплуатации средств криптографической защиты информации. Если разработка, производство, реализация шифровальных средств осуществляется относительно небольшим числом предприятий и организаций, то вопросы лицензирования эксплуатации подобных средств и оказания услуг с их использованием затрагивает интересы несравненно большего числа предприятий, организаций и учреждений. В первую очередь к таким организациям следует отнести банки и другие финансово-кредитные организации, широко применяющие шифровальные средства и средства электронной цифровой подписи для защиты информации, составляющей банковскую или коммерческую тайну, но не содержащей сведения составляющие государственную тайну.

В общем случае, как и все иные юридические лица, банк может заявлять права на осуществление любой деятельности, связанной с защитой информации в системах электронного документооборота. Поэтому более правильно, с учетом ситуации, которая "де-факто" сложилась в стране, говорить о видах деятельности, на которые необходимо получить лицензию.

На наш взгляд, таких видов деятельности три (в соответствии с перечнем видов деятельности, подлежащих лицензированию ФАПСИ):

1) *эксплуатация шифровальных средств для защиты информации при ее обработке, хранении и передаче по каналам связи* и(или) средств электронной цифровой подписи (независимо от способа реализации и контекста использования этих средств), а также шифровальных средств для защиты электронных платежей с использованием пластиковых кредитных карточек и смарт-карт;

2) *оказание услуг по защите (шифрованию) информации,*

3) *монтаж, установка (инсталляция), наладка шифровальных средств для защиты информации при ее обработке, хранении и передаче по каналам связи* и(или) средств электронной цифровой подписи, шифровальных средств для защиты электронных платежей с использованием пластиковых кредитных карточек и смарт-карт.

Как уже отмечалось выше, в соответствии с имеющимися законодательными и нормативными актами *лицензию должно получать каждое юридическое лицо, осуществляющее деятельность в области защиты информации.* Для представляющих наибольший интерес защищенных криптографическими средствами систем обмена и расчета "банк-клиент" это означает, что в классическом варианте за лицензией на эксплуатацию шифровальных средств должен обращаться как сам банк, так и его клиенты, являющиеся абонентами сети электронного документооборота. Однако, учитывая особенности банковского документооборота, ФАПСИ проработало вопрос о возможности применения иного порядка лицензирования установки (инсталляции), эксплуатации *сертифицированных ФАПСИ* шифровальных средств и предоставления услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, в корпоративных сетях типа "Банк-Клиент", системах финансового и фондового рынка при защите информации по уровню "С". В принципе, данный порядок лицензирования перечисленных видов деятельности может быть распространен на другие предприятия, организации и учреждения Российской Федерации.

Под уровнем "С" при этом полагается криптографическая защита информации на уровне потребителя. Информационно-телекоммуникационные системы создаются предприятием самостоятельно на основе сертифицированных СКЗИ, предназначенные для защиты конфиденциальной информации, встраивание которых в прикладные системы должно происходить с выполнением интерфейсных и криптографических протоколов, определенных технической документацией на СКЗИ.

Если коротко характеризовать разработанный порядок, то можно сказать, что банку (или предприятию-организатору сети) будет выдаваться лицензия на *право эксплуатации всей защищенной криптографическими средствами сети, включающей всех его клиентов.* А именно:

1. Лицензия на право установки (инсталляции), эксплуатации сертифицированных ФАПСИ шифровальных средств и предоставления услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, в конкретных корпоративных сетях типа "Банк-Клиент", системах финансового и фондового рынка, предприятий, организаций и учреждений Российской Федерации при защите информации по уровню "С" может

выдаваться заявителю, который будет эксплуатировать сеть указанного типа (далее - организатор сети). Обязанности по обеспечению безопасности применения СКЗИ устанавливаются договорами, заключаемыми организатором сети с пользователями сети. Пользователи сети эксплуатируют сертифицированные СКЗИ без оформления лицензий.

При необходимости Лицензионный центр ФАПСИ выдает пользователям такой сети по их заявкам заверенную копию лицензии организатора сети с указанием их наименования и юридического адреса. Вместе с тем, наличие подобной лицензии или ее копии не освобождает организатора сети и пользователей его корпоративной сети от необходимости получения отдельных лицензий на право эксплуатации иных средств криптографической защиты информации.

2. Для создания соответствующих условий осуществления лицензируемой деятельности заявитель вправе приобрести у изготовителя или его представителя опытную партию сертифицированных средств криптографической защиты информации, а также комплект необходимой технической или эксплуатационной документации до получения лицензии.

3. Вместо представления органа государственной власти Российской Федерации заявитель в данном случае вправе представлять копию государственной лицензии на основной вид своей деятельности (например, копию банковской лицензии).

4. Специальная экспертиза заявителей на право установки (инсталляции), эксплуатации сертифицированных ФАПСИ шифровальных средств и предоставления услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, в корпоративных сетях типа "Банк-Клиент", системах финансового и фондового рынка, предприятий, организаций и учреждений Российской Федерации при защите информации по уровню "С" проводится аттестационным центром на основании заявки и представленного заявителем перечня сведений, подтверждающих выполнение им соответствующих требований ФАПСИ, а также условий действия сертификатов соответствия на эксплуатируемые шифровальные средства.

В настоящий момент ФАПСИ разработало несколько видов требований к предприятиям, претендующим на получение лицензии Федерального агентства.

Имеющиеся типовые требования конкретизируются и дифференцируются с учетом специфики отдельных видов деятельности и заявителей. В рассматриваемом случае к заявителю на право установки (инсталляции), эксплуатации сертифицированных ФАПСИ шифровальных средств и предоставления услуг по шифрованию информации при защите информации по уровню "С" предъявляются следующие требования:

- На предприятии-заявителе руководством должны быть выделены должностные лица, ответственные за разработку и практическое осуществление мероприятий по обеспечению функционирования и безопасности СКЗИ.

- Вопросы обеспечения функционирования и безопасности СКЗИ должны быть отражены в специально разработанных документах, утвержденных руководством предприятия, с учетом эксплуатационной документации на СКЗИ.

- На предприятии должны быть созданы условия, обеспечивающие сохранность конфиденциальной информации, доверенной предприятию юридическими и физическими лицами, пользующимися его услугами.

- Размещение, специальное оборудование, охрана и режим в помещениях, в которых размещены СКЗИ (далее помещения), должны обеспечивать безопасность информации, СКЗИ и шифрключей, сведение к минимуму возможности неконтролируемого доступа к СКЗИ, просмотра процедур работы с СКЗИ посторонними лицами.

- Порядок допуска в помещения определяется внутренней инструкцией, которая разрабатывается с учетом специфики и условий функционирования конкретной структуры предприятия.

- При расположении помещений на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п., окна помещений оборудуются металлическими решетками, ставнями, охранной сигнализацией или другими средствами, препятствующими несанкционированному доступу в помещения. Эти помещения должны иметь прочные входные двери, на которые устанавливаются надежные замки.

- Для хранения шифрключей, нормативной и эксплуатационной документации, инсталляционных дискет помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей. Дубликаты ключей от

хранилищ и входных дверей должны храниться в сейфе ответственного лица, назначаемого руководством предприятия.

- Устанавливаемый руководителем предприятия порядок охраны помещений должен предусматривать периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны.

- Размещение и установка СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ.

- Системные блоки ЭВМ с СКЗИ должны быть оборудованы средствами контроля их вскрытия.

- Все поступающие для использования шифрключи и инсталляционные дискеты должны браться на предприятии на поэкземплярный учет в выделенных для этих целей журналах.

- Учет и хранение носителей шифрключей и инсталляционных дискет, непосредственная работа с ними поручается руководством предприятия специально выделенным работникам предприятия. Эти работники несут персональную ответственность за сохранность шифрключей.

- Учет изготовленных для пользователей шифрключей, регистрация их выдачи для работы, возврата от пользователей и уничтожения ведется на предприятии.

- Хранение шифрключей, инсталляционных дискет допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение.

Наряду с этим должна быть предусмотрена возможность отдельного безопасного хранения рабочих и резервных шифрключей, предназначенных для использования в случае компрометации рабочих шифрключей в соответствии с правилами пользования СКЗИ.

- При пересылке шифрключей клиентам предприятия должны быть обеспечены условия транспортировки, исключающие возможность физических повреждений и внешнего воздействия на записанную ключевую информацию.

- В случае отсутствия у оператора СКЗИ индивидуального хранилища шифрключи по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

- Уполномоченными лицами периодически должен проводиться контроль сохранности входящего в состав СКЗИ оборудования, а также всего используемого программного обеспечения для предотвращения внесения программно-аппаратных закладок и программ вирусов.

- К работе с СКЗИ допускаются решением руководства предприятия только сотрудники, знающие правила его эксплуатации, владеющие практическими навыками работы на ПЭВМ, изучившие правила пользования, эксплуатационную документацию и прошедшие обучение работе с СКЗИ.

- Руководитель предприятия или лицо, уполномоченное на руководство заявленными видами деятельности, должно иметь представление о возможных угрозах информации при ее обработке, передаче, хранении, методах и средствах защиты информации.

VI

В настоящее время сертификация средств защиты информации, отнесенных к компетенции ФАПСИ, определяется *"Системой сертификации средств криптографической защиты информации (СКЗИ)"* **РОСС RU.0001.030001**. Данный документ представляет собой нормативный акт, который включает в себя положения и нормы, определяющие правила и общий порядок проведения сертификации в рассматриваемой предметной области. Он базируется на законе Российской Федерации "О сертификации продукции и услуг", иных нормативных актах, утвержденных Госстандартом России, и соответствует вытекающим из них требованиям к порядку, схеме проведения, а также организационной структуре систем сертификации. Тем самым учитываются сложившиеся к настоящему времени международные правила организации и проведения работ по сертификации продукции. С другой стороны, учтены и обобщены особенности и накопленный многолетний опыт работы ФАПСИ в области защиты информации, оценки качества разрабатываемых и производимых средств защиты, а также права и обязанности Федерального агентства, предоставленные ему российским законодательством.

Порядок проведения сертификации средств защиты информации ФАПСИ основан на следующих основных принципах и правилах:

1. *Обязательность сертификации изделий, обеспечивающих защиту государственной тайны, или обязательность сертификации которых установлена нормативными актами Российской Федерации.*

В настоящее время такое требование установлено для средств защиты информации в системах электронного документооборота, используемых для обмена с Банком России, а также для средств и защищенных систем государственных предприятий или предприятий, на которых размещен государственный заказ.

2. Обязательность использования криптографических алгоритмов, являющихся стандартами или ранее рекомендованных либо разработанных ФАПСИ.

Специально подчеркнем, что факт одобрения ФАПСИ алгоритма до его технической реализации является одним из основных требований к представляемым на сертификацию изделиям. Это одобрение может быть осуществлено путем утверждения алгоритма:

в качестве государственного стандарта;
Правительством Российской Федерации;
Федеральным агентством.

Отсюда следует, что изделия, реализованные на базе собственных оригинальных алгоритмов, ранее не представлявшихся в ФАПСИ, а равно изделия, реализующие алгоритмы иностранной разработки, или импортные шифровальные средства на сертификацию не принимаются.

3. Принятие на сертификацию только изделий от заявителей, имеющих лицензию ФАПСИ на соответствующие виды деятельности.

Оформление установленным порядком права на осуществление деятельности в области защиты информации является первичным. Разрабатывать алгоритмы и средства защиты на их базе как продукцию, товар предлагаемый на рынок, могут только предприятия, имеющие лицензию.

4. Принятие на сертификацию только готовых изделий в целом, а не их составных частей или отдельных компонент.

В различных публикациях специалисты ФАПСИ неоднократно указывали, что сами по себе даже высоконадежные криптографические алгоритмы или отдельные блоки и модули (аппаратные, аппаратно-программные и программные), реализующие часть процесса защиты, не могут обеспечить требуемого уровня защиты информации в комплексе. Например, без реализации специальных мер эти средства могут быть просто обойдены или необходимая информация может быть получена за счет побочных электромагнитных излучений

и наводок. Для систем и комплексов, которые включают совокупность некоторого множества явно различимых как самостоятельное изделие функционально и конструктивно законченных элементов, возможно оформление сертификата на каждый из них.

5. Процедура сертификации осуществляется в отношении только технических средств или технической части системы защиты, с учетом условий их эксплуатации.

6. Двухступенчатость процесса сертификации при независимости организаций, проводящих экспертизу и сертификационные испытания: сертификация средств защиты информации осуществляется Центральным органом по сертификации, а испытания проводятся в аккредитованных испытательных центрах (лабораториях).

7. Дифференцированность подхода к уровню защиты различных видов информации.

Например, в зависимости от полноты реализуемой защиты для системы конфиденциального электронного документооборота устанавливаются три уровня обеспечения безопасности (сертификации):

Уровень "А" - сертификат выдается на систему защиты в целом и подтверждает соответствие реализации средств шифрования заданным криптографическим алгоритмам, комплексное выполнение требований ФАПСИ к шифровальным средствам с учетом их программного окружения, наличие защищенной (без недокументированных возможностей) аппаратно-программной среды;

Уровень "В" - сертификат выдается на систему защиты, включающую шифровальные средства и их программное окружение, и подтверждает соответствие реализации средств шифрования заданным криптографическим алгоритмам и требованиям ФАПСИ, выполнение требований ФАПСИ к программному окружению шифровальных средств;

Уровень "С" - сертификат выдается только на шифровальные средства и подтверждает соответствие реализации средств шифрования заданным криптографическим алгоритмам и требованиям.

8. Принятие Центральным органом по сертификации и испытательными центрами (лабораториями) на себя ответственности за выполнение возложенных

на них функций в соответствии с действующим законодательством и договорными обязательствами.

9. *Сертификационные испытания средств криптографической защиты информации могут осуществляться только аккредитованными ФАПСИ испытательными сертификационными центрами.* Действительное соответствие изделия государственным стандартам и гарантию удовлетворения требований по безопасности к шифровальным средствам соответствующего класса удостоверяет только сертификат ФАПСИ.

10. *Принятие и неуклонное соблюдение заявителем правил, установленных в системе сертификации.*

Организационная структура системы сертификации ФАПСИ включает в себя ФАПСИ как Государственный орган по сертификации средств криптографической защиты информации, Центральный орган системы сертификации и Испытательные центры (лаборатории) средств защиты информации и заявителей.

ФАПСИ как Государственный орган по сертификации создает систему сертификации средств защиты информации, устанавливает правила проведения сертификации конкретных средств защиты информации в этой системе, организует обязательную государственную сертификацию этих средств, устанавливает правила аккредитации и выдачи лицензий на проведение работ по сертификации, определяет центральный орган системы сертификации, устанавливает правила признания зарубежных сертификатов, рассматривает апелляции по вопросам сертификации, выдает сертификаты.

Центральный орган системы сертификации организует и осуществляет работы по сертификации средств защиты информации, координирует деятельность испытательных центров (лабораторий), разрабатывает номенклатуру средств защиты информации, подлежащих сертификации, совершенствует методы и средства испытаний, разрабатывает нормативные и методические документы системы сертификации, готовит материалы для аккредитации испытательных центров (лабораторий), ведет государственные реестры аккредитованных испытательных центров (лабораторий) и сертифицированных продуктов, назначает испытательный центр (лабораторию) для проведения испытаний конкретных средств защиты информации, утверждает

программы и методики испытаний конкретных средств защиты информации, осуществляет экспертизу материалов сертификационных испытаний средств защиты информации на соответствие предъявляемым требованиям, готовит материалы для выдачи сертификатов, осуществляет научно-технический контроль за стабильностью характеристик сертифицированных изделий и состоянием их производства, а также за деятельностью испытательных центров (лабораторий).

Испытательные центры (лаборатории) средств защиты информации осуществляют испытания конкретных СЗИ на основании нормативных и методических материалов Центрального органа системы сертификации, оформляют и представляют в Центральный орган системы сертификации протоколы испытаний, готовят и согласовывают с Центральным органом системы сертификации программы и методики испытаний конкретных средств защиты информации, принимают участие в совершенствовании методов и средств испытаний, разработке нормативной и методической документации, участвуют в проверке технических характеристик сертифицированной им продукции и проверке условий ее производства.

В настоящее время Федеральным агентством аккредитованны на проведение сертификационных испытаний средств криптографической защиты информации в Системе сертификации РОСС RU.0001.030001 три испытательных центра и две испытательных лаборатории на базе следующих организаций и предприятий:

НТЦ ФАПСи, аттестат аккредитации от 07.12.94

№ АФ/Ц00-01.001, лицензия на право проведения сертификационных испытаний

№ ЛФ/02-1;

Научно-исследовательский институт автоматики РГНПО "Автоматика", аттестат аккредитации от 13.09.95 № АФ/Ц00-02.002, лицензия на право проведения сертификационных испытаний № ЛФ/01-15;

Пензенский филиал НТЦ ФАПСи, аттестат аккредитации от 13.09.95

№ АФ/Ц03-03.003, лицензия на право проведения сертификационных испытаний № ЛФ/02-14;

НПО "Импульс", аттестат аккредитации от 12.11.96

№ АФ/Л11-04.004, лицензия на право проведения сертификационных испытаний № ЛФ/01-68;

НПП "Сигнал", аттестат аккредитации от 12.11.96

№ АФ/Л12-05.005, лицензия на право проведения сертификационных испытаний № ЛФ/01-71.

Заявители (разработчики, изготовители, поставщики и потребители) сертифицированной продукции обеспечивают соответствие средств защиты информации требованиям нормативных и методических документов, на соответствие которым они были сертифицированы, незамедлительно извещают Центральный орган системы сертификации о всех изменениях в технологии, конструкции (составе) средств защиты информации, которые могут оказать влияние на свойства этих изделий, обеспечивают беспрепятственное выполнение инспекционного контроля за сертифицированной продукцией, приостанавливают производство или прекращают реализацию средств защиты информации, не отвечающих предъявляемым требованиям или по истечении срока действия сертификата.

Заявление на сертификацию средств защиты информации и полный комплект технической документации подаются в Центральный орган по сертификации, который назначает испытательный центр (лабораторию) для проведения испытаний.

При отсутствии всех необходимых документов заявление на проведение сертификации не принимается.

Испытания проводятся на основании хозяйственного договора между заявителем и испытательным центром (лабораторией).

Сертификация (экспертиза материалов испытаний и подготовка документов для выдачи сертификата) осуществляется Центральным органом по сертификации на безвозмездной основе.

При отсутствии аккредитованных испытательных центров (лабораторий) испытания подлежащей сертификации продукции проводятся Центральным органом по сертификации на безвозмездной основе.

Испытания средств защиты информации проводятся на образцах, конструкция, состав и технология изготовления которых должны быть такими же, как и у образцов, поставляемых потребителю. Номера образцов продукции, на

которых проводились сертификационные испытания, и технических условий на них включаются в текст сертификата.

Сроки проведения испытаний устанавливаются договором между заявителем и испытательным центром (лабораторией).

Указанный срок должен учитывать время, необходимое на экспертизу.

Результаты испытаний оформляются протоколами, которые направляются в Центральный орган по сертификации, а копии - заявителю.

При отрицательном заключении экспертизы заявителю отказывается в выдаче сертификата.

Сертификат выдается на срок до 5 лет и подписывается генеральным директором Федерального агентства правительственной связи и информации при Президенте Российской Федерации.

Действие выданного сертификата может быть приостановлено или сертификат может быть вообще аннулирован по результатам инспекционного контроля за сертифицированными средствами защиты информации.

Причинами приостановления и аннулирования сертификата могут быть:

а) изменение нормативных и методических документов на средства защиты информации или их элементов, на испытания и контроль;

б) изменения конструкции, состава или комплектности средства защиты информации;

в) невыполнение требований технологии или технических условий на изделие;

г) отказ заявителя в допуске для проведения научно-технического и инспекционного контроля.

По состоянию на декабрь месяц 1996 года Федеральным агентством выдан 161 сертификат на средства криптографической защиты информации, в том числе 25 на шифровальные средства, предназначенные для защиты конфиденциальной коммерческой и банковской информации. В соответствии с установленным порядком, подлинники сертификатов выдаются основному заказчику и разработчику шифровальных средств с предоставлением им права выдачи потребителям заверенных копий.

В заключение настоящей работы авторы хотели бы отметить, что системы лицензирования и сертификации проходят сейчас стадию совершенствования с точки зрения развития правовой базы, механизма и правил их функционирования. Отсюда, естественно, следует, что отдельные положения, изложенные в данной статье, могут быть изменены, уточнены или дополнены. Естественно, будут пополняться и список лицензиатов, и перечень сертифицированных средств криптографической защиты информации. Все эти уточнения, пополнения и изменения будут по мере возможностей доводиться до сведения заинтересованных лиц и организаций, в том числе и через средства массовой информации.

О.А. Беззубцев

А.Н. Ковалев

Приложения

Законодательная и нормативная база лицензирования и сертификации в области защиты информации

Законы Российской Федерации

- а) "О федеральных органах правительственной связи и информации" от 19.02.93 № 4524-1.
- б) "О государственной тайне" от 21.07.93 № 5485-1.
- в) "О сертификации продукции и услуг" от 10.06.93 № 5151-1.
- г) "Об информации, информатизации и защите информации" от 20.02.95 № 24-ФЗ.
- д) "О связи" от 16.02.95 № 15-ФЗ.
- е) "О защите прав потребителей" от 07.02.92 № 2300-1.
- ж) "Об авторском праве и смежных правах" от 09.07.93 № 5352-1.
- з) "Патентный закон Российской Федерации" от 23.09.92 № 3519-1.
- и) "О стандартизации" от 10.06.93 № 5154-1.
- к) "О рекламе" от 18.07.95. № 108-ФЗ
- л) "О правовой охране программ для электронных вычислительных машин и баз данных" от 23.09.92. № 3523-1
- м) "О правовой охране топологии интегральных микросхем" от 23.09.92. № 3526-1

н) "Об участии в международном информационном обмене" от 04.07.96. № 85 ФЗ

Указы и распоряжения Президента Российской Федерации

а) "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации" от 3.04.95 № 334.

б) распоряжение Президента Российской Федерации "О контроле за экспортом из Российской Федерации отдельных видов сырья, материалов, оборудования, технологий и научно-технической информации, которые могут быть применены при создании вооружения и военной техники" от 11.02.94 № 74-рп.**Постановления Правительства Российской Федерации**

а) "О лицензировании отдельных видов деятельности" от 24.12.94 № 1418.

б) "О лицензировании и квотировании экспорта и импорта товаров (работ, услуг) на территории Российской Федерации" от 06.11.92 № 854.

в) "О поставках продукции и отходов производства, свободная реализация которых запрещена" от 10.12.92 № 959.

г) "О внесении дополнений и изменений в постановления Правительства Российской Федерации от 06.11.92 № 854 и от 10.12.92 № 959" от 15.04.94 № 331.

д) "Об утверждении Положения о порядке контроля за экспортом из Российской Федерации отдельных видов сырья, материалов, оборудования, технологий и научно-технической информации, которые могут быть применены при создании вооружения и военной техники" от 10.03.94 № 197.

е) "О мерах по совершенствованию государственного регулирования экспорта товаров и услуг" от 01.07.94 № 758.

ж) "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) услуг по защите государственной тайны"

от 15.04.95 № 333.

з) "О сертификации средств защиты информации" от 26.06.95 № 608.

Иные нормативные акты

а) "Система сертификации средств криптографической защиты информации" (Система сертификации СКЗИ)" РОСС RU.0001.030001 от 15.11.93.

б)"Правила по проведению сертификации в Российской Федерации" от 16.02.94 № 3.

в) "Положение о государственном лицензировании деятельности в области защиты информации" от 27.04.94 № 10.

г) "Положение об испытательном центре (лаборатории) средств криптографической защиты информации (ИЦ СКЗИ), аккредитованном ФАПСИ на испытания СКЗИ по требованиям безопасности информации".

е)"Положение о лицензировании деятельности в области связи в Российской Федерации".

ж) "Временное положение об аттестационном центре ФАПСИ, аккредитованном на проведение работ в области защиты информации".

Документация по лицензированию и сертификации

Бланк заявления на получение лицензии ФАПСИ

Угловой штамп

предприятия

Кому: _____

(наименование государственного органа по

лицензированию и его юридический адрес)

(наименование заявителя, организационно-правовая форма,

юридический адрес, номер расчетного счета и реквизиты соответствующего банка)

Прошу выдать лицензию на осуществление следующих
видов деятельности

(согласно Приложению 1 данного Положения)

Срок действия лицензии

Приложение: к заявлению прилагаются документы, перечисленные в разделе 3.

Место Руководитель

гербовой печати предприятия-заявителя _____

подпись

Главный бухгалтер _____

подпись

Бланк заявления на получение решения ФАПСи о выдаче лицензии

Угловой штамп

предприятия

Кому: _____

(наименование государственного органа по

лицензированию и его юридический адрес)

(наименование заявителя, организационно-правовая форма,

юридический адрес, номер расчетного счета и реквизиты соответствующего банка)

Прошу разрешить осуществление следующих видов
деятельности

(согласно Приложению 2 данного Положения)

Срок действия лицензии

Приложение: к заявлению прилагаются документы, перечисленные в разделе 3.

Место Руководитель

гербовой печати предприятия-заявителя _____

подпись

Главный бухгалтер _____

подпись

ЛИЦЕНЗИЯ

Регистрационный № _____ от " " _____ 199 г.

Действительна до " " _____ г.

**Федеральное агентство
правительственной связи и
информации при Президенте
Российской**

Федерации предоставляет Научно-

производственному объединению,

(наименование предприятия-заявителя,

000000, г. XXXXXXXXXXXXXXX, ул Иванова, 1

юридический адрес)

**право заниматься следующими видами деятельности
в области защиты информации:**

1. Разработка шифровальных средств, предназначенных для криптографической защиты информации, содержащей сведения, составляющие государственную

тайну, при ее обработке, хранении и передаче по каналам связи при реализации криптографических алгоритмов, являющихся государственными стандартами или рекомендованных ФАПСИ.

Начальник Отдела лицензирования
и сертификации ФАПСИ

Вариант лицензии ФАПСИ на подготовку и
переподготовку кадров

ЛИЦЕНЗИЯ

Регистрационный № _____ от " " _____ 1996 г.

Действительна до " " _____ г.

**Федеральное агентство
правительственной связи и
информации при Президенте
Российской**

Федерации предоставляет _Московскому

государственному техническому институту,

(наименование предприятия-заявителя,

000000, г. XXXXXXXXXXXXXXXX, ул Иванова, 1

юридический адрес)

право заниматься следующими видами деятельности в области защиты информации:

Подготовка и переподготовка кадров в области защиты информации в сфере высшего, послевузовского и дополнительного профессионального образования по специальностям:

- 1) высшее - "Прикладная математика", специализация: "Программно-аппаратные методы обеспечения безопасности информации";

Начальник Отдела лицензирования
и сертификации ФАПСИ

Типовая форма сертификата соответствия

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПРАВИТЕЛЬСТВЕННОЙ СВЯЗИ
И ИНФОРМАЦИИ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер _____ от "___" _____ 199__ г.

Действителен до "___" _____ 199__ г.

Выдан _____

(наименование предприятия-заявителя)

Настоящий сертификат удостоверяет, что _____

(наименование продукции)

соответствует требованиям безопасности информации, установленным

(наименование стандартов и других нормативных документов)

Сертификат выдан на основании результатов проведенных _____

(наименование испытательной лаборатории)

сертификационных испытаний образцов продукции (зав. №№ _____)

(наименование продукции)

обеспечивает безопасность _____ информации при

(гриф секретности информации)

выполнении _____

(наименование нормативных документов по эксплуатации)

Печать ФАПСИ

Генеральный директор

Федерального агентства _____

(подпись, и.о., фамилия)