



BUSINESS INFORMATION SECURITY ASSOCIATION
ассоциация по вопросам защиты информации

Практика получения лицензий ФСТЭК и ФСБ в Московском регионе

www.bis-expert.ru

МОСКВА 2013

Информация об авторе:

Андрей Валерьевич Семёнов, эксперт по информационной безопасности ООО "Эдвансед Трансформейшн Консалтинг" (AT Consulting)

Опыт работы в области ИБ (более 10 лет):

2011 г. – по н/в

ООО "Эдвансед Трансформейшн Консалтинг"

Эксперт по ИБ

2004 г. – 2011 г.

Банк "Возрождение" (ОАО)

Главный специалист Службы информационной безопасности

2003 г. – 2004 г.

ОАО "ИнфоТеКС" (российский разработчик СКЗИ)

Старший менеджер отдела сопровождения и клиентских проектов

Опыт по тематике лицензирования (в 2011 – 2013 г.г.):

Непосредственное участие в получении:

- 3 лицензий ФСТЭК России на деятельность по технической защите конфиденциальной информации.
- 2 лицензий ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации.
- 2 лицензий ФСБ России на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и ...
- 1 лицензия ФСБ России на осуществление работ, связанных с использованием сведений, составляющих государственную тайну.

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ	2
1. ПОСТАНОВКА ЗАДАЧИ	6
2. ОПРЕДЕЛЕНИЕ ЛИЦЕНЗИРУЕМЫХ ВИДОВ ДЕЯТЕЛЬНОСТИ И ФОИВ, ОСУЩЕСТВЛЯЮЩИХ ЛИЦЕНЗИРОВАНИЕ КОНКРЕТНЫХ ВИДОВ ДЕЯТЕЛЬНОСТИ.....	8
3. ПОЛУЧЕНИЕ ЛИЦЕНЗИЙ ФСТЭК НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ (ТЗКИ) И НА ДЕЯТЕЛЬНОСТЬ ПО РАЗРАБОТКЕ И ПРОИЗВОДСТВУ СРЕДСТВ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ (СЗКИ)	11
1.1. Перечень НПА, регламентирующих получение лицензии ФСТЭК.....	11
1.1.1. Перечень НПА, регламентирующих получение лицензии ФСТЭК на деятельность по ТЗКИ	11
1.1.2. Перечень НПА, регламентирующих получение лицензии ФСТЭК на деятельность по разработке и производству СЗКИ.....	12
1.2. Основные требования и мероприятия для получения лицензий	12
1.2.1. Заявления о предоставлении лицензии	14
1.2.2. Лицензионный сбор	18
1.2.3. Учредительные документы юридического лица	19
1.2.4. Документы, подтверждающие квалификацию специалистов по защите информации .	19
1.2.5. Правоустанавливающие документы на помещения, предназначенные для осуществления лицензируемого вида деятельности.....	20
1.2.6. Технические паспорта и аттестаты соответствия защищаемых помещений требованиям безопасности информации	20
1.2.7. Технические паспорта автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации, и аттестаты соответствия автоматизированных систем требованиям безопасности информации	22
1.2.8. Документы, подтверждающие право соискателя лицензии на программы для электронно-вычислительных машин и базы данных	23

1.2.9.	Документы, содержащие сведения о наличии, а также документы, подтверждающие права соискателя лицензии, на контрольно-измерительное, производственное и испытательное оборудование, средства защиты информации и средства контроля защищенности информации.	24
1.2.10.	Документы, содержащие сведения об имеющихся технической документации, национальных стандартах и методических документах.....	25
1.2.10.1.	Заказ документов в "Рособоронстандарт"	27
1.2.10.2.	Заказ документов во ФСТЭК.....	28
1.2.11.	Документы, подтверждающие наличие необходимой системы производственного контроля	28
1.3.	Заключительные положения	29
4.	ПОЛУЧЕНИЕ ЛИЦЕНЗИИ ФСБ НА ДЕЯТЕЛЬНОСТЬ ПО РАЗРАБОТКЕ, ПРОИЗВОДСТВУ, РАСПРОСТРАНЕНИЮ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ, ОКАЗАНИЮ УСЛУГ И ТЕХНИЧЕСКОМУ ОБСЛУЖИВАНИЮ	31
1.4.	Перечень НПА, регламентирующих получение лицензии.....	32
1.5.	Основные требования и мероприятия для получения лицензии	33
1.5.1.	Заявление о предоставлении лицензии	34
1.5.2.	Учредительные документы юридического лица	41
1.5.3.	Правоустанавливающие документы на помещения, здания, сооружения и иные объекты по месту осуществления лицензируемой деятельности, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним	41
1.5.4.	Внутренние распорядительные документы, подтверждающие наличие условий для соблюдения конфиденциальности информации, необходимых для выполнения работ и оказания услуг	42
1.5.5.	Документы, подтверждающие нахождение в штате соискателя лицензии на основной работе сотрудников.....	42
1.5.6.	Документы государственного образца (дипломы, аттестаты, свидетельства) об образовании, переподготовке, повышении квалификации по направлению "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей сотрудников	43
1.5.6.1.	Общероссийский классификатор специальностей (ОКСО)	44
1.5.6.2.	Документы государственного и установленного образца	45
1.5.7.	Должностные инструкции сотрудников	49
1.5.8.	Лицензионный сбор	49

1.6.	Заключительные положения	49
5.	ПОЛУЧЕНИЕ ЛИЦЕНЗИИ ФСБ НА ОСУЩЕСТВЛЕНИЕ РАБОТ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ.....	52
1.7.	Перечень НПА, регламентирующих получение лицензии.....	52
1.8.	Основные требования и мероприятия для получения лицензии	52
1.8.1.	Лицензионный сбор	53
1.8.2.	Спецэкспертиза и аттестация руководителя	54
1.8.2.1.	Специальная экспертиза	55
1.8.2.1.1.	Учредительные и внутренние документы.....	55
1.8.2.1.2.	Руководящие документы по защите государственной тайны и защите информации 57	
1.8.2.1.3.	Подразделение по защите государственной тайны	58
1.8.2.1.4.	Внутренние организационно-распорядительные и регламентирующие документы по защите государственной тайны и защите информации	59
1.8.2.1.5.	Взаимодействие с Заказчиком закрытых работ.....	59
1.8.2.2.	Государственная аттестация руководителя организации.....	59
1.8.2.2.1.	Допуск руководителя организации к государственной тайне.....	60
1.9.	Заключительные положения	62
6.	ЗАКЛЮЧЕНИЕ.....	63
7.	СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ ИНФОРМАЦИИ (ЛИТЕРАТУРА И ИНТЕРНЕТ-РЕСУРСЫ) 64	
8.	ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ	68
9.	Ассоциации Business Information Security (BISA)	70

1. ПОСТАНОВКА ЗАДАЧИ

Деятельность в области защиты информации ограниченного доступа, такой как персональные данные, финансовая, коммерческая, для служебного пользования, а тем более информации, содержащей сведения, составляющие государственную тайну, подлежит обязательному лицензированию.

Относительно недавно деятельность лишь небольшого круга организаций попадала под виды деятельности, подлежащие лицензированию. Однако, государственное регулирование в сфере обеспечения информационной безопасности, включая ряд федеральных законов ([1] – [3], [9] – [11]), потребовали для выполнения их положений практически от каждой организации получения той или иной лицензии в области защиты информации.

Основными регулирующими органами в области защиты информации являются Федеральная служба безопасности Российской Федерации (ФСБ России) и Федеральная служба по техническому и экспортному контролю (ФСТЭК России) ([5] – [8]). Существует и ряд других регуляторов в этой области – например, Министерство обороны Российской Федерации и Служба внешней разведки Российской Федерации. Но виды деятельности, требующие лицензий данных ведомств, носят специфичный характер и подавляющему большинству организаций не требуются.

Как правило, наиболее востребованным для "типовой" организации является наличие лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации¹.

Затем по степени уменьшения востребованности следуют:

- лицензия ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации²;
- лицензия ФСБ России на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

¹ 2282 организации в [реестре лицензий ФСТЭК](#) на деятельность по технической защите конфиденциальной информации по состоянию на сентябрь 2013 г.

² 1168 организаций в [реестре лицензий ФСТЭК](#) на деятельность по разработке и производству средств защиты конфиденциальной информации по состоянию на сентябрь 2013 г.

- лицензия ФСБ России на осуществление работ, связанных с использованием сведений, составляющих государственную тайну.

Далее в работе будут рассмотрены требования и мероприятия, направленные на получение этих четырёх лицензий.

Определится с необходимостью наличия в организации той или иной лицензии помогают [2], [3], [8], а также информационное сообщение ФСТЭК ([18]), которое даёт ряд пояснений по вопросу необходимости получения лицензии ФСТЭК на деятельность по ТЗКИ.

Несмотря на имеющиеся [НПА](#) в области лицензирования, часть их положений носит достаточно общий характер и не даёт детального представления относительно реализации лицензионных требований, процедур и состава работ, финансовых и временных затрат, которые предстоит понести организации в процессе получения лицензии. В определённых случаях может оказаться, что отказ в деятельности организации от лицензируемых видов будет предпочтительнее, чем её получение и поддержание соответствия лицензионным требованиям (например, посредством передачи соответствующих функций на аутсорсинг).

Целью данной работы является консолидация в одном месте перечня необходимых НПА при лицензировании у различных регуляторов (ФСБ и ФСТЭК), изложения практического опыта лицензирования, приведения необходимых этапов, процедур, сроков, состава документов, примерной стоимости (где это возможно) на примере одной из организаций Московского региона.

При встрече в тексте работы ссылок на конкретные организации и решений просьба не расценивать это как рекламу – приводятся реальные примеры из процесса получения лицензий. Может быть, в ряде случаев наш выбор и не был оптимальным, но это жизнь.

2. ОПРЕДЕЛЕНИЕ ЛИЦЕНЗИРУЕМЫХ ВИДОВ ДЕЯТЕЛЬНОСТИ И ФОИВ, ОСУЩЕСТВЛЯЮЩИХ ЛИЦЕНЗИРОВАНИЕ КОНКРЕТНЫХ ВИДОВ ДЕЯТЕЛЬНОСТИ

Перед каждой организацией вставляли или должны встать следующие вопросы: имеются ли в её деятельности лицензируемые виды и к какому регулятору обращаться за индульгенцией (лицензией)?

Вопросы о том, как и какой ценой получить лицензии встанут позже, а пока в ответе на первые два следует обращаться к следующим НПА:

- 1) Федеральный закон Российской Федерации от 04.05.2011 № 99-ФЗ "О лицензировании отдельных видов деятельности" [3];
- 2) Постановление Правительства РФ от 21.11.2011 № 957 "Об организации лицензирования отдельных видов деятельности" [8];
- 3) Информационное сообщение ФСТЭК России от 30.05.2012 № 240/22/2222 "По вопросу необходимости получения лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации" [18];
- 4) Федеральный закон Российской Федерации от 21.07.1993 № 5485-1 "О государственной тайне" [2].

ФЗ № 99-ФЗ регулирует отношения, возникающие между федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, юридическими лицами и индивидуальными предпринимателями в связи с осуществлением лицензирования отдельных видов деятельности, а также определяет перечень видов деятельности, на которые требуются лицензии.

Следует отметить отдельно, что положения данного ФЗ не применяются к отношениям, связанным с осуществлением лицензирования деятельности, связанной с защитой государственной тайны.

Из наиболее востребованных коммерческими и государственными организациями видов деятельности ФЗ № 99-ФЗ определяет, что лицензируемыми из них являются следующие:

- 1) Разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

- 2) Разработка и производство средств защиты конфиденциальной информации;
- 3) Деятельность по технической защите конфиденциальной информации.

В свою очередь ФЗ № 5485-1 определяет ещё один лицензируемый вид деятельности:

- 4) Проведение работ, связанных с использованием сведений, составляющих государственную тайну.

Если быть точным, он определяет ещё несколько лицензируемых видов деятельности (создание средств защиты информации и осуществление мероприятий и (или) оказание услуг по защите государственной тайны), но необходимость в таких видах деятельности встречается достаточно редко и в рамках данной работы не рассматривается.

ПП № 957 утверждает перечень федеральных органов исполнительной власти, осуществляющих лицензирование конкретных видов деятельности. Для рассматриваемых нами четырёх видов деятельности данное постановление определяет следующих регуляторов (Таблица 1):

Таблица 1 - ФОИВ, осуществляющий лицензирование и соответствующий вид деятельности

ФОИВ, осуществляющий лицензирование	Вид деятельности
ФСБ России	Разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)
ФСТЭК России	Деятельность по технической защите конфиденциальной информации
ФСБ России, ФСТЭК России	Разработка и производство средств защиты конфиденциальной информации

Регулирование вопросов, связанных с ГТ, определяется отдельным НПА [2] и к имеющейся таблице можем добавить ещё одну строку:

ФОИВ, осуществляющий лицензирование	Вид деятельности
ФСБ России	Проведение работ, связанных с использованием сведений, составляющих

ФОИВ, осуществляющий лицензирование	Вид деятельности
	государственную тайну

Таким образом, на данном этапе у организации появляется понятие о необходимости получения лицензии и о том, в какой лицензирующий орган ей следует обращаться.

Следует отметить, что имеется ряд условий, при которых определённые виды деятельности не требуют от организации получения лицензии.

Так, ПП № 957 приводит следующее исключение:

"техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, **осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя**".

ФСТЭК в своём информационном сообщении № 240/22/2222 также приводит ряд исключений:

"...получение юридическим лицом лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации является обязательным в случае, если эта деятельность направлена на получение прибыли от выполнения работ или оказания услуг по технической защите конфиденциальной информации и (или) она необходима для достижения целей деятельности, предусмотренных в учредительных документах юридического лица, а также если это юридическое лицо (уполномоченное лицо) обеспечивает техническую защиту конфиденциальной информации при её обработке в соответствии с Федеральным законом "Об информации, информационных технологиях и о защите информации" по поручению обладателя информации конфиденциального характера и (или) заказчика информационной системы.

В случае, если деятельность по технической защите конфиденциальной информации не направлена на достижение целей деятельности, предусмотренных в учредительных документах, и (или) не связана с получением прибыли от выполнения указанных работ или оказания услуг, решение о необходимости получения соответствующей лицензии может быть принято юридическим лицом самостоятельно в соответствии с законодательством Российской Федерации".

В качестве "исключения к исключению" будет не лишним привести следующую позицию ФСТЭК заключающуюся в том, что **ФСТЭК имеет право разъяснять исключительно собственные документы, изданные ими же самими; все остальные "разъяснения" не имеют юридической силы и отражают лишь собственное мнение надзорного органа по применению определенных норм законодательства, которое нередко бывает ошибочным и оспаривается вышестоящей инстанцией или в судебном порядке.**

3. ПОЛУЧЕНИЕ ЛИЦЕНЗИЙ ФСТЭК НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ (ТЗКИ) И НА ДЕЯТЕЛЬНОСТЬ ПО РАЗРАБОТКЕ И ПРОИЗВОДСТВУ СРЕДСТВ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ (СЗКИ)

В данном разделе будут рассматриваться процедуры одновременного получения лицензий ФСТЭК на ТЗКИ и СЗКИ, т. к. они имеют много общего – лицензирующий орган, ряд лицензионных требований, экспедицию и т. п.

1.1. Перечень НПА, регламентирующих получение лицензии ФСТЭК

1.1.1. Перечень НПА, регламентирующих получение лицензии ФСТЭК на деятельность по ТЗКИ

При получении данной лицензии следует руководствоваться следующими документами:

- 1) Федеральный закон Российской Федерации от 04.05.2011 № 99-ФЗ "О лицензировании отдельных видов деятельности" [3];
- 2) Постановление Правительства РФ от 21.11.2011 № 957 "Об организации лицензирования отдельных видов деятельности" [8];
- 3) Постановление Правительства РФ от 03.02.2012 № 79 "О лицензировании деятельности по технической защите конфиденциальной информации" [16];
- 4) Перечень документов, необходимых для получения лицензии на деятельность по технической защите конфиденциальной информации (в соответствии с пунктом 8 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 03.02.2012 № 79) [17];
- 5) Информационное сообщение ФСТЭК России от 30.05.2012 № 240/22/2222 "По вопросу необходимости получения лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации" [18];
- 6) Приказ ФСТЭК России от 12.07.2012 № 83 "Административный регламент Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации" [19];
- 7) Приказ ФСТЭК России от 03.04.2012 "Перечень контрольно-измерительного и испытательного оборудования, средств контроля защищенности, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 № 79" [20];
- 8) Приказ ФСТЭК России от 16.03.2012 "Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите

конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 № 79" [21].

1.1.2. Перечень НПА, регламентирующих получение лицензии ФСТЭК на деятельность по разработке и производству СЗКИ

Перечень документации частично совпадает с предыдущим перечнем, однако имеет и некоторые отличия:

- 1) Федеральный закон Российской Федерации от 04.05.2011 № 99-ФЗ "О лицензировании отдельных видов деятельности" [3];
- 2) Постановление Правительства РФ от 21.11.2011 № 957 "Об организации лицензирования отдельных видов деятельности" [8];
- 3) Постановление Правительства РФ от 03.03.2012 № 171 "Положение о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации" [22];
- 4) Перечень документов, необходимых для получения лицензии на разработку и производство средств защиты конфиденциальной информации (в соответствии с пунктом 9 Положения о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 марта 2012 № 171) [23];
- 5) Приказ ФСТЭК России от 12.07.2012 № 84 "Административный регламент Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации" [24];
- 6) Приказ ФСТЭК России от 09.04.2012 "Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения видов работ, установленных Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 марта 2012 № 171" [25].

1.2. Основные требования и мероприятия для получения лицензий

Для получения лицензий на деятельность по ТЗКИ, по разработке и производству СЗКИ соискатель лицензии направляет или представляет в лицензирующий орган следующие документы:

- 1) Заявления о предоставлении лицензии с указанием:
 - видов работ и услуг;
 - полного и (в случае, если имеется) сокращенного наименования, в том числе фирменного наименования, и организационно-правовой формы юридического лица;
 - адреса места нахождения;
 - адреса для переписки;

- адреса мест осуществления лицензируемого вида деятельности;
 - государственного регистрационного номера записи о создании юридического лица (ОГРН);
 - наименования, серии и номера, даты выдачи документа, подтверждающего факт внесения сведений о юридическом лице в единый государственный реестр юридических лиц, наименования и адреса места нахождения органа, осуществившего государственную регистрацию юридического лица;
 - идентификационного номера налогоплательщика (ИНН);
 - наименования, серии и номера, даты выдачи документа, подтверждающего факт постановки юридического лица на учет в налоговом органе, наименования и адреса места нахождения налогового органа, осуществившего постановку на налоговый учет;
 - наименования должности, фамилии, имени, отчества, номеров телефонов, адреса электронной почты (при наличии) работника, уполномоченного по вопросам лицензирования.
- 2) Документ, подтверждающий уплату государственной пошлины за предоставление лицензии
 - 3) Копии учредительных документов юридического лица, засвидетельствованные в нотариальном порядке;
 - 4) Копии документов, подтверждающих квалификацию специалистов по защите информации (дипломов, удостоверений, свидетельств);
 - 5) Копии правоустанавливающих документов на помещения, предназначенные для осуществления лицензируемого вида деятельности, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним (в случае, если такие права зарегистрированы в указанном реестре, - сведения об этих помещениях);
 - 6) Копии технических паспортов и аттестатов соответствия защищаемых помещений требованиям безопасности информации;
 - 7) Копии технических паспортов автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации (с приложениями), актов классификации автоматизированных систем по требованиям безопасности информации, планов размещения основных и вспомогательных технических средств и систем, аттестатов соответствия автоматизированных систем требованиям безопасности информации или сертификатов соответствия автоматизированных систем требованиям безопасности информации, а также перечень защищаемых в автоматизированных системах ресурсов, описание технологического процесса обработки информации в автоматизированных системах;

- 8) Копии документов, подтверждающих право соискателя лицензии на программы для электронно-вычислительных машин и базы данных, планируемые к использованию при осуществлении лицензируемого вида деятельности;
- 9) Документы, содержащие сведения о наличии контрольно-измерительного, производственного и испытательного оборудования, средств защиты информации и средств контроля защищенности информации, необходимых для осуществления лицензируемого вида деятельности, с приложением копий документов о поверке (калибровке) и маркировании контрольно-измерительного оборудования, а также документов, подтверждающих права соискателя лицензии на использование указанного оборудования, средств защиты информации и средств контроля защищенности информации;
- 10) Документы, содержащие сведения об имеющихся технической документации, национальных стандартах и методических документах, необходимых для выполнения работ и (или) оказания услуг;
- 11) Копии документов, подтверждающих наличие необходимой системы производственного контроля в соответствии с установленными стандартами (для определённых видов работ);
- 12) Опись прилагаемых документов.

Документы (копии документов), указанные в настоящем перечне, если не указано специально, подписываются (заверяются) соискателем лицензии.

Ряд документов не является обязательным для предоставления, т. к. регулятор может получать их самостоятельно, но с учётом имеющихся реалий по организации межведомственного взаимодействия данные документы лучше предоставить самостоятельно.

То же верно и в отношении формы подачи документов – сугубо из практических соображений лучше не делать это в электронной форме.

Далее будут рассмотрены те позиции, которые вызывают вопросы и требуют разъяснений.

1.2.1. Заявления о предоставлении лицензии

Пакет документов на предоставление обеих лицензий может быть общим (например, приложена только одна копия Устава), однако необходимо приложить отдельные заявления на каждую из лицензий.

Заявления должны быть распечатаны на фирменном бланке организации. Если таковой отсутствует, что не редкость, можно ограничиться вставкой в верхний колонтитул первой страницы следующих данных:

- Наименование организации;
- ИНН;
- КПП;
- ОГРН;

- Адрес;
- Контактная информация (телефон, факс).

Если имеется возможность, лучше самостоятельно отвезти пакет документов в экспедицию ФСТЭК по адресу: г. Москва, Большой Козловский пер., д. 6, 4-й ОФПС.

Пакет документов должен быть вложен в запечатанный конверт. На конверте должна стоять печать организации.

Адресуется конверт следующим образом:

Кому: Начальнику 1 Управления ФСТЭК России

Куда: 105175, г. Москва, К-175, ул. Старая Басманная, д. 17

Опись документов (реестр на сдачу отправлений) должна быть представлена отдельно в двух экземплярах – один из них Вам вернут с отметкой о приёме. На реестрах также должна быть печать организации.

Реестр на сдачу отправлений делается также на фирменном бланке организации с указанием:

- Вида отправления (пакет);
- Важности (не секретный);
- Номера отправления (может быть номером одного из заявлений на предоставление лицензии);
- Наименования отправителя;
- Сдал / Принял (с указанием Ф.И.О., сдающего пакет).

Здание экспедиции достаточно неприметное и ориентиром могут служить муляжи (?) морских мин, расположенные во дворе.

Что касается указания в заявлениях видов работ и услуг: хочется всего и сразу, так сказать "про запас". Однако на определённые виды работ и услуг накладывается ряд требований, выполнение которых для организации может быть затруднительным и / или нецелесообразным.

Таблица ниже (Таблица 2) включает лицензионные требования для обеих лицензий и перечисляет работы и услуги с отметкой тех, которые не требуют наличия КИО и / или СМК. Для удобства визуального форматирования текста при табличном представлении работы и услуги приведены в таблице в более детальном виде, чем они представлены в соответствующих Постановлениях, но состав их идентичен законодательно определённому.

Таблица 2 - Лицензируемые виды работ и услуг

Деятельность	№ п/п	Работа / услуга	Не требует КИО	Не требует СМК
Техническая защита конфиденциальной информации	1	Контроль защищенности конфиденциальной информации от утечки по техническим каналам в средствах и системах информатизации		☒
	2	Контроль защищенности конфиденциальной информации от утечки по техническим каналам в технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается		☒
	3	Контроль защищенности конфиденциальной информации от утечки по техническим каналам в помещениях со средствами (системами), подлежащими защите		☒
	4	Контроль защищенности конфиденциальной информации от утечки по техническим каналам в помещениях, предназначенных для ведения конфиденциальных переговоров		☒
	5	Контроль защищенности конфиденциальной информации от несанкционированного доступа и её модификации в средствах и системах информатизации	☒	☒
	6	Сертификационные испытания технических средств защиты информации на соответствие требованиям по безопасности информации		
	7	Сертификационные испытания защищенных технических средств обработки информации на соответствие требованиям по безопасности информации		
	8	Сертификационные испытания технических средств контроля эффективности мер защиты информации на соответствие требованиям по безопасности информации		
	9	Сертификационные испытания программных (программно-технических) средств защиты информации на соответствие требованиям по безопасности информации		
	10	Сертификационные испытания защищенных программных (программно-технических) средств обработки информации на соответствие требованиям по безопасности информации		
	11	Сертификационные испытания программных (программно-технических) средств контроля защищенности информации на соответствие требованиям по безопасности информации		
	12	Аттестационные испытания и аттестация на соответствие требованиям		☒

Деятельность	№ п/п	Работа / услуга	Не требует КИО	Не требует СМК
		по защите информации средств и систем информатизации		
	13	Аттестационные испытания и аттестация на соответствие требованиям по защите информации помещений со средствами (системами) информатизации, подлежащими защите		☒
	14	Аттестационные испытания и аттестация на соответствие требованиям по защите информации защищаемых помещений		☒
	15	Проектирование в защищенном исполнении средств и систем информатизации	☒	☒
	16	Проектирование в защищенном исполнении помещений со средствами (системами) информатизации, подлежащими защите	☒	☒
	17	Проектирование в защищенном исполнении защищаемых помещений	☒	☒
	18	Установка, монтаж, испытания, ремонт технических средств защиты информации		☒
	19	Установка, монтаж, испытания, ремонт защищенных технических средств обработки информации		☒
	20	Установка, монтаж, испытания, ремонт технических средств контроля эффективности мер защиты информации		☒
	21	Установка, монтаж, испытания, ремонт программных (программно-технических) средств защиты информации	☒	☒
	22	Установка, монтаж, испытания, ремонт защищенных программных (программно-технических) средств обработки информации	☒	☒
	23	Установка, монтаж, испытания, ремонт программных (программно-технических) средств контроля защищенности информации	☒	☒
Разработка и производство СЗКИ	24	Разработка технических средств защиты информации		☒
	25	Разработка защищенных технических средств обработки информации		☒
	26	Разработка технических средств контроля эффективности мер защиты информации		☒
	27	Разработка программных (программно-технических) средств защиты информации	☒	☒
	28	Разработка защищенных программных (программно-технических) средств обработки информации	☒	☒

Деятельность	№ п/п	Работа / услуга	Не требует КИО	Не требует СМК
	29	Разработка программных (программно-технических) средств контроля защищенности информации	☒	☒
	30	Производство технических средств защиты информации	☐	☐
	31	Производство защищенных технических средств обработки информации	☐	☐
	32	Производство технических средств контроля эффективности мер защиты информации	☐	☐
	33	Производство программных (программно-технических) средств защиты информации	☒	☐
	34	Производство защищенных программных (программно-технических) средств обработки информации	☒	☐
	35	Производство программных (программно-технических) средств контроля защищенности информации	☒	☐

После анализа данной таблицы организация может составить представление о тех видах деятельности, требованиям которых она уже соответствует, для каких потребуется приобретение специального оборудования, а на какие виды ей не следует претендовать (данная деятельность среди активностей организации не предвидится, а материальные затраты существенные).

1.2.2. Лицензионный сбор

Лицензионный сбор составляет на данный момент 6 тыс. руб.

Реквизиты для оплаты [следующие](#):

Таблица 3 - Банковские реквизиты ФСТЭК России для уплаты государственных пошлин за совершение действий, связанных с лицензированием

Банк получателя	ОПЕРУ-1 Банка России г. Москва
БИК	044501002
Получатель	Межрегиональное операционное УФК (Федеральная служба по техническому и экспортному контролю, л/с 04951005870)
Сч. №	40101810500000001901
ИНН	7701350013
КПП	770101001

ОКАТО	45286555000
-------	-------------

В документе, подтверждающем оплату в федеральный бюджет, указываются следующие коды и источники доходов:

КБК 587 1 08 07081 01 0300 110 и вид платежа:

- государственная пошлина за предоставление лицензии на деятельность по <указывается вид деятельности> - оплата 6 тыс. рублей

На сайте ФСТЭК имеются уже подготовленные [шаблоны бланков](#) для оплаты в формате PDF.

Оплатить пошлину необходимо за каждую из лицензий.

1.2.3. Учредительные документы юридического лица

Данный пункт в особых пояснениях не нуждается.

Хочется только отметить, что Учредительные документы должны предоставляться со всеми последующими протоколами (приказами и т. п.), их изменяющими. Например, если произошла смена генерального директора, регулятору будет удивительно, что все документы при заявлении на лицензирование подписаны Ивановым, хотя в первоначальном Уставе организации фигурирует Петров.

1.2.4. Документы, подтверждающие квалификацию специалистов по защите информации

Организация должна иметь в своём штате специалистов, имеющих высшее профессиональное образование в области технической защиты информации, либо высшее техническое или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации.

Каких-либо конкретных требований по объёму часов обучения и имеющемуся стажу для различных видов работ и услуг не предъявляются³.

На практике нам хватило предъявить на каждого специалиста копии профильного Удостоверения о краткосрочном повышении квалификации государственного образца с объёмом обучения, составившим 72 часа, и диплома о высшем техническом образовании.

³ Утверждение справедливо только в отношении лицензионных требований ФСТЭК на деятельность по ТЗКИ. В отношении требований для получения другой лицензии определённость имеется: "наличие в штате у соискателя лицензии не менее 2 специалистов, имеющих высшее профессиональное образование в области технической защиты информации либо высшее техническое или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам разработки и (или) производства средств защиты информации".

В действительности лучше прикладывать копии всех имеющихся обучений, свидетельств, квалификаций, которые имеют отношение к математическим, техническим, программным дисциплинам, и конечно – к области обеспечения информационной безопасности.

В Положении и Регламенте в отношении лицензии на ТЗКИ также явным образом не регламентируется минимально необходимое количество специалистов: единственная косвенная конкретика – их должно быть больше одного (*"Юридические лица должны иметь в своём штате специалистов"*). А вот насколько больше? На деле оказалось (мы заявлялись практически на все работы и услуги, за исключением сертификационных испытаний), что достаточно иметь в штате двух специалистов.

1.2.5.Правоустанавливающие документы на помещения, предназначенные для осуществления лицензируемого вида деятельности

Раздел также достаточно тривиальный и не должен вызывать вопросов.

При формировании комплекта документов следует обращать внимание, чтобы выстроилась "полная цепочка": конечный субарендатор – арендатор – владелец здания - свидетельство о государственной регистрации права (на помещение).

Важно: Арендатор должен иметь подтверждённое право на сдачу помещения в субаренду, например, в виде документа "Согласие владельца на сдачу нежилых помещений в субаренду".

1.2.6.Технические паспорта и аттестаты соответствия защищаемых помещений требованиям безопасности информации

Т. к. на данном этапе заявитель ещё не обладает лицензией на соответствующие работы и услуги, за аттестатом соответствия ЗП и сопутствующими ему документами придётся обратиться к сторонней организации.

Нужно быть готовыми, что ЗП может потребовать установки определённых средств защиты для защиты от утечки защищаемой информации по различным каналам (акустика, виброакустика, ПЭМИН), что повлечёт за собой дополнительные финансовые затраты.

На данный момент порядок цен у московских организаций за аттестацию ЗП составляет порядка 60 – 80 тыс. руб.

Комплект средств защиты, включая его установку, стоит порядка 60 тыс. руб. При этом надо понимать, что номенклатура и количество СрЗИ зависит от конкретного ЗП (размера, места расположения, материалов стен) и сопутствующих условий (актуальности тех или иных каналов утечки).

За эту стоимость (60 тыс. руб.) комплект средств защиты будет следующим (Таблица 4):

Таблица 4 - Комплект средств защиты ЗП

№ п/п	Оборудование
1	Блок питания, управления и программирования генераторов-излучателей с модулем ИК управления

	Соната-ИПЗ
2	Пульт управления ИК 2-кнопочный
3	Генератор-аудиоизлучатель 5 октав Соната-СА-65М
4	Генератор-виброизлучатель 5 октав Соната-СВ-45М
5	Фиксатор тип 3 "Уголок"
6	Фиксатор тип 5 "Хомут 3/4"
7	Кабель с разъемом для подключения генераторов излучателей

По результатам работ по аттестации ЗП Вы получите следующий комплект документации (включая и необходимые для представления регулятору):

- Комплект документов на каждое СрЗИ (руководство по эксплуатации, свидетельство о приёмки, сертификат соответствия);
- Технический паспорт на ЗП;
- Программа и методика испытаний;
- Заключение по результатам аттестационных испытаний;
- Акт внедрения технических СрЗИ;
- Протокол инструментально-расчётной оценки защищённости помещения;
- Протокол инструментального контроля возможности возникновения радиоизлучений, модулированных информативным сигналом;
- Протокол классификации факторов, которые воздействуют на информацию в ЗП;
- Протокол оценки защищённости от утечки информации по каналам электроакустических преобразований;
- Аттестат соответствия требованиям по безопасности информации защищаемого помещения.

Важно: Номера помещений, как правило, не совпадают с номерами помещений в документах об аренде и / или праве собственности на помещения. И аттестат соответствия защищаемого помещения № 101 может вызвать у регулятора вопрос – на каком праве Вы владеете этим помещением, тогда как в документах об аренде говорится только о помещении 38-А? Нужна "процедура легализации", заключающаяся в издании приказа по организации "О нумерации помещений в арендуемой комнате", сопоставляющего нумерацию по плану БТИ с фактической.

1.2.7. Технические паспорта автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации, и аттестаты соответствия автоматизированных систем требованиям безопасности информации

В данном случае ситуация аналогичная с аттестатом на ЗП – необходимо обращаться в стороннюю организацию.

Стоимость работ по аттестации АС, состоящей из автономного АРМ, составляет также примерно 60 – 80 тыс. руб.

АС необходимо также обеспечить СрЗИ – антивирусным ПО, комплексом контроля и разграничения доступа, средством контроля защищенности информации, средством анализа защищенности.

На рынке существует много поставщиков решений, из тех, что наиболее на слуху – [ООО "ЦБИ"](#) [37].

Также АС в обязательном порядке должна иметь лицензионную ОС, прикладное ПО, офисный пакет.

Стоимость программных СрЗИ в составе:

- программный комплекс системы контроля и разграничения доступа на рабочей станции "Diamond ACS Agent Workstation Net";
- антивирусное ПО Dr.Web;
- средство анализа защищенности "Сканер-ВС" (на один ip-адрес);
- средство контроля защищенности информации "Ревизор-1 ХР";
- средство контроля защищенности информации "Ревизор-2 ХР";
- средство контроля защищенности информации "Терьер 3.0".

составляет порядка 25 тыс. руб.

Как правило, необходимый состав СрЗИ определяется на этапе подготовки к проведению аттестации АС.

По результатам работ по аттестации АС Вы получите следующий комплект документации (включая и необходимые для представления регулятору), который состоит как из полностью законченных документов, так и шаблонов документов, которые предстоит адаптировать и утвердить в организации:

- Акт внедрения СрЗИ;
- Акт классификации автоматизированной системы;
- Акт классификации ИСПДн;
- Аттестат соответствия АС требованиям по безопасности информации;

- Заключение по результатам аттестационных испытаний;
- Описание технологического процесса обработки информации;
- Перечень защищаемых ресурсов на объекте информатизации;
- Перечень факторов, воздействующих на защищаемую информацию на объекте информатизации;
- Программа и методика аттестационных испытаний;
- Протокол аттестационных испытаний;
- Технический паспорт АС;
- Технологическая инструкция АИБ;
- Технологическая инструкция пользователя.

1.2.8. Документы, подтверждающие право соискателя лицензии на программы для электронно-вычислительных машин и базы данных

В отношении этих продуктов необходимо приложить копии всех документов, которые имеются в наличии. Как то:

- Договор на закупку;
- Товарная накладная;
- Счёт-фактура;
- Акт предоставления прав;
- Лицензия (в том числе и экранные снимки).

Все документы должны быть оформлены исключительно на соискателя лицензии, что необходимо учитывать в случае "родственных" организаций, когда ПО закупается на "Фирма+", а распространяется также и на "Фирма-М".

Более того, даже если ПО свободного распространение (например, используется бесплатная САПР-платформа nanoCAD), лицензия (хоть и бесплатная) также должна быть оформлена на соискателя лицензии.

Данные требования не являются формальными, в своё время мы столкнулись с необходимостью досылки недостающих сведений именно по этой части.

1.2.9. Документы, содержащие сведения о наличии, а также документы, подтверждающие права соискателя лицензии, на контрольно-измерительное, производственное и испытательное оборудование, средства защиты информации и средства контроля защищенности информации

Данное требование является одним из самых финансово затратных пунктов в процессе получения лицензий ФСТЭК.

Следует отметить, что регулятор за нас уже определил номенклатуру необходимого контрольно-измерительного и испытательного оборудования, средств контроля защищенности [20], сопоставив необходимость его наличия с конкретными работами и услугами. Лицензиату остаётся лишь определиться с оборудованием конкретного производителя.

Для наших видов деятельности мы закупили следующее КИО (Таблица 5):

Таблица 5 - КИО

№ п/п	Наименование оборудования
1	"Тритон" (спектроанализатор цифровой интегрирующий)
2	Система оценки защищенности технических средств от утечки информации по каналу ПЭМИН "Сигурд-М19"
3	"Смарт" (селективный нановольтметр, анализатор СКМ-21.1)
4	Универсальная экранированная колонка УЭК в комплекте со штативом и полужесткой транспортной укладкой.
5	Генератор сигналов G3900H, 9 кГц- 3 ГГц с программным обеспечением
6	"ИМ-1" (магнитный индуктор, 20 Гц-300 МГц)
7	Цифровой осциллограф (Fп = 300 МГц)
8	Программа расчета показателей защищенности конфиденциальной информации "ГРОЗА-К"
9	"Агент инвентаризации" (программное средство для автоматизированного сбора информации об аппаратном и программном обеспечении АРМ и серверов, функционирующих под управлением операционных систем Windows).

В любом случае, выбор конкретного КИО определяется планируемыми к выполнению видами работ и услуг.

Мы провели достаточно объёмный анализ рынка с запросом коммерческих предложений и, учитывая опыт компаний, их репутацию, сроки поставок, время присутствия на рынке и, не в последнюю очередь, цену предложений, сделали свой выбор. Финансовые затраты на приобретение комплекта в нашем случае составили впечатляющую сумму около 1 800 тыс. рублей.

Однако на рынке есть и более заманчивые предложения, заключающиеся в поставке части КИО, находившегося ранее в эксплуатации. Тут цена зависит от нескольких факторов (степень

амортизации оборудования, состав "старого" оборудования) и одно из КП было "всего лишь" порядка 800 тыс. руб. Так что варианты имеются.

Срок поставки КИО в большинстве из опрошенных организаций составляет, как правило, от 8 недель, что необходимо учитывать при составлении план-графика лицензирования.

Кроме озвученных, имеется ещё один способ приобретения КИО – аренда. И если ранее такую аренду можно было сделать достаточно формальной - без передачи КИО лицензиату (один и тот же комплект КИО одновременно сдавался различным организациям), то в настоящее время регулятор следит за недопустимостью данного положения вещей. Теперь арендуемое КИО нужно иметь "на руках". Стоимость аренды составляет порядка 60 тыс. руб. в месяц. При такой стоимости следует оценить целесообразность приобретения оборудования в собственное владение, т. к. через 30 месяцев (2,5 года) за аренду придётся отдать сумму, равную "новому" комплекту КИО.

И, наконец, последний из известных мне вариантов "обретения" КИО – закупка необходимого комплекта на одну организацию с последующим заключением договора совместного владения с дружественной организацией. В таком случае, затраты можно разделить на обе организации с соблюдением легитимности владения. Данный вариант является абсолютно законным, т. к. лицензионные требования не ограничивают варианты только непосредственной покупкой в личное владение - "наличие на праве собственности или на ином законном основании".

Как и указывалось ранее [1.2.8], в качестве документов, подтверждающих наличие оборудования, нужно предоставить договора, счета, свидетельства о поверке, ...

Важно: Как правило, оборудование следует подвергать ежегодной поверке – не пропускайте сроки и закладывайте в бюджет расходы на поверку "парка" оборудования порядка 100 тыс. руб. в год.

1.2.10. Документы, содержащие сведения об имеющихся технической документации, национальных стандартах и методических документах

Как и в отношении КИО регулятор уже сформировал перечень документов с привязкой к определённым работам и услугам, которые необходимы в лицензионной деятельности и должны иметься у лицензиата [21], [25].

Хотя указания регулятора не оговаривают форму предоставления документов, практика показывает, что документы можно представить в виде следующих групп:

- В виде материальной копии (для документов ограниченного доступа);
- В электронном виде (для открытых документов).

Таблица ниже (Таблица 6) приводит распределение документов по той или иной группе:

Таблица 6 - Перечень технической документации, национальных стандартов и методических документов

Документы в соответствии с [21], [25]	Доступ	Допустимая форма владения ⁴	Источник получения документа
"Специальные требования и рекомендации по технической защите конфиденциальной информации" (СТР-К)	ограниченный	"бумажная" копия	ФСТЭК России
Извещения о корректировке СТР-К	ограниченный	"бумажная" копия	ФСТЭК России
Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам	ограниченный	"бумажная" копия	ФСТЭК России
Извещения о корректировке Сборника временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам	ограниченный	"бумажная" копия	ФСТЭК России
Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638	ограниченный	"бумажная" копия	ФСТЭК России
Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи. Утвержден приказом ФСТЭК России от 15 марта 2012 г. № 27дсп	ограниченный	"бумажная" копия	ФСТЭК России
ГОСТ Р 51624-2000	ограниченный	"бумажная" копия	Рособоронстандарт
ГОСТ Р 51583-2000	ограниченный	"бумажная" копия	Рособоронстандарт
Прочие документы	открытый	эл. вид	Электронная система информационно-правового обеспечения

Сведения об имеющихся технической документации, национальных стандартах и методических документах предоставляются в виде соответствующих перечней (желательно отдельных по каждой лицензии) с указанием:

- 1) Наименования имеющегося документа;

⁴ Ограничение на форму владения "в электронном виде" не препятствует владению документом в виде "материальной копии".

- 2) Инвентарного / учётного номера (в обязательном порядке требуется для документов ограниченного распространения);
- 3) Дополнительных сведений, включающих в себя ссылку на источник документа, как то:
 - Собственность;
 - Собственность. Копия 1 листа прилагается (для документов ограниченного распространения);
 - Заказан в Управлении ФСТЭК России по ЦФО, исх. № ____ от дд/мм/гггг (для заказанных, но не полученных документов ограниченного распространения);
 - Система "Консультант Плюс" / "Гарант", закуплена у ____, договор № ____ от дд/мм/гггг (для открытых документов в электронном виде).

Сроки получения документов достаточно длительные – от 1 до 2 месяцев. Лучше заказать документы на самых ранних этапах процедуры получения лицензий, чтобы к моменту подачи заявления они уже имелись в наличии.

1.2.10.1. Заказ документов в "Рособоронстандарт"

Документы ограниченного распространения, которые приобретаются не во ФСТЭК, являются ГОСТ'ами (с грифом "Для служебного пользования") на автоматизированные системы в защищённом исполнении.

Для заказа ГОСТ'ов в "Рособоронстандарте" (для покупки мы выбрали эту организацию) следует направить в их адрес официальное обращение на фирменном бланке, с печатью и подписью, примерно следующего содержания:

"Прошу Вас рассмотреть возможность направить в наш адрес государственные стандарты Российской Федерации. Данные документы необходимы нам для осуществления подготовительной работы по оформлению установленным порядком документов для получения лицензий на осуществление деятельности по технической защите конфиденциальной информации (в объёме, позволяющем осуществление мероприятий и оказание услуг по технической защите конфиденциальной информации от несанкционированного доступа) и на осуществление деятельности по разработке и (или) производству средств защиты конфиденциальной информации".

Необходимо также указать реквизиты организации, для выставления Вам счёта, документы, которые планируется приобрести, и необходимое количество экземпляров.

Стоимость документов незначительная – порядка 1,5 тыс. руб. каждый.

Письмо отправляется по адресу: 119421, г. Москва, ул. Новаторов, д. 40.

На имя: Директору ФГУП "Рособоронстандарт" Шепетило С. В.

Письмо лучше отвезти курьером, о чём следует предварительно договориться по т. (495) 936-28-98 – будет уверенность в том, что письмо доставлено, и что доставлено вовремя.

При получении ГОСТ'ов их следует учесть в организации и присвоить номера.

1.2.10.2. Заказ документов во ФСТЭК

Процедуры приобретения документов ФСТЭК аналогичны тому, как приобретаются ГОСТ'ы.

Письмо аналогичного содержания отправляется по адресу: 117342, г. Москва, Севастопольский проспект, д. 56/40, стр. 1.

На имя: *Руководителю Управления ФСТЭК России по ЦФО О. В. Райкову.*

Опять же, курьерская доставка предпочтительней в силу вышеозвученных причин. Согласовать приезд курьера можно по т. (495) 334-73-17.

После одобрения заявки ожидайте счёта на оплату от Воронежского ГНИИИ ПТЗИ – именно они поставляют необходимую документацию.

Порядок цен на их продукцию аналогичный – порядка 3 тыс. руб. за весь комплект.

При получении документы также необходимо учесть.

1.2.11. Документы, подтверждающие наличие необходимой системы производственного контроля

Для ряда видов работ и услуг (Таблица 2) необходимо подтвердить наличие в организации системы производственного контроля в "соответствии с установленными стандартами".

Что это должны быть за стандарты и кем они должны устанавливаться - прямых указаний у регулятора нет.

Наша практика и практика других организаций показывает, что ФСТЭК в качестве такого доказательства "охотно" принимает сертификат соответствия на СМК по стандарту ИСО 9001:2008.

Дополнительно к самой копии сертификата необходимо приложить сопутствующие документы, описывающие:

- Политику в области качества;
- Руководство по системе менеджмента качества;
- Форму годового плана проведения внутреннего аудита СМК;
- Форму программы внутреннего аудита;
- Форму чек-листа проведения внутреннего аудита СМК;
- Форму акта о несоответствии и корректирующих действиях;
- Форму отчета о проведении внутреннего аудита СМК;
- Процедуру управления несоответствующим продуктом;
- Процедуру корректирующих и предупреждающих действий.

1.3. Заключительные положения

Ещё раз в общих шагах определимся, что нужно сделать для получения лицензий ФСТЭК:

- Обеспечить (проконтролировать) квалификационные и количественные требования в отношении специалистов;
- Закупить литературу (срок поставки до 2 месяцев);
- Закупить КИО (срок поставки от 8 недель);
- Закупить (проконтролировать наличие) лицензионного ПО (включая СрЗИ, ОС, СУБД, прикладные приложения);
- Аттестовать ЗП (подготовить в процессе аттестации необходимый комплект документов);
- Аттестовать АС (подготовить в процессе аттестации необходимый комплект документов);
- Оплатить лицензионные сборы;
- Подготовить пакет документов (копии трудовых книжек, аттестатов, и т. п.), не имеющий "срока годности";
- Подготовить пакет документов с ограниченным сроком актуальности (нотариально заверенные копии выписок из различных реестров и т. п.);
- Собрать пакет финальный документов и направить во ФСТЭК.

После того, как заявка подана не стоит быть пассивным ожидателем, а лучше периодически звонить во ФСТЭК для уточнения статуса прохождения заявки – по телефону Вы узнаете о каких-то имеющихся замечаниях (вопросах) гораздо более оперативнее, чем с использованием почтовой переписки.

Контактный [телефон дежурного](tel:+74956321448): (495) 632-14-48, (495) 693-68-68.

В случае наличия замечаний досылайте недостающие / скорректированные документы аналогичным порядком – через экспедицию ФСТЭК. В своё время получение первой лицензии потребовало от нас порядка 5 итераций⁵ – тут нет ничего исключительного.

Как только Вы получите извещение о том, что лицензии оформлены, нужно будет записаться по вышеприведённому телефону на её получение.

Также нужно будет иметь на руках доверенность от организации на получение оных.

⁵ Со своей первой заявкой мы попали на период смены регламента лицензирования (переход к бессрочным лицензиям), что повлекло изменение ряда требований (например, по наличию системы СМК).

Лицензии выдаются один раз в неделю в строго определённое время по адресу: *г. Москва, ул. Старая Басманная, д. 17.*

Срок получения лицензий достаточно большой и, к сожалению, в силу большой нагрузки на сотрудников ФСТЭК, как правило, не укладывается в рамки, отведённые административным регламентом. В наших случаях он составил 2 – 3 месяца от момента подачи заявлений до оформления лицензий.

На личном опыте даже отдалённо не было такой ситуации, но помните: ФСТЭК России считает оказание государственных услуг по лицензированию деятельности по технической защите конфиденциальной информации и деятельности по разработке и производству средств защиты конфиденциальной информации функцией, при реализации которой наиболее вероятно возникновение коррупции [26].

Дабы не давать самому себе повода для повторных отправок и следующей из-за этого временной задержки – каждый лист предоставляемой во ФСТЭК документации (за исключением нотариально заверенных копий) должен быть с подписью руководителя организации и печатью "Копия верна". Или в случае объёмных документов – документ должен быть прошит нитью, нить должна быть заклеена, поверх неё проставлена печать и подпись, указано число прошитых листов.

4. ПОЛУЧЕНИЕ ЛИЦЕНЗИИ ФСБ НА ДЕЯТЕЛЬНОСТЬ ПО РАЗРАБОТКЕ, ПРОИЗВОДСТВУ, РАСПРОСТРАНЕНИЮ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ, ОКАЗАНИЮ УСЛУГ И ТЕХНИЧЕСКОМУ ОБСЛУЖИВАНИЮ⁶

Лицензирование деятельности в области шифрования информации, осуществляемое ФСБ России по поручению Правительства РФ, началось с Указа № 334 от 1995 г., который строго запрещал в стране любую деятельность, связанную с криптографией, без лицензий и сертификатов ФАПСИ.

А именно Указ № 334 запрещал:

- 1) Использование государственными организациями несертифицированных криптосредств, а также размещение государственных заказов на предприятиях использующих несертифицированные криптосредства;
- 2) Использование коммерческими банками несертифицированных криптосредств при взаимодействии с ЦБ РФ;
- 3) Деятельность юридических и физических лиц, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных средств, а также оказанием любых услуг в области шифрования информации;
- 4) Ввоз на территорию РФ шифровальных средств иностранного производства без разрешения ФАПСИ.

Другими словами, любая деятельность в области шифрования и любые криптосредства, не имеющие сертификата установленного образца, были вне закона.

Для того, чтобы примирить столь жесткую позицию государства в отношении криптографии с суровой действительностью, в законодательство о лицензировании криптографической деятельности неоднократно вносились дополнения и уточнения. На данный момент действует Постановление Правительства РФ от 16 апреля 2012 г. № 313 "О лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем...".

⁶ Приведено сокращённое название лицензии. Полное название звучит следующим образом: "Лицензия на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)".

Из лицензирования исключены криптосредства, по которым на практике не реально осуществить лицензионные мероприятия, включая:

- криптосредства, используемые с сотовых телефонах и кредитных картах;
- криптосредства, используемые в коммерческой телевизионной и радиоаппаратуре;
- криптосредства, применяемые в банкоматах и контрольно-кассовых машинах;
- криптосредства, реализующие симметричные алгоритмы шифрования с длиной ключа не более 56 бит;
- криптосредства, реализующие ассиметричные алгоритмы шифрования с длиной с максимальной длиной ключа 122 или 512 бит (в зависимости от вида алгоритма);
- и т. д.

Теперь к шифровальным средствам относят также и средства кодирования информации, поскольку использование слова "кодирование" вместо "шифрования" в технической документации - любимый способ обхода лицензионных ограничений отечественными разработчиками ПО и системными интеграторами.

Лицензии ФСБ России на шифровальную деятельность теперь выдаются бессрочно, а не на 5 лет как раньше, и лицензирование теперь не распространяется на техническое обслуживание криптосредств, выполняемое для собственных нужд, зато ужесточились требования к квалификации персонала лицензиата.

1.4. Перечень НПА, регламентирующих получение лицензии

- 1) Федеральный закон Российской Федерации от 04.05.2011 № 99-ФЗ "О лицензировании отдельных видов деятельности" [3];
- 2) Постановление Правительства РФ от 21.11.2011 № 957 "Об организации лицензирования отдельных видов деятельности" [8];
- 3) Постановление Правительства РФ от 16.04.2012 № 313 "Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)" [12];
- 4) Приказ ФСБ России от 30.08.2012 № 440 "От утверждении административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по осуществлению лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств,

информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)" [13].

1.5. Основные требования и мероприятия для получения лицензии

Для получения данной лицензии заявитель направляет в ЦЛСЗ ФСБ России (или свой территориальный орган, если организация не из Москвы или Московской области):

- 1) Заявление о предоставлении лицензии с указанием:
 - Полного, фирменного и сокращенного наименования юридического лица;
 - Организационно-правовой формы;
 - Должности и Ф.И.О. руководителя юридического лица;
 - Номеров и наименования работ в соответствии с перечнем работ и услуг;
 - Местонахождение заявителя;
 - Адреса мест осуществления лицензируемой деятельности;
 - Телефона/факса с указанием кода города;
 - ИНН и данных документа о постановке соискателя лицензии (лицензиата) на учет в налоговом органе;
 - ОГРН и данных документа, подтверждающего факт внесения сведений о юридическом лице в Единый государственный реестр юридических лиц.
- 2) Копии учредительных документов юридического лица, засвидетельствованные в нотариальном порядке;
- 3) Копии правоустанавливающих документов на помещения, здания, сооружения и иные объекты по месту осуществления лицензируемой деятельности, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;
- 4) Копии внутренних распорядительных документов, подтверждающих наличие условий для соблюдения конфиденциальности информации, необходимых для выполнения работ и оказания услуг, определенных Положением⁷, в соответствии с требованиями о соблюдении конфиденциальности информации, установленными Федеральным законом "Об информации, информационных технологиях и о защите информации";

⁷ Здесь и далее в данном разделе имеется в виду Постановление Правительства РФ от 16.04.2012 № 313 "Об утверждении Положения о лицензировании деятельности по разработке, производству, ...".

- 5) Копии документов, подтверждающих нахождение в штате соискателя лицензии на основной работе сотрудников;
- 6) Копии документов государственного образца (дипломы, аттестаты, свидетельства) об образовании, переподготовке, повышении квалификации по направлению "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей сотрудников;
- 7) Копии трудовых книжек сотрудников;
- 8) Копии должностных инструкций сотрудников;
- 9) Копии документов, подтверждающих наличие у соискателя лицензии приборов и оборудования, прошедших поверку и калибровку в соответствии с Федеральным законом "Об обеспечении единства измерений", принадлежащих ему на праве собственности или ином законном основании и необходимых для выполнения работ и оказания услуг, указанных в пунктах 1 - 11, 16 - 19 перечня работ и услуг;
- 10) Оригинал документов, подтверждающих оплату лицензионного сбора;
- 11) Опись прилагаемых документов.

Для экономии времени, если лицензия требуется организации "вчера", имеется "недекларированный" регламент нюанс – можно отправить неполный комплект в составе основных документов, а недостающие дослать несколько позже (по мере их готовности).

В этом случае, при получении первой партии документов заявка ставится на исполнение и начинает идти срок, отведённый регламентом – 45 рабочих дней.

Недостающие документы нужно выслать до визита назначенного куратора. Как правило, на это у организации имеется от 3 до 5 недель.

Минимальный перечень документов, которые необходимо приложить к заявке выглядит следующим образом:

- 1) Документы об аренде (праве собственности) помещений;
- 2) Документы относительно кадрового обеспечения (дипломы, трудовые книжки, приказы о приёме);
- 3) Документы, подтверждающие наличие условий для соблюдения конфиденциальности информации, необходимых для выполнения работ и оказания услуг.

Далее следует рассмотрение тех позиций, которые вызывают вопросы и / или имеют неоднозначное понимание.

1.5.1. Заявление о предоставлении лицензии

Заявление о предоставлении лицензии печатается на фирменном бланке организации.

Направляется заявление заказным письмом с уведомлением о вручении по следующему адресу⁸: 101000, г. Москва, ул. Б. Лубянка, д. 2, начальнику Центра по лицензированию, сертификации и защите государственной тайны ФСБ России Васюкову Юрию Константиновичу.

В заявлении необходимо указать перечень выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств.

Полный перечень составляет 28 пунктов и не все из них требуются в деятельности организации. Некоторые пункты являются "тяжёлыми" и организация не в состоянии выполнить лицензионные требования, связанные с ними.

Ниже приведена таблица с агрегированной информацией с различиями в лицензионных требованиях по видам деятельности с шифровальными средствами (Таблица 7):

⁸ Речь идёт о практике получения лицензии для организации Московского региона. Организации из других регионов должны направлять заявления в свои территориальные управления.

Таблица 7 - Различия в лицензионных требованиях по видам деятельности с шифровальными средствами

№ п/п	Выполняема работа / оказываемая услуга	ГТ	1000 / 5	500 / 3	100 / 0	КИО
Номер работы / услуги согласно Перечня	Выполняема работа / оказываемая услуга	Требование по наличию лицензии к выполнению работ и оказанию услуг, связанных с использованием сведений, составляющих ГТ	Требование по наличию в штате у соискателя лицензии квалифицированного персонала с высшим профессиональным образованием по направлению подготовки "Информационная безопасность" (сроком обучения свыше 1000 аудиторных часов) и стажем в заявленной области деятельности не менее 5 лет	Требование по наличию в штате у соискателя лицензии квалифицированного персонала с высшим профессиональным образованием по направлению подготовки "Информационная безопасность" (сроком обучения свыше 500 аудиторных часов) и стажем в заявленной области деятельности не менее 3 лет	Требование по наличию в штате у соискателя лицензии квалифицированного персонала с высшим профессиональным образованием по направлению подготовки "Информационная безопасность" (сроком обучения свыше 100 аудиторных часов)	Требования по наличию приборов и оборудования
1	Разработка шифровальных (криптографических) средств	☑	☑			
2	Разработка защищенных с использованием шифровальных (криптографических) средств информационных систем			☑		
3	Разработка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем			☑		
4	Разработка средств изготовления ключевых документов	☑	☑			

№ п/п	Выполняема работа / оказываемая услуга	ГТ	1000 / 5	500 / 3	100 / 0	КИО
5	Модернизация шифровальных (криптографических) средств	☑	☑			
6	Модернизация средств изготовления ключевых документов	☑	☑			
7	Производство (тиражирование) шифровальных (криптографических) средств			☑		
8	Производство защищенных с использованием шифровальных (криптографических) средств информационных систем			☑		
9	Производство защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем			☑		
10	Производство средств изготовления ключевых документов			☑		
11	Изготовление с использованием шифровальных (криптографических) средств изделий, предназначенных для подтверждения прав (полномочий) доступа к информации и (или) оборудованию в информационных и телекоммуникационных системах			☑		
12	Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств			☑		

№ п/п	Выполняема работа / оказываемая услуга	ГТ	1000 / 5	500 / 3	100 / 0	КИО
13	Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем			☑		
14	Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем			☑		
15	Монтаж, установка (инсталляция), наладка средств изготовления ключевых документов			☑		
16	Ремонт шифровальных (криптографических) средств	☑	☑			☑
17	Ремонт, сервисное обслуживание защищенных с использованием шифровальных (криптографических) средств информационных систем			☑		☑
18	Ремонт, сервисное обслуживание защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем			☑		☑
19	Ремонт, сервисное обслуживание средств изготовления ключевых документов	☑	☑			☑
20	Работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд)			☑		

№ п/п	Выполняема работа / оказываемая услуга	ГТ	1000 / 5	500 / 3	100 / 0	КИО
	юридического лица или индивидуального предпринимателя)					
21	Передача шифровальных (криптографических) средств				☑	
22	Передача защищенных с использованием шифровальных (криптографических) средств информационных систем				☑	
23	Передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем				☑	
24	Передача средств изготовления ключевых документов				☑	
25	Предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей			☑		
26	Предоставление услуг по имитозащите информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей			☑		

№ п/п	Выполняема работа / оказываемая услуга	ГТ	1000 / 5	500 / 3	100 / 0	КИО
27	Предоставление юридическим и физическим лицам защищенных с использованием шифровальных (криптографических) средств каналов связи для передачи информации			☑		
28	Изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств			☑		

На основании данной таблицы можно сформировать понимание о тех видах деятельности, которым организация удовлетворяет уже сейчас, на обеспечение каких нужно закупить соответствующее оборудование и / или нанять дополнительный квалифицированный штат, если они необходимы в деятельности организации, а от каких видов деятельности лучше отказаться.

Так, с минимальными усилиями – без длительного обучения сотрудников и дополнительных затрат, - можно претендовать на лицензию со следующими видами деятельности: **21 – 24**.

Перечень разрешённых видов деятельности при этом весьма скромный, но многие организации в рамках PR активностей анонсируют лишь само наличие лицензии ФСБ без указания перечня видов деятельности. С маркетинговой точки зрения может быть востребованной и такая "неполная" лицензия.

В более приземлённом варианте, если организация в своей деятельности не занимается "чистой" криптографией (например, не является разработчиком СКЗИ), не имеет лицензий на предоставление каналов связи, а также не планирует заниматься ремонтом криптографического оборудования, то она может претендовать на более полный перечень разрешённых активностей. В этом случае он может включать в себя такие виды, как: **2, 3, 8, 9, 11, 12, 13, 14, 17, 18, 20, 21, 22, 23, 25, 26, 28**.

11 и 28 виды являются довольно специфичными и, если ими не планируется заниматься, лучше в своём заявлении от них отказаться, т. к. если они затребованы "для галочки", то после проверки в лицензировании данных видов может быть отказано.

1.5.2. Учредительные документы юридического лица

Данный пункт в особых пояснениях не нуждается.

Хочется только отметить, что Учредительные документы должны предоставляться со всеми последующими протоколами (приказами и т. п.), их изменяющими. Например, если произошла смена генерального директора, регулятору будет удивительно, что все документы при заявлении на лицензирование подписаны Ивановым, тогда как в первоначальном Уставе организации фигурирует Петров.

1.5.3. Правоустанавливающие документы на помещения, здания, сооружения и иные объекты по месту осуществления лицензируемой деятельности, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним

Раздел также достаточно тривиальный и не должен вызывать вопросов.

При формировании комплекта документов следует обращать внимание, чтобы выстроилась "полная цепочка": конечный субарендатор – арендатор – владелец здания - свидетельство о государственной регистрации права (на помещение).

Важно: Арендатор должен иметь подтверждённое право на сдачу помещения в субаренду, например, в виде документа "Согласие владельца на сдачу нежилых помещений в субаренду".

1.5.4. Внутренние распорядительные документы, подтверждающие наличие условий для соблюдения конфиденциальности информации, необходимых для выполнения работ и оказания услуг

Как правило, под основным документом, подтверждающим наличие необходимых условий, понимается аттестат соответствия автоматизированной системы (АС) требованиям безопасности информации. И хотя законодательством РФ предусмотрены также и другие формы подтверждения, а аттестация АС является обязательной только в ряде случаев, но данная форма подтверждения вызывает наименьшие вопросы со стороны регулятора и является, если можно так выразиться, стандартом "де-факто".

Также, помимо аттестата соответствия требованиям безопасности информации, потребуются (с учётом заявленных видов деятельности):

- 1) Журнал учёта СКЗИ;
- 2) Журнал учёта ключевых документов;
- 3) Инструкция администратору безопасности СКЗИ;
- 4) Инструкция по обращению с шифровальными средствами;
- 5) Приказ о допуске в помещения (в которых будет осуществляться лицензируемая деятельность);
- 6) Приказ о допуске сотрудников к работам с СКЗИ;
- 7) Приказ об утверждении инструкций и журналов.

В качестве основы для формирования разделов инструкций можно взять приказ ФСБ от 9 февраля 2005 г. № 66 "Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации" (Положение ПКЗ-2005).

Формы журналов хорошо представлены в приказе ФАПСИ от 13 июня 2001 г. № 152 "Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну".

1.5.5. Документы, подтверждающие нахождение в штате соискателя лицензии на основной работе сотрудников

Необходимо приложить копии трудовых книжек специалистов, имеющих необходимые записи.

Можно также приложить копию договора о приёме на работу, но данный документ не является обязательным.

Что касается возможности работы специалистов по совместительству – на эту тему на различных форумах сломано немало копий ([38] – [40]). Практика показывает, что решение по

данному вопросу принимается регулятором сугубо в индивидуальном порядке, а также зависит от территориального управления, в котором рассматривается заявка.

Если формально следовать духу закона, то он требует "*нахождение в штате ... на основной работе сотрудников*", что не предусматривает совместительства. Однако мне известны случаи, когда регулятор шёл в данном вопросе на встречу соискателю.

1.5.6. Документы государственного образца (дипломы, аттестаты, свидетельства) об образовании, переподготовке, повышении квалификации по направлению "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей сотрудников

Один из самых животрепещущих разделов в свете требований, предъявляемых к квалификации ПП № 313 для выполнения ряда видов деятельности.

Для руководителей и инженерно-технических работников лицензиата (которых должно быть не менее 2 человек) в зависимости от вида лицензируемой шифровальной деятельности установлены требования к подготовке по специальности по направлению "Информационная безопасность" в объеме от 100 до 1000 аудиторных часов и опыту работы от 3 до 5 лет.

Между прочим, 1000 аудиторных часов - это полноценный институтский курс по информационной безопасности, читаемый в течении 5 - 6 лет.

Эти требования служат камнем преткновения для многих организаций, решившихся легализовать свою деятельность в области криптографии. Далеко не каждый может себе позволить отправить своих сотрудников на курсы повышения квалификации в области ИБ на срок от месяца до полугода.

Бесспорным выходом из этой ситуации до 1 сентября 2013 г. служило прохождение дистанционного обучения по направлению ИБ с получением дипломов государственного образца. Однако, с вступлением в силу нового ФЗ "Об образовании в Российской Федерации" с 01.09.2013 с получением документов государственного образца всё стало не так однозначно.

Ещё один тонкий момент, на который многие соискатели не обращают внимания - опыт работы от 3 до 5 лет должен быть "*в рамках лицензируемой деятельности*". Что это означает на практике? Ваш не столь уж малый опыт деятельности (от 3 до 5 лет) должен быть в организации, уже имеющей лицензию ФСБ. Всё это время Вы должны были работать у лицензиата! И лицензия у него должна была быть не вчера или с прошлой недели, а все эти 3 – 5 лет. Только тогда к Вашему стажу можно будет апеллировать в заявлении (если Вы перешли на новое место работы и озаботились вопросом получения лицензии на этом месте), только тогда он будет легитимен.

В связи со сложившейся ситуацией даже появился рынок "специалистов с профильным образованием и стажем"⁹. В полном согласии с законами рынка спрос родил предложение.

⁹ Например, [здесь](#)

Хорошая статья, затрагивающая данные вопросы, опубликована [на сайте](#) Центра исследования безопасности информационных технологий (ЦИБИТ) [33]. Приведу некоторые её положения.

Раньше требование по стажу было более мягким - требовался стаж в **области защиты информации**. Теперь требуется стаж в **заявленной области** (т. е. стаж работы с шифровальными (криптографическими) средствами). Раньше достаточно было пройти повышение квалификации в объеме 72 часов. Теперь на самый простой вид деятельности – распространение – требуется наличие специалиста с высшим или средним профессиональным образованием по направлению подготовки "Информационная безопасность" в соответствии с действующим Общероссийским классификатором специальностей (ОКСО), и (или) прошедшем повышение квалификации в объеме более 100 аудиторных часов по одной из специальностей этого направления. На предоставление услуг и техническое обслуживание – требуется наличие не менее двух специалистов с высшим образованием по направлению подготовки "Информационная безопасность", и (или) прошедших профессиональную переподготовку в объеме более 500 аудиторных часов по одной из специальностей того же направления подготовки, а также имеющих стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 3 лет.

Требование наличия в штате лицензиата такого квалифицированного персонала представляется наиболее сложным.

Кроме количественных требований к стажу и объему часов в дополнительных программах в Положении о лицензировании содержатся еще два принципиальных требования:

- 1) Основное высшее (среднее) профессиональное образование и (или) дополнительное образование для представителей лицензиатов должно соответствовать специальностям по направлению подготовки "Информационная безопасность", установленным в действующем Общероссийском классификаторе специальностей (ОКСО);
- 2) Если представители лицензиатов получают дополнительное образование по указанным специальностям, то они должны представить в лицензирующий орган копии документов о дополнительном образовании государственного образца.

Именно по содержанию и условиям реализации этих двух требований у представителей лицензиатов и возникает наибольшее число вопросов и различных толкований, причем, подчас некорректных.

1.5.6.1. Общероссийский классификатор специальностей (ОКСО)

В направление подготовки "Информационная безопасность" (090000) ОКСО входят семь специальностей подготовки специалистов с высшим профессиональным образованием:

- 1) Криптография (090101);
- 2) Компьютерная безопасность (090102);
- 3) Организация и технология защиты информации (090103);
- 4) Комплексная защита объектов информатизации (090104);

- 5) Комплексное обеспечение информационной безопасности автоматизированных систем (090105);
- 6) Информационная безопасность телекоммуникационных систем (090106);
- 7) Противодействие техническим разведкам (090107).

Кроме того, в направление подготовки "Информационная безопасность" (090000) входит одна специальность подготовки специалистов со средним профессиональным образованием: Информационная безопасность (090108).

В системе ДПО по этой специальности может проводиться лишь **среднее** дополнительное профессиональное образование (ДПО). Однако на рекламных страницах официальных сайтов некоторых образовательных учреждений в системе ДПО можно найти объявления о том, что эти учреждения осуществляют профессиональную переподготовку (объемом свыше 500 аудиторных часов) специалистов для получения лицензии ФСБ России в соответствии с Положением именно по специальности "Информационная безопасность" (090108). Понятно, что такая реклама явно дезинформирует заказчиков.

Следует отметить, что в действующий ОКСО формально не входит направление подготовки "Информационная безопасность" (090900) высшего профессионального образования, подтверждаемого присвоением квалификации "бакалавр". Направление "Информационная безопасность" (090900) для бакалавров предусмотрено Перечнем, утвержденным Приказом Минобрнауки от 17.09.2009 № 337.

Но Приказом Минобрнауки от 17.02.2011 № 201 определено соответствие этого направления для бакалавров и направления подготовки "Информационная безопасность" (090000), а также входящим в него специальностям из ОКСО. Действующий Федеральный Закон "Об образовании" разрешает Минобрнауки устанавливать такое соответствие и обязывает образовательные организации руководствоваться установленными соответствиями. Таким образом, диплом бакалавра по направлению подготовки "Информационная безопасность" (090900) также соответствует требованиям Положения о лицензировании. Кроме того, по этому направлению может проводиться и дополнительное образование, требуемое в Положении.

Все указанные специальности по направлению подготовки "Информационная безопасность" (090000) из действующего ОКСО, соответствуют федеральным государственным образовательным стандартам (ФГОС ВПО) второго поколения. Классификатор специальностей, соответствующих Федеральным государственным стандартам (ФГОС ВПО) третьего поколения, утвержденным в январе 2011 года, пока не введен, да и сами стандарты в настоящее время перерабатываются в соответствии с новым ФЗ "Об образовании в Российской Федерации", вступившим в силу с 01 сентября 2013 года.

1.5.6.2. Документы государственного и установленного образца

До момента вступления в силу ФЗ "Об образовании в Российской Федерации" Минобрнауки различало два вида документов об образовании в системе ДПО: документы **государственного и установленного** образца.

В письме Минобрнауки России от 27.07.2012 № АК-51/06 "О выдаче документов государственного образца" специально давалось разъяснение:

"В связи с многочисленными обращениями граждан и организаций по вопросу выдачи документов государственного образца по образовательным программам дополнительного профессионального образования Минобрнауки России информирует.

В настоящее время лицам, завершившим обучение по образовательным программам дополнительного профессионального образования (далее – ОП ДПО), выдаются документы как государственного, так и установленного образца.

"Образовательное учреждение имеет право выдавать документы государственного образца только по аккредитованным образовательным программам" (Пункт 23 статьи 33.2 Закона об образовании).

"...документы **государственного образца** могут выдаваться лицам, завершившим обучение:

по образовательным программам повышения квалификации и профессиональной переподготовки, указанным в свидетельстве об аккредитации, если на момент завершения обучения у образовательного учреждения не истек срок государственной аккредитации по этим программам....

Если образовательное учреждение не имеет государственной аккредитации по реализуемым им образовательным программам, то в соответствии с лицензией выдает лицам, прошедшим итоговую аттестацию, документы о соответствующем образовании и (или) квалификации **установленного образца**. Форма указанных документов определяется самим образовательным учреждением".

В процитированном Письме Минобрнауки приведено лишь два из трех обязательных условий, выполнение которых давало право образовательному учреждению выдавать документы об образовании государственного образца.

Для лучшего и точного понимания требования Положения о лицензировании воспроизведем без изъятия начало п. 2 статьи 27 "Документы об образовании" Закона "Об образовании":

"...2. Образовательное учреждение или научная организация, имеющие государственную аккредитацию, выдают по реализуемым ими аккредитованным образовательным программам лицам, прошедшим государственную (итоговую) аттестацию, документы государственного образца об уровне образования и (или) квалификации, кроме случаев, предусмотренных Федеральным законом от 10 ноября 2009 года № 259-ФЗ "О Московском государственном университете имени М.В. Ломоносова и Санкт-Петербургском государственном университете...".

Таким образом, организация-заказчик образовательной услуги при выборе образовательного учреждения для подготовки к получению лицензии ФСБ России должна была убедиться в том, что это учреждение:

– Аккредитовано;

- Имеет необходимые аккредитованные дополнительные профессиональные образовательные программы по соответствующим специальностям из ОККО;
- В состоянии организовать и провести в установленном порядке государственную (итоговую) аттестацию по итогам обучения.

Образовательное учреждение имело право выдавать документы об образовании государственного образца, только если оно удовлетворяло одновременно этим трем условиям.

Как правило, образовательные учреждения, работающие на рынке образовательных услуг, имели и аккредитацию, и аккредитованные программы.

Вузы, реализующие дополнительные профессиональные образовательные программы вне своих основных образовательных программ (МФТИ, МАИ, МИФИ и др.), а также образовательные учреждения из системы ДПО, заключившие соответствующие соглашения с такими вузами, проводили государственную (итоговую) аттестацию установленным порядком в соответствии с требованиями федеральных государственных образовательных стандартов.

По ФЗ "Об образовании в Российской Федерации", вступившим в силу с 01 сентября 2013 года, в системе ДПО теперь выдаются документы об образовании установленного образца, поскольку государственная (итоговая) аттестация в Законе заменена в системе ДПО на итоговую аттестацию.

Как разрешится вопрос о несоответствии требований Положения этой новой норме – трудно сказать. Возможно, будет определен некоторый переходный период до корректировки Положения. Непонятно также, каким образом будут разрабатываться новые дополнительные программы по направлению "Информационная безопасность". Во всяком случае, Минобрнауки так и не определилось с Порядком их разработки. На их сайте имеется лишь проект соответствующего приказа.

С полным текстом этой познавательной статьи можно ознакомиться по этому [адресу](#).

У другого игрока на рынке образовательных программ существует несколько иная точка зрения на имеющееся положение вещей. Согласно ей нормы ПП № 313 и ФЗ "Об образовании в Российской Федерации" непротиворечивы и могут быть решены в рамках имеющегося законодательства:

*"В соответствии с ч. 1. ст. 92 Федерального закона от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации", который вступил в силу с 01.09.2013 **Государственная аккредитация образовательной деятельности проводится по основным образовательным программам, реализуемым в соответствии с федеральными государственными образовательными стандартами**, за исключением образовательных программ дошкольного образования, **а также по основным образовательным программам, реализуемым в соответствии с образовательными стандартами.***

*Программы профессиональной переподготовки к указанным категориям не относятся и **по ним, не установлены образовательные стандарты.***

В соответствии с ч. 3 ст. 60 указанного Закона, лицам, успешно прошедшим итоговую аттестацию, **выдаются документы об образовании и (или) о квалификации, образцы которых самостоятельно устанавливаются организациями, осуществляющими образовательную деятельность.**

В соответствии с ч. 8 ст. 108 указанного Закона, **свидетельства о государственной аккредитации в части имеющих государственную аккредитацию дополнительных профессиональных образовательных программ являются недействующими** со дня вступления в силу настоящего Федерального закона.

В соответствии с ч. 5 ст. 111 указанного Закона, со дня его вступления в силу, **нормативные правовые акты Президента Российской Федерации, Правительства Российской Федерации, федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, регулирующие отношения в сфере образования, применяются постольку, поскольку они не противоречат настоящему Федеральному закону** или издаваемым в соответствии с ним иным нормативным правовым актам Российской Федерации.

Таким образом, Постановление правительства РФ от 16.04.2012 № 313, после 1 сентября 2013 г. применяется в части, в которой оно не противоречит новому закону об образовании в РФ, то есть в части требования документов государственного образца, оно не действует. Поэтому органы ФСТЭК и ФСБ обязаны будут принимать документы о квалификации установленного образца".

Думаю, что со временем один из регуляторов (или совместно) должен выпустить информационное сообщение или извещение, проясняющее данные спорные вопросы.

А пока нужно формально следовать букве закона или быть готовыми отстаивать перед регулятором (а возможно – и в суде) изложенную выше позицию относительно нынешней нелегитимности требований документов государственного образца.

В качестве послесловия к данному разделу, отражающему если не невозможность, то крайнюю трудность выполнения имеющихся требований:

- Вы действительно думаете, будто мы хотим, чтобы эти законы соблюдались? - начал доктор Феррис. - Мы хотим, чтобы они нарушались. Вам лучше бы запомнить: вы имеете дело не с группой бойскаутов, и время красивых жестов прошло. За нами сила, и мы это знаем. Ваши друзья - паиньки, а мы знаем истинное положение вещей, и вам следует быть умнее. Крайне сложно управлять невинными людьми. Единственная власть, которой обладает правительство, - сила, способная сломать преступный элемент. Ну а если преступников недостаточно, нужно их создавать. Принимается такое количество законов, что человеку невозможно существовать не нарушая их. Кому нужна нация, состоящая сплошь из законопослушных граждан? Какая от нее польза? А вот издайте законы, которые нельзя будет ни соблюдать, ни проводить в жизнь, ни объективно трактовать, и вы получите нацию нарушителей, а значит сможете заработать на преступлениях. Сейчас это вошло в систему, мистер Риарден, это игра, и когда вы усвоите её правила, с вами станет гораздо легче иметь дело.

Айн Рэнд, "Атлант расправил плечи"

1.5.7. Должностные инструкции сотрудников

В должностных инструкциях сотрудников должна в явном виде указываться деятельность, связанная с видами деятельности, на которые претендует заявитель.

В инструкциях обязательно должны быть указаны функциональные обязанности, права и ответственность сотрудника.

Фактуру для должностных инструкций, в части формирования требований к квалификации и должностных обязанностей, можно брать из соответствующих ФГОС и квалификационных требований (их проектов). Тексты ФГОС (в том числе и в области ИБ) представлены на портале [Минобрнауки](#) и находятся на данной странице стандартным поиском по ключу "090".

Также за необходимыми квалификационными требованиями можно обратиться на сайт ассоциации АП КИТ (например, [сюда](#) и [сюда](#)).

1.5.8. Лицензионный сбор

Лицензионный сбор составляет на данный момент 6 тыс. руб.

Реквизиты для оплаты [следующие](#):

Счет - 40101810800000010041;

Банк получателя — Отделение 1 Московского ГТУ Банка России, г. Москва;

БИК банка- 044583001;

получатель - УФК по г. Москве в/ч 93967;

Л/сч - № 04731528140;

ИНН/КПП 7702232171/770203002;

ОКАТО - 45286570000;

ББК 189 1 08 07081 01 0300 110 – предоставление лицензии.

Информация о реквизитах для оплаты государственной пошлины за лицензии, которые предоставляются, переоформляются, продлеваются территориальными органами безопасности, уточняется в органах безопасности по месту нахождения заявителя (соискателя лицензий или лицензиата).

Оплату государственной пошлины следует производить строго по месту нахождения заявителя.

1.6. Заключительные положения

Фактический срок получения лицензии составляет примерно 2 месяца после подачи заявления, что соответствует регламенту.

Для получения оригинала лицензии необходимо будет предоставить соответствующую доверенность от организации.

Из документов, не указанных в административном регламенте, рекомендуется подготовить и предоставить следующие:

- 1) Сведения о специалистах, допущенных к работе с шифровальными средствами (указываются лица, их образование, стаж в заявленной деятельности, имевшиеся должностные обязанности);
- 2) Сведения, обосновывающие наличие необходимых условий для выполнения работ и услуг по заявленному виду деятельности. Приводятся:
 - основные направления деятельности организации;
 - заявленные виды работ и услуг;
 - описание структуры организации и её подразделений (с указанием их специализации), осуществляющих работы по каждому из заявляемых видов деятельности;
 - статус компании по отношению к ведущим фирмам-производителям программного обеспечения, вычислительной техники, телекоммуникационного оборудования;
 - перечень имеющихся производственных помещений, удовлетворяющих (имеющих соответствующий аттестат) режимным требованиям, санитарным нормам и правилам, требованиям безопасности труда и охраны окружающей среды;
 - режим охраны;
 - перечень и характеристика производственного и испытательного оборудования, а также инструмента, имеющегося для осуществления заявленных видов деятельности и соответствующего нормативно-методическим требованиям;
 - имеющиеся средства защиты информации (МСЭ, антивирус, ...);
 - метрологическое обеспечение работ, проводимых в рамках лицензируемой деятельности;
 - перечень и характеристика имеющихся информационно-вычислительных средств, задействованных в процессе осуществления заявленных видов деятельности;
 - наличие условий для профилактики и ремонта используемого производственного и испытательного оборудования;
 - наличие необходимых технологических условий для осуществления заявленных видов деятельности;
 - данные о внутрипроизводственной системе контроля качества (например, сертификат соответствия по ISO 9001:2008);

- перечень поставщиков материалов, элементной базы, комплектующих изделий и оборудования, входящих в состав изделий с отдельным указанием поставщиков шифровальных средств;
 - перечень субподрядчиков (при наличии таковых) с указанием выполняемых ими работ и договоров, на основании которых данные субподрядчики привлекаются;
 - перечень ранее выполненных и предполагаемых к выполнению работ по заявленным видам деятельности с указанием заказчиков (потребителей продукции);
 - сведения об обеспечении организации конструкторской, технологической, нормативной и методической документацией;
 - другая дополнительная информация.
- 3) Проекты договоров (о поставке, использовании, сопровождении) криптографических средств.

Данная информация поможет понять регулятору всю серьёзность Ваших намерений, Вашу степень подготовленности и обоснованность притязаний на те или иные виды деятельности. А также заранее снимет массу вопросов, которые могут возникнуть на этапе выездной проверки соответствия лицензионным требованиям. Хотя данные документы не предусмотрены административным регламентом, но по факту будут у Вас запрошены в качестве дополнительной информации после подачи Вами заявления. Так что лучше приложить их сразу.

5. ПОЛУЧЕНИЕ ЛИЦЕНЗИИ ФСБ НА ОСУЩЕСТВЛЕНИЕ РАБОТ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ¹⁰

Данная лицензия ФСБ необходима организациям, деятельность которых предполагает использование сведений, составляющих государственную тайну, для участия в различных тендерах и сотрудничества с госпредприятиями по закрытой тематике.

Лицензия ФСБ выдается Федеральной службой безопасности Российской Федерации, а в регионах на территории Российской Федерации – её территориальными органами.

По Москве и Московской области лицензирование осуществляет [ЦЛСЗ ФСБ России](#).

1.7. Перечень НПА, регламентирующих получение лицензии

- 1) Федеральный закон Российской Федерации от 21.07.1993 № 5485-1 "О государственной тайне" [2];
- 2) Постановление Правительства РФ от 15.04.1995 № 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" [14];
- 3) Приказ Федеральной службы безопасности Российской Федерации от 27.02.2009 № 75 "Об утверждении административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию 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" [15].

1.8. Основные требования и мероприятия для получения лицензии

Для получения данной лицензии ФСБ заявитель предоставляет в ФСБ России:

- 1) Заявление о выдаче лицензии с указанием:
 - Наименования и организационно-правовой формы, места нахождения предприятия, адресов мест осуществления лицензируемого вида деятельности, номера расчетного счета в банке и наименования банка;
 - Почтового адреса предприятия, контактного телефона/факса;
 - Вида деятельности, на осуществление которого должна быть выдана лицензия;
 - Срока действия лицензии (не более 5 лет);

¹⁰ Материал данного раздела, кроме привнесённого собственного опыта нашей организации, в подавляющем своём объёме написан на основании материалов компании [ООО "Научно-производственный центр "СОТИС"](#).

Важно: В случае использования услуг стороннего РСП указываемый срок действия лицензии (срок окончания её действия) не может быть большим, чем срок окончания действия лицензии РСП.

- Сведений о наличии допуска к государственной тайне у руководителя предприятия, а также сведений о наличии в уставном (складочном) капитале предприятия доли (долей) иностранных физических или юридических лиц - при подаче заявления о предоставлении лицензии на проведение работ, связанных с использованием сведений, составляющих государственную тайну;
 - Степени секретности сведений, составляющих государственную тайну, с которыми заявитель предполагает осуществлять работы, подтвержденной органом государственной власти или организацией, наделенными полномочиями по распоряжению указанными сведениями.
- 2) Нотариально заверенные копии:
- Устава;
 - Свидетельства о постановке на налоговый учет;
 - Учредительного договора или решения о создании организации, заверенную печатью организации.
- 3) Копию свидетельства о государственной регистрации.
- 4) Копию свидетельства о праве собственности на занимаемые помещения или договора аренды и копию свидетельства о праве собственности арендодателя.
- 5) Копию договора банковского счета (в ПП № 333 не прописано, на практике же требуется работниками лицензионного отдела ФСБ);
- 6) Копию договора об оказании услуг (в случае использования заявителем услуг структурного подразделения по защите государственной тайны другой организации).
- 7) Оригинал документов, подтверждающих оплату лицензионного сбора.

1.8.1. Лицензионный сбор

Реквизиты для оплаты государственной пошлины [следующие](#):

Счет - 40101810800000010041;

Банк получателя — Отделение 1 Московского ГТУ Банка России, г. Москва;

БИК банка- 044583001;

получатель - УФК по г. Москве в/ч 93967;

Л/сч - № 04731528140;

ИНН/КПП 7702232171/770203002;

ОКАТО - 45286570000;

КБК 189 1 08 07081 01 0300 110 – предоставление лицензии.

По указанным реквизитам производится оплата государственной пошлины за лицензии, которые предоставляются, переоформляются, продлеваются Центром по лицензированию, сертификации и защите государственной тайны ФСБ России.

Информация о реквизитах для оплаты государственной пошлины за лицензии, которые предоставляются, переоформляются, продлеваются территориальными органами безопасности, уточняется в органах безопасности по месту нахождения заявителя (соискателя лицензий или лицензиата).

Оплату государственной пошлины следует производить строго по месту нахождения заявителя.

1.8.2. Спецэкспертиза и аттестация руководителя

В соответствии с п. 7 ПП № 333 лицензии выдаются на основании результатов специальных экспертиз предприятий и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, и при выполнении следующих условий:

- 1) Соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;
- 2) Наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по защите информации, уровень квалификации которых достаточен для обеспечения защиты государственной тайны;
- 3) Наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

В процессе специальной экспертизы организации проверяются выполнение требований нормативно-методических документов по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам, а также соблюдение других условий, необходимых для получения лицензии.

После подачи в ФСБ заявления на получение лицензии на ГТ в течение 2-х недель аттестационному центру должно выдаваться поручение на проведение специальной экспертизы организации.

На практике после подачи заявления предписание на проведение специальной экспертизы нашей организации было получено через 3 (три) месяца.

Вряд ли этот срок является типовым, но при планировании сроков получения лицензии данный момент следует обязательно учитывать.

Экспертиза обычно длится не более 20 дней. В результате спецэкспертизы оформляется акт, в котором описываются возможности и условия ведения организацией закрытых работ.

Резюмируя вышеизложенное, для получения лицензии ФСБ организации необходимо выполнить два существенных условия:

- 1) Пройти специальную экспертизу на предмет соответствия лицензионным требованиям ФСБ России;
- 2) Провести государственную аттестацию своего руководителя.

Далее эти мероприятия будут рассмотрены более подробно.

1.8.2.1. Специальная экспертиза

Лицензия ФСБ на ГТ выдается центром по лицензированию, сертификации и защиты государственной тайны ФСБ России по результатам прохождения организацией специальной экспертизы на предмет соответствия лицензионным требованиям ФСБ России. Для этого при ФСБ России созданы специальные аттестационные центры, которые имеют лицензию ФСБ на проведение специальных экспертиз организаций. Специалисты аттестационного центра определяют возможность организации осуществлять работы со сведениями, составляющими государственную тайну.

Оплата специальной экспертизы, согласно ПП № 333, производится из средств проверяемого и составляет сумму порядка 100 тыс. руб.

Кроме аттестационных центров право на проведение спецэкспертизы имеет только сама ФСБ России.

При прохождении организацией специальной экспертизы для получения лицензии ФСБ проверяется соблюдение организацией следующих условий:

- 1) Наличие правильно оформленных учредительных и внутренних документов;
- 2) Наличие руководящих документов по защите государственной тайны и защите информации;
- 3) Наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по защите информации, уровень квалификации которых достаточен для обеспечения защиты государственной тайны;
- 4) Наличие и ведение внутренних организационно-распорядительных и регламентирующих документов по защите государственной тайны и защите информации;
- 5) Взаимодействие с Заказчиком закрытых работ.

1.8.2.1.1. Учредительные и внутренние документы

Экспертная комиссия аттестационного центра проверяет следующие документы:

- 1) Учредительный договор или Решение о создании Общества;
- 2) Свидетельство о регистрации;
- 3) Свидетельство о постановке на налоговый учет;
- 4) Договор банковского счета;
- 5) Выписку из реестра акционеров;
- 6) Выписку из ЕГРЮЛ;
- 7) Договор аренды, документ, предоставляющий право пользования юридическим адресом;
- 8) Устав с приложенными протоколами собрания Участников (акционеров) и свидетельствами о регистрации изменений;
- 9) Договора, в рамках которых необходима лицензия ФСБ России (если есть);

Важно: Наличие этого пункта на практике приводит фактически к патовой ситуации, когда для получения лицензии на ГТ нужен договор (на проведение работ с участием сведений,

составляющих ГТ). А возможность заключения такого договора существует, как правило, только тогда, когда имеется лицензия на ГТ, что часто и оговорено в конкурсных требованиях.

Очень трудно получить контракт с ГТ под обязательство получить соответствующую лицензию, особенно с учётом реальных сроков получения данной лицензии.

- 10) Лицензии на заявленные виды деятельности (если есть);
- 11) Штатное расписание (штатное и фактическое количество сотрудников).

При подготовке пакета документов для лицензирования необходимо учитывать следующее, что согласно ФЗ "О государственной тайне" от 21 июля 1993 года № 5485-1, в Уставе должны быть прописаны следующие моменты:

- В Статье "Основные виды деятельности":
 - Защита государственной тайны в соответствии с законодательством Российской Федерации.
- В Статье "Обязанности руководителя":
 - Генеральный директор несет персональную ответственность за:
 - создание условий и организацию, обеспечивающих защиту сведений, составляющих государственную тайну;
 - создание условий, при которых должностное лицо или гражданин знакомятся только с теми сведениями, составляющими государственную тайну, и в таких объемах, которые необходимы ему для выполнения его должностных (функциональных) обязанностей;
 - несоблюдение установленных ограничений по ознакомлению со сведениями, составляющими государственную тайну.
- В Статье "Реорганизация и ликвидация предприятия":
 - В случаях изменения функций, формы собственности, ликвидации или прекращения работ с использованием сведений, составляющих государственную тайну, Генеральный директор Общества обязан принять меры по обеспечению защиты этих сведений и их носителей. При этом носители сведений, составляющих государственную тайну, в установленном порядке уничтожаются, сдаются на архивное хранение либо передаются:
 - правопреемнику Общества, если этот правопреемник имеет полномочия по проведению работ с использованием указанных сведений;
 - органу государственной власти, в распоряжении которого находятся соответствующие сведения;
 - другому органу государственной власти, предприятию, учреждению или организации по указанию Межведомственной комиссии по защите государственной тайны.
- В Статье "Права и обязанности участников (акционеров) Общества":
 - Доступ участников (акционеров) Общества, членов Совета директоров Общества и Генерального директора Общества к сведениям, составляющими государственную тайну, производится в соответствии с законодательными актами Российской Федерации по защите государственной тайны.

- В Статье "Участники (акционеры) Общества":
 - Участниками (акционерами) Общества могут быть только российские физические и юридические лица.

Важно: Для получения лицензии ФСБ в Устав организации возможно придётся вносить изменения.

1.8.2.1.2. Руководящие документы по защите государственной тайны и защите информации

Получение лицензии ФСБ подразумевает, что сотрудники и руководство организации знает и умеет применять руководящие документы по ЗГТ и ЗИ. Это законы РФ, Указы и Постановления Правительства РФ, посвященные мероприятиям, направленным на защиту государственной тайны.

Ниже приведён примерный перечень правовых и нормативно-методических документов по защите информации по защите государственной тайны, который должен иметься на предприятии (Таблица 8):

Таблица 8 - Перечень правовых и нормативно-методических документов по защите информации по защите ГТ

№ п/п	Наименование документа	Примечание
1	2	3
1.	Уголовный Кодекс Российской Федерации (ст. 275, 276, 283, 284)	
Федеральные законы		
2.	"О государственной тайне" от 21 июля 1993 г. № 5485-1	
3.	"Об информации, информационных технологиях и о защите информации" от 27 июля 2006 г. № 149-ФЗ	
4.	"О порядке выезда из Российской Федерации и въезда в Российскую Федерацию" от 15 августа 1996 г. № 114-ФЗ	
Указы Президента Российской Федерации		
5.	"О перечне сведений, отнесенных к государственной тайне" от 24 января 1998 г. № 61	
6.	"Об утверждении перечня сведений конфиденциального характера" от 06 марта 1997 г. № 188	
Постановления Правительства Российской Федерации		
7.	Инструкция по обеспечению режима секретности в Российской Федерации от 05 января 2004 г. № 3-1	может предоставляться на основе договора со сторонним РСП, т. к. документ ограниченного

№ п/п	Наименование документа	Примечание
		распространения
8.	"Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне" от 06 февраля 2010 г. № 63	
9.	"Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности" от 04 сентября 1995 г. № 870	
10.	"О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны" от 18 сентября 2006 г. № 573	
11.	"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" № 333	

1.8.2.1.3. Подразделение по защите государственной тайны

Организация своего режимно-секретного подразделения (РСП) – трудоёмкий, продолжительный и достаточно затратный процесс. На практике же, если в организации не предвидится большого объема работ по закрытой тематике, достаточно заключить договор на режимно-секретное обслуживание с организацией, имеющей своё режимно-секретное подразделение и лицензию на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны.

В противном случае, чтобы открыть собственное РСП нужно:

- 1) Подготовить помещение согласно определенным требованиям (решетки на окнах, капитальные стены и перекрытия, железные двери, сигнализация, охрана и т. д.);
- 2) Получить разрешение на функционирование РСП от ФСБ России;
- 3) Разработать целую гору документации, регламентирующую порядок работы РСП и порядок работы исполнителей с закрытыми документами;
- 4) Получить закрытые (секретные) документы, касающиеся работы с государственной тайной;
- 5) Принять в штат, как минимум, двух обученных работников: начальника РСП и специалиста и согласовать с ФСБ России их назначение на должность.

Финансовые затраты составят более 500 тыс. руб., кроме того нужно будет платить ежемесячно заработную плату сотрудникам РСП. Временные затраты – от 6 месяцев.

Чтобы избежать ненужных затрат и при этом соблюсти требования законодательства РФ, для получения лицензии ФСБ гораздо проще заключить договор с одной из организаций, предоставляющих свои режимно-секретные услуги. Затраты составляют в среднем по Москве 10 - 15

тыс. рублей в месяц (как правило, оплата осуществляется ежеквартально) за оплату режимно-секретных услуг.

1.8.2.1.4. Внутренние организационно-распорядительные и регламентирующие документы по защите государственной тайны и защите информации

Это важный блок документации, подлежащей проверке аттестационным центром, который регламентирует:

- 1) Проведение закрытых работ;
- 2) Ведение допускной работы;
- 3) Взаимодействие с обслуживающей организацией (если у организации заключен договор о режимно-секретном обслуживании);
- 4) Проведение встреч с иностранцами и выезд за пределы РФ;
- 5) Использование сети "Интернет".

1.8.2.1.5. Взаимодействие с Заказчиком закрытых работ

Для того, чтобы организация получила лицензию ФСБ и её допустили к работе со сведениями, составляющими государственную тайну, необходимо основание, которым может являться действующий договор с какой-либо организацией-заказчиком, предусматривающий наличие таких работ. Если же такого договора нет (как правило, договор заключается только после получения организацией лицензии ФСБ), то Заказчик должен отправить в лицензионный отдел ФСБ России ходатайство о выдаче организации лицензии ФСБ в связи с планируемым проведением закрытых работ.

***Важно:** Заказчиком может являться только ведомственная организация (Министерства РФ, Роскосмос, Росатом и т. д.) или организация, которая имеет от ведомства письменное разрешение на передачу сведений, составляющих государственную тайну, сторонним организациям, согласно "Перечня сведений, подлежащих засекречиванию..." по ведомству.*

1.8.2.2. Государственная аттестация руководителя организации

Второе существенное условие для получения лицензии ФСБ на ГТ – государственная аттестация руководителя лицензируемой организации. Оно проводится обычно в виде собеседования, в ходе которого проверяются его знания и умения в области защиты государственной тайны.

От государственной аттестации освобождаются руководители предприятий, имеющие свидетельство об окончании учебных заведений, уполномоченных осуществлять подготовку специалистов по вопросам защиты информации, составляющей государственную тайну. На данный момент стоимость такого обучения составляет порядка 100 тыс. руб.

Для проведения государственной аттестации руководителю необходимо:

- 1) Знать руководящие и регламентирующие документы в области защиты государственной тайны, уметь ими пользоваться и руководствоваться в организации мероприятий по ЗГТ.
- 2) Иметь действующий допуск к государственной тайне.

Допуск граждан РФ к государственной тайне регламентируется Постановлением Правительства РФ № 63 от 06.02.2010 "Об утверждении инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне".

Согласно данному ПП для того, чтобы руководителю организации получить допуск, необходимо:

- 1) Пройти в ФСБ проверочные мероприятия;
- 2) Принять на себя обязательство о неразглашении сведений, составляющих государственную тайну;
- 3) Получить от Заказчика работ Распоряжение о допуске.

Распоряжение о допуске – это письменное распоряжение одного из лиц, принимающих решение организации-заказчика, разрешающее руководителю знакомиться со сведениями, составляющими государственную тайну.

Сотрудников своей организации допускает сам руководитель.

1.8.2.2.1. Допуск руководителя организации к государственной тайне

Допуск руководителя организации к государственной тайне осуществляется в следующем порядке:

- 1) Руководитель собственноручно заполняет анкету по форме № 4 (когда родился, где учился, на ком женился...) и отдает её работникам того РСП, которое будет работу по оформлению допуска;
- 2) Работники РСП оформляют:
 - карточку допуска;
 - списки на оформляемого по форме № 11;
 - учётную карточку;
 - отправляют все документы в ФСБ;
 - принимают их из ФСБ.
- 3) Заказчик издаёт распоряжение о допуске к закрытым работам руководителя организации;
- 4) Руководитель организации принимает на себя обязательства перед государством о неразглашении сведений, составляющих государственную тайну;
- 5) Руководитель получает в РСП заказчика справку о допуске.

Основаниями для отказа гражданину в допуске к государственной тайне могут являться:

- 1) Признание гражданина судом недееспособным, ограниченно дееспособным или рецидивистом, нахождение его под судом или следствием за государственные или иные тяжкие преступления, наличие у гражданина неснятой судимости за эти преступления;
- 2) Наличие у гражданина медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому федеральным органом исполнительной власти, уполномоченным в области здравоохранения и социального развития;

- 3) Постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными гражданами документов для выезда на постоянное место жительства в другие государства;
- 4) Выявление в результате проведения проверочных мероприятий действий гражданина, создающих угрозу безопасности Российской Федерации;
- 5) Уклонение гражданина от проверочных мероприятий и (или) сообщение заведомо ложных анкетных данных.

1.9. Заключительные положения

Ещё раз основными вехами отметим, что нужно сделать для получения лицензии ФСБ на работу со сведениями, составляющими государственную тайну.

- 1) Получить допуск к государственной тайне руководителю организации;
- 2) Заключение договора о режимно-секретном обслуживании;
- 3) Получить от Заказчика Ходатайство о выдаче лицензии (у Заказчика должно быть разрешение на право передачи секретных сведений из "Перечня сведений, составляющих государственную тайну..." по соответствующему ведомству);
- 4) Написать заявление о получении лицензии на гостайну и отослать его в ФСБ;
- 5) Пройти специальную экспертизу на соответствие требованиям, предъявляемым к организациям для получения лицензии ФСБ;
- 6) Провести государственную аттестацию руководителя.

После сдачи в ФСБ Акта специальной экспертизы и Акта государственной аттестации (материалы сдаются организацией, проводившей специальную экспертизу и аттестацию руководителя) принимается решение о выдаче организации лицензии ФСБ.

На практике, срок после сдачи соответствующих документов до момента получения лицензии составляет порядка 1 месяца.

Суммарный срок от момента подачи заявления составил (в нашем случае) порядка 4 месяцев. А с учётом времени, предшествующем подготовке необходимого комплекта документации, то и все...

Учитывайте это при своём календарном планировании.

6. ЗАКЛЮЧЕНИЕ

Наличие лицензий по тем или иным видам деятельности является не только конкурентным преимуществом, но также и законодательным требованием во всё больших и больших областях деятельности.

Своевременное получение этих лицензий организациями является жизненно важным аспектом их функционирования.

Данная работа даёт понимание перечня основополагающих в области лицензирования документов, этапов лицензирования, сроков, состава документов, разъясняет ряд лицензионных требований.

Удачи!

7. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ ИНФОРМАЦИИ (ЛИТЕРАТУРА И ИНТЕРНЕТ-РЕСУРСЫ)

1. Федеральный закон Российской Федерации от 27.07.2006 № 152 -ФЗ "О персональных данных".
2. Федеральный закон Российской Федерации от 21.07.1993 № 5485-1 "О государственной тайне".
3. Федеральный закон Российской Федерации от 04.05.2011 № 99-ФЗ "О лицензировании отдельных видов деятельности".
4. Федеральный закон Российской Федерации от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации".
5. Федеральный закон Российской Федерации от 03.04.1995 № 40-ФЗ "О федеральной службе безопасности".
6. Указ Президента Российской Федерации от 16.08.2004 № 1085 "Вопросы Федеральной службы по техническому и экспортному контролю".
7. Указ Президента Российской Федерации от 11.08.2003 № 960 "Вопросы Федеральной службы безопасности Российской Федерации".
8. Постановление Правительства РФ от 21.11.2011 № 957 "Об организации лицензирования отдельных видов деятельности".
9. Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".
10. Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".
11. Приказ ФСТЭК России от 11.02.2013 № 17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".
12. Постановление Правительства РФ от 16.04.2012 № 313 "Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием

шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)".

13. Приказ ФСБ России от 30.08.2012 № 440 "От утверждении административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по осуществлению лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)".

14. Постановление Правительства РФ от 15.04.1995 № 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".

15. Приказ Федеральной службы безопасности Российской Федерации от 27.02.2009 № 75 "Об утверждении административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию 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".

16. Постановление Правительства РФ от 03.02.2012 № 79 "О лицензировании деятельности по технической защите конфиденциальной информации".

17. Перечень документов, необходимых для получения лицензии на деятельность по технической защите конфиденциальной информации (в соответствии с пунктом 8 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 03.02.2012 № 79).

18. Информационное сообщение ФСТЭК России от 30.05.2012 № 240/22/2222 "По вопросу необходимости получения лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации".

19. Приказ ФСТЭК России от 12.07.2012 № 83 "Административный регламент Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации".

20. Приказ ФСТЭК России от 03.04.2012 "Перечень контрольно-измерительного и испытательного оборудования, средств контроля защищенности, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79".
21. Приказ ФСТЭК России от 16.03.2012 "Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79".
22. Постановление Правительства РФ от 03.03.2012 № 171 "Положение о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации".
23. Перечень документов, необходимых для получения лицензии на разработку и производство средств защиты конфиденциальной информации (в соответствии с пунктом 9 Положения о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 марта 2012 г. № 171).
24. Приказ ФСТЭК России от 12.07.2012 № 84 "Административный регламент Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации".
25. Приказ ФСТЭК России от 09.04.2012 "Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения видов работ, установленных Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 марта 2012 г. № 171".
26. Приказ ФСТЭК России от 21.10.2013 № 126 "Об утверждении перечня функций ФСТЭК России, при реализации которых наиболее вероятно возникновение коррупции".
27. Приказ ФАПСИ от 13 июня 2001 г. № 152 "Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну".
28. Приказ ФСБ от 9 февраля 2005 г. № 66 "Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации" (Положение ПКЗ-2005).
29. Центр по лицензированию, сертификации и защите государственной тайны ФСБ России (ЦЛСЗ ФСБ России). <http://clsz.fsb.ru/>

30. Федеральная служба по техническому и экспортному контролю (ФСТЭК России). <http://fstec.ru/>
31. Министерство образования и науки Российской Федерации. <http://минобрнауки.рф>
32. Ассоциация предприятий компьютерных и информационных технологий (АП КИТ). <http://www.apkit.ru/>
33. *Центр исследования безопасности информационных технологий (ЦИБИТ).* Особенности переходного этапа. Лицензирование деятельности с шифровальными (криптографическими) средствами и подготовка специалистов по информационной безопасности, удовлетворяющих лицензионным требованиям. <http://www.cibit.ru/news.aspx?objid=07249301-1bc2-4ccc-9ee7-80a2a005ab68>
34. Поставщик продуктов, услуг и решений для профессионального обучения "Академия АйТи". <http://www.academy.it.ru/>
35. ООО Научно-производственный центр "СОТИС". <http://www.sotis-zgt.ru/>
36. Группа компаний "МАСКОМ". <http://www.mascom.ru>
37. ООО "ЦБИ". <http://www.cbi-info.ru>
38. Интернет-форум BANKIR.RU, тема "Лицензия ФСБ на СКЗИ". <http://bankir.ru/dom/threads/83762-%D0%9B%D0%B8%D1%86%D0%B5%D0%BD%D0%B7%D0%B8%D1%8F-%D0%A4%D0%A1%D0%91-%D0%BD%D0%B0-%D0%A1%D0%9A%D0%97%D0%98>
39. Форум по вопросам информационной безопасности InformationSecurity. http://www.itsec.ru/forum.php?text=%EB%E8%F6%E5%ED%E7%E8%F0%EE%E2%E0%ED%E8%E5&searchid=1824852®enc=windows-1251&l10n=ru&web=0#1107&d=0_0_0_0_addyn
40. Интернет - портал менеджеров и экспертов в области информационной безопасности ISO27000.ru. <http://iso27000.ru/>
41. Учебно-методическое объединение высших учебных заведений России по образованию в области информационной безопасности. <http://www.isedu.ru/sostav/vuzi.htm>

8. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Сокращение	Наименование
ISO (ИСО)	International Organization for Standardization (Международная организация по стандартизации)
АС	Автоматизированная система
ВПО	Высшее профессиональное образование
ГНИИИ ПТЗИ	Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю
ГТ	Государственная тайна
ДПО	Дополнительное профессиональное образование
ЗГТ	Защита государственной тайны
ЗИ	Защита информации
ЗП	Защищаемое помещение
КИО	Контрольно-измерительное оборудование
НПА	Нормативно-правовой акт
ОКСО	Общероссийский классификатор специальностей
ПП	Постановление Правительства РФ
РСП	Режимно-секретное подразделение
РФ	Российская Федерация
СЗКИ	Средство защиты конфиденциальной информации
СКЗИ	Средство криптографической защиты информации
СМК	Система менеджмента качества
СПО	Среднее профессиональное образование
СрЗИ	Средство защиты информации
ТЗКИ	Техническая защита конфиденциальной информации
ФАПСИ	Федеральное агентство правительственной связи и информации (ныне ФСБ)
ФГОС	Федеральный государственный образовательный стандарт
ФЗ	Федеральный закон

ФОИВ	Федеральный орган исполнительной власти
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ФСБ	Федеральная служба безопасности
ЦБ	Центральный банк
ЦЛСЗ	Центр по лицензированию, сертификации и защите государственной тайны ФСБ России

9. Ассоциации Business Information Security (BISA)

Сообщество BISA создано под эгидой одноименной Ассоциации Business Information Security (BISA). Оно объединяет профессионалов в области информационной безопасности, руководителей бизнес подразделений, представителей регуляторов и других специалистов, заинтересованных в развитии информационной безопасности в России и мире.

История создания сообщества берет начало от Ассоциации «DLP-Эксперт», образованной в 2008 как объединение ведущих экспертов в области ИБ. В 2013 году Ассоциация, которая всегда пристально следила за переменами, происходящими на рынке, откликнулась на них изменением концепции и расширением списка рассматриваемых тем. Теперь деятельность Ассоциации посвящена не только DLP, но и общим вопросам, связанным с защитой информации, представляющей интерес для бизнеса.

- Мы создали дискуссионную online-площадку для популяризации идей информационной безопасности, повышения уровня знаний специалистов и обсуждения практических вопросов защиты корпоративной информации;

Посетители сайта сообщества могут:

- Узнавать самые актуальные новости по информационной безопасности
 - Читать блоги ведущих экспертов отрасли
 - Слушать вебинары с обсуждением популярных тем в области информационной безопасности
 - Принимать участие в конкурсах и рейтингах
- Мы выпускаем ежеквартальный [журнал](#) о трендах, знаниях и личном опыте в области защиты информационных активов;
 - Мы проводим круглые столы, обучающие семинары, [вебинары](#) и другие мероприятия по информационной безопасности;
 - Мы организовали, и успешно проводим одно из ведущих мероприятий отечественной отрасли информационной безопасности – конференцию [BIS Summit](#) (в прошлом – DLP-Russia).