Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Московский институт электронной техники»

КУРСОВАЯ РАБОТА

ПО ДИСЦИПЛИНЕ

«Организационное и правовое обеспечение информационной безопасности»

ТЕМА:

«Разработка предложений и проектов документов для получения лицензии на осуществление деятельности по разработке средств, защищенных программных (программно-технических) средств обработки информации»

Студент учебной группы ИБ-21 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Иванов И.И.)

*подпись (фамилия, инициалы)*

Руководитель работы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Воеводин В.А.)

*подпись (фамилия, инициалы)*

г. Москва

# РЕФЕРАТ

Курсовой проект содержит 46 страниц, 4 приложения и 8 использованных источников.

Ключевые слова: лицензирование, разработка, документы, защита информации.

Объект исследования: разработка средств, защищенных программных (программно-технических) средств обработки информации.

Целью курсового проекта является разработка пакета документов, необходимого для получения лицензии на осуществление деятельности по разработке средств, защищенных программных (программно-технических) средств обработки информации.

В данной курсовой работе были проведены анализ объекта исследования и анализ методов планирования сил, средств и ресурсов при подготовке к лицензированию.

В результате работы был представлен пакет документов на получение лицензии на осуществление деятельности по разработке средств, защищенных программных (программно-технических) средств обработки информации.

# СОДЕРЖАНИЕ

[РЕФЕРАТ 2](#_Toc198167904)

[СОДЕРЖАНИЕ 3](#_Toc198167905)

[ВВЕДЕНИЕ 5](#_Toc198167906)

[Глава 1. Краткая характеристика рассматриваемого вида деятельности 6](#_Toc198167907)

[1.1 Что такое «защищенные программные (программно-технические) средства обработки информации» 6](#_Toc198167908)

[1.2 Что такое «разработка средств, защищенных программных (программно-технических) средств обработки информации» 8](#_Toc198167909)

[Глава 2. Общие положения по организации работы по подготовке к лицензированию 10](#_Toc198167910)

[Глава 3. Разработка предложений по подготовке к лицензированию 12](#_Toc198167911)

[3.1 Разработка перечня документов, необходимых для получения лицензии по технической защите конфиденциальной информации 12](#_Toc198167912)

[3.2 Обоснование состава и квалификации инженерно-технического персонала организации, необходимого для выполнения работ и оказания услуг при осуществлении деятельности по технической защите конфиденциальной информации 15](#_Toc198167913)

[3.3 Обоснование состава производственного, контрольно-измерительного, испытательного оборудования и средств контроля защищенности информации, необходимого необходимых для выполнения работ и оказания услуг при осуществлении деятельности по технической защите конфиденциальной информации 17](#_Toc198167914)

[3.4 Обоснование состава программного обеспечения, необходимого необходимых для выполнения работ и оказания услуг при осуществлении деятельности по технической защите конфиденциальной информации 18](#_Toc198167915)

[3.5 Обоснование состава технической документации, национальных стандартов и методических документов, необходимого необходимых для выполнения работ и оказания услуг при осуществлении деятельности по технической защите конфиденциальной информации 19](#_Toc198167916)

[3.6 Оформление проекта заявления о предоставлении лицензии на деятельность 20](#_Toc198167917)

[ЗАКЛЮЧЕНИЕ 21](#_Toc198167918)

[СПИСОК ЛИТЕРАТУРЫ 22](#_Toc198167919)

[Приложение 1 23](#_Toc198167920)

[Приложение 2 25](#_Toc198167921)

[Приложение 3 27](#_Toc198167922)

[Приложение 4 37](#_Toc198167923)

# ВВЕДЕНИЕ

Перед осуществлением некоторых видов деятельности в Российской требуется получить лицензию. Перечень таких типов деятельности указан 12-ой статье федерального закона от 04.05.2011 N 99-ФЗ (ред. От 08.08.2024) «О лицензировании отдельных видов деятельности» [1]. В рамках данной работы нас интересуют лишь лицензирование деятельности по разработке и производству средств защиты конфиденциальной информации, т.к. разработка средств, защищенных программных (программно-технических) средств обработки информации относиться к данному виду деятельности.

При лицензировании деятельности по разработке средств, защищенных программных (программно-технических) средств обработки информации стоит опираться на положение из Постановления Правительства РФ от 03.03.2012 N 171 (ред. от 27.12.2024) «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» [2], в котором, согласно пункту 3а, указано, что деятельность по разработке средств, защищенных программных (программно-технических) средств обработки информации подлежит лицензированию.

В дальнейшем, в курсовой работе будет подготовлен проект пакета документов, необходимых для получения лицензии на разработку средств, защищенных программных (программно-технических) средств обработки информации.

# Глава 1. Краткая характеристика рассматриваемого вида деятельности

# 1.1 Что такое «защищенные программные (программно-технические) средства обработки информации»

Для начала, стоит уяснить, что имеется означает понятие «защищенные программные (программно-технические) средства обработки информации». Прямого термина в ГОСТ, ФЗ – нету, поэтому будем анализировать его частями:

Согласно пункту 2.4 ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности» [3] – *средства обработки информации*: Любая система обработки информации, услуга или инфраструктура, или их фактическое месторасположение.

Согласно пункту 3.2 ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения» [4] ­­­­­­­­– *безопасное программное обеспечение*: Программное обеспечение, разработанное с использованием совокупности мер, направленных на предотвращение появления и устранение уязвимостей программы.

Согласно пункту 2 ГОСТ 28806-90 «Межгосударственный стандарт. Качество программных средств» [5] – *программное средство*: Объект, состоящий из программ, процедур, правил, а также, если предусмотрено, сопутствующих им документации и данных, относящихся к функционированию системы обработки информации.

Как следствие этих трех определений, дадим понятию «защищенные программные (программно-технические) средства обработки информации» следующее определение:

*Защищенные программные (программно-технические) средства обработки информации* – это такая система обработки информации, включающая в себя программные средства (совокупность программных и технических средств), разработанная с использованием совокупности мер, направленных на предотвращение появления и устранение уязвимостей системы.

Защищенные программные (программно-технические) средства обработки информации предназначены для:

1. Обеспечения конфиденциальности данных.
   * Защита информации от несанкционированного доступа с использованием шифрования, механизмов аутентификации и разграничения прав доступа.
2. Гарантии целостности информации.
   * Предотвращение несанкционированного изменения, удаления или подмены данных.
3. Обеспечения доступности систем.
   * Защита от цифровых и физических атак на систему, аппаратно-программной избыточности и отказоустойчивости системы.
4. Соответствия требованиям регуляторов.
5. Защиты от утечек информации.
   * Контроль и блокировка передачи конфиденциальных данных за пределы контролируемой зоны.
6. Обеспечения безопасной обработки данных.

# 1.2 Что такое «разработка средств, защищенных программных (программно-технических) средств обработки информации»

Разработка средств, защищенных программных (программно-технических) средств обработки информации состоит из:

1. Анализа угроз и моделирования рисков.
   * Проведение оценки потенциальных уязвимостей системы.
   * Определение классов защищённости и требований регуляторов.
2. Проектирования архитектуры безопасности.
   * Разработка схемы защиты данных – шифрование, контроль доступа, разделение привилегий).
   * Выбор сертифицированных компонентов (криптографические модули, доверенные среды выполнения).
3. Реализации защитных механизмов.
4. Тестирования на устойчивость к атакам.
   * Проверка на соответствие требованиям ФСТЭК.
   * Выявление уязвимостей.
5. Сертификации и аттестации.
   * Прохождение процедур обязательной сертификации во ФСТЭК.
   * Получение заключения о соответствии требованиям.
6. Внедрение средств и мониторинг.
   * Развёртка средств в эксплуатационной среде с минимальными рисками.
   * Организация мониторинга безопасности средств.
7. Поддержка и обновление средств.
   * Регулярное исправление обнаруживаемых уязвимостей.
   * Адаптация к новым угрозам и изменениям в нормативно-правовой базе.

Таким образом, указанный вид деятельности, согласно Постановлению Правительства РФ от 03.03.2012 N 171 (ред. от 27.12.2024) «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» [2], подлежит лицензированию.

# Глава 2. Общие положения по организации работы по подготовке к лицензированию

При подготовке к лицензированию производятся следующие виды работ:

1. Проверка наличия у соискателя юридического лица;
2. Проверка наличия помещений, в которых созданы необходимые условия для осуществления лицензируемого вида деятельности;
3. Проверка наличия оборудования, необходимого для осуществления лицензируемого вида деятельности;
4. Проверка наличия программного обеспечения, необходимого для осуществления лицензируемого вида деятельности;
5. Проверка наличия технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения лицензируемого вида деятельности;
6. Подготовка пакета документов, необходимых для получения лицензии;
7. Проверка наличия инженерно-технического персонала соответствующей квалификации;

Для получения лицензии по рассматриваемому виду деятельности необходимо воспользоваться следующими нормативно-правовыми актами:

1. Федеральный закон от 04.05.2011 N 99-ФЗ (ред. от 08.08.2024) «О лицензировании отдельных видов деятельности»
2. Постановление Правительства РФ от 03.03.2012 N 171 (ред. от 27.12.2024) «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»
3. Перечень технической и технологической 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. N 171
4. Перечень контрольно-измерительного и испытательного оборудования, программных (программно-технических) средств, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 марта 2012 г. № 171

Отсюда можно сделать вывод что, подробно изучив перечисленные выше нормативно-правовые акты и при условии успешного прохождения всех требуемых для процесса лицензирования специальных проверок, ООО «Тест» имеет право претендовать на получение лицензии, необходимой для проведения работ по разработке средств, защищенных программных (программно-технических) средств обработки информации.

# Глава 3. Разработка предложений по подготовке к лицензированию

# 3.1 Разработка перечня документов, необходимых для получения лицензии по технической защите конфиденциальной информации

В соответствии с пунктом 9 положения о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации из Постановления Правительства РФ N 171 [2] для получения лицензии соискатель лицензии направляет или представляет в лицензирующий орган следующие документы:

1. Заявление о предоставлении лицензии с описью прилагаемых документов;
2. Копии документов, подтверждающих наличие в штате соискателя лицензии специалистов по защите информации и их квалификацию (приказов о назначении или выписок из трудовых книжек, дипломов, удостоверений, свидетельств) и (или) сведения о трудовой деятельности, предусмотренные статьей 66.1 Трудового кодекса Российской Федерации;
3. 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);
4. Копии аттестатов соответствия защищаемых помещений требованиям по безопасности информации и технических паспортов, используемых для осуществления лицензируемого вида деятельности;
5. Копии аттестатов соответствия средств обработки информации требованиям по безопасности информации и технических паспортов, используемых для осуществления лицензируемого вида деятельности;
6. Копии документов, подтверждающих право соискателя лицензии на программы для электронно-вычислительных машин и базы данных, планируемые к использованию при осуществлении лицензируемого вида деятельности;
7. Сведения о наличии производственного, испытательного и контрольно-измерительного оборудования, средств защиты информации, средств разработки и производства средств защиты конфиденциальной информации, необходимых для осуществления лицензируемого вида деятельности, с приложением копий документов о поверке (калибровке) и маркировании контрольно-измерительного оборудования, а также документов, подтверждающих право соискателя лицензии на использование указанных оборудования и средств;
8. Сведения об имеющихся технической и технологической документации, национальных стандартах и методических документах, необходимых для выполнения работ по производству технических средств контроля эффективности мер защиты информации, с приложением копий документов, подтверждающих, что документы, содержащие информацию ограниченного доступа, получены в установленном законодательством Российской Федерации порядке;
9. Копии документов, подтверждающих наличие системы производственного контроля, включающей правила и процедуры проверки и оценки системы разработки средств защиты конфиденциальной информации, учета изменений, вносимых в проектную и конструкторскую документацию на разрабатываемую продукцию.

# 3.2 Обоснование состава и квалификации инженерно-технического персонала организации, необходимого для выполнения работ и оказания услуг при осуществлении деятельности по технической защите конфиденциальной информации

В соответствии с п.2 Постановления Правительства РФ N 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» [2] лицензирование деятельности по разработке и производству средств защиты конфиденциальной информации находится в юрисдикции Федеральной службы по техническому и экспортному контролю.

В соответствии с требованиями ФСТЭК России, указанными в п.4а Постановления Правительства РФ N 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» [2] необходимо наличие в штате у соискателя лицензии по основному месту работы в соответствии со штатным расписанием следующего квалифицированного персонала:

1. Руководитель и (или) уполномоченное руководить работами по лицензируемому виду деятельности лицо, имеющие высшее образование по направлению подготовки (специальности) в области информационной безопасности и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет, или высшее образование по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технических наук и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 7 лет, или иное высшее образование и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет, прошедшие обучение по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности (нормативный срок обучения - не менее 360 аудиторных часов);
2. Инженерно-технические работники (не менее 2 человек), имеющие высшее образование по направлению подготовки (специальности) в области информационной безопасности и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет или иное высшее образование и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет, прошедшие обучение по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности (нормативный срок обучения - не менее 360 аудиторных часов);

# 3.3 Обоснование состава производственного, контрольно-измерительного, испытательного оборудования и средств контроля защищенности информации, необходимого необходимых для выполнения работ и оказания услуг при осуществлении деятельности по технической защите конфиденциальной информации

Для всех видов деятельности, лицензированием которых занимается ФСТЭК России существует «Перечень контрольно-измерительного и испытательного оборудования, программных (программно-технических) средств, необходимых для выполнения работ и оказания услуг, установленных положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденным Постановлением Правительства Российской Федерации от 3 марта 2012 г. N 171» (утв. ФСТЭК России 27.06.2018).

Выделим необходимый нам перечень по столбцу «Разработка программных (программно-технических) средств защиты информации» (а4) [6] для обоснования состава производственного, контрольно-измерительного, испытательного оборудования и средств контроля защищенности информации, необходимых для выполнения работ и оказания услуг при осуществлении рассматриваемого в курсовой работе вида деятельности. Данная выдержка приведена в приложении 1 курсовой работы.

# 3.4 Обоснование состава программного обеспечения, необходимого необходимых для выполнения работ и оказания услуг при осуществлении деятельности по технической защите конфиденциальной информации

Воспользуемся всё тем же «Перечнем контрольно-измерительного и испытательного оборудования, программных (программно-технических) средств, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденным Постановлением Правительства Российской Федерации от 3 марта 2012 г. N 171» [2], и составим выдержку из него, чтобы обосновать состав программного обеспечения. Данная выдержка приведена в приложении 2 курсовой работы.

# 3.5 Обоснование состава технической документации, национальных стандартов и методических документов, необходимого необходимых для выполнения работ и оказания услуг при осуществлении деятельности по технической защите конфиденциальной информации

Примем во внимание с официального сайта ФСТЭК России «Перечень технической и технологической 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. N 171» [7], чтобы составить из него выдержку с документацией, необходимой для выполнения работ по рассматриваемому виду деятельности. Требуемый перечень приведён в приложении 3 курсовой работы.

# 3.6 Оформление проекта заявления о предоставлении лицензии на деятельность

Заявление о предоставлении лицензии на осуществление деятельности по технической защите конфиденциальной информации юридическому лицу оформляется по образцу, который можно найти в Приказе ФСТЭК России от 12 января 2023 г. №3 «Об утверждении форм документов, используемых Федеральной службой по техническому и экспортному контролю в процессе лицензирования деятельности по технической защите конфиденциальной информации, и признании утратившими силу приказа ФСТЭК России от 17 июля 2017 г. N 134 и внесенных в него изменений» [8], размещённом на официальном сайте регулятора. Проект заявления представлен в приложении 4 данной курсовой работы.

# ЗАКЛЮЧЕНИЕ

В ходе выполнения настоящей курсовой работы была проведена работа по поиску и подробному изучению нормативно-правовых документов в заданной области лицензирования, после чего, опираясь на информацию из нормативно-правовых актов, а также из курса лекций по дисциплине «Организационное и правовое обеспечение информационной безопасности», были разработаны и сформированы предложения по подготовке к лицензированию указанного вида деятельности.

Кроме того, был собран пакет документов для получения лицензии на осуществление деятельности по разработке средств, защищенных программных (программно-технических) средств обработки информации.

Следуя действиям, указанным в настоящей курсовой работе возможно подготовить организацию к получению необходимой лицензии. Даже при подготовке к получению лицензии для смежного вида деятельности – нормативно-правовая база, документы и список действий остаются практически неизменными.

Таким образом – общая методология описана, а цель настоящей курсовой работы достигнута.

# СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 04.05.2011 N 99-ФЗ (ред. От 08.08.2024) "О лицензировании отдельных видов деятельности" [Электронный ресурс] – Справочно-правовая система «КонсультантПлюс».
2. Постановление Правительства РФ от 03.03.2012 № 171 (ред. от 27.12.2024) "О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации" (вместе с "Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации"). [Электронный ресурс] – Справочно-правовая система «КонсультантПлюс».
3. ГОСТ Р ИСО/МЭК 27002-2012 «Национальный Стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности». [Электронный ресурс] – Режим доступа: <https://docs.cntd.ru/document/1200103619> (дата обращения: 15.05.2025)
4. ГОСТ Р 56939-2016 «Национальный Стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования». [Электронный ресурс] – Режим доступа: <https://docs.cntd.ru/document/1200135525> (дата обращения: 15.05.2025)
5. ГОСТ 28806-90 «Межгосударственный Стандарт. Качество программных средств. Термины и определения» [Электронный ресурс] – Режим доступа: <https://docs.cntd.ru/document/1200009077> (дата обращения: 15.05.2025)
6. Перечень контрольно-измерительного и испытательного оборудования, программных (программно-технических) средств, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 марта 2012 г. № 171. [Электронный ресурс] – Режим доступа: <https://www.consultant.ru/document/cons_doc_LAW_333257/#dst100002> (дата обращения: 15.05.2025)
7. Перечень технической и технологической 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. N 171. [Электронный ресурс] – Режим доступа: <https://fstec.ru/dokumenty/vse-dokumenty/perechni/perechen-tekhnicheskoj-i-tekhnologicheskoj-dokumentatsii-natsionalnykh-standartov-i-metodicheskikh-dokumentov-ot-12-avgusta-2020-g> (дата обращения: 15.05.2025)
8. Приказ ФСТЭК России от 12 января 2023 г. №3 «Об утверждении форм документов, используемых Федеральной службой по техническому и экспортному контролю в процессе лицензирования деятельности по технической защите конфиденциальной информации, и признании утратившими силу приказа ФСТЭК России от 17 июля 2017 г. N 134 и внесенных в него изменений». [Электронный ресурс] – Режим доступа: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-12-yanvarya-2023-g-n-3> (дата обращения: 15.05.2025)

# Приложение 1

**Выдержка из перечня контрольно-измерительного и испытательного оборудования, программных (программно-технических) средств, необходимых для выполнения работ и оказания услуг, установленных положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденным Постановлением Правительства Российской Федерации от 3 марта 2012 г. N 171**

|  |  |  |
| --- | --- | --- |
| N п/п | Наименование оборудования, программных (программно-технических) средств | Технические и (или) функциональные характеристики |
| 1 | Средство (средства) контроля целостности программ и программных комплексов | Должно обеспечивать расчет и документирование уникальных значений контрольных сумм программного обеспечения, функционирующего в средах операционных систем Windows и Linux, по алгоритму, установленному ГОСТ Р 34.11.  Должно иметь соответствующий сертификат ФСТЭК России |
| 2 | Средство (средства) анализа программного кода | Должно (должны) обеспечивать:  решение задач контроля отсутствия в программном обеспечении, недекларированных возможностей в соответствии с требованиями руководящего документа "Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей", утвержденного приказом Гостехкомиссии России от 4 июня 1999 г. N 114;  проведение статического и динамического анализа исходных текстов программного обеспечения, а также контроль соответствия исходных текстов программного обеспечения его объектному (загрузочному) коду |
| 3 | Средство (средства) контроля (анализа) защищенности | Должны обеспечивать поиск уязвимостей в программном обеспечении, функционирующем в средах операционных систем Windows и Linux.  Должно иметь соответствующий сертификат ФСТЭК России |
| 4 | Средство поиска остаточной информации на машинных носителях информации | Должно обеспечивать поиск остаточной информации на машинных носителях информации по заданным критериям.  Должно иметь соответствующий сертификат ФСТЭК России |
| 5 | Средства антивирусной защиты (не менее 3 средств разных производителей) | Должны осуществлять поиск вредоносного программного обеспечения в программных комплексах и в информационных системах, функционирующих с применением операционных систем Windows и Linux.  Должны иметь соответствующий сертификат ФСТЭК России |

# Приложение 2

**Выдержка из перечня контрольно-измерительного и испытательного оборудования, программных (программно-технических) средств, необходимых для выполнения работ и оказания услуг, установленных положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденным Постановлением Правительства Российской Федерации от 3 марта 2012 г. N 171**

|  |  |  |
| --- | --- | --- |
| N п/п | Наименование оборудования, программных (программно-технических) средств | Технические и (или) функциональные характеристики |
| 1 | Средства разработки программ | Должны обеспечивать разработку, компиляцию и отладку программ, просмотр и редактирование бинарных файлов, разработку программ с возможностями подключения и расширения для программирования на различных языках, поиск фрагментов данных, сравнение фрагментов данных, расчет контрольных сумм фрагментов данных, проведение вычислений в системах счисления по десятичному, двоичному и шестнадцатеричному основаниям |
| 2 | Программатор | Должен обеспечивать запись и считывание информации с постоянных запоминающих устройств и считывание информации из них |
| 3 | Система управления изменениями программного обеспечения | Должна обеспечивать:  управление конфигурациями программного обеспечения;  управление реализацией новых возможностей в программном обеспечении;  управление устранением ошибок в программном обеспечении;  контроль доступа к системе |
| 4 | Средства для автоматизации процессов тестирования средств защиты информации (средства тестирования проникновения) | Автоматизация процесса тестирования проникновения средства защиты информации |

# Приложение 3

**Перечень технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения работ и (или) оказания услуг, установленных положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденным постановлением правительства российской федерации от 3 марта 2012 г. № 171.**

|  |  |
| --- | --- |
| N п/п | Наименование |
| 1 | Положение о системе сертификации средств защиты информации. Утверждено приказом ФСТЭК России от 3 апреля 2018 г. N 55 |
| 2 | Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. N 638. ДСП |
| 3 | Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20 марта 2012 г. N 28. ДСП |
| 4 | Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. N 17 |
| 5 | Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Утверждены приказом ФСТЭК России от 14 марта 2013 г. N 31 |
| 6 | Требования к средствам доверенной загрузки. Утверждены приказом ФСТЭК России от 27 сентября 2014 г. N 119. ДСП |
| 7 | Требования к средствам контроля съемных машинных носителей информации. Утверждены приказом ФСТЭК России от 28 июля 2014 г. N 87. ДСП |
| 8 | Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденным приказом ФСТЭК России от 30 июня 2018 г. N 131. ДСП |
| 9 | Требования к межсетевым экранам. Утверждены приказом ФСТЭК России от 09 февраля 2016 г. N9. ДСП |
| 10 | Требованиям безопасности информации к операционным системам, утвержденным приказом ФСТЭК России от 19 августа 2016 г. N 119. ДСП |
| 11 | Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. |
| 12 | Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. N 21 |
| 13 | Методика выявления уязвимостей и недекларированных возможностей. Утверждена ФСТЭК России 11 февраля 2019 г. ДСП |
| 14 | Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. N 282. ДСП\*\* |
| 15 | Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты ИТ.СОВ.С4.ПЗ. Утвержден ФСТЭК России 3 февраля 2012 г. |
| 16 | Профиль защиты систем обнаружения вторжений уровня сети пятого класса защиты ИТ.СОВ.С5.ПЗ. Утвержден ФСТЭК России 6 марта 2012 г. |
| 17 | Профиль защиты систем обнаружения вторжений уровня сети шестого класса защиты ИТ.СОВ.С6.ПЗ. Утвержден ФСТЭК России 6 марта 2012 г. |
| 18 | Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты ИТ.СОВ.У4.ПЗ. Утвержден ФСТЭК России 3 февраля 2012 г. |
| 19 | Профиль защиты систем обнаружения вторжений уровня узла пятого класса защиты ИТ.СОВ.У5.ПЗ. Утвержден ФСТЭК России 6 марта 2012 г. |
| 20 | Профиль защиты систем обнаружения вторжений уровня узла шестого класса защиты ИТ.СОВ.У6.ПЗ. Утвержден ФСТЭК России 6 марта 2012 г. |
| 21 | Профиль защиты средств антивирусной защиты типа "А" четвертого класса защиты ИТ.САВЗ.А4.ПЗ. Утвержден ФСТЭК России 14 июня 2012 г. |
| 22 | Профиль защиты средств антивирусной защиты типа "А" пятого класса защиты ИТ.САВЗ.А5.ПЗ. Утвержден ФСТЭК России 14 июня 2012 г. |
| 23 | Профиль защиты средств антивирусной защиты типа "А" шестого класса защиты ИТ.САВЗ.А6.ПЗ. Утвержден ФСТЭК России 14 июня 2012 г. |
| 24 | Профиль защиты средств антивирусной защиты типа "Б" четвертого класса защиты ИТ.САВЗ.Б4.ПЗ. Утвержден ФСТЭК России 14 июня 2012 г. |
| 25 | Профиль защиты средств антивирусной защиты типа "Б" пятого класса защиты ИТ.САВЗ.Б5.ПЗ. Утвержден ФСТЭК России 14 июня 2012 г. |
| 26 | Профиль защиты средств антивирусной защиты типа "Б" шестого класса защиты ИТ.САВЗ.Б6.ПЗ. Утвержден ФСТЭК России 14 июня 2012 г. |
| 27 | Профиль защиты средств антивирусной защиты типа "В" четвертого класса защиты ИТ.САВЗ.В4.ПЗ. Утвержден ФСТЭК России 14 июня 2012 г. |
| 28 | Профиль защиты средств антивирусной защиты типа "В" пятого класса защиты ИТ.САВЗ.В5.ПЗ. Утвержден ФСТЭК России 14 июня 2012 г. |
| 29 | Профиль защиты средств антивирусной защиты типа "В" шестого класса защиты ИТ.САВЗ.В6.ПЗ. Утвержден ФСТЭК России 14 июня 2012 г. |
| 30 | Профиль защиты средств антивирусной защиты типа "Г" четвертого класса защиты ИТ.САВЗ.Г4.ПЗ. Утвержден ФСТЭК России 14 июня 2012 г. |
| 31 | Профиль защиты средств антивирусной защиты типа "Г" пятого класса защиты ИТ.САВЗ.Г5.ПЗ. Утвержден ФСТЭК России 14 июня 2012 г. |
| 32 | Профиль защиты средств антивирусной защиты типа "Г" шестого класса защиты ИТ.САВЗ.Г6.ПЗ. Утвержден ФСТЭК России 14 июня 2012 г. |
| 33 | Профиль защиты средства доверенной загрузки уровня платы расширения четвертого класса защиты ИТ.СДЗ.ПР4.ПЗ. Утвержден ФСТЭК России 30 декабря 2013 г. |
| 34 | Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода четвертого класса защиты ИТ.СДЗ.УБ4.ПЗ. Утвержден ФСТЭК России 30 декабря 2013 г. |
| 35 | Профиль защиты средства доверенной загрузки уровня загрузочной записи пятого класса защиты ИТ.СДЗ.ЗЗ5.ПЗ. Утвержден ФСТЭК России 30 декабря 2013 г. |
| 36 | Профиль защиты средства доверенной загрузки уровня загрузочной записи шестого класса защиты ИТ.СДЗ.ЗЗ6.ПЗ. Утвержден ФСТЭК России 30 декабря 2013 г. |
| 37 | Профиль защиты средств контроля отчуждения (переноса) информации со съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.Н4.ПЗ. Утвержден ФСТЭК России 1 декабря 2014 г. |
| 38 | Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ. Утвержден ФСТЭК России 1 декабря 2014 г. |
| 39 | Профиль защиты средств контроля подключения съемных машинных носителей информации пятого класса защиты. ИТ.СКН.П5.ПЗ. Утвержден ФСТЭК России 1 декабря 2014 г. |
| 40 | Профиль защиты средств контроля подключения съемных машинных носителей информации шестого класса защиты. ИТ.СКН.П6.ПЗ. Утвержден ФСТЭК России 1 декабря 2014 г. |
| 41 | Профиль защиты межсетевых экранов типа "А" четвертого класса защиты ИТ.МЭ.А4.ПЗ. Утвержден ФСТЭК России 12 сентября 2016 г. |
| 42 | Профиль защиты межсетевых экранов типа "А" пятого класса защиты ИТ.МЭ.А5.ПЗ. Утвержден ФСТЭК России 12 сентября 2016 г. |
| 43 | Профиль защиты межсетевых экранов типа "А" шестого класса защиты ИТ.МЭ.А6.ПЗ. Утвержден ФСТЭК России 12 сентября 2016 г. |
| 44 | Профиль защиты межсетевых экранов типа "Б" четвертого класса защиты ИТ.МЭ.Б4.ПЗ. Утвержден ФСТЭК России 12 сентября 2016 г. |
| 45 | Профиль защиты межсетевых экранов типа "Б" пятого класса защиты ИТ.МЭ.Б5.ПЗ. Утвержден ФСТЭК России 12 сентября 2016 г. |
| 46 | Профиль защиты межсетевых экранов типа "Б" шестого класса защиты ИТ.МЭ.Б6.ПЗ. Утвержден ФСТЭК России 12 сентября 2016 г. |
| 47 | Профиль защиты межсетевых экранов типа "В" четвертого класса защиты ИТ.МЭ.В4.ПЗ. Утвержден ФСТЭК России 12 сентября 2016 г. |
| 48 | Профиль защиты межсетевых экранов типа "В" пятого класса защиты ИТ.МЭ.В5.ПЗ. Утвержден ФСТЭК России 12 сентября 2016 г. |
| 49 | Профиль защиты межсетевых экранов типа "В" шестого класса защиты ИТ.МЭ.В6.ПЗ. Утвержден ФСТЭК России 12 сентября 2016 г. |
| 50 | Профиль защиты межсетевых экранов типа "Г" четвертого класса защиты ИТ.МЭ.Г4.ПЗ. Утвержден ФСТЭК России 12 сентября 2016 г. |
| 51 | Профиль защиты межсетевых экранов типа "Г" пятого класса защиты ИТ.МЭ.Г5.ПЗ. Утвержден ФСТЭК России 12 сентября 2016 г. |
| 52 | Профиль защиты межсетевых экранов типа "Г" шестого класса защиты ИТ.МЭ.Г6.ПЗ. Утвержден ФСТЭК России 12 сентября 2016 г. |
| 53 | Профиль защиты межсетевых экранов типа "Д" четвертого класса защиты ИТ.МЭ.Д4.ПЗ. Утвержден ФСТЭК России 12 сентября 2016 г. |
| 54 | Профиль защиты межсетевых экранов типа "Д" пятого класса защиты ИТ.МЭ.Д5.ПЗ. Утвержден ФСТЭК России 12 сентября 2016 г. |
| 55 | Профиль защиты межсетевых экранов типа "Д" шестого класса защиты ИТ.МЭ.Д6.ПЗ. Утвержден ФСТЭК России 12 сентября 2016 г. |
| 56 | Профиль защиты операционных систем типа "А" четвертого класса защиты ИТ.ОС.А4.ПЗ. Утвержден ФСТЭК России 8 февраля 2017 г. |
| 57 | Профиль защиты операционных систем типа "А" пятого класса защиты ИТ.ОС.А5.ПЗ. Утвержден ФСТЭК России 8 февраля 2017 г. |
| 58 | Профиль защиты операционных систем типа "А" шестого класса защиты ИТ.ОС.А6.ПЗ. Утвержден ФСТЭК России 8 февраля 2017 г. |
| 59 | Профиль защиты операционных систем типа "Б" четвертого класса защиты ИТ.ОС.Б4.ПЗ. Утвержден ФСТЭК России 11 мая 2017 г. |
| 60 | Профиль защиты операционных систем типа "Б" пятого класса защиты ИТ.ОС.Б5.ПЗ. Утвержден ФСТЭК России 11 мая 2017 г. |
| 61 | Профиль защиты операционных систем типа "Б" шестого класса защиты ИТ.ОС.Б6.ПЗ. Утвержден ФСТЭК России 11 мая 2017 г. |
| 62 | Профиль защиты операционных систем типа "В" четвертого класса защиты ИТ.ОС.В4.ПЗ. Утвержден ФСТЭК России 11 мая 2017 г. |
| 63 | Профиль защиты операционных систем типа "В" пятого класса защиты ИТ.ОС.В5.ПЗ. Утвержден ФСТЭК России 11 мая 2017 г. |
| 64 | Профиль защиты операционных систем типа "В" шестого класса защиты ИТ.ОС.В6.ПЗ. Утвержден ФСТЭК России 11 мая 2017 г. |
| 65 | ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения |
| 66 | ГОСТ Р 58256-2018 Управление потоками информации в информационной системе. Формат классификационных меток |
| 67 | ГОСТ 2.001-2013. ЕСКД. Общие положения |
| 68 | ГОСТ 2.004-88. ЕСКД. Общие требования к выполнению конструкторских и технологических документов на печатающих и графических устройствах вывода ЭВМ |
| 69 | ГОСТ 2.101-2016. ЕСКД. Виды изделий |
| 70 | ГОСТ 2.102-2013. ЕСКД. Виды и комплектность конструкторских документов |
| 71 | ГОСТ 2.103-2013. ЕСКД. Стадии разработки |
| 72 | ГОСТ 2.104-2006. ЕСКД. Основные надписи |
| 73 | ГОСТ 2.105-95. ЕСКД. Общие требования к текстовым документам |
| 74 | ГОСТ 2.106-96. ЕСКД. Текстовые документы |
| 75 | ГОСТ 2.109-73. ЕСКД. Основные требования к чертежам |
| 76 | ГОСТ 2.111-2013. ЕСКД. Нормоконтроль |
| 77 | ГОСТ 2.114-2016. ЕСКД. Технические условия |
| 78 | ГОСТ 2.118-2013. ЕСКД. Техническое предложение |
| 79 | ГОСТ 2.119-2013. ЕСКД. Эскизный проект |
| 80 | ГОСТ 2.120-2013. ЕСКД. Технический проект |
| 81 | ГОСТ 2.123-93. ЕСКД. Комплектность конструкторских документов на печатные платы при автоматизированном проектировании |
| 82 | ГОСТ 2.125-2008. ЕСКД. Правила выполнения эскизных конструкторских документов. Общие положения |
| 83 | ГОСТ 2.503-2013. ЕСКД. Правила внесения изменений |
| 84 | ГОСТ Р 2.601-2019. ЕСКД. Эксплуатационные документы |
| 85 | ГОСТ 2.602-2013. ЕСКД. Ремонтные документы |
| 86 | ГОСТ Р 2.610-2019. ЕСКД. Правила выполнения эксплуатационных документов |
| 87 | ГОСТ 2.701-2008. ЕСКД. Схемы. Виды и типы. Общие требования к выполнению |
| 88 | ГОСТ 19.202-78. ЕСПД. Спецификация. Требования к содержанию и оформлению |
| 89 | ГОСТ 19.301-79. ЕСПД. Программа и методики испытаний. Требования к содержанию и оформлению |
| 90 | ГОСТ 19.401-78. ЕСПД. Текст программы. Требования к содержанию и оформлению |
| 91 | ГОСТ 19.402-78. ЕСПД. Описание программы |
| 92 | ГОСТ 19.502-78. ЕСПД. Описание применения. Требования к содержанию и оформлению |
| 93 | ГОСТ 19.504-79. ЕСПД. Руководство программиста. Требования к содержанию и оформлению |
| 94 | ГОСТ 19.505-79. ЕСПД. Руководство оператора. Требования к содержанию и оформлению |
| 95 | ГОСТ 19.506-79. ЕСПД. Описание языка. Требования к содержанию и оформлению |
| 96 | ГОСТ 19.507-79. ЕСПД. Ведомость эксплуатационных документов |
| 97 | ГОСТ 19.508-79. ЕСПД. Руководство по техническому обслуживанию. Требования к содержанию и оформлению |
| 98 | ГОСТ 19.601-78. ЕСПД. Общие правила дублирования, учета и хранения |
| 99 | ГОСТ 19.602-78. ЕСПД. Правила дублирования, учета и хранения программных документов, выполненных печатным способом |
| 100 | ГОСТ 19.603-78. ЕСПД. Общие правила внесения изменений |
| 101 | ГОСТ 19.604-78. ЕСПД. Правила внесения изменений в программные документы, выполненные печатным способом |
| 102 | ГОСТ 19.701-90 (ИСО 5807-85). ЕСПД. Схемы алгоритмов, программ, данных и систем. Обозначения условные и правила выполнения |
| 103 | ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения |
| 104 | ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем |
| 105 | ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания |
| 106 | ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы |
| 107 | ГОСТ 34.603-92. Информационная технология. Виды испытаний автоматизированных систем |
| 108 | ГОСТ Р ИСО 9000-2015. Системы менеджмента качества. Основные положения и словарь |
| 109 | ГОСТ Р ИСО 9001-2015. Системы менеджмента качества. Требования |
| 110 | ГОСТ Р ИСО 9004-2010. Менеджмент для достижения устойчивого успеха организации. Подход на основе менеджмента качества |
| 111 | ГОСТ Р ИСО/МЭК 9126-93. Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению |
| 112 | ГОСТ Р ИСО/МЭК ТО 9294-93. Информационная технология. Руководство по управлению документиро­ванием программного обеспечения |
| 113 | ГОСТ Р ИСО/МЭК 12207-2010. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств |
| 114 | ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель |
| 115 | ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности |
| 116 | ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности |
| 117 | ГОСТ Р ИСО/МЭК 18045-2013. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий |
| 118 | ГОСТ 19781-90. Обеспечение систем обработки информации программное. Термины и определения |
| 119 | ГОСТ 21552-84. Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортировка и хранение |
| 120 | ГОСТ 27201-87. Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования |
| 121 | ГОСТ 28195-89. Оценка качества программных средств. Общие положения |
| 122 | ГОСТ 28806-90. Качество программных средств. Термины и определения |
| 123 | ГОСТ 31814-2012. Оценка соответствия. Общие правила отбора образцов для испытаний продукции при подтверждении соответствия |
| 124 | ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования |
| 125 | ГОСТ Р 50922-2006. Защита информации. Основные термины и определения |
| 126 | ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения |
| 127 | ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения |
| 128 | ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования. ДСП |
| 129 | ГОСТ Р 53115-2008. Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства |
| 130 | ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей |
| 131 | ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем |
| 132 | ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования |
| 133 | ГОСТ Р 58412-2019 Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения |
| 134 | Р 50.1.053-2005. Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации |
| 135 | Р 50.1.056-2005. Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения |
| 136 | РД 50-682-89. Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Основные положения |

\*\* - Пометка ДСП (для служебного пользования) проставляется на документах, содержащих информацию ограниченного распространения в соответствии с Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности (с изменениями и дополнениями), утвержденном постановлением Правительства Российской Федерации от 3 ноября 1994 г. N 1233

# Приложение 4

|  |  |
| --- | --- |
| Бланк организации  (для юридического лица)  Исх. от \_\_\_\_\_\_\_\_\_ 20\_\_г.  № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Федеральная служба  по техническому  и экспортному контролю  Старая Басманная ул., д. 17,  Москва, 105066 |

Заявление

о предоставлении лицензии на осуществление деятельности

по технической защите конфиденциальной информации

юридическому лицу

Прошу предоставить *Федеральному Государственному Автономному Образовательному Учреждению Высшего Образования «Национальный исследовательский университет «Московский институт электронной техники»*

(полное и сокращенное (при наличии) наименование

юридического лица, его организационно-правовая форма)

лицензию на осуществление деятельности по технической защите конфиденциальной информации по следующим видам работ и (или) услуг:

*услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам в средствах и системах информатизации, работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации средств и систем информатизации*.

(виды работ и (или) услуг, установленные пунктом 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79, которые намерено осуществлять юридическое лицо)

Адрес в пределах места нахождения юридического лица:  
 124498, г. Москва, г. Зеленоград, площадь Шокина, дом 1.

Адреса мест осуществления лицензируемого вида деятельности: 124498, г. Москва, г. Зеленоград, площадь Шокина, дом 1.

Адрес для корреспонденции:   
124498, г. Москва, г. Зеленоград, площадь Шокина, дом 1.

(почтовый адрес юридического лица)

Телефон (факс при наличии) с указанием кода города: (499) 731-44-41

Адрес электронной почты (при наличии): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Основной государственный регистрационный номер (ОГРН): 1027739615584, серия 77 № 007397233, выдано Межрайонной инспекцией МНС России № 39 по г. Москве дата: 25 ноября 2002 г.

(данные документа, подтверждающего факт внесения сведений о юридическом лице в Единый государственный реестр юридических лиц)

Идентификационный номер налогоплательщика (ИНН):   
7735041133, серия 77 № 007397233, выдано Межрайонной инспекцией МНС России № 39 по г. Москве дата: 25 ноября 2002 г.

(данные документа, подтверждающего факт постановки юридического лица на учет в налоговом органе)

Реквизиты документа, подтверждающего факт уплаты государственной пошлины за предоставление лицензии, либо иные сведения, подтверждающие факт уплаты указанной государственной пошлины: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Работник, уполномоченный по вопросам лицензирования:

Специалист отдела по ПД ИТР и ТЗИ Носов Андрей Сергеевич, телефон: 8-(916)416-76-91, факс: 8-(499)740-92-13, e-mail: [nosov\_miet@mail.ru](mailto:nosov_miet@mail.ru).

(фамилия, имя, отчество (при наличии), номера телефонов)

Приложение: 1. Сведения, подтверждающие наличие и квалификацию персонала, согласно приложению № 1 к настоящему заявлению;

2. Сведения о наличии по месту осуществления лицензируемого вида деятельности защищаемых помещений согласно приложению № 2 к настоящему заявлению;

3. Сведения о наличии аттестованных по требованиям безопасности информации автоматизированных систем, находящихся в защищаемом помещении, предназначенных для хранения и обработки конфиденциальной информации, согласно приложению № 3 к настоящему заявлению;

4. Описание технологического процесса обработки конфиденциальной информации в автоматизированных системах согласно приложению № 4 к настоящему заявлению;

5. Перечень защищаемых в автоматизированной системе ресурсов согласно приложению № 5 к настоящему заявлению;

6. Сведения об оборудовании, необходимом для выполнения заявленных работ и (или) оказания услуг при осуществлении деятельности по технической защите конфиденциальной информации, согласно приложению № 6 к настоящему заявлению;

7. Сведения о технической и технологической документации, национальных стандартах и методических документах, необходимых для выполнения, оказания заявленных работ, услуг при осуществлении деятельности по технической защите конфиденциальной информации, согласно приложению № 7 к настоящему заявлению;

8. Иные сведения и копии документов, перечень которых определен Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79;

9. Опись прилагаемых к заявлению документов на \_\_ л. согласно приложению № 8 к настоящему заявлению.

Ю.А. Чаплыгин \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(руководитель постоянно (подпись) (инициалы, фамилия) действующего исполнительного органа юридического лица или иное лицо, имеющее право действовать от имени этого юридического лица)

М.П.

(при наличии печати)

**Министерство образования и науки Российской Федерации**

**Федеральное государственное автономное образовательное учреждение**

**высшего образования «Национальный исследовательский университет**

**«Московский институт электронной техники»**

УТВЕРЖДАЮ

Заведующий кафедрой ИБ

\_\_\_\_\_\_\_\_\_\_\_\_\_ А.А. Хорев

«\_\_\_» февраля 2025 г.

**ЗАДАНИЕ**

**НА курсовУЮ РАБОТУ**

**ПО ДИСЦИПЛИНЕ**

**«Организационное и правовое обеспечение информационной безопасности»**

**Студенту учебной группы** ИБ-21, Иванову Ивану Ивановичу

**Тема: «разработка средств, защищенных программных (программно-технических) средств обработки информации»**

**Целевая установка и исходные данные**

На основе анализа, изучения и обобщения исходной обстановки, нормативных правовых актов и нормативно-методических документов ФСТЭК России уяснить задачу и подготовить проект документов на получение лицензии на обозначенный в теме вид деятельности по технической защите информации, см. таблицу 1.

1. Для чего:
   1. Не позднее исхода **четвертой[[1]](#footnote-1)** недели семестра **уяснить задачу** и оформить в электронном виде, направить в адрес на согласование и утверждение у заведующего кафедрой.
   2. Не позднее исхода **двенадцатой** недели текущего семестра доложить о проценте выполненной работы.
   3. Не позднее исхода **пятнадцатой** недели текущего семестра направить проект отчета по курсовой работе.
   4. Не позднее исхода **семнадцатой недели текущего** семестра оформить отчет о НИР, сброшюровать отчет вместе с индивидуальным заданием и календарным планом – в электронном виде. Подготовить презентацию об основных результатах КР.
2. Результаты НИР оформить как научно-исследовательскую работу в соответствии со стандартом - <https://cloud.mail.ru/public/sLky/BF9yCrR4f>
3. Файл с индивидуальным заданием и календарным план-графиком выполнения КР прикрепить вначале отчета по КР.
4. Подготовить презентацию, результат защитить публично в соответствии с графиком.

**Основные вопросы, подлежащие разработке:**

1. Краткая характеристика рассматриваемого вида деятельности.
2. Общие положения по организации работы по подготовке к лицензированию
3. Разработка предложений по подготовке к лицензированию.
   1. Разработка перечня документов, необходимых для получения лицензии по технической защите конфиденциальной информации.
   2. Обоснование состава и квалификации инженерно-технического персонала организации, необходимогонеобходимых для выполнения работ и оказания услуг при осуществлении деятельности по технической защите конфиденциальной информации.
   3. Обоснование состава производственного, контрольно-измерительного, испытательного оборудования и средств контроля защищенности информации, необходимогонеобходимых для выполнения работ и оказания услуг при осуществлении деятельности по технической защите конфиденциальной информации
   4. Обоснование состава средств защиты информации, необходимогонеобходимых для выполнения работ и оказания услуг при осуществлении деятельности по технической защите конфиденциальной информации.
   5. Обоснование состава программного обеспечения, необходимогонеобходимых для выполнения работ и оказания услуг при осуществлении деятельности по технической защите конфиденциальной информации.
   6. Обоснование состава технической документации, национальных стандартов и методических документов, необходимогонеобходимых для выполнения работ и оказания услуг при осуществлении деятельности по технической защите конфиденциальной информации
   7. Оформление проекта заявления о предоставлении лицензии на деятельность.

Заключение

Литература

**Исходная обстановка**

Совет Директоров копании «ООО Тест» на совещании принял решение о реализации вида деятельности по технической защите информации, который определен в Уставе «ООО Тест», но до настоящего времени не был реализован.

Для чего генеральному директору «ООО Тест» была поставлена задача до первого июля текущего года получить лицензию на соответствующий вид деятельности по технической защите информации.

Генеральный директор «ООО Тест» 19 февраля текущего года поставил задачу начальнику управления безопасности «ООО Тест» организовать подготовку проекта документации на получение соответствующей лицензии. Пакет документов представить на утверждение не позднее чем 28 мая текущего года.

Начальник управления безопасности принял решение поручить подготовку пакета документов ведущему специалисту отдела информационной безопасности (ФИО в соответствии с таблицей 1)***.***

24 февраля текущего года на рабочем совещании он поставил задачу не позднее чем 02 июня текущего года «Разработать пакет документов на получение лицензии на осуществление соответствующего вида деятельности – см. задание».

Не позднее 1 марта текущего года разработать календарный план-график выполнения курсовой работы совместно с ассистентом и представить его на утверждение преподавателю.

Ежемесячно отчитываться о выполненной работе ассистенту.

Начальник управления безопасности «ООО Тест» сообщил, что заслушивание предложений по подготовке к лицензированию и по пакету документов будет назначено с 23 мая по 02 июня текущего года, о времени будет сообщено позже.

При подготовке предложений (пояснительной записки) следовать «**Методическим рекомендациям по выполнению курсовой работы по дисциплине».**

**К защите представить:** пояснительную записку объемом 25 – 30 страниц с приложением проектов документов на получение лицензии на осуществление деятельности по технической защите конфиденциальной информации.

Таблица 1. Закрепление персональной ответственности

|  |  |  |  |
| --- | --- | --- | --- |
| Номер варианта, номер в списке группы | Наименование задачи | Фамилия студента | Примечание |
| **В соответствии с Постановлением Правительства РФ от 3 марта 2012 г. N 171**  **«О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» (найти на сайте ФТЭК)** | | | |
|  | разработка средств, защищенных программных (программно-технических) средств обработки информации | Иванов Иван Иванович |  |

**Рекомендуемая литература и методические материалы**

Новиков В.К. Организационное и правовое обеспечение информационной безопасности [Текст]: в 2-х ч.: Учеб. пособие. Ч. 1: Правовое обеспечение информационной безопасности / В. К. **Новиков**; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - М.: МИЭТ, 2013. - 184 с. - Имеется электронная версия издания. - ISBN 978-5-7256-0733-8.

Новиков В.К. Организационное и правовое обеспечение информационной безопасности [Текст]: в 2-х ч.: Учеб. пособие. Ч. 2: Организационное обеспечение информационной безопасности / В. К. Новиков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - М.: МИЭТ, 2013. - 172 с. - Имеется электронная версия издания. - ISBN 978-5-7256-0738-3. ББК 67.401 - Н-731 ББК 67.401 - Н-731.

[Федеральный закон №184-ФЗ, 2002 г. «О техническом регулировании»](http://www.consultant.ru/document/cons_doc_LAW_40241/);

[Федеральный Закон № 149-ФЗ, 2006 г. «Об информации, информационных технологиях и защите информации»](http://www.consultant.ru/document/cons_doc_LAW_61798/);

[Федеральный законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».](http://www.consultant.ru/document/cons_doc_LAW_113658/)

[Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».](http://www.consultant.ru/document/cons_doc_LAW_14031/)

[Постановление Правительства Российской Федерации от 21 ноября 2011 г. № 957 «Об организации лицензирования отдельных видов деятельности».](http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=187687;fld=134;from=179020-6;rnd=189271.23858837340958416;;ts=01892719821816335897893)

[Постановление Правительства Российской Федерации № 171 от 03.03.12 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации».](http://www.consultant.ru/document/cons_doc_LAW_127010/)

[Постановление Правительства Российской Федерации № 79 от 03.02.12 г. «О лицензировании деятельности по технической защите конфиденциальной информации».](http://www.consultant.ru/document/cons_doc_LAW_125798/)

[Приказ ФСТЭК России от 12 июля 2012 г. № 83 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации.](http://www.consultant.ru/document/cons_doc_LAW_134332/2ff7a8c72de3994f30496a0ccbb1ddafdaddf518/)

[Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). – М.: Гостехкомиссия РФ, 1997. – 55 с.](file:///E:/Занятия%20учебные%20МИЭТ/Правовые%20основы%20ИБ%20курс/КР/СТР-К(РОССИЯ).doc)

[Постановление Правительства РФ от 15.06.2016 N 541 "О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам лицензирования отдельных видов деятельности".](http://www.consultant.ru/document/cons_doc_LAW_199737/)

**Дополнительная литература**

1. Галатенко, В.А.    Стандарты информационной безопасности [Текст] : Курс лекций: Учеб. пособие / В. А. Галатенко ; Под ред. В.Б. Бетелина. - 2-е изд. - М.: Интернет-Университет Информационных технологий, 2012. - 264 с. - 2000 экз. - ISBN 978-5-9556-0053-6: 262-51; 262-50.
2. Комплексная система защиты информации на предприятии: учеб. пособие / Н.В. Гришина. - М.: Форум, 2011- 240 с.
3. Основы управления информационной безопасностью: учебное пособие. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - М.: Горячая Линия-Телеком, 2012. - 244 с.
4. Петренко, С.А.   Политики информационной безопасности [Текст] / С. А. Петренко, В. А. Курбатов. - М.: АйТи, 2006. - 400 с. - (Информационные технологии для инженеров). - ISBN 5-98453-024-4: 175-00.
5. Правовое обеспечение информационной безопасности [Текст]: Учеб. пособие / Под ред. С.Я. Казанцева. - М.: Академия, 2005. - 240 с. - (Высшее профессиональное образование). - ISBN 5-7695-1209-1: 130-29.
6. Торокин А.А.    Инженерно-техническая защита информации [Текст]: Учеб. пособие / А. А. Торокин. - М.: Гелиос АРВ, 2005. - 960 с. - ISBN 5-85438-140-0: 245-19.

**Периодические издания**

1. Журнал «Специальная техника» (ВАК). Сайт журнала http://ess.ru/index.htm;
2. Журнал «Специальная техника и связь» (ВАК). Сайт журнала http://www.st-s.su/index.htm;
3. Журнал «Защита информации. Инсайд»; Сайт журнала http://www.inside-zi.ru/
4. Журнал «Безопасность информационных технологий». Сайт журнала сайт журнала <http://www.pvti.ru/articles_14.htm>.
5. Информационный бюллетень “Jet Info”. Издатель: компания «Инфосистемы Джет».Сайт журнала www.jetinfo.ru.
6. Бюро научно-технической информации «Техника для спецслужб». − <http://www.bnti.ru/about.asp>.
7. Журнал «Системы и сети». − [http://systemseti.com/](http://systemseti.com/wimax/obespechenie_bezopasnosti/1.html)
8. Журнал «Information Security/Информационная безопасность». Издатель: компания «Гротек». − http://www.itsec.ru

**Интернет-ресурсы**

<http://www.fstec.ru/> - сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России);

<http://ess.ru/index.htm> - сайт журнала «Специальная техника»;

<http://www.st-s.su/index.htm> - сайт журнала «Специальная техника и связь»;

<http://www.inside-zi.ru/> - сайт журнала «Защита информации. Инсайд»;

<http://www.pvti.ru/articles_14.htm> - сайт журнала «Безопасность информационных технологий»;

http://kafedrasib.ru/?page\_id=119 - сайт журнала «Информация и безопасность»;

http://www.sec.ru/ - портал по безопасности;

<http://www.novocom.ru/> - сайт АОЗТ «Ново»;

http://www.mascom.ru/ - сайт ЦБИ «Маском»;

<http://www.nelk.ru/node/9> - сайт НПЦ «Нелк»;

<http://www.nppgamma.ru/-> сайт ФГУП НПП «Гамма»;

<http://www.infosec.ru/> - сайт НИП «Информзащита»;

<http://www.bnti.ru/about.asp> - Бюро научно-технической информации «Техника для спецслужб»;

<http://tk.gost.ru/wps/portal/tk362> - портал технического комитета по стандартизации «Защита информации». − <http://tk.gost.ru/wps/portal/tk362>.

Руководитель курсовой работы В.А. Воеводин /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /

(подпись)

Задание получил

Студент учебной группы ИБ-21 И.И. Иванов /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /

Фамилия, имя (подпись)

«26» февраля 2025 г.

УТВЕРЖДАЮ

доцент кафедры ИБ

\_\_\_\_\_\_\_\_\_\_\_\_\_ В.А. Воеводин

«\_\_» февраля 2025 г.

Приложение 1

**Календарный план-график выполнения курсовой работы по дисциплине**

**«Организационное и правовое обеспечение информационной безопасности»**

Тема: «разработка средств, защищенных программных (программно-технических) средств обработки информации»

|  |  |  |
| --- | --- | --- |
| **Этап работы** | **Срок выполнения** | **Дата выполнения и ссылка на результат** |
| Уяснить поставленную задачу. | 1-2 неделя | 26.02.25 |
| Составить и утвердить индивидуальное задание на курсовую работу. | 2-5 неделя | 26.02.25 |
| Составить перечень материалов, используемых для написания курсовой работы. | 5-7 неделя | 17.03.25 |
| Определить понятие «защищенных программных (программно-технических) средств обработки информации» и обозреть методы их разработки. | 7-8 неделя | 24.03.25 |
| Провести анализ методологии и этапов разработки защищенных программных (программно-технических) средств обработки информации. | 8-12 неделя | 27.04.25 |
| Разработать рекомендации к методу разработки защищенных программных (программно-технических) средств обработки информации. | 12-14 неделя | 10.05.25 |
| Сформулировать итоги исследования и выводы по результатам работы. | 14 неделя | 10.05.25 |
| Оформить отчет о НИР и направить его на электронный адрес преподавателя. | 15 неделя | 15.05.25 |
| Подготовить презентацию об основных результатах КР. Защитить полученные результаты. | 16 неделя | 23.05.25 |

Студент группы ИБ-21, И.И. Иванов

Дата 26.02.2025 Подпись /Фамилия и инициалы

Руководитель курсовой работы В.А.Воеводин /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

(подпись)

Задание получил И.И. Иванов /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

Студент учебной группы ИБ-21 (подпись)

26 февраля 2025 г.

1. Превышение сроков представления отчетности стоит штрафных баллов, см. график подготовки КР. [↑](#footnote-ref-1)