=МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ

КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Ордена Трудового Красного Знамени федеральное государственное

бюджетное учреждение высшего образования

**«Московский технический университет связи и информатики»**

Кафедра «Системное программирование»

Предмет:

Информационная безопасность.

Лабораторная работа № 5 по теме:

«ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ »

Выполнил студент гр. БВТ2201

Альвицов Д.С.

Проверила: Магомедова Д.И.

г. Москва

2023

Содержание

[Цель работы: 3](#__RefHeading___Toc161_1093169984)

[Ход работы: 3](#__RefHeading___Toc868_3790591116)

# Цель работы:

закрепление теоретических знаний в области правового обеспечения информационной безопасности.

# Ход работы:

Вариант 4

Тема: Изучение положений о государственном лицензировании деятельности в области защиты информации. Контрольные вопросы

1. Какие документы предоставляются для получения лицензии?

2. Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?

3. Какие средства относятся к шифровальным?

4. Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?

5. Назовите лицензионные требования и условия при распространении шифровальных (криптографических) средств.

6. Назовите лицензионные требования и условия при осуществлении разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифрованных (криптографических) средств информационных и телекоммуникационных систем.

7. Назовите лицензионные требования и условия при предоставлении услуг в области шифрования информации.

8. Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств

Ответы на контрольные вопросы

**1) Какие документы предоставляются для получения лицензии?**

Согласно приказу Министерства Связи Российской Фклкрации от 23 августа 1994 года № 214 о государственном лицензировании деятельности в области защиты информации.  
п. 1.7 Для получения лицензии представляются:

1. Заявление
2. Представление органа государственной власти Российской Федерации;
3. Материалы экспертизы, подтверждающие наличие необходимых условий для проведения работ по заявленным видам деятельности, а также профессиональную пригодность руководителя предприятия-заявителя или лиц, уполномоченных им для руководства лицензируемой деятельностью;
4. Копии документов о государственной регистрации предпринимательской деятельности и устава предприятия.

**2) Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?**

Согласно Постановлению Правительства РФ от 16.04.2012 N 314 (ред. от 03.02.2023) "Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)"

п. 3. Лицензируемая деятельность включает в себя:  
  
а) выполнение работ по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях;  
  
б) выполнение работ по выявлению электронных устройств, предназначенных для негласного получения информации, в технических средствах.  
  
п. 4. Лицензирование деятельности, определенной настоящим Положением, осуществляется Федеральной службой безопасности Российской Федерации (далее - лицензирующий орган).

**3) Какие средства относятся к шифровальным?**

согласно Решению Коллегии Евразийской экономической комиссии от 21.04.2015 N 30 (ред. от 05.09.2023) "О мерах нетарифного регулирования"

1. Товары, содержащие в своем составе шифровальные (криптографические) средства, имеющие любую из следующих составляющих:

1) симметричный криптографический алгоритм, использующий криптографический ключ длиной, не превышающей 56 бит;

2) асимметричный криптографический алгоритм, основанный на любом из следующих методов:

разложение на множители целых чисел, размер которых не превышает 512 бит;

вычисление дискретных логарифмов в мультипликативной группе конечного поля, размер которого не превышает 512 бит;

дискретный логарифм в группе конечного поля, отличного от поля, указанного в абзаце третьем настоящего подпункта, размер которого не превышает 112 бит.

Примечания: 1. Биты четности не включаются в длину ключа.

1. Термин "криптография" не относится к фиксированным методам сжатия или кодирования данных.

2. Товары, содержащие шифровальные (криптографические) средства, обладающие следующими ограниченными функциями:

1) аутентификация, включающая в себя все аспекты контроля доступа, где нет шифрования файлов или текстов, за исключением шифрования, которое непосредственно связано с защитой паролей, персональных идентификационных номеров или подобных данных для защиты от несанкционированного доступа;

2) электронная цифровая подпись (электронная подпись).

Примечание. Функции аутентификации и электронной цифровой подписи (электронной подписи) включают в себя связанную с ними функцию распределения ключей.

3. Шифровальные (криптографические) средства, являющиеся компонентами программных операционных систем, криптографические возможности которых не могут быть изменены пользователями, которые разработаны для установки пользователем самостоятельно без дальнейшей существенной поддержки поставщиком и техническая документация (описание алгоритмов криптографических преобразований, протоколы взаимодействия, описание интерфейсов и т.д.) на которые является доступной пользователю.

4. Персональные смарт-карты (интеллектуальные карты):

1) криптографические возможности которых ограничены их использованием в категориях товаров (продукции), указанных в [пунктах 5](https://www.consultant.ru/document/cons_doc_LAW_456578/958f8d40005fdd7ad5d4ee7624015522c29b2e69/" \l "dst116449) - [8](https://www.consultant.ru/document/cons_doc_LAW_456578/958f8d40005fdd7ad5d4ee7624015522c29b2e69/" \l "dst116458) настоящего перечня;

2) для широкого общедоступного применения, криптографические возможности которых недоступны пользователю и которые в результате специальной разработки имеют ограниченные возможности защиты хранящейся на них персональной информации.

Примечание. Если персональная смарт-карта (интеллектуальная карта) может осуществлять несколько функций, контрольный статус каждой из функций определяется отдельно.

5. Приемная аппаратура для радиовещания, коммерческого телевидения или аналогичная коммерческая аппаратура для вещания на ограниченную аудиторию без шифрования цифрового сигнала, кроме случаев использования шифрования исключительно для управления видео- или аудиоканалами, отправки счетов или возврата связанной с программой информации провайдерам вещания.

6. Оборудование, криптографические возможности которого недоступны пользователю, специально разработанное и ограниченное для применения любым из следующих способов:

1) программное обеспечение исполнено в защищенном от копирования виде;

2) доступом к любому из следующего:

защищенному от копирования содержимому, хранящемуся только на доступном для чтения электронном носителе информации;

информации, хранящейся в зашифрованной форме на электронных носителях информации, которые предлагаются на продажу населению в идентичных наборах;

3) контроль копирования аудио- и видеоинформации, защищенной авторскими правами.

7. Шифровальное (криптографическое) оборудование, специально разработанное и ограниченное применением для банковских или финансовых операций.

Примечание. Финансовые операции включают в себя в том числе сборы и оплату за транспортные услуги и кредитование.

8. Портативные или мобильные радиоэлектронные средства гражданского назначения (например, для использования в коммерческих гражданских системах сотовой радиосвязи), которые не способны к сквозному шифрованию (от абонента до абонента).

9. Беспроводное радиоэлектронное оборудование, осуществляющее шифрование информации только в радиоканале с максимальной дальностью беспроводного действия без усиления и ретрансляции менее 400 м в соответствии с техническими условиями производителя.

10. Шифровальные (криптографические) средства, используемые для защиты технологических каналов информационно-телекоммуникационных систем и сетей связи.

11. Товары, криптографическая функция которых заблокирована производителем.

12. Иные товары, которые содержат шифровальные (криптографические) средства, отличные от указанных в [пунктах 1](https://www.consultant.ru/document/cons_doc_LAW_456578/958f8d40005fdd7ad5d4ee7624015522c29b2e69/" \l "dst116432) – [11](https://www.consultant.ru/document/cons_doc_LAW_456578/958f8d40005fdd7ad5d4ee7624015522c29b2e69/" \l "dst116461) настоящего перечня, и соответствуют следующим критериям:

1) общедоступны для продажи населению в соответствии с законодательством государства - члена Евразийского экономического союза без ограничений из имеющегося в наличии ассортимента в местах розничной продажи посредством любого из следующего:

продажи за наличные;

продажи путем заказа товаров по почте;

электронных сделок;

продажи по телефонным заказам;

2) шифровальные (криптографические) функциональные возможности которых не могут быть изменены пользователем простым способом;

3) разработаны для установки пользователем без дальнейшей существенной поддержки поставщиком;

**4) Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?**

согласно Постановлению Правительства РФ от 23.09.2002 N 691 "Об утверждении Положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами"

п. 5. Лицензирование деятельности по техническому обслуживанию шифровальных (криптографических) средств осуществляется Федеральным агентством правительственной связи и информации при Президенте Российской Федерации (далее именуется - лицензирующий орган).

**5) Назовите лицензионные требования и условия при распространении шифровальных (криптографических) средств.**

согласно Постановлению Правительства РФ от 29.12.2007 N 957 (ред. от 24.09.2010) "Об утверждении Положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами"

4. Лицензионными требованиями и условиями при распространении шифровальных (криптографических) средств являются:

а) наличие у соискателя лицензии (лицензиата) на праве собственности или на ином законном основании помещений, технологического, испытательного, контрольно-измерительного оборудования, иных объектов и сооружений, необходимых для осуществления лицензируемой деятельности;

б) наличие в штате у соискателя лицензии (лицензиата) следующего квалифицированного персонала:

руководитель и (или) лицо, уполномоченное руководить работами по лицензируемой деятельности, имеющие высшее профессиональное образование и (или) профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области не менее 5 лет;

инженерно-технические работники, имеющие высшее профессиональное образование или прошедшие переподготовку (повышение квалификации) в области информационной безопасности с получением специализации, необходимой для работы с шифровальными (криптографическими) средствами;

в) выполнение соискателем лицензии (лицензиатом) при осуществлении лицензируемой деятельности требований, устанавливаемых в соответствии со [статьями 11.2](https://www.consultant.ru/document/cons_doc_LAW_74104/b5e85264acb238face02146b2981659102ab5597/) и [13](https://www.consultant.ru/document/cons_doc_LAW_74104/b5e85264acb238face02146b2981659102ab5597/) Федерального закона "О федеральной службе безопасности";

г) представление соискателем лицензии (лицензиатом) в лицензирующий орган перечня шифровальных (криптографических) средств, в том числе иностранного производства, не имеющих сертификата Федеральной службы безопасности Российской Федерации или Федерального агентства правительственной связи и информации при Президенте Российской Федерации, технической документации, определяющей состав, характеристики и условия эксплуатации этих средств, и (или) образцов шифровальных (криптографических) средств;

д) использование соискателем лицензии (лицензиатом) программ для электронно-вычислительных машин и баз данных на основании договора, заключенного с правообладателем, в соответствии со [статьей 14](https://www.consultant.ru/document/cons_doc_LAW_58240/18e070c8f85e51f9132a868415c9fe574c639709/" \l "dst100091) Закона Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных".

**6) Назовите лицензионные требования и условия при осуществлении разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифрованных (криптографических) средств информационных и телекоммуникационных систем.**

согласно Постановлению Правительства РФ от 29.12.2007 N 957 (ред. от 24.09.2010) "Об утверждении Положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами"

4. Лицензионными требованиями и условиями при осуществлении разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем, являются:

а) наличие у соискателя лицензии (лицензиата) на правах собственности или на ином законном основании помещений, технологического, испытательного, контрольно-измерительного оборудования, иных объектов и сооружений, необходимых для осуществления лицензируемой деятельности;

б) наличие в штате у соискателя лицензии (лицензиата) следующего квалифицированного персонала:

руководитель и (или) лицо, уполномоченное руководить работами по лицензируемой деятельности, имеющие высшее профессиональное образование и (или) профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области не менее 5 лет;

инженерно-технические работники, имеющие высшее профессиональное образование или прошедшие переподготовку (повышение квалификации) в области информационной безопасности с получением специализации, необходимой для работы с шифровальными (криптографическими) средствами, а также стаж работы в этой области не менее 2 лет;

в) наличие у соискателя лицензии (лицензиата) допуска к проведению работ, связанных с использованием сведений, составляющих государственную тайну (только при разработке шифровальных (криптографических) средств);

г) выполнение соискателем лицензии (лицензиатом) при осуществлении лицензируемой деятельности требований и условий, устанавливаемых в соответствии со [статьями 11.2](https://www.consultant.ru/document/cons_doc_LAW_74104/90bd1a0c1022beea73de6f041de410cd0e105d72/) и [13](https://www.consultant.ru/document/cons_doc_LAW_74104/90bd1a0c1022beea73de6f041de410cd0e105d72/) Федерального закона "О федеральной службе безопасности";

д) реализация криптографических алгоритмов, рекомендованных лицензирующим органом, в разрабатываемых шифровальных (криптографических) средствах, применяемых в информационно-телекоммуникационных системах и сетях критически важных объектов, федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления и организаций, осуществляющих выполнение работ или оказание услуг с использованием шифровальных (криптографических) средств для государственных и муниципальных нужд;

у) обеспечение соискателем лицензии (лицензиатом) контролируемого доступа персонала к конфиденциальной информации и (или) работам с шифровальными (криптографическими) средствами, а также сохранности конфиденциальной информации и шифровальных (криптографических) средств, используемых при осуществлении лицензируемой деятельности;

ж) применение лицензиатом средств обработки информации, аттестованных в соответствии с требованиями по защите информации;

з) использование соискателем лицензии (лицензиатом) программ для электронно-вычислительных машин и баз данных на основании договора, заключенного с правообладателем в соответствии со [статьей 14](https://www.consultant.ru/document/cons_doc_LAW_58240/18e070c8f85e51f9132a868415c9fe574c639709/" \l "dst100091) Закона Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных".

**7) Назовите лицензионные требования и условия при предоставлении услуг в области шифрования информации.**

согласно Постановлению Правительства РФ от 29.12.2007 N 957 (ред. от 24.09.2010) "Об утверждении Положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами"

п. 4. Лицензионными требованиями и условиями при предоставлении услуг в области шифрования информации являются:

а) наличие у соискателя лицензии (лицензиата) на правах собственности или на ином законном основании помещений, технологического, испытательного, контрольно-измерительного оборудования, иных объектов и сооружений, необходимых для осуществления лицензируемой деятельности;

б) наличие в штате у соискателя лицензии (лицензиата) следующего квалифицированного персонала:

руководитель и (или) лицо, уполномоченное руководить работами по лицензируемой деятельности, имеющие высшее профессиональное образование и (или) профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области не менее 5 лет;

инженерно-технические работники, имеющие высшее профессиональное образование или прошедшие переподготовку (повышение квалификации) в области информационной безопасности с получением специализации, необходимой для работы с шифровальными (криптографическими) средствами;

в) выполнение соискателем лицензии (лицензиатом) при осуществлении лицензируемой деятельности требований, устанавливаемых в соответствии со [статьями 11.2](https://www.consultant.ru/document/cons_doc_LAW_74104/014ca06793ec7ceb8bcc7e55e8a5c2b591c96765/) и [13](https://www.consultant.ru/document/cons_doc_LAW_74104/014ca06793ec7ceb8bcc7e55e8a5c2b591c96765/) Федерального закона "О федеральной службе безопасности";

г) реализация криптографических алгоритмов, рекомендованных лицензирующим органом, в разрабатываемых шифровальных (криптографических) средствах, применяемых в информационно-телекоммуникационных системах и сетях критически важных объектов, федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления и организаций, осуществляющих выполнение работ или оказание услуг с использованием шифровальных (криптографических) средств для государственных и муниципальных нужд;

д) применение лицензиатом средств обработки информации, аттестованных в соответствии с требованиями по защите информации;

е) ведение лицензиатом учета изготовления, выдачи, возврата и уничтожения ключевых документов;

ж) обеспечение лицензиатом уничтожения исходной ключевой информации путем физического уничтожения носителя, на котором она расположена, или путем стирания (разрушения) исходной ключевой информации без повреждения носителя (для обеспечения возможности его многократного использования) в соответствии с эксплуатационной и технической документацией к соответствующим шифровальным (криптографическим) средствам, а также с указаниями организации, производившей запись исходной ключевой информации;

з) представление лицензиатом в лицензирующий орган перечня шифровальных (криптографических) средств, в том числе иностранного производства, не имеющих сертификата Федеральной службы безопасности Российской Федерации или Федерального агентства правительственной связи и информации при Президенте Российской Федерации, технической документации, определяющей состав, характеристики и условия эксплуатации этих средств, и (или) образцов шифровальных (криптографических) средств;

и) использование лицензиатом шифровальных (криптографических) средств иностранного производства при условии, что эти средства были ввезены на территорию Российской Федерации и распространялись в порядке, установленном нормативными правовыми актами Российской Федерации;

к) использование соискателем лицензии (лицензиатом) программ для электронно-вычислительных машин и баз данных на основании договора, заключенного с правообладателем в соответствии со [статьей 14](https://www.consultant.ru/document/cons_doc_LAW_58240/18e070c8f85e51f9132a868415c9fe574c639709/" \l "dst100091) Закона Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных".

**8) Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.**

согласно Постановление Правительства РФ от 23.09.2002 N 691 "Об утверждении Положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами"

п. 6. Лицензионными требованиями и условиями при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств являются:

а) выполнение нормативных правовых актов Российской Федерации и соблюдение государственных стандартов, относящихся к лицензируемой деятельности;

б) выполнение нормативных документов лицензирующего органа, регламентирующих осуществление лицензируемой деятельности, зарегистрированных в установленном порядке Министерством юстиции Российской Федерации, и методических документов, касающихся лицензируемой деятельности, издаваемых лицензирующим органом в пределах своей компетенции;

в) представление в лицензирующий орган перечня шифровальных (криптографических) средств, используемых при осуществлении лицензируемой деятельности (с предоставлением по запросу технической документации и (или) образцов шифровальных (криптографических) средств, которые не имеют сертификата Федерального агентства правительственной связи и информации при Президенте Российской Федерации);

г) использование шифровальных (криптографических) средств иностранного производства при условии, что эти средства были ввезены на территорию Российской Федерации и распространялись в порядке, установленном нормативными правовыми актами Российской Федерации;

д) наличие принадлежащих лицензиату на праве собственности или на ином законном основании сооружений, помещений, технологического, испытательного, контрольно - измерительного оборудования и иных объектов, необходимых для осуществления лицензируемой деятельности в соответствии с установленными технологическими требованиями;

е) соответствие указанных помещений требованиям, предъявляемым к такого рода помещениям технической документацией на находящееся в них оборудование;

ж) обслуживание указанного оборудования в соответствии с регламентом, предусмотренным эксплуатационной документацией;

з) проведение своевременной поверки технологического, испытательного и контрольно - измерительного оборудования, используемого при осуществлении лицензируемой деятельности;

и) использование программ для электронно - вычислительных машин и баз данных третьими лицами (пользователями) на основании договора с правообладателем;

к) наличие системы поэкземплярного учета шифровальных (криптографических) средств и документации к ним;

л) установление порядка доступа лиц к конфиденциальной информации, связанной с осуществлением лицензируемой деятельности, и обеспечение контролируемого допуска персонала лицензиата к работам, связанным с этой информацией;

м) обеспечение безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации, связанной с осуществлением лицензируемой деятельности;

н) применение средств обработки информации, аттестованных в соответствии с требованиями по защите информации;

о) наличие охраны и (или) специального оборудования, а также распорядка работ, исключающих неконтролируемый доступ к шифровальным (криптографическим) средствам;

п) хранение шифровальных (криптографических) средств, их отдельных узлов и блоков, дистрибутивов программных и программно - аппаратных шифровальных (криптографических) средств, инсталляционных дискет, нормативной, эксплуатационной и ключевой документации к ним в хранилищах (металлических шкафах, сейфах), оборудованных внутренними замками;

р) наличие следующего квалифицированного персонала:

уководитель и (или) лицо, уполномоченное им руководить работами по осуществлению лицензируемой деятельности, имеющие высшее профессиональное образование и (или) профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области не менее 5 лет;

инженерно - технический персонал, имеющий высшее профессиональное образование или прошедший переподготовку (повышение квалификации) в области информационной безопасности с получением специализации, соответствующей виду шифровальных (криптографических) средств.