

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(РГГУ)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

ТЕХНИЧЕСКОЕ РЕГУЛИРОВАНИЕ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 10.03.01 Информационная безопасность

Направленность (профиль) подготовки:

№ 3 Комплексная защита объектов информатизации

Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2017

*Техническое регулирование в области защиты информации
Рабочая программа дисциплины*

Составитель:

Кандидат технических наук, доцент кафедры КЗИ А.С. Моляков

Ответственный редактор

Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО

Протокол заседания кафедры
комплексной защиты информации

№ 6 от 24.01.2017 г. _____

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1 Цель и задачи дисциплины

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине

1.3. Место дисциплины в структуре образовательной программы

2. Структура дисциплины

3. Содержание дисциплины

4. Образовательные технологии

5. Оценка планируемых результатов обучения

5.1. Система оценивания

5.2. Критерии выставления оценок

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

7. Материально-техническое обеспечение дисциплины

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

9. Методические материалы

9.1. Планы практических занятий

Приложения

Приложение 1. Аннотация дисциплины

Приложение 2. Лист изменений

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – формирование систематизированных знаний о вопросах технического регулирования в области защиты информации.

Задачи дисциплины:

- сформировать знания о лицензировании деятельности в области защиты информации;
- сформировать представления о сертификации средств защиты информации;
- сформировать и развить компетенции, знания и практические навыки в проведении аттестации объектов информатизации по требованиям безопасности информации.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:

Коды компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	<p>Знать:</p> <ul style="list-style-type: none"> - классификацию информации, подлежащей защите - классификацию угроз информационной безопасности - виды и возможные методы реализации угроз информационной безопасности <p>Уметь:</p> <ul style="list-style-type: none"> - определять виды и формы информации, подверженной угрозам - анализировать структуру и содержания информационных процессов предприятия - определять виды и возможные пути реализации угроз информационной безопасности <p>Владеть:</p> <ul style="list-style-type: none"> - навыками определения видов и форм информации, подверженной угрозам - навыками анализа структуры и содержания информационных процессов предприятия - навыками определения видов и возможных путей реализации угроз информационной безопасности
ПСК-3.3	способностью участвовать в реализации комплекса организационно-технических мер по обеспечению информационной безопасности объекта информатизации, осуществлять установку, настройку и обслуживание элементов защиты	<p>Знать:</p> <ul style="list-style-type: none"> - организационно-технические меры по обеспечению информационной безопасности объекта информатизации <p>Уметь:</p> <ul style="list-style-type: none"> - осуществлять установку, настройку и обслуживание средств и подсистем защиты

		Владеть: - навыками настройки средств защиты информации
ПСК-3.4	способностью организовать контроль защищенности объекта информатизации в соответствии с нормативными документами	Знать: - способы контроля защищенности объекта информатизации - нормативные документы по контролю защищенности объекта информатизации Уметь: - осуществлять контроль защищенности объекта информатизации Владеть: - навыками по участию в контроле защищенности - навыками по подготовке отчетных материалов контроля защищенности

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Техническое регулирование в области защиты информации» относится к дисциплинам базовой части блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Аттестация объектов информатизации».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет 4 з.е., 144 ч., в том числе контактная работа обучающихся с преподавателем 56 ч., промежуточная аттестация 18 ч., самостоятельная работа обучающихся 70 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)					Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации
			контактная						
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	<i>Требования федерального закона о техническом регулировании</i>	6	4					20	Опрос.
2	<i>Лицензирование</i>	6	8		10			20	Опрос.

	<i>деятельности предприятий в области защиты информации</i>							Оценка выполнения практических заданий
3	<i>Сертификация средств защиты информации</i>	6	8		10		20	Опрос. Оценка выполнения практических заданий
4	<i>Аттестация объектов информатизации по требованиям безопасности информации</i>	6	4		12		10	Опрос. Оценка выполнения практических заданий
	<i>Экзамен</i>	6					18	Экзамен по билетам
	итого:		24		32		70	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	Требования федерального закона о техническом регулировании	Анализ нормативно-правовой базы в области защиты информации. Законодательство РФ в области защиты информации. Государственное регулирование в сфере применения информационных технологий. Правовое регулирование защиты государственной тайны. Правовое регулирование защиты конфиденциальной информации. Правовое регулирование информационных отношений в области коммерческой тайны. Правовое регулирование защиты персональных данных.
2	Лицензирование деятельности предприятий в области защиты информации	Лицензирование в области защиты государственной тайны. Правовые основы деятельности предприятий со сведениями, составляющими государственную тайну. Лицензирование в области защиты конфиденциальной информации. Функции и полномочия Федеральной службы по техническому и экспортному контролю. Функции и полномочия Федеральной службы безопасности. Система ответственности за правонарушения в сфере защиты информации.
3	Сертификация средств защиты информации	Система сертификации в области защиты информации. Порядок проведения сертификации. Формы подтверждения соответствия.
4	Аттестация объектов информатизации по требованиям безопасности информации	Аттестация объектов информатизации. Органы аттестации, их структура и функции. Организация проведения аттестационных работ.

4. Образовательные технологии

Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1	Требования федерального закона о техническом регулировании	Лекция 1. Самостоятельная работа	Традиционная лекция с использованием презентаций Работа с литературой
2	Лицензирование деятельности предприятий в области защиты информации	Лекция 2. Практическое занятие 1 Самостоятельная работа	Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой
3	Сертификация средств защиты информации	Лекция 3. Практическое занятие 2 Самостоятельная работа	Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой
4	Аттестация объектов информатизации по требованиям безопасности информации	Лекция 4. Практическое занятие 3 Самостоятельная работа	Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль: - практическое занятие № 1	10 баллов	10 баллов
- практическое занятие № 2	25 баллов	25 баллов
- практическое занятие № 3	25 баллов	25 баллов
Промежуточная аттестация экзамен		40 баллов
Итого за дисциплину экзамен		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F,FX	«неудовлетворительно»/ не зачтено	<p>Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

5.4. Вопросы к экзамену - проверка сформированности компетенций ОПК-7, ПСК-3.3, ПСК-3.4

1. Какие отношения регулирует Федеральный закон «О техническом регулировании»?
2. На какие объекты распространяется сфера применения Федерального закона «О техническом регулировании»?
3. Как называется документ, удостоверяющий соответствие объектов требованиям технических регламентов, положениям стандартов или условиям договоров?
4. Какое определение соответствует понятию «оценка соответствия» (в соответствии с Федеральным законом «О техническом регулировании»)?
5. Какое определение соответствует понятию «сертификация» (в соответствии с Федеральным законом «О техническом регулировании»)?
6. Что в соответствии с Федеральным законом «О техническом регулировании» представляет собой система сертификации?

7. Как в соответствии с Федеральным законом «О техническом регулировании» следует назвать юридическое лицо и индивидуального предпринимателя, в установленном порядке аккредитованных для выполнения работ по сертификации?
8. Как в соответствии с Федеральным законом «О техническом регулировании» следует назвать прямое или косвенное определение соблюдения требований, предъявляемых к объекту?
9. Как в соответствии с Федеральным законом «О техническом регулировании» следует назвать документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов или условиям договоров?
10. Система лицензирования на право проведения работ и оказания услуг в области защиты информации с ограниченным доступом.
11. Нормативные документы, определяющие порядок лицензирования в области защиты конфиденциальной информации.
12. Какие лицензии выдаются ФСТЭК России?
13. Какие лицензии выдаются ФСБ России?
14. Различаются ли между собой лицензии ФСБ и ФСТЭК на деятельность по разработке/производству средств защиты конфиденциальной информации?
15. Условия лицензирования деятельности по защите конфиденциальной информации. Виды деятельности по ТЗКИ подлежащие лицензированию.
16. Общие принципы лицензирования в области защиты конфиденциальной информации.
17. Лицензионные требования для получения лицензии на деятельность в области технической защиты конфиденциальной информации.
18. Перечень документов, представляемых для получения лицензий в области защиты конфиденциальной информации.
19. Система сертификации средств защиты информации.
20. Цели системы сертификации средств защиты информации.
21. Нормативные документы определяющие порядок сертификации средств защиты информации на соответствие требованиям безопасности информации.
22. Структура средств защиты информации, подлежащих сертификации.
23. Аттестация объектов информатизации на соответствие требованиям безопасности информации.
24. Объекты, подлежащие аттестации.
25. Общие требования по аттестации объектов информатизации, предназначенных для обработки конфиденциальной информации.
26. Порядок проведения аттестации объектов информатизации.

Примерные задания для тестирования- проверка сформированности компетенций ОПК-7, ПСК-3.3, ПСК-3.4

1. Какой закон регулирует порядок разработки СЗИ:

- а) ФЗ “О техническом регулировании”.
- б) Конституция РФ.
- в) 239 Приказ ФСТЭК РФ.

2. Для обработки сведений с грифом Совершенно секретно по какому классу нужно аттестовать выделенное помещение:

- а) 1 классу.
- б) 2 классу.
- в) 3 классу.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

1. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsdatelya-gostekhkommisii-rossii-ot-30-marta-1992-g3>, свободный. – Загл. с экрана.
2. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsdatelya-gostekhkommisii-rossii-ot-30-marta-1992-g>, свободный. – Загл. с экрана.
3. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsdatelya-gostekhkommisii-rossii-ot-30-marta-1992-g2>, свободный. – Загл. с экрана.
4. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsdatelya-gostekhkommisii-rossii-ot-25-iyulya-1997-g>, свободный. – Загл. с экрана.
5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

Дополнительные

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_10699/, свободный. – Загл. с экрана.

Литература

Основная

1. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/546679>
2. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2010. - 544 с.: ил. - ISBN 978-5-94074-518-1. - Режим доступа: <http://znanium.com/catalog/product/408107>

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. ОХРАНА.ru. Российское СМИ о безопасности. [Электронный ресурс] : Режим доступа : <https://охрана.ru/>, свободный. – Загл. с экрана.
2. Sec.ru. Портал по безопасности. [Электронный ресурс] : Режим доступа : <http://sec.ru/>, необходима регистрация. – Загл. с экрана.
3. Банк данных угроз безопасности информации. [Электронный ресурс] / ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России» – Режим доступа : <http://sec.ru/>, свободный. – Загл. с экрана.

7. Материально-техническое обеспечение дисциплины

Для проведения занятий необходимо следующее материально-техническое обеспечение:

- 1) лекционный класс с видеопроектором и компьютером, на котором должны быть установлены:
 - лицензионное ПО MS Windows 7 и старше;
 - лицензионное ПО MS Office 2010 (с обязательным наличием MS PowerPoint) и старше
- 2) компьютерный класс, оборудованный современными персональными компьютерами для каждого студента с выходом в интернет. На компьютере должны быть установлены:
 - лицензионное ПО MS Windows 7 и старше;
 - лицензионное ПО MS Office 2010 и старше;
 - программный гипервизор VMware Player

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
2	Компьютерные справочные правовые системы Консультант Плюс, Гарант

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
 - обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
 - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
 - письменные задания оформляются увеличенным шрифтом;
 - экзамен и зачет проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
 - письменные задания выполняются на компьютере в письменной форме;
 - экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере со специализированным программным обеспечением;
 - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;
 - в форме электронного документа;
 - в форме аудиофайла.
- для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа;
 - в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
 - устройством для сканирования и чтения с камерой SARA CE;
 - дисплеем Брайля PAC Mate 20;
 - принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
 - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
 - акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
 - передвижными, регулируемые эргономическими партами СИ-1;
 - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий - проверка сформированности компетенций ОПК-7, ПСК-3.3, ПСК-3.4

Практическое занятие 1 (10 ч.) «Лицензирование деятельности предприятий в области защиты информации» (проверка сформированности компетенций ОПК-7)

Задания:

1. Определить, какие лицензии требуются для осуществления деятельности, исходные данные которой следующие (по вариантам):
 - Аттестовать собственную автоматизированную систему, в которой обрабатывается конфиденциальная информация.
 - Аттестовать собственную автоматизированную систему, в которой обрабатывается информация, составляющая государственную тайну.
 - Подключиться к системе "интернет-банк".
 - Получить квалифицированную электронную подпись.
 - Организовать в собственном магазине продажу СКЗИ для защиты конфиденциальной информации и последующее гарантийное обслуживание проданных СКЗИ.
 - Организовать в собственном магазине продажу СКЗИ для защиты информации, составляющей государственную тайну, и последующее гарантийное обслуживание проданных СКЗИ.
 - Организовать производство банковских пластиковых карт.
 - Организовать производство SIM-карт.
 - Организовать производство карт тахографов.
 - Организовать производство электронных полисов медицинского страхования.
 - Организовать выявление электронных устройств, предназначенных для негласного получения информации на своей территории своими силами, а также для оказания услуг на чужой территории.
 - Организовать производство СЗИ для защиты конфиденциальной информации, а также организовать оказание услуг по установке и настройке этих СЗИ и оказание услуг по контролю защищенности.
 - Организовать производство СЗИ для защиты информации, составляющей государственную тайну, а также организовать оказание услуг по установке и настройке этих СЗИ и оказание услуг по контролю защищенности.
2. Собрать на флеш-носителе пакет документов (в виде файлов Word и сканов – электронных копий) для имитации подачи этих документов на получение лицензии на лицензируемый вид деятельности. Наименование организаций, наименование технических средств, а также фамилии физических лиц в сканах, найденных в сети Интернет, не имеют значения (по вариантам):
 - Сертификационные испытания на соответствие требованиям по безопасности информации продукции, используемой в целях защиты конфиденциальной информации.
 - Разработка шифровальных (криптографических) средств и производство (тиражирование) шифровальных (криптографических) средств.
 - Разработка, производство, передача, монтаж, установка (инсталляция), наладка, ремонт и сервисное обслуживание защищенных с использованием шифровальных (криптографических) средств информационных систем.
 - Аттестационные испытания и аттестация на соответствие требованиям по защите информации средств и систем информатизации, помещений со средствами (системами) информатизации, подлежащими защите и защищаемых помещений.
 - Передача защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем. Предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государ-

- ственную тайну, с использованием шифровальных (криптографических) средств. Работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства.
- Разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации.
 - Проведение работ, связанных с использованием сведений, составляющих государственную тайну.
 - Проектирование в защищенном исполнении средств и систем информатизации, помещений со средствами (системами) информатизации, подлежащими защите и защищаемых помещений.
 - Выявление электронных устройств, предназначенных для негласного получения информации.
 - Разработка и производство средств защиты конфиденциальной информации - технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации и программных (программно-технических) средств контроля защищенности информации.
 - Установка, монтаж, испытания и ремонт средств защиты информации.
 - Осуществление мероприятий и (или) оказания услуг в области защиты государственной тайны.
 - Контроль защищенности конфиденциальной информации от утечки по техническим каналам в средствах и системах информатизации, технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается, помещениях со средствами (системами), подлежащими защите и помещениях, предназначенных для ведения конфиденциальных переговоров, а также контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации.

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer.

Практическое занятие 2 (10 ч.) «Сертификация средств защиты информации» (проверка сформированности компетенций ПСК-3.3, ПСК-3.4)

Задание: доклад в свободной форме по темам:

- Система сертификации в области защиты информации.
- Порядок проведения сертификации.
- Формы подтверждения соответствия.

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer.

Практическое занятие 3 (12 ч.) «Аттестация объектов информатизации по требованиям безопасности информации» (проверка сформированности компетенций ПСК-3.3, ПСК-3.4)

Задания:

1. Определить класс защищенности автоматизированной системы (АС) и обосновать выбор средства защиты информации для этой АС, исходные данные которой следующие (по вариантам, задаются преподавателем):
 - Уровень конфиденциальности, обрабатываемой в АС информации (служебная тайна либо коммерческая тайна).
 - Число пользователей в АС (один либо два и более).
 - Права пользователей в АС (одинаковые либо разные).
 - Используются ли в АС «съёмные накопители информации большой емкости» (да либо нет).
 - Тип средства вычислительной техники (персональный компьютер либо ноутбук).
2. Аттестовать защищаемое помещение. Для этого, используя действующие нормативные документы и образцы файлов, доступные в сети Интернет, подготовить заявку на аттестацию и разработать технический паспорт в виде файлов Word и файлов изображений (на флеш-носителе). Общие исходные данные: все здания в округе 9-тиэтажные; в помещении имеются батареи центрального отопления, центральное кондиционирование с главным блоком, расположенным на крыше здания, приточная и вытяжная вентиляция с вентиляционными камерами, расположенными в подвале и на чердаке, потолочное освещение с расположением электрического щитка в коридоре на этаже; при наличии персонального компьютера (ПК), расположенного в помещении, он имеет активные колонки; в случае, если ПК подключен к ЛВС, то указанный ПК имеет выход в сеть Интернет. Индивидуальные исходные данные следующие (по вариантам, задаются преподавателем):
 - двери помещения (одинарная деревянная; деревянная с тамбуром; одинарная деревянная с приёмной для секретаря; деревянная с тамбуром и с приёмной для секретаря; три одинарных деревянных двери, каждая в своём дверном проёме – конференц-зал); две деревянных двери с тамбуром каждая, каждая в своём дверном проёме – конференц-зал; одинарная деревянная с наружной звуконепроницаемой обивкой; деревянная с тамбуром с наружной звуконепроницаемой обивкой; двойная распашная стеклянная; одинарная металлическая; одинарная филёнчатая – раздвижная; металлическая гермодверь; одинарная стеклянная).
 - окна помещения (выходят во внутренний глухой двор; выходят на улицу; окон нет).
 - контролируемой зоной является (территория завода, занимающая весь квартал; отдельно стоящее здание; отдельный этаж конкретного здания; само помещение).
 - посторонние потребители по цепям электропитания (есть либо нет).
 - наличие в помещении вторичных часов либо громкоговорителя пожарного оповещения.
 - линии пожарной сигнализации из помещения выходят в пожарную часть, расположенную в соседнем квартале, либо в помещение дежурного, расположенное на этом же этаже.
 - наличие охранной сигнализации (есть либо нет), при этом при её наличии линии охранной сигнализации из помещения выходят в помещение дежурного, расположенное на этом же этаже, либо в ведомственную охрану, расположенную в соседнем квартале.
 - установлен телефон городской (ГАТС) или внутренней (УАТС) станции, тип телефонной линии (аналоговая либо цифровая линия).

- наличие ПК (имеется либо отсутствует), при этом при его наличии подключение ПК к ЛВС имеется либо отсутствует.

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer.

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Техническое регулирование в области защиты информации» реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины – формирование систематизированных знаний о вопросах технического регулирования в области защиты информации.

Задачи дисциплины:

- сформировать знания о лицензировании деятельности в области защиты информации;
- сформировать представления о сертификации средств защиты информации;
- сформировать и развить компетенции, знания и практические навыки в проведении аттестации объектов информатизации по требованиям безопасности информации.

Дисциплина направлена на формирование следующих компетенций:

- ОПК-7 - способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
- ПСК-3.3 - способностью участвовать в реализации комплекса организационно-технических мер по обеспечению информационной безопасности объекта информатизации, осуществлять установку, настройку и обслуживание элементов защиты
- ПСК-3.4 - способностью организовать контроль защищенности объекта информатизации в соответствии с нормативными документами

В результате освоения дисциплины обучающийся должен:

Знать основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСТЭК и ФСБ в данной области; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; понятия сертификации средств защиты информации; понятия лицензирования в области защиты информации.

Уметь пользоваться нормативными документами по защите информации; применять отечественные стандарты в области компьютерной безопасности.

Владеть навыками работы с нормативными правовыми актами.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоёмкость освоения дисциплины составляет 4 зачётных единицы.

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	29.06.2017г.	10
2	<i>Обновлена структура дисциплины (модуля) для очной формы обучения (2018 г.)</i>	26.06.2018 г.	11
3	<i>Обновлена основная и дополнительная литература</i>	26.06.2018 г.	11
4	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	26.06.2018 г.	11
5	<i>Обновлена структура дисциплины (модуля) для очной формы обучения (2019 г.)</i>	29.08.2019 г.	1
6	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	29.08.2019 г.	1
7	<i>Обновлена структура дисциплины (модуля) для очной формы обучения (2020 г.)</i>	23.06.2020	14
8	<i>Обновлена основная и дополнительная литература</i>	23.06.2020	14
9	<i>Обновлен раздел п.4 Образовательные технологии</i>	23.06.2020	14
10	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	23.06.2020	14

1. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) (2017 г.)**Перечень ПО**

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	MicrosoftOffice 2013	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	KasperskyEndpointSecurity	Kaspersky	лицензионное
4	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное

Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель: К.т.н, доцент, А.С. Моляков

2. Обновление структуры дисциплины (модуля) для очной формы обучения (2018 г.)

Общая трудоёмкость дисциплины составляет 4 з.е., 144 ч., в том числе контактная работа обучающихся с преподавателем 56 ч., самостоятельная работа обучающихся 88 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)					Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации
			контактная						
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	<i>Требования федерального закона о техническом регулировании</i>	6	4					20	Опрос.
2	<i>Лицензирование деятельности предприятий в области защиты информации</i>	6	8		10			20	Опрос. Оценка выполнения практических заданий
3	<i>Сертификация средств защиты информации</i>	6	8		10			20	Опрос. Оценка выполнения практических заданий
4	<i>Аттестация объектов информатизации по требованиям безопасности информации</i>	6	4		12			10	Опрос. Оценка выполнения практических заданий
	<i>Зачет с оценкой</i>	6							<i>Зачет с оценкой по билетам</i>
	ИТОГО:		24		32			88	

3. Обновление раздела «Учебно-методическое и информационное обеспечение дисциплины» - обновление источников и литературы (2018)

Источники основные

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

Дополнительные

Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 03.07.2018). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_10699/, свободный. – Загл. с экрана.

Литература основная

Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М. : РИОР : ИНФРА-М, 2018. - 392 с. - (Высшее образование: Бакалавриат; Магистратура). — <https://doi.org/10.12737/4868>. - Режим доступа: <http://znanium.com/catalog/product/937469>

4. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) (2018 г.)

Перечень ПО

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное

Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2018 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2018 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель: К.Т.Н, доцент, А.С. Моляков

5. Обновление структуры дисциплины (модуля) для очной формы обучения (2019 г.)

Общая трудоёмкость дисциплины составляет 4 з.е., 144 ч., в том числе контактная работа обучающихся с преподавателем 56 ч., самостоятельная работа обучающихся 70 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)					Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации
			контактная						
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	<i>Требования федерального закона о техническом регулировании</i>	6	4					16	Опрос.
2	<i>Лицензирование деятельности предприятий в области защиты информации</i>	6	8		10			18	Опрос. Оценка выполнения практических заданий
3	<i>Сертификация средств защиты информации</i>	6	8		10			18	Опрос. Оценка выполнения практических заданий
4	<i>Аттестация объектов информатизации по требованиям безопасности информации</i>	6	4		12			18	Опрос. Оценка выполнения практических заданий
	<i>Экзамен</i>	6					18		<i>Экзамен по билетам</i>
	Итого:		24		32		18	70	

6. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2019 г.)**Перечень ПО**

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое

			няемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «АЛЬТ Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное

Перечень БД и ИСС

№п /п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2019 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2019 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель: К.т.н, доцент, А.С. Моляков

7. Обновление структуры дисциплины (модуля) для очной формы обучения (2020 г.)**Структура дисциплины (модуля) для очной формы обучения**

Общая трудоёмкость дисциплины составляет 4 з.е., 152 ч., в том числе контактная работа обучающихся с преподавателем 56 ч., самостоятельная работа обучающихся 78 ч., промежуточная аттестация – 18 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)					Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации
			контактная						
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	<i>Требования федерального закона о техническом регулировании</i>	6	4					20	Опрос.
2	<i>Лицензирование деятельности предприятий в области защиты информации</i>	6	8		10			20	Опрос. Оценка выполнения практических заданий
3	<i>Сертификация средств защиты информации</i>	6	8		10			20	Опрос. Оценка выполнения практических заданий
4	<i>Аттестация объектов информатизации по требованиям безопасности информации</i>	6	4		12			18	Опрос. Оценка выполнения практических заданий
	<i>Экзамен</i>	6						18	<i>Экзамен по билетам</i>
	Итого:		24		32			18	78

8. Обновление основной и дополнительной литературы (2020 г.)

В раздел 6. Учебно-методическое и информационное обеспечение дисциплины вносятся следующие изменения:

2. Дополнить раздел Основная литература

Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издатель-

ство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/450371>

Дополнить раздел **Дополнительная литература**

Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва: ИНФРА-М, 2020. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1018665>

9. В элемент рабочей программы **п.4 Образовательные технологии** вносятся следующие изменения:

В период временного приостановления посещения обучающимися помещений и территории РГГУ. для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств.

10. В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Состав программного обеспечения (ПО)

№п /п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное

4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «АЛТ Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное
17	Zoom	Zoom	лицензионное

Составитель:

К.т.н, доцент, А.С. Моляков