МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «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:
Безопасность автоматизированных систем
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва *2021*

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
№ 10 от 20.05.2021 г.

ОГЛАВЛЕНИЕ

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:

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-3 *Способен управлять защитой информации в автоматизированных системах*	*ПК-3.1* *Знает основные методы управления защитой информации, информационные ресурсы автоматизированных систем, подлежащие защите; основные угрозы безопасности информации, модели нарушителя в автоматизированных системах*	*Знать: основные методы управления защитой информации, информационные ресурсы и базовой модели нарушителя ФСТЭК РФ*
	ПК-3.2 *Умеет разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; классифицировать и оценивать угрозы безопасности информации; оценивать информационные риски в автоматизированных системах*	*Уметь: классифицировать угрозы, разрабатывать технические предложения по совершенствованию системы управления защиты информации автоматизированных систем, проводить аудит с целью оценки рисков*
	ПК-3.3 *Владеет навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе*	*Владеть: навыками по разработке организационно-технических по защите информации, приемы и принципы в соответствие с ЕСКД, ЕСПД и другими нормативно-правовыми документами*
ПК-10 *Способен проводить анализ информационной безопасности объектов и систем на*	*ПК-10.1* *Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные*	*Знать нормативные правовые документы в области защиты информации, основные проектные решения, средства и методы защиты информации*

соответствие требованиям стандартов в области информационной безопасности	*стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации*	*от несанкционированного доступа.*
	ПК-10.2 *Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации*	*Уметь применять комплексный подход к обеспечению информационной безопасности объекта защиты, анализировать защищаемые активы в зависимости от специфики от системы обработки информации ограниченного доступа в соответствии с законом "О техническом регулировании"*
	ПК-10.3 *Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации*	*Владеть навыками по реализации политик информационной безопасности и технологических проектов в области ИБ*

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Техническое регулирование в области защиты информации» относится к факультативным дисциплинам по выбору части, формируемой участниками образовательных отношений 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: «Защита информации от вредоносного программного обеспечения", "Безопасность программного обеспечения автоматизированных систем", "Информационная безопасность телекоммуникационных систем".

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет 2 з.е., 76 ч., в том числе контактная работа обучающихся с преподавателем 40 ч., самостоятельная работа обучающихся 36 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	*Требования федерального закона о техническом регулировании*	**2**	**4**					**10**	Опрос.
2	*Лицензирование деятельности предприятий в области защиты информации*	**2**	**8**		**8**			**8**	Опрос. Оценка выполнения практических заданий
3	*Сертификация средств защиты информации*	**2**	**8**		**6**			**10**	Опрос. Оценка выполнения практических заданий
4	*Аттестация объектов информатизации по требованиям безопасности информации*	**2**	**4**		**8**			**8**	Опрос. Оценка выполнения практических заданий
	Зачет	**2**			**2**				зачет по билетам
	итого:		**16**		**24**			**36**	

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 регулиро-

		вание 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[1]

Образовательные технологии

№ п/п	**Наименование раздела**	**Виды учебных занятий**	**Образовательные технологии**
1	**2**	**3**	**4**
1	*Требования федерального закона о техническом регулировании*	*Лекция 1.1* *Лекция 1.2* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Работа с литературой*
2	*Лицензирование деятельности предприятий в об-*	*Лекция 2.1* *Лекция 2.2*	*Традиционная лекция с использованием презентаций*

[1] В разделе указываются образовательные технологии, используемые при реализации различных видов учебных занятий для наиболее эффективного освоения дисциплины. При проведении учебных занятий обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин *(модулей)* в форме курсов, составленных на основе результатов научных исследований, в том числе с учётом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей (п.34. Приказ №301).

	ласти защиты информации	*Лекция 2.3* *Лекция 2.4* *Практическое занятие 1* *Самостоятельная работа*	 *Выполнение заданий* *Работа с литературой*
3	*Сертификация средств защиты информации*	*Лекция 3.1* *Лекция 3.2* *Лекция 3.3* *Лекция 3.4* *Практическое занятие 2* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Выполнение заданий* *Работа с литературой*
4	*Аттестация объектов информатизации по требованиям безопасности информации*	*Лекция 4.1* *Лекция 4.2* *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* *- практическое занятие № 2* *- практическое занятие № 3*	 *10 баллов* *25 баллов* *25 баллов*	 *10 баллов* *25 баллов* *25 баллов*
Промежуточная аттестация *зачет*		*40 баллов*
Итого за дисциплину *зачет*		*100 баллов*

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	***Контролируемые разделы дисциплины***	***Код контролируемой компетенции***	***Наименование оценочного средства***
1.	Темы 1 – 4	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1	Опрос
2.	Практические занятия 1 – 3	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1	План практических занятий

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»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. 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. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	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. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	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. 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. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ не зачтено	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. 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. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

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

5.4. Вопросы к зачету - *проверка сформированности компетенций ПК-10, ПК-3*

Контрольные вопросы	Реализуемые компетенции
1. Какие отношения регулирует Федеральный закон «О техническом регулировании»?	ПК-10.3, ПК-10.2, ПК-10.1
2. На какие объекты распространяется сфера применения Федерального закона «О техническом регулировании»?	ПК-10.3, ПК-10.2, ПК-10.1
3. Как называется документ, удостоверяющий соответствие объектов требованиям технических регламентов, положениям стандартов или условиям договоров?	ПК-10.3, ПК-10.2, ПК-10.1
4. Какое определение соответствует понятию «оценка соответствия» (в соответствии с Федеральным законом «О техническом регулирова-	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1

нии»)?	
5. Какое определение соответствует понятию «сертификация» (в соответствии с Федеральным законом «О техническом регулировании»)?	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1
6. Что в соответствии с Федеральным законом «О техническом регулировании» представляет собой система сертификации?	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1
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?	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1
8. Как в соответствии с Федеральным законом «О техническом регулировании» следует назвать прямое или косвенное определение соблюдения требований, предъявляемых к объекту?	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1
9. Как в соответствии с Федеральным законом «О техническом регулировании» следует назвать документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов или условиям договоров?	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1
10. Система лицензирования на право проведения работ и оказания услуг в области защиты информации с ограниченным доступом.	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1
11. Нормативные документы, определяющие порядок лицензирования в области защиты конфиденциальной информации.	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1
12. Какие лицензии выдаются ФСТЭК России?	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1
13. Какие лицензии выдаются ФСБ России?	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1
14. Различаются ли между собой лицензии ФСБ и ФСТЭК на деятельность по разработке/производству средств защиты конфиденциальной информации?	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1
15. Условия лицензирования деятельности по защите конфиденциальной информации. Виды деятельности по ТЗКИ подлежащие лицензированию.	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1
16. Общие принципы лицензирования в области защиты конфиденциальной информации.	ПК-10.3, ПК-10.2, ПК-10.1
17. Лицензионные требования для получения лицензии на деятельность в области технической защиты конфиденциальной информации.	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1
18. Перечень документов, представляемых для получения лицензий в области защиты конфиденциальной информации.	ПК-10.3, ПК-10.2, ПК-10
19. Система сертификации средств защиты информации.	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1
20. Цели системы сертификации средств защиты информации.	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1

21. Нормативные документы определяющие порядок сертификации средств защиты информации на соответствие требованиям безопасности информации.	ПК-10.3, ПК-10.2, ПК-10.1
22. Структура средств защиты информации, подлежащих сертификации.	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1
23. Аттестация объектов информатизации на соответствие требованиям безопасности информации.	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1
24. Объекты, подлежащие аттестации.	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1
25. Общие требования по аттестации объектов информатизации, предназначенных для обработки конфиденциальной информации.	ПК-10.3, ПК-10.2, ПК-10.1
26. Порядок проведения аттестации объектов информатизации.	ПК-10.3, ПК-10.2, ПК-10.1, ПК-3.3, ПК-3.2, ПК- 3.1

Примерные задания для тестирования- проверка сформированности компетенций ПК-10, ПК-3

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-predsedatelya-gostekhkomissii-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-predsedatelya-gostekhkomissii-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-predsedatelya-gostekhkomissii-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-predsedatelya-gostekhkomissii-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 (ред. от 19.07.2018). [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 (ред. от 03.07.2018). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_ LAW_10699/, свободный. – Загл. с экрана.

Литература

Основная

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

2. 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

3. 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

4. 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

5. 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

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

1. ОХРАНА.ru. Российское СМИ о безопасности. [Электронный ресурс] : Режим доступа : https://oxpaha.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) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должны быть установлены следующее ПО:

№ п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2) для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное
3	Microsoft Share Point 2010	Microsoft	лицензионное
4	Microsoft Office 2013	Microsoft	лицензионное
5	Windows 10 Pro	Microsoft	лицензионное
6	Kaspersky Endpoint Security	Kaspersky	Лицензионное
7	Vmware Player 15.5	VMWare	Режим доступа: https://www.vmware.com/products/ Демо-версия

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

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

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 зачёт 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, регулируемыми эргономическими партами СИ-1;
– компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий - проверка сформированности компетенций ПК-10, ПК-3

Практическое занятие 1 (8 ч.) «Лицензирование деятельности предприятий в области защиты информации» - проверка сформированности компетенций ПК-10, ПК-3
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 государственную 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 (6 ч.) «Сертификация средств защиты информации» - проверка сформированности компетенций ПК-10, ПК-3
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 (8 ч.) «Аттестация объектов информатизации по требованиям безопасности информации» - проверка сформированности компетенций ПК-10, ПК-3

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 «съемные 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, централь-

ное 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.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Техническое регулирование в области защиты информации» реализуется на факультете Информационных систем и безопасности для студентов 1-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – Безопасность автоматизированных систем) 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:

- ПК-3 -Способен управлять защитой информации в автоматизированных системах
- ПК-3.1 -Знает основные методы управления защитой информации, информационные ресурсы автоматизированных систем, подлежащие защите; основные угрозы безопасности информации, модели нарушителя в автоматизированных системах
- ПК-3.2 -Умеет разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; классифицировать и оценивать угрозы безопасности информации; оценивать информационные риски в автоматизированных системах
- ПК-3.3 -Владеет навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе
- ПК-10 -Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
- ПК-10.1 -Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
- ПК-10.2 -Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации
- ПК-10.3 -Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации

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 применять комплексный подход к обеспечению информационной безопасности объекта защиты, анализировать защищаемые активы в зависимости от специфики от системы обработки информации ограниченного доступа , пользоваться нормативными документами по защите информации; применять отечественные стандарты в области компьютерной безопасности в соответствии с законом “О техническом регулировании”.
Владеть навыками работы с нормативными правовыми актами.
По дисциплине предусмотрена промежуточная аттестация в форме зачета.

Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.

Приложение 2

УТВЕРЖДЕНО
Протокол заседания кафедры
№_____ от_____

ЛИСТ ИЗМЕНЕНИЙ

в рабочей программе дисциплины
Техническое регулирование в области защиты информации

по направлению подготовки 10.03.01 Информационная безопасность

на 20__/20__ учебный год

1. В _____ вносятся следующие изменения:
(элемент рабочей программы)
1.1. ……..;
1.2. ……...;
…
1.9. …… .

2. В _____ вносятся следующие изменения:
(элемент рабочей программы)
2.1. ……..;
2.2. ……...;
…
2.9. …… .

3. В _____ вносятся следующие изменения:
(элемент рабочей программы)
3.1. ……..;
3.2. ……...;
…
3.9. …… .

Составитель подпись расшифровка подписи
дата