МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
"28" апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Стандартизация и сертификация в информационной безопасности»

Направление подготовки
10.04.01 Информационная безопасность

Профиль
Системы управления информационной безопасностью

Квалификация
Магистр по направлению
«Информационная безопасность»

Формы обучения
Очная

Москва, 2022 г.

Разработчики:

Доцент кафедры «Информационная безопасность»,
к.т.н, доцент:

/ И.В. Калуцкий /

Доцент кафедры «Информационная безопасность»,
к.т.н., доцент, MBA

/ К.В. Пителинский /

Согласовано:

И.о. заведующего кафедрой «Информационная безопасность»,

А.Ю. Гневшев

Руководитель образовательной программы
Доцент. к.т.н.

/С.А. Кесель/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Стандартизация и сертификация в информационной безопасности» следует отнести:

- Развитие делового и логического мышления студентов, ознакомление студентов с основами теории, необходимыми для решения прикладных задач по метрологической и сертификационной деятельности средств информационной безопасности.

К **основным задачам** освоения дисциплины «Стандартизация и сертификация в информационной безопасности» следует отнести:

- Изучение основных вопросов современной теории подготовки нормативных документов;
- Изучение основ стандартизации;
- Воспитание делового и логического мышления на примере решения задач создания и принципов организации в области применения стандартов.

В результате освоения дисциплины «Стандартизация и сертификация в информационной безопасности» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	**Индикаторы достижения компетенции**
ПК-3. Способен проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	**знать:** • состав, характеристики и функциональные возможности систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; **уметь:** • проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; **владеть:** • средствами обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов
ПК-10. Способен проводить аттестацию объектов информатизации по требованиям безопасности информации	**знать:** • как проводить аттестацию объектов информатизации по требованиям безопасности информации; **уметь:** • проводить аттестацию объектов информатизации по требованиям безопасности информации; **владеть:** • принципами проведения аттестации объектов информатизации по требованиям безопасности информации

ПК-14. Способен организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами	**знать:** • как организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами; **уметь:** • организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами; **владеть:** • принципами организации работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами

2 Место дисциплины в структуре образовательной программы

Дисциплина «Стандартизация и сертификация в информационной безопасности» относится к числу профессиональных учебных дисциплин обязательной части цикла (Б1.1) основной образовательной программы магистра (Б1.1.4).

Дисциплина «Стандартизация и сертификация в информационной безопасности» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП в обязательной части цикла (Б1.1):

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Организационное и правовое обеспечение информационной безопасности».

Дисциплина обеспечивает изучение дисциплин «Аудит систем управления информационной безопасностью», «Управление информационной безопасностью» и подготовку выпускной квалификационной работы.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, т.е. **108** академических часов (лекции – 18 часов, лабораторные занятия – 36 часов, самостоятельная работа студентов – 54 часа, форма контроля – диф. зачет) в 1 семестре.

Структура и содержание дисциплины «Стандартизация и сертификация в информационной безопасности» по срокам и видам работы отражены в приложении.

3.1 Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
1	**Аудиторные занятия**	**54**	1	1-18
	В том числе:			
1.1	Лекции	18	1	-
1.2	Семинарские/практические занятия	-	-	-
1.3	Лабораторные занятия	36	1	1-18
2	**Самостоятельная работа**	**54**	1	1-18
3	**Промежуточная аттестация**		1	6-17
	Зачет/диф. зачет/экзамен	диф. зачет	1	По расписанию
	Итого	**108**		

3.2 Тематический план изучения дисциплины

(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1.1	Тема 1. Понятие безопасности информации.	12	2	-	4	-	6
1.2	Тема 2. Международные российские стандарты по защите информации их взаимосвязь и различия.	12	2	-	4	-	6
1.3	Тема 3. Особенности процесса стандартизации и стандарты безопасности в сети Интернет.	12	2	-	4	-	6
1.4	Тема 4. Особенности государственных стандартов программных продуктов.	12	2	-	4	-	6
1.5	Тема 5. Государственные стандарты: общие положения.	12	2	-	4	-	6
1.6	Тема 6. Руководящий документ Гостехкоммиссии Межсетевые экраны.	12	2	-	4	-	6
1.7	Тема 7. Основы сертификации (на примере средств защиты информации).	12	2	-	4	-	6

1.8	Тема 8. Сертификация на соответствие требованиям по безопасности информации.	12	2	-	4	-	6
1.9	Тема 9. Системы сертификации средств защиты информации требованиям безопасности информации.	12	2	-	4	-	6
	Итого	**108**	**18**		**36**		**54**

3.3 Содержание дисциплины

3.3.1 Лекционные занятия

Тема 1. Понятие безопасности информации.

Тема 2. Международные российские стандарты по защите информации их взаимосвязь и различия.

Тема 3. Особенности процесса стандартизации и стандарты безопасности в сети Интернет.

Тема 4. Особенности государственных стандартов программных продуктов.

Тема 5. Государственные стандарты: общие положения.

Тема 6. Руководящий документ Гостехкоммиссии Межсетевые экраны.

Тема 7. Основы сертификации (на примере средств защиты информации).

Тема 8. Сертификация на соответствие требованиям по безопасности информации.

Тема 9. Системы сертификации средств защиты информации требованиям безопасности информации.

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Лабораторные занятия

Тема 1. Понятие безопасности информации
Лабораторная работа 1. Понятие безопасности информации
Лабораторная работа 2. Понятие безопасности информации

Тема 2. Международные и российские стандарты по защите информации.
Лабораторная работа 1. Международные и российские стандарты по защите информации.
Лабораторная работа 2. Международные российские стандарты по защите информации: их взаимосвязь и различия.

Тема 3. Особенности процесса стандартизации и стандарты безопасности в сети Интернет
Лабораторная работа 1. Особенности процесса стандартизации.
Лабораторная работа 2. Стандарты безопасности в сети Интернет.

Тема 4. Особенности государственных стандартов программных продуктов

Лабораторная работа 1. Особенности государственных стандартов программных продуктов

Лабораторная работа 2. Особенности государственных стандартов программных продуктов

Тема 5. Государственные стандарты: общие положения

Лабораторная работа 1. Государственные стандарты: общие положения

Лабораторная работа 2. Государственные стандарты: общие положения

Тема 6. Руководящий документ Гостехкоммиссии Межсетевые экраны.

Лабораторная работа 1. Руководящий документ Гостехкоммиссии Межсетевые экраны.

Лабораторная работа 2. Руководящий документ Гостехкоммиссии Межсетевые экраны.

Тема 7. Основы сертификации (на примере средств защиты информации)

Лабораторная работа 1. Основы сертификации (на примере средств защиты информации).

Лабораторная работа 2. Основы сертификации (на примере средств защиты информации).

Тема 8. Сертификация на соответствие требованиям по безопасности информации.

Лабораторная работа 1. Сертификация на соответствие требованиям по безопасности информации.

Лабораторная работа 2. Сертификация на соответствие требованиям по безопасности информации.

Тема 9. Системы сертификации средств защиты информации требованиям безопасности информации.

Лабораторная работа 1. Системы сертификации средств защиты информации требованиям безопасности информации

Лабораторная работа 2. Системы сертификации средств защиты информации требованиям безопасности информации

3.5 Тематика курсовых проектов (курсовых работ)

По дисциплине «Стандартизация и сертификация в информационной безопасности» не предусмотрен курсовой проект.

4 Учебно-методическое и информационное обеспечение

4.1. Нормативные документы и ГОСТы

1. ГОСТ Р 59503-2021/ISO/IEC TR 27016:2014. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Экономика информационной безопасности организации. – М., 2021

5 Методический документ «Меры защиты информации в государственных информационных системах» (утв. ФСТЭК РФ 11 февраля 2014 г.) [Электронный ресурс] – URL: https://it-security.admin-smolensk.ru/zakonodatelstvo/normativnye-dokumenty-fstek-rossii/metodicheskij-dokument-mery-zaschity-informacii-v-gosudarstvennyh-informacionnyh-sistemah-/
6 ГОСТ Р 59712–2022 «Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты».
7 ГОСТ 7.1–84. Библиографическое описание документа. Общие требования и правила составления. – М., 1985
8 Международные стандарты информационной безопасности [Электронный ресурс] – URL: http://ypn.ru/177/international-standards-of-information-technologies-security/2/
9 ГОСТ Р ИСО/МЭК 27000-2021. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. [Электронный ресурс] – URL: https://docs.cntd.ru/document/1200179675
10 Федеральный закон № 152-ФЗ от 27.07.2006 «О персональных данных»

4.2. Основная литература

1. Мандрица, И. В. Управление проектами по информационной безопасности и экономика защиты информации. Часть 1 / И. В. Мандрица, В. И. Петренко, О. В. Мандрица. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-45723-6. — Текст : электронный // Лань : электронно-библиотечная система. — [Электронный ресурс] URL: https://e.lanbook.com/book/311825.
2. Петренко В.И., Мандрица И.В. Защита персональных данных в информационных системах. Практикум. –М. Лань, 2022 - 108 с. [Электронный ресурс] – URL: https://lanbook.com/catalog/informatika/zashchita-personalnykh-dannykh-v-informatsionnykh-sistemakh-praktikum/
3. Кудашкин Я. В. Правовое обеспечение безопасности обработки персональных данных в сети интернет. Автореф. дис. на соискание уч. ст. к.ю.н. Специальность: 12.00.13 –Информационное право. Москва – 2019. [Электронный ресурс] – URL: https://istina.msu.ru/download/212806666/1hiKtk:UrCunoF4PcIPFMt1qAIZRF_dTmA/
4. Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Материалы X Межрегиональной научно-практической конференции / под ред. О.М. Голембиовской, М.Ю. Рытова. – Брянск: БГТУ, 2018. – 187 с. [Электронный ресурс] – URL: https://www.tu-bryansk.ru/upload/medialibrary/8d4/Konf_IB_2018.pdf

4.3. Дополнительная литература

1. Лапина М. А. Защита персональных данных в информационных системах / М. А. Лапина, М. В. Песков. – Ставрополь: Изд-во СКФУ, 2014. – 199 с.

[Электронный ресурс] – URL: https://www.ncfu.ru/export/uploads/imported-from-dle/op/doclinks2015/Metod_UPPDN_10.05.03_19.05.15.pdf

2. Комплексные системы защиты информации предприятия: учебное пособие / В.Т. Еременко, М.Ю. Рытов, О.М. Голембиовская, П.Н. Рязанцев. – Орел: ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», 2016. –116 с. [Электронный ресурс] – URL: https://studfile.net/preview/16707511/page:12/#16707511
3. Параскевов А.В., Левченко А.В., Кухоль Ю.А. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом //Научный журнал КубГАУ. №110(06), 2015 года –С. 1-28. [Электронный ресурс] – URL: http://ej.kubagro.ru/2015/06/pdf/58.pdf
4. Такидзе Д.Т. Защита персональных данных в России. // Вестник магистратуры. 2021 №5-4 (116) с. 108-111. [Электронный ресурс] – URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-v-rossii
5. Виссия, Х. Э. Принятие решений в информационном обществе : учебное пособие / Х. Э. Виссия, В. В. Краснопрошин, А. Н. Вальвачев. — Санкт-Петербург : Лань, 2022. — 228 с. — ISBN 978-5-8114-3747-4. — Текст : электронный // Лань : электронно-библиотечная система. [Электронный ресурс] — URL: https://e.lanbook.com/book/206723.
6. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации – 2-е изд., испр. и доп. – СПб: Университет ИТМО, 2018. – 100 с. [Электронный ресурс] – URL: https://books.ifmo.ru/file/pdf/2372.pdf
7. Исаев А.С., Хлюпина Е.А. «Правовые основы организации защиты персональных данных» – СПб: НИУ ИТМО, 2014. – 106 с. [Электронный ресурс] – URL: https://books.ifmo.ru/file/pdf/1570.pdf
8. Кондрашов А.Э., Варламова Л.Н. Национальные стандарты РФ по различным аспектам защиты информации и информационной безопасности. [Электронный ресурс] – URL: https://www.top-personal.ru/officeworkissue.html?510

4.4. Электронные образовательные ресурсы

1. ЭОР разрабатывается
2. Московский Политех подключен к ЭБС: Юрайт, АйПиАр и Лань https://mospolytech.ru/obuchauschimsya/biblioteka/

4.5. Лицензионное и свободно распространяемое программное обеспечение

Программное обеспечение не предусмотрено

Полезные учебно-методические и информационные материалы представлены на сайтах:

1. ИТ-портал компании «Инфосистемы джет» -Режим доступа - http://www.jetinfo.ru
2. «Информационная безопасность», журнал – Режим доступа - http://itsec.ru/imag/

4.6. Современные профессиональные базы данных и информационные справочные системы

1. Банк данных угроз безопасности информации ФСТЭК России [Электронный ресурс] – URL: https://bdu.fstec.ru/
2. Лаборатория Сетевой Безопасности [Электронный ресурс] – URL: http://ypn.ru/

5. Материально-техническое обеспечение

Проведение лекционных и практических осуществляется в мультимедийной аудитории

6. Методические рекомендации

6.1. Методические рекомендации для преподавателя по организации обучения

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки магистр **10.04.01 Информационная безопасность.**

6.2. Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины «Стандартизация и сертификация в информационной безопасности» осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции. При рассмотрении учебного материалы рекомендуется делать акцент на структуру и взаимосвязь аспектов безопасности - методологии, информационного обеспечения, организации, экономических методах, кадрового обеспечения и нормативно-правовой базы. Полезно также сосредоточить внимание студентов на анализе угроз и оценке рисков информационной безопасности, оценке прямого и косвенного ущерба от риска потери информации, определении упущенной выгоды предприятия, методах оценки целесообразности и эффективности затрат на систему информационной безопасности

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к зачету, а также самостоятельно изучают отдельные темы учебной программы. В тематическом плане указанные темы выделены курсивом и снабжены пометкой «самостоятельно». Преподаватель направляет самостоятельную работу студентов, отвечает на возникающие вопросы, дает рекомендации по методике изучения тем.

Практические занятия проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ. Практические занятия проводятся по теоретическим и проблемным вопросам ИБ. Практическое занятие предполагает творческие дискуссии, активный обмен мнениями по поставленным вопросам, заслушивание и обсуждение докладов по предложенным преподавателем темам.

Важным обстоятельством является привлечение внимания студентов к обсуждаемой проблеме, стимулирование интереса к ней и организация активного обсуждения, как структуры проблемы, так и составляющих ее наиболее актуальных тем. Для повышения эффективности проведения занятия требуется предварительная подготовка всех его участников. В этой связи рекомендуется заблаговременно (не менее, чем за неделю) оповестить студентов о теме занятия, дать перечень литературы по теме, назначить из числа студентов докладчиков и содокладчиков.

При проведении практического занятия преподаватель выполняет, в основном, функции ведущего - следит за регламентом времени, помогает уточнить формулировки, обобщает результаты дискуссии, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на практическом занятии учитывается при определении итоговой оценки его знаний по дисциплине на зачете.

Самостоятельная работа по дисциплине «Стандартизация и сертификация в информационной безопасности» предполагает: выполнение студентами домашних заданий. Домашние задания являются, как правило, продолжением практических занятий и содействуют овладению практическими навыками по основным разделам дисциплины. Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др.

При выдаче заданий на самостоятельную работу используется дифференцированный подход к студентам. Перед выполнением студентами самостоятельной внеаудиторной работы преподаватель проводит инструктаж по выполнению задания, который включает: цель здания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется в устной форме.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на диф. зачете в устной форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность умений;
- оформление материала в соответствии с требованиями.

7. Фонд оценочных средств

7.1. Методы контроля и оценивания результатов обучения

Методика преподавания дисциплины «Стандартизация и сертификация в информационной безопасности» и реализация компетентностного подхода в изложении и

восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков, обучающихся:

- обсуждение и защита рефератов по дисциплине;
- подготовка, представление и обсуждение презентаций по темам рефератов на семинарских занятиях;
- использование интерактивных форм текущего контроля в форме тестирования;

Удельный вес занятий, проводимых в интерактивных формах, определен главной целью образовательной программы, особенностью контингента обучающихся, содержанием дисциплины «Стандартизация и сертификация в информационной безопасности» и в целом по дисциплине составляет 25% аудиторных занятий. Занятия лекционного типа составляют 30% от объема аудиторных занятий.

7.2. Шкала и критерии оценивания результатов обучения

7.2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ПК-3	Способен проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов
ПК-10	Способен проводить аттестацию объектов информатизации по требованиям безопасности информации
ПК-14	Способен организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

7.2.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

При этом индикаторы освоения компетенций согласно ОПОП реализуются вариативно преподавателем, ведущим данную дисциплину

ПК-3 Способен проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: состав, характеристики и функциональные возможности систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;	Обучающийся демонстрирует полное отсутствие знаний об составе, характеристиках и функциональных возможностях систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	Обучающийся демонстрирует неполное знание об составе, характеристиках и функциональных возможностях систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	Обучающийся демонстрирует частичное знание об составе, характеристиках и функциональных возможностях систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	Обучающийся демонстрирует полное знание об составе, характеристиках и функциональных возможностях систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов
уметь: проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	Обучающийся не умеет проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	Обучающийся демонстрирует неполное умение проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	Обучающийся демонстрирует частичное умение проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	Обучающийся демонстрирует полное умение проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов

владеть: средствами обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	Обучающийся не владеет средствами обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	Обучающийся не полностью владеет средствами обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	Обучающийся частично владеет средствами обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	Обучающийся в полном объеме владеет средствами обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов
ПК-10 Способен проводить аттестацию объектов информатизации по требованиям безопасности информации				
знать: как проводить аттестацию объектов информатизации по требованиям безопасности информации	Обучающийся демонстрирует полное отсутствие знаний как проводить аттестацию объектов информатизации по требованиям безопасности информации	Обучающийся демонстрирует неполное знание как проводить аттестацию объектов информатизации по требованиям безопасности информации	Обучающийся демонстрирует частичное знание как проводить аттестацию объектов информатизации по требованиям безопасности информации	Обучающийся демонстрирует полное знание как проводить аттестацию объектов информатизации по требованиям безопасности информации
уметь: проводить аттестацию объектов информатизации по требованиям безопасности информации	Обучающийся не умеет проводить аттестацию объектов информатизации по требованиям безопасности информации	Обучающийся демонстрирует неполное умение проводить аттестацию объектов информатизации по требованиям безопасности информации	Обучающийся демонстрирует частичное умение проводить аттестацию объектов информатизации по требованиям безопасности информации	Обучающийся демонстрирует полное умение проводить аттестацию объектов информатизации по требованиям безопасности информации
владеть: принципами проведения аттестации объектов информатизации по требованиям безопасности информации	Обучающийся не владеет принципами проведения аттестации объектов информатизации по требованиям безопасности информации	Обучающийся в неполном объеме владеет принципами проведения аттестации объектов информатизации по требованиям безопасности информации	Обучающийся частично владеет принципами проведения аттестации объектов информатизации по требованиям безопасности информации	Обучающийся в полном объеме владеет принципами проведения аттестации объектов информатизации по требованиям безопасности информации

ПК-14 Способен организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России				
знать: как организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами	Обучающийся демонстрирует полное отсутствие знаний как организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами	Обучающийся демонстрирует неполное знание как организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами	Обучающийся демонстрирует частичное знание как организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами	Обучающийся демонстрирует полное знание как организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами
уметь: организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами	Обучающийся не организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами	Обучающийся демонстрирует неполное умение организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами	Обучающийся демонстрирует частичное умение организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами	Обучающийся демонстрирует полное умение организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами

владеть: принципами организации работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами	Обучающийся не владеет принципами организации работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами	Обучающийся в неполном объеме владеет организации работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами	Обучающийся частично владеет принципами организации работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами	Обучающийся в полном объеме владеет принципами организации работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: диф. зачет

Промежуточная аттестация обучающихся в форме диф. зачета проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации. Присутствовал более чем на ¾ занятий
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки. Присутствовал более чем на ¾ занятий

Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность. Присутствовал более чем на ½ занятий
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации. Присутствовал менее чем на ½ занятий

7.3. Оценочные средства

7.3.1. Текущий контроль

Текущий контроль успеваемости студентов осуществляется в процессе проведения лабораторных работ и в процессе защиты презентаций рефератов, подготовленных в рамках самостоятельной работы по выбранной и согласованной теме.

Примерные темы презентаций (рефератов)

1. Модели для выявления и анализа возможностей, рисков и угроз.
2. Управление рисками в организации.
3. Модели для выявления и анализа возможностей, рисков и угроз.
4. Проблемы и перспективы использования внешних ИТ-услуг.
5. Нормативное регулирование построения и функционирование системы защиты информации. ISO/IES 27001-27005.
6. Аутсорсинг информационной безопасности — краткий обзор рынка
7. Нормативная совместимость. Нормативные акты корпоративного управления:
8. Методы оценки эффективности в сфере защиты информации от утечек.
9. Законодательные акты, регулирующие экономические вопросы защиты информации.
10. Система защиты информации и непрерывность бизнеса предприятия.
11. Особенности применения международных и российских нормативных актов и стандартов.
12. Стандартизация как научная дисциплины, её место в системе наук.
13. Методы исследования проблем стандартизации
14. Особенности стандартизации в сети Интернет.
15. Общие положения международных стандартов информации.
16. Стандарты в сфере информационной безопасности
17. Критерии и нормативы безопасности
18. Общие и специфические свойства ГОСТа Р ИСО \МЭК 15408-2002
19. Протоколы защищенности передачи данных SSL(TSL), SET IP v.6.
20. Унифицированные системы документации.
21. Государственные стандарты на документацию.
22. Протоколы стандартных способов шифрования.
23. Особенности российского рынка программных продуктов.
24. Регистрация документов и виды распорядительной документации.
25. Государственные стандарты общие положения.

7.3.2. Промежуточная аттестация

Промежуточная аттестация обучающихся в форме диф. Зачета проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Вопросы к зачету по дисциплине

1. Информационные ресурсы общества.
2. Модели для выявления и анализа возможностей, рисков и угроз.
3. Управление рисками в организации.
4. Модели для выявления и анализа возможностей, рисков и угроз.
5. Проблемы и перспективы использования внешних ИТ-услуг.
6. Нормативное регулирование построения и функционирование системы защиты информации. ISO/IES 27001-27005.
7. Аутсорсинг информационной безопасности — краткий обзор рынка
8. Нормативная совместимость. Нормативные акты корпоративного управления:
9. Федеральный закон «О персональных данных». Корпоративное управление.
10. Методы оценки эффективности в сфере защиты информации от утечек.
11. Законодательные акты, регулирующие экономические вопросы защиты информации.
12. Система защиты информации и непрерывность бизнеса предприятия.
13. Нормативное регулирование построения и функционирования системы защиты информации.
14. Особенности применения международных и российских нормативных актов и стандартов.
15. Предмет и задачи курса. Становление и развитие
16. Стандартизация как научная дисциплины, её место в системе наук.
17. Методы исследования проблем стандартизации ,Общенаучные и специальные методы
18. Особенности стандартизации в сети Интернет.
19. Понятие безопасности информации в соответствии с существующими ГОСТами.
20. Основные функции Руководящих разъяснительных документов по защите информации, их особенности.
21. Общие положение международных стандартов информации.
22. Стандарт ISO\IEC 15408-1999 .
23. ГОСТ Р ИСО\ МЭК 15408-2002
24. Критерии безопасности по ГОСТу ИСО\ МЭК 15408-2002
25. Понятие носителя документированной информации
26. Общие и специфические свойства ГОСТа Р ИСО \МЭК 15408-2002
27. Понятия «способ документирования», «средство документирования», «система документирования».
28. Понятия «информационная ёмкость», «информативность», «информационная плотность ».
29. Понятие носителя документированной информации .
30. Тождественность и отличие ГОСТ ИСО\ МЭК 15408-2002 от Международного его аналога.
31. Протоколы защищенности передачи данных SSL(TSL), SET IP v.6.
32. Сущность и особенности IPSes.

33. Унифицированные системы документации.
34. Государственные стандарты на документацию.
35. Описание стандарта SET .
36. Протоколы стандартных способов шифрования.
37. Особенности российского рынка программных продуктов.
38. Регистрация документов и виды распорядительной документации.
39. Государственные стандарты общие положения.
40. РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации.