МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

СОГЛАСОВАНО
Руководитель ОП

_____ Варлатая С.К.
(подпись) (ФИО)

УТВЕРЖДАЮ
Заведующий кафедрой

_____ Нефедев К.В.
(подпись) (ФИО.)
«__» _____ 20 _ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Проверка информационной защищенности на соответствие нормативным документам
Направление подготовки 10.03.01 Информационная безопасность
Организация и технологии защиты информации
Форма подготовки очная

курс 4 семестр 7
лекции 32 ч.
практические занятия 0 час.
лабораторные работы 32 час.
в том числе с использованием МАО лек. 32 /пр. 0 /лаб. 32 час.
всего часов аудиторной нагрузки 64 час.
в том числе с использованием МАО 0 час.
самостоятельная работа 44 час.
в том числе на подготовку к экзамену 9 час.
контрольные работы предусмотрены
курсовая работа / курсовой проект не предусмотрено
зачет 7 семестр
экзамен предусмотрен

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17.11.2020 № 1427.

Рабочая программа обсуждена на заседании кафедры Информационная безопасность протокол № 4 от «27» января 2021 г.

И.о. заведующего кафедрой Информационная безопасность, д.ф.-м.н., профессор Нефедев К.В.

Составитель

Владивосток
2021

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании кафедры/департамента:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой/Директор департамента _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры/департамента:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой/Директор департамента _____ _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании кафедры/департамента:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой/Директор департамента _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании кафедры/департамента:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой/Директор департамента _____ _____
(подпись) (И.О. Фамилия)

Цели и задачи освоения дисциплины:

Цель**:** показать способы проверки организации защиты на основе требований нормативного обеспечения информационной безопасности.

Задачи:

– установление организационных основ и принципов деятельности службы защиты информации;

– объяснение основ правового регулирования отношений в информационной сфере;

– изучение методологических и законодательных основ организации системы защиты информации;

– изучение основных аспектов практической деятельности по анализу защищенности информации.

В результате изучения данной дисциплины у обучающихся формируются следующие компетенции:

Наименование категории (группы) универсальных компетенций	**Код и наименование универсальной компетенции (результат освоения)**	**Код и наименование индикатора достижения компетенции**
Способен способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ПК-7	ПК-7.1 Демонстрирует знание методологий организации технологический процесс защиты информации ограниченного доступа
		ПК-7.2 Исследует нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю, составляет отчеты о проделанной работе, обзоры

		ПК-7.3 Разрабатывает технические отчеты о проделанной работе, обзоры, готовит публикации

Код и наименование индикатора достижения компетенции	**Наименование показателя оценивания (результата обучения по дисциплине)**
ПК-7.1 Демонстрирует знание методологий организации технологический процесс защиты информации ограниченного доступа	Знает: Информационные ресурсы, подлежащие защите и возможные пути реализации угроз безопасности
	Умеет: определять информационные ресурсы, подлежащие защите
	Владеет: Способностью анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-7.2 Исследует нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю, составляет отчеты о проделанной работе, обзоры	Знает: Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспортному контролю в данной области
	Умеет: пользоваться нормативными документами по защите информации
	Владеет: Навыками работы с нормативными правовыми актами
ПК-7.3 Разрабатывает технические отчеты о проделанной работе, обзоры, готовит публикации	Знает: Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспортному контролю в данной области
	Умеет: пользоваться нормативными и техническими документами по защите информации
	Владеет: Навыками работы с нормативными правовыми актами, способностью оформлять рабочую техническую документацию

Трудоемкость дисциплины и видов учебных занятий по дисциплине

Общая трудоемкость дисциплины составляет 4 зачётные единицы (144 академических часов).

(1 зачетная единица соответствует 36 академическим часам)

Видами учебных занятий и работы обучающегося по дисциплине являются:

Обозначение	Виды учебных занятий и работы обучающегося
Лр	Лабораторные работы
СР	Самостоятельная работа обучающегося в период теоретического обучения

Структура дисциплины:

Форма обучения – очная.

№	Наименование раздела дисциплины	Семестр	Количество часов по видам учебных занятий и работы обучающегося						Формы промежуточной аттестации
			Лек	Лаб	Пр	ОК	СР	Контроль	
1.	Раздел 1. Правовые основы использования организационных и технических средств защиты информации	7	6	9	-	-	12	-	УО-1; ПР-6
2.	Раздел 2. Построение комплексной системы защиты информации		7	5	-		12		УО-1; ПР-6
3.	Раздел 3. Управление и эксплуатация комплексной системы защиты информации		8	7	-		7		УО-1; ПР-6
4.	Раздел 4. Моделирование комплексных систем защиты информации		6	7	-		3		УО-1; ПР-6
5.	Раздел 5. Методика проверки защищенности объектов информатизации на соответствие требованиям нормативных документов		5	4	-		10		УО-1; ПР-6
	Итого:		32	32	-	-	44	-	

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел 1. Правовые основы использования организационных и

технических средств защиты информации (6 час.)

Тема 1. Назначение и структура правового обеспечения защиты информации (2 час.)

Предмет, задачи и содержание дисциплины. Терминология дисциплины. Структура курса. Методика аудиторной и самостоятельной работы студентов по изучению дисциплины. Законодательные и нормативные источники. Научная и учебная литература.

Тема 2. Законодательство РФ в области информационной безопасности (1 час.)

Понятие и структура информационной безопасности. Информационная сфера и информационная среда. Субъекты и объекты правоотношений в области информационной безопасности. Понятие и виды защищаемой информации по законодательству РФ. Отрасли законодательства, регламентирующие деятельность по защите информации. Перспективы развития законодательства в области информационной безопасности.

Тема 3. Правовые основы использования организационных и технических средств защиты информации (1 час.)

Классификация методов и средств защиты информации в различных сферах деятельности. Правовые основы организации и регулирования деятельности структурных подразделений предприятия, обеспечивающих его безопасность. Правовое регулирование использования технических средств защиты информации и противодействия угрозам информационной безопасности.

Тема 4. Лицензирование и сертификация в информационной сфере (1 час.)

Правовая основа системы лицензирования и сертификации в РФ. Виды деятельности в информационной сфере, подлежащие лицензированию. Лицензирование деятельности по защите информации. Объекты лицензирования в сфере защиты информации. Участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их

полномочия.

Понятие сертификации по российскому законодательству. Правовая регламентация сертификационной деятельности в области защиты информации. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия.

Лицензирование и сертификация в области международного информационного обмена

Тема 5. Система ответственности за нарушение норм защиты информации (1 час.)

Нормы ответственности за правонарушения в информационной сфере. Виды и условия применения правовых норм уголовной, гражданско-правовой, административной и дисциплинарной ответственности за разглашение защищаемой информации и невыполнение правил ее защиты. Понятие оперативно-розыскной деятельности и оперативно-розыскных мероприятий по законодательству РФ. Органы, уполномоченные на осуществление оперативно-розыскной деятельности. Система правовых актов, регулирующих проведение оперативно-розыскных мероприятий. Защита информации от неправомерных действий органов занимающихся оперативно-розыскной деятельностью. Защита коммерческой информации от неправомерных действий контролирующих и правоохранительных органов.

Раздел 2. Построение комплексной системы защиты информации (7 час.)

Тема 1. Виды обеспечения КСЗИ (2 час.)

Понятие видов обеспечения КСЗИ. Общая характеристика средств ЗИ. Организационное обеспечение процесса ЗИ. Правовое обеспечение процесса ЗИ. Программно-аппаратное обеспечение ЗИ. Инженерно-техническое обеспечение ЗИ. Методическое обеспечение процесса ЗИ. Математическое обеспечение процесса ЗИ.

Тема 2. Требования к автоматизированной системе в защищенном исполнении (4 час.)

Общие требования к автоматизированным системам в защищенном исполнении, функциональные требования, требования к эффективности, технические требования, экономические требования, требования к документации.

Тема 3. Методы подбора технических средств ЗИ (1 час.)

Общие понятия теории принятия технических решений, методы многокритериальных задач.

Раздел 3. Управление и эксплуатация комплексной системы защиты информации (8 час.)

Тема 1. Управление КСЗИ (4 час.)

Особенности управления КСЗИ, процесс принятия решений при управлении КСЗИ, планирование. Управление КСЗИ в условиях чрезвычайных ситуаций. Методы принятия решений в условиях чрезвычайных ситуаций, особенности чрезвычайной ситуации, методы борьбы с чрезвычайными ситуациями. Структура управления системой защиты информации предприятия.

Тема 2. Эксплуатация КСЗИ (4 час.)

Техническая эксплуатация КСЗИ. Организационные задачи. Поддержание работоспособности КСЗИ. Обеспечение технической эксплуатации. Получение технических средств. Разработка и внедрение политики информационной безопасности. Понятие информационной политики. Этапы разработки политики безопасности предприятия.

Раздел 4. Моделирование комплексных систем защиты информации (6 час.)

Тема 1. Методы и модели оценки уязвимостей (2 час.)

Угрозы безопасности информации. Основные каналы утечки информации. Выявление угроз безопасности автоматизированных систем.

Тема 2. Организационные основы и принципы деятельности службы защиты информации (2 час.)

Порядок создания службы защиты информации. Структура и

содержание положения о службе защиты информации. Основные принципы организации и деятельности службы защиты информации. Условия и факторы, влияющие на организацию работы службы защиты информации. Организация взаимодействия службы защиты информации и подразделений предприятия и соподчиненных внешних служб защиты информации.

Тема 3. Технология управления службой защиты информации (2 час.)

Состав и содержание управленческих функций. Технология управления службой защиты информации. Значение управленческих решений. Цели планирования. Виды планирования, их назначение. Содержание и структура планов. Технология планирования. Методы и формы контроля выполнения планов. Критерии эффективности службы защиты информации. Методы оценки качества службы защиты информации. Пути и способы повышения эффективности управления службой защиты информации.

Раздел 5. Методика проверки защищенности объектов информатизации на соответствие требованиям нормативных документов (5 час.)

Тема 1. Методы формирования требований по защите информации (2 час.)

Анализ нормативных документов. Оценка качества работы службы защиты информации.

Тема 2. Аналитическое обоснование необходимости создания СЗ СИ (2 час.)

Мероприятия по обеспечению режима секретности на стадии разработки системы информатизации. Оценка материальных, трудовых и финансовых затрат на внедрение СЗ.

Тема 3. Заключение по результатам проверки (1 час.)

Оценка эффективности работы комплексной системы защиты информации.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторные работы (32 час.)

Лабораторная работа №1. Выявление и анализ угроз безопасности информации в документообороте предприятия (12 час.)

Лабораторная работа №2. Подбор технических средств для обеспечения защиты информации (12 час.)

Лабораторная работа №3. Анализ рисков безопасности информации (6 час.)

Лабораторная работа №4. Проверка защищенности объекта на соответствие нормативным документам (2 час.)

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Проверка информационной защищенности на соответствие нормативным документам» включает в себя:

- план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;
- характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;
- требования к представлению и оформлению результатов самостоятельной работы.
-

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
	МОДУЛЬ 1. Основы	ПК-7.1 Демонстрирует	Знает: Информационные	ПР-1	1-8

1	правового регулирования отношений в информационной сфере	знание методологий организации технологический процесс защиты информации ограниченного доступа.	ресурсы, подлежащие защите и возможные пути реализации угроз безопасности		
			Умеет: определять информационные ресурсы, подлежащие защите	ПР-6	1-8
			Владеет: Способностью анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	ПР-7	1-8
2	МОДУЛЬ 2. Организационные основы и принципы деятельности службы защиты информации	ПК-7.2 Исследует нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю, составляет отчеты о проделанной работе, обзоры	Знает: Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспортному контролю в данной области	ПР-1	9-16
			Умеет: пользоваться нормативными документами по защите информации	ПР-6	9-16
			Владеет: Навыками работы с нормативными правовыми актами	ПР-7	9-16
3	МОДУЛЬ 3. Методика изучения основных аспектов практической деятельности по анализу защищенности информации	ПК-7.3 Разрабатывает технические отчеты о проделанной работе, обзоры, готовит публикации	Знает: Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы	ПР-4	17-24

			Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспортному контролю в данной области		
			Умеет: пользоваться нормативными и техническими документами по защите информации	ПР-6	17-24
			Владеет: Навыками работы с нормативными правовыми актами, способностью оформлять рабочую техническую документацию	ПР-7	17-24

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Информационная безопасность : учеб. пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2018. — 432 с. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие. - М.: Форум: Инфра-М, 2010. -592 с.

2. Дикарев В.И., Заренков В.А., Заренков Д.В., Койнаш Б.В. Защита объектов и информации от несанкционированного доступа/ Под ред. В.А. Заренкова.– СПб.: ОАО «Издательство Стройиздат СПб», 2010.– 320 с.

3. Комплексный технический контроль эффективности мер безопасности систем управления в органах внутренних дел: Учебн. пособие/ Под ред. А. А. Чекалина. В 2-х ч. Ч. 1. Теоретические основы технической разведки и комплексного технического контроля.– М.: Горячая линия-Телеком, 2012.– 206 с.

4. Рудометов Е.А., Рудометов В.Е. Электронные средства разведки

и защиты информации.– М.: ООО «Фирма «Издательство АСТ»; СПб.: ООО «Издательство ПОЛИГОН», 2010.– 224 с.

5. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия Телеком, 2010 – 311 с.

6. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных Системах – М.Ж Горячая линия-Телеком, 2011 – 156 с.

Дополнительная литература

1. Инженерно-техническая защита информации: программа дисциплины / А. Г. Лихоносов ; Московский гос. ун-т путей сообщ. (МИИТ), Юридический ин-т. - Москва: Юридический ин-т МИИТа, 2011. - 28 с.

2. Руководящие документы Гостехкомиссии (РД ГТК) и ГОСТы Российской Федерации по защите информации от 2010 г.

3. Корнеев И.К. Защита информации в офисе: Учебник/Гос. ун-т управления; И. К. Корнеев, Е.А. Степанов. -М.: Проспект,2011. -336 с.

Интернет-ресурсы

1. http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=4925 Пушкарев В.В. «Защита информационных процессов в компьютерных системах», Издательство: ТУСУР (Томский государственный университет систем управления и радиоэлектроники), Год: 2012, Объем: 131 стр.

2. http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=4959 Титов А.А. «Инженерно-техническая защита информации» , Учебное пособие, Издательство: ТУСУР (Томский государственный университет систем управления и радиоэлектроники), Год:2010, Объем: 197 стр.

3. https://biblio-online.ru/viewer/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-413158#page/ Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры / под ред. Т.А. Поляковой, А.А. Стрельцова — М .: Издательство Юрайт, 2018 — 325 с.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Проверка информационной защищенности на соответствие нормативным документам», составляет 64 часа. На самостоятельную работу – 44 часа. При этом аудиторная нагрузка состоит из 32 лекционных часов и 32 часов лабораторных работ.

Обучающийся получает теоретические знания на лекциях. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Подготовка к лабораторным работам предполагает повторение лекционного материала. В результате студент должен быть готов к выполнению лабораторных работ. Основной лабораторных работ является выполнение заданий с последующим предоставлением отчета о выполнении.

В рамках указанной дисциплины итоговой формы аттестации является экзамен. Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов по практическим занятиям и лабораторных работ.

Методические указания для написания реферата

Прежде всего, нужно выбрать тему реферата и подобрать соответствующую литературу. После ознакомления с литературой следует приступить к составлению плана. План реферата должен состоять из названия (темы), введения, основной части, заключения и списка использованной литературы (3-5 работ). Основная часть, как правило, разбивается на дополнительные вопросы (не более 3-4).

Объём реферата должен быть не менее 12 машинописных страниц.

Во введении описывается цель, задачи работы, а также раскрываются

смысл и значение основных понятий выбранной темы, область их применения.

В основной части необходимо:

а) ещё раз уточнить тему работы;

б) разбить основную часть работы на дополнительные вопросы;

в) дать ответы на эти вопросы, получив вспомогательные результаты. На их основе дать ответ на основной вопрос. Допускаются ссылки на дополнительную литературу.

В заключении подводятся итоги исследования. Заключение не должно быть большим по объёму.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для обеспечения данной дисциплины необходима аудитория, оснащенная презентационной техникой, компьютерный класс с программным обеспечением и возможностью использования Интернет-ресурсов, учебная лаборатория, оборудованная экспериментальными стендами и соответствующими измерительными приборами, учебные и методические пособия (учебники, программы, сборники упражнений и т.д.), расходные материалы (бумага, картридж).

Учебно-методическое обеспечение самостоятельной работы обучающихся

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-18 неделя обучения	Подготовка лабораторных работ.	9	Отчет о выполнении
2	Сессия	Подготовка к экзамену	6	Экзамен

Подготовка отчетов к лабораторным работам предполагает повторение лекционного материала и выполнение лабораторных работ. В результате студент должен представить отчеты о проделанной работе.

Методические рекомендации к работе с литературными источниками

В процессе подготовки к практическим занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме практического занятия, что позволяет студентам проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

Критерии оценки выполнения самостоятельной работы

Контроль самостоятельной работы студентов предусматривает:

- соотнесение содержания контроля с целями обучения;
- объективность контроля;
- валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить);
- дифференциацию контрольно-измерительных материалов.

Формы контроля самостоятельной работы

1. Просмотр и проверка выполнения самостоятельной работы преподавателем.

2. Самопроверка, взаимопроверка выполненного задания в группе.

3. Обсуждение результатов выполненной работы на занятии.

Критерии оценки результатов самостоятельной работы

Критериями оценок результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентов учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- умения студента активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями;
- умение ориентироваться в потоке информации, выделять главное;
- умение четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- умение показать, проанализировать альтернативные возможности, варианты действий;
- умение сформировать свою позицию, оценку и аргументировать ее.

Критерии оценки выполнения контрольных заданий для самостоятельной работы

Процент правильных ответов	**Оценка**
От 95% до 100%	отлично
От 76% до 95%	хорошо

От 61% до 75%	удовлетворительно
Менее 61 %	неудовлетворительно

Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов по лабораторным работам.

Фонд оценочных средств

Паспорт фонда оценочных средств

Код и наименование индикатора достижения компетенции	**Наименование показателя оценивания (результата обучения по дисциплине)**
ПК-7.1 Демонстрирует знание методологий организации технологический процесс защиты информации ограниченного доступа	Знает: Информационные ресурсы, подлежащие защите и возможные пути реализации угроз безопасности
	Умеет: определять информационные ресурсы, подлежащие защите
	Владеет: Способностью анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-7.2 Исследует нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю, составляет отчеты о проделанной работе, обзоры	Знает: Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспортному контролю в данной области
	Умеет: пользоваться нормативными документами по защите информации
	Владеет: Навыками работы с нормативными правовыми актами
ПК-7.3 Разрабатывает технические отчеты о проделанной работе, обзоры, готовит публикации	Знает: Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспортному контролю в данной области
	Умеет: пользоваться нормативными и техническими документами по защите информации
	Владеет: Навыками работы с нормативными правовыми актами, способностью оформлять рабочую техническую документацию

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	МОДУЛЬ 1. Основы правового регулирования отношений в информационной сфере	ПК-7.1 Демонстрирует знание методологий организации технологический процесс защиты информации ограниченного доступа.	Знает: Информационные ресурсы, подлежащие защите и возможные пути реализации угроз безопасности	ПР-1	1-8
			Умеет: определять информационные ресурсы, подлежащие защите	ПР-6	1-8
			Владеет: Способностью анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	ПР-7	1-8
2	МОДУЛЬ 2. Организационные основы и принципы деятельности службы защиты информации	ПК-7.2 Исследует нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю, составляет отчеты о проделанной работе, обзоры	Знает: Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспортному контролю в данной области	ПР-1	9-16
			Умеет: пользоваться нормативными документами по защите информации	ПР-6	9-16
			Владеет: Навыками работы с нормативными правовыми актами	ПР-7	9-16
	МОДУЛЬ 3. Методика изучения основных аспектов	ПК-7.3 Разрабатывает	Знает: Основные нормативные правовые акты в	ПР-4	17-24

3	практической деятельности по анализу защищенности информации	технические отчеты о проделанной работе, обзоры, готовит публикации	области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспортному контролю в данной области		
			Умеет: пользоваться нормативными и техническими документами по защите информации	ПР-6	17-24
			Владеет: Навыками работы с нормативными правовыми актами, способностью оформлять рабочую техническую документацию	ПР-7	17-24

Оценочные средства для промежуточной аттестации
Список вопросов на экзамен

1. Актуальность проблемы обеспечения безопасности информации.
2. Основные причины обострения проблемы обеспечения безопасности информационных технологий.
3. Конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты автоматизированных систем.
4. Анализ угроз информационной безопасности.
5. Методы и средства обеспечения информационной безопасности.
6. Методы нарушения конфиденциальности, целостности и доступности информации.
7. Причины, виды, каналы утечки и искажения информации.
8. Источники и характеристика основных угроз безопасности.
9. Политика безопасности.
10. Основные модели, применяемые при построении систем обеспечения информационной безопасности.
11. Основные положения и концепция построения общих критериев защищенности информационных технологий.
12. Управление информационной безопасностью системы.
13. Законодательство о создании и применении информационных технологий и средств их обеспечения.
14. Понятийный аппарат в области обеспечения информационной безопасности на предприятии.
15. Современные требования к средствам обеспечения безопасности.
16. Методологические основы организации комплексной системы защиты информации.
17. Влияние организационно-правовой формы предприятия на особенности защиты информации ограниченного доступа.

18. Классификация информации по видам тайны и степеням конфиденциальности.
19. Особенности помещений как объектов защиты.
20. Цели и задачи обеспечения безопасности информации.
21. Прикладные модели защиты информации в АС.
22. Характеристика основных стадий создания комплексной системы защиты информации.
23. Функции руководства предприятия.
24. Сущность и цели управления комплексной системы защиты

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Проверка информационной защищенности на соответствие нормативным документам», составляет 90 часов. На самостоятельную работу – 54 часа. При этом аудиторная нагрузка состоит из 54 лекционных часов и 36 часов лабораторных работ.

Обучающийся получает теоретические знания на лекциях. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Подготовка к лабораторным работам предполагает повторение лекционного материала. В результате студент должен быть готов к выполнению лабораторных работ. Основной лабораторных работ является выполнение заданий с последующим предоставлением отчета о выполнении.

В рамках указанной дисциплины итоговой формы аттестации является экзамен. Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов по практическим занятиям и лабораторных работ.

Методические указания для написания реферата

Прежде всего, нужно выбрать тему реферата и подобрать соответствующую литературу. После ознакомления с литературой следует приступить к составлению плана. План реферата должен состоять из названия (темы), введения, основной части, заключения и списка использованной литературы (3-5 работ). Основная часть, как правило, разбивается на дополнительные вопросы (не более 3-4).

Объём реферата должен быть не менее 12 машинописных страниц.

Во введении описывается цель, задачи работы, а также раскрываются смысл и значение основных понятий выбранной темы, область их применения.

В основной части необходимо:

г) ещё раз уточнить тему работы;

д) разбить основную часть работы на дополнительные вопросы;

е) дать ответы на эти вопросы, получив вспомогательные результаты. На их основе дать ответ на основной вопрос. Допускаются ссылки на дополнительную литературу.

В заключении подводятся итоги исследования. Заключение не должно быть большим по объёму.