



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

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ (ШКОЛА)

«СОГЛАСОВАНО»

Руководитель ОП

Боршевников А.Е.

«УТВЕРЖДАЮ»

И.о. директора департамента

Боршевников А.Е.

«25» марта 2022 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Организация и управление защитой информации на предприятии
Направление подготовки 10.03.01 Информационная безопасность
Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)

Форма подготовки очная

курс 4 семестр 8
лекции 18 ч.
практические занятия 36 час.
лабораторные работы 0 ч.
в том числе с использованием МАО лек. /пр. 18 /лаб. 0 час.
всего часов аудиторной нагрузки 54 час.
в том числе с использованием МАО 18 час.
самостоятельная работа 90 час.
в том числе на подготовку к экзамену 36 час.
курсовая работа / курсовой проект не предусмотрены
зачет не предусмотрен
экзамен 8 семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427.

Рабочая программа обсуждена на заседании департамента информационной безопасности протокол № 5а от «15» февраля 2022 г.

И.о. директора департамента информационной безопасности Боршевников А.Е.

Составитель: Боршевников А.Е.

Владивосток
2022

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании департамента:

Протокол от « ____ » _____ 20__ г. № _____

Заведующий кафедрой _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании департамента:

Протокол от « ____ » _____ 20__ г. № _____

Заведующий кафедрой _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании департамента:

Протокол от « ____ » _____ 20__ г. № _____

Заведующий кафедрой _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании департамента:

Протокол от « ____ » _____ 20__ г. № _____

Заведующий кафедрой _____
(подпись) (И.О. Фамилия)

Цели и задачи освоения дисциплины:

Цель: показать структуру, логическую организацию, систему управления службой защиты информации как основного звена систем защиты информации.

Задачи:

- определение места службы защиты информации в системе безопасности предприятия;
- объяснение функций службы защиты информации;
- обоснование оптимальной структуры и штатного состава службы защиты информации в зависимости от решаемых задач и выполняемых функций;
- установление организационных основ и принципов деятельности службы защиты информации;
- разрешение общих и специфических вопросов подбора, расстановки и обучения кадров, организации труда сотрудников службы защиты информации;
- раскрытие принципов, методов и технологии управления службой защиты информации.

В результате изучения данной дисциплины у обучающихся формируются следующие компетенции:

Код и наименование профессиональной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
ПК-1 Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1.1 Определяет состав работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
	ПК-1.2 Администрирует работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
	ПК-1.3 Применяет средства контроля работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК-2 Способен применять программные средства	ПК-2.1 Определяет состав программных средств системного, прикладного и специального назначения

системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ПК-2.2 Осуществляет проверки работоспособности программных средств системного, прикладного и специального назначения
	ПК-2.3 Применяет программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
ПК-3 Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	ПК-3.1 Использует инструментальные средства проектирования подсистем и средств обеспечения информационной безопасности
	ПК-3.2 Осуществляет анализ исходных данных для проектирования
	ПК-3.3 Проводит процедуры технико-экономического обоснования соответствующих проектных решений
ПК-4 Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ПК-4.1 Определяет состав рабочей технической документации
	ПК-4.2 Применяет технологические платформы, сервисы и информационные ресурсы создания технической документации
	ПК-4.3 Осуществляет сопровождение технической документации
ПК-5 Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-5.1 Определяет состав контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
	ПК-5.2 Осуществляет организацию, контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
	ПК-5.3 Производит аттестацию объектов вычислительной техники на соответствие требованиям по защите информации
ПК-6 Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-6.1 Определяет состав требований стандартов в области информационной безопасности
	ПК-6.2 Создает и ведет справочный ресурс для анализа информационной безопасности объектов
	ПК-6.3 Подготавливает технические отчеты по информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
ПК-7 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-7.1 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
ПК-8 Способен принимать участие в формировании,	ПК-8.1 Определяет состав мер по обеспечению информационной безопасности

организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ПК-8.2 Осуществляет стратегическое планирование процессом их реализации
	ПК-8.3 Организует и поддерживает выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения)
ПК-1.1 Определяет состав работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	<p>Знает программные интерфейсы настроек политик управления доступом в операционных системах</p> <p>Умеет использовать средства защиты информации операционных систем для противодействия угрозам безопасности информации</p> <p>Владеет навыками настройки антивирусной защиты в соответствии с действующими требованиями</p>
ПК-1.2 Администрирует работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	<p>Знает архитектуру и принципы построения и защиты операционных систем</p> <p>Умеет использовать криптографические протоколы, применяемые в компьютерных сетях</p> <p>Владеет настройкой программных и аппаратных средств построения компьютерных сетей, в том числе использующих криптографическую защиту информации</p>
ПК-1.3 Применяет средства контроля работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	<p>Знает принципы функционирования сетевых протоколов, включающих криптографические алгоритмы</p> <p>Умеет настраивать правила обработки пакетов в компьютерных сетях</p> <p>Владеет навыками установки программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации</p>
ПК-2.1 Определяет состав программных средств системного, прикладного и специального назначения	<p>Знает классификацию современных компьютерных средств системного, прикладного и специального назначения</p> <p>Умеет применять принципы функционирования программных средств криптографической защиты информации</p> <p>Владеет навыками обеспечения безопасности в базах данных</p>
ПК-2.2 Осуществляет проверки работоспособности программных средств системного, прикладного и специального назначения	<p>Знает критерии оценки эффективности и надежности средств защиты программного обеспечения</p> <p>Умеет применять аналитические и компьютерные модели систем защиты информации</p> <p>Владеет навыками проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации</p>
ПК-2.3 Применяет программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	<p>Знает основные угрозы безопасности информации и модели нарушителя</p> <p>Умеет оценивать информационные риски</p> <p>Владеет навыками расчета показателей эффективности защиты информации</p>
ПК-3.1 Использует инструментальные средства проектирования подсистем и средств обеспечения информационной	<p>Знает основы проверки работоспособности средств защиты информации от несанкционированного доступа</p> <p>Умеет проводить контроль защищенности информации от</p>

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения)
безопасности	<p>несанкционированного доступа и специальных воздействий с использованием программных и программно-аппаратных средств</p> <p>Владеет навыками оформлять отчетные документы</p>
ПК-3.2 Осуществляет анализ исходных данных для проектирования	<p>Знает принципы работы и правила эксплуатации программно-аппаратных средств защиты информации</p> <p>Умеет документировать процедуры и результаты контроля функционирования системы защиты информации</p> <p>Владеет навыками разработки программ и методик испытаний опытного образца программно-технического средства</p>
ПК-3.3 Проводит процедуры технико-экономического обоснования соответствующих проектных решений	<p>Знает национальные, межгосударственные и международные стандарты в области защиты информации</p> <p>Умеет применять руководящие и методические документы уполномоченных федеральных органов исполнительной власти</p> <p>Владеет навыками внесения изменений в эксплуатационную документацию</p>
ПК-4.1 Определяет состав рабочей технической документации	<p>Знает нормативные правовые акты в области защиты информации</p> <p>Умеет применять стандартные эксплуатации защищенных систем</p> <p>Владеет навыками самостоятельного решения в области внедрения и эксплуатации средств защиты информации</p>
ПК-4.2 Применяет технологические платформы, сервисы и информационные ресурсы создания технической документации	<p>Знает организационно-распорядительные документы по системе защиты информации</p> <p>Умеет применять Порядок аттестации объектов информатизации на соответствие требованиям безопасности информации</p> <p>Владеет методами формирования состава и содержания проектной документации</p>
ПК-4.3 Осуществляет сопровождение технической документации	<p>Знает отчетные документы, оформляемые по результатам контроля защищенности информации от утечки по каналам ПЭМИН</p> <p>Умеет проводить техническое обслуживание программно-аппаратных средств защиты информации</p> <p>Владеет методами оценки защищенности информации</p>
ПК-5.1 Определяет состав контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	<p>Знает основы проверки работоспособности средств защиты информации от несанкционированного доступа</p> <p>Умеет проводить контроль защищенности информации от несанкционированного доступа и специальных воздействий с использованием программных и программно-аппаратных средств</p> <p>Владеет навыками оформлять отчетные документы</p>
ПК-5.2 Осуществляет организацию, контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	<p>Знает организационные меры по защите информации</p> <p>Умеет разрабатывать политики безопасности информации</p> <p>Владеет навыками разрабатывать документы в области обеспечения безопасности информации</p>

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения)
ПК-5.3 Производит аттестацию объектов вычислительной техники на соответствие требованиям по защите информации	<p>Знает правовые основы организации защиты государственной тайны и конфиденциальной информации</p> <p>Умеет разрабатывать проекты инструкций, регламентов и организационно-распорядительных документов,</p> <p>Владеет навыками формулировать основные требования при лицензировании деятельности в области сертификации и аттестации по требованиям безопасности информации</p>
ПК-6.1 Определяет состав требований стандартов в области информационной безопасности	<p>Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа</p> <p>Умеет формулировать основные требования, предъявляемые к аттестации объектов информатизации на соответствие требованиям по защите информации</p> <p>Владеет навыками разрабатывать порядок аттестации объектов информатизации и выделенных помещений на соответствие требованиям безопасности информации</p>
ПК-6.2 Создает и ведет справочный ресурс для анализа информационной безопасности объектов	<p>Знает основы разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации</p> <p>Умеет разрабатывать модели угроз и модели нарушителя объекта информатизации</p> <p>Владеет навыками формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации</p>
ПК-6.3 Подготавливает технические отчеты по информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	<p>Знает основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности</p> <p>Умеет применять современную нормативную базу и ГОСТы, регламентирующие процесс разработки</p> <p>Владеет навыками участия в разработке системы обеспечения информационной безопасности объекта</p>
ПК-7.1 Демонстрирует знание методологий организации технологический процесс защиты информации ограниченного доступа	<p>Знает основные нормативные правовые акты в области обеспечения информационной безопасности</p> <p>Умеет разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации</p> <p>Владеет навыками расчета и управления рисками информационной безопасности</p>
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	<p>Знает нормативно-методические материалы по регламентации системы организационной защиты информации</p> <p>Умеет применять нормативные методические документы ФСБ России в области защиты информации</p> <p>Владеет навыками использования нормативных методических документов ФСТЭК России в области информационной безопасности</p>
ПК-7.3 Разрабатывает технические отчеты о проделанной работе, обзоры, готовит публикации	<p>Знает основные принципы создания эскизного, технического, рабочего проектов</p> <p>Умеет разрабатывать организационно-распорядительную документацию по обеспечению информационной безопасности</p> <p>Владеет навыками структурирования информации по теме исследования</p>

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения)
ПК-8.1 Определяет состав мер по обеспечению информационной безопасности	Знает перечень и содержание мероприятий по защите информации Умеет формулировать частные политики безопасности Владеет навыками приемами и методами проведения мероприятий по защите информации
ПК-8.2 Осуществляет стратегическое планирование процессом их реализации	Знает методы работы с научной информацией, принципы и правила построения суждений и оценок Умеет обосновывать и планировать состав и архитектуру системы обеспечения информационной безопасности Владеет навыками организации совместных разработок.
ПК-8.3 Организует и поддерживает выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Знает особенности современных программно-аппаратных средств защиты информации Умеет обоснованно выбирать наиболее подходящие методы и средства защиты информации Владеет навыком использовать современные автоматизированные технологии проектной деятельности

Трудоёмкость дисциплины и видов учебных занятий по дисциплине

Общая трудоёмкость 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
Лек	Лекции
Пр	Практические занятия
СР	Самостоятельная работа обучающегося в период теоретического обучения
Контроль	Самостоятельная работа обучающегося и контактная работа обучающегося с преподавателем в период промежуточной аттестации

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. МЕСТО И РОЛЬ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ	8	9	-	20	-	28	36	УО-1; ПР-6
2.	Раздел 2. ОРГАНИЗАЦИЯ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ		9	-	16	-	26		УО-1; ПР-6
Итого:			18	-	36	-	54	36	

СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

РАЗДЕЛ 1. МЕСТО И РОЛЬ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ (9 час.)

ТЕМА 1. Место и роль службы защиты информации в системе защиты информации (3 час.)

Предмет, задачи и содержание курса. Значение и место курса в подготовке кадров по специальности "Организация и технология защиты информации". Научная и учебная взаимосвязь курса и других дисциплин специальности. Структура курса. Распределение тем по видам аудиторных занятий. Формы проведения практических занятий. Формы проверки знаний. Анализ источников, научной и учебной литературы по курсу. Методика самостоятельной работы студентов. Знания и умения студентов, которые должны быть получены в результате изучения курса.

ТЕМА 2. Задачи и функции службы защиты информации (3 час.)

Организационные задачи и функции службы защиты информации. Технологические задачи и функции службы защиты информации. Координационные задачи и функции службы защиты информации.

Взаимосвязь и соотношение организационных, технологических и координационных задач и функций. Факторы, влияющие на определение задач и функций службы защиты информации.

ТЕМА 3. Структура и штаты службы защиты информации (3 час.)

Изучить структуру и штаты службы защиты информации. Общая структурная схема службы защиты информации. Подразделения службы защиты информации. Факторы, определяющие конкретную структуру службы защиты информации. Виды и типы организационных структур службы защиты информации. Централизованная и децентрализованная структуры службы защиты информации, условия, критерии, определяющие выбор структур. Должностной состав сотрудников службы защиты информации

РАЗДЕЛ 2. ОРГАНИЗАЦИЯ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ (9 час.)

ТЕМА 1. Организационные основы и принципы деятельности службы защиты информации (2 час.)

Порядок создания службы защиты информации. Структура и содержание положения о службе защиты информации. Состав и содержание других нормативных документов, регламентирующих деятельность службы 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 2. Подбор, расстановка и обучение сотрудников службы защиты информации (2 час.)

Общие и специфические требования, предъявляемые к сотрудникам службы защиты информации. Особенности подбора кадров. Методы получения информации о кандидатурах на должности. Социально-психологические факторы, влияющие на расстановку кадров. Формы

создания и способы поддержания необходимого микроклимата в коллективе. Формы повышения квалификации сотрудников. Подготовка кадрового резерва. Деятельность службы защиты информации зависит от того какую информацию и какими средствами необходимо защищать.

ТЕМА 3. Организация труда сотрудников службы защиты информации (1 час.)

Специфика деятельности сотрудников службы защиты информации. Распределение обязанностей между сотрудниками службы защиты информации. Обеспечение персональной ответственности за сохранность носителей информации. Структура и содержание должностных инструкций сотрудников службы защиты информации.

ТЕМА 4. Принципы и методы управления службой защиты информации (1 час.)

Принципы управления службой защиты информации. Понятие и сущность методов управления. Система методов управления. Административно-правовые методы управления. Экономические методы управления. Социально-психологические методы управления. Взаимосвязь методов управления. Необходимость комплексного и системного применения методов управления службой защиты информации.

ТЕМА 5. Технология управления службой защиты информации (3 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.

СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (36 час.)

Практическое занятие 1: Система организационно-правового обеспечения информационной безопасности (12 час.)

Практическое занятие 2: Правовая основа информационной безопасности (12 час.)

Практическое занятие 3: Криминалистическая характеристика способов незаконного получения защищаемой информации (6 час.)

Практическое занятие 4: Мероприятия, методы и средства защиты информации (6 час.)

I. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Организация и управление защитой информации на предприятии» 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.

II. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
	РАЗДЕЛ 1. МЕСТО	ПК-1.1	знает	ПР-1	1-17

1	И РОЛЬ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ	<p>Определяет состав работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;</p> <p>ПК-1.2 Администрирует работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;</p> <p>ПК-1.3 Применяет средства контроля работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации</p> <p>ПК-2.1 Определяет состав программных средств системного, прикладного и специального назначения</p> <p>ПК-2.2 Осуществляет проверки работоспособности программных средств</p>	умеет	ПР-4	1-17
			владеет	ПР-7	1-17

системного,
прикладного и
специального
назначения

ПК-2.3
Применяет
программные
средства
системного,
прикладного и
специального
назначения,
инструментальны
е средства, языки
и системы
программировани
я для решения
профессиональны
х задач

ПК-3.1
Использует
инструментальны
е средства
проектирования
подсистем и
средств
обеспечения
информационной
безопасности

ПК-3.2
Осуществляет
анализ исходных
данных для
проектирования

ПК-3.3 Проводит
процедуры
техничко-
экономического
обоснования
соответствующих
проектных
решений

ПК-4.1
Определяет
состав рабочей
технической
документации

ПК-4.2
Применяет
технологические
платформы,
сервисы и
информационные
ресурсы создания
технической
документации

ПК-4.3

--	--	--	--

		Осуществляет сопровождение технической документации			
2	РАЗДЕЛ 2. ОРГАНИЗАЦИЯ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ	ПК-5.1 Определяет состав контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	знает	ПР-1	18-40
		ПК-5.2 Осуществляет организацию, контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	умеет	ПР-7	18-40
		ПК-5.3 Производит аттестацию объектов вычислительной техники на соответствие требованиям по защите информации	владеет	ПР-7	18-40
		ПК-6.1 Определяет состав требований стандартов в области информационной безопасности			
		ПК-6.2 Создает и ведет справочный ресурс для анализа информационной безопасности объектов			

		<p>ПК-6.3 Подготавливает технические отчеты по информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности</p> <p>ПК-7.1 Демонстрирует знание методологий организации технологический процесс защиты информации ограниченного доступа</p> <p>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</p> <p>ПК-7.3 Разрабатывает технические отчеты о проделанной работе, обзоры, готовит публикации</p> <p>ПК-8.1 Определяет состав мер по обеспечению информационной безопасности</p> <p>ПК-8.2 Осуществляет</p>			
--	--	---	--	--	--

	стратегическое планирование процессом их реализации			
	ПК-8.3 Организует и поддерживает выполнение комплекса мер по обеспечению информационной безопасности, управлять их процессом их реализации			

III. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО- МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Информационные технологии: учебное пособие / И. А. Коноплева, О. А. Хохлова, А. В. Денисов – Москва: Проспект, 2016 – 328 с.
2. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.
3. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы»
4. Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации»

Дополнительная литература

1. Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. № Пр-646.
2. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.
3. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс]: учебное пособие/ Сычев Ю.Н.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 195 с.
4. Информационная безопасность : учебное пособие / Ю. Н. Егорова ; [отв. ред. В. П. Желтов] ; Чувашский государственный университет – Чебоксары : Изд-во Чувашского университета, 2015 – 131 с.
5. Руководящие документы Гостехкомиссии (РД ГТК) и ГОСТы Российской Федерации по защите информации.

Интернет источники

1. http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5792,
Васильев В.И. - Интеллектуальные системы защиты информации;
Издательство: «Машиностроение», Год:2013, Издание: Второе издание,
исправленное и дополненное, Объем:172 стр.
2. http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1122,
Шаньгин В.Ф. - Защита компьютерной информации. Издательство:
«ДМК Пресс», Год:2010, Объем: 544стр.
3. <http://padabum.com/d.php?id=2562> - В. Олифер, Н. Олифер
«Компьютерные сети. Принципы, технологии, протоколы» СПб.:
Питер, 2010, 944 с.

IV. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Организация и управление защитой информации на предприятии», составляет 54 часа. На самостоятельную работу – 54 часов. При этом аудиторная нагрузка состоит из 36 лекционных часов и 18 часов практических занятий.

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

Подготовка к практическим занятиям предполагает повторение лекционного материала. В результате студент должен быть готов к выполнению заданий на практическом занятии и выполнению лабораторных работ. Основной практической составляющей является выполнение одного практического задания 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.

V. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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

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 практических заданий.	54	Отчет о выполнении
2	Сессия	Подготовка к экзамену	36	Экзамен

Подготовка отчетов к практическим заданиям предполагает повторение лекционного материала и выполнение практических заданий. В результате студент должен представить отчет 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.
4. Текущее тестирование.

Критерии оценки результатов самостоятельной работы

Критериями оценок результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентами 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, материалов по практическим занятиям и лабораторным работам.

Фонд оценочных средств

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	РАЗДЕЛ 1. МЕСТО И РОЛЬ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ	<p>ПК-1.1 Определяет состав работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;</p> <p>ПК-1.2 Администрирует работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;</p> <p>ПК-1.3 Применяет средства контроля работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации</p> <p>ПК-2.1 Определяет состав</p>	знает	ПР-1	1-17
			умеет	ПР-4	1-17
			владеет	ПР-7	1-17

		<p>программных средств системного, прикладного и специального назначения</p> <p>ПК-2.2 Осуществляет проверки работоспособности программных средств системного, прикладного и специального назначения</p> <p>ПК-2.3 Применяет программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач</p> <p>ПК-3.1 Использует инструментальные средства проектирования подсистем и средств обеспечения информационной безопасности</p> <p>ПК-3.2 Осуществляет анализ исходных данных для проектирования</p> <p>ПК-3.3 Проводит процедуры технико-экономического обоснования соответствующих проектных решений</p> <p>ПК-4.1 Определяет состав рабочей технической</p>			
--	--	--	--	--	--

		<p>документации</p> <p>ПК-4.2 Применяет технологические платформы, сервисы и информационные ресурсы создания технической документации</p> <p>ПК-4.3 Осуществляет сопровождение технической документации</p>			
2	РАЗДЕЛ 2. ОРГАНИЗАЦИЯ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ	<p>ПК-5.1 Определяет состав контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации</p> <p>ПК-5.2 Осуществляет организацию, контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации</p> <p>ПК-5.3 Производит аттестацию объектов вычислительной техники на соответствие требованиям по защите информации</p> <p>ПК-6.1 Определяет состав требований</p>	знает	ПР-1	18-40
			умеет	ПР-7	18-40
			владеет	ПР-7	18-40

	<p>стандартов в области информационной безопасности</p> <p>ПК-6.2 Создает и ведет справочный ресурс для анализа информационной безопасности объектов</p> <p>ПК-6.3 Подготавливает технические отчеты по информационной безопасности объектов и систем на соответствие требованиям стандартам в области информационной безопасности</p> <p>ПК-7.1 Демонстрирует знание методологий организации технологического процесса защиты информации ограниченного доступа</p> <p>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</p> <p>ПК-7.3 Разрабатывает технические отчеты о проделанной работе, обзоры,</p>			
--	---	--	--	--

	<p>готовит публикации</p> <p>ПК-8.1 Определяет состав мер по обеспечению информационной безопасности</p> <p>ПК-8.2 Осуществляет стратегическое планирование процессом их реализации</p> <p>ПК-8.3 Организует и поддерживает выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации</p>			
--	--	--	--	--

Оценочные средства для промежуточной аттестации
Список вопросов на экзамен

- 1) Место службы защиты информации в системе безопасности предприятия.
- 2) Назначение службы защиты информации.
- 3) Организационные задачи и функции службы защиты информации.
- 4) Факторы, влияющие на определение задач и функций службы защиты информации.
- 5) Виды и типы организационных структур службы защиты информации.
- 6) Основные принципы организации и деятельности службы защиты информации.
- 7) Общие и специфические требования, предъявляемые к сотрудникам службы защиты информации.
- 8) Методы оценки качества службы защиты информации.

для проведения зачёта по учебной дисциплине

9) Основные задачи и функциональная структура службы безопасности предприятия. Какие подразделения данной службы могут объединяться в службу защиты информации и для выполнения каких основных задач.

10) Цели и задачи службы защиты информации на предприятии.

11) Функции руководителя службы защиты информации на предприятии.

12) Принципы создания и функционирования службы защиты информации на предприятии.

13) Организационные задачи и функции службы защиты информации на предприятии.

14) Технологические задачи и функции службы защиты информации на предприятии.

15) Координационные задачи и функции службы защиты информации на предприятии.

16) Общая структурная схема службы защиты информации.

17) Факторы, определяющие конкретную структуру службы защиты информации. Основные методы расчёта численности персонала службы защиты информации.

18) Виды и типы организационных структур службы защиты информации. Централизованная и децентрализованная структуры службы защиты информации, условия и критерии, определяющие выбор оптимальных структур.

19) Должностной состав сотрудников службы защиты информации, его зависимость от характера, выполняемых работ.

20) Задачи и функции руководителя службы защиты информации на предприятии.

21) Задачи и функции начальника группы режима службы защиты информации на предприятии.

22) Задачи и функции начальника группы защиты информации от несанкционированного доступа в средствах вычислительной техники службы защиты информации на предприятии.

23) Задачи и функции начальника криптографической группы службы защиты информации на предприятии.

24) Задачи и функции начальника группы противодействия техническим средствам разведки службы защиты информации на предприятии.

25) Основная нормативно-правовая база, регламентирующая вопросы деятельности службы защиты информации на предприятии.

26) Условия и факторы, влияющие на организацию работы службы защиты информации.

27) Порядок создания службы защиты информации.

28) Организация взаимодействия службы защиты информации и подразделений предприятия.

29) Общие и специфические требования, предъявляемые к сотрудникам службы защиты информации. Особенности подбора кадров.

30) Методы получения информации о кандидатурах на должности сотрудников службы защиты информации предприятия.

31) Особенности конкурсного отбора кандидатов и качества проведения испытательных сроков с ними.

32) Социально-психологические факторы, влияющие на расстановку кадров. Формы создания и способы поддержания необходимого микроклимата в коллективе.

33) Формы повышения квалификации сотрудников. Подготовка кадрового резерва.

34) Принципы управления службой защиты информации.

35) Понятие и сущность методов управления.

36) Система методов управления.

37) Административно-правовые, экономические и социально-

психологические методы управления. Взаимосвязь методов управления.

38) Состав и содержание управленческих решений. Значение управленческих решений.

39) Цели планирования. Виды планирования, их назначение.

40) Планы, их содержание и структура. Методы и формы контроля выполнения планов.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Организация и управление защитой информации на предприятии», составляет 54 часа. На самостоятельную работу – 90 часов, в том числе 36 час. на подготовку к экзамену. При этом аудиторная нагрузка состоит из 18 лекционных часов и 36 часов практических занятий.

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

Подготовка к практическим занятиям предполагает повторение лекционного материала. В результате студент должен быть готов к выполнению заданий на практическом занятии и выполнению лабораторных работ. Основной практической составляющей является выполнение одного практического задания 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.