



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

---

---

**ШКОЛА ЕСТЕСТВЕННЫХ НАУК**

СОГЛАСОВАНО  
Руководитель ОП

УТВЕРЖДАЮ  
И.о. заведующего кафедрой

\_\_\_\_\_ Варлатая С.К.  
(подпись) (Ф.И.О. рук. ОП)

\_\_\_\_\_ Нефедев К.В.  
(подпись) (Ф.И.О. рук. ОП)

«\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**  
Комплексная защита объектов информатизации  
**Направление 10.03.01 Информационная безопасность**  
Организация и технологии защиты информации  
**Форма подготовки очная**

курс 4 семестр 8

лекции 36 час.

практические занятия 18 час.

лабораторные работы 36 час.

В том числе с использованием МАО лек. 36 / пр. 18 / лаб. 18 час. всего часов аудиторной нагрузки 90 час.

в том числе с использованием МАО 40 час. самостоятельная работа 63 час.

в том числе на подготовку к экзамену 27 час.

контрольные работы (количество) не предусмотрено

курсовая работа / курсовой проект не предусмотрено

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 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 доцент, к.т.н. Варлатая С.К.

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 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:

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1	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-

		<p>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>Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач</p>	<p>ПК-2</p>	<p>ПК-2.1 Определяет состав 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>Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений</p>	<p>ПК-3</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</p>

		проектных решений
Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ПК-4	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
Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-5	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
Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-6	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
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
Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ПК-8	ПК-8.1 Определяет состав мер по обеспечению информационной безопасности
		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

<b>Код и наименование индикатора достижения компетенции</b>	<b>Наименование показателя оценивания (результата обучения по дисциплине)</b>
ПК-1.1 Определяет состав работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знает:
	Умеет
	Владеет
ПК-1.2 Администрирует работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знает
	Умеет
	Владеет
ПК-1.3 Применяет средства контроля работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знает
	Умеет
	Владеет
ПК-2.1 Определяет состав программных средств системного, прикладного и специального назначения	Знает
	Умеет
	Владеет
ПК-2.2 Осуществляет проверки работоспособности программных средств системного, прикладного и специального назначения	Знает
	Умеет
	Владеет
ПК-2.3 Применяет программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знает
	Умеет
	Владеет
ПК-3.1 Использует инструментальные средства проектирования подсистем и средств обеспечения информационной безопасности	Знает
	Умеет
	Владеет
ПК-3.2 Осуществляет анализ исходных данных для проектирования	Знает
	Умеет
	Владеет
ПК-3.3 Проводит процедуры технико-экономического обоснования соответствующих проектных решений	Знает
	Умеет
	Владеет
ПК-4.1 Определяет состав рабочей технической документации	Знает
	Умеет
	Владеет
ПК-4.2 Применяет технологические платформы, сервисы и информационные ресурсы создания технической документации	Знает
	Умеет
	Владеет
ПК-4.3 Осуществляет сопровождение технической	Знает

документации	Умеет
	Владеет
ПК-5.1 Определяет состав контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Знает
	Умеет
	Владеет
ПК-5.2 Осуществляет организацию, контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Знает
	Умеет
	Владеет
ПК-5.3 Производит аттестацию объектов вычислительной техники на соответствие требованиям по защите информации	Знает
	Умеет
	Владеет
ПК-6.1 Определяет состав требований стандартов в области информационной безопасности	Знает
	Умеет
	Владеет
ПК-6.2 Создает и ведет справочный ресурс для анализа информационной безопасности объектов	Знает
	Умеет
	Владеет
ПК-6.3 Подготавливает технические отчеты по информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Знает
	Умеет
	Владеет
ПК-7.1 Демонстрирует знание методологий организации технологического процесса защиты информации ограниченного доступа	Знает
	Умеет
	Владеет
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
	Умеет
	Владеет
ПК-7.3 Разрабатывает технические отчеты о проделанной работе, обзоры, готовит публикации	Знает
	Умеет
	Владеет
ПК-8.1 Определяет состав мер по обеспечению информационной безопасности	Знает
	Умеет
	Владеет
ПК-8.2 Осуществляет стратегическое планирование процессом их реализации	Знает
	Умеет
	Владеет
ПК-8.3 Организует и поддерживает выполнение	Знает



комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Умеет
	Владеет

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
Пр	Практические занятия
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. МЕСТО И РОЛЬ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ	8	18	36	9	-	31	27	УО-1; ПР-6
2.	Раздел 2. ОРГАНИЗАЦИЯ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ		18		9		32		УО-1; ПР-6
	Итого:		36	36	18	-	63	27	

### 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 ЛАБОРАТОРНЫХ РАБОТ**

**Лабораторная работа 1:** Выявление источников и носителей информации на промышленном предприятии (10 часов).

**Лабораторная работа 2:** Выявление и анализ угроз безопасности информации в документообороте предприятия (8 часов).

**Лабораторная работа 3:** Подбор технических средств для обеспечения защиты информации (8 часов).

**Лабораторная работа 4:** Анализ рисков безопасности информации (10 часов).

### **СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА**

**Практические занятия (18 час.)**

**Практическое занятие 1:** Система организационно-правового обеспечения информационной безопасности (6 час.)

**Практическое занятие 2:** Правовая основа информационной безопасности (6 час.)

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

**Практическое занятие 4:** Мероприятия, методы и средства защиты информации (3 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	<p><b>И РОЛЬ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ</b></p>	<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 системного, прикладного и специального</p>	<p>умеет</p> <p>владеет</p>	<p>ПР-4</p> <p>ПР-7</p>	<p>1-17</p> <p>1-17</p>
---	---	---	-----------------------------	-------------------------	-------------------------

	<p>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 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>			
РАЗДЕЛ 2.	ПК-5.1	знает	ПР-1	18-40

2	<p><b>ОРГАНИЗАЦИЯ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ</b></p>	<p>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 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</p>	<p>умеет</p> <p>владеет</p>	<p>ПР-7</p> <p>ПР-7</p>	<p>18-40</p> <p>18-40</p>
---	--	---	-----------------------------	-------------------------	---------------------------



требованиям  
стандартов в  
области  
информационной  
безопасности

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-8.1  
Определяет состав  
мер по  
обеспечению  
информационной  
безопасности

ПК-8.2  
Осуществляет  
стратегическое  
планирование  
процессом их  
реализации

ПК-8.3  
Организует и  
поддерживает  
выполнение  
комплекса мер по  
обеспечению  
информационной  
безопасности,

	управлять процессом реализации	их			
--	--------------------------------------	----	--	--	--

### **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](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](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 «Ктомплексная защита объектов информатизации», составляет 90 часа. На самостоятельную работу – 90 часов. При этом аудиторная нагрузка состоит из 36 лекционных часов, 36 лабораторных 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**

<b>№ п/п</b>	<b>Дата/сроки выполнения</b>	<b>Вид самостоятельной работы</b>	<b>Примерные нормы времени на выполнение</b>	<b>Форма контроля</b>
1	1-18 неделя обучения	Подготовка практических заданий.	9	Отчет о выполнении
2	Сессия	Подготовка к экзамену	9	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**

<b>Процент правильных ответов</b>	<b>Оценка</b>
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.

## Паспорт фонда 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 криптографическ их) и технических средств защиты информации;</p> <p>ПК-1.2 Администрирует работы по установке, настройке и обслуживанию программных, программно- аппаратных (в том числе криптографическ их) 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 криптографическ их) и технических средств защиты информации</p> <p>ПК-2.1 Определяет состав программных средств системного,</p>	знает	ПР-1	1-17
			умеет	ПР-4	1-17
			владеет	ПР-7	1-17



		<p>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 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</p>	знает	ПР-1	18-40
			умеет	ПР-7	18-40
			владеет	ПР-7	18-40

		<p>требований 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</p>			
--	--	--	--	--	--

	<p>проделанной работе, обзоры, 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>			
--	--	--	--	--

### Контроль достижения целей курса

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1	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

		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
Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ПК-2	ПК-2.1 Определяет состав программных средств системного, прикладного и специального назначения
		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
Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать	ПК-3	ПК-3.1 Использует инструментальные средства проектирования подсистем и средств обеспечения информационной безопасности

в проведении технико-экономического обоснования соответствующих проектных решений		ПК-3.2 Осуществляет анализ исходных данных для проектирования
		ПК-3.3 Проводит процедуры технико-экономического обоснования соответствующих проектных решений
Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ПК-4	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
Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-5	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
Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-6	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
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
Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ПК-8	ПК-8.1 Определяет состав мер по обеспечению информационной безопасности
		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

**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 «Комплексная защита объектов информатизации», составляет 90 часа. На самостоятельную работу – 90 часа. При этом аудиторная нагрузка состоит из 36 лекционных часов, 36 лабораторных 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.