



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**  
Комплексная защита объектов информатизации  
**Направление 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 36 час.  
практические занятия 18 час.  
лабораторные работы 36 час.  
В том числе с использованием МАО лек.   / пр.   / лаб. 30 час.  
всего часов аудиторной нагрузки 90 час.  
в том числе с использованием МАО 30 час.  
самостоятельная работа 90 час.  
в том числе на подготовку к экзамену 27 час.  
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 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 доцент, к.т.н. Варлатая С.К.

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:

I. **Цель:** изучение основ построения комплексной защиты объектов информатизации, необходимых для формирования у обучающихся практических навыков для построения системы защиты информации на предприятии.

### Задачи:

- изучение структур и тенденций развития современных принципов защиты информации для обеспечения информационной безопасности на предприятии;
- формирование основных теоретических и практических знаний;
- изучение основ, необходимых для создания комплексной системы защиты информации на предприятии и соответствующего организационно-правового обеспечения защиты информации.

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы, характеризуют формирование следующих компетенций:

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 системного, прикладного и специального назначения,	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

инструментальные средства, языки и системы программирования для решения профессиональных задач	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-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-8 Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	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)</b>
ПК-1.1 Определяет состав работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и	Знает программные интерфейсы настроек политик управления доступом в операционных системах Умеет использовать средства защиты информации операционных систем для противодействия угрозам

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения)
технических средств защиты информации	<p>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 безопасности	<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>

<b>Код и наименование индикатора достижения компетенции</b>	<b>Наименование показателя оценивания (результата обучения)</b>
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 эксплуатационные 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-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	<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</p>

<b>Код и наименование индикатора достижения компетенции</b>	<b>Наименование показателя оценивания (результата обучения)</b>
объектов	объекта информатизации Владеет навыками формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации
ПК-6.3 Подготавливает технические отчеты по информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Знает основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности Умеет применять современную нормативную базу и ГОСТы, регламентирующие процесс разработки Владеет навыками участия в разработке системы обеспечения информационной безопасности объекта
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 5 зачётных единиц (180 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
Лаб	Лабораторные занятия
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	
1.	Раздел 1. МЕСТО И РОЛЬ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ	8	18	36	9	-	31	экзамен
2.	Раздел 2. ОРГАНИЗАЦИЯ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ		18		9		32	
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 ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА**

### **ЛАБОРАТОРНЫЕ ЗАНЯТИЯ**

**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).

### **Практические занятия**

**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.)

## **УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ**

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине включает в себя план-график выполнения самостоятельной работы по дисциплине.

**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	В течение семестра	Работа с литературой. Подготовка к лабораторным и практическим занятиям.	63	ПР-6
2	В течение семестра	Подготовка к экзамену	27	Экзамен

Подготовка отчетов к лабораторным работам предполагает повторение лекционного материала и выполнение практических заданий и 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.

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.

### КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ 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	ПК-1; ПК-2; ПК-3; ПК-4; ПК-6; ПК-8	знает	ПР-7 ПР-6	Вопросы к экзамену 1-17
			умеет	ПР-6	
			владеет	ПР-6	
2	РАЗДЕЛ 2. ОРГАНИЗАЦИЯ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ	ПК-1; ПК-2; ПК-3; ПК-4; ПК-6; ПК-8	знает	ПР-7 ПР-6	Вопросы к экзамену 18-40
			умеет	ПР-6	
			владеет	ПР-6	

## **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.

### **МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ**

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 заданий на практическом занятии. 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, материалов по практическим занятиям и лабораторным работам.

### **Методические указания для подготовки к лабораторным занятиям**

#### *Структура отчета по лабораторной работе*

Отчеты по лабораторным работам представляются в электронной форме, подготовленные как текстовые документы в редакторе MSWord.

Отчет должен быть обобщающим документом, включать всю информацию по выполнению заданий, в том числе таблицы список литературы необходимыми пояснениями и иллюстрациями.

Структурно отчет по лабораторной работе, как текстовый документ, комплектуется по следующей схеме:

✓ *Титульный лист* – обязательная компонента отчета, первая страница отчета, по принятой для лабораторных работ форме (титульный лист отчета должен размещаться в общем файле, где представлен текст отчета);

✓ *Исходные данные к выполнению заданий* – обязательная компонента отчета, с новой страницы, содержат указание варианта, темы и т.д.);

✓ *Основная часть* – материалы выполнения заданий, разбивается по рубрикам, соответствующих заданиям работы, с иерархической структурой: разделы – подразделы – пункты – подпункты и т. д.

Рекомендуется в основной части отчета заголовки рубрик (подрубрик) давать исходя из формулировок заданий, в форме отглагольных существительных;

✓ *Выводы* – обязательная компонента отчета, содержит обобщающие выводы по работе (какие задачи решены, оценка результатов, что освоено



при выполнении работы);

✓ *Список литературы* – обязательная компонента отчета, с новой страницы, содержит список источников, использованных при выполнении работы, включая электронные источники (список нумерованный, в соответствии с правилами описания библиографии);

✓ *Приложения* – необязательная компонента отчета, с новой страницы, содержит дополнительные материалы к основной части отчета.

#### Оформление отчета по лабораторной работе

Необходимо обратить внимание на следующие аспекты в оформлении отчетов работ:

- набор текста;
- структурирование работы;
- оформление заголовков всех видов (рубрик-подрубрик-пунктов-подпунктов, рисунков, таблиц, приложений);
- оформление перечислений (списков с нумерацией или маркировкой);
- оформление таблиц;
- оформление иллюстраций (графики, рисунки, фотографии, схемы, «скриншоты»);
- набор и оформление математических выражений (формул);
- оформление списков литературы (библиографических описаний) и ссылок на источники, цитирования.

#### Набор текста

Набор текста осуществляется на компьютере, в соответствии со следующими требованиями:

- ✓ печать – на одной стороне листа белой бумаги формата А4 (размер 210 на 297 мм.);
- ✓ интервал межстрочный – полуторный;
- ✓ шрифт – TimesNewRoman;
- ✓ размер шрифта – 14 пт., в том числе в заголовках (в таблицах допускается 10-12 пт.);

- ✓ выравнивание текста – «по ширине»;
- ✓ поля страницы – левое - 30 мм., правое - 10 мм., верхнее и нижнее - 20 мм.;
- ✓ нумерация страниц – в правом нижнем углу страницы (для страниц с книжной ориентацией), сквозная, от титульного листа до последней страницы, арабскими цифрами (первой страницей считается титульный лист, на котором номер не ставится, на следующей странице проставляется цифра «2» и т. д.).
- ✓ режим автоматического переноса слов, за исключением титульного листа и заголовков всех уровней (перенос слов для отдельного абзаца блокируется средствами MSWord с помощью команды «Формат» – абзац при выборе опции «запретить автоматический перенос слов»).

Если рисунок или таблица размещены на листе формата больше А4, их следует учитывать, как одну страницу. Номер страницы в этих случаях допускается не проставлять.

Список литературы и все приложения включаются в общую сквозную нумерацию страниц работы.

## МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус D, ауд. D 733,733а. Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций,	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 13) Оборудование: ЖК-панель 47", Full HD, LG M4716 CCBA – 1 шт. Доска аудиторная, Моноблок Lenovo C360G-i34164G500UDK с лицензионными программами Microsoft Office 2013(13 шт.) и аудиовизуальными средствами проектор Panasonic DLPPjectorPT-D2110XE	1С Предприятия8 (8.2), 7-Zip, ABBYY Lingvo12,Alice 3, Anaconda3,Autodesk,CodeBlocks,CorelDRAW X7,Dia,Directum4.8,DosBox-0.74,Farmanager,Firebird 2.5,FlameRobin,Foxit Reader,Free Pascal,Geany,Ghostscript,Git,Greenfoot,gsview,Inscapе0.91,Java,Java development Kit,Kaspersky,Lazarus,LibreOffice4.4,MatLab R2017b,Maxima 5.37.2,Microsoft Expression,Microsoft Office 2013,Microsoft Silverlight,Microsoft Silverlight 5SDK-русский,MicrosoftSistem Center,Microsoft Visial Studio 2012,MikTeX2.9,MySQL,NetBeans,Notepad++,Oracle VM VirtualBox,PascalABC.NET,PostgreSQL 9.4,PTC Mathcad,Putty,PyQt GPL v5.4.1 for Pythonv 3.4,Python2.7(3.4,3.6),QGIS Brighton,RStudio,SAM CoDeC Pack,SharePoint,Strawberry

текущего контроля и промежуточной аттестации		Perl, Tecnomatix, TeXnicCenter, TortoiseSVN, Unity2017.3.1f1, Veusz, Vim8.1, Visual Paradigm CE, Visual Studio2013, Windows Kits, Windows Phone SDK8.1, Xilinx Design Tools Acrobat ReaderDC, AdobeBridge CS3, AdobeDeviceCentralCS3, Adobe ExtendScript Toolkit 2, Adobe Photoshope CS3, DVD-студия Windows, GoogleChrome, Internet Explorer, ITMOproctor, Mozilla Firefox, Visual Studio Installer, Windows Media Center, WinSCP,
690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус А, ауд. А1042 Аудитория для самостоятельной работы студентов	Моноблок Lenovo C360G-i34164G500UDK – 115 шт.; Интегрированный сенсорный дисплей Polymedia FlipBox; Копир-принтер-цветной сканер в e-mail с 4 лотками Xerox WorkCentre 5330 (WC5330C; Полноцветный копир-принтер-сканер Xerox WorkCentre 7530 (WC7530CPS Оборудование для инвалидов и лиц с ограниченными возможностями здоровья: Дисплей Брайля Focus-40 Blue – 3 шт.; Дисплей Брайля Focus-80 Blue; Рабочая станция Lenovo ThinkCentre E73z – 3 шт.; Видео увеличитель ONYX Swing-Arm PC edition; Маркер-диктофон Touch Memo цифровой; Устройство портативное для чтения плоскочечатных текстов PEarl; Сканирующая и читающая машина для незрячих и слабовидящих пользователей SARA; Принтер Брайля Emprint SpotDot - 2 шт.; Принтер Брайля Everest - D V4; Видео увеличитель ONYX Swing-Arm PC edition; Видео увеличитель Topaz 24" XL стационарный электронный; Обучающая система для детей тактильно-речевая, либо для людей с ограниченными возможностями здоровья; Увеличитель ручной видео RUBY портативный – 2 шт.; Экран Samsung S23C200B; Маркер-диктофон Touch Memo цифровой.	Microsoft Windows 7 Pro MAGic 12.0 Pro, Jaws for Windows 15.0 Pro, Open book 9.0, Duxbury BrailleTranslator, Dolphin Guide (контракт № А238-14/2); Неисключительные права на использование ПО Microsoft рабочих станций пользователей (контракт ЭА-261-18 от 02.08.2018): - лицензия на клиентскую операционную систему; - лицензия на пакет офисных продуктов для работы с документами включая формат.docx , .xlsx , .vsd , .ppt.; - лицензия па право подключения пользователя к серверным операционным системам , используемым в ДВФУ : Microsoft Windows Server 2008/2012; - лицензия на право подключения к серверу Microsoft Exchange Server Enterprise; - лицензия па право подключения к внутренней информационной системе документооборота и portalу с возможностью поиска информации во множестве удаленных и локальных хранилищах, ресурсах, библиотеках информации, включая порталные хранилища, используемой в ДВФУ: Microsoft SharePoint; - лицензия на право подключения к системе централизованного управления рабочими станциями, используемой в ДВФУ: Microsoft System Center.

### ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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	Знает программные интерфейсы настроек политик управления доступом в операционных системах  Умеет использовать средства защиты информации операционных систем для противодействия угрозам

<b>Код и наименование индикатора достижения компетенции</b>	<b>Наименование показателя оценивания (результата обучения)</b>
числе криптографических) и технических средств защиты информации	<p>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 безопасности	<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>

<b>Код и наименование индикатора достижения компетенции</b>	<b>Наименование показателя оценивания (результата обучения)</b>
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 эксплуатационные 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-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	<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</p>

<b>Код и наименование индикатора достижения компетенции</b>	<b>Наименование показателя оценивания (результата обучения)</b>
объектов	объекта информатизации Владеет навыками формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации
ПК-6.3 Подготавливает технические отчеты по информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Знает основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности Умеет применять современную нормативную базу и ГОСТы, регламентирующие процесс разработки Владеет навыками участия в разработке системы обеспечения информационной безопасности объекта
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

### Контроль достижения целей курса

№ 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	ПК-1; ПК-2; ПК-3; ПК-4; ПК-6; ПК-8	знает	ПР-7 ПР-6	Вопросы к экзамену 1-17
			умеет	ПР-6	
			владеет	ПР-6	
2	РАЗДЕЛ 2. ОРГАНИЗАЦИЯ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ	ПК-1; ПК-2; ПК-3; ПК-4;	знает	ПР-7 ПР-6	Вопросы к экзамену 18-40
			умеет	ПР-6	

		ПК-6; ПК-8	владеет	ПР-6	
--	--	---------------	---------	------	--

### Текущая аттестация

**ПР-7 Конспект** - продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции.

Цели конспектирования состоят в:

- развитию умений систематизировать знания и выделять причинно-следственные связи, выявлять закономерности;
- развитию умений перерабатывать любую информацию, придавая ей иной вид, тип, форму;
- развитию навыков осмысленной переработки текста, структурирования информации, использования основных категорий анализа, работы с большими объемами информации;
- созданию модели проблемы (понятийную или структурную).

### **Требования к представлению и оцениванию материалов (результатов):**

В связи с объективным характером конспектирования не предлагается единых и обязательных параметров конспектируемого текста (степень сокращения информации). Объем законспектированного текста определяется самим студентом. Конспект должен быть подготовлен каждым студентом самостоятельно и отражать основные идеи изученной темы.

Перечень вопросов, необходимых для конспектирования определяется темой лекционного занятия. Конспекты выполняются во время лекционных занятий, и проверяются преподавателем в конце семестра.

### **Критерии оценки:**

Уровень освоения	Критерии оценки результатов обучения	Количество баллов / оценка
Повышенный	Конспекты лекций в наличии. Студент демонстрирует отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей научной области. Логически корректное изложение материала.	100-86 Зачтено
Базовый	Конспекты лекций в наличии. Студент показывает умение пользоваться концептуально-понятийным аппаратом. В целом логически корректное, но не	85-76 Зачтено

	всегда точное изложение материала.	
Пороговый	Конспекты лекций в наличии. Студент показывает затруднение с использованием научно-понятийного аппарата; частичные затруднения с выполнением конспекта.	75-61 Зачтено
Уровень не достигнут	Конспекты лекций отсутствуют или студент показывает отрывочное представление о теме.	60-0 Не зачтено

**Лабораторная работа (ПР-6)** – средство для закрепления и практического освоения материала по определенной теме.

Цель лабораторных работ – выработка у учащихся профессиональных умений применять полученные знания для решения практических задач, умений и навыков пользоваться подходами и методами информационной безопасности для осуществления профессиональной деятельности.

Во всех лабораториях существуют особые правила поведения студентов, которые необходимо неукоснительно соблюдать – правила техники безопасности. За знание правил техники безопасности и обязательство их выполнять каждый студент должен расписаться в соответствующем журнале.

Обработка результатов и оформление отчета проводится в течение недели после выполнения работы. Студент, не сдавший отчета в срок, к следующей работе не допускается.

**Требования к представлению и оцениванию материалов (результатов):**

Выполнение лабораторной работы осуществляется студентом самостоятельно в часы лабораторных занятий.

При оценке работы студента преподаватель учитывает все этапы работы студента над отчетом. Если отчет не был принят преподавателем и возвращен для доработки, то все исправления вносятся в тот же экземпляр отчета.



При оценке учитывается правильность выполнения отчета.  
Выставляется дифференцированный зачет.

**Критерии оценки:**

Уровень освоения	Критерии оценки результатов обучения	Количество баллов / оценка
Повышенный	Студент показал прочные знания основных понятий и их взаимосвязей, сущности процессов, рассматриваемых в работе, и умение их объяснить, знание методов, используемых в работе, методики обработки результатов. Показано хорошее понимание профессиональной значимости изучаемых вопросов. При выполнении экспериментальной части работы и оформлении отчета студент показал умение работать с данными и владение навыками представления и обработки результатов, умение делать выводы по результатам работы. Отчет по работе оформлен аккуратно, в соответствии с требованиями, структурирован, не содержит ошибок; правильно и полно сформулирован вывод по работе.	100 – 86  Зачтено  (отлично)
Базовый	Студент показал знания основных понятий и их взаимосвязей, сущности процессов, рассматриваемых в работе, и умение их объяснить, знание методов, используемых в работе, методики обработки результатов. Показано хорошее понимание профессиональной значимости изучаемых вопросов. При выполнении экспериментальной части работы и оформлении отчета студент показал умение работать с данными и владение навыками представления и обработки результатов, умение делать выводы по результатам работы. Отчет по работе оформлен аккуратно, в основном – в соответствии с требованиями, структурирован; правильно и полно сформулирован вывод по работе. Допускаются не более 2-х недочетов в оформлении отчета.	85-76  Зачтено  (хорошо)
Пороговый	Студент показал базовые знания основных понятий и их взаимосвязей, сущности процессов, рассматриваемых в работе, и умение их объяснить, демонстрирует, в целом, знание методов, используемых в работе, методики обработки результатов. При выполнении экспериментальной части работы и оформлении отчета студент в целом показал	75-61  Зачтено  (удовлетворительно)

	умение работать с данными и владение навыками представления и обработки результатов, умение делать выводы по результатам работы. Отчет по работе оформлен аккуратно, в основном в соответствии с требованиями, не содержит грубых ошибок, вывод по работе сформулирован.	
Уровень не достигнут	Студент не выполнил лабораторную работу, либо показал незнание основных понятий, сущности процессов, рассматриваемых в работе, демонстрирует плохое знание или незнание методов, методики обработки результатов. Слабо сформировано или не сформировано умение работать с данными, отсутствуют выводы по результатам работы. Отчет не соответствует требованиям, не сделан или сделан с грубыми ошибками.	60-0 Не зачтено (неудовлетворительно)

## 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.

### Критерии выставления оценки студенту на экзамене:

Баллы (рейтингов ой оценки)	Оценка (стандартная)	Требования к сформированным компетенциям
86-100	«отлично»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
76-85	«хорошо»	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
61-75	«удовлетворительно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.
0-60	«неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

<b>ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения по дисциплине</b>				
Оценка	2 (не зачтено)	3 (зачтено)	4 (зачтено)	5 (зачтено)
виды оценочных средств				
<b>Знания</b>	Отсутствие	Фрагментарные	Общие, но не	Сформированные

<i>(виды оценочных средств: конспект, лабораторная работа)</i>	знаний	знания	структурированные знания	систематические знания
<b>Умения</b> <i>(виды оценочных средств: лабораторная работа)</i>	Отсутствие умений	В целом успешное, но не систематическое умение	В целом успешное, но содержащее отдельные пробелы умение (допускает неточности не принципиального характера)	Успешное и систематическое умение
<b>Навыки (владения, опыт деятельности)</b>	Отсутствие навыков (владений, опыта)	Наличие отдельных навыков (наличие фрагментарного опыта)	В целом, сформированные навыки (владения), но используемые не в активной форме	Сформированные навыки (владения), применяемые при решении задач