



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



**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

Проверка информационной защищенности на соответствие нормативным документам

**Направление подготовки 10.03.01 Информационная безопасность**

Организация и технологии защиты информации  
(по отрасли или в сфере профессиональной деятельности)

**Форма подготовки очная**

курс 4 семестр 7

лекции 32 ч.

практические занятия 0 час.

лабораторные работы 32 час.

в том числе с использованием МАО лек. 0 /пр. 0 /лаб. 18 час.

всего часов аудиторной нагрузки 64 час.

в том числе с использованием МАО 18 час.

самостоятельная работа 80 час.

в том числе на подготовку к экзамену 36 час.

контрольные работы предусмотрены

курсовая работа / курсовой проект не предусмотрено

зачет не предусмотрен

экзамен 7 семестр

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

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

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

Составитель Боршевников А.Е.

Владивосток  
2022

**Оборотная сторона титульного листа РПД**

**I. Рабочая программа пересмотрена на заседании департамента:**

Протокол от « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г. № \_\_\_\_

Заведующий кафедрой \_\_\_\_\_  
(подпись) (И.О. Фамилия)

**II. Рабочая программа пересмотрена на заседании департамента:**

Протокол от « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г. № \_\_\_\_

Заведующий кафедрой \_\_\_\_\_  
(подпись) (И.О. Фамилия)

**III. Рабочая программа пересмотрена на заседании департамента:**

Протокол от « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г. № \_\_\_\_

Заведующий кафедрой \_\_\_\_\_  
(подпись) (И.О. Фамилия)

**IV. Рабочая программа пересмотрена на заседании департамента:**

Протокол от « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г. № \_\_\_\_

Заведующий кафедрой \_\_\_\_\_  
(подпись) (И.О. Фамилия)

## Цели и задачи освоения дисциплины:

**Цель:** обучить основным способам проверки организации защиты на основе требований нормативного обеспечения информационной безопасности.

### Задачи:

- обучение организационным основам, необходимым для работы на предприятии, осуществляющем свою деятельность в области информационной безопасности;
- объяснение основ правового регулирования отношений в информационной сфере;
- изучение методологических и законодательных основ организации системы защиты информации;
- изучение основных аспектов практической деятельности по анализу защищенности информации.

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

<b>Код и наименование профессиональной компетенции (результат освоения)</b>	<b>Код и наименование индикатора достижения компетенции</b>
ПК-7 Способен способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ПК-7.1 Демонстрирует знание методологий организации технологический процесс защиты информации ограниченного доступа
	ПК-7.2 Исследует нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю, составляет отчеты о проделанной работе, обзоры
	ПК-7.3 Разрабатывает технические отчеты о проделанной работе, обзоры, готовит публикации

<b>Код и наименование индикатора достижения компетенции</b>	<b>Наименование показателя оценивания (результата обучения по дисциплине)</b>
ПК-7.1 Демонстрирует знание методологий организации технологический процесс защиты информации ограниченного доступа	<p>Знает основные нормативные правовые акты в области обеспечения информационной безопасности</p> <p>Умеет разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации</p> <p>Владеет навыками расчета и управления рисками информационной безопасности</p>
ПК-7.2 Исследует нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю, составляет отчеты о проделанной работе, обзоры	<p>Знает нормативно-методические материалы по регламентации системы организационной защиты информации</p> <p>Умеет применять нормативные методические документы ФСБ России в области защиты информации</p> <p>Владеет навыками использования нормативных методических документов ФСТЭК России в области информационной безопасности</p>
ПК-7.3 Разрабатывает технические отчеты о проделанной работе, обзоры, готовит публикации	<p>Знает основные принципы создания эскизного, технического, рабочего проектов</p> <p>Умеет разрабатывать организационно-распорядительную документацию по обеспечению информационной безопасности</p> <p>Владеет навыками структурирования информации по теме исследования</p>

### Трудоемкость дисциплины и видов учебных занятий по дисциплине

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

(1 зачетная единица соответствует 36 академическим часам)

Видами учебных занятий и работы обучающегося по дисциплине являются:

Обозначение	Виды учебных занятий и работы обучающегося
Лек	Лекции
Лаб	Лабораторные работы
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					Контроль	Формы промежуточной аттестации
			Лек	Лаб	Пр	ОК	СР		
1.	Раздел 1. Правовые основы использования организационных и технических средств защиты информации	7	6	32	-	-	12	36	экзамен
2.	Раздел 2. Построение комплексной системы защиты информации		6		-		12		экзамен
3.	Раздел 3. Управление и эксплуатация комплексной системы защиты информации		8		-		6		экзамен
4.	Раздел 4. Моделирование комплексных систем защиты информации		6		-		4		экзамен
5.	Раздел 5. Методика проверки защищенности объектов информатизации на соответствие требованиям нормативных документов		6		-		10		экзамен
Итого:			32	32	-	-	44	36	

## **I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА**

### **Раздел 1. Правовые основы использования организационных и технических средств защиты информации**

#### **Тема 1. Назначение и структура правового обеспечения защиты информации**

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

Научная и учебная литература.

## **Тема 2. Законодательство РФ в области информационной безопасности**

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

## **Тема 3. Правовые основы использования организационных и технических средств защиты информации**

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

## **Тема 4. Лицензирование и сертификация в информационной сфере**

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

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

Лицензирование и сертификация в области международного информационного обмена

## **Тема 5. Система ответственности за нарушение норм защиты информации**

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

### **Раздел 2. Построение комплексной системы защиты информации**

#### **Тема 1. Виды обеспечения КСЗИ**

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

#### **Тема 2. Требования к автоматизированной системе в защищенном исполнении**

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

#### **Тема 3. Методы подбора технических средств ЗИ**

Общие понятия теории принятия технических решений, методы многокритериальных задач.

## **Раздел 3. Управление и эксплуатация комплексной системы защиты информации**

### **Тема 1. Управление КСЗИ**

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

### **Тема 2. Эксплуатация КСЗИ**

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

## **Раздел 4. Моделирование комплексных систем защиты информации**

### **Тема 1. Методы и модели оценки уязвимостей**

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

### **Тема 2. Организационные основы и принципы деятельности службы защиты информации**

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

### **Тема 3. Технология управления службой защиты информации**



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

## **Раздел 5. Методика проверки защищенности объектов информатизации на соответствие требованиям нормативных документов**

### **Тема 1. Методы формирования требований по защите информации**

Анализ нормативных документов. Оценка качества работы службы защиты информации.

### **Тема 2. Аналитическое обоснование необходимости создания СЗ СИ**

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

### **Тема 3. Заключение по результатам проверки**

Оценка эффективности работы комплексной системы защиты информации.

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

### **Лабораторные работы**

**Лабораторная работа №1.** Выявление и анализ угроз безопасности информации в документообороте предприятия

**Лабораторная работа №2.** Подбор технических средств для обеспечения защиты информации

**Лабораторная работа №3.** Анализ рисков безопасности информации

**Лабораторная работа №4.** Проверка защищенности объекта на соответствие нормативным документам

### **III. 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 занятиям.	44	ПР-6
2	В течение семестра	Подготовка к экзамену	36	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 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.

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.

#### IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

2	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций	Оценочные средства - наименование	
			текущий контроль	промежуточная аттестация
Раздел 1	ПК-7.1 ПК-7.2 ПК-7.3	знает	ПР-7	экзамен
		умеет	ПР-6	
		владеет		
Раздел 2	ПК-7.1 ПК-7.2 ПК-7.3	знает	ПР-7	экзамен
		умеет	ПР-6	
		владеет		
Раздел 3	ПК-7.1 ПК-7.2 ПК-7.3	знает	ПР-7	экзамен
		умеет	ПР-6	
		владеет		
Раздел 4	ПК-7.1 ПК-7.2 ПК-7.3	знает	ПР-7	экзамен
		умеет	ПР-6	
		владеет		
Раздел 5	ПК-7.1 ПК-7.2 ПК-7.3	знает	ПР-7	экзамен
		умеет	ПР-6	
		владеет		

Методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в ФОС.

## **V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

### **Основная литература**

1. Информационная безопасность : учеб. пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2018. — 432 с. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие. - М.: Форум: Инфра-М, 2010. -592 с.
2. Дикарев В.И., Заренков В.А., Заренков Д.В., Койнаш Б.В. Защита объектов и информации от несанкционированного доступа/ Под ред. В.А. Заренкова.– СПб.: ОАО «Издательство Стройиздат СПб», 2010.– 320 с.
3. Комплексный технический контроль эффективности мер безопасности систем управления в органах внутренних дел: Учебн. пособие/ Под ред. А. А. Чекалина. В 2-х ч. Ч. 1. Теоретические основы технической разведки и комплексного технического контроля.– М.: Горячая линия-Телеком, 2012.– 206 с.
4. Рудометов Е.А., Рудометов В.Е. Электронные средства разведки и защиты информации.– М.: ООО «Фирма «Издательство АСТ»; СПб.: ООО «Издательство ПОЛИГОН», 2010.– 224 с.
5. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия Телеком, 2010 – 311 с.
6. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных Системах – М.Ж Горячая линия-Телеком, 2011 – 156 с.

### **Дополнительная литература**

1. Инженерно-техническая защита информации: программа

дисциплины / А. Г. Лихоносков ; Московский гос. ун-т путей сообщ. (МИИТ),  
Юридический ин-т. - Москва: Юридический ин-т МИИТа, 2011. - 28 с.

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

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

### **Интернет-ресурсы**

1. [http://e.lanbook.com/books/element.php?pl1\\_cid=25&pl1\\_id=4925](http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=4925)  
Пушкарев В.В. «Защита информационных процессов в компьютерных системах», Издательство: ТУСУР (Томский государственный университет систем управления и радиоэлектроники), Год: 2012, Объем: 131 стр.

2. [http://e.lanbook.com/books/element.php?pl1\\_cid=25&pl1\\_id=4959](http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=4959) Титов  
А.А. «Инженерно-техническая защита информации» , Учебное пособие, Издательство: ТУСУР (Томский государственный университет систем управления и радиоэлектроники), Год:2010, Объем: 197 стр.

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

## **VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ**

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 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 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
<p>690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус Д, ауд. Д 733,733а. Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации</p>	<p>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 DLPPProjectorPT-D2110XE</p>	<p>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 Perl,Tecnomatix,TeXnicCenter,TortoiseSVN,Unity2017.3.1f1, Veusz,Vim8.1,Visual Paradigm CE,Visual Studio2013,Windows Kits,Windows Phone SDK8.1,Xilinx Design ToolsAcrobat 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,</p>



<p>690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус А, ауд. А1042 Аудитория для самостоятельной работы студентов</p>	<p>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.</p>	<p>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 порталу 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.</p>
--	--	---

## ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)
ПК-7.1 Демонстрирует знание методологий организации технологический процесс защиты информации ограниченного доступа	<p>Знает основные нормативные правовые акты в области обеспечения информационной безопасности</p> <p>Умеет разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации</p> <p>Владеет навыками расчета и управления рисками информационной безопасности</p>

ПК-7.2 Исследует нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю, составляет отчеты о проделанной работе, обзоры	<p>Знает нормативно-методические материалы по регламентации системы организационной защиты информации</p> <p>Умеет применять нормативные методические документы ФСБ России в области защиты информации</p> <p>Владеет навыками использования нормативных методических документов ФСТЭК России в области информационной безопасности</p>
ПК-7.3 Разрабатывает технические отчеты о проделанной работе, обзоры, готовит публикации	<p>Знает основные принципы создания эскизного, технического, рабочего проектов</p> <p>Умеет разрабатывать организационно-распорядительную документацию по обеспечению информационной безопасности</p> <p>Владеет навыками структурирования информации по теме исследования</p>

### Контроль достижения целей курса

2	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций	Оценочные средства - наименование	
			текущий контроль	промежуточная аттестация
Раздел 1	ПК-7.1 ПК-7.2 ПК-7.3	знает	ПР-7	экзамен
		умеет	ПР-6	
		владеет		
Раздел 2	ПК-7.1 ПК-7.2 ПК-7.3	знает	ПР-7	экзамен
		умеет	ПР-6	
		владеет		
Раздел 3	ПК-7.1 ПК-7.2 ПК-7.3	знает	ПР-7	экзамен
		умеет	ПР-6	
		владеет		
Раздел 4	ПК-7.1 ПК-7.2 ПК-7.3	знает	ПР-7	экзамен
		умеет	ПР-6	
		владеет		
Раздел 5	ПК-7.1 ПК-7.2 ПК-7.3	знает	ПР-7	экзамен
		умеет	ПР-6	
		владеет		

		владеет		
--	--	---------	--	--

### 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 всегда точное изложение материала.	85-76 Зачтено

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	100 – 86

	<p>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.</p>	<p>Зачтено (отлично)</p>
Базовый	<p>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.</p>	<p>85-76  Зачтено (хорошо)</p>
Пороговый	<p>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 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.</p>	<p>75-61  Зачтено (удовлетворительно)</p>
Уровень не достигнут	<p>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</p>	<p>60-0  Не зачтено (неудовлетворительно)</p>

	сформировано умение работать с данными, отсутствуют выводы по результатам работы. Отчет не соответствует требованиям, не сделан или сделан с грубыми ошибками.	
--	--	--

## **Оценочные средства для промежуточной аттестации**

### **Список вопросов на экзамен**

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

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

#### **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> (виды оценочных средств: конспект, лабораторная работа)	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
<b>Умения</b> (виды оценочных средств: лабораторная работа)	Отсутствие умений	В целом успешное, но не систематическое умение	В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципиального 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