

МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования «Кабардино-Балкарский государственный университет им. Х.М.  
Бербекова» (КБГУ)

ИНСТИТУТ ИНФОРМАТИКИ, ЭЛЕКТРОНИКИ И РОБОТОТЕХНИКИ  
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СОГЛАСОВАНО

УТВЕРЖДАЮ

Руководитель образовательной программы  
\_\_\_\_\_ А.С. Ксенофонтов

Директор ИИЭР  
\_\_\_\_\_ Н.В. Черкесова

«\_\_\_» \_\_\_\_\_ 2020 г.

«\_\_\_» \_\_\_\_\_ 2020 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Антивирусные системы защиты информации**

Направление подготовки  
**10.03.01 Информационная безопасность**

Профиль подготовки  
Организация и технология защиты информации

Квалификация (степень) выпускника  
Бакалавр

Форма обучения  
Очная

Нальчик 2020

Рабочая программа дисциплины «Антивирусные системы защиты информации» /  
сост. С.М. Арванова – Нальчик: ФГБОУ КБГУ, 2020. – 28 с.

Рабочая программа предназначена для преподавания дисциплины вариативной части математического и естественнонаучного цикла студентам очной формы обучения по направлению подготовки 10.03.01. «Информационная безопасность» в 7 семестре.

Рабочая программа составлена с учетом Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01. «Информационная безопасность», утвержденного приказом Министерства образования и науки Российской Федерации «01» декабря 2016 г. № 1515.

## СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ .....	4
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО .....	4
3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	4
4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ .....	6
5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО И РУБЕЖНОГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ .....	8
Вопросы контроля самостоятельной работы студентов.....	11
6. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ.....	15
7. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ .....	17
7.1. Нормативно-правовая база.....	17
7.2. Основная литература .....	17
7.3. Дополнительная литература .....	18
7.4. Периодические издания .....	18
7.5. Интернет-ресурсы .....	19
7.6. Современные профессиональные базы данных.....	19
7.7. Методические указания по проведению различных учебных занятий и другим видам самостоятельной работы.....	19
8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.....	25
ПРИЛОЖЕНИЕ .....	<b>Ошибка! Закладка не определена.</b>

## 1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины являются формирование знаний о базовых классах вредоносных программ, принципах действия антивирусных средств и технологии защиты от вирусов, необходимых для профессионального решения проблем информационной безопасности в условиях становления современного информационного общества.

Задачи дисциплины:

- формирование знаний о базовых классах вредоносных программ;
- формирование знаний, умений и навыков о принципах действия антивирусных средств и технологии защиты от вирусов.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Антивирусные системы защиты информации» относится к дисциплинам по выбору студентов учебного плана по направлению подготовки ВО 10.03.01 «Информационная безопасность», профиль: Организация и технология защиты информации.

Дисциплине «Антивирусные системы защиты информации» предшествуют дисциплины: «Основы информационной безопасности», «Теория и методология информационной безопасности», «Программно - аппаратные средства защиты информации».

Освоение данной дисциплины, в свою очередь, необходимо для успешной научной и практической деятельности после окончания университета.

## 3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты освоения основной образовательной программы высшего профессионального образования (ОПОП ВО) бакалавриата определяются приобретаемыми выпускником компетенциями, т.е. его способностью применять знания, умения и личные качества в соответствии с задачами профессиональной деятельности.

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по направлению подготовки 10.03.01 «Информационная безопасность»:

а) общепрофессиональными компетенциями (ОПК):

способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7);

б) профессиональными компетенциями (ПК):

способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2).

В результате освоения дисциплины обучающийся должен:

Знать:

- цели, задачи, принципы и основные направления обеспечения информационной безопасности предприятия, угрозы предприятия на основе анализа структуры и содержания информационных процессов его, угрозы информационной безопасности государства, содержание информационной войны, методы и средства ее ведения, понимать угрозы безопасности информации, методы анализа структуры и особенности функционирования объекта защиты,

принципы организации информационных систем в соответствии с требованиями по защите информации.

- современные средства программного системного, прикладного и специального назначения, инструментальные средства языки и системы программирования.
- как программно реализовать алгоритмы решения типовых задач обеспечения информационной безопасности;
- основные методы, инструменты и типовые методики разработки программного обеспечения;
- программные средства системного, прикладного и специального назначения, инструментальные средств, языки и системы программирования для решения профессиональных задач;
- основные понятия и методы математической логики и теории алгоритмов, теории информации и кодирования, математические методы обработки экспериментальных данных

Уметь:

- применять современные подходы к построению систем защиты информации, выбирать и анализировать показатели качества и критерии оценки систем информационного нападения и систем защиты информации, определять информационные ресурсы, подлежащие защите, проводить классификацию объектов и субъектов информационных систем.
- применять программные средства системного, прикладного и специального назначения, инструментальные средств, языки и системы программирования для решения профессиональных задач;
- использовать основные методы и инструменты разработки и моделирования программного обеспечения;
- использовать инструментальные средства и системы программирования для решения профессиональных задач;

Владеть:

- навыками формальной постановки и решения задачи обеспечения информационной безопасности, навыками определения возможных путей нейтрализации угроз, принципами распределения прав и ответственности при организации доступа к объектам.
- навыками применения современных программных средств для решения профессиональных задач информационной безопасности на основе использования микроконтроллеров;
- навыками применения программных средств системного, прикладного и специального назначения, инструментальных средств, языков и систем программирования для решения профессиональных задач;
- способностью сбора и проведения анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;
- основными методами и инструментами разработки и моделирования программного обеспечения;

- методами использования основных приемов обработки и представления экспериментальных данных; организации технического обслуживания и настройки СНС

#### 4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

В таблице 1 приводится описание содержания дисциплины, структурированное по разделам, с указанием по каждому разделу формы текущего контроля: защита лабораторной работы (ЛР), коллоквиум (К), рубежный контроль (РК), тестирование (Т).

Таблица 1

	Наименование раздела	Содержание раздела/ темы	Код контролируемой компетенции (или ее части)	Форма текущего контроля
1	<i>Введение</i>	Понятие «вирус» и «антивирус». История развития вирусов и начало «борьбы» с ними. Средства защиты информации. Области применения.	ОПК-7	К, Т, ЛР
2	<i>История компьютерных вирусов</i>	Понятия «компьютерный вирус», атака, утечка информации. Способы обнаружения вирусов.	ОПК-7	К, Т, ЛР
3	<i>Классификация вирусов</i>	Основные классы вирусов.	ОПК-7	К, Т, ЛР
4	<i>Признаки присутствия на компьютере вредоносных программ</i>	Программные и аппаратные средства обнаружения вирусов. Виды вирусов. ПО для защиты информации.	ОПК-7, ПК-2	К, Т, ЛР
5	<i>Основные признаки присутствия на компьютере вредоносных программ</i>	Типы компьютерных вирусов. Методы обнаружения атак на ПК. Форматы вирусных файлов.	ОПК-7, ПК-2	К, Т, ЛР
6	<i>Методы защиты от вредоносных программ</i>	Специфика использования антивирусов. Методы проверки ПК.	ПК-2	К, Т, ЛР
7	<i>Основы работы антивирусных программ.</i>	Последовательность работы продукта - антивируса. Основные приемы и инструменты, используемые для защиты ПК. Основные виды защиты и методов «лечения» файлов.	ПК-2	К, Т, ЛР
8.	<i>Классификация антивирусов</i>	Стандартные антивирусы, их достоинства и недостатки.	ПК-2	К, Т, ЛР
9.	<i>Антивирусная защита компьютерной сети.</i>	Обзор антивирусов обеспечивающих сетевую защиту.	ПК-2	К, Т, ЛР
10.	<i>Антивирусная защита персонального компьютера</i>	Обзор антивирусов обеспечивающих защиту ПК	ПК-2	К, Т, ЛР
11.	<i>Антивирусная защита мобильных пользователей.</i>	Обзор антивирусных программ для защиты смартфонов, на базе ОС Android и других мобильных устройств.	ПК-2	К, Т, ЛР

#### Структура дисциплины

Таблица 2. Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 часов).

Вид работы	Трудоемкость, часы	
	7 семестр	Всего

<b>Общая трудоемкость (в часах)</b>	<b>144</b>	<b>144</b>
<b>Контактная работа (в часах):</b>	56	56
<i>Лекционные занятия (Л)</i>	28	28
<i>Практические занятия (ПЗ)</i>	28	28
<i>Семинарские занятия (СЗ)</i>		
<i>Лабораторные работы (ЛР)</i>		
<b>Самостоятельная работа (в часах):</b>	61	61
Курсовая работа (КР)/ Курсовой проект (КП)		
Самостоятельное изучение разделов/тем	61	61
<b>Подготовка и прохождение промежуточной аттестации</b>	27	27
<b>Вид промежуточной аттестации</b>	<b>экзамен</b>	<b>экзамен</b>

Таблица 3. Лекционные занятия

<b>№ п/п</b>	<b>Тема</b>
1.	<i>История компьютерных вирусов</i>
2.	<i>Классификация вирусов</i>
3.	<i>Признаки присутствия на компьютере вредоносных программ</i>
4.	<i>Основные признаки присутствия на компьютере вредоносных программ</i>
5.	<i>Методы защиты от вредоносных программ</i>
6.	<i>Основы работы антивирусных программ.</i>
7.	<i>Классификация антивирусов</i>
8.	<i>Антивирусная защита компьютерной сети.</i>
9.	<i>Антивирусная защита персонального компьютера</i>
10.	<i>Антивирусная защита мобильных пользователей.</i>

Таблица 4. Практические занятия

<b>№ п/п</b>	<b>Тема</b>
1.	ПО BitDefender
2.	ПО Avira
3.	ПО Dr.Web Security Space Pro
4.	ПО Emsisoft
5.	ПО Eset Smart Security
6.	ПО F-Secure
7.	ПО Kaspersky Internet Security
8.	ПО McAfee Internet Security
9.	ПО Microsoft Security Essentials 4.6
10.	ПО Online Solutions Security Suite
11.	ПО PC Tools Internet Security
12.	ПО Sophos Anti-Virus

Таблица 5. Самостоятельное изучение разделов дисциплины

<b>№ п/п</b>	<b>Вопросы, выносимые на самостоятельное изучение</b>
1.	Новые технологии в методах защиты информации.
2.	Объектно-ориентированные технологии защиты информации.
3.	Антивирусные системы с облачной архитектурой

4.	DOS вирусы;
5.	WINDOWS вирусы;
6.	MACRO вирусы;
7.	NIX вирусы.
8.	Компьютерные вирусы: методы распространения, профилактика заражения
9.	Антивирусные программы.
10.	Компьютерные вирусы. Разновидности вирусов.
11.	Меры защиты информации от компьютерных вирусов.
12.	Информации в компьютерных сетях.

## 5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО И РУБЕЖНОГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Формы контроля текущих, рубежных и промежуточных знаний студентов по дисциплине определяются в соответствии с учебным планом образовательной программы и в соответствии с действующим Положением о балльно-рейтинговой системе оценки успеваемости студентов КБГУ.

От обучающихся требуется посещение занятий, выполнение лабораторных работ, знакомство с рекомендованной литературой.

При аттестации обучающихся оценивается качество работы на занятиях (умение вести дискуссию, способность четко и ёмко формулировать свои мысли), уровень подготовки к самостоятельной деятельности, качество выполнения заданий (презентаций, докладов, выполнение лабораторных работ и др.).

Конечными результатами освоения программы дисциплины являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего семестра по этапам в рамках различного вида занятий и самостоятельной работы.

### 5.1. Оценочные материалы для текущего контроля.

Цель текущего контроля – оценка результатов работы в семестре и обеспечение своевременной обратной связи, для коррекции обучения, активизации самостоятельной работы обучающегося. Объектом текущего контроля являются конкретизированные результаты обучения (учебные достижения) по дисциплине.

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины, оценка качества подготовки на основании выполненных заданий ведется преподавателем (с обсуждением результатов), баллы

#### **Критерии формирования оценок (оценивания) устного опроса**

Устный опрос является одним из основных способов учёта знаний обучающегося по дисциплине. Развёрнутый ответ должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения.

В результате устного опроса знания, обучающегося оцениваются по следующей шкале:

<b>3 балла</b>	<b>2 балла</b>	<b>1 балл</b>	<b>0 баллов</b>
----------------	----------------	---------------	-----------------



<p>ставится, если обучающийся:</p> <p>1) полно излагает изученный материал, даёт правильное определенное экономических понятий;</p> <p>2) обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные;</p> <p>3) излагает материал последовательно и правильно с точки зрения норм литературного языка.</p>	<p>ставится, если обучающийся даёт ответ, удовлетворяющий тем же требованиям, что и для балла «1», но допускает 1-2 ошибки, которые сам же исправляет, и 1-2 недочёта в последовательности и языковом оформлении излагаемого.</p>	<p>ставится, если обучающийся обнаруживает знание и понимание основных положений данной темы, но:</p> <p>1) излагает материал неполно и допускает неточности в определении понятий;</p> <p>2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры;</p> <p>3) излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.</p>	<p>ставится, если обучающийся обнаруживает незнание большей части соответствующего раздела изучаемого материала, допускает ошибки в формулировке.</p>
--	---	--	---

Баллы «1», «2», «3» могут ставиться не только за единовременный ответ, но и за рассредоточенный во времени, т.е. за сумму ответов, данных на протяжении занятия. начисляются в зависимости от сложности задания.

## **5.2. Оценочные материалы для самостоятельной работы обучающегося ( типовые задачи) (при наличии)**

Рабочая программа предусматривает проведение лекционных, лабораторных занятий, а также самостоятельную работу обучающихся. В ФГБОУ ВО «Кабардино-Балкарский государственный университет» действует балльно-рейтинговая система оценки учебных достижений, обучающихся по образовательным программам, реализуемым на основании федеральных государственных образовательных стандартов. Балльно-рейтинговая система оценки знаний является одной из составляющих системы управления качеством образовательной деятельности в университете.

### ***Вопросы, выносимые на коллоквиум*** **(контролируемая компетенция ОПК-5, ПК-2)**

#### **1 точка:**

1. Понятие «вирус» и «антивирус».
2. История развития вирусов и начало «борьбы» с ними.
3. Средства защиты информации.
4. Области применения.
5. Понятия «компьютерный вирус», атака, утечка информации.
6. Способы обнаружения вирусов.
7. Основные классы вирусов.
8. Программные и аппаратные средства обнаружения вирусов.
9. Виды вирусов.
10. ПО для защиты информации.

## **2 точка:**

1. Типы компьютерных вирусов.
2. Методы обнаружения атак на ПК.
3. Форматы вирусных файлов.
4. Специфика использования антивирусов.
5. Методы проверки ПК.
6. Последовательность работы продукта - антивируса.
7. Основные приемы и инструменты, используемые для защиты ПК.
8. Основные виды защиты и методов «лечения» файлов.

## **3 точка:**

1. Стандартные антивирусы, их достоинства и недостатки.
2. Обзор антивирусов обеспечивающих сетевую защиту.
3. Обзор антивирусов, обеспечивающих защиту ПК.
4. Обзор антивирусных программ для защиты смартфонов, на базе ОС Android и других мобильных устройств.

### ***Примеры тестовых заданий на 1 точку:***

**Полный перечень тестовых заданий представлен в ЭОИС  
(контролируемая компетенция ОПК-5, ПК-2)**

I:

S: ... информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

- -: Угроза
- +: Защита
- -: Сохранение

I:

S: В число логических атак на смарт-карты входят:

- + : отслеживание зависимостей между входными данными операций, выполняемых смарт-картой, и результатами
- + : использование некорректных входных данных
- : нарушение целостности данных, передаваемых смарт-картой

I:

S: В число основных понятий обобщенного прикладного программного интерфейса службы безопасности входят:

- +: механизм безопасности
- -: сервис безопасности
- +: контекст безопасности

### ***Примеры тестовых заданий на 2 точку:***

**Полный перечень тестовых заданий представлен в ЭОИС  
(контролируемая компетенция ОПК-5, ПК-2)**

I:

S: ... безопасности информации в современных системах её обработки определяются умышленными (преднамеренные угрозы) и естественными (непреднамеренные угрозы).

- + : Угрозы
- : Имитозащита

-: Гамирование

I:

S: В число основных понятий обобщенного прикладного программного интерфейса службы безопасности входят:

+: удостоверение

-: билет

-: мандат

I:

S: Угрозы безопасности информации в современных системах её обработки определяются умышленными (преднамеренные угрозы) и (непреднамеренные угрозы).

+: Естественными

-: Ложными

-: Неестественными

### **Примеры тестовых заданий на 3 точку:**

**Полный перечень тестовых заданий представлен в ЭОИС  
(контролируемая компетенция ОПК-5, ПК-2)**

I:

S: ... - разработка методов подтверждения подлинности сторон и самой информации в процессе информационного взаимодействия

- -: Имитозащита

- +: Обеспечение аутентификации

- -: Обеспечение конфиденциальности

I:

S: Осуществление угроз информационной безопасности может быть произведено: через ... в органах коммерческих структур, государственного управления, имеющих возможность получения конфиденциальной информации

- -: Шпионов

- +: Агентурные источники

- -: Вредоносных программ

I:

S: Установление градаций важности защиты защищаемой информации (объекта защиты) называют ... защищаемой информации

- -: Атакой

- +: Категорированием

- -: Составлением

### **Вопросы контроля самостоятельной работы студентов (контролируемая компетенция ОПК-5, ПК-2)**

1. Технические аспекты безопасности компьютерных данных.
2. Резервное копирование пользовательских данных.
3. Создание резервных копий системы.
4. Разграничение доступа.
5. Сетевые настройки. Настройка брандмауэра Windows.
6. Настройка системных функций защиты ПК.
7. ПО Kaspersky Internet Security.

8. ПО F-Secure Internet Security.
9. ПО Dr. Web Security Space.
10. ПО BitDefender Internet Security.

### 5.3. Формы и содержание рубежного контроля

Рубежный и промежуточный контроль освоения студентом дисциплины осуществляется в рамках балльно-рейтинговой системы. Распределение баллов в соответствии с действующим Положением о балльно-рейтинговой системе оценки успеваемости студентов КБГУ приведено в таблице 7.

Таблица 7

Распределение баллов в соответствии с действующим Положением о балльно-рейтинговой системе

№ рейтинговой точки	Коллоквиум	Лаб.практикум	Посещаемость	Тестирование	Итого
1	7	8	3	5	23
2	7	8	3	5	23
3	7	8	4	5	24

Таблица 8

#### Критерии оценки

Вид мероприятия	Критерии оценки	Баллы
Коллоквиум (устный опрос по теме)	- ясность, четкость и доказательность изложения ответов на вопросы; - владение специальными терминами; - системность знаний по тематике	0-21 балл
Лабораторное занятие	- понимание цели и задач работы - выполнение заданий и обработка результатов - отчет и защита лабораторной работы	0-24 балла
Компьютерное тестирование по разделам дисциплины	Результаты тестирования (Количество баллов = 5*φ, φ - доля правильно отвеченных тестов по теме).	0-15 баллов
Посещение занятий	При более 3 пропусках без уважительной причины занятий аннулируются баллы	0-10 баллов
Экзамен	ясность, четкость и доказательность изложения ответов на вопросы; - владение специальными терминами; - системность знаний по тематике дисциплины в целом	0-30 баллов
Итоговая оценка		0-100 баллов

#### Вопросы, выносимые на экзамен (контролируемые компетенции ОПК-7, ПК-2)

1. Защита информации от компьютерных вирусов.
2. Компьютерные вирусы: методы распространения, профилактика заражения.
3. Антивирусные программы.
4. Компьютерные вирусы. Разновидности вирусов.
5. Меры защиты информации от компьютерных вирусов.
6. Классификация вирусов.
7. Признаки присутствия на компьютере вредоносных программ.
8. Основные признаки присутствия на компьютере вредоносных программ.

9. Методы защиты от вредоносных программ.
10. Основы работы антивирусных программ.
11. Классификация антивирусов.
12. Антивирусная защита компьютерной сети.
13. Антивирусная защита домашнего компьютера.
14. Антивирусная защита мобильных пользователей.
15. Обновление антивирусных баз.
16. DOS вирусы.
17. WINDOWS вирусы.
18. MACRO вирусы.
19. Unix вирусы.
20. Создание защищенных каналов передачи данных.
21. Обеспечение защиты программ от взлома.
22. Защита информации в компьютерных сетях.
23. Несанкционированный доступ.
24. Закон «Об информации, информатизации и защите информации»
25. Классификация угроз безопасности информации при обработке и хранении
26. Технические аспекты безопасности компьютерных данных.
27. Резервное копирование пользовательских данных.
28. Создание резервных копий системы.
29. Разграничение доступа.
30. Сетевые настройки. Настройка брандмауэра Windows.
31. Настройка системных функций защиты ПК.
32. ПО Kaspersky Internet Security.
33. ПО F-Secure Internet Security.
34. ПО Dr. Web Security Space.
35. ПО BitDefender Internet Security.
36. Информация, относящаяся к государственной тайне.
37. Персональные данные.
38. Информация, составляющая коммерческую тайну.
39. Объекты информационной безопасности.
40. Информационные системы и их классификация.
41. Информационные процессы.
42. Случайные и целенаправленные угрозы нарушения сохранности информации.
43. Дезинформация.
44. Риски ИБ.
45. Информационное оружие.
46. Информационные войны.
47. Технические средства промышленного шпионажа.
48. Критерии безопасности.
49. «Оранжевая книга» США.
50. Классы безопасности.
51. Аудит информационной безопасности.
52. История хакерства.
53. Хакерство в России.
54. Правовые механизмы защиты информации на разных уровнях.
55. Понятие тайны, секрета и конфиденциальности.
56. Задачи и способ функционирования межсетевого экрана.
57. Политика безопасности администратора сети и брандмауэра.
58. Цели интеграции межсетевых экранов.
59. Определите три цели безопасности.

60. Укажите различие между пассивными и активными атаками на секретную информацию.
61. Перечислите и определите пять служб безопасности.
62. Определите восемь механизмов безопасности.

### **Контроль курсовых работ**

Курсовые работы не предусмотрены.

#### **Критерии формирования оценок по промежуточной аттестации**

**Оценка «отлично» – от 91 до 100 баллов** – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы. Все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному. На экзамене студент демонстрирует глубокие знания предусмотренного программой материала, умеет четко, лаконично и логически последовательно отвечать на поставленные вопросы.

**Оценка «хорошо» – от 81 до 90 баллов** – теоретическое содержание курса освоено, необходимые практические навыки работы сформированы, выполненные учебные задания содержат незначительные ошибки. На экзамене студент демонстрирует твердые знания основного (программного) материала, умеет четко, грамотно, без существенных неточностей отвечать на поставленные вопросы.

**Оценка «удовлетворительно» – от 61 до 80 баллов** – теоретическое содержание курса освоено не полностью, необходимые практические навыки работы сформированы частично, выполненные учебные задания содержат грубые ошибки. На экзамене студент демонстрирует знание только основного материала, ответы содержат неточности, слабо аргументированы, нарушена последовательность изложения материала.

**Оценка «неудовлетворительно» – от 36 до 60 баллов** – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к существенному повышению качества выполнения учебных заданий. На экзамене студент демонстрирует незнание значительной части программного материала, существенные ошибки в ответах на вопросы, неумение ориентироваться в материале, незнание основных понятий дисциплины.

#### **Методические рекомендации для подготовки к экзамену**

Экзамен в 8-м семестре является формой итогового контроля знаний и умений студентов по данной дисциплине, полученных на лекциях, лабораторных занятиях и в процессе самостоятельной работы. К экзамену допускаются студенты, набравшие не менее 36 баллов по итогам текущего и промежуточного контроля. На экзамене студент может набрать от 15 до 30 баллов.

В период подготовки к экзамену студенты вновь обращаются к учебно-методическому материалу и закрепляют промежуточные знания.

Подготовка студента к экзамену включает три этапа:

- самостоятельная работа в течение семестра;
- непосредственная подготовка в дни, предшествующие экзамену по темам курса;
- подготовка к ответу на экзаменационные вопросы.

При подготовке к экзамену студентам целесообразно использовать материалы лекций, учебно-методические комплексы, нормативные документы, основную и дополнительную литературу.

На экзамен выносится материал в объеме, предусмотренном рабочей программой учебной дисциплины за семестр. Экзамен проводится в устной форме.

При проведении экзамена в письменной (устной) форме ведущий преподаватель составляет экзаменационные билеты, которые включают в себя: тестовые задания; теоретические задания; задачи или ситуации. Формулировка теоретических задания совпадает с формулировкой перечня экзаменационных вопросов, доведенного до сведения студентов накануне экзаменационной сессии. Содержание вопросов одного билета относится к различным разделам программы с тем, чтобы более полно охватить материал учебной дисциплины.

В аудитории, где проводится экзамен, должно одновременно находиться не более шести студентов на одного преподавателя, принимающего экзамен. На подготовку ответа на билет на экзамене отводится 20 минут.

При проведении письменного экзамена на работу отводится 60 минут.

## 6. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ

Общий балл текущего и рубежного контроля складывается из следующих составляющих (приложение 2). Критерием оценки уровня сформированности компетенций в рамках учебной дисциплин в 8 семестре является экзамен. Целью промежуточных аттестаций по дисциплине является оценка качества освоения дисциплины обучающимися. Типовые задания, обеспечивающие формирование компетенции ОПК-7, ПК-2 представлены в таблице 9.

Таблица 9. Результаты освоения учебной дисциплины, подлежащие проверке.

Результаты обучения (компетенции)	Основные показатели оценки результатов обучения	Вид оценочного материала
Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)	<u>Знать:</u> цели, задачи, принципы и основные направления обеспечения информационной безопасности предприятия, угрозы предприятия на основе анализа структуры и содержания информационных процессов его, угрозы информационной безопасности государства, содержание информационной войны, методы и средства ее ведения, понимать угрозы безопасности информации, методы анализа структуры и особенности функционирования объекта защиты, принципы организации информационных систем в соответствии с требованиями по защите информации.	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)
	<u>Уметь:</u> применять современные подходы к построению систем защиты информации, выбирать и анализировать показатели качества и критерии оценки систем информационного нападения и систем защиты информации, определять информационные ресурсы, подлежащие защите, проводить классификацию	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)

	объектов и субъектов информационных систем.	
	<u>Владеть:</u> навыками формальной постановки и решения задачи обеспечения информационной безопасности, навыками определения возможных путей нейтрализации угроз, принципами распределения прав и ответственности при организации доступа к объектам.	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)
способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)	<u>Знать:</u> современные средства программного системного, прикладного и специального назначения, инструментальные средства языки и системы программирования. как программно реализовать алгоритмы решения типовых задач обеспечения информационной безопасности; основные методы, инструменты и типовые методики разработки программного обеспечения; программные средства системного, прикладного и специального назначения, инструментальные средств, языки и системы программирования для решения профессиональных задач; основные понятия и методы математической логики и теории алгоритмов, теории информации и кодирования, математические методы обработки экспериментальных данных	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)
	<u>Уметь:</u> применять программные средства системного, прикладного и специального назначения, инструментальные средств, языки и системы программирования для решения профессиональных задач; использовать основные методы и инструменты разработки и моделирования программного обеспечения; использовать инструментальные средства и системы программирования для решения профессиональных задач	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)
	<u>Владеть:</u> навыками применения современных программных средств для решения профессиональных задач информационной безопасности на основе использования микроконтроллеров; навыками применения программных средств системного, прикладного и	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)



	<p>специального назначения, инструментальных средств, языков и систем программирования для решения профессиональных задач; способностью сбора и проведения анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; основными методами и инструментами разработки и моделирования программного обеспечения; методами использования основных приемов обработки и представления экспериментальных данных; организации технического обслуживания и настройки СНС.</p>	
--	---	--

## 7. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 7.1. Нормативно-правовая база

1. Федеральный закон от 29 июня 2015 г. № 188-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и статью 14 Федерального закона "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд"»
2. Федеральный закон от 05 апреля 2013 г. № 44-ФЗ (ред. от 31.12.2014) «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;
3. Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;
4. Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
5. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»;
6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
7. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
8. Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
9. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;
10. Федеральный закон от 07 июля 2003 г. № 126-ФЗ «О связи»;
11. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»

### 7.2. Основная литература

1. Прокушев Я.Е. Программно-аппаратные средства защиты информации: учебное пособие / Я.Е. Прокушев. СПб.: Интермедия, 2017. — 160 с. <http://www.iprbookshop.ru/66799.html>
2. Помешкин А.А. Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса «SECRET NET 5.0»: учебно-методическое пособие / А.А. Помешкин, И.В. Коротких. Новосибирск: Новосибирский

государственный технический университет, 2012. — 47 с.  
<http://www.iprbookshop.ru/45015.html>

3. Горев А.И. Обработка и защита информации в компьютерных системах: учебно-практическое пособие / А.И. Горев, А.А. Симаков. Омск: Омская академия МВД России, 2016. — 88 с. <http://www.iprbookshop.ru/72856.html>
4. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства/ В.Ф. Шаньгин. Саратов: Профобразование, 2017. — 544 с. <http://www.iprbookshop.ru/63592.html>

### **7.3.Дополнительная литература**

1. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие / С.В. Петров, П.А. Кисляков. — Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015. — 326 с. — 978-5-906-17271-6. — Режим доступа: <http://www.iprbookshop.ru/33857.html>
2. Горюхина Е.Ю. Информационная безопасность [Электронный ресурс]: учебное пособие / Е.Ю. Горюхина, Л.И. Литвинова, Н.В. Ткачева. — Электрон. текстовые данные. — Воронеж: Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2015. — 221 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/72672.html>
3. Фомин Д.В. Информационная безопасность [Электронный ресурс]: учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика» / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 125 с. — 978-5-4487-0299-0. — Режим доступа: <http://www.iprbookshop.ru/77318.html>

### **7.4.Периодические издания**

1. <http://pravo.gov.ru/> Официальный интернет-портал правовой информации
2. PCI Security Standards Council – <http://www.pcisecuritystandards.org>.
3. Стандарты информационной безопасности в кредитно-финансовой сфере. Стандарты Банка России – <http://www.abiss.ru/doc>
4. Threatpost <https://threatpost> Сайт об информационной безопасности от Kaspersky Lab. Авторитетный источник, на который ссылаются ведущие новостные агентства, такие как The New York Times и The Wall Street Journal.
5. Security Lab <http://www.securitylab.ru/> Проект компании Positive Technologies. Помимо новостей, экспертных статей, софта, форума, на сайте есть раздел, где оперативно публикуется информация об уязвимостях, а также даются конкретные рекомендации по их устранению.
6. Anti-Malware <https://www.anti-malware.ru/> Информационно-аналитический центр, посвященный информационной безопасности. Anti-Malware проводит сравнительные тесты антивирусов, публикует аналитические статьи, эксперты принимают участие в дискуссиях на форуме.
7. Информационная безопасность банков <https://ib-bank.ru/> Отраслевой портал
8. <http://VOID.RU> Сайт VOID.RU представляет собою независимую прессу, освещающую вопросы информационной безопасности - уязвимостей в программном обеспечении, технологий сбора информации, технологий сохранения целостности систем.

9. <http://Security.NNOV.ru> Security.NNOV является одним из наиболее посещаемых Российских ресурсов посвященных информационной безопасности и безопасности IT технологий и доступен как на русском, так и на английском языках.

### **7.5.Интернет-ресурсы**

1. Защита от компьютерных вирусов. Антивирусные программы [Электронный ресурс] – [www.lessons-tva.info/edu/e-inf1/e-inf1-4-1-3.html](http://www.lessons-tva.info/edu/e-inf1/e-inf1-4-1-3.html)
2. Антивирусная защита информации: способы и средства- <https://www.google.ru/webhpsourceid=chrome-instant&ion=1&espv>

### **7.6.Современные профессиональные базы данных**

1. База данных Science Index (РИНЦ) <http://elibrary.ru>
2. Национальная электронная библиотека РГБ <https://нэб.рф>
3. Крупнейшая единая база данных, содержащая аннотации и информацию о цитируемости рецензируемой научной литературы, со встроенными инструментами отслеживания, анализа и визуализации данных. [www.scopus.com](http://www.scopus.com)

### **7.7.Методические указания по проведению различных учебных занятий и другим видам самостоятельной работы**

#### **Методические рекомендации при работе над конспектом во время проведения лекции**

В процессе лекционных занятий целесообразно конспектировать учебный материал. Для этого используются общие и утвердившиеся в практике правила, и приемы конспектирования лекций:

Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист которой должен иметь поля, на которых делаются пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Целесообразно записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки, красные строки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные карандаши и фломастеры.

Названные в лекции ссылки на первоисточники надо пометить на полях, чтобы при самостоятельной работе найти и вписать их. В конспекте дословно записываются определения понятий, категорий и законов. Остальное должно быть записано своими словами.

Каждому студенту необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий.

#### ***Методические рекомендации при подготовке к коллоквиуму***

- проработать конспекты лекций по вопросам коллоквиума;
- прочитать основную и дополнительную литературу, рекомендованную по изучаемым вопросам;
- ответить на вопросы коллоквиума;
- при затруднениях, проконсультироваться с преподавателем.

#### ***Критерии оценивания***

Оценка			
неудовлетворительно	удовлетворительно	хорошо	отлично

<b>2 балла</b>	<b>4 балла</b>	<b>6 баллов</b>	<b>8 баллов</b>
Студент не знает значительной части вопросов, допускает существенные ошибки в ответах на вопросы.	Студент поверхностно знает вопросы коллоквиума, допускает неточности в ответе на вопрос	Студент хорошо знает материал, грамотно и по существу излагает его, допуская некоторые неточности в ответе на вопрос.	Студент в полном объеме знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.

### ***Методические рекомендации по организации самостоятельной работы***

Самостоятельная работа (по В.И. Далю «самостоятельный – человек, имеющий свои твердые убеждения») осуществляется при всех формах обучения: очной и заочной.

Самостоятельная работа обучающихся - способ активного, целенаправленного приобретения студентом новых для него знаний и умений без непосредственного участия в этом процесса преподавателей. Повышение роли самостоятельной работы обучающихся при проведении различных видов учебных занятий предполагает:

- оптимизацию методов обучения, внедрение в учебный процесс новых технологий обучения, повышающих производительность труда преподавателя, активное использование информационных технологий, позволяющих обучающемуся в удобное для него время осваивать учебный материал;
- широкое внедрение компьютеризированного тестирования;
- совершенствование методики проведения практик и научно-исследовательской работы обучающихся, поскольку именно эти виды учебной работы в первую очередь готовят обучающихся к самостоятельному выполнению профессиональных задач;
- модернизацию системы курсового и дипломного проектирования, которая должна повышать роль студента в подборе материала, поиске путей решения задач.

Самостоятельная работа приводит студента к получению нового знания, упорядочению и углублению имеющихся знаний, формированию у него профессиональных навыков и умений. Самостоятельная работа выполняет ряд функций:

- развивающую;
- информационно-обучающую;
- ориентирующую и стимулирующую;
- воспитывающую;
- исследовательскую.

В рамках курса выполняются следующие виды самостоятельной работы:

1. Проработка учебного материала (по конспектам, учебной и научной литературе);
2. Выполнение разноуровневых задач и заданий;
3. Работа с тестами и вопросами для самопроверки;
4. Выполнение итоговой контрольной работы.

Студентам рекомендуется с самого начала освоения курса работать с литературой и предлагаемыми заданиями в форме подготовки к очередному аудиторному занятию. При этом актуализируются имеющиеся знания, а также создается база для усвоения нового материала, возникают вопросы, ответы на которые студент получает в аудитории.

Необходимо отметить, что некоторые задания для самостоятельной работы по курсу имеют определенную специфику. При освоении курса студент может пользоваться библиотекой вуза, которая в полной мере обеспечена соответствующей литературой. Значительную помощь в подготовке к очередному занятию может оказать имеющийся в учебно-методическом комплексе краткий конспект лекций. Он же может использоваться и для закрепления полученного в аудитории материала. Самостоятельная работа студентов

предусмотрена учебным планом и выполняется в обязательном порядке. Задания предложены по каждой изучаемой теме и могут готовиться индивидуально или в группе. По необходимости студент может обращаться за консультацией к преподавателю. Выполнение заданий контролируется и оценивается преподавателем.

Для успешного самостоятельного изучения материала сегодня используются различные средства обучения, среди которых особое место занимают информационные технологии разного уровня и направленности: электронные учебники и курсы лекций, базы тестовых заданий и задач. Электронный учебник представляет собой программное средство, позволяющее представить для изучения теоретический материал, организовать апробирование, тренаж и самостоятельную творческую работу, помогающее студентам и преподавателю оценить уровень знаний в определенной тематике, а также содержащее необходимую справочную информацию. Электронный учебник может интегрировать в себе возможности различных педагогических программных средств: обучающих программ, справочников, учебных баз данных, тренажеров, контролирующих программ.

Для успешной организации самостоятельной работы все активнее применяются разнообразные образовательные ресурсы в сети Интернет: системы тестирования по различным областям, виртуальные лекции, лаборатории, при этом пользователю достаточно иметь компьютер и подключение к Интернету для того, чтобы связаться с преподавателем, решать вычислительные задачи и получать знания. Использование сетей усиливает роль самостоятельной работы студента и позволяет кардинальным образом изменить методику преподавания.

Студент может получать все задания и методические указания через сервер, что дает ему возможность привести в соответствие личные возможности с необходимыми для выполнения работ трудозатратами. Студент имеет возможность выполнять работу дома или в аудитории. Большое воспитательное и образовательное значение в самостоятельном учебном труде студента имеет самоконтроль. Самоконтроль возбуждает и поддерживает внимание и интерес, повышает активность памяти и мышления, позволяет студенту своевременно обнаружить и устранить допущенные ошибки и недостатки, объективно определить уровень своих знаний, практических умений. Самое доступное и простое средство самоконтроля с применением информационно-коммуникационных технологий - это ряд тестов «on-line», которые позволяют в режиме реального времени определить свой уровень владения предметным материалом, выявить свои ошибки и получить рекомендации по самосовершенствованию.

#### ***Методические рекомендации по работе с литературой***

Всю литературу можно разделить на учебники и учебные пособия, оригинальные научные монографические источники, научные публикации в периодической печати. Из них можно выделить литературу основную (рекомендуемую), дополнительную и литературу для углубленного изучения дисциплины.

Изучение дисциплины следует начинать с учебника, поскольку учебник – это книга, в которой изложены основы научных знаний по определенному предмету в соответствии с целями и задачами обучения, установленными программой.

При работе с литературой необходимо учитывать, что имеются различные виды чтения, и каждый из них используется на определенных этапах освоения материала.

*Предварительное* чтение направлено на выявление в тексте незнакомых терминов и поиск их значения в справочной литературе. В частности, при чтении указанной литературы необходимо подробнейшим образом анализировать понятия.

*Сквозное чтение* предполагает прочтение материала от начала до конца. Сквозное чтение литературы из приведенного списка дает возможность студенту сформировать свод основных понятий из изучаемой области и свободно владеть ими.

*Выборочное* – наоборот, имеет целью поиск и отбор материала. В рамках данного курса выборочное чтение, как способ освоения содержания курса, должно использоваться при подготовке к практическим занятиям по соответствующим разделам.

*Аналитическое чтение* – это критический разбор текста с последующим его конспектированием. Освоение указанных понятий будет наиболее эффективным в том случае, если при чтении текстов студент будет задавать к этим текстам вопросы. Часть из этих вопросов сформулирована в ФОС в перечне вопросов для собеседования. Перечень этих вопросов ограничен, поэтому важно не только содержание вопросов, но сам принцип освоения литературы с помощью вопросов к текстам.

Целью *изучающего* чтения является глубокое и всестороннее понимание учебной информации. Есть несколько приемов изучающего чтения:

1. Чтение по алгоритму предполагает разбиение информации на блоки: название; автор; источник; основная идея текста; фактический материал; анализ текста путем сопоставления имеющихся точек зрения по рассматриваемым вопросам; новизна.

2. Прием постановки вопросов к тексту имеет следующий алгоритм:

- медленно прочитать текст, стараясь понять смысл изложенного;
- выделить ключевые слова в тексте;
- постараться понять основные идеи, подтекст и общий замысел автора.

3. Прием тезирования заключается в формулировании тезисов в виде положений, утверждений, выводов.

К этому можно добавить и иные приемы: прием реферирования, прием комментирования.

Важной составляющей любого солидного научного издания является список литературы, на которую ссылается автор. При возникновении интереса к какой-то обсуждаемой в тексте проблеме всегда есть возможность обратиться к списку относящейся к ней литературы. В этом случае вся проблема как бы разбивается на составляющие части, каждая из которых может изучаться отдельно от других. При этом важно не терять из вида общий контекст и не погружаться чрезмерно в детали, потому что таким образом можно не увидеть главного.

Подготовка к экзамену должна проводиться на основе лекционного материала, материала практических занятий с обязательным обращением к основным учебникам по курсу. Это позволит исключить ошибки в понимании материала, облегчит его осмысление, прокомментирует материал многочисленными примерами.

### ***Методические рекомендации по написанию рефератов***

Реферат представляет собой сокращенный пересказ содержания первичного документа (или его части) с основными фактическими сведениями и выводами. Написание реферата используется в учебном процессе вуза в целях приобретения студентом необходимой профессиональной подготовки, развития умения и навыков самостоятельного научного поиска: изучения литературы по выбранной теме, анализа различных источников и точек зрения, обобщения материала, выделения главного, формулирования выводов и т. п. С помощью рефератов студент глубже постигает наиболее сложные проблемы курса, учится лаконично излагать свои мысли, правильно оформлять работу, докладывать результаты своего труда. Процесс написания реферата включает: выбор темы; подбор нормативных актов, специальной литературы и иных источников, их изучение; составление плана; написание текста работы и ее оформление; устное изложение реферата.

Рефераты пишутся по наиболее актуальным темам. В них на основе тщательного анализа и обобщения научного материала сопоставляются различные взгляды авторов и определяется собственная позиция студента с изложением соответствующих аргументов. Темы рефератов должны охватывать и дискуссионные вопросы курса. Они призваны отражать передовые научные идеи, обобщать тенденции практической деятельности, учитывая при этом изменения в текущем законодательстве. Рекомендованная ниже тематика рефератов примерная. Студент при желании может сам предложить ту или иную тему, предварительно согласовав ее с научным руководителем.

Реферат, как правило, состоит из введения, в котором кратко обосновывается актуальность, научная и практическая значимость избранной темы, основного материала,

содержащего суть проблемы и пути ее решения, и заключения, где формируются выводы, оценки, предложения. Общий объем реферата 20 листов.

Технические требования к оформлению реферата следующие. Реферат оформляется на листах формата А4, с обязательной нумерацией страниц, причем номер страницы на первом, титульном, листе не ставится. Поля: верхнее, нижнее, правое, левое – 20 мм. Абзацный отступ – 1,25; Рисунки должны создаваться в циклических редакторах или как рисунок Microsoft Word (сгруппированный). Таблицы выполнять табличными ячейками Microsoft Word. Сканирование рисунков и таблиц не допускается. Выравнивание текста (по ширине страницы) необходимо выполнять только стандартными способами, а не с помощью пробелов. Размер текста в рисунках и таблицах – 12 кегль. На титульном листе реферата нужно указать: название учебного заведения, факультета, номер группы и фамилию, имя и отчество автора, тему, место и год его написания. Рекомендуемый объем работы складывается из следующих составляющих: титульный лист (1 страница), содержание (1 страница), введение (1 – 2 страницы), основная часть, которую можно разделить на главы или разделы (10 – 15 страниц), заключение (1 – 3 страницы), список литературы (1 страница), приложение (не обязательно). Если реферат содержит таблицу, то ее номер и название располагаются сверху таблицы, если рисунок, то внизу рисунка.

Содержательные части реферата – это введение, основная часть и заключение. Введение должно содержать рассуждение по поводу того, что рассматриваемая тема актуальна (то есть современна и к ней есть большой интерес в настоящее время), а также постановку цели исследования, которая непосредственно связана с названием работы. Также во введении могут быть поставлены задачи (но не обязательно, так как работа невелика по объему), которые детализируют цель. В заключении пишутся конкретные, содержательные выводы.

Содержание реферата студент докладывает на семинаре, кружке, научной конференции. Предварительно подготовив тезисы доклада, студент в течение 7 - 10 минут должен кратко изложить основные положения своей работы. После доклада автор отвечает на вопросы, затем выступают оппоненты, которые заранее познакомились с текстом реферата, и отмечают его сильные и слабые стороны. На основе обсуждения обучающемуся выставляется соответствующая оценка.

#### ***Методические рекомендации для подготовки к экзамену:***

Экзамен в 7 семестре является формой итогового контроля знаний и умений, обучающихся по данной дисциплине, полученных на лекциях, практических занятиях и в процессе самостоятельной работы. Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой. К экзамену допускаются студенты, набравшие 36 и более баллов по итогам текущего и промежуточного контроля. На экзамене студент может набрать от 15 до 30 баллов.

В период подготовки к экзамену обучающиеся вновь обращаются к учебно-методическому материалу и закрепляют промежуточные знания.

Подготовка обучающегося к экзамену включает три этапа:

- самостоятельная работа в течение семестра;
- непосредственная подготовка в дни, предшествующие экзамену по темам курса;
- подготовка к ответу на экзаменационные вопросы.

При подготовке к экзамену обучающимся целесообразно использовать материалы лекций, учебно-методические комплексы, нормативные документы, основную и дополнительную литературу.

На экзамен выносятся материалы в объеме, предусмотренном рабочей программой учебной дисциплины за семестр. Экзамен проводится в письменной / устной форме.

При проведении экзамена в письменной (устной) форме, ведущий преподаватель составляет экзаменационные билеты, которые включают в себя: тестовые задания; теоретические задания; задачи или ситуации. Формулировка теоретических задания совпадает с формулировкой перечня экзаменационных вопросов, доведенных до сведения обучающихся накануне экзаменационной сессии. Содержание вопросов одного билета относится к

различным разделам программы с тем, чтобы более полно охватить материал учебной дисциплины.

В аудитории, где проводится устный экзамен, должно одновременно находиться не более шести студентов на одного преподавателя, принимающего экзамен. На подготовку ответа на билет на экзамене отводится 40 минут.

При проведении письменного экзамена на работу отводится 60 минут.

Результат устного (письменного) экзамена выражается оценками:

**Оценка «отлично» – от 91 до 100 баллов** – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы. Все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному. На экзамене студент демонстрирует глубокие знания предусмотренного программой материала, умеет четко, лаконично и логически последовательно отвечать на поставленные вопросы.

**Оценка «хорошо» – от 81 до 90 баллов** – теоретическое содержание курса освоено, необходимые практические навыки работы сформированы, выполненные учебные задания содержат незначительные ошибки. На экзамене студент демонстрирует твердые знания основного (программного) материала, умеет четко, грамотно, без существенных неточностей отвечать на поставленные вопросы.

**Оценка «удовлетворительно» – от 61 до 80 баллов** – теоретическое содержание курса освоено не полностью, необходимые практические навыки работы сформированы частично, выполненные учебные задания содержат грубые ошибки. На экзамене студент демонстрирует знание только основного материала, ответы содержат неточности, слабо аргументированы, нарушена последовательность изложения материала.

**Оценка «неудовлетворительно» – от 36 до 60 баллов** – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к существенному повышению качества выполнения учебных заданий. На экзамене студент демонстрирует незнание значительной части программного материала, существенные ошибки в ответах на вопросы, неумение ориентироваться в материале, незнание основных понятий дисциплины.

### ***Методические рекомендации по выполнению лабораторных работ***

Выполнение каждой лабораторной работы складывается из следующих этапов.

1. Самостоятельная подготовка студентов к работе. Перед началом работы студенты должны четко представлять себе цель работы, изучить теоретические сведения к лабораторной работе.

2. Выполнение работы. Этот этап осуществляется в соответствии с методическими указаниями, которые содержатся в описании к каждой работе. Сформулировать выводы по проделанной работе.

3. Составление отчета о проделанной работе. К отчету о выполненной работе предъявляются следующие требования:

Отчет должен содержать исчерпывающие данные, как о цели работы, так и о результатах в следующей последовательности:

- Титульный лист
- цель работы
- задание на лабораторную работу для своего варианта
- ответы на контрольные вопросы
- результаты выполнения работы
- выводы по работе.

4. Защита лабораторной работы с представлением отчета. Защита лабораторной работы проходит в форме свободной беседы по теме лабораторной работы.



### ***Методические рекомендации по подготовке к тестированию***

Тесты – это вопросы или задания, предусматривающие конкретный, краткий, четкий ответ на имеющиеся эталоны ответов. При самостоятельной подготовке к тестированию студенту необходимо:

а) готовясь к тестированию, проработать информационный материал по дисциплине. Проконсультироваться с преподавателем по вопросу выбора учебной литературы;

б) четко выясните все условия тестирования заранее. Знать, сколько тестов Вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.

в) приступая к работе с тестами, внимательно и до конца прочтите вопрос и предлагаемые варианты ответов. Выберите правильные (их может быть несколько). На отдельном листке ответов выпишите цифру вопроса и буквы, соответствующие правильным ответам;

г) в процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант.

д) если Вы встретили чрезвычайно трудный для Вас вопрос, не тратьте много времени на него. Переходите к другим тестам. Вернитесь к трудному вопросу в конце.

е) обязательно оставьте время для проверки ответов, чтобы избежать механических ошибок.

### ***Критерии оценивания***

<b>Оценка</b>			
<b>неудовлетворительно 0 баллов</b>	<b>удовлетворительно 3 балла</b>	<b>хорошо 4 балла</b>	<b>отлично 5 баллов</b>
Менее 50 % правильно выполненных заданий.	50-70% правильно выполненных заданий.	71-85% правильно выполненных заданий.	86-100% правильно выполненных заданий.

## **8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

### **8.1. Требования к материально-техническому обеспечению**

Специализированная аудитория, используемая при проведении занятий лекционного типа №43, №48а, №50, №58 оснащена мультимедийным проектором и комплектом аппаратуры, позволяющей демонстрировать текстовые и графические материалы.

Лаборатории оснащены необходимым оборудованием: Комплект учебного оборудования «Криптографические системы», Комплект учебного оборудования «Сетевая безопасность», Учебно-методическими комплексами VipNet, Microsoft Office, 7-zip, Adobe Acrobat Reader DC и др.

Студенты имеют доступ через Интернет доступ к единому образовательному portalу, где в открытом доступе имеются ресурсы учебно-методической литературы, являющиеся разработками ведущих ВУЗов России.

### **Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья**

Для студентов с ограниченными возможностями здоровья созданы специальные условия для получения образования. В целях доступности получения высшего образования по образовательным программам инвалидами и лицами с ограниченными возможностями здоровья университетом обеспечивается:

1. Альтернативная версия официального сайта в сети «Интернет» для слабовидящих;
  2. Для инвалидов с нарушениями зрения (слабовидящие, слепые):
    - присутствие ассистента, оказывающего обучающемуся необходимую помощь, дублирование вслух справочной информации о расписании учебных занятий; наличие средств для усиления остаточного зрения, брайлевской компьютерной техники, видеоувеличителей, программ невидимого доступа к информации, программ-синтезаторов речи и других технических средств приема-передачи учебной информации в доступных формах для студентов с нарушениями зрения;
    - задания для выполнения на экзамене зачитываются ассистентом;
    - письменные задания выполняются на бумаге, надиктовываются ассистенту обучающимся;
  3. Для инвалидов и лиц с ограниченными возможностями здоровья по слуху (слабослышащие, глухие):
    - на зачете/экзамене присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
    - зачет/экзамен проводится в письменной форме;
  4. Для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, созданы материально-технические условия, обеспечивающие возможность беспрепятственного доступа обучающихся в учебные помещения, объекты питания, туалетные и другие помещения университета, а также пребывания в указанных помещениях (наличие расширенных дверных проемов, поручней и других приспособлений).
    - письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
    - по желанию студента экзамен проводится в устной форме.
- Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

## **Лист переутверждения рабочей программы дисциплины**

Рабочая программа:

одобрена на 2020/2021 учебный год. Протокол № \_\_\_\_ заседания кафедры от «\_\_» \_\_ 2020 г.

Разработчик программы \_\_\_\_\_

Зав. кафедрой \_\_\_\_\_