

УТВЕРЖДАЮ  
 Декан факультета

\_\_\_\_\_  
 (подпись)      Страхов С. Ю.  
 ФИО  
 «\_\_\_» \_\_\_\_\_ 20\_\_

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Направление/специальность подготовки	09.03.01 Информатика и вычислительная техника
Специализация/профиль/программа подготовки	Автоматизированные системы обработки информации и управления
Уровень высшего образования	Бакалавриат
Форма обучения	Очная
Факультет	И Информационных и управляющих систем
Выпускающая кафедра	И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра-разработчик рабочей программы	И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

КУРС	СЕМЕСТР	ОБЩАЯ ТРУДОЁМКОСТЬ (ЗАЧЕТНЫХ ЕДИНИЦ)	ЧАСЫ (по наличию видов занятий)									ВИД ПРОМЕЖУТОЧНОГО КОНТРОЛЯ
			ОБЩАЯ ТРУДОЁМКОСТЬ	АУДИТОРНЫЕ ЗАНЯТИЯ				САМОСТОЯТЕЛЬНАЯ РАБОТА				
				ВСЕГО	ЛЕКЦИИ	ЛАБОРАТОРНЫЙ ПРАКТИКУМ	ПРАКТИЧЕСКИЕ ЗАНЯТИЯ	ВСЕГО	КУРСОВОЙ ПРОЕКТ	КУРСОВАЯ РАБОТА	ДРУГИЕ ВИДЫ САМОСТ. РАБОТЫ	
4	7	4	144	51	34	0	17	93	0	0	93	ЭКЗ.

*ЛИСТ СОГЛАСОВАНИЯ*

РАБОЧАЯ ПРОГРАММА СОСТАВЛЕНА В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФЕДЕРАЛЬНОГО  
ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ (ФГОС ВО)

**09.03.01 Информатика и вычислительная техника**

год набора группы: 2024

Программу составил:

Кафедра И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ  
ТЕХНОЛОГИЙ \_\_\_\_\_

Емельянов Валентин Юрьевич, к.т.н., доцент, доцент

Программа рассмотрена

на заседании кафедры-разработчика

рабочей программы **И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ**

Заведующий кафедрой Матвеев С.А., к.т.н., доц. \_\_\_\_\_

Программа рассмотрена

на заседании выпускающей кафедры

**И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ**

Заведующий кафедрой Матвеев С.А., к.т.н., доц. \_\_\_\_\_

# **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ**

## **Разделы рабочей программы**

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО
3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

## **Приложения к рабочей программе дисциплины**

- Приложение 1. Аннотация рабочей программы
- Приложение 2. Технологии и формы обучения
- Приложение 3. Фонды оценочных средств

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-2 — способность понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности
--

ОПК-3 — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
--

Формированию компетенций служит достижение следующих результатов образования:

### **ОПК-2**

*знания:*

технологий и программных средств защиты информации;

*умения:*

применять полученные знания в практике построения защищенных систем;

*навыки:*

применения, установки и настройки антивирусных систем и систем распознавания угроз и атак.

### **ОПК-3**

*знания:*

основных принципов административно-правовой, программной и технической защиты информации;

*умения:*

быстро реагировать на различные угрозы информационной безопасности, применять современные технологии защиты информации;;

*навыки:*

обнаружения компьютерных вирусов различными способами и применения методов борьбы с вирусами различной природы.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.01 Информатика и вычислительная техника*.

Содержание дисциплины является логическим продолжением дисциплин: **ТЕОРИЯ ИНФОРМАЦИИ И КОДИРОВАНИЕ, БАЗЫ ДАННЫХ, ДИСКРЕТНАЯ МАТЕМАТИКА И МАТЕМАТИЧЕСКАЯ ЛОГИКА**.

Содержание дисциплины является основой для освоения дисциплин: **ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ, ВЫПОЛНЕНИЕ И ЗАЩИТА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-1 — Способен применять естественнонаучные и общетехнические знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности
- ОПК-8 — Способен разрабатывать алгоритмы и программы, пригодные для практического применения
- ОПК-9 — Способен осваивать методики использования программных средств для решения практических задач
- ПК-94 — способен к управлению информацией и данными, поиску источников информации и данных, восприятию, анализу, запоминанию и передаче информации с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач
- ПСК-1.2 — Способен осуществлять концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности
- ПСК-1.4 — Способен разрабатывать аппаратные и программные средства автоматизации обработки информации и управления в технических системах

### 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч.

#### 3.1. Содержание (дидактика) дисциплины

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %	
				ВСЕГО	Лекции	Практические занятия		ОПК-2	ОПК-3
4	7	Раздел 1. Основные составляющие информационной безопасности. 1.1. Основные понятия информационной безопасности. 1.2. Классификация угроз. 1.3. Классификация средств защиты информации. 1.4. Методы и средства организационно-правовой защиты информации. 1.5. Методы и средства инженерно-технической защиты. 1.6. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.	12	4	4	0	8	10	20
4	7	Раздел 2. Правовое обеспечение информационной безопасности. 2.1. Информация, информационные технологии и защита информации. 2.2. Безопасность персональных данных. 2.3. Результаты интеллектуальной деятельности. Авторское право. 2.4. Право промышленной собственности. Коммерческая тайна и правовой режим обеспечения ее безопасности. 2.5. Государственная тайна и ее правовая защита. 2.6. Электронная подпись и правовое обеспечение безопасности переписки. 2.7. Правовое обеспечение безопасности при использовании сетей связи. 2.8. Характеристика и последствия преступлений в сфере информационной безопасности.	18	6	6	0	12	0	20
4	7	Раздел 3. Организационное обеспечение информационной безопасности. 3.1. Государственная система обеспечения информационной безопасности. 3.2. Организация работ по защите конфиденциальной информации. Лицензирование.	6	2	2	0	4	0	5
4	7	Раздел 4. Защита информации в современных информационных системах. 4.1. Способы контактного и бесконтактного съема информации. 4.2. Возможности атаки на ОС, их классификация. 4.3. Парольная защита ПК. Взлом паролей Windows NT и UNIX. Защита от взлома. 4.4.Идентификация и аутентификация пользователей ОС. Windows, UNIX, Linux. 4.5. Формальные модели защищаемых систем и их применение в современных ОС. 4.6. Методы и средства ограничения доступа к ресурсам и компонентам ПК.	44	18	10	8	26	45	25
4	7	Раздел 5. Защита информации в компьютерных сетях. 5.1. Основные угрозы безопасности сетей. Модели угроз и модели противодействия. 5.2. Методы аутентификации пользователей в сети. 5.3. Разновидности вирусных программ. 5.4. Программные средства защиты: сканеры вирусов, сетевая защита, брандмауэры и др. 5.5. Системы обнаружения сетевого вторжения. 5.6. Безопасность глобальных сетей и электронной почты.	64	21	12	9	43	45	30
Всего за 7 семестр			144	51	34	17	93	100	100
Всего по дисциплине			144	51	34	17	93	100	100

#### 3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 4. Защита информации в современных информационных системах.	Разработка защищенных приложений. Программное управление учетной записью.	2
2		Управление правами пользователей.	3
3		Применение механизмов разграничения доступа пользователей.	3
4	Раздел 5. Защита информации в компьютерных сетях.	Моделирование атак в сети и способов их нейтрализации	6
5		Динамическая маршрутизация	3
Всего за 7 семестр			17

#### 3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Основные составляющие информационной безопасности.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	8
2	Раздел 2. Правовое обеспечение информационной безопасности.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	12

3	Раздел 3. Организационное обеспечение информационной безопасности.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	4
4	Раздел 4. Защита информации в современных информационных системах.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	14
5		Подготовка к выполнению практических заданий и оформление отчетов	12
6	Раздел 5. Защита информации в компьютерных сетях.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	28
7		Подготовка к выполнению практических заданий и оформление отчетов	15
Всего за 7 семестр			93

#### 4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

СЕМЕСТР	НЕДЕЛИ СЕМЕСТРА																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
7						ДР		Отч. по ПЗ		ДР						ДР	Отч. по ПЗ, Вопр. Экз

Условные обозначения:

- ДР – диагностическая работа;
- Отч. по ПЗ – отчет по практическому заданию;
- Вопр. Экз – вопросы к экзамену.

**Текущий контроль успеваемости** студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- отчет по практическому заданию;
- вопросы к экзамену.

**Промежуточная аттестация** проводится в формах:

- экзамен.

## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 5.1. Основная литература по дисциплине:

1. А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности. М.: Изд-во МГТУ им. Н. Э. Баумана, 2018, эл. рес.
2. А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности. М.: Изд-во МГТУ им. Н. Э. Баумана, 2018, 30 экз.
3. В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации. СПб.: Питер, 2011, 27 экз.
4. В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность. М.: РУСАЙНС, 2017, 70 экз.
5. Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019, 42 экз.
6. Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019, эл. рес.
7. М. В. Тумбинская, М. В. Петровский. . Комплексное обеспечение информационной безопасности на предприятии. Санкт-Петербург: Лань, 2022, эл. рес.
8. С. А. Нестеров. . Основы информационной безопасности. СПб.: Лань, 2019, 22 экз.
9. С. А. Нестеров. . Основы информационной безопасности. Санкт-Петербург: Лань, 2022, эл. рес.

### 5.2. Дополнительная литература по дисциплине:

не требуется.

### 5.3. Периодические издания:

не требуются.

### 5.4. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины, электронные библиотечные системы:

1. <http://library.voenmeh.ru/jirbis2> — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
2. <http://e.lanbook.com> — ЭБС Лань;
3. <https://urait.ru> — Образовательная платформа «Юрайт». Для вузов и ссузов..

### Современные профессиональные базы данных:

1. <https://rusneb.ru> – Национальная электронная библиотека (НЭБ);
2. <https://cyberleninka.ru/> - Научная электронная библиотека «Киберленинка»;
- <http://www.rfbr.ru/rffi/ru/library> - Полнотекстовая электронная библиотека Российского фонда фундаментальных исследований.

### Информационные справочные системы:

1. Техэксперт – Информационный портал технического регулирования: Нормы, правила, стандарты РФ;
2. [http://library.voenmeh.ru/jirbis2/index.php?option=com\\_irbis&view=irbis&Itemid=457](http://library.voenmeh.ru/jirbis2/index.php?option=com_irbis&view=irbis&Itemid=457) - БД ГОСТов собственной генерации БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова;
3. <http://www.consultant.ru/>- КонсультантПлюс- информационный портал правовой информации.

### 5.5. Программное обеспечение:

1. Microsoft SQL Server 2005 Express Edition;
2. Microsoft Windows.

### 5.6. Информационные технологии:

взаимодействие с обучающимися посредством ЭИОС Moodle БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.



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

### **6.1. Лекционные занятия:**

специализированные требования по оборудованию отсутствуют; аудитория с посадочными местами по количеству студентов; доска.

### **6.2. Практические занятия:**

1. Проектор;
2. Аудитория с числом посадочных мест не меньше количества обучающихся;
3. Microsoft SQL Server 2005 Express Edition;
4. Microsoft Windows.

### **6.3. Прочее:**

1. рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
2. рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

### **Аннотация рабочей программы**

Дисциплина **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.01 Информатика и вычислительная техника*. Дисциплина реализуется на факультете *И Информационных и управляющих систем* БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой *И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ*.

Дисциплина нацелена на формирование *компетенций*:

ОПК-2 способность понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности;

ОПК-3 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Содержание дисциплины охватывает круг вопросов, связанных с основными понятиями и составляющими информационной безопасности, видами угроз и комплексом мер по их нейтрализации.

Программой дисциплины предусмотрены следующие **виды контроля**:

**Текущий контроль успеваемости** студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- отчет по практическому заданию;
- вопросы к экзамену.

**Промежуточная аттестация** проводится в формах:

- экзамен.

Общая трудоемкость освоения дисциплины составляет **4 з.е., 144 ч.** Программой дисциплины предусмотрены лекционные занятия (**34 ч.**), практические занятия (**17 ч.**), самостоятельная работа студента (**93 ч.**).

## ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

### Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 144 ч., из них 51 ч. аудиторных занятий, и 93 ч., отведенных на самостоятельную работу студента.

Рекомендации по распределению учебного времени по видам самостоятельной работы и разделам дисциплины приведены в таблице.

Контроль освоения дисциплины производится в соответствии с Положением о текущем, рубежном контроле успеваемости и промежуточной аттестации обучающихся.

Формы контроля и критерии оценивания приведены в приложении 3 к Рабочей программе.

Наименование работы	Рекомендуемая литература	Трудоемкость, час.
<b>Раздел 1. Основные составляющие информационной безопасности.</b>		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (глава 1) Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (раздел 1) С. А. Нестеров. . Основы информационной безопасности: СПб.: Лань, 2019 (парагр. 1.1-1.3) А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (глава 1)	8
Итого по разделу 1		8
<b>Раздел 2. Правовое обеспечение информационной безопасности.</b>		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (главы 2,4-15) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (главы 2-3)	12
Итого по разделу 2		12
<b>Раздел 3. Организационное обеспечение информационной безопасности.</b>		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	М. В. Тумбинская, М. В. Петровский. . Комплексное обеспечение информационной безопасности на предприятии: Санкт-Петербург: Лань, 2022 (глава 1.1) А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (главы 3,16-18)	4
Итого по разделу 3		4
<b>Раздел 4. Защита информации в современных информационных системах.</b>		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (глава 9) Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (разделы 2-6)	14
Подготовка к выполнению практических заданий и оформление отчетов	С. А. Нестеров. . Основы информационной безопасности: Санкт-Петербург: Лань, 2022 (парагр. 1.4-1.5)	12

	В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (глава 4)	
Итого по разделу 4		26
<b>Раздел 5. Защита информации в компьютерных сетях.</b>		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (глава 20) С. А. Нестеров. . Основы информационной безопасности: Санкт-Петербург: Лань, 2022 (главы 4,5)	28
Подготовка к выполнению практических заданий и оформление отчетов	Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (разделы 7-9,11)	15
Итого по разделу 5		43

## ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств, позволяющие оценить результаты обучения по данной дисциплине, включают в себя:

- диагностическая работа
- вопросы к экзамену;
- отчет по практическому заданию;
- экзамен.

### Критерии оценивания

#### Диагностическая работа

Диагностическая работа проводится в форме теста в ЭИОС Moodle:

- при правильном ответе менее чем на 60% вопросов - не аттестация;
- при правильном ответе на 60% вопросов и более - аттестация.

#### Вопросы к экзамену

Комплект вопросов к экзамену размещен в УМК дисциплины.

#### Отчет по практическому заданию

Требования к выполнению практических заданий (ПЗ):

По всем ПЗ необходимо выполнить поставленную задачу согласно заданию, а также внимательно прочитать сопутствующую информацию о программном обеспечении, в котором осуществляется работа.

Отчет по ПЗ:

По каждому ПЗ необходимо подготовить отчет в электронном виде. После выполнения отчета его необходимо предоставить на проверку преподавателю (либо лично, либо посредством электронной почты). При оформлении отчета руководствоваться ГОСТ 7.32-2017. Состав отчета описывается в постановке задачи каждого ПЗ.

Защита ПЗ:

Защита ПЗ предусматривает обсуждение порядка решения предусмотренных его тематикой задач, включая проверку усвоения студентом соответствующих сведений из теории.

Типовые практические задания включены в состав УМК дисциплины.

Балльная оценка выполненного практического задания определяется технологической картой дисциплины.

#### Экзамен

Итоговый контроль по дисциплине проходит в форме экзамена. Экзаменационный билет включает в себя два теоретических вопроса.

Для студентов, планомерно и успешно освоивших содержание учебной дисциплины, предусматривается возможность оформления экзаменационной оценки по результатам работы в семестре в соответствии с технологической картой дисциплины.

Паспорт фонда оценочных средств

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %		НАИМЕНОВАНИЕ ОЦЕНОЧНОГО СРЕДСТВА
				ВСЕГО	Лекции	Практические занятия		ОПК-2	ОПК-3	
4	7	Раздел 1. Основные составляющие информационной безопасности.	12	4	4	0	8	10	20	Вопросы к экзамену
4	7	Раздел 2. Правовое обеспечение информационной безопасности.	18	6	6	0	12	0	20	Вопросы к экзамену
4	7	Раздел 3. Организационное обеспечение информационной безопасности.	6	2	2	0	4	0	5	Вопросы к экзамену
4	7	Раздел 4. Защита информации в современных информационных системах.	44	18	10	8	26	45	25	Отчет по практическому заданию, Вопросы к экзамену
4	7	Раздел 5. Защита информации в компьютерных сетях.	64	21	12	9	43	45	30	Отчет по практическому заданию, Вопросы к экзамену
Всего за 7 семестр			144	51	34	17	93	100	100	
Всего по дисциплине			144	51	34	17	93	100	100	

## Критерии оценивания

### ОПК-2

*Вопросы открытого типа:*

- № 1 **Условие, при котором в распоряжении аналитика находится возможность получить результат зашифровки для произвольно выбранного им зашифрованного сообщения размера  $n$  используется в анализе:**
- № 2 **Основные отличия протоколов L2TP и PPTP состоят в следующем:**
- № 3 **Назовите отличия концентраторов (hub) от коммутаторов 2-го уровня (switch):**
- № 4 **Служба IPSec может быть использована:**
- № 5 **Что означает MAC-адрес?**
- № 6 **Понятие криптографии. Симметричные и ассиметричные алгоритмы шифрования**
- № 7 **Виды электронной подписи по ФЗ №63-ФЗ «Об электронной подписи»**
- № 8 **Сертификат электронной подписи, назначение и содержание сертификата по ФЗ №63-ФЗ «Об электронной подписи»**
- № 9 **Определение DMZ, примеры применения**
- № 10 **Политики сетевой безопасности на основе межсетевого экрана**

*Вопросы закрытого типа:*

- № 1 **Этапы действия программного вируса:**
1. Размножение, вирусная атака.
  2. Запись в файл, размножение.
  3. Запись в файл, размножение, уничтожение программы.
- № 2 **Что называют вирусной атакой?**
1. Неоднократное копирование кода вируса в код программы.
  2. Отключение компьютера в результате попадания вируса.
  3. Нарушение работы программы, уничтожение данных, форматирование жёсткого диска.
- № 3 **Какие существуют методы реализации антивирусной защиты?**
1. Аппаратные и программные.
  2. Программные и административные.
  3. Только программные.
- № 4 **Какие существуют основные средства защиты данных?**
1. Резервное копирование наиболее ценных данных.
  2. Аппаратные средства.
  3. Программные средства.
- № 5 **На чем основано действие антивирусной программы?**
1. На ожидании начала вирусной атаки.
  2. На сравнении программных кодов с известными вирусами.
  3. На удалении заражённых файлов.
- № 6 **Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к?**
1. Аппаратным средствам защиты
  2. Программным средствам защиты
  3. Техническим средствам защиты
  4. Правовым средствам защиты
- № 7 **Технические меры защиты можно разделить на:**

1. Средства аппаратной защиты, включающие средства защиты кабельной системы, систем электропитания, и т.д.
2. Правовые, организационные, технические
3. Правовые, аппаратные, программные
4. Личные, организационные

№ 8 **К наиболее важному элементу аппаратной защиты можно отнести**

1. Защита от сбоев серверов, рабочих станций и локальных компьютеров
2. Защиту от вирусов
3. Защиту от хакеров
4. Все перечисленное

№ 9 **Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.**

1. Защита от сбоев в электропитании
2. Защита от сбоев серверов, рабочих станций и локальных компьютеров
3. Защита от сбоев устройств для хранения информации
4. Защита от утечек информации электромагнитных излучений

№ 10 **Какая из перечисленных атак на поток информации является пассивной:**

1. Перехват.
2. Имитация.
3. Модификация.
4. Фальсификация.
5. Прерывание.

### **ОПК-3**

*Вопросы открытого типа:*

№ 1 **Государственная тайна это:**

№ 2 **Что можно отнести к правовым мерам ИБ?**

№ 3 **Что можно отнести к организационным мерам ИБ?**

№ 4 **Что можно отнести к техническим мерам ИБ?**

№ 5 **Что такое компьютерный вирус?**

№ 6 **Основные типы компьютерных вирусов:**

№ 7 **Ответьте на вопрос «Что называется вирусной атакой?»**

№ 8 **Программные средства защиты можно разделить на:**

№ 9 **Наибольшую угрозу для безопасности сети представляют:**

№ 10 **Технические каналы утечки информации делятся на...**

*Вопросы закрытого типа:*

№ 1 **Как называется умышленно искажённая информация?**

1. - Дезинформация
2. - Информативный поток
3. - Достоверная информация
4. Перестает быть информацией

№ 2 **В зависимости от формы представления информация может быть разделена на?**

1. - Речевую, документированную и телекоммуникационную
2. - Мысль, слово и речь
3. - Цифровая, звуковая и тайная
4. Цифровая, звуковая

№ 3 **К каким процессам относят процессы сбора, обработки, накопления,**



**хранения, поиска и распространения информации?**

1. - Информационным процессам
2. - Мыслительным процессам
3. - Машинным процессам
4. - Микропроцессам

**№ 4 Что называют защитой информации?**

1. - Называют деятельность по предотвращению утечки защищаемой информации
2. - Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
3. - Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию
4. Называют деятельность по предотвращению преднамеренных воздействий

**№ 5 Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлён только тем лицам, которые на это имеют право**

1. - Управление доступом
2. - Конфиденциальность
3. - Аутентичность
4. - Целостность
5. - Доступность

**№ 6 Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе**

1. - Информационная безопасность
2. - Защитные технологии
3. - Заземление
4. - Конфиденциальность

**№ 7 Можно выделить следующие направления мер информационной безопасности**

1. - Правовые
2. - Организационные
3. - Все ответы верны
4. - Технические

**№ 8 Обеспечение достоверности и полноты информации и методов ее обработки.**

1. - Конфиденциальность
2. - Целостность
3. - Доступность
4. - Целесообразность

**№ 9 Целью информационной безопасности является?**

1. - Обезопасить ценности системы
2. - Защитить и гарантировать точность и целостность информации
3. - Минимизировать разрушения
4. – Модифицировать ценность

**№ 10 К правовым мерам следует отнести?**

1. - Разработку норм, устанавливающих ответственность за компьютерные преступления и защиту авторских прав программистов

2. - Охрану вычислительного центра и аппаратуры связи
3. - Проектирование ЛВС и ГБС
4. - Средства идентификации и аутентификации пользователей