МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

Кафедра «Информационный и электронный сервис»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б.1.О.04.11 «Защита информации»

Направление подготовки:
09.03.02 «Информационные системы и технологии»

Направленность (профиль):
«Информационные системы и технологии»

Квалификация выпускника: **бакалавр**

Тольятти 2021 г.

Рабочая программа дисциплины «Защита информации» разработана в соответствии с федеральным государственным образовательным стандартом высшего образования - *бакалавриат* по направлению подготовки 09.03.02 «Информационные системы и технологии», утверждённым приказом Министерства образования и науки Российской Федерации от 19.09.2017 г. № 926.

Составители:

к.т.н., доцент (учёная степень, учёное звание) Т.С. Яницкая (ФИО)

РПД обсуждена на заседании кафедры «Информационный и электронный сервис»

« 28 » 05 20 21 г., протокол № 10

Заведующий кафедрой, д.т.н., профессор (уч.степень, уч.звание) В.И. Воловач (ФИО)

Рабочая программа дисциплины утверждена в составе основной профессиональной образовательной программы решением Ученого совета от 29.06.2021 Протокол № 16

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель освоения дисциплины

Целью освоения дисциплины является:

- формирование у обучающихся общепрофессиональных компетенций в области использования информационно-коммуникационных технологий.

1.2. Перечень планируемых результатов обучения по дисциплине

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**	**Основание (ПС)** *для профессиональных компетенций
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИОПК-3.1. Использует современные информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры ИОПК-3.2. Применяет в практической деятельности знания основных требований информационной безопасности ИОПК-3.3. Владеет методами поиска и анализа информации для подготовки документов на основе информационной и библиографической культуры, с учетом соблюдения авторского права и требований информационной безопасности	**Знает:** методы и средства обеспечения информационной безопасности компьютерных систем **Умеет:** инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных иинформационных систем; выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в информационной системе. **Владеет:** навыками защиты информации компьютерных систем.	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к *обязательной части* Блока 1. Дисциплины (модули) образовательной программы (Б1.О.04. Общепрофессиональный модуль).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем и структура дисциплины

Общая трудоёмкость дисциплины составляет **4 з.е. (144 часа)**, их распределение по видам работ и семестрам представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины, час	**144**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**48/14**
занятия лекционного типа (лекции)	18/6
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	18/4
лабораторные работы	12/4
Самостоятельная работа всего, в т.ч.:	**96/126**
Самоподготовка по темам (разделам) дисциплины	96/126
Выполнение курсового проекта /курсовой работы	- / -
Контроль (часы на экзамен, зачет)	**- /4**
Промежуточная аттестация	**Зачет**

Примечание:-/- *объем часов соответственно для очной, заочной форм обучения*

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

В процессе освоения дисциплины может применяться электронное обучение и дистанционные образовательные технологии.

В процессе освоения дисциплины обучающиеся обеспечены доступом к электронной информационно-образовательной среде и электронно-библиотечным системам.

3.2. Содержание дисциплины, структурированное по темам

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
ОПК-3 ИОПК-3.1, ИОПК-3.2, ИОПК-3.3	**ТЕМА 1. ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ** Основное содержание 1. Информационная безопасность. Основные понятия. 2. Модели информационной безопасности. 3. Виды защищаемой информации	3/1				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по темам лекционных занятий
	Практическое занятие №1 Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности			3/0,5		Отчет по практической работе
	Самостоятельная работа				16/21	Самостоятельное изучение учебных материалов
ОПК-3 ИОПК-3.1, ИОПК-3.2, ИОПК-3.3	**ТЕМА 2. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** Основное содержание	3/1				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по темам лекционных

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
	1. Основные нормативно-правовые акты в области информационной безопасности. 2. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны					занятий
	Лабораторная работа №1 Прототип «Командного процессора» с элементами защиты		3/1			Отчет по лабораторной работе
	Практическое занятие №2 Использование криптографических средств защиты информации			3/0,5		Отчет по практической работе
	Самостоятельная работа				16/21	Самостоятельное изучение учебных материалов
ОПК-3 ИОПК-3.1, ИОПК-3.2, ИОПК-3.3	**ТЕМА 3. ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** Основное содержание 1. Основные стандарты в области обеспечения информационной безопасности. 2. Политика безопасности. Экономическая безопасность предприятия.	3/1				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по темам лекционных занятий
	Лабораторная работа №2. Криптографические методы защиты информации. Алгоритмы шифрования		3/1			Отчет по лабораторной работе
	Практическое занятие №3 Реализация работы инфраструктуры открытых ключей			3/1		Отчет по практической работе
	Самостоятельная работа				16/21	Самостоятельное изучение учебных материалов
ОПК-3 ИОПК-3.1, ИОПК-3.2, ИОПК-3.3	**ТЕМА 4. ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ** Основное содержание 1. Инженерная защита объектов. 2. Защита информации от утечки по техническим каналам.	3/1				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по темам лекционных занятий
	Практическое занятие №4 Средства стеганографии для защиты информации			3/1		Отчет по практической работе
	Самостоятельная работа				16/21	Самостоятельное изучение учебных материалов
ОПК-3 ИОПК-3.1, ИОПК-3.2, ИОПК-3.3	**ТЕМА 5. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** Основное содержание 1. Основные виды сетевых и компьютерных угроз. 2. Средства и методы защиты от сетевых	3/1				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по темам лекционных занятий

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
	компьютерных угроз					
	Лабораторная работа №3. Использование сторонних криптографических элементов		3/1			Отчет по лабораторной работе
	Практическое занятие №5 Настройка безопасного сетевого соединения			3/0,5		Отчет по практической работе
	Самостоятельная работа				16/21	Самостоятельное изучение учебных материалов
ОПК-3 ИОПК-3.1, ИОПК-3.2, ИОПК-3.3	**ТЕМА 6. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ** Основное содержание 1. Симметричные и ассиметричные системы шифрования. 2. Цифровые подписи (Электронные подписи). 3. Инфраструктура открытых ключей. 4. Криптографические протоколы.	3/1				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по темам лекционных занятий
	Лабораторная работа №4. Стеганография		3/1			Отчет по лабораторной работе
	Практическое занятие №6 Антивирусные средства защиты информации			3/0,5		Отчет по практической работе
	Самостоятельная работа				16/21	Самостоятельное изучение учебных материалов
	ИТОГО	**18/6**	**12/4**	**18/4**	**96/126**	

Примечание:-/- *объем часов соответственно для очной, заочной форм обучения*

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

4.1. Общие методические рекомендации по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курса, составленного на основе результатов научных исследований, проводимых университетом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Преподавание дисциплины ведется с применением следующих видов **образовательных технологий:**

-балльно-рейтинговая технология оценивания;

- электронное обучение;

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

4.2. Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины. Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала.

Лекционные занятия проводятся в поточной аудитории с применением мультимедийного проектора в виде учебной презентации или в ЭИОС университета.

В ходе лекционных занятий рекомендуется конспектирование учебного материала. Возможно ведение конспекта лекций в виде интеллект-карт.

Отдельные темы предлагаются для самостоятельного изучения (конспектируются).

Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям / лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

4.3. Методические указания для обучающихся по освоению дисциплины на лабораторных работах

Подготовку к каждой лабораторной работе студент должен начать с ознакомления с планом занятия, который отражает содержание предложенной темы. Каждая выполненная работа с оформленным отчетом по ней подлежит защите преподавателю.

При оценивании лабораторных работ учитывается следующее:

–качество выполнения экспериментально-практической части работы и степень соответствия результатов работы заданным требованиям;

–качество оформления отчета по работе;

–качество устных ответов на контрольные вопросы при защите работы.

Лабораторные работы организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

4.4. Методические указания для обучающихся по освоению дисциплины на занятиях семинарского типа/ на практических занятиях

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;

- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;

- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Практические занятия организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

4.5. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

Самостоятельная работа студентов включает:

1. *Изучение учебной литературы по курсу.*
2. *Работу с ресурсами Интернет*
3. *Самостоятельное изучение учебных материалов*

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы.

Для обучающихся по заочной форме обучения самостоятельная работа является основным видом учебной деятельности.

Для обеспечения самостоятельной работы обучающихся используется электронный учебный курс, созданный в ЭИОС университета http://sdo.tolgas.ru/.

4.6. Методические указания для выполнения курсового проекта / работы (не предусмотрено учебным планом).

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Вся литература, включенная в данный перечень, представлена в виде электронных ресурсов в электронной библиотеке университета (ЭБС). Литература, используемая в печатном виде, представлена в научной библиотеке университета в объеме не менее 0,25 экземпляров на одного обучающегося.

Основная литература:

1. Баранова, Е. К. Моделирование системы защиты информации. Практикум : учеб. пособие для вузов по направлению "Приклад. информатика" / Е. К. Баранова, А. В. Бабаш. - 3-е изд., перераб. и доп. - Документ read. - Москва : РИОР [и др.], 2020. - 320 с. - (Высшее образование). - Прил. - URL: https://znanium.com/read?id=371348 (дата обращения: 25.01.2021). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01848-4. - 978-5-16-108538-7. - Текст : электронный.

2. Зайцев, А. П. Технические средства и методы защиты информации : учеб. для вузов по группе специальностей "Информ. безопасность" / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов ; под ред. А. П. Зайцева и А. А. Шелупанова. - 7-е изд. - Москва : Горячая линия - Телеком, 2020. - 442 с. : ил. - Прил. - ISBN 978-5-9912-0233-6 : 577-72. - Текст : непосредственный.

3. Защита информации : учеб. пособие для вузов по направлению подгот. Инфокоммуникац. технологии и системы связи квалификации (степ.) "бакалавр" и квалификации (степ.) "магистр" / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - 3-е изд. - Документ read. - Москва : РИОР [и др.], 2021. - 400 с. - (Высшее образование: Бакалавриат; Магистратура). - URL: https://znanium.com/read?id=367588 (дата обращения: 09.12.2020). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01759-3. - 978-5-16-013801-5. - 978-5-16-106478-8. - Текст : электронный.

4. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учеб. пособие / С. Н. Никифоров. - Изд. 3-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2020. - 93 с. - Прил. - URL: https://e.lanbook.com/reader/book/148474/#1 (дата обращения: 02.02.2021). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-6527-9. - Текст : электронный.

5. Никифоров, С. Н. Методы защиты информации. Защищенные сети : учеб. пособие / С. Н. Никифоров. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2021. - 94 с. - (Учебники для вузов. Специальная литература). - URL: https://e.lanbook.com/reader/book/169311/#1 (дата обращения: 07.04.2021). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-3099-4. - Текст : электронный.

6. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование : учеб. пособие / С. Н. Никифоров. - Изд. 3-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2020. - 121 с. - Прил. - URL: https://e.lanbook.com/reader/book/146885/#1 (дата обращения: 02.02.2021). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-6352-7. - Текст : электронный.

7. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. - Изд. 2-е, испр. - Документ Reader. - Санкт-Петербург : Лань, 2020. - 124 с. - (Учебники для вузов. Специальная литература). - URL: https://e.lanbook.com/reader/book/133924/#1 (дата обращения: 15.10.2020). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-4404-5. - Текст : электронный.

8. Хорев, П. Б. Программно-аппаратная защита информации : учеб. пособие для вузов по направлению "Информ. безопасность" / П. Б. Хорев. - 3-е изд., испр. и доп. - Документ read. - Москва : ИНФРА-М, 2021. - 327 с. : ил. - (Высшее образование - Бакалавриат). - URL: https://znanium.com/read?id=365036 (дата обращения: 18.03.2021). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-015471-8. - 978-5-16-107928-7. - Текст : электронный.

Дополнительная литература:

9. Баранова, Е. К. Основы информатики и защиты информации : учеб. пособие для вузов по специальности "Приклад. информатика" и др. экон. специальностям / Е. К. Баранова. - Документ read. - Москва : РИОР [и др.], 2018. - 182 с. - (Высшее образование). - Прил. - URL: https://znanium.com/read?id=334901 (дата обращения: 25.01.2021). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01169-0. - 978-5-16-006484-0. - 978-5-16-104837-5. - Текст : электронный.

10. Башлы, П. Н. Информационная безопасность : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Документ Bookread2. - Москва : РИОР, 2013. - 222 с. : ил. - Слов. терминов. - URL: https://new.znanium.com/read?id=213488 (дата обращения: 15.10.2020). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-001178-2. - Текст : электронный.

11. Каратунова, Н. Г. Защита информации. Курс лекций : учеб.-метод. пособие / Н. Г. Каратунова ; Кубан. соц.-экон. ин-т, Каф. математики и информатики. - Документ Bookread2. - Краснодар : Кубан. соц.-экон. ин-т, 2014. - 188 с. - Прил. - URL: http://znanium.com/bookread2.php?book=503511 (дата обращения: 15.10.2020). - Режим доступа: для авториз. пользователей. - Текст : электронный.

12. Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для вузов по специальности "Информ. системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 6-е изд., стер. - Москва : Академия, 2012. - 336 с. : ил., табл. - (Высшее профессиональное образование. Информатика и вычислительная техника). - ISBN 978-5-7695-9222-5 : 431-20. - Текст : непосредственный.

13. Платонов, В. В. Программно-аппаратные средства защиты информации : учеб. для вузов по направлению подгот. "Информ. безопасность" / В. В. Платонов. - Москва : Академия, 2013. - 63,7 МБ, 332 с. : ил., табл. - (Высшее профессиональное образование. Бакалавриат). - CD-ROM. - Систем. требования: Windows XP и выше; DVD-Drive. - Прил. - ISBN 978-5-7695-9327-7 : 11634-80. - Текст : электронный.

5.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. КонсультантПлюс [Электронный ресурс]: Справочная правовая система. - Режим доступа: http://www.consultant.ru/.
2. Электронная библиотечная система Поволжского государственного университета сервиса [Электронный ресурс]. – Режим доступа: http://elib.tolgas.ru./ - Загл. с экрана.
3. Электронно-библиотечная система Znanium.com [Электронный ресурс]. - Режим доступа: http://znanium.com/. – Загл. с экрана.
4. Электронно-библиотечная система «Издательство Лань» [Электронный ресурс]. - Режим доступа: https://e.lanbook.com/. – Загл. с экрана.
5. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. - Режим доступа: http://elibrary.ru/defaultx.asp. - Загл с экрана.
6. Polpred.com. Обзор СМИ. Полнотекстовая, многоотраслевая база данных (БД) [Электронный ресурс]. - Режим доступа: http://polpred.com/. – Загл. с экрана.
7. Центральный научно-исследовательский институт швейной промышленности [Электронный ресурс]. – Режим доступа: http://www.cniishp.ru/. – Загл. с экрана.
8. Материалы для швейного производства [Электронный ресурс]. – Режим доступа: http://hymo.ru/. – Загл. с экрана.
9. Базы данных Всероссийского института научной и технической информации (ВИНИТИ РАН) по естественным, точным и техническим наукам Электронный ресурс]. - Режим доступа: http://www.viniti.ru. – Загл. с экрана.
10. Университетская информационная система Россия [Электронный ресурс]. - Режим доступа: http://uisrussia.msu.ru/. – Загл. с экрана.
11. Официальная статистика. Официальный сайт Федеральной службы государственной статистики [Электронный ресурс]. - Режим доступа: https://www.gks.ru/ – Загл. с экрана.
12. Финансово-экономические показатели Российской Федерации [Электронный ресурс]. - Режим доступа: https://www.minfin.ru/ru/statistics/ – Загл. с экрана.

5.3. Программное обеспечение

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№ п/п	Наименование	Условия доступа
1	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	Microsoft Office Professional Plus	из внутренней сети университета (лицензионный договор)
3	КонсультантПлюс	из внутренней сети университета (лицензионный договор)
4	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)
5.	Браузер	из любой точки, в которой имеется доступ к сети Интернет (свободно распространяемое)
6.	WinRAR	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)
7.	PGP	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)

6. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных учебным планом и рабочей программой дисциплины, оснащенные оборудованием и техническими средствами обучения.

Занятия лекционного типа. Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Занятия семинарского типа. Учебные аудитории для занятий семинарского типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук).

Лабораторные работы. Для проведения лабораторных работ используется учебная аудитория «Лаборатория **Т404, Т407-409, Т412, Т413**», оснащенная следующим оборудованием: персональными компьютерами и доступом к сети Интернет.

Промежуточная аттестация. Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Самостоятельная работа. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интеренет» и доступом к электронной информационно-образовательной среде университета. Для организации самостоятельной работы обучающихся используются:

- компьютерные классы университета;
- библиотека (медиазал), имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети Интернет.

Электронная информационно-образовательная среда университета (ЭИОС). Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

ЭИОС университета обеспечивает:

доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;

формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации образовательной программы с применением электронного обучения, дистанционных образовательных технологий ЭИОС дополнительно обеспечивает:

фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательной программы;

проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети "Интернет".

7. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида, могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

Шкала оценки результатов освоения дисциплины, сформированности результатов обучения

Форма проведения промежуточной аттестации	Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины		
	Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
Зачёт	допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
	пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
			70-85,9	«хорошо» / 4	зачтено
	повышенный	86-100	86-100	«отлично» / 5	зачтено

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами (по накопительному рейтингу). Студентам, набравшим в ходе текущего контроля успеваемости по дисциплине от 61 до 100 баллов и выполнившим все обязательные виды запланированных учебных занятий, по решению преподавателя без прохождения промежуточной аттестации выставляется оценка в соответствии со шкалой оценки результатов освоения дисциплины.

***Результат обучения считается сформированным (повышенный уровень)**, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует повышенному уровню сформированности результатов обучения.*

***Результат обучения считается сформированным (пороговый уровень)**, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует пороговому уровню сформированности результатов обучения.*

***Результат обучения считается несформированным**, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует допороговому уровню.*

Формы текущего контроля успеваемости

Формы текущего контроля	Количество контрольных точек	Количество баллов за 1 контр. точку	Макс. возм. кол-во баллов
Отчет по практической работе	2	15	30
Отчет по лабораторной работе	2	15	30
Тестирование по темам лекционных занятий	3	10	30
Творческий рейтинг (участие в конференциях, олимпиадах и т.п.)	1	10	10
Итого по дисциплине			**100 баллов**

Система оценивания представлена в электронном учебном курсе по дисциплине http://sdo.tolgas.ru/.

8.2. Типовые контрольные задания или иные материалы для ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

8.2.1. Типовые задания к практическим (семинарским) занятиям

Практическая работа №1 «Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности».

Определить название фирмы, выбрать вид и область деятельности из перечисленных в таблице (в файле). Составить план мероприятий по защите коммерческой тайны. Указать перечень внутрифирменных документов, используемых в целях правовой защиты секретов данной фирмы

Практическая работа №2 «Использование криптографических средств защиты информации»

Создать зашифрованный файл и криптоконтейнер и расшифровать их.

Практическая работа №3 «Реализация работы инфраструктуры открытых ключей»

Создать удостоверяющий центр, сгенерировать открытые и секретные ключи, создать сертификаты открытых ключей, создать электронные подписи, проверить электронные подписи.

Практическая работа №4 «Средства стеганографии для защиты информации»

Использование средств стеганографии для защиты файлов

Практическая работа №5 «Настройка безопасного сетевого соединения»

Создать защищенный канал связи средствами виртуальной частной сети.

Практическая работа №6 «Антивирусные средства защиты информации»

Открыть любым, известным способом антивирусную программу Kaspersky. Ознакомиться с окном программы, просмотрите пункты меню. Просмотреть, что проверяется при выборе того или иного режима проверки. Определить, какие действия предлагает программа выполнять с найденными вирусами и зараженной информацией. Используя выборочный режим проверки, проверить на наличие вируса

8.2.2. Типовые задания для лабораторных работ

Лабораторная работа №1. «Прототип «Командного процессора» с элементами защиты».

Реализовать в «командном процессоре» защиту на уровне пользователя с применением метода паролей или его модификаций; реализовать процедуру управления системой защиты на уровне пользователя

Лабораторная работа №2. «Криптографические методы защиты информации. Алгоритмы шифрования»

Освоить практические приемов криптографического преобразования информации

Лабораторная работа №3. «Использование сторонних криптографических элементов»

Создать приложение, выполняющее функции шифрования и дешифрования файла методом DES, реализованного в библиотеке DCPcrypt (разделения по вариантам нет)

Лабораторная работа №4. «Стеганография»

Создать приложение, выполняющее две функции: функцию скрытия исходного текста в контейнере стеганографическим методом и функцию извлечения текста из контейнера

Типовые тестовые задания по темам

1) Вредоносная программа - это...

- любое ПО, предназначенное для получения несанкционированного доступа к информации, которая хранится на компьютере, с целью причинения вреда владельцу компьютера.
- любое ПО, предназначенное для получения санкционированного доступа к информации, которая хранится на компьютере, с целью причинения вреда владельцу компьютера.
- любое ПО, предназначенное для обеспечения контроля над компьютером злоумышленника.
- любое ПО, предназначенное для обеспечения контроля над компьютерами учащихся.

2) Шпионские программы - это...

- ПО, которое тайно устанавливается и используется для доступа к информации, хранимой на компьютере.
- ПО, которое открыто устанавливается и используется для доступа к информации, хранимой на компьютере.
- ПО, которое предназначено для удаления информации с компьютера.
- ПО, которое предназначено для удалённого управления и сортировки информации на компьютере.

3) Антивирусная программа - это...

- программа, предназначенная для обнаружения и удаления компьютерных вирусов, а также для эффективной защиты от них.
- программа, предназначенная для сокрытия компьютерных вирусов.
- программа, предназначенная для обнаружения вирусов и извещения о них правоохранительных органов.
- программа, которая используется правоохранительными органами для выявления несанкционированного доступа к образовательным ресурсам.

4) Файловые вирусы - это...

- вредоносные программы, работа которых заключается в распространении своих копий по всему компьютеру.
- вредоносные программы, которые заражают загрузочный сектор гибкого или жёсткого диска.
- заражают файлы *.exe, *.sys, *.dll
- вирусы, которые поражают файлы приложений Microsoft Office.

5) Загрузочные вирусы - это...

- вредоносные программы, которые заражают загрузочный сектор гибкого или жёсткого диска.
- вредоносные программы, работа которых заключается в распространении своих копий по всему компьютеру.
- вредоносные программы, которые тайно устанавливается и используется для доступа к информации, хранимой на компьютере.
- вредоносные программы, которые распространяются через электронную почту и сеть Интернет.

6) Сетевые вирусы - это...

- вирусы, которые распространяются по компьютерной сети.
- вредоносные программы, которые осуществляют тайные действия по сбору, изменению и передаче информации злоумышленникам.

- вредоносные программы, с помощью которых можно выполнять скрытое удалённое управление компьютером.
- программное обеспечение, которое может нанести косвенный вред компьютеру, на котором установлено, или другим компьютерам в сети.

7) Макровирусы - это...

- вирусы, которые поражают файлы приложений Microsoft Office.
- вирусы, которые заражают загрузочный сектор гибкого или жёсткого диска.
- вирусы, которые тайно устанавливаются и используются для доступа к информации, хранимой на компьютере.
- вирусы, которые распространяются через электронную почту и сеть Интернет.

8) Какие существуют типы вредоносных программ?

- Вирусы, черви, троянские и хакерские программы.
- Шпионские и рекламные программы.
- Потенциально опасное программное обеспечение.
- Трояны-шпионы.
- Сигнатуры.
- Макросы

9) Какие действия может выполнять антивирусная программа с обнаруженным заражённым файлом?

- Только отчёт.
- Лечить.
- Удалить.
- Переименовать.
- Пропустить.
- Карантин.
- Создать копию.
- Удалить только расширение.

10) Выберите верные утверждения, которыми нужно пользоваться при задании пароля.

- Пароль не должен легко раскрываться.
- Подбор пароля должен быть максимально сложным.
- В основе пароля не должно находится ваше имя, кличка животного, дата рождения и т. д.
- Не стоит записывать пароль.
- Для большей надёжности нужно записать пароль куда-либо и положить рядом с компьютером.
- В основе пароля должно находится ваше имя, кличка животного, дата рождения и т. д.

8.3. Типовые контрольные задания или иные материалы для проведения ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Форма проведения промежуточной аттестации по дисциплине: *зачет (по результатам накопительного рейтинга или в форме компьютерного тестирования).*

Устно-письменная форма по экзаменационным билетам предполагается, как правило, для сдачи академической задолженности.

Защита курсового проекта/ работы (не предусмотрено учебным планом).

Перечень вопросов для подготовки к зачёту
(ОПК-3: ИОПК-3.1, ИОПК-3.2, ИОПК-3.3)

1.Кто в РФ осуществляет общее руководство системой информационной безопасности

2.В каком году был принят закон РФ «Об информации, информационных технологиях и о защите информации»

3. Аутентификация субъекта — это

4. Как классифицируются угрозы безопасности информационным системам
5. Политика безопасности - это
6. Алгоритмы криптографического преобразования информации - это
7. Доступ к информации различают
8. Санкционированный доступ к информации — это
9. Несанкционированный доступ к информации характеризуется
10. Угрозы безопасности ИС по природе возникновения бывают

Примерный тест для итогового тестирования:

1. Raid-массив это:

Набор жестких дисков, подключенных особым образом

Антивирусная программа

Вид хакерской утилиты

2. Выберите составные части современного антивируса

Модем

Сканер

Межсетевой экран

Принтер

3. К вредоносным программам относятся:

Потенциально опасные программы

Вирусы, черви, трояны

Межсетевой экран, брандмауэр

4. К биометрической системе защиты относятся

Защита паролем

Физическая защита данных

Идентификация по отпечатку пальца

5. Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется

Загрузочный вирус

Макровирус

Троян

Сетевой червь

Файловый вирус

6. Вредоносная программа - это...

любое ПО, предназначенное для получения несанкционированного доступа к информации, которая хранится на компьютере, с целью причинения вреда владельцу компьютера.

любое ПО, предназначенное для получения санкционированного доступа к информации, которая хранится на компьютере, с целью причинения вреда владельцу компьютера.

любое ПО, предназначенное для обеспечения контроля над компьютером злоумышленника.

любое ПО, предназначенное для обеспечения контроля над компьютерами учащихся.

7. Шпионские программы - это...

ПО, которое тайно устанавливается и используется для доступа к информации, хранимой на компьютере.

ПО, которое открыто устанавливается и используется для доступа к информации, хранимой на компьютере.

ПО, которое предназначено для удаления информации с компьютера.

ПО, которое предназначено для удалённого управления и сортировки информации на компьютере.

8. Антивирусная программа - это...

программа, предназначенная для обнаружения и удаления компьютерных вирусов, а также для эффективной защиты от них.

программа, предназначенная для сокрытия компьютерных вирусов.

программа, предназначенная для обнаружения вирусов и извещения о них правоохранительных органов.

программа, которая используется правоохранительными органами для выявления несанкционированного доступа к образовательным ресурсам.

9. Файловые вирусы - это...

вредоносные программы, работа которых заключается в распространении своих копий по всему компьютеру.

вредоносные программы, которые заражают загрузочный сектор гибкого или жёсткого диска.

заражают файлы *.exe, *.sys, *.dll

вирусы, которые поражают файлы приложений Microsoft Office.

10. Загрузочные вирусы - это...

вредоносные программы, которые заражают загрузочный сектор гибкого или жёсткого диска.

вредоносные программы, работа которых заключается в распространении своих копий по всему компьютеру.

вредоносные программы, которые тайно устанавливается и используется для доступа к информации, хранимой на компьютере.

вредоносные программы, которые распространяются через электронную почту и сеть Интернет.

11. Сетевые вирусы - это...

вирусы, которые распространяются по компьютерной сети.

вредоносные программы, которые осуществляют тайные действия по сбору, изменению и передаче информации злоумышленникам.

вредоносные программы, с помощью которых можно выполнять скрытое удалённое управление компьютером.

программное обеспечение, которое может нанести косвенный вред компьютеру, на котором установлено, или другим компьютерам в сети.

12. Макровирусы - это...

вирусы, которые поражают файлы приложений Microsoft Office.

вирусы, которые заражают загрузочный сектор гибкого или жёсткого диска.

вирусы, которые тайно устанавливаются и используются для доступа к информации, хранимой на компьютере.

вирусы, которые распространяются через электронную почту и сеть Интернет.

13. Какие существуют типы вредоносных программ?

Вирусы, черви, троянские и хакерские программы.

Шпионские и рекламные программы.

Потенциально опасное программное обеспечение.

Трояны-шпионы.

Сигнатуры.

Макросы

14. Какие действия может выполнять антивирусная программа с обнаруженным заражённым файлом?

Только отчёт.

Лечить.

Удалить.

Переименовать.

Пропустить.

Карантин.

Создать копию.

Удалить только расширение.

15. Выберите верные утверждения, которыми нужно пользоваться при задании пароля.

Пароль не должен легко раскрываться.

Подбор пароля должен быть максимально сложным.

В основе пароля не должно находится ваше имя, кличка животного, дата рождения и т. д.

Не стоит записывать пароль.

Для большей надёжности нужно записать пароль куда-либо и положить рядом с компьютером.

В основе пароля должно находится ваше имя, кличка животного, дата рождения и т. д.

Полный фон оценочных средств для проведения промежуточной аттестации размещен в банке вопросов электронного учебного курса дисциплины в ЭИОС университета http://sdo.tolgas.ru/, а также хранится в бумажном и (или) электронном виде на кафедре-разработчике.