

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Выборнова Раиса Александровна

Должность: Ректор

Дата подписания: 07.10.2026 14:04:44

Уникальный программный ключ:

c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

Высшая школа интеллектуальных систем и кибертехнологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»

Направление подготовки:

10.03.01 «Информационная безопасность»

Направленность (профиль):

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

Квалификация выпускника: **бакалавр**

Рабочая программа дисциплины «Основы информационной безопасности» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 г. № 1427.

Составители:

старший преподаватель	Ю.С. Мунирова
(ученая степень, ученое звание)	(ФИО)
ассистент	Е.А. Курцев
(ученая степень, ученое звание)	(ФИО)

РПД обсуждена на заседании ученого совета Высшей школы интеллектуальных систем и кибертехнологий

23.05. 2025 г., протокол № _10__

Директор	к.э.н., доцент	О.А. Филиппова
	(уч.степень, уч.звание)	(ФИО)

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

1.1. Цель освоения дисциплины

Целями освоения дисциплины являются:

- формирование у обучающихся системных теоретических знаний о сущности и содержании информационной безопасности, видах и источниках угроз информации, основных направлениях, методах и средствах защиты информации;
- формирование способности оценивать роль информации, информационных технологий и информационной безопасности в жизни личности, общества и государства;
- формирование умения применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации, в сфере профессиональной деятельности.
- формирование у обучающихся общепрофессиональных компетенций *в области использования информационно-коммуникационных технологий и т.п.*

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-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИОПК-1.1. Понимает роль информации в современном обществе ИОПК-1.3. Понимает значимость информационной безопасности в защите интересов личности, общества и государства	Знает: – основные понятия и категории информационной безопасности; роль и место информации в жизни личности, общества и государства – виды, источники и модели угроз информационной безопасности Умеет: – оценивать значимость информации и информационной безопасности для обеспечения интересов личности, общества и государства – классифицировать угрозы информационной безопасности и объекты защиты Владеет: – навыками анализа роли	

		информационных технологий и информационной безопасности в современном обществе	
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ИОПК-5.1. Использует нормативные правовые документы в своей профессиональной деятельности ИОПК-5.2. Осуществляет подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности	Знает: – систему нормативных правовых актов Российской Федерации в области защиты информации – основные методические документы регуляторов (ФСТЭК России, ФСБ России) в сфере информационной безопасности Умеет: – осуществлять подбор и анализ нормативных правовых и методических документов, регламентирующих защиту информации – обобщать научно-техническую информацию по методам обеспечения информационной безопасности Владеет: – навыками применения нормативных правовых актов при решении задач обеспечения информационной безопасности	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к обязательной части Блока 1. Дисциплины (модули) программы бакалавриата (Общепрофессиональный модуль).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем и структура дисциплины

Общая трудоёмкость дисциплины составляет **2 з.е. (72 час.)**, их распределение по видам работ представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины, час	72
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	58/24
занятия лекционного типа (лекции)	24/12
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	34/12
Самостоятельная работа всего, в т.ч.:	14/39
Самоподготовка по темам (разделам) дисциплины	-
Выполнение курсового проекта /курсовой работы	—
Контроль (часы на экзамен, зачет)	-/9
Промежуточная аттестация	Зачет

Примечание: -/- объем часов соответственно для очной и очно-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	Практические занятия, час		
ОПК-1 ИОПК-1.1. ИОПК-1.3.	ТЕМА 1. ИНФОРМАЦИЯ КАК ОБЪЕКТ ЗАЩИТЫ. ПРЕДМЕТ И ЗАДАЧИ ДИСЦИПЛИНЫ Основное содержание: 1. Понятие информации, её свойства и виды. 2. Информация как объект права собственности, товар и стратегический ресурс. 3. Основные понятия и определения в области информационной безопасности (ИБ): защита информации, безопасность информации, информационная сфера.	3/1			Устный опрос
	Практическое занятие № 1. Основные понятия и категории информационной безопасности		4/1		
	Самостоятельная работа			2/1	Самостоятельное изучение материалов, подготовка к практическому занятию

ОПК-1 ИОПК-1.1. ИОПК-1.3.	ТЕМА 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПОНЯТИЕ, КЛАССИФИКАЦИЯ, ИСТОЧНИКИ Основное содержание: 1. Понятие угрозы безопасности информации. 2. Классификация угроз по природе возникновения, по цели реализации, по объекту воздействия. 3. Источники угроз: антропогенные, техногенные, стихийные.	3/1			Устный опрос / тестирование
	Практическое занятие № 2. Классификация угроз информационной безопасности		4/1		
	Самостоятельная работа			2/1	Самостоятельное изучение материалов, подготовка к практическому занятию
ОПК-1 ИОПК-1.1. ИОПК-1.3	ТЕМА 3. МОДЕЛЬ НАРУШИТЕЛЯ И ОБЪЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ Основное содержание: 1. Понятие нарушителя информационной безопасности, его категории и возможности. 2. Модель нарушителя и модель угроз как основа построения системы защиты. 3. Объекты защиты: информационные ресурсы, средства и системы информатизации, информационная инфраструктура.	3/1			Практическое задание
	Практическое занятие № 3. Разработка модели нарушителя для типовой информационной системы		4/1		
	Самостоятельная работа			2/2	Самостоятельное изучение материалов,

					подготовка к практическому занятию
ОПК-5 ИОПК-5.1 ИОПК-5.2.	ТЕМА 4. ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ Основное содержание: 1. Конституционные основы информационной безопасности. 2. Федеральные законы «Об информации, информационных технологиях и о защите информации», «О персональных данных», «О государственной тайне», «О коммерческой тайне». 3. Доктрина информационной безопасности Российской Федерации.	3/1			Доклад/сообщение
	Практическое занятие № 4. Анализ нормативных правовых актов в области защиты информации		4/1		
	Самостоятельная работа			2/2	Самостоятельное изучение материалов, подготовка к практическому занятию
ОПК-5 ИОПК-5.1, ИОПК-5.2	ТЕМА 5. ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ. ОРГАНЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Основное содержание: 1. Структура государственной системы защиты информации в РФ. 2. Полномочия ФСТЭК России и ФСБ России в области защиты информации. 3. Лицензирование и сертификация в области защиты информации.	3/2			Устный опрос
	Практическое занятие № 5.		4/2		

	Изучение полномочий регуляторов в сфере информационной безопасности (ФСТЭК России, ФСБ России)				
	Самостоятельная работа			2/2	Самостоятельное изучение материалов, подготовка к практическому занятию
ОПК-5 ИОПК-5.2	ТЕМА 6. ОРГАНИЗАЦИОННЫЕ И ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ Основное содержание: 1. Организационные меры защиты информации: разграничение доступа, режим и охрана, работа с кадрами. 2. Политика информационной безопасности организации. 3. Категорирование информации и объектов информатизации.	3/2			Практическое задание
	Практическое занятие № 6. Разработка фрагмента политики информационной безопасности организации		4/2		
	Самостоятельная работа			1/2	
ОПК-1 ИОПК-1.3	ТЕМА 7. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ И МЕТОДЫ ЗАЩИТЫ ОТ УТЕЧКИ Основное содержание: 1. Понятие технического канала утечки информации. 2. Виды технических каналов: акустический, виброакустический, электромагнитный, оптический. 3. Основные методы и средства защиты информации от утечки по техническим каналам.	3/2			Практическое задание
	Практическое занятие № 7. Анализ технических каналов		4/2		

	утечки информации типового объекта				
	Самостоятельная работа			1/2	Самостоятельное изучение материалов, подготовка к практическому занятию
ОПК-5 ИОПК-5.1, ИОПК-5.2	ТЕМА 8. ПРОГРАММНО-АППАРАТНЫЕ И КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ: ОБЩАЯ ХАРАКТЕРИСТИКА Основное содержание: 1. Общая характеристика программно-аппаратных средств защиты информации: средства защиты от несанкционированного доступа, антивирусные средства, межсетевые экраны. 2. Основы криптографической защиты информации: понятие шифрования, электронной подписи. 3. Средства защиты информации отечественного производства, включенные в реестры ФСТЭК России и ФСБ России.	3/2			Практическое задание / тестирование
	Практическое занятие № 8. Обзор и сравнительный анализ отечественных программно-аппаратных средств защиты информации		6/2		
	Самостоятельная работа			2/2	Самостоятельное изучение материалов, подготовка к практическому занятию
	ИТОГО	24/12	34/12	14/39	

Примечание: -/- объем часов соответственно для очной и очно-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 системного и критического мышления, работы с нормативными правовыми актами, анализа угроз и рисков информационной безопасности (включая проведение интерактивных лекций, разбора практических ситуаций, анализ нормативных документов и типовых моделей угроз).

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- балльно-рейтинговая технология оценивания;
- электронное обучение;
- проблемное обучение;
- разбор конкретных ситуаций (кейс-метод);
- информационные технологии, применяемые в электронной информационно-образовательной среде университета.

Для оценки знаний, умений, навыков и уровня сформированности компетенций по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. 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 аудитории с применением мультимедийного проектора в виде учебной презентации или в ЭИОС университета.

Отдельные вопросы предлагаются для самостоятельного изучения (конспектируются).

Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям, 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 занятиях семинарского типа / на практических занятиях

Практические занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы дисциплины. Основной формой проведения практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение практических задач, разбор нормативных документов, типовых моделей угроз и ситуаций.

Практические занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и навыков анализа угроз, нормативных правовых актов и подготовки докладов/сообщений 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.

4.4. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине.

Самостоятельная работа студентов включает:

- изучение учебной литературы и нормативных правовых актов по курсу;
- подготовку докладов и сообщений;
- решение практических ситуаций и задач;
- работу с ресурсами информационно-телекоммуникационной сети «Интернет», в том числе с официальными сайтами регуляторов в области ИБ;
- подготовку к тестированию по темам курса;
- подготовку к промежуточной аттестации по курсу.

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

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. Мельников, В. П. Информационная безопасность и защита информации : учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков. – Москва : Академия. – Текст : электронный.
2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – Москва : ДМК Пресс. – Текст : электронный.
3. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : учебное пособие / А. А. Малюк. – Москва : Горячая линия – Телеком. – Текст : электронный.
4. Родичев, Ю. А. Информационная безопасность: нормативно-правовые аспекты : учебное пособие / Ю. А. Родичев. – Санкт-Петербург : Питер. – Текст : электронный.

Дополнительная литература:

5. Ярочкин, В. И. Информационная безопасность : учебник для вузов / В. И. Ярочкин. – Москва : Академический Проект. – Текст : непосредственный.
6. Гатчин, Ю. А. Теория информационной безопасности и методология защиты информации / Ю. А. Гатчин, В. В. Сухостат. – Санкт-Петербург : СПбГУ ИТМО. – Текст : непосредственный.
7. Бабаш, А. В. Информационная безопасность. Лабораторный практикум / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. – Москва : КноРус. – Текст : непосредственный.
8. Учебно-методическое пособие по дисциплине «Основы информационной безопасности» : для студентов направления подготовки 10.03.01 «Информационная безопасность» / Поволж. гос. ун-т сервиса (ФГБОУ ВО «ПВГУС»); сост.: Ю. С. Мунирова, Е. А. Курцев. – Тольятти : ПВГУС. – Текст : электронный.

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

1. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) : сайт. – URL: <https://fstec.ru> – Текст : электронный.
2. Банк данных угроз безопасности информации ФСТЭК России (БДУ) : сайт. – URL: <https://bdu.fstec.ru> – Текст : электронный.
3. Официальный сайт Федеральной службы безопасности Российской Федерации : сайт. – URL: <https://www.fsb.ru> – Текст : электронный.
4. eLIBRARY.RU : научная электронная библиотека : сайт. – URL: <https://elibrary.ru> – Текст : электронный.

5. КонсультантПлюс : справочная правовая система : сайт. – URL: <http://www.consultant.ru> – Текст : электронный.

6. Электронная библиотечная система Поволжского государственного университета сервиса : сайт / ФГБОУ ВО «ПВГУС». – Тольятти. – URL: <http://elib.tolgas.ru> – Режим доступа: для авториз. пользователей. – Текст : электронный.

7. Электронно-библиотечная система Znanium.com : сайт / ООО «ЗНАНИУМ». – Москва. – URL: <https://znanium.com/> – Режим доступа: для авториз. пользователей. – Текст : электронный.

8. Электронно-библиотечная система Лань : сайт / ООО «ЭБС ЛАНЬ». – Москва. – URL: <https://e.lanbook.com/> – Режим доступа: для авториз. пользователей. – Текст : электронный.

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	из внутренней сети университета (лицензионный договор)
3	КонсультантПлюс	из внутренней сети университета (лицензионный договор)
4	Антивирусное программное обеспечение отечественного производства	из внутренней сети университета (лицензионный договор)
5	СДО MOODLE	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).

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 «Интернет» 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; 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 балльная шкала, %	100 балльная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
зачет	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	Баллов за 1 точку	Макс. балл
Устный опрос	4	5	20
Решение практических заданий	8	5	40
Тестирование по темам курса	2	10	20
Доклад/сообщение	2	10	20
Итого			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 занятиям (темы докладов/сообщений, практических заданий)

1. Основные понятия и категории информационной безопасности (информация, защита информации, безопасность информации, конфиденциальность, целостность, доступность).

2. Классификация угроз информационной безопасности: по природе возникновения, по объекту воздействия, по способу реализации.

3. Разработка модели нарушителя для типовой автоматизированной (информационной) системы.

4. Анализ Федерального закона «Об информации, информационных технологиях и о защите информации» и иных нормативных правовых актов в области защиты информации.

5. Полномочия и функции ФСТЭК России и ФСБ России в области обеспечения информационной безопасности.

6. Разработка фрагмента политики информационной безопасности организации: цели, задачи, ответственность.

7. Технические каналы утечки информации и организационно-технические методы защиты от утечки.

8. Обзор и сравнительный анализ отечественных программно-аппаратных и криптографических средств защиты информации.

8.2.2. Типовые тестовые задания для текущего контроля

Правильные варианты ответов выделены жирным шрифтом.

1. Что из перечисленного относится к основным свойствам защищаемой информации:

А) конфиденциальность, целостность, доступность

Б) стоимость, объем, актуальность

В) язык, формат, носитель

Г) автор, дата создания, гриф

2. Угроза, реализуемая в результате случайных ошибок персонала, относится к угрозам:

А) техногенным

Б) антропогенным

В) стихийным

Г) программным

3. Совокупность предположений о возможностях нарушителя, которые он может использовать для разработки и проведения атак, называется:

- А) моделью угроз
- Б) моделью нарушителя**
- В) политикой безопасности
- Г) аудитом безопасности

4. Основным федеральным законом, регулирующим отношения в сфере защиты информации в РФ, является:

- А) Федеральный закон «Об информации, информационных технологиях и о защите информации»**
- Б) Гражданский кодекс РФ
- В) Трудовой кодекс РФ
- Г) Федеральный закон «О рекламе»

5. Орган государственной власти, осуществляющий техническое регулирование в области защиты информации в РФ:

- А) ФСТЭК России**
- Б) Роспотребнадзор
- В) Федеральная налоговая служба
- Г) Росстат

6. К организационным мерам защиты информации относится:

- А) установка межсетевого экрана
- Б) разграничение доступа сотрудников к информационным ресурсам**
- В) шифрование трафика
- Г) применение антивирусного программного обеспечения

7. Технический канал утечки информации, связанный с преобразованием акустических сигналов в электрические, называется:

- А) электромагнитным
- Б) акустоэлектрическим**
- В) оптическим
- Г) материально-вещественным

8. Документ, содержащий систематизированное описание угроз безопасности информации, актуальных для информационных систем, поддерживаемый ФСТЭК России, называется:

- А) банк данных угроз безопасности информации**
- Б) реестр отечественного программного обеспечения
- В) доктрина информационной безопасности
- Г) технический регламент

Вопросы для устного опроса

1. Понятие информации, её свойства и виды.
2. Информация как объект права собственности и стратегический ресурс.
3. Основные понятия и определения в области информационной безопасности.
4. Соотношение понятий «защита информации» и «информационная безопасность».

5. Роль и место информации в жизни личности, общества и государства.
6. Понятие угрозы безопасности информации, её основные характеристики.
7. Классификация угроз информационной безопасности по природе возникновения.
8. Классификация угроз информационной безопасности по объекту воздействия.
9. Источники угроз информационной безопасности: антропогенные, техногенные, стихийные

Темы докладов/сообщений

1. Конституционные основы обеспечения информационной безопасности в Российской Федерации.
2. Федеральный закон «Об информации, информационных технологиях и о защите информации»: общая характеристика.
3. Правовой режим персональных данных: основные требования законодательства.
4. Правовой режим государственной тайны.
5. Правовой режим коммерческой тайны.
6. Доктрина информационной безопасности Российской Федерации: цели и задачи.
7. Структура государственной системы защиты информации в Российской Федерации.
8. Полномочия и функции ФСТЭК России в области защиты информации.
9. Полномочия и функции ФСБ России в области защиты информации.
10. Лицензирование деятельности в области защиты информации.
11. Сертификация средств защиты информации.

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 вопросам к зачету предполагается, как правило, для сдачи академической задолженности.

Перечень вопросов для подготовки к зачету

ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

1. Понятие информации, её свойства и виды.
2. Информация как объект права собственности и стратегический ресурс.
3. Основные понятия и определения в области информационной безопасности.
4. Соотношение понятий «защита информации» и «информационная безопасность».
5. Роль и место информации в жизни личности, общества и государства.
6. Понятие угрозы безопасности информации, её основные характеристики.
7. Классификация угроз информационной безопасности по природе возникновения.
8. Классификация угроз информационной безопасности по объекту воздействия.
9. Источники угроз информационной безопасности: антропогенные, техногенные, стихийные.
10. Понятие нарушителя информационной безопасности, его категории.
11. Модель нарушителя и её роль при построении системы защиты информации.
12. Модель угроз безопасности информации: назначение и структура.
13. Объекты защиты информации: информационные ресурсы, средства и системы информатизации.
14. Технические каналы утечки информации: понятие и классификация.
15. Акустический и виброакустический каналы утечки информации.
16. Электромагнитный канал утечки информации.
17. Основные методы защиты информации от утечки по техническим каналам.
18. Значение информационной безопасности для обеспечения интересов личности, общества и государства.

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

1. Конституционные основы обеспечения информационной безопасности в Российской Федерации.
2. Федеральный закон «Об информации, информационных технологиях и о защите информации»: общая характеристика.
3. Правовой режим персональных данных: основные требования законодательства.
4. Правовой режим государственной тайны.
5. Правовой режим коммерческой тайны.
6. Доктрина информационной безопасности Российской Федерации: цели и задачи.
7. Структура государственной системы защиты информации в Российской Федерации.
8. Полномочия и функции ФСТЭК России в области защиты информации.
9. Полномочия и функции ФСБ России в области защиты информации.
10. Лицензирование деятельности в области защиты информации.
11. Сертификация средств защиты информации.
12. Организационные меры защиты информации: разграничение доступа, режим и охрана.
13. Политика информационной безопасности организации: назначение и структура.

14. Категорирование информации и объектов информатизации.
15. Общая характеристика программно-аппаратных средств защиты информации.
16. Общая характеристика средств антивирусной защиты и межсетевого экранирования.
17. Основы криптографической защиты информации: понятие шифрования и электронной подписи.
18. Реестры отечественных программно-аппаратных средств защиты информации.