Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2026 13:38:13
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

Б.1.О.03.16 «Основы управления информационной безопасностью»

Направление подготовки:

10.03.01 «Информационная безопасность»

Направленность (профиль):

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

Квалификация выпускника: **бакалавр**

Тольятти 2025

Рабочая программа дисциплины «Основы управления информационной безопасностью» 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 принципах, функциях и методах управления информационной безопасностью организации;

– формирование способности участвовать в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;

– формирование умения организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами и методическими документами ФСТЭК России и ФСБ России.

- формирование у обучающихся общепрофессиональных компетенций, *направленных на развитие навыков исследовательской деятельности*

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-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ИОПК-10.1. Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики ИОПК-10.2. Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности ИОПК-10.3. Осуществляет управление процессом обеспечения информационной безопасности	Знает: – принципы и функции управления информационной безопасностью; структуру и порядок разработки политики информационной безопасности организации – основы построения и функционирования системы менеджмента информационной безопасности, методы оценки и управления рисками Умеет: – разрабатывать отдельные разделы политики информационной безопасности организации – организовывать выполнение комплекса мер по обеспечению информационной безопасности и управлять процессом их реализации на объекте защиты Владеет: – навыками управления процессом обеспечения	

		информационной безопасности, включая планирование, контроль и совершенствование системы защиты	
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИОПК-6.1. Применяет технологии, методы и средства защиты информации ограниченного доступа ИОПК-6.2. Знает и применяет положения действующих в РФ нормативных правовых актов, нормативных и методических документов по вопросам организации защиты информации ограниченного доступа	Знает: – технологии, методы и средства защиты информации ограниченного доступа – нормативные правовые акты, нормативные и методические документы ФСТЭК России и ФСБ России по вопросам организации защиты информации ограниченного доступа Умеет: – организовывать защиту информации ограниченного доступа с учетом требований регуляторов – применять нормативные и методические документы при решении задач управления информационной безопасностью Владеет: – навыками организации защиты информации ограниченного доступа в соответствии с действующими нормативными правовыми актами	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к обязательной части Блока 1. Дисциплины (модули) программы бакалавриата (Б.1.О.03 Общепрофессиональный модуль).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем и структура дисциплины

Общая трудоёмкость дисциплины составляет **4 з.е. (144 час.)**, их распределение по видам работ 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.:	**76/36**
занятия лекционного типа (лекции)	28/12
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	48/24
Самостоятельная работа, всего	**41/99**
Самоподготовка по темам (разделам) дисциплины	-/ -
Выполнение курсового проекта /курсовой работы	- / -
Контроль (часы на экзамен)	**27/9**
Промежуточная аттестация	**Экзамен**

Примечание: *-/- объем часов соответственно для очной, 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, час			Формы текущего контроля (наименование оценочного средства)
		Контактная работа		Самостоятельная работа, час	
		Лекции, час	Практические занятия, час		
ОПК-10 ИОПК-10.1	**ТЕМА 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ОБЪЕКТ УПРАВЛЕНИЯ**	4/2			Устный опрос
	Основное содержание: 1. Понятие, цели и задачи управления информационной безопасностью. 2. Субъекты и объекты управления информационной безопасностью организации. 3. Принципы и функции управления информационной безопасностью (планирование, организация, контроль).				
	Практическое занятие № 1. Определение целей и задач управления информационной безопасностью для типовой организации		6/2		
	Самостоятельная работа			5/11	Самостоятельное изучение материалов, подготовка к практическому заданию
ОПК-10 ИОПК-10.1	**ТЕМА 2. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ**	3/2			Практическое задание
	Основное содержание: 1. Понятие и назначение политики информационной				

	безопасности. 2. Структура и порядок разработки политики информационной безопасности. 3. Ответственность за нарушение положений политики информационной безопасности.				
	Практическое занятие № 2. Разработка фрагмента политики информационной безопасности организации		6/2		
	Самостоятельная работа			5/11	Самостоятельное изучение материалов, подготовка к практическому заданию
ОПК-10 ИОПК-10.2	**ТЕМА 3. СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**	4/2			Устный опрос / тестирование
	Основное содержание: 1. Понятие системы менеджмента информационной безопасности (СМИБ). 2. Цикл Деминга (PDCA) в управлении информационной безопасностью. 3. Стандарты серии ГОСТ Р ИСО/МЭК 27001 и их применение при построении СМИБ.				
	Практическое занятие № 3. Анализ структуры системы менеджмента информационной безопасности типовой организации		6/2		
	Самостоятельная работа			5/11	Самостоятельное изучение материалов, подготовка к практическому заданию

ОПК-10 ИОПК-10.2, ИОПК-10.3	**ТЕМА 4. ОЦЕНКА И УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**	3/2			Практическое задание
	Основное содержание: 1. Понятие риска информационной безопасности, его составляющие. 2. Методы идентификации и оценки рисков информационной безопасности. 3. Способы обработки рисков: снижение, принятие, передача, уклонение.				
	Практическое занятие № 4. Оценка рисков информационной безопасности для типовой информационной системы		6/2		
	Самостоятельная работа			5/11	Самостоятельное изучение материалов, подготовка к практическому заданию
ОПК-6 ИОПК-6.1	**ТЕМА 5. ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА**	4/2			Доклад/сообщение
	Основное содержание: 1. Понятие и виды информации ограниченного доступа (государственная тайна, конфиденциальная информация, персональные данные). 2. Технологии, методы и средства защиты информации ограниченного доступа. 3. Порядок допуска и доступа к информации ограниченного доступа.				
	Практическое занятие № 5.		6/2		

	Разработка перечня сведений конфиденциального характера организации				
	Самостоятельная работа			5/11	Самостоятельное изучение материалов, подготовка к практическому заданию
ОПК-6 ИОПК-6.2	**ТЕМА 6. НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ**	3/2			Устный опрос
	Основное содержание: 1. Система нормативных правовых актов, регламентирующих управление информационной безопасностью в РФ. 2. Методические документы ФСТЭК России и ФСБ России в области защиты информации ограниченного доступа. 3. Локальные нормативные акты организации в области информационной безопасности.				
	Практическое занятие № 6. Анализ методических документов регуляторов в области защиты информации ограниченного доступа		6/2		
	Самостоятельная работа			5/11	
ОПК-10 ИОПК-10.3	**ТЕМА 7. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**	4/2			Практическое задание
	Основное содержание: 1. Понятие инцидента информационной безопасности, его классификация. 2. Процесс управления				

	инцидентами: обнаружение, реагирование, расследование, устранение последствий. 3. Порядок информирования о компьютерных инцидентах, взаимодействие с ГосСОПКА.				
	Практическое занятие № 7. Разработка регламента реагирования на инциденты информационной безопасности		6/2		
	Самостоятельная работа			5/11	
ОПК-10, ИОПК-10.3; ОПК-6 ИОПК-6.1, ИОПК-6.2	**ТЕМА 8. КОНТРОЛЬ И АУДИТ ЭФФЕКТИВНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ**	3/2			Практическое задание / тестирование
	Основное содержание: 1. Понятие и виды контроля (аудита) информационной безопасности. 2. Показатели и критерии оценки эффективности системы управления информационной безопасностью. 3. Порядок проведения внутреннего аудита информационной безопасности организации.				
	Практическое занятие № 8. Разработка программы внутреннего аудита информационной безопасности организации		6/2		
	Самостоятельная работа			5/11	
	ИТОГО	**28/12**	**48/24**	**41/99**	

Примечание: *-/- объем часов соответственно для очной, 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. Аверченков, В. И. Организационная защита информации : учебное пособие / В. И. Аверченков, М. Ю. Рытов. – Москва : Флинта. – Текст : электронный.

2. Родичев, Ю. А. Информационная безопасность: нормативно-правовые аспекты : учебное пособие / Ю. А. Родичев. – Санкт-Петербург : Питер. – Текст : электронный.

3. Петренко, С. А. Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. – Москва : ДМК Пресс. – Текст : электронный.

4. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : учебное пособие / А. А. Малюк. – Москва : Горячая линия – Телеком. – Текст : электронный.

Дополнительная литература:

5. Милославская, Н. Г. Управление информационной безопасностью организации : учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва : Горячая линия – Телеком. – Текст : непосредственный.

6. Курило, А. П. Аудит информационной безопасности / А. П. Курило [и др.]. – Москва : БДЦ-пресс. – Текст : непосредственный.

7. ГОСТ Р ИСО/МЭК 27001. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Москва : Стандартинформ. – Текст : непосредственный.

8. Учебно-методическое пособие по дисциплине «Основы управления информационной безопасностью» : 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. Федеральное агентство по техническому регулированию и метрологии (Росстандарт) : сайт. – URL: https://www.rst.gov.ru – Текст : электронный.

5. eLIBRARY.RU : научная электронная библиотека : сайт. – URL: https://elibrary.ru – Текст : электронный.

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

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

8. Электронно-библиотечная система Znanium.com : сайт / ООО «ЗНАНИУМ». – Москва. – URL: https://znanium.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 компетенций по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. 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
Экзамен	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. Определение целей и задач управления информационной безопасностью для типовой организации.
2. Разработка фрагмента политики информационной безопасности организации: цели, задачи, ответственность.
3. Анализ структуры системы менеджмента информационной безопасности (СМИБ) организации на основе ГОСТ Р ИСО/МЭК 27001.
4. Оценка рисков информационной безопасности для типовой информационной системы, выбор способа обработки риска.
5. Разработка перечня сведений конфиденциального характера организации.
6. Анализ методических документов регуляторов (ФСТЭК России, ФСБ России) в области защиты информации ограниченного доступа.
7. Разработка регламента реагирования на инциденты информационной безопасности.
8. Разработка программы внутреннего аудита информационной безопасности организации.

8.2.2. Типовые тестовые задания для текущего контроля

Правильные варианты ответов выделены жирным шрифтом.

1. Совокупность взаимосвязанных элементов организации (политики, процедуры, ресурсы), предназначенных для установления политики и целей информационной безопасности и достижения этих целей, называется:

А) системой менеджмента информационной безопасности

Б) моделью нарушителя

В) реестром угроз

Г) технической документацией

2. Международный стандарт, устанавливающий требования к системе менеджмента информационной безопасности, — это:

А) ISO 9001

Б) ISO/IEC 27001

В) ISO 14001

Г) ISO 45001

3. Цикл управления, лежащий в основе построения системы менеджмента информационной безопасности (Plan-Do-Check-Act), называется циклом:

А) Деминга

Б) Портера
В) Файоля
Г) Тейлора

4. Документ, определяющий цели, задачи и принципы обеспечения информационной безопасности организации, называется:
А) политикой информационной безопасности
Б) моделью угроз
В) техническим заданием
Г) сметой расходов

5. Вероятностная характеристика возможности реализации угрозы и наступления неблагоприятных последствий для активов организации — это:
А) риск информационной безопасности
Б) инцидент информационной безопасности
В) аудит информационной безопасности
Г) политика информационной безопасности

6. Способ обработки риска, при котором организация решает продолжать деятельность без принятия дополнительных мер, называется:
А) снижением риска
Б) передачей риска
В) принятием риска
Г) уклонением от риска

7. Событие или группа событий, которые повлекли или могут повлечь за собой нарушение функционирования информационной системы, называются:
А) инцидентом информационной безопасности
Б) политикой информационной безопасности
В) моделью нарушителя
Г) аудитом информационной безопасности

8. Систематический, независимый и документированный процесс получения свидетельств и объективной оценки состояния информационной безопасности организации называется:
А) категорированием
Б) лицензированием
В) аудитом информационной безопасности
Г) сертификацией

Вопросы для устного опроса

1. Понятие, цели и задачи управления информационной безопасностью организации.
2. Субъекты и объекты управления информационной безопасностью.
3. Принципы и функции управления информационной безопасностью.
4. Понятие и назначение политики информационной безопасности организации.
5. Структура и порядок разработки политики информационной безопасности.
6. Ответственность за нарушение положений политики информационной безопасности.
7. Понятие системы менеджмента информационной безопасности (СМИБ).
8. Цикл Деминга (PDCA) в управлении информационной безопасностью.

Темы докладов/сообщений

1. Понятие и виды информации ограниченного доступа.
2. Правовой режим государственной тайны.
3. Правовой режим конфиденциальной информации и персональных данных.
4. Технологии, методы и средства защиты информации ограниченного доступа.
5. Порядок допуска и доступа персонала к информации ограниченного доступа.
6. Разработка перечня сведений конфиденциального характера организации.

7. Система нормативных правовых актов, регламентирующих управление информационной безопасностью в РФ.

8. Методические документы ФСТЭК России в области защиты информации ограниченного доступа.

9. Методические документы ФСБ России в области защиты информации ограниченного доступа.

10. Локальные нормативные акты организации в области информационной безопасности.

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

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

Устно-письменная форма по вопросам к экзамену предполагается, как правило, для сдачи академической задолженности.

Перечень вопросов для подготовки к экзамену

ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

1. Понятие, цели и задачи управления информационной безопасностью организации.
2. Субъекты и объекты управления информационной безопасностью.
3. Принципы и функции управления информационной безопасностью.
4. Понятие и назначение политики информационной безопасности организации.
5. Структура и порядок разработки политики информационной безопасности.
6. Ответственность за нарушение положений политики информационной безопасности.
7. Понятие системы менеджмента информационной безопасности (СМИБ).
8. Цикл Деминга (PDCA) в управлении информационной безопасностью.
9. Стандарты серии ГОСТ Р ИСО/МЭК 27001 и их применение при построении СМИБ.
10. Понятие риска информационной безопасности, его составляющие.
11. Методы идентификации и оценки рисков информационной безопасности.
12. Способы обработки рисков информационной безопасности.
13. Понятие инцидента информационной безопасности, его классификация.
14. Процесс управления инцидентами информационной безопасности.
15. Порядок информирования о компьютерных инцидентах, взаимодействие с ГосСОПКА.
16. Понятие и виды контроля (аудита) информационной безопасности.
17. Показатели и критерии оценки эффективности системы управления информационной безопасностью.
18. Порядок проведения внутреннего аудита информационной безопасности организации.

ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

1. Понятие и виды информации ограниченного доступа.
2. Правовой режим государственной тайны.
3. Правовой режим конфиденциальной информации и персональных данных.
4. Технологии, методы и средства защиты информации ограниченного доступа.
5. Порядок допуска и доступа персонала к информации ограниченного доступа.
6. Разработка перечня сведений конфиденциального характера организации.

7. Система нормативных правовых актов, регламентирующих управление информационной безопасностью в РФ.

8. Методические документы ФСТЭК России в области защиты информации ограниченного доступа.

9. Методические документы ФСБ России в области защиты информации ограниченного доступа.

10. Локальные нормативные акты организации в области информационной безопасности.

11. Лицензирование деятельности в области защиты информации.

12. Сертификация средств защиты информации.

13. Категорирование информации и объектов информатизации.

14. Организация защиты информации ограниченного доступа при взаимодействии с контрагентами.

15. Ответственность за нарушение требований по защите информации ограниченного доступа.