Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 31.05.2024 09:09:41
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.02.04 «ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки:
10.04.01 «Информационная безопасность»

Направленность (профиль):
«Информационная безопасность интеллектуальных и информационно-аналитических систем»

Квалификация выпускника: **магистр**

Тольятти 2022

Рабочая программа дисциплины *«Технологии обеспечения информационной безопасности»* разработана в соответствии с федеральным государственным образовательным стандартом высшего образования - *магистратура* по направлению подготовки *10.04.01 «Информационная безопасность»*, утвержденным приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. №1455
.

Составители:

Старший преподаватель (ученая степень, ученое звание) Ю.С. Мунирова (ФИО)

РПД обсуждена на заседании высшей школы интеллектуальных систем и кибертехнологий «02» 12 2022г., протокол № 4

Директор высшей школы интеллектуальных систем и кибертехнологий к. э. н., доцент (уч.степень, уч.звание) /О.А. Филиппова (ФИО)

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, направленных на развитие навыков исследовательской деятельности;
- формирование у обучающихся общепрофессиональных компетенций, необходимых для выбора и обоснования технологий обеспечения информационной безопасности объектов.

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 обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ИОПК-1.1. Понимает принципы, требования и структуру системы обеспечения информационной безопасности и защиты информации ИОПК-1.2. Проектирует техническое задание на создание системы обеспечения информационной безопасности и защиты информации	**Знает:** требования к системе обеспечения информационной безопасности; **Умеет:** разрабатывать проект технического задания на создание системы обеспечения информационной безопасности; **Владеет:** инструментарием формирования требований к системе обеспечения информационной безопасности	
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ИОПК-2.2. Проектирует систему обеспечения информационной безопасности, ее компоненты и подсистемы ИОПК-2.3. Разрабатывает технические проекты защищённых информационных систем	**Знает:** методы концептуального проектирования технологий систем обеспечения информационной безопасности **Умеет:** разрабатывать технический проект системы (подсистемы, либо компонента системы) обеспечения информационной безопасности **Владеет:** навыками проектирования подсистемы обеспечения информационной безопасности	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к *обязательной части* Блока 1. Дисциплины (модули) образовательной программы (Б1.О.02 Общепрофессиональный модуль).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем и структура дисциплины

Общая трудоёмкость дисциплины составляет **5 з.е. (180 час.)**, их распределение по видам работ и семестрам представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины, час	**180**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**30/14**
занятия лекционного типа (лекции)	12/6
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	10/6
лабораторные работы	8/2
Самостоятельная работа всего, в т.ч.:	**123/157**
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.

3.1. 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-1 ИОПК-1.1 ИОПК-1.2 ОПК-2 ИОПК-2.2 ИОПК-2.3	**ТЕМА 1. ПОНЯТИЕ СИСТЕМЫ, ТЕХНОЛОГИИ ФУНКЦИОНИРОВАНИЯ. СЛОЖНЫЕ СИСТЕМЫ. ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.**	2/2				
	Лабораторная работа № 1. Методы построения обобщенных критериев.		2/1			
	Практическое занятие № 1 «Понятие системы, технологии функционирования. Сложные системы. Технология обеспечения информационной безопасности»			2/2		Отчет по лабораторной работе
	Самостоятельная работа. Самостоятельное изучение учебных материалов.				23/27	Отчет по практической работе
ОПК-1 ИОПК-1.1 ИОПК-1.2 ОПК-2 ИОПК-2.2 ИОПК-2.3	**ТЕМА 2. ПРОЕКТИРОВАНИЕ И СОВЕРШЕНСТВО-ВАНИЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ЭТАПЫ. ЦЕЛИ И ЗАДАЧИ. ТРЕБОВАНИЯ. МЕТОДЫ И СПОСОБЫ. ПРОЕКТИРОВАНИЯ**	2/2				
	Лабораторная работа № 2. Экспертные методы оценок критериев.		2/1			
	Практическое занятие № 2. Проектирование и совершенствование технологии обеспечения информационной безопасности. Этапы. Цели и задачи. Требования. Методы и способы проектирования			2/2		Отчет по лабораторной работе
	Самостоятельная работа. Самостоятельное изучение учебных материалов.				20/26	Отчет по практической работе
ОПК-1 ИОПК-1.1 ИОПК-1.2 ОПК-2 ИОПК-2.2 ИОПК-2.3	**ТЕМА 3. АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ. МЕТОДОЛОГИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ**	2/2				
	Лабораторная работа № 3. Анализ характеристик системы управления на основе информационного графа		2/ -			
	Практическое занятие № 3. Автоматизированные системы. Методология обеспечения информационной безопасности автоматизированных систем			2/2		Отчет по лабораторной работе
	Самостоятельная работа. Самостоятельное изучение учебных материалов.				20/26	Отчет по практической работе
ОПК-1 ИОПК-1.1 ИОПК-1.2 ОПК-2 ИОПК-2.2 ИОПК-2.3	**ТЕМА 4. ТЕХНОЛОГИЯ СОЗДАНИЯ ЗАЩИЩЕННЫХ СИСТЕМ. АНАЛИЗ ТРЕБОВАНИЙ, УГРОЗ, УЯЗВИМОСТЕЙ ОБЪЕКТА ЗАЩИТЫ.**	2/-				
	Лабораторная работа № 4. Технология создания защищенных систем. Анализ требований, угроз, уязвимостей объекта		2/ -			Отчет по лабораторной работе Отчет по практической работе

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		
	защиты.					
	Практическое занятие № 4 . Способы описания структурного сопряжения элементов			2/-		
	Самостоятельная работа. Особенности построения защищенных информационных систем.				20/26	
ОПК-1 ИОПК-1.1 ИОПК-1.2 ОПК-2 ИОПК-2.2 ИОПК-2.3	**ТЕМА 5. ОСОБЕННОСТИ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ.**	2/-				Отчет по практической работе
	Практическое занятие № 5. Описание структурного сопряжения элементов и анализ взаимосвязей между ними.			2/-		
	Самостоятельная работа. Особенности построения защищенных информационных систем.				20/26	
ОПК-1 ИОПК-1.1 ИОПК-1.2 ОПК-2 ИОПК-2.2 ИОПК-2.3	**ТЕМА 6. ВЫЧИСЛЕНИЕ СТРУКТУРНО-ТОПОЛОГИЧЕСКИХ ХАРАКТЕРИСТИК СИСТЕМ УПРАВЛЕНИЯ.**	2/-				Устный опрос по теме
	Самостоятельная работа. Вычисление числовых характеристик системы управления с помощью задания числовой функции на структурном графе системы				20/26	
	ИТОГО	**12 / 6**	**8 / 2**	**10 / 6**	**123/ 157**	

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 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;*

- *проблемное обучение;*

- *разбор конкретных ситуаций;*

- *информационные технологии: Яндекс-документы, ЭИОС ПВГУС*

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.

Выполнение лабораторных работ 1-4 связанны 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.

Практическая подготовка предусматривает: решение прикладной задачи (кейса) при изучении тем 1-5.

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. Решение практических ситуаций и задач

Подготовка рефератов

3. Работу с ресурсами Интернет
4. Решение практических ситуаций в виде кейсов
5. Изучение практических материалов деятельности конкретных предприятий
6. Подготовку к экзамену по темам курса

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/

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. Информационная безопасность и защита информации : учеб. пособие по направлению "Приклад. информатика" / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - Документ read. - Москва : РИОР [и др.], 2022. - 336 с. - (Высшее образование). - Прил. - URL: https://znanium.com/read?id=393765 (дата обращения: 25.02.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01761-6. - 978-5-16-106532-7. - Текст : электронный. URL: https://znanium.com/read?id=393765

2. Нестеров, С. А. Основы информационной безопасности : учеб. пособие / С. А. Нестеров. - Изд. 5-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2022. - 322 с. - (Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/206279 (дата обращения: 20.10.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-4067-2. - Текст : электронный. URL: https://reader.lanbook.com/book/206279

3. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. - Изд. 4-е, стер. - Документ Reader. - Санкт-Петербург : Лань, 2022. - 124 с. - (Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/217445 (дата обращения: 06.10.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-44201-0. - Текст : электронный. URL: https://reader.lanbook.com/book/217445

Дополнительная литература

4. Ворона, В. А. Теоретические основы обеспечения безопасности объектов информатизации : учеб. пособие для вузов по направлению "Информ. безопасность" / В. А. Ворона, В. А. Тихонов, Л. В. Митрякова. - Москва : Горячая линия -Телеком, 2016. - 304 с. : ил. - (Учебное пособие для высших учебных заведений). - ISBN 978-5-9912-0524-5 : 588-50. - Текст : непосредственный.

5. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью : учеб. пособие для студентов вузов по направлению подгот. 090900 "Информ. безопасность" (уровни - бакалавр, магистр) / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - Москва : Горячая линия - Телеком, 2014. - 214 с. - (Вопросы управления информационной безопасностью. Кн. 4). - Прил. - ISBN 978-5-9912-0364-7 : 524-00. - Текст : непосредственный.

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

1. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации [Электронный ресурс]/ ФСТЭК России – ФСТЭК России. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty, свободный. – Заглавие с экрана.
2. Банк данных угроз безопасности информации // Федеральная служба по техническому и экспортному контролю. - Режим доступа: https://bdu.fstec.ru, свободный. – Заглавие с экрана.
3. Архив изданий по информационной безопасности [Электронный ресурс] – Режим доступа: http://lib.itsec.ru/articles2/allpubliks, свободный. – Заглавие с экрана.

4. Security Lab [Электронный ресурс] – Режим доступа: http://www.securitylab.ru/, свободный. – Заглавие с экрана.

5. Научный журнал «Вопросы кибербезопасности» [Электронный ресурс] – Режим доступа: http://cyberrus.com/, свободный. – Заглавие с экрана.

6. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы eLIBRARY.RU: научная электронная библиотека

7. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы Консультант Плюс [Электронный ресурс]: Справочная правовая система. - Режим доступа: http://www.consultant.ru/.

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	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)
5	Microsoft Windows, Linux;	Программное обеспечение для выполнения лабораторных работ операционные системы семейств

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 Г-402,405,413,409», оснащенная следующим оборудованием: 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 «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
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	Количество баллов за 1 контр. точку	Макс. возм. кол-во баллов
Устный опрос по теме	1	5	5
Отчет по лабораторной работе	4	10	40
Отчет по практическому занятию	5	10	50
Творческий рейтинг (участие в конференциях, олимпиадах и т.п.) Дополнительные баллы за активное изучение дисциплины и др.	1	5	5
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

8.1.1. Типовые задания к практическим (семинарским) занятиям

Примерный список вопросов для устного контроля:

1. Какой вид идентификации и аутентификации получил наибольшее распространение?:
2. Заключительным этапом построения системы защиты является
3. Какие угрозы безопасности информации являются преднамеренными?
4. Какой подход к обеспечению безопасности имеет место?
5. Таргетированная атака — это.
6. Кто является основным ответственным за определение уровня классификации информации?
7. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует обычно предпринять руководству?
8. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены
9. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
10. Называется процедурой пошаговая инструкция по выполнению задачи?

8.1.1. Типовые задания к практическим занятиям

Практическое занятие 1. Понятие системы, технологии функционирования. Сложные системы. Технология обеспечения информационной безопасности

- Изучение принципов работы сложных систем и их влияние на информационную безопасность.
- Анализ технологий функционирования информационных систем.
- Оценка уязвимостей сложных систем и разработка мер по обеспечению информационной безопасности.

Практическое занятие 2. Проектирование и совершенствование технологии обеспечения информационной безопасности. Этапы. Цели и задачи. Требования. Методы и способы проектирования.

- Проектирование технологии обеспечения информационной безопасности для конкретной организации или проекта.
- Определение целей и задач обеспечения безопасности информации.

- Разработка требований к системе безопасности, выбор методов и способов обеспечения безопасности.

Практическое занятие 3. Автоматизированные системы. Методология обеспечения информационной безопасности автоматизированных систем

Изучение методологии обеспечения информационной безопасности автоматизированных систем.

- Анализ уязвимостей автоматизированных систем и разработка мер по защите информации.
- Практическое тестирование систем на проникновение и анализ результатов.

Практическое занятие 4.Способы описания структурного сопряжения элементов

-Составление структурных схем элементов информационной системы.

- Описание структурного сопряжения элементов и анализ взаимосвязей между ними.

Практическое занятие 5. Описание структурного сопряжения элементов и анализ взаимосвязей между ними

Выполняется на основе 4 практической работы

-Составление структурных схем элементов информационной системы.

- Описание структурного сопряжения элементов и анализ взаимосвязей между ними.
- Проведение аудита системы на предмет соответствия описанным структурным связям и выявление возможных уязвимостей.

8.1.2. Типовые задания для лабораторных работ

Лабораторная работа № 1. Методы построения обобщенных критериев.

Изучение различных методов построения обобщенных критериев оценки информационной безопасности.

- Сравнение и анализ эффективности различных методов на примере конкретной информационной системы.
- Разработка математической модели обобщенного критерия для оценки уровня информационной безопасности.

Лабораторная работа № 2. Экспертные методы оценок критериев.

Изучение экспертных методов оценки критериев информационной безопасности.

- Проведение экспертного опроса для оценки важности различных критериев безопасности.
- Анализ результатов экспертной оценки и принятие решений по улучшению информационной безопасности.

Лабораторная работа № 3. Анализ характеристик системы управления на основе информационного графа

- Построение информационного графа системы управления информационной безопасностью.
- Анализ структуры графа, выявление ключевых элементов и связей между ними.
- Оценка эффективности системы управления на основе полученных характеристик и предложение улучшений.

Лабораторная работа № 4. Технология создания защищенных систем. Анализ требований, угроз, уязвимостей объекта защиты.

- Анализ требований к системе защиты информации на примере конкретного объекта.
- Определение потенциальных угроз и уязвимостей объекта защиты.
- Разработка технологии создания защищенной системы, включая меры по предотвращению угроз и устранению уязвимостей.

8.2. 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 экзаменационным билетам предполагается, как правило, для сдачи академической задолженности.

Перечень вопросов для подготовки к экзамену по дисциплине «Технологии обеспечения информационной безопасности»

ОПК-1: ИОПК-1.1, ИОПК-1.2. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.

1. Что такое информация, субъекты информационных отношений?
2. Дайте определение Информационной технологии.
3. Компьютерная система-это…
4. Элементы и подсистемы, управление и информация, самоорганизация.
5. Раскройте терм информационная безопасность
6. Определение автоматизированной системы
7. Свойства информации
8. Что такое уязвимость?
9. Основные принципы системного подхода при создании сложных систем.
10. Технология функционирования сложной системы.
11. Перечислите основные объекты информационной безопасности. Дайте их определения.
12. Понятия ущерба, риска и угрозы.
13. Основные угрозы безопасности информации АС и их классификация.
14. Каково назначение Политики информационной безопасности?
15. Для чего нужна стандартизация в сфере информационной безопасности?
16. Какую информацию относят к секретной, конфиденциальной?
17. Цели и задачи проектирования ИБ
18. Что такое система физической защиты объекта?
19. Перечислите основные риски ИБ. Дайте их определения.

ОПК-2: ИОПК-2.2, ИОПК-2.3. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.

20. Какие требования предъявляются к комплексной системе безопасности объекта?
21. В чем суть гарантированного уничтожения данных?
22. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
23. Охарактеризуйте понятие большие данные.
24. Какую информацию относят к секретной, конфиденциальной?
25. Какие характеристики сотрудников и почему косвенно могут указывать на них как на потенциальных злоумышленников или нарушителей политики обеспечения информационной безопасности?
26. Какие применяются методы защиты информации от промышленного шпионажа?
27. Какие цели и задачи проведения тренингов по безопасности для сотрудников организации?
28. Какие организационные меры обеспечения безопасности Вы знаете?
29. Какие технические меры обеспечения безопасности Вы знаете?
30. Основные принципы обеспечения ИБ
31. Основные функции системы безопасности.
32. Основные принципы политики ИБ.

33. Какое свойство информации является наиболее актуальным при обеспечении ИБ? Дайте его определение.
34. Свойство информации при котором невозможно ее искажение…
35. Охарактеризуйте ИБ поиска информации.
36. Охарактеризуйте ИБ обработки данных.
37. Охарактеризуйте эмерджентные технологии.
38. При использовании какого метода защиты пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности?
39. Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)?
40. Какие средства защиты информации предназначены для выполнения функций защиты информационной системы с помощью программных средств?
41. Укажите модель управления доступом, к которой относится основная теорема безопасности.
42. Какие виды информации существуют в зависимости от категории доступа к ней?
43. Защищаемая информация – это..
44. Правовые методы обеспечения ИБ
45. Способы представления информации о правах доступа.
46. Характеристика качества
47. Показатели и критерии эффективности
48. Методические вопросы оценки эффективности сложных систем.
49. Дайте определение понятию «ядро безопасности»
50. Кратко опишите архитектуру защищенной системы.