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.В.01.06 «Интеграция систем обработки и защиты информации»

Направление подготовки:
10.04.01 «Информационная безопасность»

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

Квалификация выпускника: **магистр**

Тольятти 2022

Рабочая программа дисциплины «Интеграция систем обработки и защиты информации» 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	Ю.С. Мунирова
(ученая степень, ученое звание)	(ФИО)

РПД обсуждена на заседании высшей школы интеллектуальных систем и кибертехнологий 02.12.2022 г., протокол № 4

Директор высшей школы интеллектуальных систем и кибертехнологий

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

Целью освоения дисциплины является:

– формирование у обучающихся профессиональных компетенций, необходимых для решения задач профессиональной деятельности;

– 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
ПК-4. Способен разработать архитектуру системы защиты информации и провести анализ уязвимости и эффективности её модели с учетом специфики деятельности организации и обрабатываемых данных	ИПК-4.3. Разрабатывает архитектуру системы защиты информации автоматизированных систем, а также интеллектуальных и информационно-аналитических систем в частности	**Знает:** Принципы построения архитектуры систем защиты информации. Основные угрозы и уязвимости, с которыми сталкиваются информационные системы. **Умеет:** Разрабатывать архитектуру системы защиты информации с учетом специфики деятельности организации. Проводить анализ уязвимостей информационных систем и разрабатывать меры по их устранению. **Владеет:** Умением проводить анализ рисков безопасности и разрабатывать соответствующие стратегии защиты..	06.033 Специалист по защите информации в автоматизированных системах
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:** Принципы построения защищенных информационных систем; Технические меры обеспечения информационной безопасности; **Умеет:** Разрабатывать технический проект системы обеспечения информационной безопасности; Проектировать компоненты и подсистемы защищенных информационных систем. **Владеет:** Навыками применения технических мер безопасности в разработке информационных систем; Методиками анализа угроз и рисков информационной безопасности.	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1. Дисциплины профессиональный модуль образовательной программы (Б.1.В.01 Профессиональный 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 и семестрам представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины, час	**144**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**28/12**
занятия лекционного типа (лекции)	12/4
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	8/4
лабораторные работы	8/4
Самостоятельная работа всего, в т.ч.:	**116/128**
Самоподготовка по темам (разделам) дисциплины	-/-
Выполнение курсового проекта /курсовой работы	-/-
Контроль (часы на зачет)	**-/4**
Промежуточная аттестация	**Зачет**

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-2 ИОПК-2.2 ИОПК-2.3 ПК-4 ИПК-4.3	**ТЕМА 1. РАЗРАБОТКА И РЕАЛИЗАЦИЯ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ, ВКЛЮЧАЮЩИХ В СЕБЯ ТЕХНИЧЕСКИЕ, ОРГАНИЗАЦИОННЫЕ И ПРАВОВЫЕ МЕРЫ**	2 / 2				Отчет по лабораторной работе Отчет по практическому занятию
	Лабораторная работа № 1. Разработка и реализация системы мониторинга уязвимостей в информационной инфраструктуре организации.		2/ 2			
	Практическое занятие № 1 Разработка и реализация комплексных систем защиты информации, включающих в себя технические, организационные и правовые меры			2 / 2		
	Самостоятельная работа. Изучение комплексных систем защиты информации				23 / 25	
ОПК-2 ИОПК-2.2 ИОПК-2.3 ПК-4 ИПК-4.3	**ТЕМА 2. ИССЛЕДОВАНИЕ МЕТОДОВ И ТЕХНОЛОГИЙ ИНТЕГРАЦИИ РАЗЛИЧНЫХ СИСТЕМ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ, В ТОМ ЧИСЛЕ С ИСПОЛЬЗОВАНИЕМ ОБЛАЧНЫХ ТЕХНОЛОГИЙ**	2 / 2				Отчет по лабораторной работе Отчет по практическому занятию
	Лабораторная работа № 2 Проведение аудита безопасности информационной системы с целью выявления уязвимостей и разработка плана их устранения		2/ 2			
	Практическое занятие № 2. Управление корпоративными данными и дата-центричная архитектура			2/ 2		
	Самостоятельная работа. Технологий интеграции различных систем обработки и защиты информации				23/25	
ОПК-2 ИОПК-2.2 ИОПК-2.3 ПК-4 ИПК-4.3	**ТЕМА 3. АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РАЗРАБОТКА СТРАТЕГИЙ ИХ МИНИМИЗАЦИИ**	2/ -				Отчет по лабораторной работе Отчет по практическому занятию
	Лабораторная работа № 3 Анализ системы защиты информации.		2/ -			
	Практическое занятие № 3 Моделирование системы защиты информации			2/ -		
	Самостоятельная работа. Разработка стратегий минимизации рисков ИБ				23/25	
ОПК-2 ИОПК-2.2 ИОПК-2.3 ПК-4 ИПК-4.3	**ТЕМА 4. ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ И РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ИХ ОПТИМИЗАЦИИ**	2/ -				Отчет по лабораторной работе Отчет по практическому занятию
	Лабораторная работа № 4 Эволюция подходов к построению интегрированной информационной системы предприятия на основании запросов бизнеса к ИБ		2/ -			
	Практическое занятие № 4. Оценка эффективности систем обработки и защиты информации.			2/ -		

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		
	Самостоятельная работа. Оценка эффективности систем обработки и защиты информации и разработка рекомендаций по их оптимизации				23/25	
ОПК-2 ИОПК-2.2 ИОПК-2.3 ПК-4 ИПК-4.3	**ТЕМА 5. ИССЛЕДОВАНИЕ ВОПРОСОВ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИНТЕГРАЦИИ СИСТЕМ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ**	4/-				
	Самостоятельная работа. Развитие технологий и стандартов интеграции				24/28	
	ИТОГО	**12 / 4**	**8 / 4**	**8/ 4**	**116/ 128**	

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: Miro, 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 1-4.

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
3. Работу с ресурсами Интернет
4. Решение практических ситуаций в виде кейсов
5. Изучение практических материалов деятельности конкретных предприятий
6. Подготовка рефератов
7. Подготовку к тестированию по темам курса
8. Подготовку к промежуточной аттестации зачет по курсу

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. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник по направлению подгот. "Информ. безопасность" / М. В. Тумбинская, М. В. Петровский. - Изд. 2-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2022. - 344 с. - (Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/256133 (дата обращения: 29.09.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-45046-6 : 0-00. - Текст : электронный. URL: https://reader.lanbook.com/book/256133

Дополнительная литература

2. 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.

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

1. КонсультантПлюс [Электронный ресурс]: Справочная правовая система. - Режим доступа: http://www.consultant.ru/.
2. Электронная библиотечная система Поволжского государственного университета сервиса [Электронный ресурс]. – Режим доступа: http://elib.tolgas.ru./ - Загл. с экрана.
3. Электронно-библиотечная система Znanium.com [Электронный ресурс]. - Режим доступа: http://znanium.com/. – Загл. с экрана.
4. Электронно-библиотечная система «Издательство Лань» [Электронный ресурс]. - Режим доступа: https://e.lanbook.com/. – Загл. с экрана.
5. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. - Режим доступа: http://elibrary.ru/defaultx.asp. - Загл с экрана.
6. Открытое образование [Электронный ресурс]. - Режим доступа: https://openedu.ru/. - Загл с экрана.
7. Polpred.com. Обзор СМИ. Полнотекстовая, многоотраслевая база данных (БД) [Электронный ресурс]. - Режим доступа: http://polpred.com/. – Загл. с экрана.
8. Базы данных Всероссийского института научной и технической информации (ВИНИТИ РАН) по естественным, точным и техническим наукам Электронный ресурс]. - Режим доступа: http://www.viniti.ru. – Загл. с экрана.
9. Университетская информационная система Россия [Электронный ресурс]. - Режим доступа: http://uisrussia.msu.ru/. – Загл. с экрана.

5.3. Программное обеспечение

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

№ п/п	Наименование	Условия доступа
1	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	Microsoft Office	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
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	Количество баллов за 1 контр. точку	Макс. возм. кол-во баллов
Отчет по лабораторной работе	4	10	40
Отчет по практическому занятию	4	10	40
Творческий рейтинг (участие в конференциях, олимпиадах и т.п.) Дополнительные баллы за активное изучение дисциплиныи др.	1	20	20
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

Практическое занятие № 1 Разработка и реализация комплексных систем защиты информации, включающих в себя технические, организационные и правовые меры

- Разработать план комплексной системы защиты информации для конкретной организации, учитывая технические, организационные и правовые аспекты.
- Провести анализ угроз безопасности информации и определить необходимые меры по их предотвращению.
- Составить схему внедрения выбранных мер защиты информации и оценить их эффективность.

Практическое занятие № 2. Управление корпоративными данными и дата-центричная архитектура

- Проанализировать структуру корпоративных данных организации и разработать дата-центричную архитектуру информационной системы.
- Оценить текущий уровень управления корпоративными данными и предложить пути их улучшения.
- Разработать план по внедрению дата-центричной архитектуры и обосновать его целесообразность.

Практическое занятие № 3. Моделирование системы защиты информации

- Провести моделирование системы защиты информации с использованием специализированных инструментов или программных средств.
- Создать диаграмму угроз и уязвимостей информационной системы и определить ключевые моменты для улучшения безопасности.
- Разработать план мер по устранению выявленных уязвимостей и проверить их эффективность.

Практическое занятие № 4. Оценка эффективности систем обработки и защиты информации.

- Провести оценку эффективности текущих систем обработки и защиты информации в организации с использованием соответствующих методик.
- Составить отчет о результатах оценки, выявить слабые места в системах обработки и защиты информации.
- Предложить конкретные меры по улучшению эффективности систем обработки и защиты информации и обосновать их необходимость.

8.1.2. Типовые задания для лабораторных работ

Лабораторная работа 1 Разработка и реализация системы мониторинга уязвимостей в информационной инфраструктуре организации

- Настройка системы мониторинга уязвимостей в сети организации с использованием специализированных инструментов (например, OpenVAS, Nessus).
- Проведение сканирования сети на наличие уязвимостей и анализ результатов.
- Разработка отчета о выявленных уязвимостях и предложение мер по их устранению**.**

Лабораторная работа 2 Проведение аудита безопасности информационной системы с целью выявления уязвимостей и разработка плана их устранения

- Проведение аудита безопасности информационной системы с использованием методик аудита (например, OWASP Top 10, NIST SP 800-53).
- Анализ результатов аудита и выявление уязвимостей в ИС.
- Разработка плана мер по устранению уязвимостей с определением приоритетов и сроков.

Лабораторная работа 3 Анализ системы защиты информации

- Изучение текущей системы защиты информации в организации.
- Анализ структуры защиты информации, включая противодействие угрозам, контроль доступа, шифрование данных и т.д.
- Оценка эффективности системы защиты и предложение мер по ее улучшению.

Лабораторная работа 4 Эволюция подходов к построению интегрированной информационной системы предприятия на основании запросов бизнеса к ИБ

- Изучение запросов бизнеса к информационной безопасности предприятия.
- Анализ существующих подходов к построению интегрированной информационной системы на основе запросов бизнеса.
- Разработка концепции эволюции информационной системы предприятия с учетом требований к безопасности данных и процессов.

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

Форма проведения промежуточной аттестации по дисциплине: зачет по результатам накопительного рейтинга, в форме компьютерного тестирования)

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

Перечень вопросов и заданий для подготовки к зачету

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

1. Понятие интегрированной корпоративной информационной системы.
2. Основные типы интеграционных задач
3. Методология «открытых систем» и проблема интеграции.
4. Базовые модели интеграции (передача файлов, обмен сообщениями, удаленный вызов процедуры, использование общей базы данных) и их сильные и слабые стороны.
5. Уровни интеграции корпоративных приложений
6. Проблема стандартизации. Основные организации, занимающиеся утверждением стандартов.
7. Сценарии интеграции данных. Получение данных для хранилищ данных и систем бизнес-аналитики (технология ETL).
8. Платформы для интеграции корпоративной информации (Oracle Data Integrator,

Informatica power center, IBM Information Server).

9. Технологии Big Data и проблема интеграции.
10. Опишите самый современный подход интеграции бизнес процессов
11. Чего помогает добиться Композитное (составное) приложение
12. Как называется система позволяющая наращивать и записывать в себя информацию и выстраивающая интеграционную систему
13. Управления рисками информационной безопасности
14. Основные источники угроз и виды нарушений в области информационной безопасности.
15. Процесс управления непрерывностью. Преимущества и проблемы процесса.
16. Процесс управления безопасностью. Цели и преимущества процесса
17. Основные положения стандарта BS7799
18. Основные положения стандарта ISO 17799.
19. Система информационной безопасности предприятия (задачи системы, объекты защиты) Основные источники угроз и виды нарушений в области информационной безопасности.
20. Цели и задачи интеграции систем обработки и защиты информации
21. Что такое ИСОЗИ и какие принципы лежат в её основе?
22. Какие методы и технологии используются для защиты информации в интегрированных системах?
23. Как обеспечить совместимость между различными системами обработки и защиты информации?
24. Какие роли и обязанности возлагаются на интегратора систем обработки и защиты информации?
25. Какие технологии шифрования применяются для защиты информации в интегрированных системах обработки и защиты?
26. Как происходит интеграция систем мониторинга и аудита в информационной безопасности?
27. Как происходит проектирование и настройка интегрированных систем обработки и защиты информации?
28. Какие меры предпринимаются для обеспечения защиты от DDoS-атак в интегрированных системах обработки и защиты информации?

ПК-4: ИПК-4.3. Способен разработать архитектуру системы защиты информации и провести анализ уязвимости и эффективности её модели с учетом специфики деятельности организации и обрабатываемых данных.

29. Как обеспечить безопасность при передаче данных между различными подсистемами в интегрированных системах?
30. Какие методы аутентификации и авторизации используются в интегрированных системах обработки и защиты информации?
31. Каким образом осуществляется интеграция различных уровней защиты в информационных системах?
32. Какие протоколы и стандарты используются при интеграции систем обработки и защиты информации?
33. Какие меры предпринимаются для обеспечения защиты физической инфраструктуры в интегрированных системах обработки и защиты информации?
34. Какие меры предпринимаются для обеспечения безопасности в случае вывода из эксплуатации информационных систем или оборудования?
35. Какие методы и технологии используются для обнаружения и предотвращения утечек конфиденциальной информации в интегрированных системах обработки и защиты информации?
36. Как осуществляется обучение и повышение осведомленности сотрудников по вопросам информационной безопасности в интегрированных системах обработки и защиты информации?
37. Какие меры безопасности применяются для защиты от социальной инженерии в интегрированных системах обработки и защиты информации?

38. Какие меры предпринимаются для обеспечения безопасности виртуальных сред и облачных решений в интегрированных системах обработки и защиты информации?
39. Какие методы обеспечения целостности данных используются в интегрированных системах обработки и защиты информации?
40. Каким образом осуществляется резервное копирование и восстановление данных в интегрированных системах обработки и защиты информации?
41. Как обеспечивается защита от вредоносных программ и вирусов в интегрированных системах обработки и защиты информации?
42. Каким образом реализуется система управления уязвимостями в интегрированных системах обработки и защиты информации?
43. Какие методы используются для защиты от атак на прикладные уровни в интегрированных системах обработки и защиты информации?
44. Как обеспечивается безопасность в интернете вещей (IoT) в интегрированных системах обработки и защиты информации?
45. Какие методы используются для защиты от атак переполнения буфера в интегрированных системах обработки и защиты информации?
46. Как осуществляется мониторинг и анализ сетевого трафика в интегрированных системах обработки и защиты информации?
47. Каким образом осуществляется управление и контроль доступа к ресурсам в интегрированных системах обработки и защиты информации?
48. Как обеспечивается защита от атак на инфраструктуру облачных вычислений в интегрированных системах обработки и защиты информации?
49. Каким образом осуществляется контроль и защита информации при передаче
50. Понятие интегрированной корпоративной информационной системы. Концепция ERP (Enterprise Resource Planning)
51. Типовая архитектура ERP-систем. ERP-система как центр интеграционного решения.
52. Какие методы и технологии используются при разработке архитектуры системы защиты информации?
53. Какие уязвимости чаще всего находиться в модели защиты информации организации и какие меры предлагаются для их устранения?
54. Как учитывается специфика деятельности организации при разработке системы защиты информации?
55. Как оценить эффективность модели защиты информации и какие критерии оценки эффективности использовались?
56. Какие особенности обрабатываемых данных влияют на выбор методов защиты информации и какие меры принимаются для обеспечения их безопасности?
57. Интеграция систем обработки и защиты информации – это
58. Как организовать мониторинг безопасности в интегрированных системах обработки и защиты информации?
59. Как оценить уровень риска при использовании интегрированных систем?
60. Как можно оценить уровень готовности организации к внедрению интегрированных систем обработки и защиты информации?
61. Какие технологии используются для интеграции систем обработки и защиты информации?
62. Какие этапы проектирования интегрированных систем обработки и защиты информации выделяются?
63. Какие методики используются при проектировании интегрированных систем обработки и защиты информации
64. Как осуществляется реализация интегрированных систем обработки и защиты информации?
65. Как проводится оценка эффективности интегрированных систем?
66. Какие критерии эффективности учитываются при оценке интегрированных систем обработки и защиты информации?
67. Принципы построения архитектуры систем защиты информации.

68. Технические и организационные меры по обеспечению безопасности информационных систем

69. Сравнение и позиционирование подходов, рекомендации по использованию технологий. Критерии выбора оптимального способа интеграции приложений.

70. Какие меры предпринимаются для обеспечения безопасности виртуальных сред.