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.02.02 «Защищенные информационные системы»

Направление подготовки:
10.04.01 «Информационная безопасность»

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

Квалификация выпускника: **магистр**

Тольятти 2022

Рабочая программа дисциплины *«Защищенные информационные системы»* 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:

– изучение основ теории и практики разработки и эксплуатации защищённых информационных систем;

– 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-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ИОПК-2.3. Разрабатывает технические проекты защищённых информационных систем	**Знать:** методы разработки систем и комплексы управления информационной безопасностью с учетом особенностей объектов защиты; основные компоненты технического проекта; перечень необходимых исходных данных для проектирования подсистем либо компонентов системы. **Уметь:** организовывать и осуществлять контроль за разработкой технических проектов систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты; находить ведомственные документы в части проектирования подсистем и применения средств обеспечения информационной безопасности **Владеть:** навыками управления проектами систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты; навыками разработки проектов и комплексов управления информационной безопасностью с учетом особенностей объектов защиты.	
ОПК-4. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	ИОПК-4.3. Формирует планы и проекты технических разработок защищённых информационных систем	**Знать:** методы сбора, обработки, анализа и систематизации научно-технической информации; современную научно-техническую литературу, нормативные и методические документы по вопросам информационной безопасности. **Уметь:** выбирать методы и средства решения задачи в рамках проводимого исследования, вырабатывать планы и программы проведения научных исследований и технических разработок. **Владеть:** навыками сбора и обработки информации, разработки планов и программ научных исследований; навыками использования результатов обзора научно-технической литературы при решении вопросов информационной безопасности телекоммуникационных систем и сетей.	

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 **3 з.е. (108 час.)**, их распределение по видам работ и семестрам представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины, час	**108**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**34/10**
занятия лекционного типа (лекции)	12/4
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	12/4
лабораторные работы	10/2
Самостоятельная работа всего, в т.ч.:	**74/94**
Самоподготовка по темам (разделам) дисциплины	74/94
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-2.3; ОПК-4 ИОПК-4.3	**ТЕМА 1. ВВЕДЕНИЕ В ПРЕДМЕТ «ЗАЩИЩЁННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ»** Начальные сведения о задачах защищённых информационных систем (зис). Постановка и классификация задач. Конкретные аппаратные устройства и приложения для обеспечения информационной безопасности.	2/2				Устный опрос по теме
	Лабораторная работа № 1 «Защищенная web-ориентированная информационная система»		2/-			Отчет по лабораторной работе
	Самостоятельная работа: -Понятие системы, ее элементов и связей между ними. - Принципы работы систем и их классификация. - Взаимодействие подсистем в рамках информационных систем.				12/15	
ОПК-2, ИОПК-2.3; ОПК-4 ИОПК-4.3	**ТЕМА 2. ИНТЕГРАЛЬНАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ** Понятие о задаче интегральной безопасности информационных систем. Примеры конкретных задач интегральной безопасности. Физическая	2/-				Устный опрос по теме

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		
	безопасность информационных систем. Безопасность сетей и устройств. Безопасность ПО.					Отчет по лабораторной работе Отчет по практическому занятию
	Практическое занятие № 1 «Построение диаграммы вариантов использования в объектно-ориентированном языке UML»			2/-		
	Лабораторная работа № 2 «Пен-тест защищенной web-ориентированной системы»		2/-			
	Самостоятельная работа: -Системный подход к решению проблем и принятию решений. - моделирование систем и процессов в них. - методы оптимизации работы информационных систем.				12/15	
ОПК-2, ИОПК-2.3; ОПК-4 ИОПК-4.3	**ТЕМА 3.** **БЕЗОПАСНОСТЬ ХРАНЕНИЯ И ПЕРЕДАЧИ ИНФОРМАЦИИ** Обеспечение конфиденциальности, целостности и доступности данных. Постановка задачи, её структура. Частный, комплексный и интегральных подходы к решению проблемы передачи и хранения данных.	2/2				Устный опрос по теме Отчет по лабораторной работе Отчет по практическому занятию
	Лабораторная работа № 3 «Безопасность хранения и передачи информации»		2/2			
	Практическое занятие № 2 «Построение диаграммы классов и диаграммы последовательности»			2/2		
	Самостоятельная работа: -анализ уязвимостей информационных систем. - разработка стратегий защиты информации.				13/15	
ОПК-2, ИОПК-2.3; ОПК-4 ИОПК-4.3	**ТЕМА 4.** **МЕТОДЫ ПРОЕКТИРОВАНИЯ И АНАЛИЗА ИНФОРМАЦИОННЫХ СИСТЕМ** Постановка задачи проектирования и анализа защищенной информационной системы. Модель системы с общим перекрытием. Концептуальные требования направленные на обеспечение безопасности функционирования информационной системы. Важнейшие принципы построения архитектуры зис. Анализ безопасности зис.	2/-				Устный опрос по теме Отчет по лабораторной работе Отчет по практическому занятию
	Лабораторная работа № 4 «Защищенная система архитектуры Клиент-Сервер»		2/-			
	Практическое занятие №3 «Построение диаграммы коммуникаций и диаграммы деятельности»			2/2		
	Самостоятельная работа: - Постановка задачи проектирования и анализа защищенной информационной системы ,методы обнаружения и предотвращения кибератак.				13/15	
ОПК-2, ИОПК-2.3; ОПК-4 ИОПК-4.3	**ТЕМА 5.** **ОПРЕДЕЛЕНИЕ СТЕПЕНИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ** Постановка задачи защищённости ис. Наличие и полнота политики безопасности. Гарантированность безопасности.	2/-				Устный опрос по теме

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		
	Трёхуровневая модель параметров оценки защищенности ис. Аудит сетей связи. Мониторинг функционирования, обнаружение атак и принятие мер противодействия.					Отчет по лабораторной работе Отчет по практическому занятию
	Лабораторная работа № 5 «Пен-тест защищенной системы архитектуры Клиент-Сервер»		1/-			
	Практическое занятие № 4 «Построение диаграммы пакетов и диаграммы объектов»			2/-		
	Самостоятельная работа: -Определение степени защищенности информационной системы -Решение задач и кейсов, связанных с информационной безопасностью с использованием методов системного анализа.				12/17	
ОПК-2, ИОПК-2.3; ОПК-4 ИОПК-4.3	**ТЕМА 6. РЕАЛИЗАЦИЯ ПРОГРАММ ИНФОРМАЦИОННОЙ ЗАЩИТЫ И ЗАЩИТЫ ИНФОРМАЦИИ** Средства обеспечения надежного хранения информации с использованием технологии защиты на файловом уровне (file encryption system – fes). Средства авторизации и разграничения доступа к информационным ресурсам, а также защита от несанкционированного доступа к информации с использованием технологии токенов (смарт-карты, touch-memory, ключи для usb-портов и т.п.). Классификация vpn.средства обеспечения централизованного управления системой иб в соответствии с согласованной и утвержденной политикой безопасности.	2/-				Устный опрос по теме Отчет по лабораторной работе Отчет по практическому занятию
	Лабораторная работа № 6 «Защита информационной системы, обрабатывающей персональные данные»		1/-			
	Практическое занятие № 5 «Построение диаграмм коммуникации, обзора взаимодействия. Построение диаграммы компонентов и диаграммы развертывания».			4/-		
	Самостоятельная работа: -Средства защиты от внешних угроз при подключении к общедоступным сетям связи, а также средства управления доступом интернета с использованием технологии межсетевых экранов (firewall) и содержательной фильтрации (content inspection).				12/17	
	ИТОГО	**12/ 4**	**10/ 2**	**12/ 4**	**74/ 94**	

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 2- 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 1-6.

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. Жук А. П., Жук Е. П.,. Лепешкин О. М, Тимошкин А. И.. - 3-е изд. - Документ read. - Москва : РИОР [и др.], 2021. - 400 с. - (Высшее образование: Бакалавриат; Магистратура). - URL: https://znanium.com/read?id=367588 (дата обращения: 09.12.2020). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01759-3. - 978-5-16-013801-5. - 978-5-16-106478-8. - Текст : электронный.URL: https://znanium.com/read?id=367588

2. Баранова, Е. К.Моделирование системы защиты информации. Практикум : учеб. пособие для вузов по направлению "Приклад. информатика" / Е. К. Баранова, А. В. Бабаш. - Изд. 3-е, перераб. и доп. - Документ read. - Москва : РИОР [и др.], 2023. - 320 с. - (Высшее образование). - Прил. - URL: https://znanium.ru/read?id=435530 (дата обращения: 20.02.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01848-4. - 978-5-16-108538-7. - Текст : электронный.URL: https://znanium.ru/read?id=435530

Дополнительная литература

3. Бабаш, А. В. Актуальные вопросы защиты информации : монография / А. В. Бабаш, Е. К. Баранова. - Документ read. - Москва : РИОР [и др.], 2021. - 112 с. - (Научная мысль). - URL: https://znanium.com/read?id=375285 (дата обращения: 03.03.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01680-0. - 978-5-16-106277-7. - Текст : электронный. URL: https://znanium.com/read?id=375285

4. Бухтояров В. В., М. Н. Жукова, В. В. Золотарев [и др.]. Поддержка принятия решений при проектировании систем защиты информации : монография / - Документ read. - Москва : ИНФРА-М, 2020. - 131 с. - (Научная мысль). - URL: https://znanium.com/read?id=343296 (дата обращения: 02.03.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-100714-3. - Текст : электронный. URL: https://znanium.com/read?id=343296

5. Гвоздева, Т. В.Проектирование информационных систем. Стандартизация : учеб. пособие / Т. В. Гвоздева, Б. А. Баллод. - Изд. 2-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2021. - 250 с. - (Учебники для вузов. Специальная литература). - Прил. - URL: https://reader.lanbook.com/book/169810 (дата обращения: 21.03.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-7963-4. - Текст : электронный. URL: https://reader.lanbook.com/book/169810

6. Дубинин, Е. А. Оценка относительного ущерба безопасности информационной системы : монография / Е. А. Дубинин, Ф. Б. Тебуева, В. В. Копытов. - Документ read. - Москва : РИОР [и др.], 2022. - 192 с. - (Научная мысль). - Прил. - URL: https://znanium.com/read?id=400262 (дата обращения: 02.03.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01371-7. - 978-5-16-101863-7. - Текст : электронный. URL: https://znanium.com/read?id=400262

7. Клименко, И. С. Информационная безопасность и защита информации. Модели и методы управления : монография / И. С. Клименко. - Документ read. - Москва : Инфра-М, 2022. - 180 с. - (Научная мысль). - URL: https://znanium.com/read?id=397337 (дата обращения: 02.03.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-108124-2. - Текст : электронный. URL: https://znanium.com/read?id=397337

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 КонсультантПлюс [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	StarUML	Программное обеспечение для выполнения лабораторных работ
7	Ramus	Программное обеспечение для выполнения лабораторных работ
8	Bizagi Modeler	Программное обеспечение для выполнения лабораторных работ

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
Устный опрос по теме	6	5	30
Отчет по лабораторной работе	3	10	30
Отчет по практическому занятию	3	10	30
Творческий рейтинг (участие в конференциях, олимпиадах и т.п.) Дополнительные баллы за активное изучение дисциплины и др.	1	10	10
Итого по дисциплине			**100 баллов**

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

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

8.1.1. Типовые задания к практическим (семинарским) занятиям

Примерный список вопросов для устного контроля:

1. Что не относится к видам сервисов безопасности?
2. Что не относится к сервисам безопасности?
3. Что не является направлением инженерно-технической защиты информации?
4.К какому направлению инженерно-технической защиты информации относится «дезинформирование»?
5. Что не относится к средствам обнаружения злоумышленника?
6. Какое освещение не используется в качестве средства защиты?
7. Из-за чего возникает побочное электромагнитное излучение?
8. Какие технические средства не являются источниками излучения в технических каналах?
9. Что не относится к техническим методам защиты информации?
10. Что не является методом повышения надежности автоматизированных систем?

8.1.1. Типовые задания для практических работ

Практическое занятие № 1 «Построение диаграммы вариантов использования в объектно-ориентированном языке UML»

Цель работы: Познакомиться с процессом построения диаграммы вариантов использования (use case diagram) в объектно-ориентированном языке UML.

Задачи:

1. Изучить основные элементы диаграммы вариантов использования.
2. Выбрать предметную область для построения диаграммы.
3. Определить актеров и варианты использования.
4. Построить диаграмму вариантов использования в среде моделирования UML.

Требования к выполнению работы:

1. Должны быть определены как минимум 3 актера и 5 вариантов использования.
2. Диаграмма должна быть построена с использованием стандартных символов и нотаций UML.
3. Каждый вариант использования должен быть корректно описан и связан с соответствующим актером.
4. Должна быть представлена легенда, поясняющая обозначения на диаграмме.

Практическое занятие № 2 «Построение диаграммы классов и диаграммы последовательности»

Цель работы: Познакомиться с процессом построения диаграммы классов и диаграммы последовательности в объектно-ориентированном языке UML.

Задачи:

1. Изучить основные элементы диаграммы классов и диаграммы последовательности.
2. Выбрать предметную область для построения диаграмм.
3. Определить классы, атрибуты и методы для диаграммы классов.
4. Построить диаграмму классов и диаграмму последовательности в среде моделирования UML.

Требования к выполнению работы:

1. Должны быть определены как минимум 5 классов с их атрибутами и методами.
2. Должна быть построена связь между классами на диаграмме классов.
3. Должна быть представлена последовательность взаимодействия объектов на диаграмме последовательности.
4. Каждый метод должен быть корректно описан на диаграмме последовательности.
5. Должна быть представлена легенда, поясняющая обозначения на диаграммах.

Практическое занятие № 3 «Построение диаграммы коммуникаций и диаграммы деятельности»

Цель работы: Ознакомиться с процессом построения диаграммы коммуникаций и диаграммы деятельности в языке UML.

Задачи:

1. Изучить основные элементы диаграммы коммуникаций и диаграммы деятельности.
2. Выбрать предметную область для построения диаграмм.
3. Определить участников и связи между ними для диаграммы коммуникаций.
4. Построить диаграмму коммуникаций, отображающую взаимодействие участников.
5. Определить последовательность действий и условия для диаграммы деятельности.
6. Построить диаграмму деятельности, отражающую последовательность выполнения действий.

Требования к выполнению работы:

1. Должны быть определены как минимум 3 участника для диаграммы коммуникаций.
2. Должны быть опоказаны связи и сообщения между участниками на диаграмме коммуникаций.
3. Должна быть представлена последовательность действий с использованием различных узлов на диаграмме деятельности.
4. Каждый узел на диаграмме деятельности должен быть корректно описан.
5. Должна быть представлена легенда, поясняющая обозначения на диаграммах.

Практическое занятие № 4 «Построение диаграммы пакетов и диаграммы объектов»

Цель работы: Ознакомиться с процессом построения диаграммы пакетов и диаграммы объектов в языке UML.

Задачи:

1. Изучить основные элементы диаграммы пакетов и диаграммы объектов.
2. Выбрать предметную область для построения диаграмм.
3. Определить структуру пакетов и их взаимосвязи для диаграммы пакетов.
4. Построить диаграмму пакетов, отображающую структуру системы.
5. Определить объекты и их взаимодействие для диаграммы объектов.
6. Построить диаграмму объектов, отражающую взаимодействие объектов.

Требования к выполнению работы:

1. Должны быть определены как минимум 3 пакета для диаграммы пакетов.
2. Должны быть показаны связи между пакетами на диаграмме пакетов.
3. Должны быть определены как минимум 3 объекта для диаграммы объектов.
4. Должны быть показаны взаимодействия между объектами на диаграмме объектов.

5. Каждый объект на диаграмме объектов должен быть корректно описан.
6. Должна быть представлена легенда, поясняющая обозначения на диаграммах.

Практическое занятие № 5. «Построение диаграмм коммуникации, обзора взаимодействия. Построение диаграммы компонентов и диаграммы развертывания»
Цель занятия: научить студентов строить диаграммы коммуникации, обзора взаимодействия, а также диаграммы компонентов и развертывания для моделирования архитектуры программного обеспечения.
Требования к выполнению работы:
1. Введение в тему: объяснение студентам важности использования диаграмм для моделирования архитектуры ПО и обзора взаимодействия между компонентами.
2. Объяснение концепций диаграмм коммуникации и обзора взаимодействия: рассмотрение основных элементов, символов и правил построения этих типов диаграмм.

8.1.2. Типовые задания для лабораторных работ

Лабораторная работа № 1 «Защищенная web-ориентированная информационная система»
Цель работы: Создать защищенную web-ориентированную информационную систему с использованием современных технологий безопасности.
Задачи:
1. Изучить основные принципы безопасности web-приложений.
2. Выбрать технологический стек для разработки информационной системы.
3. Разработать архитектуру системы с учетом требований безопасности.
4. Создать пользовательский интерфейс для взаимодействия с системой.
5. Реализовать механизм аутентификации и авторизации пользователей.
6. Обеспечить защиту данных, передаваемых между клиентом и сервером.
7. Провести тестирование системы на уязвимости.
Требования к выполнению работы:
1. Использование HTTPS для обеспечения безопасной передачи данных.
2. Реализация механизма аутентификации с использованием хэширования паролей.
3. Ограничение доступа к определенным функциональностям в зависимости от роли пользователя.
4. Защита от распространенных уязвимостей, таких как XSS, CSRF и SQL инъекции.
5. Наличие документации по развертыванию и использованию системы.

Лабораторная работа № 2 «Пен-тест защищенной web-ориентированной системы»
Цель работы: Провести пенетрационное тестирование защищенной web-ориентированной информационной системы для выявления уязвимостей и оценки уровня ее безопасности.
Задачи:
1. Изучить функциональность и архитектуру системы.
2. Провести сканирование системы на наличие открытых портов и служб.
3. Выполнить сканирование уязвимостей с использованием специализированных инструментов.
4. Попытаться провести атаки на систему, включая SQL инъекции, XSS, CSRF и другие типичные уязвимости.
5. Оценить уровень безопасности системы и подготовить отчет о проведенном тестировании.
Требования к выполнению работы:
1. Согласование проведения пен-теста с владельцем системы.
2. Использование специализированных инструментов для сканирования и тестирования уязвимостей.
3. Ответственное обращение с полученной информацией об уязвимостях.
4. Подготовка подробного отчета о проведенном пен-тесте.

Лабораторная работа № 3 «Безопасность хранения и передачи информации»
Цель работы: Изучить основные принципы безопасности хранения и передачи информации, провести анализ уязвимостей и разработать меры по их устранению.
Задачи:
1. Изучить методы шифрования и хэширования данных.
2. Провести анализ уязвимостей при передаче информации по сети.
3. Разработать план защиты информации при хранении на сервере.
4. Проверить соблюдение принципов безопасности при работе с паролями пользователей.
5. Оценить уровень безопасности системы и предложить улучшения.
Требования к выполнению работы:
1. Изучение основных методов шифрования и хэширования данных.
2. Анализ уязвимостей при передаче информации по сети.
3. Разработка плана защиты информации на сервере.
4. Проверка безопасности хранения паролей пользователей.
5. Подготовка рекомендаций по улучшению безопасности системы.

Лабораторная работа № 4 «Защищенная система архитектуры Клиент-Сервер»
Цель работы: Провести пен-тест (пенетрационное тестирование) защищенной системы архитектуры Клиент-Сервер для выявления уязвимостей и оценки уровня безопасности.
Задачи:
1. Подготовить план пен-теста, определить цели и методику проведения.
2. Исследовать архитектуру Клиент-Сервер и выявить потенциальные уязвимости.
3. Произвести сканирование системы на наличие открытых портов и служб.
4. Провести анализ безопасности сервера и клиентских устройств.
5. Оценить уровень защиты данных при передаче между клиентом и сервером.
6. Составить отчет о результатах пен-теста и предложить меры по устранению обнаруженных уязвимостей.
Требования к выполнению работы:
1. Подготовка плана пен-теста с описанием целей и методики.
2. Анализ архитектуры Клиент-Сервер и выявление уязвимостей.
3. Проведение сканирования системы на наличие уязвимостей.
4. Оценка безопасности сервера и клиентских устройств.
5. Проверка защиты данных при передаче между клиентом и сервером.
6. Подготовка отчета о проведенном пен-тесте и предложение мер по устранению уязвимостей.

Лабораторная работа № 5 «Пен-тест защищенной системы архитектуры Клиент-Сервер»
Цель работы: Провести пенетрационное тестирование защищенной системы архитектуры Клиент-Сервер для выявления уязвимостей и оценки уровня безопасности.
Задание:
1. Разработать план пенетрационного тестирования, включающий цели, методику проверки и последовательность действий.
2. Изучить архитектуру защищенной системы Клиент-Сервер и выявить потенциальные уязвимости.
3. Провести сканирование системы на предмет открытых портов и служб.
4. Оценить безопасность сервера и клиентских устройств, выявить уязвимости в конфигурации и настройках.
5. Проверить механизмы защиты данных при передаче между клиентом и сервером.
6. Составить подробный отчет о результатах пенетрационного тестирования, включающий обнаруженные уязвимости, рекомендации по устранению и общую оценку уровня безопасности системы.
Требования к выполнению:
1. Подготовить план пенетрационного тестирования с описанием целей и методики проверки.

2. Проанализировать архитектуру системы Клиент-Сервер и выявить потенциальные уязвимости.
3. Провести сканирование системы на наличие открытых портов и служб.
4. Оценить безопасность сервера и клиентских устройств, выявить уязвимости в конфигурации.
5. Проверить механизмы защиты данных при передаче между клиентом и сервером.
6. Подготовить отчет о проведенном пенетрационном тестировании с рекомендациями по устранению обнаруженных уязвимостей.

Лабораторная работа № 6 «Защита информационной системы, обрабатывающей персональные данные»

Цель работы: Изучить меры защиты информационной системы, обрабатывающей персональные данные, с целью обеспечения конфиденциальности, целостности и доступности данных.

Задание:

1. Изучить законодательные акты и нормативные документы, регулирующие обработку персональных данных.
2. Оценить уровень защиты информационной системы, обрабатывающей персональные данные, с учетом требований к конфиденциальности и безопасности.
3. Провести анализ угроз безопасности информационной системы и выявить потенциальные уязвимости.
4. Разработать план мер по обеспечению безопасности информационной системы и защите персональных данных.
5. Провести аудит безопасности информационной системы с учетом рекомендаций по защите персональных данных.
6. Подготовить отчет о проведенном аудите безопасности информационной системы, содержащий выявленные уязвимости, предложенные меры по устранению и оценку уровня безопасности.

Требования к выполнению:

1. Изучить законодательные акты и нормативные документы, касающиеся обработки персональных данных.
2. Оценить уровень защиты информационной системы с учетом требований к конфиденциальности и безопасности.
3. Выявить и проанализировать угрозы безопасности информационной системы, особенно в контексте обработки персональных данных.
4. Разработать план мер по обеспечению безопасности информационной системы и защите персональных данных.
5. Провести аудит безопасности информационной системы, учитывая особенности обработки персональных данных.
6. Подготовить отчет о проведенном аудите безопасности с рекомендациями по улучшению безопасности информационной системы и защите персональных данных.

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

Форма проведения промежуточной аттестации по дисциплине: зачет по результатам накопительного рейтинга / форме компьютерного тестирования

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

Перечень вопросов для подготовки к зачету

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

1. Общие определения и характеристики информационных систем. Структура и классификация систем.
2. Понятие сложности, критерии и свойства. Критерии и свойства для информационной системы.
3. Вероятностная модель системы и пример пограничных состояний. Базовые информационные процессы в системах.
4. Основные принципы обеспечения информационной безопасности для информационных систем.
5. Методическая и нормативная база для построения защищенных систем.
6. Виды защищенных информационных систем в соответствии с требованиями ГОСТ.
7. Принципы защиты информации в автоматизированных системах в соответствии с требованиями ГОСТ.
8. Понятие о задаче интегральной безопасности информационных систем.
9. Примеры задач интегральной безопасности.
10. Физическая безопасность информационных систем.
11. Безопасность сетей и телекоммуникационных устройств.
12. Безопасность ПО.
13. Обеспечение конфиденциальности, целостности и доступности данных.
14. Постановка задачи, её структура.
15. Частный, комплексный и интегральных подходы к решению проблемы передачи и хранения данных.
16. Постановка задачи проектирования и анализа информационной системы. 17. Модель системы с общим перекрытием.
17. Концептуальные требования направленные на обеспечение безопасности функционирования информационной системы.
18. Важнейшие принципы построения архитектуры ИС.

ОПК-4: ИОПК-4.3.Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок

19. Анализ безопасности ИС.
20. Постановка задачи защищённости ИС.
21. Наличие и полнота политики безопасности.
22. Гарантированность безопасности.
23. Трёхуровневая модель параметров оценки защищенности ИС.
24. Аудит сетей связи. Мониторинг функционирования, обнаружение атак и принятие адекватных мер противодействия.
25. Средства обеспечения надежного хранения информации с использованием технологии защиты на файловом уровне (File Encryption System – FES).

26. Средства авторизации и разграничения доступа к информационным ресурсам, а также защита от несанкционированного доступа к информации с использованием технологии токенов (смарт-карты, touch-memory, ключи для USB-портов и т.п.).

27. Средства защиты от внешних угроз при подключении к общедоступным сетям связи, а также средства управления доступом Интернета с использованием технологии межсетевых экранов (FireWall) и содержательной фильтрации (Content Inspection).

28. Политика реализации межсетевых экранов и их функциональные возможности. Классификация межсетевых экранов. Недостатки фильтрующего маршрутизатора (Filter Router - FR).

29. Шлюз сеансового уровня (Session Level Gateway - SLG). Шлюз уровня приложений (Application Layer Gateway - ALG). Преимущества ALG.

30. Что такое Антивирусы?

31. Средства обеспечения активного исследования защищенности информационных ресурсов с использованием технологии обнаружения атак (Intrusion Detection).

32. Инфраструктура открытых ключей (Public Key Infrastruture - PKI).

33. Средства обеспечения конфиденциальности, целостности, доступности и подлинности информации, передаваемой по открытым каналам связи с использованием технологии защищенных виртуальных частных сетей (VPN).

34. Четыре вида архитектуры организации защиты информации на базе применения технологии VPN. Классификация VPN.

35. Средства обеспечения централизованного управления системой ИБ в соответствии с согласованной и утвержденной политикой безопасности.

36. Информация и данные. Свойства информации. Функции информации.

37. Информационная безопасность и защита информации. Задачи информационной безопасности.

38. Направления информационной безопасности.

39. Составляющие информационной безопасности.

40. Нормативно-правовое обеспечение информационной безопасности. Основные документы.

41. Государственная тайна и ее защита.

42. Ответственность за нарушения в сфере информационной безопасности.

43. Защита персональных данных. Понятия и основные документы.

44. Регуляторы в области защиты персональных данных. Их функции и требования.

45. Ответственность за несоблюдение требований законодательства в сфере защиты персональных данных.

46. Угрозы и риски информационной безопасности. Источники угроз. Виды угроз.

47. Риски нарушения информационной безопасности. Систематизация рисков. Измерение рисков, шкалы рисков.

48. Технологии оценки угроз, уязвимостей, рисков и потерь. Оптимизация потерь.

49. Экономические проблемы информационных ресурсов. Основные подходы к определению затрат на защиту информации.