Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования

Пермский национальный исследовательский политехнический университет

УТВЕРЖДАЮ
Проректор по образовательной деятельности

_____ А.Б. Петроченков

« 06 » апреля 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Технология построения защищенных распределенных приложений
(наименование)

Форма обучения: очная
(очная/очно-заочная/заочная)

Уровень высшего образования: специалитет
(бакалавриат/специалитет/магистратура)

Общая трудоёмкость: 288 (8)
(часы (ЗЕ))

Направление подготовки: 10.05.03 Информационная безопасность автоматизированных систем
(код и наименование направления)

Направленность: Безопасность открытых информационных систем (СУОС)
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

освоение дисциплинарных компетенций, связанных с созданием и изучением современных распределенных защищенных информационных систем различного применения и степени сложности.

- Изучение этапов и технологий проектирования и создания безопасных распределенных информационных систем; классификации средств защиты информации в корпоративных вычислительных сетях и системах; инструментальных программных и аппаратных средств анализа их защищенности.
- Формирование умений в разработке проектов комплексных защищенных инфраструктур для типовых современных применений, отвечающую предъявляемым требованиям к уровню защищенности, выполняемых с использованием современных программных, программно-аппаратных и аппаратных средств защиты информации.
- Овладение навыками разработки и внедрения комплексной защищен-ной инфраструктуры на предприятиях, включающих навыки базовой и расширенной настройки и использования современных программных и аппаратных средств защиты информации: файрволлов, интерактивных детекторов атак, защищенных доменных сервисов.

1.2. Изучаемые объекты дисциплины

методы и средства защиты информации в корпоративных вычислительных сетях и системах;

основные угрозы информации в современных сложных сетевых информационных системах;

программные, программно-аппаратные и аппаратные средства защиты информации, применяемые при обеспечении комплексной информационной безопасности;

программные средства анализа текущего уровня защищенности

современные технологии построения безопасных информационных систем и сетей

1.3. Входные требования

знание компьютерных сетей, ОС и языков программирования

2. Планируемые результаты обучения по дисциплине

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-2.1	ИД-1ПК-2.1	методики оценки рисков информационной безопасности распределенных систем; нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты; требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования.	Знает национальные, межгосударственные и международные стандарты в области защиты информации; нормативные правовые акты в области защиты информации; принципы работы и правила эксплуатации программно-аппаратных средств защиты информации; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем; руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации.	Тест
ПК-2.1	ИД-2ПК-2.1	использовать методы и средства определения технологической без-опасности функционирования распределенной информационной системы; использовать CASE-технологии и структурный подход при проектировании информационных систем;	Умеет документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям	Отчёт по практическом у занятию
ПК-2.1	ИД-3ПК-2.1	методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения;	Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы; разработки программ и методик испытаний опытного	Защита лабораторной работы

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
			образца программно-технического средства защиты информации от НДС и специальных воздействий на соответствие техническим условиям	
ПК-2.3	ИД-1ПК-2.3	методики оценки рисков информационной безопасности распределенных систем; принципы построения распределенных систем и объектно¬-ориентированных систем управления базами данных	Знает основные методы управления проектами в области информационной безопасности; национальные, межгосударственные и международные стандарты в области защиты информации	Тест
ПК-2.3	ИД-2ПК-2.3	умеет использовать современные модели оценки угроз и модели нарушителя для распределенных информационных систем; умеет использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы; определять ресурсы, необходимые для обеспечения безопасности информационной системы.	Умеет разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем	Курсовая работа
ПК-2.3	ИД-3ПК-2.3	Владеет навыками семантического моделирования данных.и методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения;	Владеет навыками формирования требований по защите информации, включая использование математического аппарата для решения прикладных задач	Защита лабораторной работы

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		10	11
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	108	54	54
- лекции (Л)	48	24	24
- лабораторные работы (ЛР)	32	16	16
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	22	10	12
- контроль самостоятельной работы (КСР)	6	4	2
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	144	90	54
2. Промежуточная аттестация			
Экзамен	36	36	
Дифференцированный зачет			
Зачет	9		9
Курсовой проект (КП)			
Курсовая работа (КР)	18	18	
Общая трудоемкость дисциплины	288	180	108

4. Содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
10-й семестр				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Проектирование защищенных распределенных приложений	24	16	10	90
Введение Основные понятия, термины и определения. Предмет и задачи дисциплины. Тема 1. Основы проектирования защищенных распределенных приложений Перечень необходимой документации для создания защищенных распре-деленных приложений. Создание удаленной виртуальной инфраструктуры для разработки защищенного распределенного приложения. Способы подключения к виртуальной инфраструктуры. Понятие гипервизора. Тема 2. Распределенные базы данных как ядро распределенного приложения База данных MS SQL, и ее использование при создании защищенных распределенных приложений. Типы связи базы данных с распределенными приложениями. Создание подключения с помощью графического интерфейса и консольных команд.				
ИТОГО по 10-му семестру	24	16	10	90
11-й семестр				
Разработка, отладка и ввод в эксплуатацию системы защиты распределенных приложений.	24	16	12	54
Тема 3. Методы отладки защищенных распределенных приложений Создание шифрованного канала связи для отладки и мониторинга распре-деленного приложения. Настройка средств шифрования. Основные способы отладки защищенных распределенных приложений. Поиск и предотвращение типовых уязвимостей. Использование стандартных программных продуктов. Тема 4. Ввод в эксплуатацию защищенного распределенного приложения Перечень основных этапов и мероприятий процесса ввода защищенного распределенного приложения в эксплуатацию. Нормативные документы. Принципы построения отчетов. Сбор данных о ходе процесса ввода в эксплуатацию. Развертывание программно-аппаратной платформы на оборудовании заказчика.				
ИТОГО по 11-му семестру	24	16	12	54
ИТОГО по дисциплине	48	32	22	144

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Обзор типов удаленного подключения к виртуальной инфраструктуре
2	Защищенные архитектуры распределенных приложений
3	Фреймворки тестирование безопасности распределенных приложений
4	Принципы сбора отладочных данных в распределенных приложениях

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Криптографическая защита в распределенных приложениях
2	Безопасность протоколов, применяемых в веб-приложениях
3	Безопасность сетевых сервисов
4	Аудит информационной безопасности распределенных приложений

Тематика примерных курсовых проектов/работ

№ п.п.	Наименование темы курсовых проектов/работ
1	технологии проектирования распределенных приложений
2	Модель угроз распределенного приложения
3	Криптографическая защита в распределенных приложениях
4	Безопасность сетевых сервисов
5	Мониторинг и расследование инцидентов информационной безопасности в распределенных системах

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при котором учащиеся являются активными участниками занятия, отвечающие на заранее намеченный преподавателем список вопросов, стимулирующих ассоциативное мышление и установления связей с ранее освоенным материалом.
Практические занятия проводятся на основе реализации метода обучения действием: определяются проблемные области; формируются группы для их решения; каждое практическое занятие проводится по своему алгоритму.
Сформированные на практических занятиях знания и умения находят за-крепление в выполнении индивидуальных заданий по их тематике.
Проведение лабораторных занятий основывается на интерактивном методе обучения, при котором учащиеся взаимодействуют не только с преподавателем, но и друг с другом. При этом доминирует активность учащихся в процессе обучения. Место преподавателя в интерактивных лабораторных занятиях – направление деятельности учащихся на достижение целей занятия.
Тематика лабораторных работ непосредственно связана с получением практических навыков по настройке и использованию комплексных средств защиты информации в инфокоммуникационных системах
Выполнение СРС по дисциплине естественным образом опирается на проектный подход к образованию, который основан на идее использования проектирования как компоненты организации обучения и как основы учебно-познавательной (учебно-профессиональной) деятельности обучающегося в рамках используемых образовательных технологий.
Реализация процесса освоения дисциплины «Технология проектирования защищенных распределенных приложений» на основе проектного подхода и широкого применения средств автоматизации проектирования при решении частных задач и комплексной задачи проектирования обеспечивает достижение обучаемыми высокого уровня освоения заданных компетенций.

5.2. Методические указания для обучающихся по изучению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:
1. Изучение учебной дисциплины должно вестись систематически.
2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.
3. Особое внимание следует уделить выполнению отчетов по практическим занятиям, лабораторным работам и индивидуальным комплексным заданиям на самостоятельную работу.
4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

6. Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Печатная учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1. Основная литература		

1	Мельников Д. А. Информационная безопасность открытых систем : учебник / Д. А. Мельников. - Москва: Флинта, Наука, 2013.	11
2	Основы управления информационной безопасностью : учебное пособие для вузов / А. П. Курило [и др.]. - Москва: Горячая линия-Телеком, 2014.	15
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Оголюк А. А. Защита приложений от модификации : учебное пособие / Оголюк А. А. - Санкт-Петербург: НИУ ИТМО, 2013.	10
2	Стандарты информационной безопасности : курс лекций / В. А. Галатенко ; Под ред. В. Б. Бетелина ; Интернет-университет информационных технологий ; Под ред. В. Б. Бетелина .— Москва : ИНТУИТ, 2006 .— 322 с.	19
2.2. Периодические издания		
1	Вестник ПНИПУ. Электротехника, информационные технологии, системы управления.	
2.3. Нормативно-технические издания		
	Не используется	
3. Методические указания для студентов по освоению дисциплины		
	Не используется	
4. Учебно-методическое обеспечение самостоятельной работы студента		
	Не используется	

6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Методические указания для студентов по освоению дисциплины	Практикум «Технологии построения распределенных защищенных приложений»	online.at.pstu.ru	локальная сеть; авторизованный доступ
Основная литература	Учебно-методическое пособие «Технологии построения распределенных защищенных приложений»	online.at.pstu.ru	локальная сеть; авторизованный доступ

6.3. Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Вид ПО	Наименование ПО
Операционные системы	Debian (GNU GPL)
Операционные системы	Windows 10 (подп. Azure Dev Tools for Teaching)

Вид ПО	Наименование ПО
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017
Прикладное программное обеспечение общего назначения	VMware Workstation Player (VMware Academic)
Прикладное программное обеспечение общего назначения	Wireshark
Системы управления проектами, исследованиями, разработкой, проектированием, моделированием и внедрением	EVE NG Community Edition (Free Edition)
Среды разработки, тестирования и отладки	Microsoft Visual Studio (подп. Azure Dev Tools for Teaching)

6.4. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Наименование	Ссылка на информационный ресурс
База данных научной электронной библиотеки (eLIBRARY.RU)	https://elibrary.ru/
База данных уязвимостей CVE Mitre	https://cve.mitre.org/
Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю	https://bdu.fstec.ru/
Научная библиотека Пермского национального исследовательского политехнического университета	http://lib.pstu.ru/
Электронно-библиотечеая система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
Электронная библиотека диссертаций Российской государственной бибилиотеки	http://www.diss.rsl.ru/
База данных компании EBSCO	https://www.ebsco.com/
Информационно-справочная система нормативно-технической документации "Техэксперт: нормы, правила, стандарты и законодательства России"	https://техэксперт.сайт/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Курсовая работа	Все компьютеры с возможностью подключения к сети Интернет и обеспечением доступа в электронную образовательную среду	20
Лабораторная работа	Все компьютеры с возможностью подключения к сети Интернет и обеспечением доступа в электронную образовательную среду	20
Лекция	Стандартное оборудование лекционной аудитории - компьютер, проектор, доска	1

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Практическое занятие	Все компьютеры с возможностью подключения к сети Интернет и обеспечением доступа в электронную образовательную среду	20

8. Фонд оценочных средств дисциплины

фос

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Пермский национальный исследовательский политехнический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации обучающихся по дисциплине «Технология построения защищенных распределенных приложений»
Приложение к рабочей программе дисциплины

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

Направленность (профиль) образовательной программы: Безопасность открытых информационных систем

Квалификация выпускника: специалитет

Выпускающая кафедра: Автоматика и телемеханика

Форма обучения: Очная

Курс: 5 **Семестр**: 10, 11

Трудоёмкость:
Кредитов по рабочему учебному плану: 8 ЗЕ
Часов по рабочему учебному плану: 288 ч.

Форма промежуточной аттестации:
Экзамен: 10 семестр
Курсовая работа: 10 семестр
Зачет: 11 семестр

Пермь 2021

Фонд оценочных средств для проведения промежуточной аттестации обучающихся для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок**.** Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

1. Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД, освоение учебного материала дисциплины запланировано в течение двух семестров (10-го и 11-го семестров учебного плана) и разбито на 4 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные и лабораторные занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируется компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по лабораторным работам и экзамена. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	**Вид контроля**					
	Текущий		**Рубежный**		**Итоговый**	
	С	**ТО**	**ОЛР**	**Т/КР**		**Экзамен**
Усвоенные знания						
З.1 Знает методики оценки рисков информационной безопасности распределенных систем; нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты; требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования.		ТО1	ОЛР1 ОЛР2 ОЛР3 ОЛР4	КР1		
З.2 Знает методики оценки рисков информационной безопасности распределенных систем; принципы построения распределенных систем и объектно¬-ориентированных систем управления базами данных		ТО2	ОЛР1 ОЛР2 ОЛР3 ОЛР4			КЗ
Освоенные умения						
У.1 Умеет использовать методы и средства определения технологической без□опасности функционирования распределенной информационной системы; использовать CASE□технологии и структурный подход при проектировании информационных систем;автоматизированных систем в защищенном исполнении.			ОЛР1 ОЛР2 ОЛР3 ОЛР4			КЗ
У.2 Умеет использовать современные модели оценки		ТО3	ОЛР1			КЗ

угроз и модели нарушителя для распределенных информационных систем; умеет использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы; определять ресурсы, необходимые для обеспечения безопасности информационной системы.			ОЛР2 ОЛР3 ОЛР4			
Приобретенные владения						
В.1 Владеет методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения;			ОЛР1 ОЛР2 ОЛР3 ОЛР4	КР1		
В.2 Владеет навыками семантического моделирования данных.и методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения;			ОЛР1 ОЛР2 ОЛР3 ОЛР4			КЗ

С – собеседование по теме; ТО – коллоквиум (теоретический опрос); КЗ – кейс-задача (индивидуальное задание); ОЛР – отчет по лабораторной работе; Т/КР – рубежное тестирование (контрольная работа, курсовая работа); ТВ – теоретический вопрос; ПЗ – практическое задание; КЗ – комплексное задание экзамена.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде экзамена, проводимая с учетом результатов текущего и рубежного контроля.

2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

- входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;

- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;

- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;

- контроль остаточных знаний.

2.1. Текущий контроль усвоения материала

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в книжку преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме защиты лабораторных работ (после изучения каждого модуля учебной дисциплины) и курсовой работы (после изучения всех модулей учебной дисциплины).

Всего запланировано 4 лабораторных работ. Типовые темы лабораторных работ приведены в РПД.

Защита лабораторной работы проводится индивидуально каждым студентом. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

Тема курсовой работы приведена в РПД. Курсовая работа содержит расчетную часть и практическое задание – разработать программную модель в указанной среде моделирования.

Защита курсовой работы проводится индивидуально каждым студентом путем собеседования по расчетной части и демонстрации результатов разработки программной модели. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.3. Промежуточная аттестация (итоговый контроль)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех лабораторных работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

Промежуточная аттестация, согласно РПД, проводится в виде экзамена по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний и практические задания (ПЗ) для проверки освоенных умений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций. Форма билета представлена в общей части ФОС образовательной программы.

2.3.1. Типовые вопросы и задания для экзамена по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Перечень необходимой документации для создания защищенных распределенных приложений
2. Создание удаленной виртуальной инфраструктуры для разработки защищенного распределенного приложения

3. Способы подключения к виртуальной инфраструктуры. Понятие гипервизора.
4. Распределенные базы данных как ядро распределенного приложения База данных MS SQL, и ее использование при создании защищенных распределенных приложений
5. Типы связи базы данных с распределенными приложениями
6. Создание шифрованного канала связи для отладки и мониторинга распределенного приложения
7. Основные способы отладки защищенных распределенных приложений.
8. Перечень основных этапов и мероприятий процесса ввода защищенного распределенного приложения в эксплуатацию
9. Сбор данных о ходе процесса ввода в эксплуатацию. Развертывание программно-аппаратной платформы на оборудовании заказчика

Типовые вопросы и практические задания для контроля освоенных умений:

1. Разработка защищенной архитектуры распределенных приложений
2. Криптографическая защита в распределенных приложениях
3. Безопасность протоколов, применяемых в веб-приложениях
4. Аудит информационной безопасности распределенных приложениях

2.3.2. Шкалы оценивания результатов обучения на экзамене

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь, владеть* заявленных компетенций проводится по 4-х балльной шкале оценивания путем выборочного контроля во время экзамена.

Типовые шкала и критерии оценки результатов обучения при сдаче экзамена для компонентов *знать, уметь и владеть* приведены в общей части ФОС образовательной программы.

3. Критерии оценивания уровня сформированности компонентов и компетенций

3.1. Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций в рамках выборочного контроля при экзамене считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

Типовые критерии и шкалы оценивания уровня сформированности компонентов компетенций приведены в общей части ФОС образовательной программы.

3.2. Оценка уровня сформированности компетенций

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля в виде интегральной оценки по 4-х балльной шкале. Все результаты контроля заносятся в

оценочный лист и заполняются преподавателем по итогам промежуточной аттестации.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы.

При формировании итоговой оценки промежуточной аттестации в виде экзамена используются типовые критерии, приведенные в общей части ФОС образовательной программы.