Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
Балтийская государственная академия рыбопромыслового флота
(ФГБОУ ВО «КГТУ»)
БГАРФ

УТВЕРЖДАЮ
И.о. декана РТФ
_____/В.А. Баженов/
27. июня 2018 г.

Фонд оценочных средств для аттестации по дисциплине

(приложение к рабочей программе дисциплины)

Технология построения защищённых распределённых приложений
(наименование дисциплины)

базовой части образовательной программы по специальности

10.05.03 Информационная безопасность автоматизированных систем
(код и наименование специальности)

Специализация «Обеспечение информационной безопасности распределённых информационных систем»

Факультет Радиотехнический
(наименование)

Кафедра Информационная безопасность
(наименование)

Калининград 2018

ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

«Технология построения защищенных распределенных приложений»
(наименование дисциплины)

№ п/п	Контролируемые модули, разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Оценочные средства		Способ контроля
			наименование	№№ заданий	
1	WindowsCommunicationFoundation (WCF) – современная технология построения защищенных распределенных систем.	ОПК – 4.1	собеседование, доклад	1	устный
2	Контракты	ПК-20.1 ПК-9.1	лабораторная работа, доклад	2	письменный
3	Экспонирование служб	ПК-20.1 ПК-9.1	лабораторная работа, доклад	3	письменный
4	Создание в WCF работающих с базами данных клиент-серверных приложений	ПК-20.1 ПК-9.1	лабораторная работа	4	письменный
			лабораторная работа, доклад	5	письменный
			лабораторная работа	6	письменный
5	Использование служб	ПК-20.1 ПК-9.1	лабораторная работа	7	письменный
			лабораторная работа	8	письменный
			лабораторная работа	9	устный
6	Настройка WCF	ПК-20.1 ПК-9.1	защита лабораторного практикума	10	письменный
			защита лабораторного практикума	11	устный
			защита лабораторного практикума	12	письменный
7	Средства контроля	ПК-20.1 ПК-9.1	защита лабораторного практикума	13	письменный
8	Инфраструктура безопасности	ПСК-7.1.3 ПК-9.1	защита лабораторного практикума	14	устный
9	Обработка транзакций	ПСК-7.1.3, ПК-20.1	защита лабораторного практикума	15	устный

ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

«Технология построения защищенных распределенных приложений»

(наименование дисциплины)

Компетенции выпускника ОП ВО и этапы их формирования в результате изучения дисциплины	**Этапы формирования компетенции**		**Знания, умения и навыки, характеризующие этапы формирования компетенций**
1			2
ОПК-4.1способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информациив компьютерных системах, сетях, библиотечных фондах	**Знать:**		**Знать:** Основные способы создания защищенных распределенных приложений **Уметь** Использовать знания о принципах построения защищенных приложений, применять знания на практике **Владеть** основными методами научного познания
	Уровень 1	типовые структуры и принципы организации компьютерных сетей;	
	Уровень 2	общие принципы построения и использования современных языков программирования высокого уровня; современные технологии и методы программирования;	
	Уровень 3	классификацию современных компьютерных систем.	
	Уметь		
	Уровень 1	пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет;	
	Уровень 2	работать с интегрированной средой разработки программного обеспечения; формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения;разрабатывать прикладные программы, осуществляющие	

		взаимодействие с базами данных;	
	Уровень 3	проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети;разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных;применять средства обеспечения безопасности данных.	
	Владеть		
	Уровень 1	методами теоретического исследования физических явлений и процессов;	
	Уровень 2	навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;	
	Уровень 3	навыками использования ЭВМ в анализе простейших шифров; навыками математического моделирования в криптографии.	
ПК-9.1: способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	**Знать:**		**Знать:** Основные средства и способы обеспечения информационной безопасности и принципы построения систем защиты информации **Уметь:** реализовывать политику безопасности баз данных и проводить выбор программно-аппаратных средств с целью обеспечения требуемого уровня защищенности **Владеть:**
	Уровень 1	физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем; язык программирования высокого уровня (объектно-ориентированное программирование);	
	Уровень 2	основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;	
	Уровень 3	автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; основные меры по защите информации в автоматизированных	

		системах (организационные, правовые, программно-аппаратные, криптографические, технические).	навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем
	Уметь		
	Уровень 1	анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности;	
	Уровень 2	реализовывать политику безопасности баз данных;	
	Уровень 3	проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы.	
	Владеть		
	Уровень 1	навыками применения математического аппарата для решения прикладных теоретико-информационных задач;	
	Уровень 2	методами и средствами технической защиты информации;	
	Уровень 3	навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; методами теоретического исследования физических явлений и процессов.	
ПК-20.1: способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	**Знать:**		**Знать:** принципы построения распределенных систем и объектно-ориентированных систем управления базами данных **Уметь:** разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных
	Уровень 1	принципы построения распределенных систем и объектно-ориентированных систем управления базами данных, технологии автоматизированного проектирования баз данных и хранилищ данных;	
	Уровень 2	требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования;	

	Уровень 3	методы, обеспечивающие безопасность клиент-серверных приложений в WCF.	**Владеть:** методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения
	Уметь		
	Уровень 1	разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных;	
	Уровень 2	использовать технологии автоматизированного проектирования и структурный подход при проектировании информационных систем;	
	Уровень 3	определять ресурсы, необходимые для обеспечения безопасности информационной системы, использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы.	
	Владеть		
	Уровень 1	навыками семантического моделирования данных, навыками проектирования информационных систем на базе корпоративных систем управления базами данных;	
	Уровень 2	методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения;	
	Уровень 3	методами, обеспечивающими безопасность распределенных приложений в WCF.	
ПСК-7.1.3: способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	**Знать:**		**Знать:**
	Уровень 1	критерии оценки эффективности и надежности средств защиты операционных систем; средства обеспечения безопасности данных;	Критерии оценки эффективности средств защиты, основные средства и способы обеспечения информационной безопасности в распределенных информационных системах

	Уровень 2	основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;	**Уметь:** разрабатывать модели угроз нарушителя информационной безопасности и реализовывать политику безопасности баз данных **Владеть:** навыками разработки, эксплуатации и анализа политики безопасности распределенных информационных систем
	Уровень 3	основные задачи и понятия криптографии; модели шифров и математические методы их исследования; методы обеспечения информационной безопасностиавтоматизированной системы; методы аттестации уровня защищенности автоматизированных систем.	
	Уметь		
	Уровень 1	оценивать эффективность и надежность защиты операционных систем;	
	Уровень 2	реализовывать политику безопасности баз данных; применять средства обеспечения безопасности данных;	
	Уровень 3	определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите.	
	Владеть		
	Уровень 1	навыками эксплуатации и администрирования программных систем с учетом требований по обеспечению информационной безопасности;	
	Уровень 2	навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности;	
	Уровень 3	навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем.	

ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ИЗУЧЕНИЯДИСЦИПЛИНЫ

«Технология построение защищенных распределенных приложений»
(наименование дисциплины)

Семестр 8

№ п/п	Код контролируемой компетенции (или ее части)	№ учебной недели																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
		Этапы формирования компетенции																	
1.	ОПК-4.1	+		+	+				+					+					
2.	ПК-9.1	+		+	+			+	+		+		+	+				+	
3.	ПК-20.1		+		+	+	+		+		+				+	+		+	
4.	ПСК-7.1.3									+	+						+	+	+

ПОКАЗАТЕЛИ И КРИТЕРИИ ОПРЕДЕЛЕНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

№ п/п	Код контролируемой компетенции (или ее части)	Уровни сформированности компетенции		
		пороговый	продвинутый	высокий
1	ОПК-4.1	Знать:		
		типовые структуры и принципы организации компьютерных сетей;	общие принципы построения и использования современных языков программирования высокого уровня; современные технологии и методы программирования;	Основные способы создания защищенных распределенных приложений классификацию современных компьютерных систем.
		Уметь:		
		пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет;	работать с интегрированной средой разработки программного обеспечения; формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения;разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных;	проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети;разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных;применять средства обеспечения безопасности данных.
		Владеть:		
		методами теоретического исследования физических явлений и процессов;	навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;	навыками использования ЭВМ в анализе простейших шифров; навыками математического моделирования в криптографии.
2	ПК-9.1	Знать:		
		физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем; язык программирования высокого уровня (объектно-ориентированное программирование);	основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;	автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические).
		Уметь:		
		анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопас-	реализовывать политику безопасности баз данных;	проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого

		ности;		уровня защищенности автоматизированной системы.
		Владеть:		
		навыками применения математического аппарата для решения прикладных теоретико-информационных задач;	методами и средствами технической защиты информации;	навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; методами теоретического исследования физических явлений и процессов.
3	ПК-20.1	Знать:		
		принципы построения распределенных систем и объектно-ориентированных систем управления базами данных, технологии автоматизированного проектирования баз данных и хранилищ данных;	требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования;	методы, обеспечивающие безопасность клиент-серверных приложений в WCF.
		Уметь:		
		разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных;	использовать технологии автоматизированного проектирования и структурный подход при проектировании информационных систем;	определять ресурсы, необходимые для обеспечения безопасности информационной системы, использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы.
		Владеть:		
		навыками семантического моделирования данных, навыками проектирования информационных систем на базе корпоративных систем управления базами данных;	методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения;	методами, обеспечивающими безопасность распределенных приложений в WCF.
4	ПСК-7.1.3	Знать:		
		критерии оценки эффективности и надежности средств защиты операционных систем; средства обеспечения безопасности данных;	основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;	основные задачи и понятия криптографии; модели шифров и математические методы их исследования; методы обеспечения информационной безопасностиавтоматизированной системы; методы аттестации уровня защищенности автоматизированных систем.
		Уметь:		
		оценивать эффективность и надежность защиты операционных систем;	реализовывать политику безопасности баз данных; применять средства обеспечения безопасности данных;	определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите.
		Владеть:		
		навыками эксплуатации и администрирования программных систем с учетом требований по обеспечению информационной безопасности;	навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности;	навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем.

ПЕРЕЧЕНЬ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Доклад, сообщение	Доклад – это краткое публичное устное изложение результатов индивидуальной учебно-исследовательской деятельности, имеет регламентированную структуру, содержание и оформление. Доклады направлены на более глубокое самостоятельное изучение лекционного материала или рассмотрения вопросов для дополнительного изучения. Задачами являются: формирование умений самостоятельной работы обучающихся с источниками литературы, их систематизация; развитие навыков логического мышления; углубление теоретических знаний по проблеме исследования; развитие навыков изложения своих мыслей и идей перед аудиторией, умения уверенно пользоваться научной терминологией.	Темы докладов, сообщений.
Лабораторная работа	Лабораторные работы служат средством освоения тем дисциплины и практического применения знаний, полученных на лекционной чсти дисциплины	отчет
Экзамен	Экамены служат формой проверки качества выполнения студентами лабораторных работ, усвоения учебного материала практических и семинарских занятий, успешного прохождения производственной и преддипломной практик и выполнения в процессе этих практик всех учебных поручений в соответствии с утвержденной программой.	Вопросы на экзамен

ФГБОУ ВО «КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
БАЛТИЙСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ РЫБОПРОМЫСЛОВОГО ФЛОТА

Типовые вопросы к экзамену

Дисциплина:	Технология построения защищенных распределенных приложений	Специальность:	10.05.03.
Семестр:	8		
Кафедра:	Информационная безопасность		

1. Основные понятия WCF. Контракты. Привязки. Адреса.
2. Контракты служб. Контракты ошибок. Примеры.
3. Visual Studio. C#.
4. Шаблоны проектов WCF в Visual Studio.
5. Контракты данных. Коллекции.
6. Контракты сообщений. Пример.
7. Сериализация.
8. Суть конечных точек службы.
9. Создание конечных точек с помощью файла конфигурации. Базовые адреса.
10. Создание конечной точки с помощью программного кода. Публикация метаданных посредством конечных точек.
11. Общие сведения об архитектуре метаданных.
12. Настройка стандартных привязок. Нестандартные привязки.
13. Работа с базой данных Access.
14. Работа с Microsoft SQL Server 2005.
15. Использование утилиты svcutil для генерирования прокси-класса.
16. Использование среды Visual Studio для генерирования прокси-класса.
17. Определение прокси-класса вручную.
18. Динамическое создание прокси-класса.
19. Использование служб, отличных от WCF-ориентированных.
20. Конфигурирование конечной точки клиента.
21. Динамическое конфигурирование службы.
22. Базовая трассировка в WCF.
23. Сквозная трассировка.
24. Обеспечение безопасности на транспортном уровне.
25. Привязки и безопасность. Обеспечение безопасности на уровне сообщений.
26. Основы проверки подлинности. Политика безопасности.
27. Учетные данные клиентов. Учетные данные службы. Собственная проверка подлинности.
28. Учетные данные клиентов. Учетные данные в виде сертификата. Учетные данные в виде выдаваемых маркеров. Учетные данные Windows.
29. Авторизация и персонификация.
30. Авторизация. Авторизация на основе заявок. Проверка подлинности с помощью маркеров безопасности.
31. Персонификация.
32. Свойства транзакций. Протоколы транзакций.
33. Распространение транзакций. Транзакции и однонаправленные вызовы.

34. Программирование транзакций.
35. Обработка клиентских исключений.
36. Безопасность сообщений и безопасность транспорта. Сравнительные характеристики.
37. Обработка ошибок. Типы ошибок и способы их устранения
38. Основные сценарии безопасности в WCF и их особенности

Вопросы рассмотрены и утверждены на заседании кафедры	Дата:	Протокол №
Заведующий кафедрой	подпись	

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Макеты методических материалов, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

ТЕМЫ РЕФЕРАТОВ, ДОКЛАДОВ

по дисциплине «Технология построения защищенных распределенных приложений»
(наименование дисциплины)

1. Язык описания WSDL.
2. Язык определения XML-схемы (XSD).
3. Протокол SOAP.
4. Классы в C#.
5. Коллекции в C#.
6. Наследование в C#.
7. Сериализация.
8. Делегаты в C#.
9. Общие сведения об архитектуре метаданных.
10. Конфигурирование службы с помощью программного кода и использование различных привязок.
11. Работас Microsoft SQL Server 2005.
12. Использование служб, отличных от WCF-ориентированных.
13. Конфигурирование конечной точки клиента.
14. Динамическое конфигурирование службы.
15. Базовая трассировка в WCF.
16. Сквозная трассировка.
17. Учетные данные клиентов. Учетные данные в виде сертификата.
18. Учетные данные в виде выдаваемых маркеров. Учетные данные Windows.
19. Программирование транзакций.
20. Обработка клиентских исключений.

Критерии оценивания за устное выступление при обсуждении вопроса

5 «Отлично»	выступление (доклад) отличается последовательностью, логикой изложения. Легко воспринимается аудиторией. При ответе на вопросы выступающий (докладчик) демонстрирует глубину владения представленным материалом. Ответы формулируются аргументировано, обосновывается собственная позиция в проблемных ситуациях.
4 «Хорошо»	выступление (доклад) отличается последовательностью, логикой изложения. Но обоснование сделанных выводов не достаточно аргументировано. Неполно раскрыто содержание проблемы.
3 «Удовлетворительно»	выставляется, если выступающий (докладчик) передает содержание проблемы, но не демонстрирует умение выделять главное, существенное. Выступление воспринимается ауди-

	торией сложно.
2 «Неудовлетворительно»	выступление (доклад) краткий, неглубокий, поверхностный.

Критерии оценивания доклада с презентацией

2 «Неудовлетворительно»	Студент демонстрирует первичное восприятие некоторых основных элементов медиаработы. Она проста и незакончена. Проблема не раскрыта. Отсутствуют выводы. Не использованы возможности визуализации материала в PowerPoint. Больше 4 ошибок в представляемой информации.
3 «Удовлетворительно»	Некоторая степень владения большинством элементов медиаработы. Частично присутствует гармоничная интеграция элементов в целое, но работа незавершенная. Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы. Частично использованы возможности визуализации материала в PowerPoint. 3-4 ошибки в представляемой информации.
4 «Хорошо»	Студент показывает владение элементами медиаработы. В основном, она ясная и целостная. Проблема раскрыта. Проведен анализ проблемы без привлечения дополнительной литературы. Не все выводы сделаны и/или обоснованы. Использованы информационные технологии (PowerPoint). Не более 2 ошибок в представляемой информации.
5 «Отлично»	Студент продемонстрировал уверенное владение и интеграцию всех элементов медиаработы. Работа целостна, креативна. Использован творческий подход. Проблема раскрыта полностью. Проведен анализ проблемы с привлечением дополнительной литературы. Выводы обоснованы. Широко использованы информационные технологии (PowerPoint). Отсутствуют ошибки в представляемой информации.

Критерии оценивания экзамена

Критерии оценок на **дифференцированном экзамене** по дисциплине (отлично, хорошо, удовлетворительно, неудовлетворительно):

- «ОТЛИЧНО» выставляется в случае правильных, полных и четких ответов на теоретические вопросы, с их проецированием и интерпретацией на сегодняшнюю ситуацию. Допускаются непринципиальные погрешности или небольшая незавершенность ответов, диктуемых лимитом времени.

- «ХОРОШО» выставляется в случаях: правильных и четких ответов при незначительных замечаниях, неточностях.

- «УДОВЛЕТВОРИТЕЛЬНО» выставляется в случаях ответа на большую часть (не менее 50% основных положений); при правильном ответе на один вопрос или неполных ответах на два вопроса.

- «НЕУДОВЛЕТВОРИТЕЛЬНО» выставляется при ответах, не удовлетворяющих критериям, указанным в предыдущих пунктах.

Зачет по дисциплине осуществляется при условии выполнения заданий всех практических занятий, самостоятельной работы, а также результатами проведенной оценки остаточных знаний.

Формат сведений о ФОС и ее согласовании

Фонд оценочных средств для аттестации по дисциплине представляет собой приложение к рабочей программе дисциплины:

«Технология построения защищенных распределенных приложений»
(наименование дисциплины)

образовательной программы специалитета по специальности

10.05.03. Информационная безопасность информационных систем
(код и наименование направления)

специализация программы
Обеспечение информационной безопасности распределенных информационных систем
(наименование специализации)

утвержденной «27» июня 2018г.

Автор фонда – ассистент кафедры информационной безопасности Бабаева А.А.

_____

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры «Информационной безопасности»

(протокол от 14 июня 2018г. № 9)

Зав. кафедрой информационной безопасности _____/Великите Н.Я./

Фонд оценочных средств рассмотрен и одобрен на заседании методической комиссии радиотехнического факультета БГАРФ

(протокол № 6 от 27 июня 2018г.)

Председатель методической комиссии _____/А.Г. Жестовский/

Согласовано

Начальник отдела мониторинга и контроля БГАРФ

_____/Борисевич Ю.В./