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

« 29 » августа 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Методы проектирования защищенных распределенных информационных систем
(наименование)

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

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

Общая трудоёмкость: 144 (4)
(часы (ЗЕ))

Направление подготовки: 10.04.01 Информационная безопасность
(код и наименование направления)

Направленность: Комплексные системы информационной безопасности
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Формирование комплекса знаний, умений и навыков в области проектирования систем защиты информации в распределенных информационных системах

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

Безопасность вычислительных сетей, безопасность систем баз данных, безопасность операционных систем, исследование операций, криптографические методы защиты информации

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
ПК-1.2	ИД-1ПК-1.2	Знает нормативные правовые акты в области защиты информации.в области безопасности распределенных информационных систем и автоматизированных систем управления технологическим процессом	Знает нормативные правовые акты в области защиты информации.	Тест
ПК-1.2	ИД-2ПК-1.2	Умеет анализировать компьютерную систему с целью определения уровня защищенности и доверия в соответствии со стандартами безопасности распределенных информационных систем	Умеет анализировать компьютерную систему с целью определения уровня защищенности и доверия	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
ПК-1.2	ИД-3ПК-1.2	Владеет навыками выработки предложений по устранению выявленных уязвимостей в распределенных информационных системах	Владеет навыками выработки предложений по устранению выявленных уязвимостей	Отчёт по практическому занятию
ПК-2.1	ИД-1ПК-2.1	Знает принципы организации и структуру систем защиты информации программного обеспечения автоматизированных систем управления технологическим процессом	Знает принципы организации и структуру систем защиты информации программного обеспечения автоматизированных систем.	Тест
ПК-2.1	ИД-2ПК-2.1	Умеет определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в распределенных информационных системах и автоматизированных системах управления технологическим процессом	Умеет определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах.	Отчёт по практическому занятию
ПК-2.1	ИД-3ПК-2.1	Владеет навыками оценивания информационных рисков в распределенных информационных системах и автоматизированных системах управления технологическими процессами и определения информационной инфраструктуры и информационных ресурсов, подлежащие защите	Владеет навыками оценивания информационных рисков в автоматизированных системах и опреде-ления информационной инфраструктуры и информационных ресурсов, подлежащие защите	Отчёт по практическому занятию
ПК-3.2	ИД-1ПК-3.2	Знает методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных в рамках	Знает методов и средств защиты информации в компьютерных сетях, операционных системах и системах управления базами данных; Методы	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
		концепции глубокоэшелонированной обороны; Методы анализа безопасности компьютерных систем; Принципы построения систем защиты информации распределенных информационных систем	анализа безопасности компьютерных систем; Принципы построения систем защиты информации компьютерных систем.	
ПК-3.2	ИД-2ПК-3.2	Умеет использовать приемы защиты от типовых атак компьютерных систем; применять методы и средства тестирования безопасности распределенных информационных систем	Умеет использовать приемы защиты от типовых атак компьютерных систем; применять методы и средства тестирования.	Отчет по практике
ПК-3.2	ИД-3ПК-3.2	Владеет навыками проведения контрольных проверок работоспособности и эффективности систем и средств защиты информации применяемых в распределенных информационных системах	Владеет навыками проведения контрольных проверок работоспособности и эффективности систем и средств защиты информации	Защита лабораторной работы

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		4
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	42	42
- лекции (Л)	12	12
- лабораторные работы (ЛР)	16	16
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	12	12
- контроль самостоятельной работы (КСР)	2	2
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	102	102
2. Промежуточная аттестация		
Экзамен		
Дифференцированный зачет	9	9
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)		
Общая трудоемкость дисциплины	144	144

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
4-й семестр				
Проектирование защищенных распределенных информационных систем	6	8	6	51
Введение. Модели распределенных информационных систем (РИС). Модель РИС как объекта атаки-защиты Архитектуры, защищенных РИС Особенности разработки политики безопасности РИС				
Технические механизмы и средства обеспечения информационной безопасности защищенных распределенных информационных систем.	6	8	6	51
Криптографические средства защиты Межсетевое экранирование Системы обнаружения и предотвращения вторжений Инструментальные средства аудита безопасности РИС				
ИТОГО по 4-му семестру	12	16	12	102
ИТОГО по дисциплине	12	16	12	102

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Защита компьютерных сетей от атак на конфиденциальность, целостность и доступность
2	Защита серверов приложений и данных
3	Аудит и мониторинг инцидентов информационной безопасности

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Проектирование ззащищённых каналов связи в РИС
2	Проектирование архитектуры защищенной РИС
3	Интеграция системы обнаружения и предотвращения вторжений в РИС
4	Технический аудит информационной безопасности

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при которой учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала, а также на развитие логического мышления. Преподаватель заранее намечает 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. При проведении практических занятий преследуются следующие цели: применение знаний отдельных дисциплин и креативных методов для решения проблем и приятия решений; отработка у обучающихся навыков командной работы, межличностных коммуникаций и развитие лидерских качеств; закрепление основ теоретических знаний.

Проведение лабораторных занятий основывается на интерактивном методе обучения, при котором обучающиеся взаимодействуют не только с преподавателем, но и друг с другом. При этом доминирует активность учащихся в процессе обучения. Место преподавателя в интерактивных занятиях сводится к направлению деятельности обучающихся на достижение целей занятия.

При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.

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	Основы безопасности информационных систем : учебное пособие для вузов / Д. П. Зегжда, А. М. Ивашко .— Москва : Горячая линия-Телеком, 2000 .— 451 с.	18
2	Теоретические основы компьютерной безопасности : учебное пособие для вузов / П. Н. Девянин [и др.] .— Москва : Радио и связь, 2000 .— 190 с	30
2.2. Периодические издания		
	Не используется	
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	Конспект лекций и методические указания по выполнению лабораторных работ	at.pstu.ru	локальная сеть; свободный доступ

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

Вид ПО	Наименование ПО
Операционные системы	Windows 10 (подп. Azure Dev Tools for Teaching)
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017
Прикладное программное обеспечение общего назначения	Wireshark

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/
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
Лабораторная работа	Лицензия на использование программного обеспечения (ПО) СОТСБИ-guard от 18.07.2017 выдана ООО «НТЦ СОТСБИ» авторизационный номер №2014610703;	10
Лекция	Все компьютеры с возможностью подключения к сети Интернет и обеспечением доступа в электрон-ную образовательную среду: мониторы Acer K222HQL – 9 шт., Samsung E1920NR – 1шт.; клавиа-туры Logitech K120 – 9 шт., клавиатура у преподава-теля – 1шт.; компьютерные мыши Logitech M90 – 9 шт, компьютерная мышь у преподавателя – 1шт.;, системные блоки с процессорами Intel Core i3-4160CPU 3.60 GHz – 9 шт., системный блок у препо-давателя – 1шт.; Переносное мультимедийное оборудование:	10
Практическое занятие	Все компьютеры с возможностью подключения к сети Интернет и обеспечением доступа в электрон-ную образовательную среду: мониторы Acer K222HQL – 9 шт., Samsung E1920NR – 1шт.; клавиа-туры Logitech K120 – 9 шт., клавиатура у преподава-теля – 1шт.; компьютерные мыши Logitech M90 – 9 шт, компьютерная мышь у преподавателя – 1шт.;, системные блоки с процессорами Intel Core i3-4160CPU 3.60 GHz – 9 шт., системный блок у препо-давателя – 1шт.; Переносное мультимедийное оборудование:	10

8. Фонд оценочных средств дисциплины

Описан в отдельном документе

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 «Методы проектирования защищенных распределенных информационных систем»

Приложение к рабочей программе дисциплины

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль) образовательной программы: Комплексные системы информационной безопасности

Квалификация выпускника: Магистр

Выпускающая кафедра: Автоматика и телемеханика

Форма обучения: Очная

Курс: 2 **Семестр**: 4

Трудоёмкость:
Кредитов по рабочему учебному плану: 4 ЗЕ
Часов по рабочему учебному плану: 144 ч.

Форма промежуточной аттестации:
Зачёт с оценкой: 4 семестр

Пермь 2021

Фонд оценочных средств 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 одного семестра (4-го семестра учебного плана) и разбито на 2 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные, практические и лабораторные занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируются 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 зачета. 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**		**Зачёт**
Усвоенные знания						
З.1 Знает нормативные правовые акты в области защиты информации.в области безопасности распределенных информационных систем и автоматизированных систем управления технологическим процессом		ТО1				КЗ
Знает принципы организации и структуру систем защиты информации программного обеспечения автоматизированных систем управления технологическим процессом						КЗ
Знает методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных в рамках концепции глубокоэшелонированной обороны; Методы анализа безопасности компьютерных систем; Принципы построения систем защиты информации распределенных информационных систем						КЗ
Освоенные умения						
У.1 Умеет анализировать компьютерную систему с целью определения уровня защищенности и доверия в соответствии со стандартами безопасности распределенных информационных систем			ОЛР1 ОЛР2 ОЛР3 ОЛР4			КЗ

Умеет определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в распределенных информационных системах и автоматизированных системах управления технологическим процессом			ОЛР1 ОЛР2 ОЛР3 ОЛР4			КЗ
Умеет использовать приемы защиты от типовых атак компьютерных систем; применять методы и средства тестирования безопасности распределенных информационных систем			ОЛР1 ОЛР2 ОЛР3 ОЛР4			КЗ
Приобретенные владения						
В.1 Владеет навыками выработки предложений по устранению выявленных уязвимостей в распределенных информационных системах			ОЛР1 ОЛР2 ОЛР3 ОЛР4			КЗ
Владеет навыками оценивания информационных рисков в распределенных информационных системах и автоматизированных системах управления технологическими процессами и определения информационной инфраструктуры и информационных ресурсов, подлежащие защите			ОЛР1 ОЛР2 ОЛР3 ОЛР4			КЗ
Владеет навыками проведения контрольных проверок работоспособности и эффективности систем и средств защиты информации применяемых в распределенных информационных системах			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); ТВ – теоретический вопрос; ПЗ – практическое задание; КЗ – комплексное задание дифференцированного зачета.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде зачета, проводимая с учётом 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.

2.2.1. Защита лабораторных работ

Всего запланировано 4 лабораторные работы. 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.

2.3. Выполнение комплексного индивидуального задания на самостоятельную работу

Для оценивания навыков и опыта деятельности (владения), как результата обучения по дисциплине, не имеющей курсового проекта или работы используется индивидуальное комплексное задание студенту.

Типовые шкала и критерии оценки результатов защиты индивидуального комплексного задания приведены в общей части ФОС образовательной программы.

2.4. 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.

2.4.1. Процедура промежуточной аттестации без дополнительного аттестационного испытания

Промежуточная аттестация проводится в форме зачета. Зачет по дисциплине основывается на результатах выполнения предыдущих индивидуальных заданий студента по данной дисциплине.

Критерии выведения итоговой оценки за компоненты компетенций при проведении промежуточной аттестации в виде зачета приведены в общей части ФОС образовательной программы.

2.4.3. Типовые вопросы для оценивания при защите лабораторных работ

1. Какие задачи выполняет протокол ICMP?
2. Как сканирование может быть использовано злоумышленником?
3. Как определяется открытый порт на хосте?
4. Какие данные позволяют предположить проведение атаки типа «сканирование»?
5. На каких уровнях модели OSI могут быть реализованы угрозы?
6. Какие алгоритмы симметричного шифрования вы знаете?
7. Какие алгоритмы ассиметричного шифрования вы знаете?
8. Опишите алгоритм Диффи-Хеллмана. В чем его недостатки?
9. Какие способы классификации угроз вы знаете?
10. Какую информацию и на каких уровнях анализирует сетевой трафик МСЭ?
11. Какие функции выполняет модули МСЭ state и recent?
12. Какие функции выполняет модуль МСЭ connlimit и hashlimit?
13. В чем разница между МСЭ и СОВ?
14. Какие схемы интеграции МСЭ и СОВ существуют? В чем их преимущества и недостатки?
15. Какие существуют паттерны для определения атаки типа «подбор пароля»?
16. В чем заключается функция демилитаризованных зон (DMZ)?
17. Какие критерии безопасности являются приоритетными в РИУС?
18. Какие методики аудита безопасности вы знаете?
19. В чем недостатки активных методов аудита?
20. В чем недостатки пассивных методов аудита?
21. Для каких систем запрещено использовать активные методы аудита?
22. Какое место занимают системы «Honeypot» и «Sandbox» в системе защиты?
23. Против каких нарушителей использование honeypot актуально?
24. Какие проблемы возникают при решении задачи мониторинга РИУС?
25. В чем назначение proxy-агентов системы мониторинга?
26. В чем отличие активных и пассивных методов сбора информации?

2.4.2. Шкалы оценивания результатов обучения на зачете

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

Типовые шкала и критерии оценки результатов обучения при сдаче зачета 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 зачете считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

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 зачета используются типовые критерии, приведенные в общей части ФОС образовательной программы.