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
« 11 » сентября 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Нормативные документы и стандарты по информационной безопасности
(наименование)

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

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

Общая трудоёмкость: 108 (3)
(часы (ЗЕ))

Направление подготовки: 10.03.01 Информационная безопасность
(код и наименование направления)

Направленность: Информационная безопасность (общий профиль, СУОС)
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Цель дисциплины - освоение дисциплинарных компетенций по знанию и практическому применению нормативных документов и стандартов по информационной безопасности и защите информации.
- изучение основных положений и порядка применения нормативно-правовых актов по технической защите информации;
- изучение нормативных документов по обеспечению информационной безопасности объектов КИИ;
- изучение нормативных документов и административных регламентов по организации и осуществлению лицензионной деятельности в области технической защиты информации;
- изучение нормативных документов по сертификации средств защиты информации;
- изучение основных нормативных документов по аттестации объектов информатизации по требованиям безопасности информации;
- изучение состава и содержания основных стандартов по обеспечению информационной безопасности и защите информации;
- изучение основных нормативных, методических документов и регламентов ФСБ России по информационной безопасности и защите информации.

1.2. Изучаемые объекты дисциплины

- нормативно-правовые акты по технической защите информации;
- нормативные документы по обеспечению информационной безопасности объектов КИИ;
- административные регламенты по лицензионной деятельности в области технической защиты информации;
- нормативные документы по сертификации средств защиты информации;
- нормативные документы по аттестации объектов информатизации по требованиям безопасности информации;
- стандарты по обеспечению информационной безопасности и защите информации;
- нормативные, методические документы и регламенты ФСБ России по информационной безопасности и защите информации.

1.3. Входные требования

Не предусмотрены

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-2.2	ИД-1ПК-2.2	Знает критерии оценки защищенности объекта информатизации на основе нормативных документов и стандартов по информационной безопасности	Знает критерии оценки защищенности объекта информатизации; технические средства контроля эффективности мер защиты информации; методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации.	Отчёт по практическому занятию
ПК-2.2	ИД-2ПК-2.2	Умеет осуществлять контроль обеспечения уровня защищенности объектов информатизации на основе требований нормативных документов и стандартов по информационной безопасности	Умеет осуществлять контроль обеспечения уровня защищенности объектов информатизации	Отчёт по практическому занятию
ПК-2.2	ИД-3ПК-2.2	Владеет навыками оценки защищенности объектов информатизации на основе требований нормативных документов и стандартов по информационной безопасности	Владеет навыками оценки защищенности объектов информатизации с помощью типовых программных средств	Отчёт по практическому занятию

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	48	48
- лекции (Л)	22	22
- лабораторные работы (ЛР)		
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	22	22
- контроль самостоятельной работы (КСР)	4	4
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	60	60
2. Промежуточная аттестация		
Экзамен		
Дифференцированный зачет	9	9
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)		
Общая трудоемкость дисциплины	108	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
8-й семестр				
Введение в дисциплину	2	0	2	7
Структура дисциплины. Цель и задачи дисциплины. Основные понятия и определения. Взаимосвязь с другими дисциплинами. Необходимые требования к специалисту по защите информации по знанию и умению применять нормативные документы и стандарты по информационной безопасности				
Основные нормативно-правовые акты по технической защите информации	2	0	2	7
Состав и содержание основных нормативно-правовых актов по технической защите информации. Приказы. Положения. Специальные нормативные документы				
Нормативные документы по обеспечению объектов КИИ	2	0	2	8
Состав и содержание основных нормативных документов по обеспечению информационной безопасности объектов КИИ				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Нормативные документы по обеспечению лицензионной деятельности	2	0	2	8
Состав и содержание основных нормативных документов по организации и осуществлению лицензионной деятельности в области технической защиты информации. Административные регламенты. Реестры и иные нормативные документы				
Нормативные документы по сертификации средств защиты информации	4	0	4	8
Состав и содержание основных нормативных документов по сертификации средств защиты информации. Положения. Реестры и иные нормативные документы				
Нормативные документы по аттестации объектов информатизации	2	0	2	7
Состав и содержание основных нормативных документов по аттестации объектов информатизации по требованиям безопасности информации				
Стандарты по информационной безопасности и защите информации	4	0	4	8
Состав и содержание основных стандартов по обеспечению информационной безопасности безопасности и защите информации				
Основные нормативные, методические документы и регламенты ФСБ России по информационной безопасности	4	0	4	7
Состав и содержание основных нормативных, методических документов и регламентов ФСБ России по информационной безопасности и защите информации				
ИТОГО по 8-му семестру	22	0	22	60
ИТОГО по дисциплине	22	0	22	60

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Требования к специалисту по защите информации по знанию и умению применять нормативные документы и стандарты по информационной безопасности
2	Основные нормативно-правовые акты по технической защите информации. Приказы. Положения. Специальные нормативные документы
3	Нормативные документы по обеспечению информационной безопасности объектов КИИ
4	Нормативные документы по организации и осуществлению лицензионной деятельности в области технической защиты информации. Административные регламенты и реестры

№ п.п.	Наименование темы практического (семинарского) занятия
5	Основные нормативные документы по сертификации средств защиты информации. Положения и реестры
6	Основные нормативные документы по аттестации объектов информатизации по требованиям безопасности информации
7	Основные стандарты по обеспечению информационной безопасности безопасности и защите информации
8	Нормативные, методические документы и регламенты ФСБ России по информационной безопасности и защите информации

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 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 установление 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.

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 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	Защита информации : учебное пособие для вузов / Жук А. П., Жук Е. П., Лепёшкин О. М., Тимошкин А. И. 2-е изд. Москва : РИОР : ИНФРА-М, 2015. 392 с. 24,5 усл. печ. л.	5
2	Родичев Ю. А. Информационная безопасность: нормативно-правовые аспекты : учебное пособие для вузов. Санкт-Петербург [и др.] : Питер, 2008. 272 с.	8
3	Родичев Ю. А. Нормативная база и стандарты в области информационной безопасности : учебное пособие. Санкт-Петербург [и др.] : Питер, 2017. 254 с. 20,64 усл. печ. л.	6
4	Родичев Ю. А., Кубанков Ю. А., Симонов П. И. Безопасность инфокоммуникаций: стандартизация, измерения соответствия и подготовка кадров : учебное пособие для вузов. Москва : Горячая линия-Телеком, 2018. 159 с.	1
5	Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты : учебное пособие для вузов. М. : Гелиос АРВ, 2006. 527 с.	9
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Гринберг А. С., Горбачев Н. Н., Тепляков А. А. Защита информационных ресурсов государственного управления : учебное пособие для вузов. Москва : ЮНИТИ, 2003. 327 с.	4
2	Основы информационной безопасности : учебное пособие для вузов / Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. М. : Горячая линия-Телеком, 2006. 544 с.	26
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)
Дополнительная литература	Защита информации. Система стандартов. Основные положения	https://files.stroyinf.ru/Data2/1/4293780/4293780502.pdf	сеть Интернет; свободный доступ

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

Вид ПО	Наименование ПО
Операционные системы	MS Windows 8.1 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	Microsoft Office Professional 2007. лиц. 42661567
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017

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

Наименование	Ссылка на информационный ресурс
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/
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
Лекция	Мультимедийное оборудование	1
Практическое занятие	Персональный компьютер	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 «Нормативные документы и стандарты по информационной безопасности»
Приложение к рабочей программе дисциплины

Направление подготовки: 10.03.01 Информационная безопасность
Направленность (профиль) образовательной программы: Организация и технология защиты информации

Квалификация выпускника: Бакалавр

Выпускающая кафедра: Автоматика и телемеханика

Форма обучения: Очная

Курс: 4 **Семестр**: 8

Трудоёмкость:
Кредитов по рабочему учебному плану: 3 ЗЕ
Часов по рабочему учебному плану: 108 ч.

Форма промежуточной аттестации:
Диф. зачет: 8 семестр

Пермь 2023

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 одного семестра (8-го семестра учебного плана) и разбито на 3 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные и практические 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 практическим заданиям 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**	**ПЗ**	**Т/КР**		**Экзамен**
Усвоенные знания						
З.1 Знать критерии оценки защищенности объекта информатизации на основе нормативных документов и стандартов по информационной безопасности		ТО1 ТО2	ПЗ1 ПЗ 2	Т		ТВ
Освоенные умения						
У.1 уметь осуществлять контроль обеспечения уровня защищенности объектов информатизации на основе требований нормативных документов и стандартов по информационной безопасности			ПЗ 3 ПЗ 4 ПЗ 5 ПЗ 6	Т		ПЗ
Приобретенные владения						
В.1 владеть навыками оценки защищенности объектов информатизации на основе требований нормативных документов и стандартов по информационной безопасности			ПЗ 7 ПЗ 8	Т		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 в рамках контроля самостоятельной работы студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в журнал 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 отчета по результатам практических заданий (после изучения каждого модуля учебной дисциплины).

Всего запланировано 11 практических занятий. Темы практических занятий приведены в РПД.

Отчет по выполнению практического задания проводится индивидуально каждым студентом. 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. Определение и цели информационной безопасности. Основные направления информационной безопасности.
2. Государственная система защиты информации. (Положение-93). Основные функции ГСЗИ РФ.
3. Правовые акты и ОРД определяющие место и роль службы защиты информации в системе обеспечения безопасности на предприятии.
4. Задачи и функции службы защиты информации на предприятии. Полномочия службы защиты информации на предприятии.
5. Организационные основы и принципы деятельности службы защиты информации на предприятии.
6. Структура службы защиты информации на предприятии, взаимодействие с другими службами.
7. Организационная структура государственной системы обеспечения информационной безопасности.
8. Трехуровневая система защиты информации в федеральном округе. Обеспечение информационной безопасности на уровне субъектов Российской Федерации.
9. Реализация Федерального закона «Об информации, информационных технологиях и о защите информации» № 149-ФЗ. Основные положения федерального закона № 149-ФЗ, касающиеся защиты информации.
10. Организация работы подразделения по защите информации по реализации задач по обеспечению информационной безопасности.

11. Сущность и содержание комплексной защиты информации. Основные направления и ключевые задачи управления системой защиты информации на предприятии.
12. Основные элементы системы защиты информации на предприятии. Разработка положения о ПДТК.
13. Требования ФСТЭК к разработке Руководства (Положения) по защите информации на предприятии.
14. Сущность и содержание комплексной защиты информации. Структура и основное содержание Концепции комплексной безопасности предприятия.
15. Нормативно-правовая база деятельности службы защиты информации на предприятии.
16. Особенности организации защиты информации при возложении обязанностей на системных администраторов.
17. Направления защиты информации на объекте защиты.
18. Последовательность и содержание работ по организации комплексной защиты информации.
19. Основные принципы защиты информации от несанкционированного доступа. Дайте определение способов НСД к охраняемым сведениям конфиденциального характера.
20. Разработка организационно-распорядительных документов, регламентирующих деятельность службы защиты информации, ее подразделений и сотрудников.
21. Требования к оборудованию и техническим средствам, используемым сотрудниками службы защиты информации. Функции службы защиты информации по эксплуатации СрЗИ.
22. Трехуровневая система организации защиты информации в федеральном округе. Обеспечение информационной безопасности на объектовом уровне.
23. Особенности организации защиты информации в федеральном округе. Основы организации защиты информации в Приволжском федеральном округе.
24. Порядок проведения основных мероприятий по технической защите информации. Применение современных инженерно-технические средств защиты информации.
25. Основные методы защиты информации техническими средствами.
26. Требования и рекомендации по защите конфиденциальной информации в автоматизированных системах.
27. Требования и рекомендации по защите информации**,** циркулирующей в защищаемых помещениях.
28. Значение Доктрины информационной безопасности Российской Федерации в создании системы защиты информации.
29. Система лицензирования деятельности в области технической защиты конфиденциальной информации.
30. Система сертификации средств защиты информации в Российской Федерации.
31. Порядок проведения основных мероприятий по созданию на предприятии системы технической защиты информации по требованиям государственных органов, уполномоченных в области безопасности.

32. Особенности функциональных обязанностей руководителя службы защиты информации.
33. Компетентностные уровни профессионалов в области информационной безопасности.
34. Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации.
35. Особенности квалификационных характеристик специалистов по защите информации, в соответствии с федеральными государственными стандартами.
36. Учет вопросов информационной безопасности в должностных обязанностях работников предприятия.
37. Профессиональные компетенции специалиста по защите информации в области компьютерной форензики.

Типовые практические задания для контроля освоенных умений:

1. Разработайте алгоритм и раскройте содержание работ по организации ТЗИ на объектах информатизации.
2. Определите задачи, функции, обязанности, права и ответственность администратора ИБ подразделения по ТЗИ в организации.
3. Разработайте алгоритм создания системы ТЗИ и раскройте содержание основных мероприятий по технической защите информации.

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.