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
« 21 » сентября 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Безопасность открытых информационных систем
(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

Целями освоения дисциплины «Безопасность открытых информационных систем- БОИС» является приобретение студентами фундаментальных представлений о функциях современной БОИС и о структуре ее функциональных компонентов, дается определение задач БОИС и ее границ, говорится об адекватном позиционировании и средствах интеграции БОИС в современной ИТ структуре.
Современная проблема обеспечения безопасности информационных систем компаний, фирм, производств, Госучреждений является довольно сложным комплексом и объективными причинами появления этой проблемы и ее решения являются внутренние (сбои техники и программного обеспечения, ошибки и недоработки в проектировании, наладке систем, недостатки в масштабировании, обслуживания системы, администрирования мониторинга, аудита систем, преднамеренные и целенаправленные действия обслуживающего персонала, ведущие к нарушению сохранности информации), внешние (наличие объективных причин уязвимостей действующих систем и, как следствие, хакерские атаки и взлом систем) причины.. В курсе делается попытка создания единой системы обеспечения безопасности начиная от идеи создания такой системы, проектирования ее, наладке, эксплуатации и масштабирования. Отдельной темой будет раскрытие понятий, что такое система, информация ,безопасность, открытые и закрытые системы.
?
Цели изучения дисциплины.

- Уметь анализировать классы задач и процессов, создания защищенных информационных систем и навыков их поддержания ;
- Описывать основные функциональные подсистемы и их взаимодействие в рамках комплексной БОИС;
- Владеть методикой выбора средств автоматизации и методология процесса внедрения системы;
- Знать разницу решения данной проблемы в отечественных организациях и зарубежных компаниях;
- Понимать, персоналу разрешено все, что не запрещено, строгое соблюдение инструкций и этапов выполнение работ, уяснения понятия важности каждой должности в едином организме фирмы, справедливой системы материального поощрения;
- Приобретение навыков в диагностировании работы алгоритмов, техники, протоколов, коррекция инструкций и положений;
- Единое требование к безопасности- всеобщая система двойной парольной защиты, хранение любой информации в зашифрованном формате и система допуска к технике, программному обеспечению и атрибутам информации.

1.2. Изучаемые объекты дисциплины

Открытые информационные системы

1.3. Входные требования

- Знание основ курса “Криптографические основы защиты информации”;
- Знание основ курса “Информационная безопасность “
- Знание основ курса “Дискретная математика “
- Понятие “OSI”, основные протоколы? алгоритмы, машрутизация пакетов передачи данных.

трены

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-2.1	ИД-1ПК-2.1	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.	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.	Экзамен
ПК-2.1	ИД-2ПК-2.1	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	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	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-2.1	ИД-3ПК-2.1	Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы; разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НДС и специальных воздействий на соответствие техническим условиям	Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы; разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НДС и специальных воздействий на соответствие техническим условиям	Отчет по практике

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:	126	72	54
- лекции (Л)	60	36	24
- лабораторные работы (ЛР)	32	16	16
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	30	18	12
- контроль самостоятельной работы (КСР)	4	2	2
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	126	72	54
2. Промежуточная аттестация			
Экзамен	36	36	
Дифференцированный зачет			
Зачет	9		9
Курсовой проект (КП)			
Курсовая работа (КР)			
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				
Методологические основы обеспечения безопасности информационных систем (БИС)	18	8	10	36
1.1 Философское трактование понятий открытых и закрытых систем и подсистем 1.2. Архитектура и основы (БИС) 1.3. Концепсия. (БИС) 1.4.Теоретические основы утентификации 1.5.Основные положения управление доступа к элеменам информации. 1.6.Понятие положений конфиденциальности, сохранности, ответственности и авторства информации 1.7.Обеспечение основ мониторинга и аудита (БИС) 1.8. Криптографические основы (БИС)				
Математические, технические, прооамные средства обеспечения (БИС)	18	8	8	36
2.1. Администрирование, масштабирование, настройка (БИС) 2.2. Настройка экранов. Брандмауэров, антивирусная защита.				
ИТОГО по 10-му семестру	36	16	18	72
11-й семестр				
Основные положения способы создания защищенных сетей на базе сетей интернета.	24	16	12	54
1.Сети Win VPN, OpenVpn., Cisko Pacet Tracer. 1.2. Моделирование . (БИС) На основе Virtual Box. 1.3. Моделирование . (БИС) На основе OpenVpn/ .1.4. Моделирование . (БИС) На основе. Cisko Pacet Tracer 1.5. Построение сетей в терминальных классах. 1.6. Построение сетей на оборудовании домашних компьютеров студентов. 1.7.Организация систем удаленного доступа				
ИТОГО по 11-му семестру	24	16	12	54
ИТОГО по дисциплине	60	32	30	126

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия

№ п.п.	Наименование темы практического (семинарского) занятия
1	Философское трактование понятий открытых и закрытых систем и подсистем
2	Архитектура и основы БИС
3	Концепция БИС
4	Теоретические основы утентификации
5	Основные положения управление доступа к элементам информации
6	Понятие положений конфиденциальности, сохранности, ответственности и авторства информации
7	Обеспечение основ мониторинга и аудита БИС
8	Криптографические основы БИС
9	Администрирование, масштабирование, настройка БИС
10	Настройка экранов. Брандмауэров, антивирусная защита
11	Основы работы Win VPN
12	Основы работы OpenVPN
13	Основы работы Cisko Packet Tracer

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Изучение и опробование системы крипто-защиты WinApi
2	Разработка сети в пакете Cisko Packet Tracer
3	Разработка Config клиентов и серверов OpenVPN
4	Построение сетей в терминальных классах.
5	Организация систем удаленного доступа
6	Построение сетей на оборудовании домашних компьютеров студентов

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.

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	Бабаш А. В. Криптография / А. В. Бабаш, Г. П. Шанкин. - Москва: СОЛОН-Р, 2002.	2
2	Основы информационной безопасности : учебное пособие для вузов / Е. Б. Белов [и др.]. - Москва: Горячая линия-Телеком, 2011.	2
3	Основы криптографии : учебное пособие для вузов / А. П. Алферов [и др.]. - Москва: Гелиос АРВ, 2002.	2

4	Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В.Романец,П.А.Тимофеев,В.Ф.Шаньгин. - М.: Радио и связь, 1999.	4
5	Смарт Н. Криптография : пер. с англ. / Н. Смарт. - Москва: Техносфера, 2006.	5
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Анин Б., Петрович А. Радиошпионаж. М.: Международные отношения, 1996	2
2	Григорьев В.А. Передача сообщений по зарубежным информаци¬ онным сетям. Л.: ВАС, 1989.	2
3	Диффи У. Первые десять лет криптографии с открытым ключом / / ТИИЭР. 1988	2
4	Ярочкин В.И. Обеспечение сохранения коммерческой тайны предприятия.— М.: ИПКИР, 1998.	2
5	Ярочкин В.И. Технические каналы утечки информа- ции.— М.: ИПКИР, 1994.	2
6	Ярочкин В.И., Шевцова ГЛ. Каталог обобщенных мероприятий по защите конфиденциальной информации.— М.: ИПКИР, 1997.	2
2.2. Периодические издания		
1	Журнал официальной информации КАДАСТР.	2
2	Иностранец	2
3	Научная информация	2
4	Финансовая газета.	2
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	Милославская Н. Г. Сетевые атаки на открытые системы на примере Интранета : учебное пособие для вузов / Милославская Н. Г. - Москва: НИЯУ МИФИ, 2012.	http://elib.pstu.ru/Record/lan75789	сеть Интернет; авторизованный 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.	Adobe Acrobat Reader DC. бесплатное ПО просмотра PDF
Офисные приложения.	Microsoft Office Professional 2007. лиц. 42661567
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017
Прикладное программное обеспечение общего назначения	WinRAR (лиц№ 879261.1493674)

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

Наименование	Ссылка на информационный ресурс
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/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лабораторная работа	Персональный компьютер IBM PC	8
Лекция	Проектор	1
Практическое занятие	Персональный компьютер IBM PC	8

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 «Безопасность открытых информационных систем»
Приложение к рабочей программе дисциплины

Специальность:	10.05.03 Информационная безопасность автоматизированных систем
Специализация (профиль) образовательной программы:	Безопасность открытых информационных систем
Квалификация выпускника:	Специалист
Выпускающая кафедра:	Автоматика и телемеханика
Форма обучения:	Очная

Курс: 5,6 **Семестр**: 10,11

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

Форма промежуточной аттестации:
Экзамен: 10 семестр
Зачет: 11 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 двух семестров (10,11-го семестров учебного плана) и разбито на 3 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные и лабораторные занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируется компоненты профессиональной компетенции **ПК-2.1**: Способен разрабатывать, и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности. З*нать, 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 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		ТО1	ПЗ1 ПЗ2 ПЗ7 ПЗ12 ПЗ13	Т		ТВ
Освоенные умения						

У.1 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			ПЗ 2 ПЗ 3 ПЗ 6 ПЗ 8 ПЗ 10	Т		ПЗ
Приобретенные владения						
В.1 Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы			ПЗ 4 ПЗ 5 ПЗ 7 ПЗ 9 ПЗ 11	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 13 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 и умений:

1. Загрузка , наладка, системы OpenVpnна роутерах
2. Настройка двух и более OpenVpn серверов на одном сервере.
3. Настройка двух и более OpenVpn клиентов на одном сервере.
4. Программная обработка журналов событий в OpenVpn.
5. Загрузка OpenVpn в системе «Облако».
6. Создание корпоративных сетей в системе Hamchi.
7. Анализ эффективности систем защиты Hamchi и OpenVpn.
8. Создание двойногоVpn на основе OpenVpn.
9. Создание системы OpenVpn на виртуальных компьютерах.

10.Система шифрования –дешифрования в OpenVpn_в режиме on-line.

11.Система шифрования –дешифрования в OpenVpn на базе OpenSsll.

12.Система шифрования –дешифрования в OpenVpn на базе GryptowinApi.

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.