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

« 07 » марта 20 23 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**Дисциплина:** Безопасность и защита информации
(наименование)

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

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

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

**Направление подготовки:** 09.04.01 Информатика и вычислительная техника
(код и наименование направления)

**Направленность:** Компьютерные системы и сети
(наименование образовательной программы)

Пермь 2023

## 1. Общие положения

### 1.1. Цели и задачи дисциплины

Цель учебной дисциплины – изучение современных средств и методов защиты компьютерной информации от несанкционированного доступа: средств современных операционных систем, криптографических алгоритмов, межсетевых экранов, научиться применять стандартные прикладные пакеты для обеспечения безопасности информации, а также проектировать собственные средства защиты.
Задачи учебной дисциплины:
- изучение средств защиты, стандартов оценки защищенности и основных уязвимостей программного обеспечения;
- формирование умения осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных средств;
- формирование навыков администрирования безопасности, выявления и устранения уязвимостей программного обеспечения.

### 1.2. Изучаемые объекты дисциплины

Предметом освоения дисциплины являются следующие объекты:
- основные типы угроз;
- основные способы защиты от угроз;
- технические средства защиты;
- организационные и юридические средства защиты;
- основы разработки средств защиты.

### 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 |
|---|---|---|---|---|
| ОПК-5 | ИД-1ОПК-5 | Знает: основные понятия информационной безопасности и защиты информации; источники, риски, формы атак на информацию; методы обеспечения надежности программ. | Знает и выбирает нормативно-техническую информацию для разработки проектной, распорядительной документации | Дифференцированный зачет |
| ОПК-5 | ИД-2ОПК-5 | Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных средств защиты. | Умеет оформлять проекты нормативных и распорядительных документов организации в сфере профессиональной деятельности | Дифференцированный зачет |

| Компетенция | Индекс индикатора | Планируемые результаты обучения по дисциплине (знать, уметь, владеть) | Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения | Средства оценки |
|---|---|---|---|---|
| ОПК-5 | ИД-3ОПК-5 | Владеет средствами анализа информационной безопасности. | Владеет навыками разработки и оформления проектной документации в сфере профессиональной деятельности в соответствии действующими нормами | 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:<br>1.1. Контактная аудиторная работа, из них: | 72 | 72 |
| - лекции (Л) | 18 | 18 |
| - лабораторные работы (ЛР) | 24 | 24 |
| - практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ) | 26 | 26 |
| - контроль самостоятельной работы (КСР) | 4 | 4 |
| - контрольная работа | | |
| 1.2. Самостоятельная работа студентов (СРС) | 72 | 72 |
| 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 | | | | |

| Наименование разделов дисциплины с кратким содержанием | Объем аудиторных занятий по видам в часах | | | Объем внеаудиторных занятий по видам в часах |
|---|---|---|---|---|
| | Л | ЛР | ПЗ | СРС |
| Понятие информационной безопасности | 8 | 12 | 12 | 36 |
| Введение. Основные определения и понятия. Основы информационной безопасности и защиты информации. Тема 1. Основные определения и понятия. Основы информационной безопасности и защиты информации.<br>Основные понятия и определения: информация. Система обработки информации. Объект информатизации. Информационные ресурсы (активы). Защищаемая информация. Безопасность информации. Защита информации. Парольная система. Техническая защита информации. Физическая защита информации. Способ защиты информации. Средство защиты информации. Тема 2. Источники, риски, формы атак на информацию.<br>Обзор и параметры классификации угроз безопасности информации. Понятие и подходы к построению модели угроз. Основные понятия: угроза, уязвимость, источник угрозы безопасности информации, защита информации от несанкционированного доступа. Классификация угроз информационной безопасности. Угрозы коммерческой информации. Классификация злоумышленников. Основные методы реализации угроз информационной безопасности. Причины. Виды и каналы утечки информации. Тема 3. Политика безопасности. Стандарты безопасности.<br>Политика ИБ: общее понятие и место в системе защиты информации. Организационные вопросы обеспечения безопасности. Современные международные подходы в области управления безопасностью корпоративных информационных систем. Общие критерии безопасности. Действующие стандарты и рекомендации в области информационной безопасности. Регламентирующие документы в области информационной безопасности. Особенности информационной безопасности компьютерных сетей. Тема 4. Администрирование компьютерных сетей. Планирование развития сети. Устранение неисправностей сети. Установка и настройка программного обеспечения. Модернизация компьютерного оборудования. Мероприятия по обеспечению безопасности сети. Техническая поддержка пользователей сети. Защита от несанкционированного доступа: идентификация, аутентификация, управление доступом. Алгоритмы аутентификации пользователей. Парольные системы аутентификации: идентификатор пользователя, пароль пользователя, учетная запись пользователя. | | | | |
| | | | | |

| Наименование разделов дисциплины с кратким содержанием | Объем аудиторных занятий по видам в часах | | | Объем внеаудиторных занятий по видам в часах |
|---|---|---|---|---|
| | Л | ЛР | ПЗ | СРС |
| Средства защиты информации<br>Тема 5. Криптопрограммирование. Криптопрограммирование посредством использования инкрементальных алгоритмов. Основные элементы инкрементальной криптографии. Методы защиты данных посредством инкрементальных алгоритмов маркирования. Вопросы стойкости инкрементальных схем. Применение инкрементальных алгоритмов для защиты от вирусов. Тема 6. Методы обеспечения надежности программ, используемые для контроля их технологической безопасности. Исходные данные, определения и условия. Краткий анализ существующих моделей надежности программного обеспечения. Описание модели Нельсона. Оценка технологической безопасности программ на базе метода Нельсона. Тема 7. Самотестирующиеся и самокорректирующиеся программы. Вводные замечания. Общие принципы создания двухмодульных вычислительных процедур и методология самотестирования. Устойчивость, линейная и единичная состоятельность. Метод создания самокорректирующейся процедуры вычисления теоретико-числовой функции дискретного экспоненцирования. Метод создания самотестирующейся расчетной программы с эффективным тестирующим модулем. Исследования процесса верификации расчетных программ. Области применения самотестирующихся и самокорректирующихся программ и их сочетаний. Тема 8. Правовая и организационная поддержка процессов разработки и применения программного обеспечения. Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации. Сертификационные испытания программных средств. Безопасность программного обеспечения и человеческий фактор. Заключение. Перспективы развития средств защиты программного обеспечения. | 10 | 12 | 14 | 36 |
| ИТОГО по 4-му семестру | 18 | 24 | 26 | 72 |
| ИТОГО по дисциплине | 18 | 24 | 26 | 72 |

Тематика примерных практических занятий

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

| № п.п. | Наименование темы практического (семинарского) занятия |
|---|---|
| 1 | Построение модели угроз безопасности информации. |
| 2 | Противодействие основным методам реализации угроз информационной безопасности. |
| 3 | Планирование развития компьютерной сети. |
| 4 | Мероприятия по обеспечению безопасности сети. Техническая поддержка пользователей сети. |
| 5 | Применение инкрементальных алгоритмов для защиты от вирусов. |
| 6 | Применение самотестирующихся и самокорректирующихся программ и их сочетаний. |

Тематика примерных лабораторных работ

| № п.п. | Наименование темы лабораторной работы |
|---|---|
| 1 | Исследование эффективности работы программных средств защиты от несанкционированного доступа. |
| 2 | Изучение основных средств безопасности Windows. |
| 3 | Анализ уязвимостей данных в ОС Windows и средств их устранения. |
| 4 | Анализ средств безопасности ASP.NET. Аутентификация. |
| 5 | Инсталляция и администрирование средств сетевой защиты распределенных хранилищ данных. |
| 6 | Криптопрограммирование с использованием стандартов DES и RSA. |

## 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 | Семененко В.А. Информационная безопасность : учебное пособие для вузов. 2-е изд., стер. М. : Изд-во МГИУ, 2006. 276 с. | 10 |
| **2. Дополнительная литература** | | |
| **2.1. Учебные и научные издания** | | |
| 1 | Лапонина О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие. 2-е изд., испр. Москва : ИНТУИТ : БИНОМ. Лаб. знаний, 2007. 531 с. | 4 |
| **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) |
|---|---|---|---|
| Учебно-методическое обеспечение самостоятельной работы студентов | Безопасность и защита информации. Курс лекций. | ftp://itas.pstu.ru | 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 | Windows 10 (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 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/ |

### 7. Материально-техническое обеспечение образовательного процесса по дисциплине

| Вид занятий | Наименование необходимого основного оборудования и технических средств обучения | Количество единиц |
|---|---|---|

| Вид занятий | Наименование необходимого основного оборудования и технических средств обучения | Количество единиц |
|---|---|---|
| Лабораторная работа | Персональные компьютеры. | 20 |
| Лекция | Мультимедийный проектор, экран. | 1 |
| Практическое занятие | Персональные компьютеры. | 20 |

## 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 и защита информации»**
***Приложение к рабочей программе дисциплины***

| | |
|---|---|
| **Направление подготовки:** | 09.04.01Информатика и вычислительная техника |
| **Направленность (профиль) образовательной программы:** | Информационные технологии интеллектуальной обработки больших данных (Big Data).<br>Автоматизированные системы обработки информации и управления.<br>Технологии искусственного интеллекта в социальных и экономических системах.<br>Компьютерные системы и сети. |
| **Квалификация выпускника:** | «Магистр» |
| **Выпускающая кафедра:** | Информационные технологии и автоматизированные системы |
| **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:**
Дифференцированный зачет: 4 семестр

Пермь 2023 г.

**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). В семестре предусмотрены аудиторные лекционные и лабораторные и практические занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируется компоненты компетенций (ОПК-5) *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (таблица 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, практическим заданиям и дифференцированного 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** | | **Промежуточный /рубежный** | | |
| | **С** | **ТО** | **ОЛР** | **КЗ** | **Диф. зачет** |
| **Усвоенные знания** | | | | | |
| **З.1** знать основные понятия информационной безопасности и защиты информации; источники, риски, формы атак на информацию; методы обеспечения надежности программ | С1 | ТО1 | | | ТВ1 |
| **Освоенные умения** | | | | | |
| **У.1** уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных средств защиты | С2 | ТО2 | ОЛР1 | КЗ1 | ПЗ1 |
| **Приобретенные владения** | | | | | |
| **В.1** владеть средствами анализа информационной безопасности | С3 | ТО3 | ОЛР2 | КЗ2 | ПЗ2 |

*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 дифференцированного зачета, проводимая с

учетом результатов текущего и рубежного контроля.

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

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

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

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

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

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

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

- контроль остаточных знаний.

### 2.1. Текущий контроль усвоения материала

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

### 2.2. Рубежный (промежуточный) контроль

Рубежный (промежуточный) контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (таблица 1.1) проводится в форме защиты лабораторных работ и практических заданий.

#### 2.2.1. Защита лабораторных работ

Всего запланировано 9 лабораторных работ. Типовые темы лабораторных работ приведены в РПД.

Защита лабораторной работы проводится индивидуально каждым студентом

или группой студентов. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

**2.2.2. Защита практических заданий**

Всего запланировано 6 практических занятий. Типовые темы практических занятий приведены в РПД.

Защита практических заданий проводится индивидуально каждым студентом или группой студентов. 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 дифференцированного зачета. Дифференцированный 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.

**2.4.2. Процедура промежуточной аттестации с проведением аттестационного испытания**

В отдельных случаях (например, в случае переаттестации дисциплины) промежуточная аттестация в виде дифференцированного зачета по дисциплине может проводиться с проведением аттестационного испытания по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний, практические задания (ПЗ) для проверки освоенных умений и комплексные задания (КЗ) для контроля уровня приобретенных владений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности всех заявленных компетенций.

**2.4.2.1. Типовые вопросы и задания для зачета по дисциплине**

**Типовые вопросы для контроля усвоенных знаний**:

1. Система обработки информации.
2. Объект информатизации.
3. Защищаемая информация.
4. Безопасность информации.
5. Техническая защита информации.
6. Способ защиты информации.

**Типовые вопросы и практические задания для контроля освоенных умений**:

1. Изучить основные средства безопасности Windows.
2. Исследовать эффективность работы программных средств защиты от несанкционированного доступа.
3. Владеть навыками противодействия основным методам реализации угроз информационной безопасности.

**Типовые комплексные задания для контроля приобретенных владений:**

1. Построить модель угроз безопасности информации.
2. Провести анализ уязвимостей данных в ОС Windows и средств их устранения.
3. Провести криптопрограммирование с использованием стандартов DES и RSA.

**2.4.2.2. Шкалы оценивания результатов обучения на дифференцированном 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 дифференцированном 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

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