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
« 27 » сентября 20 22 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Информационная безопасность и кибербезопасность цифрового производства
(наименование)

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

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

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

Направление подготовки: 09.03.03 Прикладная информатика
(код и наименование направления)

Направленность: Прикладная информатика (общий профиль, СУОС)
(наименование образовательной программы)

Пермь 2022

1. Общие положения

1.1. Цели и задачи дисциплины

Цели: ознакомление студентов с основными понятиями, методологией и практическими приемами управления информационной безопасностью; организационной и технической инфраструктурой обеспечения информационной безопасности организации (цифрового предприятия).

Задачи:

- изучение стандартов управления информационной безопасностью;
- освоение принципов формирования политики информационной безопасности;
- изучение методов оценки рисков, методов управления инцидентами информационной безопасности;
- овладение навыками эксплуатации подсистем управления информационной безопасностью.

1.2. Изучаемые объекты дисциплины

- стандарты управления информационной безопасностью;
- политика информационной безопасности;
- методы оценки рисков и управления инцидентами информационной безопасности;
- инфраструктура обеспечения информационной безопасности организации, в том числе современного цифрового производства.

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-3	ИД-1опк-3	Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; основы бухгалтерского и управленческого учета.	Индивидуальное задание

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ОПК-3	ИД-2опк-3	Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; умеет проводить анализ и оценку состояния защищенности объектов информатизации на основе действующих отечественных и международных стандартов информационной безопасности.	Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; умеет применять современные информационно-коммуникационные технологии для бухгалтерского и управленческого учета.	Индивидуальное задание
ОПК-3	ИД-3опк-3	Владеет навыками подготовки обзоров, аннотаций, рефератов, отчетов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности; резервного копирования и архивирования документации; владеет навыками эксплуатации подсистем управления информационной безопасностью.	Владеет навыками подготовки обзоров, аннотаций, рефератов, отчетов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности; резервного копирования и архивирования документации.	Индивидуальное задание

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:	54	54
- лекции (Л)	20	20
- лабораторные работы (ЛР)		
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	30	30
- контроль самостоятельной работы (КСР)	4	4
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	54	54
2. Промежуточная аттестация		
Экзамен		
Дифференцированный зачет		
Зачет	9	9
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				
Модуль 1. Основы управления информационной безопасностью (ИБ).	8	0	8	18
Тема 1. Введение. Основные определения. Цели, задачи и принципы управления ИБ. Тема 2. Стандарты систем и процессов ИБ. История стандартизации в области ИБ. Современные стандарты: ISO, ISO\IEC, BS, CoBiT, ГОСТ, СТО БР ИББС. Преимущества и недостатки стандартов. Тема 3. Политика ИБ. Понятие, цели, требования, принципы разработки и внедрения политики ИБ. Содержание и жизненный цикл политики ИБ. Ответственность за выполнение политики ИБ.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Модуль 2. Управление рисками, инцидентами и аудит ИБ.	8	0	8	18
Тема 4. Система управления ИБ организации (СУИБ) . Построение и внедрение процессов СУИБ. Методы управления ИБ организации. Тема 5. Оценка и обработка рисков. Порядок и методы оценки рисков. Варианты обработки рисков. Система управления инцидентами. Тема 6. Цели, виды и принципы аудита ИБ. Метрики эффективности СУИБ.				
Модуль 3. Технические аспекты управления ИБ.	4	0	14	18
Тема 7. Управление логическим доступом к активам организации. Обязанности пользователя. Управление сетевым доступом, доступом к операционной системе и приложениям. Мобильные устройства и дистанционная работа. Тема 8. Управление защищенной передачей данных и операционной деятельностью. Документированные процедуры. Разделение полномочий, разграничение сред разработки и промышленной эксплуатации. ИБ в процессах разработки и сопровождения информационных систем.				
ИТОГО по 8-му семестру	20	0	30	54
ИТОГО по дисциплине	20	0	30	54

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Сущность и функции управления ИБ
2	Применение современных стандартов по управлению ИБ
3	Разработка политики ИБ
4	Система управления ИБ (СУИБ)
5	Оценка и обработка рисков ИБ
6	Управление инцидентами ИБ
7	Организация аудита ИБ
8	Управление логическим доступом к активам организации
9	Управление защищенной передачей данных и операционной деятельностью
10	Выработка требований по обеспечению безопасности в процессах разработки и сопровождения ИС
11	Управление конфигурациями, изменениями и обновлениями

№ п.п.	Наименование темы практического (семинарского) занятия
12	Компетенции для эксплуатации подсистем управления ИБ цифрового производства

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	Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации : учебное пособие. 4-е изд., перераб. и доп. Москва : РИОР : ИНФРА-М, 2022. 335 с. 21 усл. печ. л.	3
2	Зенков А. В. Основы информационной безопасности : учебное пособие. Москва Вологда : Инфра-Инженерия, 2022. 101 с.	3

3	Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Зегжда Д. П., Александрова Е. Б., Калинин М. О., Марков А. С. Москва : Горячая линия-Телеком, 2021. 559 с.	3
4	Малюк А. А., Горбатов В. С., Королев В. И. Введение в информационную безопасность : учебное пособие для вузов. Москва : Горячая линия-Телеком, 2021. 287 с.	6
5	Медведев В. А. Информационная безопасность. Введение в специальность : учебник. Москва : КНОРУС, 2021. 143 с. 9,0 усл. печ. л.	1
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Гришина Н. В. Основы информационной безопасности предприятия : учебное пособие. Москва : ИНФРА-М, 2021. 185 с. 13,5 усл. печ. л.	3
2	Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны. Безопасность инфраструктуры тактик Красной и Синей команд : пер. с англ. Москва : ДМК Пресс, 2020. 325 с. 26,49 усл. печ. л.	1
3	Малюк А. А. Основы политики безопасности критических систем информационной инфраструктуры. Курс лекций : учебное пособие. Москва : Горячая линия-Телеком, 2021. 313 с. 19,63 усл. печ. л.	11
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	Прохорова О. В. Информационная безопасность и защита информации. 2-е изд., испр. Санкт-Петербург : Лань, 2020. 124 с.	URL: https://elib.pstu.ru/Record/lanRU-LAN-BOOK-133924	локальная сеть; авторизованный доступ
Основная литература	Нестеров С. А. Основы информационноu? безопасности. Санкт-Петербург : Лань, 2021. 324 с.	URL: https://elib.pstu.ru/Record/lanRU-LAN-BOOK-165837	локальная сеть; 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

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/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лекция	Презентационный комплекс: экран, проектор, компьютер	1
Практическое занятие	Компьютерный класс: компьютеры, объединенные в локальную сеть, с постоянным выходом в Интернет, проектор.	1

8. Фонд оценочных средств дисциплины

Описан в отдельном документе

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Пермский национальный исследовательский политехнический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации обучающихся по дисциплине

«Информационная безопасность и кибербезопасность цифрового производства»

Приложение к рабочей программе дисциплины

Направление подготовки:	09.03.03 Прикладная информатика
Направленность (профиль) образовательной программы:	Цифровые технологии в менеджменте Цифровые технологии в финансах
Квалификация выпускника:	Бакалавр
Выпускающая кафедра:	Менеджмент и маркетинг, Экономика и финансы
Форма обучения:	Очная
Форма промежуточной аттестации	Зачет

Пермь 2020 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 (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 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, выполнении практических заданий и зачета. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Контролируемые результаты обучения по дисциплине

Контролируемые результаты освоения дисциплины (ЗУВы)	**Вид контроля**		
	Текущий	**Рубежный**	**Промежуточная аттестация Зачет**
Усвоенные знания			
З.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ТО		КИЗ
Освоенные умения			
У.1. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; умеет проводить анализ и оценку состояния защищенности объектов информатизации на основе действующих отечественных и международных стандартов информационной безопасности.		ИЗ	КИЗ
Приобретенные владения			

В.1. Владеет навыками подготовки обзоров, аннотаций, рефератов, отчетов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности; резервного копирования и архивирования документации; владеет навыками эксплуатации подсистем управления информационной безопасностью.		ИЗ	КИЗ

Условные обозначения:
ТО – теоретический опрос;
ИЗ – индивидуальное задание;
КИЗ – комплексное индивидуальное задание.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде 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), 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

Текущий контроль усвоения материала лекций (знаний) проводится по каждой теме в форме текущего опроса (ТО). Результаты по 4-балльной шкале оценивания заносятся в книжку преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

Типовые задания для текущего опроса (ТО)

1. Под информационной безопасностью понимается…

А) **защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.**

Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

В) нет правильного ответа

2. Защита информации – это..

А) **комплекс мероприятий, направленных на обеспечение информационной безопасности.**

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

3. Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

4. Доступность – это…

А) **возможность за приемлемое время получить требуемую информационную услугу.**

Б) логическая независимость

В) нет правильного ответа

5. Целостность – это..

А) **целостность информации**

Б) непротиворечивость информации

В) защищенность от разрушения

6. Конфиденциальность – это..

А) **защита от несанкционированного доступа к информации**

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

7. Угроза – это…

А) **потенциальная возможность определенным образом нарушить информационную безопасность**

Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных

В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

8. Атака – это…

А) **попытка реализации угрозы**

Б) потенциальная возможность определенным образом нарушить информационную безопасность

В) программы, предназначенные для поиска необходимых программ.

9. Источник угрозы – это..

А) **потенциальный злоумышленник**
Б) злоумышленник
В) нет правильного ответа

10. Окно опасности – это…
А) **промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.**
Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

11. Предпосылки появления угроз:
А) **объективные**
Б) субъективные
В) преднамеренные

12. СЗИ (система защиты информации) делится:
А) **ресурсы автоматизированных систем**
Б) организационно-правовое обеспечение
В) человеческий компонент

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания освоенных умений и приобретенных владений (табл. 1.1) проводится по каждому модулю в форме выполнения индивидуального задания.

Типовые примеры индивидуального задания (ИЗ)

1. Составьте алгоритм работы файлового вируса/макровируса/загрузочного вируса, опишите его структуру.

2. Опишите порядок действий пользователя при обнаружении заражения ПК.

3. Составьте рекомендации по практической реализации парольной системы, оценки стойкости этой системы и методы хранения паролей.

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

2.3. Выполнение комплексного индивидуального задания на самостоятельную работу

Индивидуальное задание является комплексным, охватывает все темы курса и представляет собой отчет о разработанном и проведенном студентом самостоятельном исследовании. Тема индивидуального задания формулируется по выбранному модулю изучаемой дисциплины самостоятельно студентом по согласованию с преподавателем дисциплины.

Примерные темы комплексного индивидуального задания (КИЗ)

1. Опишите структуру системы защиты от угроз нарушения доступности в организации, поясните основные составляющие.

2. Для промышленного предприятия опишите криптографические методы обеспечения целостности информации: реализацию механизма цифровой подписи, криптографические хэш-функции и преимущества, коды проверки подлинности.

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 положительная интегральная оценка по результатам текущего и рубежного контроля и выполнение комплексного индивидуального задания.

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.

2.4.2. Процедура промежуточной аттестации с проведением аттестационного испытания

В отдельных случаях (например, в случае переаттестации дисциплины) промежуточная аттестация в виде зачета по дисциплине может проводиться с проведением аттестационного испытания – выполнения и защиты комплексного индивидуального задания. Примерные темы задания приведены в п. 2.3.

Все учебно-методические материалы для изучения дисциплины (в т.ч. индивидуальные задания) размещены на учебном портале Гуманитарного факультета http://portal-hsb.pstu.ru/ и доступны студентам кафедры после регистрации.

2.4.2.1. 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

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.