ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДЕНА
приказ ректора
от «07» июня 2021 г. № 78

Б1.О.54 Методы и средства криптографической защиты информации

рабочая программа дисциплины

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – Безопасность открытых информационных систем
Квалификация выпускника – Специалист по защите информации
Форма обучения – очная
Нормативный срок обучения – 5 лет 6 мес.
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 5
Часов по учебному плану – 180

Формы промежуточной аттестации в семестрах:
экзамен 7, курсовая работа 7

Распределение часов дисциплины по семестрам

Семестр	7	**Итого**
Число недель в семестре	17	
Вид занятий	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий	**85**	**85**
– лекции	34	34
– практические (семинарские)	17	17
– лабораторные	34	34
Самостоятельная работа	**59**	**59**
Экзамен	**36**	**36**
Итого	**180**	**180**

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета), утвержденным Приказом Министерства образования и науки Российской Федерации от 26.11.2020 г. № 1457

Программу составил:
д.т.н., профессор кафедры «ИСиЗИ» Ю.М. Краковский

Рабочая программа дисциплины обсуждена и рекомендована к применению в образовательном процессе на заседании кафедры «Информационные системы и защита информации». Протокол от «04» 06 2021 г. № 11/2

И.о.зав. кафедрой, к.э.н, доцент Т.К. Кириллова

1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1 Цели освоения дисциплины	
1	формирование у обучающихся важнейших представлений о современных методах защиты информации; раскрытие сущности криптографической защиты информации, характеристика составляющих защиты информации; формирование компетенций в области моделей и методов защиты информации.
1.2 Задачи освоения дисциплины	
1	изучение теоретических основ и приобретение практических навыков по созданию и использованию современных средств криптографической защиты информации с учетом требований информационной безопасности;
2	освоить современные криптографические методы защиты информации, обеспечивающих целостность, конфиденциальность и доступность информации.

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

Цель воспитания обучающихся – разностороннее развитие личности будущего конкурентоспособного специалиста с высшим образованием, обладающего высокой культурой, интеллигентностью, социальной активностью, качествами гражданина-патриота.

Задачи воспитательной работы с обучающимися:

– развитие мировоззрения и актуализация системы базовых ценностей личности;

– приобщение студенчества к общечеловеческим нормам морали, национальным устоям и академическим традициям;

– воспитание уважения к закону, нормам коллективной жизни, развитие гражданской и социальной ответственности как важнейшей черты личности, проявляющейся в заботе о своей стране, сохранении человеческой цивилизации;

– воспитание положительного отношения к труду, развитие потребности к творческому труду, воспитание социально значимой целеустремленности и ответственности в деловых отношениях;

– обеспечение развития личности и ее социально-психологической поддержки, формирование личностных качеств, необходимых для эффективной профессиональной деятельности;

– выявление и поддержка талантливых обучающихся, формирование организаторских навыков, творческого потенциала, вовлечение обучающихся в процессы саморазвития и самореализации.

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
1	Б1.О.35 Основы информационной безопасности
2	Б1.0.51 Кибербезопасность
3	Б1.0.48 Теоретические основы компьютерной безопасности
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.0.24 Аттестация объектов информатизация
2	Б1.0.53 Теория и практика защиты информации в АСЖДТ
3	Б1.0.62 Моделирование процессов и систем защиты информации

3 ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности.	ОПК-9.1. **Знает** средства криптографической и технической защиты информации для решения задач профессиональной деятельности. ОПК-9.2. **Умеет** применять доверенное хранение, защиту	Знать: средства криптографической защиты информации, методы защиты электронного документооборота, методы защиты от несанкционированного доступа при обработке информации. Уметь: пользоваться методами криптографической защиты информации,

	каналов связи и электронного документооборота. ОПК-9.3. **Имеет** навыки работы с алгоритмами криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и для защиты информации от несанкционированного доступа при ее обработке и хранении	пользоваться национальными стандартами защиты электронного документооборота, объяснить особенности функционирования алгоритмов криптографического преобразования. Владеть: навыками пользования ЭП, навыками использования методов и средств КЗИ, навыками защиты информации от несанкционированного доступа.

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часы				*Код индикатора достижения компетенции
			Лек	Пр	Лаб	Срс	
	Раздел 1. Криптографические методы защиты информации на основе симметричных криптосистем	7					ОПК-10.1 ОПК-10.2 ОПК-10.3
1.1	Основные понятия криптографии. /Лек/	7	2				
1.2	Поточное шифрование /Лек/	7	2				
1.3	Блочные симметричные криптосистемы /Лек/	7	2				
1.4	Российский алгоритм криптографического преобразования /Лек/	7	2				
1.5	Национальный стандарт РФ по ГОСТ 34.13-2018 /Лек/		2				
1.6	Закрепление лекционного материала раздела 1 на практических занятиях /Пр/	7		5			
1.7	Проработка лекционного материала и подготовка к лабораторным занятиям раздела 1 /Ср/	7				19	
1.8	Лабораторные работы по разделу 1 /Лаб/				10		
	Раздел 2. Криптографические методы защиты информации на основе двухключевых криптосистем	7					ОПК-10.1 ОПК-10.2 ОПК-10.3
2.1	Определение двухключевых криптосистем /Лек/	7	2				
2.2	Обмен Диффи-Хеллмана /Лек/	7	2			4	
2.3	Двухключевые криптосистемы шифрования. Алгоритм RSA /Лек/	7	4				
2.4	Современные технологии шифрования /Лек/	7	2				
2.5	Закрепление лекционного материала раздела 2 на практических занятиях /Пр/	7		5			
2.6	Проработка лекционного материала и подготовка к лабораторным занятиям раздела 2 /Ср/	7				20	
2.7	Лабораторные работы по разделу 2 /Лаб/	7			10		
	Раздел 3. Криптографические методы защиты электронного документооборота	7					ОПК-10.1 ОПК-10.2 ОПК-10.3
3.1	Хеш-функция. Российский стандарт 2018 /Лек/	7					
3.2	Правовое обеспечение электронной подписи /Лек/	7	2				
3.3	Российские стандарты электронной подписи /Лек/	7	4				
3.4	Инфраструктура управления открытыми	7	2				

	ключами /Лек/						
3.5	Характеристика криптографических методов защиты в КриптоПро CSP /Лек/	7	2				
3.6	Характеристика зарубежных криптосистем /Лек/	7	2				
3.7	Технологии и методы аутентификации на основе криптографии /Лек/	7	2				
3.8	Закрепление лекционного материала раздела 3 на практических занятиях /Пр/	7		3			
3.9	Проработка лекционного материала и подготовка к лабораторным занятиям раздела 3 /Ср/	7				15	
3.10	Лабораторные работы по разделу 3 /Лаб/	7			14		
3.11	Проработка теоретической части курсовой работы /Ср/	7				2	
3.12	Разработка практической части курсовой работы /Ср/	7				3	
3.13	Защита курсовой работы /Пр/	7		4			
	Подготовка к промежуточной аттестации (Экзамен)	7	34	17	34	59 (36)	ОПК-10.1 ОПК-10.2 ОПК-10.3

* Код индикатора достижения компетенции проставляется или для всего раздела или для каждой темы или для каждого вида работы.

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по данной дисциплине оформляется в виде приложения № 1 к рабочей программе дисциплины и размещаются в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет.

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
6.1.1.1	Краковский Ю.М.	Информационная безопасность и защита информации	Иркутск: ИрГУПС, 2016	80
6.1.1.2	Корниенко А.А. и др.	Информационная безопасность и защита информации на ж-д. транспорте: учебное пособие.	УМЦ по образованию на ж.-д. трансп., 2014.	30

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
6.1.2.1	Бутин А.А.	Методы и средства защиты информации от несанкционированного доступа.	ИрГУПС, 2015.	43
6.1.2.2	Паршин К.А.	Оценка уровня информационной безопасности на объекте информатизации: учебное пособие для вузов ж.-д. транспорте.	УМЦ по образованию на ж.-д. трансп., 2015	19

6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)

	Авторы,	Заглавие	Издательство,	Кол-во экз.

	составители		год издания/ Личный кабинет обучающегося	в библиотеке/ 100% онлайн
6.1.3.1	Краковский Ю.М.	Информационная безопасность и защита информации: учебное пособие с методическими указаниями.	ИКЦ «Март», 2008	20
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»				
6.2.1	Березкин Е.Ф. Основы теории информации и кодирования : учебное пособие : http://biblioclub.ru/index.php?page=book&id=231898.			
6.3 Программное обеспечение и информационные справочные системы				
6.3.1 Базовое программное обеспечение				
6.3.1.1	OCMicrosoftWindows 7 Professional, количество – 100, лицензия № 49379844			
6.3.1.2	Офисный пакет MicrosoftOffice 2010, количество – 155, лицензия № 48288083; LibreOffice v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org			
6.3.2 Специализированное программное обеспечение				
6.3.2.1	Использование специализированного ПО не предусмотрено.			
6.3.3 Информационные справочные системы				
6.3.3.1	Использование информационных справочных систем не предусмотрено.			
6.4Правовые и нормативные документы				
6.4.1	Использование правовых и нормативных документов не предусмотрено.			

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л – по адресу г. Иркутск, ул. Лермонтова, д.80.
2	Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых проектов, работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа имеются учебно-наглядные пособия (презентации).
3	Учебные лаборатории Д-523 «Средства и методы защиты информации», Д-525 «Средства и методы защиты информации».
4	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507.
5	Помещение А-521 (для хранения и профилактического обслуживания учебного оборудования).

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки. Обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Уделить внимание следующим понятиям (перечисление понятий) и др.

Лабораторное занятие	Лабораторное занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют лабораторные задания. Лабораторные задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Лабораторные занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На лабораторных занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому лабораторному занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины. Особое внимание следует обращать на определение основных понятий дисциплины. Обучающийся должен подробно разбирать примеры, которые поясняют понятия
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить задание на самостоятельную работу и выучить лекционный материал к следующей теме. Систематическое выполнение заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины.
Курсовая работа	Изучение научной, учебной, нормативной и другой литературы. Отбор необходимого материала; формирование выводов и разработка конкретных рекомендаций по решению поставленной задачи; проведение практических исследований по заданной теме. Инструкция по выполнению требований к оформлению курсовой работы (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции).
Самостоятельная работа	Для эффективного освоения дисциплины изучение материала курса предполагает самостоятельную внеаудиторную работу, которая включает в себя выполнение индивидуальных заданий, подготовку к практическим занятиям, конспектирование. Для успешного выполнения домашних заданий следует обратиться к задачам, решенным на предыдущих практических занятиях, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделах основная и дополнительная литература. Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия или лектора по дисциплине.
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины, размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.	

Лист регистрации дополнений и изменений рабочей программы дисциплины

№ п/п	Часть текста, подлежавшего изменению в документе			Общее количество страниц		Основание для внесения изменения, № документа	Подпись отв. исп.	Дата
	№ раздела	№ пункта	№ подпункта	до внесения изменений	после внесения изменений			

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине Б1.О.54 Методы и средства криптографической защиты информации

Приложение № 1 к рабочей программе

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – Безопасность открытых информационных систем

ИРКУТСК

1. Общие положения

Фонд оценочных средств является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися образовательной программы.

Фонды оценочных средств (ФОС) предназначены для использования обучающимися, преподавателями, администрацией Университета, а также сторонними образовательными организациями для оценивания качества освоения образовательной программы и уровня сформированности компетенций у обучающихся.

В соответствии с требованиями действующего законодательства в сфере образования, оценочные средства представляются в виде ФОС для проведения промежуточной аттестации обучающихся по дисциплине. С учетом действующего в Университете Положения о формах, периодичности и порядке текущего контроля успеваемости и промежуточной аттестации обучающихся (высшее образование – бакалавриат, специалитет, магистратура), в состав ФОС для проведения промежуточной аттестации по дисциплине включаются оценочные средства для проведения текущего контроля успеваемости обучающихся.

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины.

– обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс;

– самоподготовка и самоконтроль обучающихся в процессе обучения.

Фонд оценочных средств сформирован на основе ключевых принципов оценивания: валидность, надежность, объективность, эффективность.

Для оценки уровня сформированности компетенций используется трехуровневая система:

– минимальный уровень освоения, обязательный для всех обучающихся по завершению освоения ОПОП; дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;

– базовый уровень освоения, превышение минимальных характеристик сформированности компетенций; позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;

– высокий уровень освоения, максимально возможная выраженность характеристик компетенций; предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.

2. Перечень компетенций с указанием этапов их формирования. Показатели оценивания компетенций, критерии оценки

Дисциплина «Методы и средства криптографической защиты информации» участвует в формировании компетенций:

ОПК-10.1: Знает средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

ОПК-10.2: Умеет применять доверенное хранение, защиту каналов связи и электронного документооборота.

ОПК-10.3: Имеет навыки работы с алгоритмами криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и для защиты информации от несанкционированного доступа при ее обработке и хранении.

Программа контрольно-оценочных мероприятий очная форма обучения

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятие/тема/раздел и т.д. дисциплины)	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
7 семестр					
1	1-5	Текущий контроль	Раздел 1. Криптографические методы защиты информации на основе симметричных криптосистем	ОПК-10.1 ОПК-10.2 ОПК-10.3	Рабочая тетрадь (письменно), Защита лабораторной работы (устно)
2	6-10	Текущий контроль	Раздел 2. Криптографические методы защиты информации на основе двухключевых криптосистем	ОПК-10.1 ОПК-10.2 ОПК-10.3	Рабочая тетрадь (письменно), Защита лабораторной работы (устно)
3	11-17	Текущий контроль	Раздел 3. Криптографические методы защиты электронного документооборота	ОПК-10.1 ОПК-10.2 ОПК-10.3	Рабочая тетрадь (письменно), Защита лабораторной работы (устно)
4	15-17	Текущий контроль	«Защита курсовой работы»	ОПК-10.1 ОПК-10.2 ОПК-10.3	Собеседование (устно)
5		Промежуточная аттестация – экзамен	Все разделы.	ОПК-10.1 ОПК-10.2 ОПК-10.3	Собеседование (устно)

*Форма проведения контрольно-оценочного мероприятия: устно, письменно.

Описание показателей и критериев оценивания компетенций на различных этапах их формирования. Описание шкал оценивания

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

Перечень оценочных средств, используемых для оценивания компетенций на различных этапах их формирования, а также краткая характеристика этих средств приведены в таблице.

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Собеседование	Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Может быть использовано для оценки знаний обучающихся	Вопросы по темам/разделам дисциплины
2	Рабочая тетрадь	Дидактический комплекс, предназначенный для самостоятельной работы обучающегося и позволяющий оценивать уровень усвоения им учебного материала. Может быть использовано для оценки умений обучающихся	Образец рабочей тетради
3	Защита лабораторной работы	Средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Темы лабораторных работ и требования к их защите
4	Курсовой проект (работа)	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся в предметной или межпредметной областях.	Темы типовых групповых и / или индивидуальных проектов и типовое задание на курсовой проект (работу)
5	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (билетов) к экзамену

Критерии и шкалы оценивания компетенций в результате изучения дисциплины/ прохождении практики при проведении промежуточной аттестации в форме зачета и/или экзамена. Шкала оценивания уровня освоения компетенций

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенции
«отлично»	«зачтено»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
«хорошо»		Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении	Базовый

		задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	
«удовлетворительно»		Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный
«неудовлетворительно»	«не зачтено»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенция не сформирована

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Защита лабораторной работы

Шкала оценивания	Критерии оценивания
«отлично»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет без замечаний. Лабораторная работа выполнена обучающимся в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; показал необходимые для проведения работы теоретические знания, практические умения и навыки. Работа (отчет) оформлена аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет с небольшими недочетами. Лабораторная работа выполнена обучающимся в полном объеме и самостоятельно. Допущены отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Работа показывает знание обучающимся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Допущены неточности и небрежность в оформлении результатов работы (отчета)
«удовлетворительно»	Лабораторная работа выполнена с задержкой, письменный отчет с недочетами. Лабораторная работа выполняется и оформляется обучающимся при посторонней помощи. На выполнение работы затрачивается много времени. Обучающийся показывает знания теоретического материала, но испытывает затруднение при самостоятельной работе с источниками знаний или приборами
«неудовлетворительно»	Лабораторная работа не выполнена, письменный отчет не представлен. Результаты, полученные обучающимся не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Показывается плохое знание теоретического материала и отсутствие необходимых умений. Лабораторная работа не выполнена, у учащегося отсутствуют необходимые для проведения работы теоретические знания, практические умения и навыки

Курсовой проект (работа)

Шкала оценивания	Критерии оценивания
«отлично»	Содержание курсового проекта (работы) полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсового проекта (работы) логически и методически выдержана. Все выводы и предложения убедительно аргументированы. Оформление курсового проекта (работы) и полученные результаты полностью отвечают требованиям, изложенным в методических указаниях. При защите курсового проекта (работы) обучающийся правильно и уверенно отвечает на вопросы преподавателя, демонстрирует глубокое знание теоретического материала, способен аргументировать собственные утверждения и выводы
«хорошо»	Содержание курсового проекта (работы) полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура

	курсового проекта (работы) логически и методически выдержана. Большинство выводов и предложений аргументировано. Оформление курсового проекта (работы) и полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две несущественные ошибки в использовании терминов, в построенных диаграммах и схемах. Наличествует незначительное количество грамматических и/или стилистических ошибок. Программа демонстрирует устойчивую работу на тестовых наборах исходных данных, подготовленных обучающимся, но обрабатывает не все исключительные ситуации. При защите курсового проекта (работы) обучающийся правильно и уверенно отвечает на большинство вопросов преподавателя, демонстрирует хорошее знание теоретического материала, но не всегда способен аргументировать собственные утверждения и выводы. При наводящих вопросах преподавателя исправляет ошибки в ответе
«удовлетворительно»	Содержание курсового проекта (работы) частично не соответствует заданию. Результаты обзора литературных и иных источников представлены недостаточно полно. Есть нарушения в логике изложения материала. Аргументация выводов и предложений слабая или отсутствует. Имеются одно-два существенных отклонений от требований в оформлении курсового проекта (работы). Полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две существенных ошибки в использовании терминов, в построенных диаграммах и схемах. Много грамматических и/или стилистических ошибок. Программа работает неустойчиво, не обрабатывает исключительные ситуации, тестовые наборы исходных данных не подготовлены. При защите курсового проекта (работы) обучающийся допускает грубые ошибки при ответах на вопросы преподавателя и /или не дал ответ более чем на 30% вопросов, демонстрирует слабое знание теоретического материала, в большинстве случаев не способен уверенно аргументировать собственные утверждения и выводы
«неудовлетворительно»	Содержание курсового проекта (работы) в целом не соответствует заданию. Имеются более двух существенных отклонений от требований в оформлении курсового проекта (работы). Большое количество существенных ошибок по сути работы, много грамматических и стилистических ошибок и др. Полученные результаты не отвечают требованиям, изложенным в методических указаниях. Программа не разработана и/или находится в нерабочем состоянии. При защите курсового проекта (работы) обучающийся демонстрирует слабое понимание программного материала. Курсовой проект (работа) не представлена преподавателю. Обучающийся не явился на защиту курсового проекта (работы)

Рабочая тетрадь

Шкала оценивания	Критерии оценивания
«отлично»	Обучающийся полно и грамотно дает ответы на поставленные вопросы, аргументировано поясняет схемы, алгоритмы, умеет выделять главное, обобщать, делать выводы, устанавливать межпредметные связи; отсутствуют ошибки и недочеты при воспроизведении изученного материала
«хорошо»	Обучающийся знает весь изученный программный материал, но в ответе на вопросы допускает недочеты, незначительные (негрубые) ошибки, применяет полученные знания на практике, испытывает затруднения при самостоятельном воспроизведении
«удовлетворительно»	Обучающийся при ответе допускает существенные недочеты (не менее 60% правильных ответов от общего числа), знает материал на уровне минимальных требований программы, затрудняется при ответах на видоизмененные вопросы
«неудовлетворительно»	Обучающийся показывает знание и усвоение материала на уровне ниже минимальных требований программы, дает ответы с существенными недочетами (менее 60% правильных ответов от общего числа), отсутствуют умения работать на уровне воспроизведения, допускает затруднения при ответах на стандартные вопросы

Защита лабораторной работы

Шкала оценивания	Критерии оценивания
«отлично»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет без замечаний. Лабораторная работа выполнена обучающимся в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью

	самостоятельно; показал необходимые для проведения работы теоретические знания, практические умения и навыки. Работа (отчет) оформлена аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет с небольшими недочетами. Лабораторная работа выполнена обучающимся в полном объеме и самостоятельно. Допущены отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Работа показывает знание обучающимся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Допущены неточности и небрежность в оформлении результатов работы (отчета)
«удовлетворительно»	Лабораторная работа выполнена с задержкой, письменный отчет с недочетами. Лабораторная работа выполняется и оформляется обучающимся при посторонней помощи. На выполнение работы затрачивается много времени. Обучающийся показывает знания теоретического материала, но испытывает затруднение при самостоятельной работе с источниками знаний или приборами
«неудовлетворительно»	Лабораторная работа не выполнена, письменный отчет не представлен. Результаты, полученные обучающимся не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Показывается плохое знание теоретического материала и отсутствие необходимых умений. Лабораторная работа не выполнена, у учащегося отсутствуют необходимые для проведения работы теоретические знания, практические умения и навыки

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.1 Перечень типовых тем курсовых работ

1. Процесс симметричного шифрования.
2. Поточные системы симметричного шифрования.
3. Создание поточного ключа.
4. Схема Фейстеля.
5. Системы контроля и управления доступом.
6. Целостность информации и ее контроль.
7. Стандарт криптографической.
8. Алгоритм DES и ее развитие.
9. Канал утечки видеоизображения за счет ПЭМИН.
10. Обмен Диффи-Хеллмана.
11. Двухключевые системы шифрования.
12. Блочные шифры.
13. Технологии измерения ПЭМИН.
14. Характеристика ГОСТ 28147-89.
15. Характеристика ГОСТ 34.12-2018.
16. Характеристика ГОСТ 34.13-2018.
17. Сравнение симметричных и асимметричных криптосистем.
18. Хэш-функция по ГОСТ Р 34.11-94.
19. Хэш-функция по ГОСТ 34.11-2018.
20. Характеристика зарубежных хэш-функций.
21. Виды ЭП, простая ЭП.
22. ЭП по ГОСТ 34.10-2018.
23. ЭП по ГОСТ 34.10-2018.

24. Криптосистемы США для ЭП.
25.Инфраструктура управления открытыми ключами.

3.2 Перечень теоретических вопросов к экзамену

(для оценки знаний)

1. Аспекты безопасности информации.
2. Основные понятия криптографии.
3. Классификация криптосистем.
4. Общая схема шифрования.
5. Способы формирования ключей для поточного шифрования.
6. Вопросы по поточному шифрованию.
7. Что такое угроза и уязвимость.
8. Конфиденциальность информации и методы ее защиты.
9. Стандарт криптографической защиты AES.
10. Российский алгоритм криптографического преобразования: режимы шифрования.
11. Российский алгоритм криптографического преобразования: режим имитовставки.
12. Несимметричные системы шифрования. Современный протокол шифрования данных.
13. Алгоритм RSA. Сравнение симметричных и несимметричных криптосистем.
14. Определение и назначение хэш-функции, российский стандарт.
15. Электронная подпись: определения, назначение, роль в электронном документообороте.
16. Российский стандарт ЭП: технология создания и проверки.
17. Обмен Диффи-Хеллмана. Назначение мастер-ключа.

3.3 Перечень типовых простых практических заданий к экзамену

(для оценки умений)

1) Размер хэш-образа по российскому стандарту (ГОСТ-2012) равен:

А) 256 бит или 512 бит

Б) 512 бит или 160 бит

В) 160 бит

Г) 320 бит

2) Современный протокол шифрования данных базируется на совместном применении как симметричной криптосистемы так и несимметричной:

А) ДА

Б) НЕТ

3) Хэш-функция – это криптографическое преобразование информации, переводящее строку битов произвольной длины в строку битов фиксированной длины:

А) ДА

Б) НЕТ

4) В электронном документообороте наилучшим способом контроля целостности данных является:

А) шифрование

Б) электронная цифровая подпись

В) хэширование

5) Увеличение длины ЭЦП в 2 раза по сравнению с хэш-образом это свойство ЭЦП:

А) ДА

Б) НЕТ

3.4 Перечень типовых практических заданий к экзамену

(для оценки навыков и (или) опыта деятельности)

6) При шифровании данных несимметричной криптосистемой, используется:

А) секретный ключ

Б) открытый ключ

В) сначала открытый, а затем секретный ключ

Г) сначала секретный, а затем открытый ключ

7) При создании ЭЦП секретный ключ по длине больше, чем открытый:

А) ДА

Б) НЕТ

8) В современном протоколе шифрования данных при шифровании сообщений используется двухключевая криптосистема:

А) ДА

Б) НЕТ

9) Размер ЭЦП по американскому стандарту *DSS* равен:

А) 256 бит

Б) 512 бит

В) 1024 бит

Г) 320 бит

10) В электронном документообороте наилучшим способом обеспечения конфиденциальности данных является:

А) шифрование

Б) электронная цифровая подпись

В) хэширование

11) Укажите одностороннюю функцию для алгоритма Эль-Гамаля:

А) $(e \cdot d) \bmod k = 1;\ k=p \cdot (q-1);$

Б) $y = a^x \bmod p;$

В) $n = p \cdot q;$

Г) $c = m^e \bmod (n-1);$

12) Двухключевую криптосистему называют криптосистемой с открытым ключом, т.к. при шифровании открытый ключ создает отправитель, а секретный – получатель:

А) ДА

Б) НЕТ

13) Пару ключей при шифровании данных криптосистемой с открытым ключом создает отправитель:

А) ДА

Б) НЕТ

14) Владельцем пары ключей при создании ЭЦП является отправитель:

А) ДА
Б) НЕТ

15) Хэширование сообщения при создании ЭЦП осуществляется, чтобы:
А) обеспечить конфиденциальность информации
Б) увеличить время создания ЭЦП
В) стандартизовать время создания ЭЦП и ее размер

16) Хэш-функция может применяться в следующих случаях:
А) для создания сжатого образа сообщения, используемого в механизме цифровой подписи;
Б) для защиты пароля;
В) при контроле целостности данных;
Г) для сохранения конфиденциальности информации.

17) Коллизия в хэш-функции, это когда разные сообщения имеют одинаковый хэш-образ:
А) ДА
Б) НЕТ

18) В современном протоколе шифрования данных для шифрования секретного ключа симмерично криптосистемы используется двухключевая криптосистема:
А) ДА
Б) НЕТ

19) Двухключевая криптосистема может применяться в следующих случаях:
А) для шифрования небольших по объему данных;
Б) при создании электронно-цифровой подписи;
В) в задачах аутентификации;
Г) для обеспечения доступности информации.

3.5 Рабочая тетрадь

Темы лекций:
Конспект по теме «Российский алгоритм криптографического преобразования».
Конспект по теме «Двухключевые криптосистемы шифрования. Алгоритм RSA».
Конспект по теме «Российские стандарты электронной подписи».
Конспект по теме «Характеристика зарубежных криптосистем».

3.6 Защита лабораторных работ

Темы лабораторных работ:
1 Лабораторная работа № 1 «Контроль целостности информации при случайных воздействиях».
2 Лабораторная работа № 2 «Поточное шифрование».
3 Лабораторная работа № 3 «Генерирование секретных ключей для симметричной криптосистемы».
4 Лабораторная работа №4 «Обмен Диффи-Хеллмана».
5 Лабораторная работа № 5 «Шифрование сообщений криптосистемой RSA».
6 Лабораторная работа № 6 «Технология электронной подписи».
7 Лабораторная работа № 7 «Методика определения информационных рисков».
8 Лабораторная работа № 8 «Взаимная аутентификация субъектов на основе ЭП».

3.7 Фонд тестовых заданий по дисциплине «Методы и средства криптографической защиты информации»

Раздел 1. Криптографические методы защиты информации на основе симметричных криптосистем

1. В симметричной криптосистеме используется:
   а) два секретных ключа;
   б) два ключа, один закрытый, другой открытый;
   в) один секретный ключ.
2. Дополнить. По технологии шифрования симметричные криптосистемы делятся на:
   ……

3. Добавить. В российском алгоритме криптографического преобразования (ГОСТ-89) используется ___ режимов.
4. Перечислить режимы в российском алгоритме криптографического преобразования (ГОСТ-89). Самим развернуть.
5. При поточном шифровании используется операция:
   а) сложение по модулю 2;
   б) сложение по модулю 2^n;
   в) циклическое сложение.
6. При блочном симметричном шифровании сообщение разбивается на числовые блоки:
   А) ДА
   Б) НЕТ
7. Поточные криптосистемы отличаются технологией создания поточного ключа (гаммы):
   А) ДА
   Б) НЕТ
8. Выполните операцию сложения по модулю 2 двух слов, заданных в шестнадцатеричной системе счисления:

   C4A7(+)BCA8
9. Выполните операцию сложения по модулю 2 двух слов, заданных в шестнадцатеричной системе счисления:

   CA95(+)ACB3
10. Найдите контрольную сумму, используя операцию сложения по модулю 2 двух слов, заданных в шестнадцатеричной системе счисления:

    DA9F(+)AFE4
11. Найдите контрольную сумму, используя операцию сложения по модулю 2^{16} двух слов, заданных в шестнадцатеричной системе счисления:

    DA9F I+I AFE4
12. Найдите контрольную сумму, используя операцию сложения по модулю 2 двух слов, заданных в шестнадцатеричной системе счисления:

    CA9F(+)DCB9

Раздел 2. Криптографические методы защиты информации на основе двухключевых криптосистем

13. Укажите двухключевую криптосистему:
    А) DES
    Б) RSA
    В) AES
    Г) ГОСТ 28147-89

14. Укажите одностороннюю функцию для алгоритма *RSA*:
А) $(e \cdot d) \bmod k = 1; k=p \cdot (q-1)$;
Б) $y = a^x \bmod p$;
В) $n = p \cdot q$;
Г) $c = m^e \bmod (n-1)$.
15. При зашифровании данных несимметричной криптосистемой, используется:
А) секретный ключ
Б) открытый ключ
В) сначала открытый, а затем секретный ключ
Г) сначала секретный, а затем открытый ключ
16. Двухключевая криптосистема по сравнению с одноключевой имеет более высокую производительность при шифровании данных:
А) ДА
Б) НЕТ
17. Современный протокол шифрования данных базируется на совместном применении как симметричной криптосистемы так и несимметричной:
А) ДА
Б) НЕТ
18. Алгоритм RSA это блочная симметричная криптосистема шифрования:
А) ДА
Б) НЕТ
19. Протокол Диффи-Хеллмана заключается в обмене закрытыми ключами:
А) ДА
Б) НЕТ
20. Назначение протокола Диффи-Хеллмана заключается в шифровании сообщений:
А) ДА
Б) НЕТ
21. При использовании двухключевых криптосистем шифрования владельцем ключей является отправитель:
А) ДА
Б) НЕТ
22. При использовании двухключевых криптосистем шифрования зашифрование осуществляется закрытым ключом:
А) ДА
Б) НЕТ
23. При использовании двухключевых криптосистем шифрования расшифрование осуществляется закрытым ключом:
А) ДА
Б) НЕТ
24. При использовании двухключевых криптосистем шифрования зашифрование осуществляется открытым ключом:
А) ДА
Б) НЕТ
25. При использовании двухключевых криптосистем шифрования расшифрование осуществляется открытым ключом:
А) ДА
Б) НЕТ
26. Выберите наиболее эффективную криптосистему для шифрования незначительных по объему данных:
А) RSA
Б) AES
В) DES

Г) ГОСТ 28147-89

Раздел 3. Криптографические методы защиты электронного документооборота

27. Размер ЭЦП по российскому стандарту (ГОСТ-2012) равен:
    А) 256 бит 512 бит
    Б) 512 бит или 1024 бит
    В) 1024 бит
    Г) 320 бит
28. Хэш-функция может применяться в следующих случаях:
    А) для создания сжатого образа сообщения, используемого в механизме цифровой подписи;
    Б) для защиты пароля;
    В) при контроле целостности данных;
    Г) для сохранения конфиденциальности информации.
29. Размер хэш-образа по американскому стандарту *SHA*-1 равен:
    А) 256 бит
    Б) 512 бит
    В) 160 бит
    Г) 320 бит
30. Коллизия в хэш-функции, это когда разные сообщения имеют одинаковый хэш-образ:
    А) ДА
    Б) НЕТ
31. В электронном документообороте наилучшим способом обеспечения конфиденциальности данных является:
    А) шифрование
    Б) электронная цифровая подпись
    В) хэширование
32. Владельцем пары ключей при создании ЭЦП является отправитель:
    А) ДА
    Б) НЕТ
33. Хэширование сообщения при создании ЭЦП осуществляется, чтобы:
    А) обеспечить конфиденциальность информации
    Б) увеличить время создания ЭЦП
    В) стандартизовать время создания ЭЦП и ее размер
34. Какая технология более предпочтительна при контроле целостности при преднамеренных воздействиях:
    А) Технология электронной подписи
    Б) Режим имитовставки (имитозащиты)
35. Дополнить. На чем основаны методы строгой аутентификации: самим дополнить.
36. Используется ли при двухфакторной аутентификации пароль?
    А) ДА
    Б) НЕТ.

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

В таблице приведены описания процедур проведения контрольно-оценочных мероприятий и процедур оценивания результатов обучения с помощью оценочных средств в соответствии с рабочей программой дисциплины.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Собеседование	Преподаватель оценивает выполненное практическое занятие обучающимися в конце данного занятия. Он сразу же информирует обучающихся о результатах оценки занятия после проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения. Если обучающийся не выполнил критерии контрольно-оценочного мероприятия, то ему преподаватель назначает время для устранения задолженности
Рабочая тетрадь	Преподаватель оценивает ведение конспекта обучающимися после каждой пройденной темы раздела дисциплины на последнем запланированном практическом занятии или лабораторной работе в соответствии с расписанием занятий. Он сразу же информирует обучающегося о результатах ведения конспекта после проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения. В случаях, когда тема дисциплины не предполагает кроме лекций других видов занятий, то преподаватель проводит контрольно-оценочные мероприятия и процедуры оценивания результатов обучения вначале практического занятия или лабораторной работы следующей темы дисциплины
Защита лабораторной работы	Преподаватель оценивает выполненную лабораторную работу обучающимися в конце данного занятия. Он сразу же информирует обучающегося о результатах оценки работы после проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения. Если обучающийся не выполнил критерии контрольно-оценочного мероприятия, то преподаватель назначает ему время для устранения задолженности
Курсовой проект (работа)	Обучаемый самостоятельно, под руководством преподавателя выполняет курсовую работу на заданную тему. Тема предлагается в общем виде. Обучаемый подбирает литературу по теме, не менее 3-4 источников, включая самостоятельный поиск в интернет (обязательно), разрабатывает ее, готовит пояснительную записку, предоставляет ее преподавателю, отвечает на его вопросы в ходе собеседования. Оценка ставится по представленным результатам и результатам собеседования. Преподаватель информирует обучающихся о результатах проверки работы на следующем занятии после проведения контрольно-оценочного мероприятия (или указание другого срока информирования); оцененные/проверенные работы преподаватель возвращает обучающимся.

Для организации и проведения промежуточной аттестации (в форме зачета) составляются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы:

– перечень теоретических вопросов к зачету для оценки знаний;

– перечень типовых простых практических заданий к зачету для оценки умений;

– перечень типовых практических заданий к зачету для оценки навыков и (или) опыта деятельности.

Перечень теоретических вопросов и перечни типовых практических заданий разного уровня сложности к зачету обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

Описание процедур проведения промежуточной аттестации в форме экзамена и оценивания результатов обучения

При проведении промежуточной аттестации в форме экзамена преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра. Оценочные средства и типовые контрольные задания, используемые при текущем контроле, позволяют оценить знания, умения и владения навыками/опытом деятельности обучающихся при освоении дисциплины. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок).

Шкала и критерии оценивания уровня сформированности компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета по результатам текущего контроля (без дополнительного аттестационного испытания)

Средняя оценка уровня сформированности компетенций по результатам текущего контроля	Оценка
Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю	«зачтено»
Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю	«не зачтено»

Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета без дополнительного аттестационного испытания, то промежуточная аттестация в форме зачета проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач (не более двух теоретических и двух практических). Промежуточная аттестация в форме зачета с проведением аттестационного испытания в форме собеседования проходит на последнем занятии по дисциплине.