ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

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

Б1.О.51 Кибербезопасность

рабочая программа дисциплины

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

Общая трудоемкость в з.е. – 4
Часов по учебному плану (УП) – 144

Формы промежуточной аттестации в семестрах
зачет 6 семестр

Распределение часов дисциплины по семестрам

Семестр	6	**Итого**
Число недель в семестре	17	
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	**85**	**85**
– лекции	34	34
– практические (семинарские)	51	51
– лабораторные	–	–
Самостоятельная работа	**59**	**59**
Зачет	–	–
Итого	**144**	**144**

* В форме ПП – в форме практической подготовки.

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:
к.э.н. доцент, и. о. зав кафедры «ИСиЗИ» Т. К. Кириллова

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «04» 06 2021 г. № 11/2

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

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цели дисциплины	
1	формирование общих представлений о безопасности в информационном обществе;
2	сформировать понимание технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах деятельности.
1.2 Задачи дисциплины	
1	формирование общих представления о безопасности в информационном обществе;
2	описать общие принципы технологий, применяемых в информационной безопасности;
3	привить умения применять правила кибербезопасности во всех сферах деятельности;
4	освоение знаний, составляющих начала представлений об информационной картине мира и информационных процессах;
5	развитие навыков ориентирования в информационных потоках.

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	
Б1.О.33 Основы информационной безопасности (межпредметные связи)	
Б1.О.30 Безопасность операционных систем (межпредметные связи)	
Б1.О.48 Теоретические основы компьютерной безопасности (межпредметные связи)	
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.О.24 Аттестация объектов информатизации
2	Б1.О.57 Методы принятия организационно-технических решений
3	Б1.О.38 Организационное и правовое обеспечение информационной безопасности
4	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
5	Б3.02(Д) Защита выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ		
Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения**
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ОПК-1.3 Оценивает роль, сущность и значение информационной безопасности для обеспечения объективных потребностей	**Знать:** – объекты компьютерных технологий, используемые в обеспечении кибербезопасности; – понятийный аппарат информационных технологий и особенности терминологии кибербезопасности; – нормативно-правовые акты,

	личности, общества и государства	нормативные и методические документы, регламентирующие деятельность по защите информации; **Уметь:** – анализировать угрозы, уязвимости, риски в области безопасности информации; – применять знания о нормативных и методических документов, регламентирующие деятельность по защите информации в решении поставленных задач; – применять знания по информационной безопасности в современном обществе; **Владеть:** – знаниями о современных технологиях, применяемых в области кибербезопасности; – навыками составления документов с учетом требований нормативно-правовой документации – навыками оформления документов по организации защиты информации
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;	ОПК-9.1. Проводит анализ профессиональной деятельности для решения задач защиты информации, сетей и систем передачи данных ОПК-9.2 Знает основные информационные технологии, используемые в автоматизированных системах, их состояние и тенденции развития ОПК-9.3 Знает текущее состояние и тенденции развития сетей и систем передачи информации	**Знать:** – основные термины и понятия защиты информации, сетей и систем передачи данных; – особенности информационные технологии, используемые в автоматизированных системах; – тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации. **Уметь:** – ставить цели, формулировать задачи, связанные с обеспечением кибербезопасности; – анализировать тенденции развития систем обеспечения кибербезопасности; – применять знания о сетях и систем передачи информации при решении поставленных задач. **Владеть:** –методами проведения анализа профессиональной деятельности для решения задач защиты информации, сетей и систем передачи данных; –навыками работы с информационными технологиями, используемыми в автоматизированных системах; - алгоритмами обработки информации, в сфере информационной безопасности.

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работы	Семестр	Часы				*Код индикатора достижения компетенции
			Лек	Пр	Лаб	СР	
1.0	**Раздел 1. Основные составляющие кибербезопасности**	6					ОПК-1.3 ОПК-9.1 ОПК-9.2
1.1	Введение в проблему кибербезопасности		2	2			ОПК-1.3 ОПК-9.1
1.2	Основы правового регулирования защиты информации		2	4		8	ОПК-1.3
1.3	Общие сведения о безопасности ПК и интернета, проблема интернет-зависимости.		2	6		6	ОПК-9.1 ОПК-9.2
1.4	Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы		2	4		4	ОПК-9.1 ОПК-9.2
1.5	Сведения о безопасности ПК и интернета		2	4		4	ОПК-9.1 ОПК-9.2
1.6	Теоретические основы и практические аспекты защиты киберпространства		2	4		4	ОПК-1.3 ОПК-9.1
1.7	Мошеннические действия в интернете, киберпреступления против личности, общества и государства, хакерские атаки и кибертерроризм		4	4		4	ОПК-1.3 ОПК-9.1 ОПК-9.2
2.0	**Раздел 2. Современные технологии, в области кибербезопасности и государственная политика**	6					ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3
2.1	Организация и проведение работ по технической защите информации в компьютерных сетях и системах		2	2		6	ОПК-1.3 ОПК-9.1
2.2	Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации		2	4		4	ОПК-9.1 ОПК-9.2 ОПК-9.3
2.3	Техническая защита информации в компьютерных сетях и системах /		2	2		4	ОПК-1.3 ОПК-9.1
2.4	Государственная политика в области кибербезопасности и государственный аудит.		4	4		4	ОПК-1.3
2.5	Законодательства в области защиты информации		4	6		6	ОПК-1.3
2.6	Сохранность и конфиденциальность данных		4	5		5	ОПК-1.3 ОПК-9.1
3.0	**Зачет**	6					ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3
3.1	Зачёт						ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3

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 дисциплине: оформлен в виде приложения № 1 к рабочей программе дисциплины и размещен 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
Л1.1	Диогенес, Ю.	Кибербезопасность. стратегия атак и обороны; перевод с английского Д. А. Беликова. [Электронный ресурс] .https://e.lanbook.com/book/131717	Москва: ДМК Пресс, 2020	100 % онлайн
Л1.2	Белоус, А. И.	Кибероружие и кибербезопасность. О сложных вещах простыми словами / [Электронный ресурс] https://e.lanbook.com/book/148383	Вологда : Инфра-Инженерия, 2020.	100 % онлайн
Л1.3	Белоус, А. И.	Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения : энциклопедия [Электронный ресурс] https://e.lanbook.com/book/181222	Москва : Техносфера, 2021	100 % онлайн
6.1.2 Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/100 % онлайн
Л2.1	Ники Белоус, А. И.	Программные и аппаратные трояны — способы внедрения и методы противодействия. Первая техническая энциклопедия : в 2 книгах [Электронный ресурс]: https://e.lanbook.com/book/140565	Москва : Техносфера, 2019	100 % онлайн
Л2.2	Булычев, Г. Г.	Программно-аппаратные средства обеспечения информационной безопасности : методические рекомендации [Электронный ресурс]: https://e.lanbook.com/book/163932	Москва : РТУ МИРЭА, 2020 — Часть 1 — 2020.	100 % онлайн
Л2.3	Казарин, О. В.	Надежность и безопасность программного обеспечения : учебное пособие для вузов / [Электронный ресурс] — https://urait.ru/bcode/493262	Юрайт, 2022.	100 % онлайн
6.1.3 Методические разработки				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/100 % онлайн
Л3.1	Н.И. Глухов	Оценка информационных рисков предприятия, учебное пособие.	Иркутск: ИрГУПС, 2013.	67
6.1.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/100 % онлайн
Л4. 1	Булычев, Г. Г..	Программно-аппаратные средства обеспечения информационной безопасности : методические указания [Электронный ресурс] — :https://e.lanbook.com/book/163812	Москва : РТУ МИРЭА, 2020	100 % онлайн

6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»	
6.2.1	Электронная библиотека Университета (http://www.irgups.ru/htb/)
6.2..2	Электронно-библиотечная система «Университетская библиотека онлайн» (http://www.biblioclub.ru);
6.2.3	Электронно-библиотечная система издательства «Лань» (http://www.e.lanbook.com);
6.3 Программное обеспечение и информационные справочные системы	
6.3.1 Базовое программное обеспечение	
6.3.1.1	ОС Microsoft Windows 7 Professional, количество – 100, лицензия № 49379844, обновление - Контракт № 0334100010016000113-0000756-02 от 25.11.2016г., обновление - договор №31705062861

	от 06.06.2017 АО СофтЛайнТрейд, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд
6.3.1.2	Офисный пакет Microsoft Office 2010, количество – 155, Лицензия № 48288083, обновление - Контракт № 0334100010016000113-0000756-02 от 25.11.2016г., обновление - договор №31705062861 от 06.06.2017 АО СофтЛайнТрейд, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд; LibreOffice v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org
6.3.2 Специализированное программное обеспечение	
6.3.2.1	СЗИ НСД Dallas Lock (свободное ПО для вузов);
6.3.2.2	Пакет PrZamena (свободное ПО);
6.3.2.3	Dr.Web Cureit! (свободное ПО);
6.3.2.4	360 Total Security (свободное ПО).
6.3.3 Информационные справочные системы	
6.3.3.1	КонсультантПлюс – студенческая версия (Онлайн–версия КонсультантПлюс: Студент, https://student2.consultant.ru/cgi/online.cgi?req=home;rnd=0.8160556428138959)
6.4Правовые и нормативные документы	
6.4.1	Федеральный закон от 27 июля 2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».
6.4.2	Федеральный закон от 26 июня 2017г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
6.4.3	Федеральный закон от 27.07.2006 N 152-ФЗ"О персональных данных"
6.4.4	Федеральный закон от 04 мая 2011г. №99-ФЗ «О лицензировании отдельных видов деятельности».
6.4.5	Федеральный закон от 29 июня 2015г. №162-ФЗ «О стандартизации отдельных видов деятельности».
6.4.6	Перечень сведений, отнесенных к государственной тайне. Утвержден указом Президента Российской Федерации от 30 ноября 1995г. №1203.

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ УЧЕБНОГО 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, плакаты, таблицы), обеспечивающие тематические иллюстрации содержания дисциплины:Д-518,521,623,Д-216.
3	Помещения для самостоятельной работы обучающихся: – Читальный зал А-606. Учебная мебель, стеллажи, витрина, компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета, мультимедийный проектор, экран. – Аудитория Д-523,508,514. Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета, мультимедийный проектор, экран.
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.

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.
Практическое занятие	Обсуждение лекционного материала и материала, выносимого на самостоятельное изучение, закрепление изученного материала при помощи выполнения различных практических заданий.
Самостоятельная работа	Самостоятельная работа обучающихся проводится в целях закрепления и систематизации теоретических знаний, а также формирования практических навыков по их применению при решении прикладных задач в выбранной предметной области. Она включает проработку лекционного материала, самоподготовку обучающихся к практическим занятиям, выполнение практических задач, самостоятельное изучение тем, выходящих за рамки лекционного курса.
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.51 Кибербезопасность

Приложение № 1 к рабочей программе

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – N 5 «Безопасность открытых информационных систем»

ИРКУТСК

1. Общие положения

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

Фонд оценочных средств предназначен для использования обучающимися, преподавателями, администрацией Университета, а так же сторонними образовательными организациями для оценивания качества освоения образовательной программы и уровня сформированности компетенций у обучающихся.

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины «Документоведение»;

– 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 образовательной программы; 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, в формировании которых участвует дисциплина.
Программа контрольно-оценочных мероприятий.
Показатели оценивания компетенций, критерии оценки

Дисциплина «Кибербезопасность» участвует в формировании компетенций:

ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации.

Программа контрольно-оценочных мероприятий очная форма обучения

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятие/тем/раздел и т.д. дисциплины)	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
_6_ семестр					
1	1-3	Текущий контроль	Тема Введение в проблему кибербезопасности	ОПК-1.3 ОПК-9.1	Собеседование (устно)
2	4-6	Текущий контроль	Тема Общие сведения о безопасности ПК и интернета, проблема интернет-зависимости	ОПК-1.3	Сообщение (устно) Диктант (письменно)
3	7-9	Текущий контроль	Тема Теоретические основы и практические аспекты защиты киберпространства	ОПК-9.1 ОПК-9.2	Сообщение (устно) Творческое задание (устно)
4	10-13	Текущий контроль	Тема Организация и проведение работ по технической защите информации в компьютерных сетях и системах (лекция в форме ПП)	ОПК-9.1 ОПК-9.2	Собеседование (устно) Сообщение (устно) Ситуационная задача (письменно)
5	14-15	Текущий контроль	Тема Государственная политика в области кибербезопасности и государственный аудит	ОПК-1.3	Собеседование (устно)
6	17	Текущий контроль	Тема Информационное противоборство в бизнесе, обеспечение сохранности и конфиденциальности данных	ОПК-1.3 ОПК-9.1	Сообщение (устно) Ситуационная задача (письменно)

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

Описание показателей и критериев оценивания компетенций. Описание шкал оценивания

Контроль качества освоения дисциплины/прохождения практики 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.

Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и/или двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций, а также краткая характеристика этих средств приведены в таблице

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Терминологический диктант	Средство проверки степени овладения категориальным аппаратом темы, раздела, дисциплины. Может быть использовано для оценки знаний обучающихся	Перечень понятий по темам дисциплины
2	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	Вопросы по темам/разделам дисциплины

		т.п. Может быть использовано для оценки знаний обучающихся	
3	Сообщение, доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов, сообщений
4	Зачет	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 зачету

Критерии и шкалы оценивания компетенций в результате изучения дисциплины «Кибербезопасность» при проведении промежуточной аттестации в форме зачета. 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 задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
«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

Терминологический диктант

Пять терминов, за каждый правильный ответ один балл. Перевод в четырехбалльную систему происходит следующим образом:

Число набранных баллов	Оценка
5 баллов	«отлично»
4 балла	«хорошо»
3 балла	«удовлетворительно»
меньше трех баллов	«неудовлетворительно»

Собеседование

Шкала оценивания	Критерии оценивания
«отлично»	Глубокое и прочное усвоение программного материала. Полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания. Обучающийся свободно справляется с поставленными задачами, может обосновать принятые решения, демонстрирует владение разносторонними навыками и приемами выполнения практических работ
«хорошо»	Знание программного материала, грамотное изложение, без существенных неточностей в ответе на вопрос, правильное применение теоретических знаний, владение необходимыми навыками при выполнении практических задач
«удовлетворительно»	Обучающийся демонстрирует усвоение основного материала, при ответе допускаются неточности, при ответе недостаточно правильные формулировки, нарушение последовательности в изложении программного материала, затруднения в выполнении практических заданий Слабое знание программного материала, при ответе возникают ошибки, затруднения при выполнении практических работ
«неудовлетворительно»	Не было попытки выполнить задание

Доклад, сообщение

Шкала оценивания	Критерии оценивания
«отлично»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint,Flash–презентация, видео-презентация и др.) Использованы дополнительные источники информации. Содержание заданной темы раскрыто в полном объеме. Отражена структура доклада (вступление, основная часть, заключение, присутствуют выводы и примеры). Оформление работы. Оригинальность выполнения (работа сделана самостоятельно, представлена впервые)
«хорошо»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint,Flash–презентация, видео-презентация и др.) Содержание доклада включает в себя информацию из основных источников (методическое пособие), дополнительные источники информации не использовались. Содержание заданной темы раскрыто не в полном объеме. Структура доклада сохранена (вступление, основная часть, заключение, присутствуют выводы и примеры)
«удовлетворительно»	Доклад сделан устно, без использования компьютерных технологий. Содержание доклада ограничено информацией только из методического пособия. Содержание заданной темы раскрыто не в полном объеме. Отсутствуют выводы и примеры. Оригинальность выполнения низкая
«неудовлетворительно»	Доклад сделан устно, без использования компьютерных технологий и других наглядных материалов. Содержание ограничено информацией только из методического пособия. Заданная тема доклада не раскрыта, основная мысль сообщения не передана

Оценочное средство «Тест».

Тестирование с применением компьютерных технологий проводится по окончанию изучения дисциплины и (или) в течение года по завершению изучения дисциплины (контроль/проверка остаточных знаний, умений, навыков и (или) опыта деятельности).

Тесты формируются из фонда тестовых заданий по дисциплине. Структура фонда тестовых заданий по дисциплине, структуры тестов по итогам итогового теста по дисциплине и типовые примеры тестов приведены в разделе 3 данного документа.

Результаты тестирования могут быть использованы при проведении промежуточной аттестации в форме зачета.

Промежуточная аттестация в форме зачета:

Критерии оценивания	Шкала оценивания
Обучающийся набрал при тестировании более 69 баллов	«зачтено»
Обучающийся набрал при тестировании менее 69 баллов	«не зачтено»

Преподаватель вправе предусмотреть тесты для самоконтроля обучающихся по разделам дисциплины, сформировав их из материалов фонда тестовых заданий дисциплины. Требования к тестам для самоконтроля аналогичны требованиям к итоговым тестам по семестрам и дисциплине в целом.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

3.1 Образец типового варианта терминологического диктанта

по всей дисциплине:

Предел длительности контроля – 45 минут.

1. Дать определение понятию «Аутентификация»
2. Дать определение понятию «APT-угроза, APT-атака»
3. Дать определение понятию «Резервные копии»
4. Дать определение понятию «Облачные вычисления, вычисления в облаке»
5. Дать определение понятию «Кибербезопасность»
6. Дать определение понятию «Утечка данных»
7. Дать определение понятию «Безопасность оконечных»
8. Дать определение понятию «Шифрование»
9. Что такое «Управление рисками предприятия»
10. Что такое «Межсетевой экран (файрволл, брандмауэр)»
11. Что такое «Хакер, злоумышленник»
12. Что такое «Провайдер интернет-услуг (ISP, internet service provider)»
13. Что такое «Система предотвращения вторжений (IPS, intrusion prevention system)»
14. Что такое «Клавиатурный шпион (кейлоггер)»
15. Что такое «Вредоносное ПО»
16. Что такое «Фишинг»
17. Что такое «Оценка рисков»
18. Что такое «Шпионское ПО»
19. Что такое «VPN»
20. Что такое «Вирус»
21. Что такое «Червь»
22. Что такое «Конфиденциальность»
23. Что такое «Угроза»
24. Что такое «Криптография»

25. Что такое «Аудит»
26. Что такое «Цифровая подпись»
27. Что такое «База данных»

Примеры оформления оценочных средств:

3.2. Перечень тем типовых докладов, сообщений

Доклады по теме: «Основы правового регулирования защиты информации», раздел 1 Основные составляющие кибербезопасности.

Темы докладов:

1. Понятие безопасности и её составляющие. Безопасность информации.
2. Обеспечение информационной безопасности: содержание и структура понятия.
3. Национальные интересы в информационной сфере.
4. Источники и содержание угроз в информационной сфере.
5. Соотношение понятий «информационная безопасность» и «национальная безопасность»
6. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.
7. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.
8. Система обеспечения информационной безопасности. Обеспечение информационной безопасности Российской Федерации.
9. Понятие информационной войны. Проблемы информационной войны.

Собеседования

Собеседование по теме: «Внутренние и внешние угрозы, связанные с новыми информационными технологиями», раздел 2 «Современные технологии, в области кибербезопасности и государственная политика».

Вопросы для собеседования

1. Ключевые свойства информации. Понятие угрозы.
2. Угроза нарушения конфиденциальности.
3. Угроза отказа служб.
4. Виды противников или "нарушителей".
5. Виды и каналы утечки информации.
6. Классификация атак.
7. Сетевые атаки
8. Классификация угроз и методы минимизации последствий.
9. Описание методик атак, использующих уязвимости операционной системы семейства Windows.
10. Принципы обеспечения информационной безопасности

Критерии оценки:

оценка «зачтено» выставляется обучающемуся, если: полностью раскрыт вопрос, приведены практические примеры, обучающийся ответил на дополнительные вопросы;

оценка «не зачтено» выставляется обучающемуся, если тема не раскрыта или ответ сделан формально, без приведения практических примеров, не отражена связь между процессом принятия решения по концепции и методом управления.

3.3 Перечень теоретических вопросов к зачету

(для оценки знаний)

Раздел 1 Основные составляющие кибербезопасности»

1.1 Требования к безопасности в кибернетических системах

1.2 Internet как среда для компьютерных преступлений.

1.3 Основные задачи информационной безопасности.

1.4 Основные методы обеспечения защиты информационной системы.
1.5 Потенциальные противники: классификация и характеристика.
1.6 Каналы утечки информации.
1.7 Классификация атак и их характеристики.
1.8 Сетевые атаки: основные виды.
1.9 Основные положения информационной безопасности.
1.10 Принципы обеспечения информационной безопасности.
1.11 Формальные модели доступа к данным.
1.12 Роль человека в кибернетических системах.
1.13 Технологии Internet вещей и smart things как частные случаи

Раздел 2 Современные технологии, в области кибербезопасности и государственная политика

2.1 Политика безопасности информационных систем
2.2 Таксономия нарушений информационной безопасности вычислительной системы.
2.3 Уровни правового обеспечения информационной безопасности.
2.4 Доктрина информационной безопасности России.
2.5 Задачи и методы криптографии.
2.6 Модели основных криптоаналитических атак.
2.7 Основные аппаратные средства защиты. Основные программные средства защиты.
2.8 Основные методы идентификации и аутентификации.
2.9 Сервисы управления доступом.
2.10 Протоколирование и аудит. Задачи аудита.
2.11 Основы защиты Internet-подключений.
2.12 Вирусы. Виды вирусов.
2.13 Антивирусное программное обеспечение.
2.14 Стандарты обеспечения информационной безопасности.
2.15 Общие принципы построения защищенных систем

3.4 Перечень типовых простых практических заданий к зачету

(для оценки умений)

1 Сформировать концепцию персональной кибербезопасности для формирования и анализа требований с системе защиты персональных данных

2 Составить информационную модель системы защиты персональных данных, включающую в себя описание основных объектов системы и взаимодействия между ними.

3 Сформировать аналитический обзор инструментов персональной кибербезопасности (русских и зарубежных)

4 Рассмотреть защиту всех аппаратных средств и средств связи, в том числе персонального компьютера, ноутбука, смартфона и устройств подключения к сети Интернет.

5 В соответствии с полученным заданием выполнить анализ и дать его описание со скриншотами выполненных действий. Покажите на скриншотах результат проведенного анализа

Таблица 1.1 – Варианты заданий

№	Объект защиты	Область защиты
1	Студент университета	Ноутбук, смартфон, средства связи
3	IT-специалист на удаленном доступе	Персональный компьютер, ноутбук, смартфон, средства связи

4	Модератор информационного ресурса	Персональный компьютер, ноутбук, смартфон, средства связи
5	Блогер	Ноутбук, смартфон, средства связи
6	Менеджер среднего звена на удаленном доступе	Персональный компьютер, ноутбук, смартфон, средства связи
7	Разработчик сайтов на удаленном доступе	Персональный компьютер, ноутбук, смартфон, средства связи
8	Программист на удаленном доступе	Персональный компьютер, ноутбук, смартфон, средства связи

6 Оценить экономический эффект применения инструментов персональной кибербезопасности
7 Рассчитать минимальную, среднюю и максимальную смету внедрения инструментов персональной кибербезопасности.
8 Описать принцип работы антивирусной защиты персональных компьютеров и мобильных устройств
9 Привести пример компонентов аппаратных средств защиты информации
10 Пояснить преимущества и недостатки существующих методов обоснования инвестиций в средства обеспечения персональной кибербезопасности.

3.5 Тестирование по дисциплине

3.5.1 Структура фонда тестовых заданий по дисциплине

Структура фонда тестовых заданий по дисциплине «Кибербезопасность»

Раздел дисциплины	Тема раздела	Количество тестовых заданий (ТЗ), типы ТЗ
1. Основные составляющие кибербезопасности	1.1 Введение в проблему кибербезопасности	4 – тип А 2 – тип В
	1.2 Основы правового регулирования защиты информации	4 – тип А 2 – тип В 2 - тип С
	1.3 Общие сведения о безопасности ПК и интернета, проблема интернет-зависимости.	3 – тип А 2 – тип Д
	1.4 Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы	5 – тип А 2 – тип В
	1.5 Сведения о безопасности ПК и интернета	4 – тип А 2 – тип В
	1.6 Теоретические основы и практические аспекты защиты киберпространства	4 – тип А 2 – тип В
	1.7 Мошеннические действия в интернете, киберпреступления против личности, общества и государства, хакерские атаки и кибертерроризм	2 – тип А 2 – тип В
		∑ 40 24 – тип А 12 – тип В 2 – тип С 2 – тип Д

2. Современные технологии, в области кибербезопасности и государственная политика	2.1 Организация и проведение работ по технической защите информации в компьютерных сетях и системах	4 – тип А 3 – тип В 1 - тип С
	2.2 Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации	6 – тип А 4 – тип В
	2.3 Техническая защита информации в компьютерных сетях и системах /	5 – тип А 2 – тип Д
	2.4 Государственная политика в области кибербезопасности и государственный аудит.	4 – тип А 3 – тип В
	2.5 Законодательства в области защиты информации	6 – тип А 4 – тип В
		∑32 19 – тип А 10 – тип В 1– тип С 2– тип Д

Используемые типы тестовых заданий (ТЗ):

ТЗ типа А: тестовое задание закрытой формы (ТЗ с выбором одного или нескольких правильных ответов);

ТЗ типа В: тестовое задание открытой формы (с конструируемым ответом: ТЗ с кратким регламентируемым ответом (ТЗ дополнения); ТЗ свободного изложения (с развернутым ответом в произвольной форме);

ТЗ типа С: тестовое задание на установление соответствия;

ТЗ типа Д: тестовое задание на установление правильной последовательности.

3.5.2 Структура и образец типового теста за 6 семестр по дисциплине за весь период ее освоения

Структура типового теста за 6 семестр/итогового теста по дисциплине за весь период ее освоения

Описание требований к тесту: итоговый тест по дисциплине «Кибербезопасность» предполагает оценку того, насколько студент:

– знает: объекты компьютерных технологий, используемые в обеспечении кибербезопасности; понятийный аппарат информационных технологий и особенности терминологии кибербезопасности;

– умеет: использовать основные нормы и требования, указанные в нормативно-методических документах по делопроизводству, анализировать документ, выявлять недочеты и вносить коррективы, в том числе, в оформление технической документации, и документации в сфере информационной безопасности; оформлять документы по организации защиты информации;

– владеет: знаниями о современных технологиях, применяемых в области кибербезопасности; навыками составления документов с учетом требований нормативно-правовой документации, навыками оформления документов по организации защиты информации.

Студенту необходимо выполнить 41 тестовых заданий. Максимальное количество составляет 100%. Проходной составляет 75%. Обучающийся, набравший более 75%правильных ответов сдал тест, менее 75% – нет. Время на выполнение тестового задания – 60 минут.

Раздел дисциплины	Тема раздела	Количество тестовых заданий (ТЗ), типы ТЗ
	1.1 Введение в проблему кибербезопасности	4 – тип А 2 – тип В

1. Основные составляющие кибербезопасности	1.2 Основы правового регулирования защиты информации	4 – тип А 2 – тип В 2 - тип С
	1.3 Общие сведения о безопасности ПК и интернета, проблема интернет-зависимости.	3 – тип А 2 – тип Д
	1.4 Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы	5 – тип А 2 – тип В
	1.5 Сведения о безопасности ПК и интернета	4 – тип А 2 – тип В
	1.6 Теоретические основы и практические аспекты защиты киберпространства	4 – тип А 2 – тип В
	1.7 Мошеннические действия в интернете, киберпреступления против личности, общества и государства, хакерские атаки и кибертерроризм	2 – тип А 2 – тип В
		∑ 40 24 – тип А 12 – тип В 2 – тип С 2 – тип Д
2. Современные технологии, в области кибербезопасности и государственная политика	2.1 Организация и проведение работ по технической защите информации в компьютерных сетях и системах	4 – тип А 3 – тип В 1 - тип С
	2.2 Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации	6 – тип А 4 – тип В
	2.3 Техническая защита информации в компьютерных сетях и системах /	5 – тип А 2 – тип Д
	2.4 Государственная политика в области кибербезопасности и государственный аудит.	4 – тип А 3 – тип В
	2.5 Законодательства в области защиты информации	6 – тип А 4 – тип В
		∑32 19 – тип А 10 – тип В 1– тип С 2– тип Д

Образец типового *теста*
за 6 семестр/итогового теста по дисциплине за весь период ее освоения

Описание требований к тесту: итоговый тест по дисциплине «Кибербезопасность» предполагает оценку того, насколько студент:

– знает: объекты компьютерных технологий, используемые в обеспечении кибербезопасности; понятийный аппарат информационных технологий и особенности терминологии кибербезопасности;

– умеет: использовать основные нормы и требования, указанные в нормативно-методических документах по делопроизводству, анализировать документ, выявлять недочеты и вносить коррективы, в том числе, в оформление технической документации, и документации в сфере информационной безопасности; оформлять документы по организации защиты информации;

– владеет: знаниями о современных технологиях, применяемых в области кибербезопасности; навыками составления документов с учетом требований нормативно-правовой документации, навыками оформления документов по организации защиты информации.

Студенту необходимо выполнить 41 тестовых заданий. Максимальное количество составляет 100%. Проходной составляет 75%. Обучающийся, набравший более 75%правильных ответов сдал тест, менее 75% – нет. Время на выполнение тестового задания – 60 минут.

Образец типового теста содержит задания для оценки знаний, для оценки умений, для оценки навыков и (или) опыта деятельности:

1. Что можно делать на видеохостинге в YouTube?
1. Размещать материалы без согласия их авторов
2. Выражать своё несогласие с мнением другого в уважительной форме
3. Размещать противозаконные, оскорбительные материалы
4. Грубить в комментариях

2. Какой из паролей является надёжным?
1. Alex2001
2. 19032001
3. 12345678
4. Vbif20hjvfyjd01

3. Что НЕ следует делать, если ты столкнулся с троллем в Сети?
1. Игнорировать выпады тролля
2. Заблокировать тролля
3. Проучить или доказать свою правоту
4. Сообщить модераторам сайта

4. Откуда НЕ стоит брать информацию в Интернете для реферата?
1. Сайты средств массовой информации
2. Википедия
3. Электронные библиотеки
4. Сообщества в социальных сетях

5. Что является признаком достоверности информации в Сети?
1. Возможность перепроверить эту информацию в других источниках и на официальных сайтах
2. Правдоподобность информации
3. Качественное оформление информации
4. Грамотное изложение информации

6. Как НЕ стоит себя вести, если вы стали жертвой кибербуллинга?

7. Какие данные из нижеперечисленных можно сообщать по электронной почте?
1. Номера банковских счетов (кредитных карт)
2. Секретные слова (ответы) на специальные секретные вопросы, используемые при идентификации вашего аккаунта
3. PIN-коды
4. Ваши имя и фамилию

8. Когда можно доверять письму от неизвестного отправителя?
1. Отправитель ссылается на ваших друзей
2. Отправитель использует логотип авторитетной компании
3. К вам обращаются по имени

4. Никогда нельзя доверять письму от неизвестного отправителя

9. В каком случае нарушается авторское право?
1. При размещении на YouTube собственного видеоролика с концерта какой-либо группы
2. При чтении романа И. Тургенева «Отцы и дети» в Интернете
3. При использовании материалов Википедии для подготовки доклада со ссылкой на источник
4. При просмотре трансляций на официальном сайте телеканала

10. Как защититься от негативного контента?
1. Использовать безопасный поиск Google и безопасный режим на YouTube
2. Установить антивирус
3. Не обращать на него внимания
4. Обратиться к автору негативного контента

11. Что из следующего является примером «фишинговой» атаки?
1. Отправка кому-либо текстового сообщения, содержащего вредоносную ссылку, замаскированную под уведомление о том, что этот человек выиграл в лотерею.
2. Все вышеперечисленное
3. Отправка кому-то электронного письма, содержащего вредоносную ссылку, замаскированную под письмо от знакомого человека
4. Не знаю
5. Создание поддельного веб-сайта, который выглядит почти идентично реальному веб-сайту, чтобы обманом заставить пользователей ввести свои данные для входа

12. Группа компьютеров, объединенных в сеть и используемых хакерами для кражи информации, называется?

13. Когда можно полностью доверять новым онлайн-друзьям?
1. Поговорив по телефону
2. После длительной переписки
3. После обмена фотографиями
4. Ничего не может дать100 % гарантию того, что онлайн-другу можно доверять

14. Что НЕ поможет защитить свою электронную почту от взлома?
1. Создавать разные пароли от разных аккаунтов
2. Периодически менять адрес электронной почты, менять провайдеров
3. Не открывать сообщения с незнакомых и подозрительных адресов
4. Никому не сообщать свой пароль

15. **Что обозначает «https: //» в начале URL-адреса, а не «http: //» (без буквы «s»)?**
1. Сайт имеет особое высокое разрешение
2. Сайт недоступен для определенных компьютеров
3. Ничего из вышеперечисленного
4. На сайте имеется самая последняя доступная версия
5. Информация, введенная на сайт, зашифрована

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и опыта деятельности

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

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Терминологический диктант	Средство проверки степени овладения категориальным аппаратом темы, раздела, дисциплины. Может быть использовано для оценки знаний обучающихся	Перечень понятий по темам дисциплины
2	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
3	Сообщение, доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов, сообщений
4	Зачет	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 зачету

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 зачета и оценивания результатов обучения

При проведении промежуточной аттестации в форме зачета преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра и результатами тестирования по материалам, изученным в течении семестра. Оценочные средства и типовые контрольные задания, используемые при текущем контроле, в совокупности с тестированием, 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). Время проведения тестирования объявляется обучающимся заранее.

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

Средняя оценка уровня сформированности компетенций по результатам текущего контроля и тестирования за семестр	Оценка
Оценка не менее 3.0, нет ни одной неудовлетворительной оценки по текущему контролю и обучающийся набрал при тестировании более 69 баллов	«зачтено»
Оценка менее 3.0, или получена хотя бы одна неудовлетворительная оценка по текущему контролю, или обучающийся набрал при тестировании менее 69 баллов	«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.