ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом ректора
от «02» июня 2023 г. № 424-1

Б1.О.51 Кибербезопасность

рабочая программа дисциплины

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

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

Формы промежуточной аттестации
очная форма обучения:
зачет 6 семестр

Очная форма обучения **Распределение часов дисциплины по семестрам**

Семестр	6	**Итого**
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**
Итого	144	**144**

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем утвержденным Приказом Минобрнауки России от от 26.11.2020 № 1457.

Программу составил(и):
К.э.н., доцент, заведующий кафедрой, Т. К. Кириллова

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «2» июня 2023 г. № 12

Зав. кафедрой, к.э.н., доцент Т.К. Кириллова

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1 Цели дисциплины

1	изучение и усвоение обучающимися теоретических основ и общих представлений о безопасности в информационном обществе;
2	освоение обучающимися 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

Профессионально-трудовое воспитание обучающихся

Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда.
Цель достигается по мере решения в единстве следующих задач:
– формирование сознательного отношения к выбранной профессии;
– воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность;
– формирование психологии профессионала;
– формирование профессиональной культуры, этики профессионального общения;
– формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Блок/часть ОПОП	Блок 1. Дисциплины / Обязательная часть

2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины

1	Б1.О.33 Основы информационной безопасности
2	Б1.О.36 Сети и системы передачи информации
3	Б1.О.47 Информационные технологии

2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее

1	Б1.О.24 Аттестация объектов информатизации
2	Б1.О.31 Безопасность сетей ЭВМ
3	Б1.О.39 Программно-аппаратные средства защиты информации
4	Б1.О.42 Открытые информационные системы
5	Б1.О.45 Виртуальные частные сети
6	Б1.О.55 Защита объектов критической информационной инфраструктуры
7	Б1.О.56 Защита информации в государственных информационных системах
8	Б1.О.62 Моделирование процессов и систем защиты информации
9	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
10	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	ОПК-1.3 Оценивает роль, сущность и значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства	Знать: объекты компьютерных технологий, используемые в обеспечении кибербезопасности; понятийный аппарат информационных технологий и особенности терминологии кибербезопасности; нормативно-правовые акты, 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,

значение для обеспечения объективных потребностей личности, общества и государства		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	Знать: основные термины и понятия защиты информации, сетей и систем передачи данных
		Уметь: ставить цели, формулировать задачи, связанные с обеспечением кибербезопасности
		Владеть: методами проведения анализа 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	Знать: особенности информационные технологии, используемые в автоматизированных системах
		Уметь: анализировать тенденции развития систем обеспечения кибербезопасности
		Владеть: навыками работы с информационными технологиями, используемыми в автоматизированных системах
	ОПК-9.3 Знает текущее состояние и тенденции развития сетей и систем передачи информации	Знать: тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации
		Уметь: применять знания о сетях и систем передачи информации при решении поставленных задач
		Владеть: алгоритмами обработки информации, в сфере информационной безопасности

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
1.0	**Раздел 1. Основные составляющие кибербезопасности.**						
1.1	Введение в проблему кибербезопасности	6	2	2			ОПК-1.3 ОПК-9.1 ОПК-9.3
1.2	Основы правового регулирования защиты информации	6	2	4		8	ОПК-1.3
1.3	Общие сведения о безопасности ПК и интернета, проблема интернет-зависимости	6	2	6		6	ОПК-9.1 ОПК-9.2
1.4	Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы	6	2	4		4	ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3
1.5	Сведения о безопасности ПК и интернета	6	2	4		4	ОПК-9.1 ОПК-9.2
1.6	Теоретические основы и практические аспекты защиты киберпространства	6	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	6	4	4		4	ОПК-1.3 ОПК-9.1 ОПК-9.2
2.0	**Раздел 2. Современные технологии, в области кибербезопасности и государственная политика.**						
2.1	Организация и проведение работ по технической защите информации в компьютерных сетях и системах	6	2	2		6	ОПК-1.3 ОПК-9.1
2.2	Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации	6	2	4		4	ОПК-9.1 ОПК-9.2 ОПК-9.3
2.3	Техническая защита информации в компьютерных сетях и системах	6	2	2		4	ОПК-1.3 ОПК-9.1
2.4	Государственная политика в области кибербезопасности и государственный аудит.	6	4	4		4	ОПК-1.3

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
2.5	Законодательства в области защиты информации	6	4	6		6	ОПК-1.3
2.6	Сохранность и конфиденциальность данных	6	4	5		5	ОПК-1.3 ОПК-9.1
	Форма промежуточной аттестации – зачет	6					
	Итого часов (без учёта часов на промежуточную аттестацию)		34	51		59	

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

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.1.1	Интернет-технологии : учебно-методическое пособие / . Казань : Поволжская ГАФКСиТ, 2016. - 96с. - Текст: электронный. - URL: https://e.lanbook.com/book/154942 (дата обращения: 19.04.2023)	Онлайн
6.1.1.2	Информационная безопасность : лабораторный практикум / . Пермь : ПГГПУ, 2018. - 87с. - Текст: электронный. - URL: https://e.lanbook.com/book/129509 (дата обращения: 19.04.2023)	Онлайн
6.1.1.3	Информационная безопасность: современная теория и практика: сборник научных трудов студентов, аспирантов и преподавателей по материалам II Межвузовской научно-практической конференции : сборник научных трудов / . Омск : СибАДИ, 2019. - 145с. - Текст: электронный. - URL: https://e.lanbook.com/book/163756 (дата обращения: 19.04.2023)	Онлайн
6.1.1.4	Технологии программной защиты в интернете: учебное пособие / . Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2015. - 60с. - Текст: электронный. - URL: https://e.lanbook.com/book/180095 (дата обращения: 19.04.2023)	Онлайн
6.1.1.5	Воробьев, С. П. Компьютерные сети и сетевая безопасность : учебное пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. Новочеркасск : ЮРГПУ (НПИ), 2022. - 216с. - Текст: электронный. - URL: https://e.lanbook.com/book/292247 (дата обращения: 19.04.2023)	Онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Технологии программной защиты в интернете: учебное пособие / . Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2015. - 76с. - Текст: электронный. - URL: https://e.lanbook.com/book/180096 (дата обращения: 19.04.2023)	Онлайн
6.1.2.2	Айвазян, В. Б. Интернет-технологии : методические указания по выполнению лабораторных работ / В. Б. Айвазян. Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2013. - 76с. - Текст: электронный. - URL: https://e.lanbook.com/book/181496 (дата обращения: 19.04.2023)	Онлайн
6.1.2.3	Архипов, В. В. Интернет-право : учебник и практикум для вузов / В. В. Архипов.. Москва : Юрайт, 2022. - 249с. - Текст: электронный. - URL: https://urait.ru/bcode/489683 (дата обращения: 09.09.2022)	Онлайн

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

	Библиографическое описание	Кол-во экз.

		в библиотеке/ онлайн
6.1.3.1	Кириллова, Т.К. Методические указания по изучению дисциплины Б1.О.51 Кибербезопасность по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация Безопасность открытых информационных систем / Т. К. Кириллова; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 12 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_8786_1529_2023_1_signed.pdf	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Научная электронная библиотека «КиберЛенинка» — https://cyberleninka.ru/	
6.2.2	Научная электронная библиотека eLIBRARY.RU — https://elibrary.ru/	
6.2.3	Электронная библиотека Учебно-методического центра по образованию на железнодорожном транспорте «ЭБ УМЦ ЖДТ» — https://umczdt.ru/books/	
6.2.4	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/	
6.2.5	Электронно-библиотечная система «Образовательная платформа ЮРАЙТ», https://urait.ru/	
6.2.6	Электронно-библиотечная система «Университетская библиотека онлайн», https://biblioclub.ru/	
6.3 Программное обеспечение и информационные справочные системы		
6.3.1 Базовое программное обеспечение		
6.3.1.1	Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.2	Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.3	FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/	
6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/	
6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License	
6.3.2 Специализированное программное обеспечение		
6.3.2.1	Не предусмотрено	
6.3.3 Информационные справочные системы		
6.3.3.1	Не предусмотрены	
6.4 Правовые и нормативные документы		
6.4.1	Не предусмотрены	

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 ИрГУПС находится – по адресу г. Иркутск, ул. Лермонтова, д.80
2	Учебная аудитория Д-216 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор,экран, (ноутбук переносной)
3	Учебная аудитория Д-518 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор,экран, (ноутбук переносной)
4	Учебная аудитория Д-521 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор,экран, (ноутбук переносной)
5	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; – помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. 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	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 домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Самостоятельная работа	Обучение по дисциплине «Кибербезопасность» предусматривает активную самостоятельную работу обучающегося. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а также указана необходимая учебная литература: обучающийся изучает учебный материал, разбирает примеры и решает разноуровневые задачи в рамках выполнения как общих домашних заданий, так и индивидуальных домашних заданий (ИДЗ) и других видов работ, предусмотренных рабочей программой дисциплины. При выполнении домашних заданий обучающемуся следует обратиться к задачам, решенным на предыдущих практических занятиях, решенным домашним работам, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора. Домашние задания, индивидуальные домашние задания и другие работы, предусмотренные рабочей программой дисциплины должны быть выполнены обучающимся в установленные преподавателем сроки в соответствии с требованиями к оформлению текстовой и графической документации, сформулированным в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль»
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет	

Приложение № 1 к рабочей программе

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

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 ИрГУПС, а также 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;

– 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

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
6 семестр				
1.0	**Раздел 1. Основные составляющие кибербезопасности**			
1.1	Текущий контроль	Введение в проблему кибербезопасности	ОПК-1.3 ОПК-9.1 ОПК-9.3	Собеседование (устно)
1.2	Текущий контроль	Основы правового регулирования защиты информации	ОПК-1.3	Собеседование (устно)
1.3	Текущий контроль	Общие сведения о безопасности ПК и интернета, проблема интернет-зависимости	ОПК-9.1 ОПК-9.2	Сообщение (устно)
1.4	Текущий контроль	Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы	ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3	Доклад (устно)
1.5	Текущий контроль	Сведения о безопасности ПК и интернета	ОПК-9.1 ОПК-9.2	Собеседование (устно)
1.6	Текущий контроль	Теоретические основы и практические аспекты защиты киберпространства	ОПК-1.3 ОПК-9.1	Сообщение (устно) Творческое задание (письменно)
1.7	Текущий контроль	Мошеннические действия в интернете, киберпреступления против личности, общества и государства, хакерские атаки и кибертерроризм	ОПК-1.3 ОПК-9.1 ОПК-9.2	Собеседование (устно)
2.0	**Раздел 2. Современные технологии, в области кибербезопасности и государственная политика**			
2.1	Текущий контроль	Организация и проведение работ по технической защите информации в компьютерных сетях и системах	ОПК-1.3 ОПК-9.1	Ситуационная задача (письменно) Собеседование (устно) Сообщение (устно)
2.2	Текущий контроль	Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации	ОПК-9.1 ОПК-9.2 ОПК-9.3	Собеседование (устно)
2.3	Текущий контроль	Техническая защита информации в компьютерных сетях и системах	ОПК-1.3 ОПК-9.1	Сообщение (устно)
2.4	Текущий контроль	Государственная политика в области кибербезопасности и государственный аудит.	ОПК-1.3	Доклад (устно)
2.5	Текущий контроль	Законодательства в области защиты информации	ОПК-1.3	Сообщение (устно)
2.6	Текущий контроль	Сохранность и конфиденциальность данных	ОПК-1.3 ОПК-9.1	Собеседование (устно)

	Промежуточная аттестация	Раздел 1. Основные составляющие кибербезопасности. Раздел 2. Современные технологии, в области кибербезопасности и государственная политика.		Зачет (собеседование) Зачет - тестирование (компьютерные технологии)

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

Описание показателей и критериев оценивания компетенций.
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.

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

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

Текущий контроль

№	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 для собеседования по темам/разделам дисциплины
2	Ситуационная задача	Проблемное задание, в котором обучающемуся предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности, а также отдельных компетенций (в рамках дисциплины)	Типовое задание для решения ситуационной задачи
3	Сообщение	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 сообщений
4	Доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.	Темы докладов

		Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	
5	Творческое задание	Частично регламентированное задание, имеющее нестандартное решение и позволяющее диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения. Может выполняться в индивидуальном порядке или группой обучающихся. Может быть использовано для оценки знаний, навыков и (или) опыта деятельности обучающихся	Темы творческих заданий
6	Диктант	Средство проверки степени овладения лексикой и / или грамматическими структурами темы/ раздела. В зависимости от типа диктанта (переводной, диктант с пропусками, диктант с грамматическими трансформациями, диктоглосс и т.д.) становится возможным также оценить уровень сформированности комплексных речевых умений, а также орфографических и слуховых навыков обучающихся. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень языковых и речевых единиц, текстов для диктанта

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	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 к зачету
2	Тест – промежуточная аттестация в форме зачета	Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине (модулю) с использованием информационно-коммуникационных технологий. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета. Шкала оценивания уровня освоения компетенций

Шкала оценивания	Критерии оценивания	Уровень освоения компетенции
«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
	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
	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного	Минимальный

	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	
«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

Тест – промежуточная аттестация в форме зачета

Шкала оценивания	Критерии оценивания
«зачтено»	Обучающийся верно ответил на 70 % и более тестовых заданий при прохождении тестирования
«не зачтено»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Собеседование

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	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 зачтено»	Не было попытки выполнить задание

Ситуационная задача

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Обучающийся излагает материал логично, грамотно, без ошибок; свободное владеет профессиональной терминологией; умеет высказывать и обосновать свои суждения; дает четкий, полный, правильный ответ на теоретические вопросы; организует связь теории с практикой
«хорошо»		Обучающийся грамотно излагает материал; ориентируется в материале; владеет профессиональной терминологией; осознанно применяет теоретические знания для решения кейса, но содержание и форма ответа имеют отдельные неточности. Ответ обучающегося правильный, полный, с незначительными неточностями или недостаточно полный
«удовлетворительно»		Обучающийся излагает материал неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения кейса, не может доказательно обосновать свои суждения; обнаруживается недостаточно глубокое понимание

		изученного материала
«неудовлетворительно»	«не зачтено»	У обучающегося отсутствуют необходимые теоретические знания; допущены ошибки в определении понятий, искажен их смысл, не решен кейс. В ответе обучающийся проявляется незнание основного материала учебной программы, допускаются грубые ошибки в изложении, не может применять знания для решения кейса

Сообщение

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

Доклад

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	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»	«не зачтено»	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 доклада не передана

Творческое задание

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Представленная работа демонстрирует точное понимание задания и

		полное ему соответствие. В работе приводятся конкретные факты и примеры. Материал изложен логично. Работа и форма её представления является авторской, выполнена самостоятельно и содержит большое число оригинальных, изобретательных примеров. Эффективное использование изображений, видео, аудио и других мультимедийных возможностей, чтобы представить свою тему и вызвать интерес. Презентация имеет все необходимые разделы, данные об авторе, ссылки на источники, оформлена в одном стиле. Текст не избыточен на слайде, не имеет орфографических и речевых ошибок
«хорошо»		Представленная работа демонстрирует понимание задания. В работу включаются как материалы, имеющие как непосредственное отношение к теме, так и материалы, не имеющие отношения к ней. Содержание работы соответствует заданию, но не все аспекты задания раскрыты. В работе есть элементы творчества. Используются однотипные мультимедийные возможности, или некоторые из них отвлекают внимание от темы презентации. Основные требования к презентации соблюдены, но отсутствует выполнение требований либо к оформлению, либо к содержанию. Текст на слайде не избыточен, но плохо читается, несколько неудачных речевых выражений
«удовлетворительно»		В работу включена собранная обучающимся информация, но она не анализируется и не оценивается. Нарушение логики в изложении материала. Обычная, стандартная работа, элементы творчества отсутствуют. Не используются изображения, видео, аудио и другие мультимедийные возможности, или их использование отвлекает внимание. Не соблюдены требования к оформлению презентации. Слишком много текста, или две и более орфографических ошибок, или речевые и орфографические ошибки
«неудовлетворительно»	«не зачтено»	Включены материалы, не имеющие непосредственного отношения к теме работы, содержание работы не относится в рассматриваемой проблеме. Отсутствует логики в изложении материала. Не используются изображения, видео, аудио и другие мультимедийные возможности, или их использование отвлекает внимание. Не соблюдены требования к оформлению презентации

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

3.1 Типовые контрольные задания для проведения собеседования

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для проведения собеседований.

1. Что такое кибербезопасность?
2. Какие основные угрозы кибербезопасности существуют?
3. Как вы понимаете концепцию «трех линий обороны» в кибербезопасности?
4. Что такое «атаки нулевого дня» и как они представляют угрозу для организаций?
5. Какие существуют виды атак на веб-приложения и как их предотвратить?

Образец типового варианта вопросов для проведения собеседования
«Основы правового регулирования защиты информации»

1. Дайте определение информации и укажите основные свойства, которыми она обладает.
2. Перечислите и кратко охарактеризуйте основные нормативно-правовые акты, регулирующие отношения, связанные с информацией и информационными

технологиями.
3. Что такое персональные данные и каким образом они регулируются законодательством?
4. В каких случаях требуется согласие субъекта на обработку его персональных данных?
5. Что входит в понятие «конфиденциальная информация» и какие нормативно-правовые документы регулируют ее защиту?

Образец типового варианта вопросов для проведения собеседования
«Сведения о безопасности ПК и интернета»

Образец типового варианта вопросов для проведения собеседования
«Мошеннические действия в интернете, киберпреступления против личности, общества и государства, хакерские атаки и кибертерроризм»

1. Расскажите о своем опыте в обеспечении кибербезопасности и о ролях и обязанностях пользователей в этом процессе.
2. Какие основные принципы безопасности вы соблюдаете при работе с электронной почтой и приложениями для обмена сообщениями?
3. Какие методы вы используете для защиты от вредоносных ссылок и вирусов в электронных письмах?
4. Как вы обеспечиваете безопасность своих банковских операций и онлайн-платежей?
5. Какие меры вы принимаете для защиты своих личных данных при использовании онлайн-магазинов и социальных сетей?

Образец типового варианта вопросов для проведения собеседования
«Организация и проведение работ по технической защите информации в компьютерных сетях и системах»

1. В чем заключаются основные задачи технической защиты информации в компьютерных системах и сетях?
2. Опишите основные этапы работ по технической защите информации.
3. Какие методы и средства используются для защиты информации от несанкционированного доступа в компьютерных системах?
4. Какие технические меры применяются для защиты информации при ее передаче по сетям связи?
5. Как осуществляется защита информации от вредоносного программного обеспечения в компьютерных системах?

Образец типового варианта вопросов для проведения собеседования
«Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации»

1. Что такое аттестация объектов вычислительной техники и для чего она проводится?
2. Какие основные этапы включает в себя процедура аттестации объектов вычислительной техники?
3. Какие требования и стандарты учитываются при проведении аттестации объектов вычислительной техники?
4. Что такое система безопасности информации и как она формируется?
5. Какие меры необходимо предпринять для обеспечения защиты информации на объекте вычислительной техники?

Образец типового варианта вопросов для проведения собеседования
«Сохранность и конфиденциальность данных»

1. Объясните понятие «Информационная безопасность».
2. Назовите основные угрозы информационной безопасности.
3. Опишите процесс обеспечения сохранности и конфиденциальности данных.
4. Каковы основные меры по обеспечению конфиденциальности данных?

5. Расскажите о методах защиты информации от утечки.

Образец типового варианта ситуационной задачи

«Организация и проведение работ по технической защите информации в компьютерных сетях и системах»

Задача 1: Оценка уровня защищенности компьютерной системы от внешних угроз.

Цель: Оценить уровень защищенности компьютерной системы предприятия от внешних угроз безопасности информации.

Исходные данные: Техническое описание компьютерной системы, информация об угрозах, связанных с внешними источниками.

Требуется: Провести анализ компьютерной системы на предмет наличия уязвимостей, провести оценку уровня защищенности и предложить меры по усилению защиты.

Задача 2: Защита информации при передаче по сети.

Цель: Организация защиты информации, передаваемой по сети предприятия.

Исходные данные: Структура сети передачи данных предприятия, информационные ресурсы, подлежащие защите.

Требуется: Выбрать и обосновать необходимые средства защиты, разработать рекомендации по их использованию, а также предложить мероприятия по контролю защищенности сети.

3.3 Типовые контрольные темы для написания сообщений

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов тем для написания сообщений.

Образец тем сообщений

«Общие сведения о безопасности ПК и интернета, проблема интернет-зависимости»

1. Роли и обязанности пользователей в обеспечении кибербезопасности.
2. Основные принципы безопасности при работе с электронной почтой и приложениями для обмена сообщениями.
3. Методы защиты от вредоносных ссылок и вирусов в электронных письмах.
4. Безопасность банковских операций и онлайн-платежей.
5. Защита от кражи личных данных при использовании онлайн-магазинов и социальных сетей.
6. Защита от взлома аккаунтов и утечки паролей.
7. Основные принципы безопасности при скачивании файлов и программ из интернета.
8. Роли антивирусных программ, фаерволов и других инструментов в обеспечении безопасности ПК и интернета.
9. Безопасность домашних сетей Wi-Fi и методы защиты от несанкционированного доступа.
10. Правила безопасного использования облачных сервисов и хранения данных в облаке.
11. Определение и предотвращение кибершпионажа и кибервойны.

Образец тем сообщений

«Теоретические основы и практические аспекты защиты киберпространства»

1. Основные принципы кибербезопасности и их роль в обеспечении безопасности информации и систем.
2. Виды угроз в киберпространстве и методы их предотвращения.
3. Методы защиты от вредоносного программного обеспечения и предотвращения его воздействия на системы и данные.
4. Меры предосторожности при использовании общественных Wi-Fi сетей для защиты данных.
5. Шаги по защите личных данных в интернете, включая использование сильных

паролей и двухфакторной аутентификации.

Образец тем сообщений

«Организация и проведение работ по технической защите информации в компьютерных сетях и системах»

1. “Технические аспекты защиты информации в компьютерных системах”
2. “Криптографические методы защиты информации”
3. “Защита информации от вредоносного ПО”
4. “Организация контроля доступа к информационным ресурсам”
5. “Физическая защита объектов информатизации”
6. “Обеспечение информационной безопасности в беспроводных сетях”
7. “Защита информации при ее передаче по сетям”
8. “Методы и средства защиты от несанкционированного доступа”
9. “Правовые аспекты защиты информации”
10. “Аттестация объектов вычислительной техники”
11. “Роль стандартов и сертификации в обеспечении информационной безопасности”

Образец тем сообщений

«Техническая защита информации в компьютерных сетях и системах»

1. Основные аспекты технической защиты информации.
2. Методы и средства обеспечения информационной безопасности.
3. Защита информации от вредоносного программного обеспечения.
4. Криптографические методы защиты данных.
5. Организация физической защиты объектов информатизации.
6. Контроль доступа к информационным ресурсам.
7. Защита информации при ее передаче по компьютерным сетям.
8. Правовые аспекты технической защиты информации.
9. Стандарты и сертификация в области информационной безопасности.
10. Техническая защита информации на предприятиях и в государственных учреждениях.

Образец тем сообщений

«Законодательства в области защиты информации»

1. Понятие и основные принципы законодательства о защите информации.
2. Международные соглашения и конвенции в области защиты информации.
3. Нормативно-правовая база защиты информации в Российской Федерации.
4. Права и обязанности субъектов в области защиты информации.
5. Ответственность за нарушение законодательства о защите информации.
6. Защита персональных данных: законодательство и практика.
7. Конфиденциальная информация и ее защита.
8. Информационное право: понятие и основные принципы.
9. Защита информации в информационно-телекоммуникационных сетях.
10. Электронная подпись и ее использование в законодательной практике.

3.4 Типовые контрольные темы для написания докладов

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов тем для написания докладов.

Образец тем докладов

«Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы»

Образец тем докладов

«Государственная политика в области кибербезопасности и государственный аудит.»

1. Роль государства в обеспечении кибербезопасности.
2. Основные направления государственной политики в области кибербезопасности.
3. Государственный аудит как инструмент обеспечения кибербезопасности.

4. Законодательное регулирование кибербезопасности на государственном уровне.
5. Взаимодействие государства и бизнеса в области кибербезопасности.
6. Международное сотрудничество в сфере кибербезопасности.
7. Проблемы и перспективы развития государственной политики в области кибербезопасности.

3.5 Типовые контрольные задания для выполнения творческих заданий

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для выполнения творческих заданий.

Образец творческого задания
«Теоретические основы и практические аспекты защиты киберпространства»

3.6 Типовые контрольные задания для проведения тестирования

Фонд тестовых заданий по дисциплине содержит тестовые задания, распределенные по разделам и темам, с указанием их количества и типа.

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-1.3 ОПК-9.1 ОПК-9.3	Введение в проблему кибербезопасности	Знание	2 – ОТЗ 2 – ЗТЗ
ОПК-1.3	Основы правового регулирования защиты информации	Знание	2 – ОТЗ 2 – ЗТЗ
ОПК-9.1 ОПК-9.2	Общие сведения о безопасности ПК и интернета, проблема интернет-зависимости	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3	Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	4 – ОТЗ 4 – ЗТЗ
ОПК-9.1 ОПК-9.2	Сведения о безопасности ПК и интернета	Знание	6 – ОТЗ 6 – ЗТЗ
ОПК-1.3 ОПК-9.1	Теоретические основы и практические аспекты защиты киберпространства	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
ОПК-1.3 ОПК-9.1 ОПК-9.2	Мошеннические действия в интернете, киберпреступления против личности, общества и государства, хакерские атаки и кибертерроризм	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
ОПК-1.3 ОПК-9.1	Организация и проведение работ по технической защите информации в компьютерных сетях и системах	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	4 – ОТЗ 4 – ЗТЗ
ОПК-9.1 ОПК-9.2 ОПК-9.3	Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации	Знание	2 – ОТЗ 2 – ЗТЗ

ОПК-1.3 ОПК-9.1	Техническая защита информации в компьютерных сетях и системах	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
ОПК-1.3	Государственная политика в области кибербезопасности и государственный аудит.	Знание	2 – ОТЗ 2 – ЗТЗ
ОПК-1.3	Законодательства в области защиты информации	Знание	2 – ОТЗ 2 – ЗТЗ
ОПК-1.3 ОПК-9.1	Сохранность и конфиденциальность данных	Знание	2 – ОТЗ 2 – ЗТЗ
		Итого	100

Полный комплект ФТЗ хранится в электронной информационно-образовательной среде ИрГУПС и обучающийся имеет возможность ознакомиться с демонстрационным вариантом ФТЗ.

Ниже приведен образец типового варианта итогового теста, предусмотренного рабочей программой дисциплины.

1. Кто является основным ответственным за определение уровня классификации информации?

а) Руководитель среднего звена

б) Высшее руководство

в) Владелец

г) Пользователь

2. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

а) Владельцы данных

б) Пользователи

в) Администраторы

г) Руководство

3. Что является основой для формирования государственной политики в сфере информации?

Ответ: Доктрина

4. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

а) Анализ рисков

б) Анализ затрат / выгоды

в) Результаты ALE

г) Выявление уязвимостей и угроз, являющихся причиной риска

5. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

а) Внедрение управления механизмами безопасности

б) Классификацию данных после внедрения механизмов безопасности

в) Уровень доверия, обеспечиваемый механизмом безопасности

г) Соотношение затрат / выгод

6. Какая угроза возникает в результате технологической неисправности за пределами информационной системы?

Ответ: Техническая

7. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

а) Чтобы убедиться, что проводится справедливая оценка

б) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ

в) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа

г) Поскольку люди в различных подразделениях сами являются одной из причин

рисков, они должны быть ответственны за их оценку

8. Основными рисками информационной безопасности являются:

Ответ: Потеря, искажение, утечка информации

9. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

а) Список стандартов, процедур и политик для разработки программы безопасности

б) Текущая версия ISO 17799

в) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях

г) Открытый стандарт, определяющий цели контроля

10. К угрозам какого характера относятся действия направленные на сотрудников компании с целью получения конфиденциальной информации?

Ответ: Организационного

11. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

Ответ: Целостность

12. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

а) Анализ связующего дерева

б) AS/NZS

в) NIST

г) Анализ сбоев и дефектов

13. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

Ответ: Защищаемой

14. Защита информации от утечки — это деятельность по предотвращению:

а) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

б) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

в) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

г) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

д) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

15. Способ представления информации в вычислительных системах

Ответ: Двоичный код

16. Доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации

Ответ: Несанкционированным доступом

17. К посторонним лицам нарушителям информационной безопасности относится:

а) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;

б) персонал, обслуживающий технические средства;

в) технический персонал, обслуживающий здание;

г) пользователи;

д) сотрудники службы безопасности.

е) представители конкурирующих организаций.

ё) лица, нарушившие пропускной режим;

18. Утечкой информации в системе называется ситуация, характеризуемая:
Ответ: Потерей данных в системе

3.7 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

3.8 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.

Оценочное средство «Тест».

Тестирование с применением компьютерных технологий проводится по окончанию каждого семестра и по окончанию изучения дисциплины 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 каждого семестра и 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»

3.9 Перечень типовых практических заданий к зачету

(для оценки навыков и (или) опыта деятельности)

1. Характеристики информации, применительно к задачам защиты.
2. Информационная безопасность в условиях функционирования в России глобальных сетей.
3. Основные задачи информационной безопасности.

4. Основные методы обеспечения защиты информационной системы.
5. Определение и классификация угроз.
6. Классификация угроз и методы минимизации последствий.
7. Классификация нарушителей: пользователи, хакеры, специальные агентства
8. Непосредственные и косвенные каналы утечки.
9. Характеристика атак.
10. Подходы к обеспечению информационной безопасности.
11. Принципы обеспечения информационной безопасности.
12. Формальные модели доступа к данным.
13. Монитор безопасности и его функции.
14. Административный уровень защиты информации.
15. Разработка и реализация политики безопасности.
16. Таксономия нарушений информационной безопасности вычислительной системы
17. Анализ способов нарушений безопасности.
18. Основные нормативные руководящие документы
19. Место информационной безопасности экономических систем в национальной безопасности страны.

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) 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.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Собеседование	Собеседование, предусмотренное рабочей программой дисциплины, проводится на практическом занятии. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся тему, вопросы для подготовки к собеседованию. Результаты собеседования преподаватель доводит до обучающихся сразу после завершения собеседования
Ситуационная задача	Преподаватель не мене, чем за неделю до срока решения ситуационных задач должен довести до сведения обучающихся предлагаемые ситуационные задачи. Решенные ситуационные задачи в назначенный срок сдаются на проверку преподавателю
Сообщение	Защита сообщений, предусмотренных рабочей программой дисциплины, проводится во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему сообщений и требования, предъявляемые к их выполнению и защите
Доклад	Защита докладов, предусмотренных рабочей программой дисциплины, проводится во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему докладов и требования, предъявляемые к их выполнению и защите
Творческое задание	Творческие задания выдаются на практических занятиях, предшествующих изучению предлагаемой темы. Задания выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет. Индивидуальные задания должны быть выполнены в установленный преподавателем срок и в соответствии с требованиями к оформлению (текстовой и графической частей), сформулированными в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль» (в последней редакции). Выполненные задания в назначенный срок сдаются на проверку

Для организации и проведения промежуточной аттестации 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 и типовые практические задания разного уровня сложности для проведения промежуточной аттестации 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. 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	Шкала оценивания
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 проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач или в форме компьютерного тестирования.

Промежуточная аттестация в форме зачета с проведением аттестационного испытания проходит на последнем занятии по дисциплине.

При проведении промежуточной аттестации в форме компьютерного тестирования вариант тестового задания формируется из фонда тестовых заданий по дисциплине случайным образом, но с условием: 50 % заданий должны быть заданиями открытого типа и 50 % заданий – закрытого типа.