ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом и.о. ректора
от «17» июня 2022 г. № 77

Б1.В.ДВ.05.01 Введение в специальность

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. – 3
Часов по учебному плану (УП) – 108

Формы промежуточной аттестации
очная форма обучения:
зачет 2 семестр

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

Семестр	2	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	68	**68**
– лекции	34	**34**
– практические (семинарские)	34	**34**
– лабораторные		
Самостоятельная работа	40	**40**
Итого	108	**108**

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, доцент (к.н.), С.П. Серёдкин
ассистент, Г.Н. Шурховецкий

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «17» июня 2022 г. № 12

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

1 ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цель дисциплины	
1	раскрытие основных положений государственного образовательного стандарта по специальности, структуры и организации учебного процесса и научно-исследовательской работы в рамках образовательной программы по дисциплине, а также изложение основополагающих принципов защиты информации
1.2 Задачи дисциплины	
1	изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации;
2	изучение образовательного стандарта по специальности, структуры и организации учебного процесса и научно-исследовательской работы в рамках образовательной программы по дисциплине
1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины	

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
Блок/часть ОПОП	Блок 1. Дисциплины / Часть, формируемая участниками образовательных отношений
2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины	
1	Дисциплина изучается на начальном этапе формирования компетенции
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.В.ДВ.03.01 Теория автоматов и формальных языков
2	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
3	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**
ПК-1 Способен проектировать системы защиты информации автоматизированных систем	ПК-1.1 Формулирует структуру и этапы построения решений по защите информации в автоматизированных системах	Знать: структуру и этапы построения решений по защите информации в автоматизированных системах
		Уметь: формулировать структуру и этапы построения решений по защите информации в автоматизированных системах
		Владеть: знаниями по формулированию структуры и этапов построения решений по защите информации в автоматизированных системах

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. Сущность и значение специальности «Информационная безопасность автоматизированных систем».**						
1.1	Основы информационной безопасности: введение в понятия, принципы и задачи информационной безопасности. Рассмотрение основных угроз, рисков и противодействия им.	2	5	5		6	ПК-1.1
1.2	Криптография и защита информации: основные принципы криптографии, алгоритмы шифрования, симметричное и асимметричное шифрование, электронная подпись, протоколы защиты информации.	2	5	5		6	ПК-1.1
1.3	Сетевая безопасность: основы построения безопасных сетей, фаерволы (firewall), внутренняя и внешняя защита сетевых ресурсов, обнаружение и анализ инцидентов, протоколы защиты сетевого трафика.	2	5	5		6	ПК-1.1
1.4	Защита операционных систем: угрозы, связанные с операционными системами, безопасность серверов и рабочих станций, аутентификация и авторизация, защита от вредоносного ПО.	2	5	5		6	ПК-1.1

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
1.5	Безопасность приложений: основы создания безопасных приложений, уязвимости веб-приложений, SQL-инъекции, кросс-сайтовые скрипты, принципы безопасного программирования.	2	5	5		6	ПК-1.1
1.6	Управление информационной безопасностью: планирование, организация и контроль информационной безопасности в организации, стандарты и методологии управления информационной безопасностью, аудит и мониторинг.	2	5	5		5	ПК-1.1
1.7	Этические и правовые аспекты информационной безопасности: этический кодекс профессионала информационной безопасности, правовые нормы и требования, ответственность и последствия нарушений в области информационной безопасности.	2	4	4		5	ПК-1.1
	Форма промежуточной аттестации – зачет	2					ПК-1.1
	Итого часов (без учёта часов на промежуточную аттестацию)		34	34		40	

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	Теоретические и прикладные вопросы реализации проектов в области информационной безопасности. Материалы межвузовской научно-теоретической конференции (в рамках Сибирского форума «Информационная безопасность – 2021»), 29 ноября – 3 декабря 2021 г. : материалы конференции / . Новосибирск : СибГУТИ, 2021. - 153с. - Текст: электронный. - URL: https://e.lanbook.com/book/257288 (дата обращения: 19.04.2023)	Онлайн
6.1.1.2	Бурова, М.А. Информационная безопасность и защита информации. Часть 1 : конспект лекций / рец.: М. А. Кораблин, А. П. Долгинцев. Самара : СамГУПС, 2012. - 150с. - Текст: электронный. - URL: https://umczdt.ru/books/1311/263437/	Онлайн
6.1.1.3	Бурова, М.А. Информационная безопасность и защита информации. Часть 2 : конспект лекций / рец.: М. А. Кораблин, А. П. Долгинцев. Самара : СамГУПС, 2012. - 150с. - Текст: электронный. - URL: https://umczdt.ru/books/1311/263434/	Онлайн
6.1.1.4	Шаньгин, В. Ф. Информационная безопасность :/ В. Ф. Шаньгин. Москва : ДМК Пресс, 2014. - 702с. - Текст: электронный. - URL: http://e.lanbook.com/books/element.php?pl1_id=50578 (дата обращения: 19.04.2023)	Онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Защита и обработка конфиденциальных документов : практикум. направление подготовки 10.03.01 – информационная безопасность. бакалавриат / . Ставрополь : СКФУ, 2016. - 116с. - Текст: электронный. - URL: https://e.lanbook.com/book/155221 (дата обращения: 19.04.2023)	Онлайн
6.1.2.2	Информационная безопасность цифровой экономики. Материалы XVII научно-теоретической конференции VIII Пленума регионального отделения Федерального учебнометодического объединения в системе высшего	Онлайн

	образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» по Сибирскому и Дальневосточному федеральным округам (СибРОУМО), 13 октября – 15 октября 2021 г. : материалы конференции / . Новосибирск : СибГУТИ, 2021. - 124с. - Текст: электронный. - URL: https://e.lanbook.com/book/257252 (дата обращения: 19.04.2023)	
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	Серёдкин С.П., Шурховецкий Г.Н. Методические указания по изучению дисциплины Б1.В.ДВ.05.01 Введение в специальность по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация Безопасность открытых информационных систем / С.П. Серёдкин, Г.Н. Шурховецкий ; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 13 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_327_1529_2022_1_signed.pdf	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Электронно-библиотечная система «Образовательная платформа ЮРАЙТ», https://urait.ru/	
6.2.2	Научная электронная библиотека eLIBRARY.RU — https://elibrary.ru/	
6.2.3	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/	
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	MathCAD_student 15.0 Academic_License, Customer Number 434692, контракт от 03.12.2012 № 0334100010012000148-0000756-01	
6.3.2.2	Python 3.9, свободно распространяемое программное обеспечение https://docs.python.org/3/license.html	
6.3.2.3	Dev-C++, свободная интегрированная среда разработки приложений для языков программирования C/C++, https://code-live.ru/post/dev-cpp-free-cpp-ide-for-windows/	
6.3.2.4	MatLab Classroom, R2015a, R2015b, контракт от 09.07.2014 № 0334100010014000028-0000756-01.	
6.3.2.5	MatLab Classroom, R2010a, R2010b, лицензия от 16.03.2011 № 689810, ГК № 0334100010011000032-00000756-01.	
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-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)
3	Учебная аудитория Д-417 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	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
Лабораторная работа	Основной целью лабораторных работ является теоретическое обоснование, наглядное и/или экспериментальное подтверждение и/или проверка существенных теоретических положений (законов, закономерностей) анализ существующих методик и методов их реализации и т.д. Они занимают преимущественное место при изучении дисциплин обязательной части и части, формируемой участниками образовательных отношений Блока 1. Исходя из цели, содержанием лабораторных работ могут быть: - экспериментальная проверка формул, методик расчета; - проведение натурных измерений свойств, рабочих параметров, режимов работы при помощи лабораторного оборудования и/или стендов и макетов; - ознакомление, анализ и теоретические выкладки по устройству, принципу действия и способам обслуживания аппаратов, деталей машин, механизмов, процессов, протекающих в них при этом и т.д.; - наглядная графическая интерпретация чертежей, схем, объемных поверхностей и т.д., воспроизводимых с помощью специализированного программного обеспечения; - имитационное моделирование процессов, протекающих в сложных химических, физических, механических, электрических и пр. объектах;

	- наглядное представление о работе персонала конкретной организации или подразделения ОАО «РЖД» посредством моделирования штатных и внештатных ситуаций в виртуальных специализированных АРМ (автоматизированных рабочих мест); - установление и подтверждение закономерностей (путем сравнения проведенного эксперимента и рассчитанных значений) и т.д.; - ознакомление с методиками проведения экспериментов, наглядным устройством стенд-макетов и пр.; - установление свойств веществ, их качественных и количественных характеристик; - анализ различных характеристик процессов, в том числе производственных и иных процессов; - расчет параметров различных явлений и процессов, смоделировать которые не возможно в реальных условиях (например, чрезвычайные ситуации и пр.); - наблюдение развития явлений, процессов и др. Допускается иное содержание лабораторных работ, если это будет способствовать реализации целей и задач дисциплины и формированию соответствующих компетенций. По характеру выполняемых лабораторных работ возможны: - ознакомительные работы, используемые для закрепления изученного теоретического материалы; - аналитические работы, используемые для получения новой информации на основе формализованных методов; - творческие работы, ориентированные на самостоятельный выбор подходов решения задач. Прежде, чем приступить к лабораторным занятиям, обучающимся необходимо повторить теоретический материал по теме работы. Каждая лабораторная работа оснащена методическими указаниями, разработанными преподавателями, ведущими дисциплину
Самостоятельная работа	Обучение по дисциплине «Введение в специальность» 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 «Введение в специальность» участвует в формировании компетенций:

ПК-1. Способен проектировать системы защиты информации автоматизированных систем

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
2 семестр				
1.0	**Раздел 1. Сущность и значение специальности «Информационная безопасность автоматизированных систем»**			
1.1	Текущий контроль	Основы информационной безопасности: введение в понятия, принципы и задачи информационной безопасности. Рассмотрение основных угроз, рисков и противодействия им.	ПК-1.1	Доклад (устно) Реферат (письменно) Аудирование (устно/письменно) Дебаты (устно)
1.2	Текущий контроль	Криптография и защита информации: основные принципы криптографии, алгоритмы шифрования, симметричное и асимметричное шифрование, электронная подпись, протоколы защиты информации.	ПК-1.1	Доклад (устно) Реферат (письменно) Аудирование (устно/письменно) Дебаты (устно)
1.3	Текущий контроль	Сетевая безопасность: основы построения безопасных сетей, фаерволы (firewall), внутренняя и внешняя защита сетевых ресурсов, обнаружение и анализ инцидентов, протоколы защиты сетевого трафика.	ПК-1.1	Доклад (устно) Реферат (письменно) Аудирование (устно/письменно) Дебаты (устно)
1.4	Текущий контроль	Защита операционных систем: угрозы, связанные с операционными системами, безопасность серверов и рабочих станций, аутентификация и авторизация, защита от вредоносного ПО.	ПК-1.1	Доклад (устно) Реферат (письменно) Аудирование (устно/письменно) Дебаты (устно)
1.5	Текущий контроль	Безопасность приложений: основы создания безопасных приложений, уязвимости веб-приложений, SQL-инъекции, кросс-сайтовые скрипты, принципы безопасного программирования.	ПК-1.1	Доклад (устно) Реферат (письменно) Аудирование (устно/письменно) Дебаты (устно)
1.6	Текущий контроль	Управление информационной безопасностью: планирование, организация и контроль информационной безопасности в организации, стандарты и методологии управления информационной безопасностью, аудит и мониторинг.	ПК-1.1	Доклад (устно) Реферат (письменно) Аудирование (устно/письменно) Дебаты (устно)
1.7	Текущий контроль	Этические и правовые аспекты информационной безопасности:	ПК-1.1	Доклад (устно) Реферат (письменно)

		этический кодекс профессионала информационной безопасности, правовые нормы и требования, ответственность и последствия нарушений в области информационной безопасности.		Аудирование (устно/письменно) Дебаты (устно)
	Промежуточная аттестация		ПК-1.1	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	Дебаты	Оценочные средства, позволяющие включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения. Может быть использовано для оценки знаний и умений обучающихся	Перечень дискуссионных тем для проведения дебатов
2	Реферат	Продукт самостоятельной работы обучающегося, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор реферата раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. Может быть использовано для оценки знаний и умений обучающихся	Темы рефератов
3	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

4	Аудирование	Средство, позволяющее оценивать умение понимать основное содержание аудиотекстов и наиболее значимые факты аутентичной специальной аудио и видеоинформации с последующим выполнением дидактической задачи. Может быть использовано для оценки умений обучающихся	Оригинальные неадаптированные аудио и видеоматериалы с заданиями к ним

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 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
«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

Дебаты

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Выбранная обучающимся тема (проблема) актуальна в данном курсе; представлен подробный план-конспект, в котором отражены вопросы для дебатов; временной регламент обсуждения обоснован; даны возможные варианты ответов; использованы примеры из науки и практики
«хорошо»		Выбранная обучающимся тема (проблема) актуальна в данном курсе; представлен сжатый план-конспект, в котором отражены вопросы для диспута; временной регламент обсуждения обоснован; отсутствуют возможные варианты ответов; приведен один пример из практики
«удовлетворительно»		Выбранная обучающимся тема (проблема) недостаточно актуальна в данном курсе; представлен содержательно краткий план-конспект, в котором отражены вопросы для диспута; отсутствует временной регламент обсуждения; отсутствуют возможные варианты ответов; отсутствуют примеры из практики
«неудовлетворительно»	«не зачтено»	Выбранная обучающимся тема (проблема) не актуальна для данного курса; частично представлены вопросы для диспута; отсутствует временной регламент обсуждения; отсутствуют возможные варианты ответов; отсутствуют примеры из практики

Реферат

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы
«хорошо»		Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы
«удовлетворительно»		Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод
«неудовлетворительно»	«не зачтено»	Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы. Реферат обучающимся не представлен

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

Аудирование

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Обучающийся понял основные факты, сумел выделить отдельную, значимую для себя информацию, догадался о значении части незнакомых слов по контексту, сумел использовать информацию для решения поставленной задачи
«хорошо»		Обучающийся понял не все основные факты. При решении коммуникативной задачи он использовал только 2/3 информации
«удовлетворительно»		Обучающийся понял только 50% текста. Отдельные факты понял неправильно. Не сумел полностью решить поставленную перед ним коммуникативную задачу
«неудовлетворительно»	«не зачтено»	Обучающийся понял менее 50% текста и выделил из него менее половины основных фактов. Не смог решить поставленную перед ним речевую задачу

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

3.1 Типовые контрольные задания для проведения дебатов

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

Ниже приведен образец типовых вариантов заданий для проведения дебатов.

Образец вопросов для проведения дебатов
«Тема 6. Управление информационной безопасностью: планирование, организация и контроль информационной безопасности в организации, стандарты и методологии управления информационной безопасностью, аудит и мониторинг.»

1. Какие основные принципы управления информационной безопасностью следует придерживаться в организации?
2. Какие стандарты и методологии управления информационной безопасностью существуют и какие применяются в современных организациях?
3. Какие основные шаги необходимо предпринять при планировании мер по

обеспечению информационной безопасности в организации?
4. Каким образом организации могут проводить аудит информационной безопасности и какие методы используются для оценки уровня защищенности данных?
5. Какие инструменты и технологии можно применять для мониторинга информационной безопасности в реальном времени?
6. Каким образом организации могут реагировать на инциденты информационной безопасности и какие процедуры следует предпринимать в случае возникновения угрозы или нарушения безопасности данных?
7. Каким образом управление информационной безопасностью влияет на бизнес-процессы и стратегическое развитие организации?
8. Какие основные вызовы и проблемы могут возникнуть при реализации системы управления информационной безопасностью, и как их можно преодолеть?
9. Каким образом обучение и осведомленность сотрудников о вопросах информационной безопасности могут повлиять на уровень защиты организации от угроз?
10. Какие успешные примеры реализации системы управления информационной безопасностью существуют в современном бизнесе?

Эти вопросы покрывают основные аспекты управления информационной безопасностью и могут быть использованы для проведения дебатов на данную тему.

3.2 Типовые контрольные темы для написания рефератов

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.
Ниже приведен образец типовых вариантов вариантов тем для написания рефератов.

Образец тем рефератов
«Тема 2. Криптография и защита информации: основные принципы криптографии, алгоритмы шифрования, симметричное и асимметричное шифрование, электронная подпись, протоколы защиты информации.»

1. **Основы Криптографии и ее Роль в Защите Информации:** В этом реферате можно рассмотреть основные принципы криптографии и как она используется для защиты информации. Обсудить историю криптографии и ее развитие до современных методов.
2. **Симметричное и Асимметричное Шифрование:** Этот реферат может сосредоточиться на сравнении симметричных и асимметричных алгоритмов шифрования. Объяснить, как они работают, и когда лучше использовать один тип шифрования вместо другого.
3. **Электронная Подпись и Ее Роль в Защите Документов:** В этом реферате можно рассмотреть, как работает электронная подпись, и как она помогает обеспечить целостность и аутентичность документов. Также можно обсудить применение электронных подписей в различных областях, таких как электронная коммерция и правительственные документы.
4. **Протоколы Защиты Информации:** Этот реферат может охватить различные протоколы, используемые для защиты информации, включая SSL/TLS для безопасных соединений в Интернете, протоколы аутентификации и протоколы защиты электронной почты.
5. **Защита Информации в Сфере Кибербезопасности:** В этом реферате можно сосредоточиться на современных вызовах и методах защиты информации в контексте кибербезопасности. Обсудить методы борьбы с хакерами и вредоносным программным обеспечением, а также меры предосторожности для предотвращения утечек данных.
6. **Защита Информации в Мобильных Приложениях:** Этот реферат может рассмотреть специфические аспекты защиты информации в мобильных приложениях,

включая шифрование данных на устройствах и защиту от атак на приложения.

Эти темы позволяют более глубоко изучить различные аспекты криптографии и защиты информации, и их можно использовать в рефератах или исследованиях.

7. **Блокчейн и Криптография:** Рассмотрите, как криптография используется в технологии блокчейн для обеспечения безопасности и надежности децентрализованных систем.
8. **Защита Информации в Облаке:** Исследуйте методы и технологии для защиты данных, хранящихся в облачных сервисах, и рассмотрите риски, связанные с облачным хранением информации.
9. **Квантовая Компьютерная Угроза для Криптографии:** Обсудите потенциальные угрозы, которые представляют для существующих криптографических методов развитие квантовых компьютеров, и возможные меры по защите информации.
10. **Защита Информации в Интернете Вещей (IoT):** Исследуйте уникальные проблемы и решения, связанные с обеспечением безопасности в мире IoT, включая умные устройства и сети.
11. **Криптовалюты и Криптография:** Рассмотрите, как криптография играет важную роль в функционировании криптовалют, таких как Биткоин, и как обеспечивается их безопасность.
12. **Защита Личных Данных и Конфиденциальности:** Обсудите вопросы, связанные с защитой личных данных и приватности в цифровой эпохе, а также инструменты и методы для обеспечения конфиденциальности.
13. **Стеганография и Ее Роль в Скрытии Информации:** Рассмотрите стеганографию как метод скрытия информации в изображениях, аудио и видеофайлах, и ее использование в защите данных.
14. **Кибератаки и Криптография:** Исследуйте роль криптографии в предотвращении и реагировании на кибератаки, включая защиту от DDoS и атак на серверы.
15. **Этические и Юридические Аспекты Криптографии:** Рассмотрите этические и юридические вопросы, связанные с использованием криптографии, включая вопросы правительственного надзора и персональной свободы.
16. **Обзор Современных Криптографических Тенденций и Направлений:** Обобщите актуальные тенденции и направления в области криптографии, включая новые методы и вызовы.

Эти темы предоставляют широкий спектр аспектов, связанных с криптографией и защитой информации, и могут быть использованы для подготовки интересных и информативных рефератов.

3.3 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

«Тема 3. Сетевая безопасность: основы построения безопасных сетей, фаерволы (firewall), внутренняя и внешняя защита сетевых ресурсов, обнаружение и анализ инцидентов, протоколы защиты сетевого трафика.»

1. **Основы Сетевой Безопасности:** В этом докладе можно представить основные понятия и принципы сетевой безопасности, объяснить, почему она важна для организаций и какие угрозы могут возникнуть.
2. **Роль Фаерволов в Сетевой Безопасности:** Исследуйте, как работают фаерволы и как они используются для защиты сетей. Рассмотрите различные типы фаерволов и их применение.
3. **Внутренняя и Внешняя Защита Сетевых Ресурсов:** Обсудите методы и технологии, используемые для обеспечения безопасности внутри сети организации и

на граничных точках с внешней средой.

4. **Обнаружение и Анализ Сетевых Инцидентов:** Рассмотрите процессы обнаружения и анализа инцидентов в сетях, включая методы мониторинга и инструменты для выявления аномалий.
5. **Протоколы Защиты Сетевого Трафика:** Исследуйте различные протоколы и меры, используемые для защиты сетевого трафика, такие как VPN, IPSec и SSL/TLS.
6. **Управление Уязвимостями в Сетях:** Обсудите методы управления уязвимостями в сетях, включая сканирование уязвимостей и патч-менеджмент.
7. **Безопасность Беспроводных Сетей:** Рассмотрите угрозы и методы обеспечения безопасности в беспроводных сетях, таких как Wi-Fi, и сравните различные методы шифрования.
8. **Примеры Сетевых Инцидентов и Их Расследование:** Представьте реальные случаи сетевых инцидентов и расскажите, как они были обнаружены, анализированы и устранены.
9. **Сетевая Безопасность в Облаке:** Исследуйте уникальные вызовы и методы обеспечения безопасности данных в облачных средах.
10. **Развитие Трендов в Сетевой Безопасности:** Обобщите современные тенденции и вызовы в области сетевой безопасности, такие как защита от распределенных атак и IoT-устройств.

Эти темы позволяют более глубоко изучить различные аспекты сетевой безопасности и могут быть использованы для подготовки информативных докладов.

3.4 Типовые контрольные задания для проведения аудирования

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

Ниже приведен образец типовых вариантов заданий по аудированию.

Образец задания для проведения аудирования
«Тема 7. Этические и правовые аспекты информационной безопасности: этический кодекс профессионала информационной безопасности, правовые нормы и требования, ответственность и последствия нарушений в области информационной безопасности.»

Задание для аудирования 1

Название темы: Этические и правовые аспекты информационной безопасности
Цель: Оценить уровень понимания студентами этических и правовых аспектов в области информационной безопасности.
Инструкции:

1. Вам будет предложено прослушать аудиозапись лекции на тему "Этические и правовые аспекты информационной безопасности." Вам следует внимательно слушать лекцию и делать записи по ключевым пунктам.
2. После прослушивания лекции, вам будут предложены вопросы. Ответьте на каждый вопрос, используя информацию, которую вы услышали в лекции.

Вопросы:

1. Какие основные принципы включает в себя этический кодекс профессионала информационной безопасности?
2. Какие правовые нормы и требования регулируют информационную безопасность?
3. Какие могут быть последствия нарушений в области информационной безопасности с юридической точки зрения?
4. Почему важно соблюдать этические и правовые нормы в работе с информационной безопасностью?
5. Какие шаги можно предпринять, чтобы минимизировать риски нарушений информационной безопасности в организации?

Заметки:

- Обратите внимание на ключевые термины и примеры, упомянутые в лекции.

- Ваши ответы должны быть краткими, но информативными.
- У вас будет ограниченное время для ответов на вопросы, поэтому используйте свои записи для поддержки ответов.

Это задание поможет оценить знание студентов по важным аспектам этики и права в области информационной безопасности.

Задание для аудирования 2
Название темы: Этические и правовые аспекты информационной безопасности
Цель: Проверить понимание студентами основных этических и правовых аспектов в сфере информационной безопасности.
Инструкции:

1. Вам будет предложено прослушать интервью с экспертом в области информационной безопасности. Пожалуйста, слушайте внимательно и делайте записи по ключевым моментам и выводам эксперта.
2. По окончании интервью, вам будут предложены вопросы. Ответьте на каждый вопрос, используя информацию из интервью.

Вопросы:

1. Какие основные принципы и ценности связаны с этическими аспектами информационной безопасности, о которых упоминал эксперт?
2. Какие современные вызовы и угрозы информационной безопасности существуют согласно мнению эксперта?
3. Какие советы или рекомендации предоставил эксперт по соблюдению этики и правовых норм в работе с информационной безопасностью?
4. Какие юридические последствия могут возникнуть в случае нарушения правовых норм в области информационной безопасности, как указал эксперт?
5. Какие шаги можно предпринять, чтобы подготовиться к этическим и юридическим аспектам информационной безопасности в профессиональной карьере?

Заметки:

- Постарайтесь выделить ключевые советы и рекомендации эксперта.
- Ваши ответы должны быть краткими и отражать основную суть сказанного в интервью.
- Помните о важности этического и юридического соблюдения в сфере информационной безопасности.

Это задание поможет проверить, насколько студенты понимают и могут применять этические и правовые аспекты в области информационной безопасности, а также обобщить информацию из интервью с экспертом.

Задание для аудирования 3
Название темы: Этические и правовые аспекты информационной безопасности
Цель: Оценить знание студентами ключевых аспектов этики и законодательства в области информационной безопасности.
Инструкции:

1. Вам будет предложено прослушать диалог между двумя экспертами в области информационной безопасности. Внимательно слушайте и делайте заметки по важным моментам, которые будут обсуждаться.
2. По окончании диалога, вам будут заданы вопросы. Ответьте на каждый вопрос, используя информацию из диалога.

Вопросы:

1. Какие основные этические принципы были подчеркнуты экспертами в контексте информационной безопасности?
2. Какие правовые нормы и законы, согласно диалогу, имеют решающее значение для обеспечения информационной безопасности?

3. Какие могут быть последствия для организации при несоблюдении законодательства в области информационной безопасности, о которых говорили эксперты?
4. Какие стратегии и методы, упомянутые в диалоге, можно использовать для соблюдения этических и правовых норм в информационной безопасности?
5. Какова роль профессионалов информационной безопасности в обеспечении соблюдения этики и законодательства?

Заметки:

- Обратите внимание на примеры и иллюстрации, представленные в диалоге.
- Ваши ответы должны быть лаконичными, но информативными.
- Уделите особое внимание соблюдению этических и правовых аспектов информационной безопасности в контексте профессиональной деятельности.

Это задание поможет студентам лучше понять и оценить важность соблюдения этических и юридических аспектов в информационной безопасности, а также применять эти знания на практике.

3.5 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
ПК-1.1	Основы информационной безопасности: введение в понятия, принципы и задачи информационной безопасности. Рассмотрение основных угроз, рисков и противодействия им.	Один или несколько вариантов ответов	3
		Короткий ответ	3
		Развёрнутый ответ	3
ПК-1.1	Криптография и защита информации: основные принципы криптографии, алгоритмы шифрования, симметричное и асимметричное шифрование, электронная подпись, протоколы защиты информации.	Соответствие	3
		Последовательность	3
		Заполнение пропусков	3
ПК-1.1	Сетевая безопасность: основы построения безопасных сетей, фаерволы (firewall), внутренняя и внешняя защита сетевых ресурсов, обнаружение и анализ инцидентов, протоколы защиты сетевого трафика.	Логическая задача	3
		Ситуационная	3
		Один или несколько вариантов ответов	3
ПК-1.1	Защита операционных систем: угрозы, связанные с операционными системами, безопасность серверов и рабочих станций, аутентификация и авторизация, защита от вредоносного ПО.	Короткий ответ	3
		Развёрнутый ответ	3
		Соответствие	3
ПК-1.1	Безопасность приложений: основы создания безопасных приложений, уязвимости веб-приложений, SQL-инъекции, кросс-сайтовые скрипты, принципы безопасного программирования.	Последовательность	3
		Заполнение пропусков	3
		Логическая задача	3
ПК-1.1	Управление информационной безопасностью: планирование, организация и контроль информационной безопасности в организации, стандарты и методологии управления информационной безопасностью, аудит и мониторинг.	Ситуационная	3
		Один или несколько вариантов ответов	3
		Короткий ответ	3
ПК-1.1	Этические и правовые аспекты информационной безопасности: этический кодекс профессионала информационной безопасности, правовые нормы и требования, ответственность и последствия нарушений в области информационной безопасности.	Развёрнутый ответ	3
		Соответствие	3
		Последовательность	3
		Итого	63

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.

Один или несколько вариантов ответов:

1. Вопрос: Какие из перечисленных элементов являются основными компонентами информационной безопасности?
   - ☐ Антивирусное ПО
   - ☑ Аутентификация
   - ☑ Шифрование
   - ☐ Процессор
   - ☑ Бекапы
2. Вопрос: Какие виды атак могут быть направлены на информационные системы?
   - ☑ DDoS-атаки
   - ☑ Фишинг
   - ☐ Восстановление данных
   - ☑ SQL-инъекции
   - ☐ Оптимизация производительности
3. Вопрос: Какие из следующих принципов информационной безопасности относятся к конфиденциальности данных?
   - ☑ Необходимость-зависимость
   - ☐ Целостность
   - ☑ Разграничение доступа
   - ☐ Надежность

Короткий ответ:

4. Вопрос: Что такое биометрическая аутентификация?

Ответ: Это метод аутентификации, использующий биологические характеристики человека, такие как отпечаток пальца или сканирование сетчатки глаза, для проверки личности.

5. Вопрос: Что такое атака "Межсетевой экран"?

Ответ: Это атака, направленная на обход или проникновение через брандмауэр, используемый для защиты сети от несанкционированного доступа.

6. Вопрос: Что представляет собой "политика паролей"?

Ответ: Это набор правил и требований, определяющих, какие пароли допускаются для использования в информационной системе, и как они должны быть созданы и управляться.

Развёрнутый ответ:

7. Вопрос: Какова роль пожарной стены (firewall) в обеспечении информационной безопасности сети?

Ответ: Пожарная стена - это средство, используемое для фильтрации и контроля сетевого трафика между внутренней сетью и внешними сетями, такими как интернет. Её роль заключается в защите от несанкционированного доступа и вредоносных атак. Пожарная стена принимает решения о разрешении или блокировке сетевого трафика на основе заранее определенных правил и политик безопасности. Она также может выполнять проверку пакетов данных на наличие вредоносного содержимого, что помогает предотвратить атаки, такие как вирусы и вредоносное ПО.

8. Вопрос: Какие меры могут быть предприняты для защиты от социальной инженерии в контексте информационной безопасности?

Ответ: Защита от социальной инженерии важна, и её можно обеспечить путем обучения сотрудников на предмет определения и предотвращения манипуляций со стороны злоумышленников. Меры могут включать проведение обучения и тренингов по обнаружению фишинговых писем и манипуляциям, ограничение доступа к конфиденциальной информации для непривилегированных сотрудников, и установку политик, которые обязывают сотрудников проверять подлинность запросов на доступ к конфиденциальным данным.

9. Вопрос: Какой процесс следует пройти при разработке и реализации бизнес-континуитетного плана для обеспечения информационной безопасности?

Ответ: Процесс разработки бизнес-континуитетного плана (BCP) начинается с идентификации критических бизнес-процессов и ресурсов. Затем определяются потенциальные риски и уязвимости. На основе этой информации разрабатывается стратегия восстановления и план действий в случае чрезвычайных ситуаций. BCP также включает в себя процедуры для регулярного тестирования и обновления плана, чтобы обеспечить его актуальность и эффективность в случае реального инцидента.

Соответствие:

10. Вопрос: Сопоставьте типы атак с их описаниями:

- **DDoS-атака**
- **Фишинг**
- **SQL-инъекция**

Описания:

- ☐ Атака, направленная на обход брандмауэра.
- ☐ Атака, при которой злоумышленник пытается взломать базу данных, внедряя вредоносный код.
- ☐ Атака, при которой атакующий засылает большое количество запросов к цели с целью перегрузки её ресурсов.
- ☐ Атака, при которой злоумышленник выдает себя за надежное лицо и пытается получить конфиденциальную информацию у жертвы.

Последовательность:

11. Вопрос: Укажите последовательность этапов разработки политики информационной безопасности.

Ответ: Правильная последовательность:

1. Определение целей и области действия политики.
2. Сбор информации о рисках и уязвимостях.
3. Разработка политики и стандартов безопасности.
4. Утверждение политики руководством.
5. Обучение сотрудников и внедрение политики.
6. Регулярное обновление и адаптация политики к новым угрозам.

Заполнение пропусков:

12. Вопрос: В рамках процесса информационной безопасности, **авторизация** представляет собой процесс проверки личности пользователя и предоставления ему **доступа** к определенным ресурсам на основе его **роли** и **прав.**

Логическая задача:

13. Вопрос: Если организация обнаруживает, что хакер получил доступ к их внутренней сети и украл конфиденциальные данные, какие действия они должны предпринять? Объясните свои шаги.

Ответ: Организация должна предпринять следующие действия:

- Изолировать компрометированные системы: Остановить любой дальнейший доступ хакера к системам, отключив зараженные устройства или сегменты сети.
- Анализ инцидента: Провести детальное исследование инцидента, чтобы определить масштаб и методы атаки, а также определить, какие данные были скомпрометированы.

- Уведомление: В случае утечки конфиденциальных данных, уведомить органы регулирования и затронутых клиентов, чтобы соблюсти законодательные требования и уведомить сторонние лица о возможной угрозе для их данных.
- Восстановление: Очистить системы от вредоносного ПО, восстановить данные из резервных копий и укрепить системы безопасности, чтобы предотвратить подобные инциденты в будущем.
- Усиление безопасности: Проанализировать слабые места, которые привели к инциденту, и улучшить политики безопасности и меры контроля доступа.

Ситуационная:

14. Вопрос: Вашей компании поступил запрос на предоставление доступа к чувствительным данным от сотрудника, который забыл свой пароль. Какие шаги вы предпримете, чтобы проверить подлинность запроса и обеспечить безопасность данных?

Ответ: В данной ситуации:

- Проверьте подлинность запроса: Сначала удостоверьтесь, что запрос действительно исходит от сотрудника, проверяя его личность через дополнительные средства аутентификации, например, звонок на заранее известный телефонный номер сотрудника или личное посещение офиса.
- Примените политики безопасности: Убедитесь, что ваша компания следует установленным политикам и процедурам восстановления паролей, которые могут включать в себя проверку личности, а также регистрацию и аудит запросов на сброс пароля.
- Ограничьте доступ: Предоставьте временный доступ к данным, который будет отозван после восстановления пароля, чтобы минимизировать риски в случае нежелательного доступа.
- Обучение сотрудников: Обучите сотрудников правилам безопасности и процедурам восстановления паролей, чтобы предотвратить подобные ситуации в будущем.

3.2 Перечень теоретических вопросов к зачету

(для оценки знаний)

1. Что такое информационная безопасность, и какие основные аспекты она включает в себя?
2. Какие угрозы информационной безопасности существуют, и как классифицировать эти угрозы?
3. Какие принципы информационной безопасности существуют, и как они применяются в практике?
4. Что такое управление рисками в информационной безопасности, и какие этапы включает процесс управления рисками?
5. Какие методы аутентификации и авторизации используются для обеспечения доступа к информации?
6. Что такое криптография, и какие методы она предоставляет для защиты данных?
7. Какие законы и нормативные акты регулируют область информационной безопасности в вашей стране?
8. Что такое атаки на информационную безопасность, и какие виды атак существуют?
9. Какие методы обнаружения и предотвращения атак используются в информационной безопасности?
10. Какие основные принципы восстановления после инцидентов информационной безопасности?
11. Что такое социальная инженерия и какие методы могут использоваться социальными инженерами для атаки на информационную безопасность?
12. Какие методы и инструменты используются для мониторинга и анализа сетевой активности с целью выявления инцидентов информационной безопасности?
13. Какие основные принципы безопасной разработки программного обеспечения (Secure

SDLC) существуют, и какие этапы включает этот процесс?
14. Что такое внутренняя угроза информационной безопасности, и как она может быть обнаружена и предотвращена?
15. Какие методы шифрования данных на уровне хранения и передачи данных используются для защиты конфиденциальной информации?
16. Что представляет собой двухфакторная аутентификация, и какие преимущества она предоставляет по сравнению с однофакторной аутентификацией?
17. Какие стандарты и фреймворки используются для обеспечения информационной безопасности, например, ISO 27001 и NIST Cybersecurity Framework?
18. Что такое защита от внешних угроз, и какие средства защиты могут быть применены на периметре сети?
19. Какие меры безопасности рекомендуется применять при работе с облачными сервисами и хранилищами данных?
20. Какие основные принципы и практики обеспечения конфиденциальности, целостности и доступности данных существуют в информационной безопасности?

3.3 Перечень типовых простых практических заданий к зачету
(для оценки умений)

1. Создание пароля: Попросите студентов создать надежный пароль для учетной записи, следуя рекомендациям по безопасности.
2. Анализ угроз: Задайте ситуацию, где студентам нужно проанализировать возможные угрозы информационной безопасности для организации и предложить соответствующие меры по их минимизации.
3. Установка антивирусного ПО: Попросите студентов установить антивирусное программное обеспечение на виртуальную машину и выполнить сканирование файлов.
4. Настройка брандмауэра: Попросите студентов настроить брандмауэр на виртуальной машине и определить правила для блокировки или разрешения сетевых соединений.
5. Защита Wi-Fi: Предложите студентам настроить безопасную беспроводную сеть Wi-Fi, включая использование WPA2 или WPA3.
6. Шифрование данных: Попросите студентов зашифровать некоторый текст с использованием инструмента для шифрования и дешифрования данных.
7. Обучение пользователям: Предложите студентам разработать и провести короткую лекцию или обучающий вебинар о базовых принципах информационной безопасности для непрофессиональных пользователей.
8. Обнаружение уязвимостей: Задайте студентам задачу по поиску уязвимостей в предоставленном программном обеспечении и предложите меры для их устранения.
9. Исследование социальной инженерии: Попросите студентов провести исследование и подготовить отчет о методах социальной инженерии и способах защиты от нее.
10. Экстренное реагирование на инцидент: Предложите студентам сценарий инцидента информационной безопасности и попросите их разработать план экстренного реагирования.

3.4 Перечень типовых практических заданий к зачету
(для оценки навыков и (или) опыта деятельности)

1. Создание политики паролей: Попросите студентов разработать политику паролей для организации, учитывая требования к сложности паролей и периодичность их смены.
2. Сетевой анализ трафика: Дайте студентам задание проанализировать сетевой трафик на предмет аномалий с использованием инструментов анализа сетевого трафика.

3. Составление отчета о безопасности: Попросите студентов создать отчет о текущем состоянии безопасности информационных систем организации и предложить улучшения.
4. Тестирование на уязвимости: Предложите студентам провести тестирование на уязвимости веб-приложения с использованием инструментов для сканирования уязвимостей.
5. Управление доступом: Задайте студентам сценарий, в котором они должны настроить систему управления доступом с использованием ролей и прав.
6. Мониторинг безопасности: Попросите студентов настроить систему мониторинга безопасности и дать им живой поток событий для анализа и реагирования.
7. Логирование и анализ журналов: Дайте студентам журнал событий и попросите проанализировать его для выявления потенциальных инцидентов безопасности.
8. Эмуляция атаки: Предложите студентам эмулировать определенный вид атаки (например, атаку типа "фишинг") и разработать план защиты от нее.
9. Защита от вредоносных программ: Задайте студентам задачу установить антивирусное ПО и антиспайвар программное обеспечение, а затем провести сканирование и удаление вредоносных программ.
10. Разработка плана аварийного восстановления: Попросите студентов разработать план аварийного восстановления информационных систем организации и определить шаги для восстановления после инцидентов.

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

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.