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 «07» июня 2021 г. № 79

Б1.О.47 Теоретические основы компьютерной безопасности

рабочая программа дисциплины

Специальность/направление подготовки – 10.03.01 Информационная безопасность
Специализация/профиль – Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)
Квалификация выпускника – Бакалавр
Форма и срок обучения – очная форма 4 года
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 1 семестр

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

Семестр	1	**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

Электронный документ выгружен из ЕИС ФГБОУ ВО ИрГУПС и соответствует оригиналу
Подписант ФГБОУ ВО ИрГУПС Трофимов Ю.А.
00920FD815CE68F8C4CA795540563D259C с 07.02.2024 05:46 по 02.05.2025 05:46 GMT+03:00
Подпись соответствует файлу документа

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденным Приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 № 1427.

Программу составил(и):
старший преподаватель, А.С. Вергасов

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «4» июня 2021 г. № 11-2

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

1 ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цель дисциплины	
1	обучить обучающихся основным принципам и базовым методикам в области защиты информации (ЗИ), комплексного проектирования, построения, эксплуатации защищенных автоматизированных систем (АС)
1.2 Задачи дисциплины	
1	изучить возможности механизмов/сервисов ЗИ
2	изучить методические аспекты проектирования и построения защищенных АС
3	изучить критерии и методы оценки защищенности АС
4	изучить основы формирования политики информационной безопасности (ПИБ) АС предприятия
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	Дисциплина изучается на начальном этапе формирования компетенции
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.О.26 Теория информации
2	Б1.О.27 Основы информационной безопасности
3	Б1.О.33 Сети и системы передачи информации
4	Б1.О.36 Основы управления информационной безопасностью
5	Б1.О.40 Информационные технологии
6	Б1.О.50 Комплексная защита в информационных системах персональных данных
7	Б1.О.53 Методология построения защищенных автоматизированных систем
8	Б2.О.01(У) Учебная - ознакомительная практика
9	Б2.О.02(У) Учебная - учебно-лабораторная практика
10	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
11	Б3.02(Д) Защита выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей	ОПК-1.3 Имеет навыки применения методов и средств защиты информации для обеспечения объективных потребностей личности, общества и государства	Знать: основные понятия теории компьютерной безопасности; основные принципы обеспечения информационной безопасности (ИБ)
		Уметь: выделять информацию, подлежащую защите
		Владеть: навыками анализа информационных рисков

личности, общества и государства;		
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1 Знает основные требования к формированию политики информационной безопасности, программные средства скрытого информационного воздействия, утечки информации по техническим каналам	Знать: критерии защищенности АС
		Уметь: применять основные критерии защищенности АС; оценивать эффективность комплексной системы защиты информации (КСЗИ)
		Владеть: методологией разработки и реализации ПИБ
	ОПК-10.2 Умеет применять методы определения причин, видов, источников и каналов утечки, искажения информации, организовывает и поддерживает выполнение комплекса мер по обеспечению информационной безопасности	Знать: причины, виды и каналы утечки информации
		Уметь: проводить аудит ИБ
		Владеть: методикой реализации комплекса мер по обеспечению информационной безопасности
	ОПК-10.3 Имеет навыки работы технического специалиста по организации и обеспечению информационной безопасности компьютерных систем при обработке информации на объекте защиты	Знать: этапы создания КСЗИ
		Уметь: оценивать объём работ по реализации необходимых мероприятий
		Владеть: навыками работ при реализации ПИБ

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 понятия. Модель угроз безопасности информации. Критерии и классы защищенности.**						
1.1	Модели безопасности; понятие и струк-тура ПИБ	1	4	4		2	ОПК-1.3 ОПК-10.1
1.2	Критерии и классы защищенности средств вычислительной техники и АС в соответствии с руководящими докумен-тами Гостехкомиссии РФ. Стандарты по оценке защищенных систем	1	8	8		4	ОПК-1.3 ОПК-10.1
1.3	Примеры практической реализации; построение парольных систем	1	4	4		6	ОПК-1.3 ОПК-10.1
2.0	**Раздел 2. Примеры практической реализации методов защиты информации. Защита носителей информации. Построение парольных систем. Особенности применения криптографических методов защиты информации.**						
2.1	Особенности применения криптографических методов защиты информации; способы реализации криптографиче-ской подсистемы	1	6	6		8	ОПК-1.3 ОПК-10.2 ОПК-10.3
2.2	Методология обследования объекта и проектирования систем защиты	1	4	4		12	ОПК-1.3 ОПК-10.2 ОПК-10.3
2.3	. Методы построения защищенных АС; исследование корректности КСЗИ	1	8	8		8	ОПК-1.3 ОПК-10.2 ОПК-10.3
	Форма промежуточной аттестации – зачет	1					ОПК-1.3 ОПК-10.1

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ							
Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
							ОПК-10.2 ОПК-10.3
	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	Введение в специальность : методические указания к выполнению курсовой работы для студентов специальностей 10.05.01 «компьютерная безопасность», 10.05.02 «информационная безопасность телекоммуникационных систем», 10.05.03 «информационная безопасность автоматизированных систем» очной формы обучения. — Воронеж : ВГТУ, 2023. — 26 с. — URL: https://e.lanbook.com/book/383372 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.2	Документальное обеспечение информационной безопасности : учебное пособие для студентов, обучающихся по направлению 10.03.01 «информационная безопасность». — Севастополь : СевГУ, 2022. — 142 с. — URL: https://e.lanbook.com/book/261899 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.3	Конкин, Ю. В. Основы информационной безопасности : учебное пособие / Ю. В. Конкин, Ю. М. Кузьмин, В. Н. Пржегорлинский. — Рязань : РГРТУ, 2021. — 96 с. — URL: https://e.lanbook.com/book/220418 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.4	Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2024. — 324 с. — URL: https://e.lanbook.com/book/370967 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ 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	А.С. Вергасов. Методические указания по изучению дисциплины Б1.О.47 Теоретические основы компьютерной безопасности по направлению подготовки 10.03.01 Информационная безопасность, профиль Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности) / А.С. Вергасов; ИрГУПС. – Иркутск: ИрГУПС, 2023. – 13 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_9310_1480_2021_1_signed.pdf	Онлайн

6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»

6.2.1	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	прогр.средство защиты от НСД Secret Net4.0, клиент серв.безоп.Secret Net 4.0, сервер безопасности С Secret Net4.0, система разгр.доступа Dallas Lock 7.0
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- 623 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). Для проведения занятий имеются учебно-наглядные пособия (презентации).
4	Лаборатория Д-523 «Моделирование и разработка программных систем и защита информации».«Безопасность программно-аппаратных средств защиты информации» 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 (переносной), экран (переносной), компьютер измеритель шумов и вибрации 003-МЗ
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
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 «Теоретические основы компьютерной безопасности» 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 «Теоретические основы компьютерной безопасности» 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-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
1 семестр				
1.0	**Раздел 1. Основные понятия. Модель угроз безопасности информации. Критерии и классы защищенности**			
1.1	Текущий контроль	Модели безопасности; понятие и струк-тура ПИБ	ОПК-1.3 ОПК-10.1	Тестирование (компьютерные технологии)
1.2	Текущий контроль	Критерии и классы защищенности средств вычислительной техники и АС в соответствии с руководящими докумен-тами Гостехкомиссии РФ. Стандарты по оценке защищенных систем	ОПК-1.3 ОПК-10.1	Тестирование (компьютерные технологии)
1.3	Текущий контроль	Примеры практической реализации; построение парольных систем	ОПК-1.3 ОПК-10.1	Тестирование (компьютерные технологии)
2.0	**Раздел 2. Примеры практической реализации методов защиты информации. Защита носителей информации. Построение парольных систем. Особенности применения криптографических методов защиты информации**			
2.1	Текущий контроль	Особенности применения криптографических методов защиты информации; способы реализации криптографиче-ской подсистемы	ОПК-1.3 ОПК-10.2 ОПК-10.3	Тестирование (компьютерные технологии)
2.2	Текущий контроль	Методология обследования объекта и проектирования систем защиты	ОПК-1.3 ОПК-10.2 ОПК-10.3	Тестирование (компьютерные технологии)
2.3	Текущий контроль	. Методы построения защищенных АС; исследование корректности КСЗИ	ОПК-1.3 ОПК-10.2 ОПК-10.3	Тестирование (компьютерные технологии)
	Промежуточная аттестация	Все темы	ОПК-1.3 ОПК-10.1 ОПК-10.2 ОПК-10.3	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	Тестирование (компьютерные технологии)	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий

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	Базовый

	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	
	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

Тестирование

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования
«хорошо»		Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования
«удовлетворительно»		Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования
«неудовлетворительно»	«не зачтено»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

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

3.1 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-10.1	Модели безопасности; понятие и струк-тура ПИБ		5 – ОТЗ 5 – ЗТЗ

ОПК-1.3 ОПК-10.1	Критерии и классы защищенности средств вычислительной техники и АС в соответствии с руководящими докумен-тами Гостехкомиссии РФ. Стандарты по оценке защищенных систем		5 – ОТЗ 5 – ЗТЗ
ОПК-1.3 ОПК-10.1	Примеры практической реализации; построение парольных систем		5 – ОТЗ 5 – ЗТЗ
ОПК-1.3 ОПК-10.2 ОПК-10.3	Особенности применения криптографических методов защиты информации; способы реализации криптографиче-ской подсистемы		5 – ОТЗ 5 – ЗТЗ
ОПК-1.3 ОПК-10.2 ОПК-10.3	Методология обследования объекта и проектирования систем защиты		5 – ОТЗ 5 – ЗТЗ
ОПК-1.3 ОПК-10.2 ОПК-10.3	. Методы построения защищенных АС; исследование корректности КСЗИ		5 – ОТЗ 5 – ЗТЗ
		Итого	30 – ОТЗ 30 – ЗТЗ

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. «Несанкционированный доступ к информации» - это:

○ доступ, реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

○ доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств;

○ доступ с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация;

○ доступ к информации, реализуемый путём уничтожения технических средств информационной системы.

2. «Угроза информационной безопасности (ИБ)» - это

○ некоторая уязвимость АС;

○ потенциально возможное событие/действие, которое может нанести ущерб информации.

3. При реализации системой защиты мандатного принципа контроля доступа субъект может читать объект, только если иерархическая классификация субъекта _____, чем иерархическая классификация объекта:

○ больше;

○ меньше;

○ не больше;

○ не меньше.

4. Начиная с класса _____ требований ГТК РФ по защите информации в многопользова-тельских АС с различным уровнем доступа, необходимо управление потоками информа-ции:

○ 1Г

○ 2Б

○ 1В

○ 3А

○ 1Б
○ 2А
○ 3Б

5. «Сборка мусора» - это
○ поиск удаленной информации на носителях;
○ вскрытие шифров криптозащиты информации;
○ внедрение программных/аппаратных закладок.

6. Политика информационной безопасности – это
○ общий документ, где перечисляются правила доступа в хранилище информации;
○ набор документов, регламентирующих порядок хранения, обработки и передачи информации.

7. Модели разграничения доступа могут быть классифицированы следующим образом (выделить все верные варианты):
○ модели разграничения доступа, построенные по принципу предоставления прав;
○ модели разграничения доступа, использующие принципы математической статистики.
○ модели разграничения доступа, построенные на основе принципов теории информа-ции.

8. Основными типами моделей, построенных на предоставлении прав, являются модели (выделить все верные варианты
○ дискреционного доступа;
○ дискретного доступа;
○ мандатного доступа;
○ непрерывного доступа.

9. Модель Белла- ЛаПадула относится к классу моделей
○ дискреционного доступа;
○ дискретного доступа;
○ мандатного доступа.

10. Модель Биба контроля целостности имеет следующее количество вариаций;
○ 2;
○ 3;
○ 4.

11. Парольные системы аутентификации имеют следующий уровень стойкости:
○ низкий;
○ средний;
○ высокий.

12. Основная аксиома безопасности формулируется так:
○ все вопросы безопасности информации определяются доступами субъектов к объектам;
○ все вопросы безопасности информации определяются матрицей предоставления прав доступа субъектов к объектам;
○ все вопросы безопасности информации определяются правилами аутентификации и авторизации субъектов.

13. Определите последовательность следующих процедур (1-2-3):
○ авторизация субъекта (3);
○ аутентификация субъекта (2);
○ идентификация субъекта (1).

14. «Информационная система» - это:
○ совокупность информации, информационных технологий и технических средств;
○ совокупность информации, информационных технологий, технических средств и персонала, обслуживающего систему;
○ совокупность информационных технологий и технических средств;
○ совокупность информации, технических средств и персонала, обслуживающего информационную систему
○ совокупность информации, технических средств и персонала, обслуживающего и эксплуатирующего информационную систему.

15. Документ РД ГТК «Средства вычислительной техники (СВТ). Защита от НСД к

информации. Показатели защищенности от НСД к информации» определяет _____ классов защищенности СВТ:

○ 4
○ 5
○ 6
○ 7

16. Третья группа СВТ (РД ГТК «(СВТ). Защита от НСД к информации. Показатели защищенности от НСД к информации») характеризуется _____ защитой и содержит четвертый, третий и второй классы:

○ дискреционной:
○ ролевой;
○ мандатной;
○ непрерывной.

17. Дискреционный принцип контроля доступа для СВТ требуется для следующих показателей защищенности СВТ от НСД к информации (обозначить все варианты):

○ 1;
○ 2;
○ 4;
○ 5.

18. «Специальные исследования (специсследования)» - это:

○ выявление с помощью контрольно - измерительной аппаратуры возможных каналов утечки информации;

○ определение соответствия условий эксплуатации объектов информатизации требованиям аттестатов соответствия, и других руководящих документов по спецзащите без применения контрольно - измерительной аппаратуры;

○ проверки технических средств иностранного и совместного производства на наличие внедренных электронных устройств перехвата информации.

19. Пассивными способами защиты информации являются:

○ создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях технических средств.

○ ослабление наводок ПЭМИ в посторонних проводниках и соединительных линиях технических средств, выходящих за пределы контролируемой зоны.

20. Модель Харрисона -Руззо-Ульмана относится к классу моделей _____ (дискреционного) разграничения доступа.

21. Угроза ИБ всегда направлена на определенную _____ (уязвимость)АС.

22. ¬¬¬¬¬¬¬¬¬¬¬¬¬_____ (Подстановки) могут быть полиалфавитными и моноалфавитными.

23. Средство, осуществляющее перехват всех обращений субъектов к объектам и разграничивающее доступ в соответствии с заданным принципом разграничения доступа, называется _____ (диспетчером) доступа.

24. Выделяют 4 классических вида угроз безопасности информации: угрозы конфиденциальности, целостности, доступности и _____ (раскрытия) параметров АС.

25. Ал¬го¬ритм RSA опирается на следующий тип необратимых преобразований: разложения больших чисел на простые _____ (множители).

26. Алгоритм _____ (Диффи-Хэллмана) представляет собой метод получения секретного ключа для участников сессии обмена конфиденциальной информацией.

27. Одним из способов аутентификации является предъявление _____ (ключевого) носителя.

28. Существует ли абсолютно невскрываемый шифр? Если да, опишите его свойства.

29. Приведите правило Кергхоффа.

30. В чем заключаются основные проблемы симметричных криптосистем?

31. Что такое гаммирование?

32. Нарисуйте схему асимметричного шифрования.

33. Приведите требования к системам с открытым ключом.

3.2 Перечень теоретических вопросов к зачету

(для оценки знаний)

1. Краткие сведения о компонентах электронных систем обработки данных.
2. Функциональные назначения компонентов.
3. Модель АС и модели безопасности. Основные понятия.
4. Описание типовых ПИБ: модели разграничения доступа, построенные по принципу предоставления прав.
5. Описание типовых ПИБ: модели разграничения доступа - информационные модели.
6. Описание типовых ПИБ: модели разграничения доступа - вероятностные модели.
7. Описание типовых ПИБ: механизм защиты от отказа в обслуживании (DoS).
8. Понятия доступа, монитора безопасности.
9. Изолированная программная среда.
10. Требования к защите конфиденциальной информации.
11. Требования к защите секретной информации.
12. Зарубежные критерии безопасности АС (ITSEC, «Единые критерии»). Общие подходы к построению парольных систем защиты от НСДИ.
13. Требования к выбору паролей.
14. Средства криптографической защиты информации (СКЗИ). Требования к СКЗИ
15. Предварительное и динамическое шифрование.
16. Методы шифрования с симметричным ключом.
17. Системы шифрования с открытым ключом и электронной цифровой подписи
18. Этапы создания комплексной системы защиты информации.
19. Краткие сведения о компонентах электронных систем обработки данных.
20. Функциональные назначения компонентов.
21. Модель АС и модели безопасности. Основные понятия.
22. Описание типовых ПИБ: модели разграничения доступа, построенные по принципу предоставления прав.
23. Описание типовых ПИБ: модели разграничения доступа - информационные модели.
24. Описание типовых ПИБ: модели разграничения доступа - вероятностные модели.
25. Описание типовых ПИБ: механизм защиты от отказа в обслуживании (DoS).
26. Понятия доступа, монитора безопасности.
27. Изолированная программная среда.
28. Требования к защите конфиденциальной информации.
29. Требования к защите секретной информации.
30. Зарубежные критерии безопасности АС (ITSEC, «Единые критерии»). Общие подходы к построению парольных систем защиты от НСДИ.
31. Требования к выбору паролей.
32. Средства криптографической защиты информации (СКЗИ). Требования к СКЗИ
33. Предварительное и динамическое шифрование.
34. Методы шифрования с симметричным ключом.
35. Системы шифрования с открытым ключом и электронной цифровой подписи
36. Этапы создания комплексной системы защиты информации.
37. Математические основы моделей безопасности.
38. Элементы теории автоматов и графов. Модель «решетки». Основные виды моделей безопасности.
39. Модель Харрисона -Руззо-Ульмана.
40. Модель распространения прав доступа Take-Grant.
41. Расширенная модель Take-Grant.
42. Классическая модель Белла-ЛаПадула.
43. Монитор безопасности объектов. Монитор безопасности субъектов.
44. Изолированная программная среда.

3.3 Перечень типовых простых практических заданий к зачету

(для оценки умений)

1. Построить модель решетки
2. Построить модель ХРУи ТМД
3. Постротиь классическую модел TakeGrant

3.4 Перечень типовых практических заданий к зачету

(для оценки навыков и (или) опыта деятельности)

1. Построить расширенную модель TakeGrant
2. Построить модель СВС
3. Построить модель ролевого управления доступом

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
Тестирование (компьютерные технологии)	Тестирование проводится по результатам освоения тем или разделов дисциплины или по окончанию ее изучения во время практических занятий. Во время проведения тестирования пользоваться учебниками, справочниками, конспектами лекций, тетрадями для практических занятий не разрешено. Преподаватель на практическом занятии, предшествующем занятию проведения теста, доводит до обучающихся: темы, количество заданий в тесте, время выполнения. Результаты тестирования видны обучающемуся на компьютере сразу после прохождения теста

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.