ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

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

Б1.О.48 Теоретические основы компьютерной безопасности

рабочая программа дисциплины

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – № 5 Безопасность открытых информационных систем
Квалификация выпускника – Специалист по защите информации
Форма и срок обучения – 5 лет 6 месяцев, очная форма
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 6
Часов по учебному плану (УП)– 216

Формы промежуточной аттестации
в семестрах:
экзамен 6 зачет 5 курсовая работа 6

Распределение часов дисциплины по семестрам

Семестр	5	6	**Итого**
Число недель в семестре	17	17	
Вид занятий	Часов по УП	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	**51**	**51**	**102**
– лекции	34	17	51
– лабораторные	17	17	34
– практические (семинарские)	-	17	17
Самостоятельная работа	**21**	**57**	**78**
Зачёт			
Экзамен		**36**	**36**
Итого	**72**	**144**	**216**

* В форме ПП – в форме практической подготовки.

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – специалитет по специальности 10.05.03«Информационная безопасность автоматизированных систем», утверждённым приказом Минобрнауки России от 26.11.2020 г. № 1457.

Программу составил:
к.ф.-м.н., доцент _____А.А. Бутин

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

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

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1 Цели преподавания дисциплины

1	обучение базовым принципам и методикам в области защиты информации (ЗИ), комплексного проектирования, построения, эксплуатации защищенных автоматизированных систем (АС)

1.2 Задачи дисциплины

1	освоение методических аспектов проектирования и построения защищенных АС; критериев и методов оценки защищенности АС; основ формирования политики информационной безопасности (ПИБ) АС организации

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

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

Задачи воспитательной работы с обучающимися:

– развитие мировоззрения и актуализация системы базовых ценностей личности;

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

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

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

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

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

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1 Требования к предварительной подготовке обучающегося

Б1.О.13 «Информатика»;
Б1.О.33 «Основы информационной безопасности»; Б1.О.35 «Организация ЭВМ и вычислительных систем»;
Б1.О.47 «Информационные технологии»;
Б1.В.ДВ.02.01 «Основы системного анализа»

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

1	Б1.О.31 «Безопасность сетей ЭВМ»;
2	Б1.О.39 «Программно-аппаратные средства защиты информации»;
3	Б1.О.40 «Разработка и эксплуатация автоматизированных систем в защищенном исполнении»;
4	Б1.О.41 «Управление информационной безопасностью»;
5	Б1.О.44 «Информационная безопасность открытых систем»;
6	Б1.О.55 «Защита объектов критической информационной инфраструктуры»;
7	Б1.О.57 «Методы принятия организационно-технических решений»;
8	Б1.О.59 «Проектирования систем защиты объектов информатизации»;
9	Б1.О.60 «Защита информации от несанкционированного доступа»;
10	Б2.В.01(П) «Производственная - технологическая практика»;
11	Б2.В.02 (П) «Производственная - эксплуатационная»;
12	Б2.В.03(П) «Производственная - проектно-технологическая»;
13	Б2.В.04(Н) «Производственная - научно-исследовательская работа»;
14	Б2.В.05(Пд) «Производственная - преддипломная»

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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения

ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1. Оценивает сущность и значение информации в современном обществе ОПК-1.2. Оценивает значение информационных технологий в развитии современного общества ОПК-1.3. Оценивает роль, сущность и значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства	**Знать:** – основные понятия теории компьютерной безопасности; – причины, виды и каналы утечки информации; – основные принципы обеспечения информационной безопасности (ИБ); – критерии защищенности АС; – этапы создания комплексной системы защиты информации (КСЗИ). **Уметь:** – выделять информацию, подлежащую защите; – применять основные критерии защищенности АС; – оценивать эффективность КСЗИ. **Владеть:** – навыками анализа информационных рисков; – методологией разработки и реализации ПИБ.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работы	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Лаб	Пр	СР	
1.0	**Архитектура электронных систем обработки данных. Формальные модели; модели безопасности; политика информационной безопасности (ПИБ). Критерии и классы защищенности СВТ и АС в соответствии с РД ГТК РФ. Стандарты по оценке защищенных систем**						ОПК-1.1. ОПК-1.2. ОПК-1.3.
1.1	Краткие сведения о компонентах электронных систем обработки данных. Функциональные назначения компонентов	5	2				
1.2	Три аспекта рассмотрения архитектурных решений	5				3	
1.3	Модель АС и модели безопасности. Основные понятия. Описание типовых ПИБ: модели разграничения доступа, построенные по принципу предоставления прав. Описание типовых ПИБ: модели разграничения доступа - информационные модели. Описание типовых ПИБ: модели разграничения доступа - вероятностные модели. Описание типовых ПИБ: механизм защиты от отказа в обслуживании (DoS). Понятия доступа, монитора безопасности. Изолированная программная среда	5	4				
1.4	Стандарт оценки безопасности компьютерных систем TCSEC. Концепция защиты АС и средств вычислительной техники (СВТ) по руководящим документам (РД) Гостехкомиссии (ГТК) РФ	5				3	

1.5	Средства борьбы с вредоносным программным обеспечением	5		5			
1.6	Требования к защите конфиденциальной информации. Требования к защите секретной информации. Зарубежные критерии безопасности АС (ITSEC, «Единые критерии»). Стратегия защиты информации	5	4			6	
1.7	Защита от несанкционированного доступа к информации (НСДИ). Термины и определения	6			2		
1.8	СВТ. Защита от НСДИ. Показатели защищенности от НСДИ	6			2		
1.9	АС. Защита от НСДИ Классификация АС и требования по защите информации	6			2		
2.0	**Примеры практической реализации; построение парольных систем. Особенности применения криптографических методов; способы реализации криптографической подсистемы; особенности реализации систем с симметричными и асимметричными ключами**	5					ОПК-1.1. ОПК-1.2. ОПК-1.3
2.1	Общие подходы к построению парольных систем защиты от НСДИ. Требования к выбору паролей.Проблемы передачи паролей по сети. Задача удаленной аутентификации	5	6				
2.2	Парольные системы. Технология выбора пароля в ОС Windows и проверка его стойкости	5		6			
2.3	Назначение и порядок работы сканеров безопасности	5		6			
2.4	Примеры механизмов и сервисов безопасности (аудит, обнаружение вторжений)	5				9	
2.5	Средства криптографической защиты информации (СКЗИ). Требования к СКЗИ. Предварительное и динамическое шифрование. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом и электронной цифровой подписи	5	6				
2.6	Положение о государственном лицензировании деятельности в области защиты информации	6			2		
2.7	Криптоанализ шифра простой замены (на основе криптопакетаPrZamena)	6		9			
2.8	Криптоанализ шифра простой замены (на основе программной реализации метода частотного анализа)	6		8			
2.9	Криптографическая защита на транспортном и прикладном уровнях распределенных АС. Особенности сертификации и стандартизации криптографических средств. Перспективы использования криптозащиты	6				12	

	информации в АС. Стеганографические методы защиты информации						
3.0	**Методология обследования и проектирования систем защиты. Методы построения защищенных АС; исследование корректности КСЗИ. Основные понятия и определения, используемые при описании математических моделей безопасности АС. Модели систем дискреционного и мандатного разграничения доступа. Субъектно-ориентированная модель изолированной программной среды**						ОПК-1.1. ОПК-1.2. ОПК-1.3
3.1	Этапы создания комплексной системы защиты информации. Научно-исследовательская разработка КСЗИ. Создание организационной структуры КСЗИ	5	4				
3.2	Проработка лекционного материала , подготовка к семинарским занятиям	6				12	
3.3	Концепция создания защищенных АС.Построение систем защиты от угроз нарушения конфиденциальности, целостности, доступности информации и угрозы раскрытия параметров АС.Подходы к оценке эффективности КСЗИ: классический подход; официальный подход; экспериментальный подход	5	4				
3.4	Математические основы моделей безопасности. Элементы теории автоматов и графов. Модель «решетки». Основные виды моделей безопасности	5	4				
3.5	Модель «Решетки». Решение задач	6			2		
3.6	Классификация угроз безопасности информации. Алгоритмически разрешимые и алгоритмически неразрешимые проблемы	6				12	
3.7	Модель Харрисона -Руззо-Ульмана (ХРУ).Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant	6	6				
3.8	Классическая модель Белла-ЛаПадула.Политика low-watermark в модели Белла-ЛаПадула	6	6				
3.9	Модель Take-Grant. Решение задач	6			3		
3.10	Модель Белла-ЛаПадула. Решение задач	6			4		
3.11	Анализ безопасности систем ХРУ	6				12	
3.12	Монитор безопасности объектов. Монитор безопасности субъектов. Изолированная программная среда	6	5				

3.13	Проработка лекционного материала	6				9	
	Зачёт	5					ОПК-1.1. ОПК-1.2. ОПК-1.3
4.0	**Экзамен**	6				36	ОПК-1.1. ОПК-1.2. ОПК-1.3

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

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

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/100% онлайн
6.1.1.1	Щеглов А. Ю., Щеглов К. А.	Защита информации: основы теории : учебник для вузов/309 с. https://urait.ru/bcode/490019	Юрайт, 2022.	100 % онлайн
6.1.1.2	Т. А. Полякова А. А. Стрельцов	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов /325 с. https://urait.ru/bcode/498844	Юрайт, 2022.	100% онлайн
6.1.1.3	Каширская Е. Н	Криптографический анализ и методы защиты информации : учебное пособие/91 с. https://e.lanbook.com/book/163861	Лань, 2020	100% онлайн

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/100% онлайн
6.1.2.1	Никитин И. А. ,Цулая М. Т.	Процессы анализа и управления рисками в области ИТ: Учебная литература для ВУЗов; http://biblioclub.ru/index.php?page=book_red&id=429089:	М.: Национальный Открытый Университет «ИНТУИТ», 2016	100% онлайн
6.1.2.2	Коваленко Ю.И.	Правовой режим лицензирования и сертификации в сфере информационной безопасности: Для ВПО и курсов переподготовки http://e.lanbook.com/books/element.php?pl1_id=5163	М.: Горячая линия-Телеком, 2012	100% онлайн
6.1.2.3	Девянин П.Н.	Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учебное пособие http://e.lanbook.com/books/element.php?pl1_id=63235	Горячая линия-Телеком, 2013	100% онлайн
6.1.2.4	Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А.	Основы информационной безопасности: Для ВПО http://e.lanbook.com/books/element.php?pl1_id=5121	М:. Горячая линия- Телеком, 2006	100% онлайн

6.1.3 Учебно-методические разработки (в т.ч. для самостоятельной работы обучающихся)обучающихся по дисциплине				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/100% онлайн
6.1.3.1	Паршин К. А.	Методы и средства проектирования информационных систем и технологий : учебно-методическое пособие / — 129 с. https://e.lanbook.com/book/121337	Лань, 2018	100% онлайн
6.1.3.2	Рагозин Ю. Н., Мельник В. А.	Организация и управление подразделением защиты информации на предприятии : учебное пособие / — 240 с. , https://e.lanbook.com/book/161357	Лань, 2019	100% онлайн
6.1.3.3	Завгородний В.И.	«Комплексная защита информации в компьютерных системах»; http://www.proklondike.com/books/defence/zavgorodniy_complex_defence.html; http://bezopasnik.org/article/book/zavgorodniy_-_Complex_Defend.pdf	Личный кабинет	100% онлайн

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»		
6.2.1	Сайт ФСТЭК РФ	http://fstec.ru/
6.2.2	Сайт ФСБ РФ	http://www.fsb.ru/
6.2.3	Материалы "Единые критерии"	http://oplib.ru/random/view/273781
6.2.4	РД ГТК	http://www.studmed.ru/docs/document16873?view=50&page=5
6.2.5	РД ГТК	http://oplib.ru/random/view/441942
6.2.6	Материалы "Парольные системы"	http://infoprotect.net/category/note
6.2.7	Материалы "Сканеры безопасности, сетевые угрозы"	http://www.securitylab.ru/analytics/365241.php
6.2.8	Материалы "Комплексная защита информации в компьютерных системах"	http://mexalib.com/view/2248
6.2.9	Материалы "Теоретические основы компьютерной безопасности"	http://elar.urfu.ru/bitstream/10995/1778/5/1335332_schoolbook.pdf

6.3 Программное обеспечение и информационные справочные системы	
6.3.1 Базовое программное обеспечение	
6.3.1.1	ОС Microsoft Windows XP Professional with Service Pack 2, лицензия Open License;
6.3.1.2	ОС MicrosoftWindows 7 Professional, лицензия № 49379844, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд WindowsEduPerDevice 10 Education, Соглашение № V6760694, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд
6.3.1.3	Офисный пакет MicrosoftOffice 2010, Лицензия № 48288083, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; OfficeProfessional 2019 - Соглашение № V0709762, контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; LibreOffice v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org
6.3.1.4	BorlandDelphi 7.
6.3.2 Перечень специализированных средств и программного обеспечения	
6.3.2.1	Средство антивирусной защиты Dr. Webcureit! (свободное программное обеспечение (ПО));
6.3.2.2	Учебная программа PrZamena (свободное ПО);
6.3.2.3	Учебная программа «Генератор безопасных паролей spass.exe» (свободное ПО);
6.3.2.4	Учебная программа «Генератор безопасных паролей PassGen.exe» (свободное ПО);
6.3.2.5	Учебная программа «lcp4.exe» (свободное ПО);
6.3.2.6	Учебная программа «lc4setup.exe» (свободное ПО);
6.3.2.7	Учебная программа «lc3setup02.exe» (свободное ПО);
6.3.2.8	Сканер «XSpider.exe 7.x» (demo-версия);
6.3.2.9	Сканер Nessus-3.x (версия: свободное ПО);

6.3.2.10	Сканер SSS v5.27 (demo-версия).
6.3.3 Перечень информационных справочных систем	
6.3.3.1	КонсультантПлюс – студенческая версия (Онлайн–версия КонсультантПлюс: Студент, https://student2.consultant.ru/cgi/online.cgi?req=home;rnd=0.8160556428138959)

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

1	Учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории.
2	Учебная лаборатория «Средства и методы защиты информации», Д-523. Оснащена компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечена доступом в электронную информационно-образовательную среду ИрГУПС. Перечень установленных программных средств: MicrosoftOffice 2010, OpenOffice 3.0.1, 7-zip, BorlandDelphi 7, AbodeReaderXI, MicrosoftSecurityEssentials, а также специализированное ПО.
3	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на лабораторной работе.
Практическое (семинарское) занятие	Обобщение, расширение и углубление пройденного материала на лекции. Выступление с докладами по заданной теме, формирование навыков самостоятельной работы, анализа литературных источников, публичного выступления и аргументации собственного мнения. Обсуждение вопросов, вызвавших затруднение, с преподавателем. Участие в дискуссиях. Контроль качества усвоения пройденного материала.
Лабораторная работа	Один из видов практической работы, проводимой с целью углубления и закрепления теоретических знаний, развития навыков самостоятельной деятельности. Включает подготовку необходимых программно-аппаратных средств, составление плана работы, ее проведение и написание отчета
Курсовая работа	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся в предметной или межпредметной областях
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины, размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.	

Лист регистрации дополнений и изменений рабочей программы дисциплины

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

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине Б1.О.48 Теоретические основы компьютерной безопасности

Приложение 1 к рабочей программе

Специальность – 10.05.03 Информационная безопасность автоматизированных систем;
Специализация – № 5 "Безопасность открытых информационных систем"

ИРКУТСК

1. Общие положения

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

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

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

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины (модуля) или прохождения практики;

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

– самоподготовка и самоконтроль обучающихся в процессе обучения.

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

Для оценки уровня сформированности компетенций используется трехуровневая система:

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

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

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

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

Дисциплина «Теоретические основы компьютерной безопасности» участвует в формировании компетенции:

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

Программа контрольно-оценочных мероприятий **очная форма обучения**

№	Неде-ля	Наименование контрольно-	Объект контроля (понятие/тем/раздел и т.д. дисци-	Код индикатора до-	Наименование оценочного средства

		оценочного мероприятия	плины)	стижения компетенции	(форма проведения*)
5 семестр					
1	1-17	Текущий контроль	Лабораторные работы (см. п.4 РПД, разделы 1-3)	ОПК-1.1, ОПК-1.2, ОПК-1.3	Защита лабораторных работ (устно)
2	17	Тест	Разделы 1-3 РПД	ОПК-1.1, ОПК-1.2, ОПК-1.3	Фонд тестовых заданий (письменно)
3	17	Промежуточная аттестация –зачет	Разделы 1-3 РПД	ОПК-1.1, ОПК-1.2, ОПК-1.3	Зачет (устно)
			6 семестр		
1	1-17	Текущий контроль	Лабораторные работы (см. п.4 РПД, разделы 1-3)	ОПК-1.1, ОПК-1.2, ОПК-1.3	Защита лабораторных работ (устно)
3	1-17	Текущий контроль	Индивидуальное выступление с докладом на семинарском занятии по теме в соответствии с п.4 РПД по данной дисциплине; решение задач	ОПК-1.1, ОПК-1.2, ОПК-1.3	Сообщение, доклад (устно); наличие презентации; решение задач
4	17	Тест	Раздел 3 РПД	ОПК-1.1, ОПК-1.2, ОПК-1.3	Фонд тестовых заданий (письменно)
5	17	Оценка курсовой работы	Курсовая работа	ОПК-1.1, ОПК-1.2, ОПК-1.3	Защита курсовой работы (устно)
6		Промежуточная аттестация – экзамен	Разделы 1-3 РПД	ОПК-1.1, ОПК-1.2, ОПК-1.3	Экзамен (устно)

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

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

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

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

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

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

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС

1	Сообщение, доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов, сообщений
2	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использован для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
2	Защита лабораторной работы	Средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Темы лабораторных работ и требования к их защите
3	Курсовая работа	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся в предметной или межпредметной областях	Темы типовых групповых и / или индивидуальных проектов и типовое задание на курсовую работу
4	Зачет	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов) к зачету
5	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов билетов к экзамену

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

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

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

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Защита лабораторной работы

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

Доклад, сообщение

Шкала оценивания	Критерии оценивания
«отлично»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint,Flash–презентация, видео-презентация и др.) Использованы дополнительные источники информации. Содержание заданной темы раскрыто в полном объеме. Отражена структура доклада (вступление, основная часть, заключение, присутствуют выводы и примеры). Оформление работы. Оригинальность выполнения (работа сделана самосто-

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

Курсовая работа

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

Оценочное средство «Тест»

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

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

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

Критерии оценивания	Шкала оценивания
Обучающийся набрал при тестировании 60 и более баллов	«зачтено»
Обучающийся набрал при тестировании менее 60 баллов	«не зачтено»

Промежуточная аттестация в форме экзамена – результаты тестирования могут являться допуском к экзамену:

Критерии оценивания	Шкала оценивания
Обучающийся набрал при тестировании более 69 баллов	Обучающийся к экзамену допущен
Обучающийся набрал при тестировании менее 69 баллов	Обучающийся к экзамену не допущен

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

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

3.1. Темы докладов, сообщений

См. п. 4 РПД

3.2. Перечень типовых тем курсовых работ

1. Методы и средства обеспечения конфиденциальности информации;
2. Методы и средства обеспечения целостности информации;
3. Методы и средства обеспечения доступности информации;
4. Защита от угрозы раскрытия параметров АС;
5. Исследование корректности функционирования системы защиты информации в АС;
6. Средства и методы анализа защищенности информации в АС;
7. Подходы к формированию множества угроз ИБ. Системная классификация угроз ИБ;
8 Система и содержание показателей уязвимости информации;
9. Оценка требуемого уровня защиты информации;
10. Состав и правила функционирования службы ИБ;
11. Виды и категории информации ограниченного доступа;

12. Порядок определения потенциальных каналов и способов несанкционированного доступа к информации в АС;
13. Методики оценки качества комплексной системы информационной безопасности;
14. Понятие, состав и процесс формирования политики информационной безопасности предприятия;
15. Формирование модели потенциального нарушителя ИБ на предприятии;
16. Архитектура электронных систем обработки информации;
17. Сравнение российских и зарубежных нормативных требований защищенности ин формации в АС;
18. Роль аудита в структуре комплексной системы информационной безопасности;
19. Биометрические средства аутентификации;
20. Компьютерная стеганография;
21. Экономические аспекты построения КСЗИ;
22. Практические методы и средства защиты информации от вредоносного программного обеспечения

3.3 Перечень теоретических вопросов к зачету

Раздел 1

1.1. Краткие сведения о компонентах электронных систем обработки данных.
1.2. Функциональные назначения компонентов.
1.3. Модель АС и модели безопасности. Основные понятия.
1.4. Описание типовых ПИБ: модели разграничения доступа, построенные по принципу предоставления прав.
1.5. Описание типовых ПИБ: модели разграничения доступа - информационные модели.
1.6. Описание типовых ПИБ: модели разграничения доступа - вероятностные модели.
1.7. Описание типовых ПИБ: механизм защиты от отказа в обслуживании (DoS).
1.8. Понятия доступа, монитора безопасности.
1.9. Изолированная программная среда.
1.10. Требования к защите конфиденциальной информации.
1.11. Требования к защите секретной информации.
1.12. Зарубежные критерии безопасности АС (ITSEC, «Единые критерии»).

Раздел 2

2.1. Общие подходы к построению парольных систем защиты от НСДИ.
2.2. Требования к выбору паролей.
2.3. Средства криптографической защиты информации (СКЗИ). Требования к СКЗИ
2.4. Предварительное и динамическое шифрование.
2.5. Методы шифрования с симметричным ключом.
2.6. Системы шифрования с открытым ключом и электронной подписи

3.4 Перечень теоретических вопросов к экзамену

Раздел 1

1.1. Краткие сведения о компонентах электронных систем обработки данных.
1.2. Функциональные назначения компонентов АС.
1.3. Модель АС и модели безопасности. Основные понятия.
1.4. Описание типовых ПИБ: модели разграничения доступа, построенные по принципу предоставления прав.
1.5. Описание типовых ПИБ: модели разграничения доступа - информационные модели.
1.6. Описание типовых ПИБ: модели разграничения доступа - вероятностные модели.
1.7. Описание типовых ПИБ: механизм защиты от отказа в обслуживании (DoS).
1.8. Понятия доступа, монитора безопасности.

1.9. Изолированная программная среда.
1.10. Требования к защите конфиденциальной информации.
1.11. Требования к защите секретной информации.
1.12. Зарубежные критерии безопасности АС (ITSEC, «Единые критерии»).

Раздел 2

2.1. Общие подходы к построению парольных систем защиты от НСДИ.
2.2. Требования к выбору паролей.
2.3. Средства криптографической защиты информации (СКЗИ). Требования к СКЗИ
2.4. Предварительное и динамическое шифрование.
2.5. Методы шифрования с симметричным ключом.
2.6. Системы шифрования с открытым ключом и электронной подписи

Раздел 3

3.1. Этапы создания комплексной системы защиты информации.
3.2. Математические основы моделей безопасности.
3.3. Элементы теории автоматов и графов. Модель «решетки». Основные виды моделей безопасности.
3.4. Модель Харрисона -Руззо-Ульмана.
3.5. Модель распространения прав доступа Take-Grant.
3.6. Расширенная модель Take-Grant.
3.7. Классическая модель Белла-ЛаПадула.
3.8. Монитор безопасности объектов. Монитор безопасности субъектов.
3.9. Изолированная программная среда.

3.5 Тестирование по дисциплине

3.5.1 Структура фонда тестовых заданий по дисциплине

Структура фонда тестовых заданий по дисциплине «Теоретические основы компьютерной безопасности»

Раздел дисциплины	Тема раздела	Количество тестовых заданий (ТЗ), типы ТЗ
1. Архитектура электронных систем обработки данных. Формальные модели; модели безопасности; политика информационной безопасности (ПИБ). Критерии и классы защищенности СВТ и АС в соответствии с РД ГТК РФ. Стандарты по оценке защищенных систем	Краткие сведения о компонентах электронных систем обработки данных. Функциональные назначения компонентов . Модель АС и модели безопсности. Основные понятия. Описание типовых ПИБ: модели разграничения доступа, построенные по принципу предоставления прав. Описание типовых ПИБ: модели разграничения доступа - информационные модели. Описание типовых ПИБ: модели разграничения доступа - вероятностные модели. Понятия доступа, монитора безопасности. Требования к защите конфиденциальной информации. Требования к защите секретной информации. Зарубежные критерии безопасности АС (ITSEC, «Единые критерии»)	34 – тип А 1 – тип В 1 – тип D
Итого по разделу		**∑ 36** **34– тип А** **1- тип В**

		1- тип D
2. Примеры практической реализации; построение парольных систем. Особенности применения криптографических методов; способы реализации криптографической подсистемы; особенности реализации систем с симметричными и асимметричными ключами	Общие подходы к построению парольных систем защиты от НСДИ. Требования к выбору паролей.Проблемы передачи паролей по сети. Задача удаленной аутентификации; Средства криптографической защиты информации (СКЗИ). Требования к СКЗИ. Предварительное и динамическое шифрование. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом и электронной цифровой подписи	36 – тип А
	Итого по разделу	**∑ 36** **36– тип А**
3. Методология обследования и проектирования систем защиты. Методы построения защищенных АС; исследование корректности КСЗИ. Основные понятия и определения, используемые при описании математических моделей безопасности АС. Модели систем дискреционного и мандатного разграничения доступа. Субъектно-ориентированная модель изолированной программной среды	Этапы создания комплексной системы защиты информации. Научно-исследовательская разработка КСЗИ. Создание организационной структуры КСЗИ. Математические основы моделей безопасности. Элементы теории автоматов и графов. Модель «решетки». Основные виды моделей безопасности. Модель Харрисона -Руззо-Ульмана (ХРУ).Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant. Классическая модель Белла-ЛаПадула. Политика low-watermark в модели Белла-ЛаПадула	36 – тип А
	Итого по разделу	**∑ 36** **36 – тип А**
	Итого по дисциплине	**∑ 108** **106 – тип А** **1 – тип В** **1 – тип D**

Используемые типы тестовых заданий (ТЗ):

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

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

ТЗ типа С: тестовое задание на установление соответствия;

ТЗ типа D: тестовое задание на установление правильной последовательности.

3.5.2 Структура и образец
итогового теста по дисциплине за весь период ее освоения

Структура типового итогового теста по дисциплине за весь период ее освоения

Раздел дисциплины	Тема раздела	Количество тестовых заданий (ТЗ), типы ТЗ
1. Архитектура электронных систем обработки данных. Формальные модели; модели безопасности; политика информационной безопасности (ПИБ). Критерии и классы защищенности СВТ и АС в соответствии с РД ГТК РФ. Стандарты по оценке защищенных систем	Краткие сведения о компонентах электронных систем обработки данных. Функциональные назначения компонентов . Модель АС и модели безопсности. Основные понятия. Описание типовых ПИБ: модели разграничения доступа, построенные по принципу предоставления прав. Описание типовых ПИБ: модели разграничения доступа - информационные модели. Описание типовых ПИБ: модели разграничения доступа - вероятностные модели. Понятия доступа, монитора безопасности. Требования к защите конфиденциальной информации. Требования к защите секретной информации. Зарубежные критерии безопасности АС (ITSEC, «Единые критерии»)	8 – тип А 1 – тип В 1 – тип D
	Итого по разделу	**∑ 10** **8– тип А** **1- тип В** **1- тип D**
2. Примеры практической реализации; построение парольных систем. Особенности применения криптографических методов; способы реализации криптографической подсистемы; особенности реализации систем с симметричными и асимметричными ключами	Общие подходы к построению парольных систем защиты от НСДИ. Требования к выбору паролей.Проблемы передачи паролей по сети. Задача удаленной аутентификации; Средства криптографической защиты информации (СКЗИ). Требования к СКЗИ. Предварительное и динамическое шифрование. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом и электронной цифровой подписи	10 – тип А
	Итого по разделу	**∑ 10** **10– тип А**
3. Методология обследования и проектирования систем защиты. Методы построения защищенных АС; исследование корректности КСЗИ. Основные понятия и определения, используемые при описании математических моделей безопасности АС. Модели систем дискреционного и мандатного разграничения доступа. Субъектно-ориентированная	Этапы создания комплексной системы защиты информации. Научно-исследовательская разработка КСЗИ. Создание организационной структуры КСЗИ. Математические основы моделей безопасности. Элементы теории автоматов и графов. Модель «решетки». Основные виды моделей безопасности.	10 – тип А

модель изолированной программной среды	Модель Харрисона -Руззо-Ульмана (ХРУ).Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant. Классическая модель Белла-ЛаПадула. Политика low-watermark в модели Белла-ЛаПадула	
Итого по разделу		**∑ 10** **10 – тип A**
Итого по дисциплине		**∑ 30** **28 – тип A** **1 – тип B** **1 – тип D**

Образец типового теста
за 5/6 семестр/итогового теста по дисциплине/за весь период ее освоения

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 многопользовательских АС с различным уровнем доступа, необходимо управление потоками информации:
   ○ 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 информации.
8. Основными типами моделей, построенных на предоставлении прав, являются модели (выделить все верные варианты)
   ○ дискреционного доступа;
   ○ дискретного доступа;
   ○ мандатного доступа;
   ○ непрерывного доступа.
9. Использование парольной системы обеспечивает выполнение требования _____ при входе субъекта в АС.
10. Алгоритмы шифрования группы асимметричных криптосистем требуют более _____ ключей по сравнению с симметричными криптосистемами:
   ○ длинных;
   ○ коротких;
   ○ средних.
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;
   ○ аутентификация субъекта;
   ○ идентификация субъекта.
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. Вставить одно слово на место пропущенных:
«Идентификация» (Identification) – это присвоение субъектам и объектам доступа _____ и/или сравнение предъявляемого _____ с перечнем присвоенных _____ .

21. Угроза ИБ всегда направлена на определенную _____ АС.

22. _____ 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 _____ доступа.

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

25. Алгоритм RSA опирается на следующий тип необратимых преобразований: разложения больших чисел на простые _____ .

26. Алгоритм _____представляет собой метод получения секретного ключа для участников сессии обмена конфиденциальной информацией.

27. Одним из способов аутентификации является предъявление _____ 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.

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

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

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Сообщение, доклад	Обучаемый получает тему от преподавателя изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит доклад (сообщение), объемом до 10 стр. текста размером 12 пунктов, интервал 1,2; предоставляет доклад (сообщение) преподавателю, отвечает на его вопросы. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Тест	Обучаемый самостоятельно отвечает на вопросы теста в письменной форме. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся
Защита лабораторной работы	Обучаемый самостоятельно, под руководством преподавателя выполняет лабораторную работу на заданную тему. Тема (задание) предлагается в конкретном виде. Методы и инструменты для ее разработки предлагаются преподавателем. После выполнения задания обучаемый готовит пояснительную записку, предоставляет ее преподавателю, отвечает на его вопросы в ходе собеседования (защиты). Оценка ставится по представленным результатам и результатам собеседования. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся

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

– перечень теоретических вопросов к зачету/экзамену для оценки знаний;

Перечень теоретических вопросов и перечни типовых практических заданий разного уровня сложности к зачету/экзамену 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. Оценочные средства и типовые контрольные задания, используемые при текущем контроле, позволяют оценить знания, умения и владения навыками/опытом деятельности обучающихся при освоении дисциплины. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок).

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

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

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

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

При проведении промежуточной аттестации в форме экзамена могут быть использованы результаты тестирования:

Критерии оценивания	Шкала оценивания
Обучающийся набрал при тестировании более 69 баллов	Обучающийся к экзамену допущен
Обучающийся набрал при тестировании менее 69 баллов	Обучающийся к экзамену не допущен

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам.

Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену.

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект билетов не выставляется в электронную информационно-образовательную среду ИрГУПС, а хранится на кафедре-разработчике ФОС на бумажном носителе в составе ФОС по дисциплине.

На экзамене обучающийся берет билет, для подготовки ответа на экзаменационный билет обучающемуся отводится время в пределах 45 минут. В процессе ответа обучающегося на вопросы и задания билета преподаватель может задавать дополнительные вопросы.

Каждый вопрос билета оценивается по четырехбалльной системе, а далее вычисляется среднее арифметическое оценок, полученных за каждый вопрос/задание. Среднее арифметическое оценок округляется до целого по правилам округления.

Образец экзаменационного билета

ИРГУПС 2021-2022	**Экзаменационный билет № 1** **по дисциплине ТОКБ** 9 **семестр**	Утверждаю: Заведующий кафедрой ИСиЗИ ИрГУПС _____

учебный год		
1. Понятия доступа, монитора безопасности; 2. Системы шифрования с открытым ключом и электронной подписи Билет формата А5 – 148*210мм		