ИРКУТСК
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом ректора
от «7» июня 2021 г. № 78

Б1.О.40 Разработка и эксплуатация автоматизированных систем в защищенном исполнении

рабочая программа дисциплины

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – 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. –5
Часов по учебному плану (УП) –180

Формы промежуточной аттестации в семестрах
Экзамен: 10, курсовой работа 10

Распределение часов дисциплины по семестрам

Семестр	10	**Итого**
Число недель в семестре	17	
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в форме ПП*	**68**	**68**
– лекции	34	34
– практические (семинарские)	17	17
– лабораторные	17	17
Самостоятельная работа	**76**	**76**
Экзамен	**36**	**36**
Итого	**180**	**180**

* В форме ПП – в форме практической подготовки.

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – магистратура по направлению подготовки 10.03.01 Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности), утверждённым приказом Минобрнауки России от 17.11.2020 г. № 1427.

Программу составил(и):
Ассистент _____ *А.С.Вергасов*

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «*ИСиЗИ*», протокол от «4» июня 2021 г №11/2

Зав. кафедрой*, канд. экон.наук* _____ *Т.К.Кириллова*

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цели дисциплины	
1	Целью изучения дисциплины Информационная безопасность автоматизированных систем является формирование важнейших представлений о теории и практике создания защищенных автоматизированных систем.
1.2 Задачи дисциплины	
1	формирование итоговых основ по защите информации, включая вопросы ее конфиденциальности, целостности и доступности;
2	формирование умения применять полученные знания для решения прикладных задач по защите автоматизированных систем с учетом развития информационных технологий и программного обеспечения.
1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины	
Цель воспитания обучающихся – разностороннее развитие личности будущего конкурентоспособного специалиста с высшим образованием, обладающего высокой культурой, интеллигентностью, социальной активностью, качествами гражданина-патриота. Задачи воспитательной работы с обучающимися: – развитие мировоззрения и актуализация системы базовых ценностей личности; – приобщение студенчества к общечеловеческим нормам морали, национальным устоям и академическим традициям; – воспитание уважения к закону, нормам коллективной жизни, развитие гражданской и социальной ответственности как важнейшей черты личности, проявляющейся в заботе о своей стране, сохранении человеческой цивилизации; – воспитание положительного отношения к труду, развитие потребности к творческому труду, воспитание социально значимой целеустремленности и ответственности в деловых отношениях; – обеспечение развития личности и ее социально-психологической поддержки, формирование личностных качеств, необходимых для эффективной профессиональной деятельности; – выявление и поддержка талантливых обучающихся, формирование организаторских навыков, творческого потенциала, вовлечение обучающихся в процессы саморазвития и самореализации;	

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП		
2.1 Требования к предварительной подготовке обучающегося		
Б1.О.33 Основы информационной безопасности		
Б1.О.41 Управление информационной безопасностью		
Б1.О.51 Кибербезопасность		
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее		
1	Б2.В.04(Н)	Производственная - научно-исследовательская работа
2	Б2.В.05(Пд)	Производственная - преддипломная
3	Б3.01(Д)	Подготовка к процедуре защиты 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.7 Способен создавать программы на языках общего назначения,	ОПК.7-1 Знает основные языки программирования и работы с базами данных, операционные системы и оболочки, современные	**Знать:** - основные информационные технологии, используемые в автоматизированных системах; – основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения

применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;	программные среды разработки программных средств для решения задач в профессиональной деятельности, Администрирование систем баз данных ОПК.7-2 Умеет применять языки программирования и работы с базами данных, современные программные среды разработки программных средств для автоматизации бизнес-процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ ОПК.7-3 Имеет навыки программирования, отладки и тестирования прототипов программно-технических комплексов задач	информационной безопасности в автоматизированных и телекоммуникационных системах; –основные языки программирования используемые для написания компонентов автоматизированных систем в защищенном исполнении; – основы администрирования баз данных. – **Уметь:** - разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем. – применять языки программирования используемые для написания компонентов автоматизированных систем в защищенном исполнении: - администрировать подсистемы информационной безопасности автоматизированных систем; **Владеть:** – навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; – навыками программирования на языках программирования используемых для написания компонентов автоматизированных систем в защищенном исполнении –навыками администрирования баз данных.
ОПК.2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК.2-1 Применяет современные программные средства системного и прикладного назначений, в том числе отечественного производства, при решении задач профессиональной деятельности	**Знать:** – основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах; – основные информационные технологии, используемые в автоматизированных системах; - основные меры по защите информации в автоматизированных системах (программно-аппаратные, криптографические, технические); **Уметь:** – администрировать подсистемы информационной безопасности автоматизированных систем; – восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях; **Владеть:** – навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; – навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем. –
УК.2 Способен управлять проектом на всех этапах его жизненного цикла	УК.2-1 Владеет навыками целеполагания; постановки и приоритета задач для достижения генеральной цели и совокупности целей проекта; создания системы комплексного и прогнозирующего планирования работ и параметров проекта, а также системы контроля и регулирования хода выполнения проекта на всех	**Знать:** – основные информационные технологии, используемые в автоматизированных системах; – основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; – автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; - методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем - содержание и порядок деятельности персонала по

	этапах его жизненного цикла	эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; - методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; - основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); **Уметь:** – исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений; разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; - разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем. **Владеть:** - методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; – навыками анализа основных узлов и устройств современных автоматизированных систем; – навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; – методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;

* Код индикатора достижения компетенции проставляется или для всего раздела или для каждой темы или для каждого вида работы.

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работы	Семестр	Часы				*Код индикатора достижения компетенции
			Лек	Пр	Лаб	СР	
	Раздел 1. Угрозы безопасности информационных систем и их классификация.		**4**			**12**	
1.1	Цели и задачи безопасности и защиты программных систем. Основные виды угроз. Характеристика и классификация угроз и атак /Лек/	10	4				
1.2	Проработка лекционного материала: цели и задачи безопасности и защиты программных систем, основные виды угроз, характеристика и классификация угроз и атак /Ср/	10				12	
	Раздел 2. Управление информационными рисками .		**8**	**5**	**4**	**14**	
2.1	Неопределенность и риск. Модели оценки рисков. Трехфакторная модель оценки информационных рисков /Лек/	10	8				
2.2	Проработка лекционного материала: неопределенность и риск, модели оценки рисков, трехфакторная модель оценки информационных рисков /Ср/	10				14	
2.3	Подготовка к лабораторному занятию «Контроль	10		5			

	целостности информации при случайных воздействиях» / Пр /						
2.4	Контроль целостности информации при случайных воздействиях /Лаб/	10			4		
	Раздел 3. Обеспечение конфиденциальности обрабатываемой программой информации.		**8**	**4**	**5**	**16**	
3.1	Основные понятия криптографии. Российский алгоритм криптографического преобразования /Лек/	10	4				
3.2	Проработка лекционного материала: основные понятия криптографии, российский алгоритм криптографического преобразования /Ср/	10				8	
3.3	Двухключевые криптосистемы. Современный протокол шифрования информации /Лек/	10	4				
3.4	Проработка лекционного материала: двухключевые криптосистемы, современный протокол шифрования информации /Ср/	10				8	
3.5	Подготовка к лабораторному занятию «Методика определения информационных рисков» /Пр/	10		4			
3.6	Методика определения информационных рисков /Лаб/	10			5		
	Раздел 4. Технология электронной подписи при обработке программой информации.		**8**	**4**	**4**	**18**	
4.1	Хэш-функции, российский стандарт. Правовое обеспечение электронной подписи /Лек/	10	4				
4.2	Проработка лекционного материала: Хэш-функции, российский стандарт, правовое обеспечение электронной подписи /Ср/	10				9	
4.3	Криптографические методы технологии электронной подписи, российский стандарт /Лек/	10	4				
4.4	Проработка лекционного материала: криптографические методы технологии электронной подписи, российский стандарт /Ср/	10				9	
4.5	Подготовка к Лабораторному занятию «Порядок проведения классификация информационных систем в РФ» / Пр /	10		4			
4.6	Порядок проведения классификация информационных систем в РФ /Лаб/	10			4		
	Раздел 5. Технологии и методы аутентификации		**6**	**4**	**4**	**16**	
5.1	Основные понятия и определения. Инфраструктура управления открытыми ключами /Лек/	10	6				
5.2	Проработка лекционного материала: основные понятия и определения, инфраструктура управления открытыми ключами /Ср/	10				16	
5.3	Подготовка к лабораторному занятию «Технология применения электронной подписи» / Пр /	10		4			
5.4	Технология применения электронной подписи /Лаб/	10			4		
	Экзамен	10				36	

* Код индикатора достижения компетенции проставляется или для всего раздела или для каждой темы или для каждого вида работы.

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 разработан в соответствии с Положением о формировании фондов оценочных средств для проведения текущего контроля успеваемости, промежуточной и государственной итоговой аттестации № П.312000.06.7.188-2017.

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по данной 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	Никитин В. Н.	Проведение анализа защищённости информации в информационной системе: Учебное пособие Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/179382	Хабаровск : ДВГУПС, 2020.	100% онлайн
6.1.1.2	Бутин А.А.	Методы и средства защиты информации от несанкционированного доступа. Программно-аппаратный уровень : учеб. пособие	Иркутск: ИрГУПС, 2015	100% онлайн
6.1.1.3	Краковский Ю. М.	Методы защиты информации Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401	Санкт-Петербург : Лань, 2021.	100% онлайн

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
6.1.2.1	Давидюк Н. В.	Разработка автоматизированных систем обработки информации в защищенном исполнении: Практикум для укрупненной группы специальностей 10.00.00 «Информационная безопасность» Текст : электронный // Лань : электронно-библиотечная система.	Санкт-Петербург : Интермедия, 2020.	100% онлайн
6.1.2.2	Козичев В. Н., Протасов А. А., Ширманов А. В., Крейдин С. В.	Автоматизированные системы управления специального назначения: Учебное пособие Текст : электронный // Лань : электронно-библиотечная система.	Москва : МГТУ им. Баумана, 2020.	100% онлайн

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

	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
6.1.3.1	Беловицкий К. Б.	Коммерческий шпионаж (противодействие): Учебное пособие Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176522	Москва : РТУ МИРЭА, 2021.	100% онлайн
6.1.3.2	Бутырин О.В.	Курс лекций «Теория языков	Личный кабинет	100% онлайн

		программирования и методы трансляции».	обучающегося	
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»				
6.2.1	Википедия: свободная энциклопедия. https://ru.wikipedia.org			
6.2..2	Национальный открытый университет ИНТУИТ http://www.intuit.ru			
6.3 Программное обеспечение и информационные справочные системы				
6.3.1 Базовое программное обеспечение				
6.3.1.1	ОС Microsoft Windows 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 Windows Edu Per Device 10 Education, Соглашение № V6760694, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд			
6.3.1.2	Офисный пакет Microsoft Office 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; Office Professional 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			
6.3.2 Специализированное программное обеспечение				
6.3.2.1	Borland Delphi 7			
6.3.3 Информационные справочные системы				
6.3.3.1	Информационно-справочная система КонсультантПлюсhttp://www.consultant.ru			

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

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л – по адресу г. Иркутск, ул. Лермонтова, д.80.
2	*Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых проектов, работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа имеются учебно-наглядные пособия (презентации, плакаты, таблицы), обеспечивающие тематические иллюстрации содержания дисциплины.* Помещения для хранения и профилактического обслуживания учебного оборудования – А-521.
3	Учебная лаборатория «Средства и методы защиты информации», Д-523.
4	Помещения для хранения и профилактического обслуживания учебного оборудования – А-521.
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.

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮДИСЦИПЛИНЫ

Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки. Обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на

	практическом занятии. Уделить внимание следующим понятиям (перечисление понятий) и др.
Лабораторная работа	Внимательно ознакомиться с целью, задачами и описанием лабораторной работы. Изучить теоретический материал, выполнить практическое задание, используя необходимые программные и аппаратно-технические средства, оформить отчет в соответствии с заданием и требованиями нормоконтроля. Ответить на вопросы по теме лабораторной работы. В ходе выполнения лабораторных работ раскрываются основные вопросы в рамках рассматриваемой темы, делаются акценты на наиболее сложные, проблемные и моменты изучаемого материала, которые должны быть приняты студентами во внимание. Основной целью лабораторных занятий является расширение и углубление материала практического характера, контроль качества усвоения пройденного материала и ходом выполнения студентами заданий. При подготовке к зачету необходимо ориентироваться на лекции, результаты выполненных лабораторных работ и рекомендуемую литературу.
Практические (семинарские) занятия	Обобщение, расширение и углубление пройденного материала на лекции. Решение задач на закрепление практических навыков. 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 и коллоквиумах. Контроль качества усвоения пройденного материала.
Курсовая работа	Изучение научной, учебной, нормативной и другой литературы. Отбор необходимого материала; формирование выводов и разработка конкретных рекомендаций по решению поставленной задачи; проведение практических исследований по заданной теме. Инструкция по выполнению требований к оформлению курсовой работы (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции).
Самостоятельная работа	Изучение лекционного материала и восстановление в памяти изученного в ходе выполнения лабораторной работы материала, который необходим для защиты лабораторной работы, понимания нового материала, подготовки к экзамену. Работа с учебником, лекцией, лабораторным практикумом, сетью Интернет. Со стороны преподавателя: формулировка указаний и инструкций по выполнению самостоятельной работы, описание формы контроля и критериев оценивания.
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.	

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.40 Разработка и эксплуатация автоматизированных систем в защищенном исполнении*

Приложение № 1 к рабочей программе

Специальность– *10.05.03 Информационная безопасность автоматизированных систем*
Специализация/ – *Специалист по защите информации*

ИРКУТСК

1. Общие положения

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

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

Задачами ФОС являются:

– оценка достижений обучающихся в процессе *изучения дисциплины (модуля)*

– 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 «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» участвует в формировании компетенций:

ОПК.7 Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;

ОПК.2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;

УК.2 Способен управлять проектом на всех этапах его жизненного цикла

Программа контрольно-оценочных мероприятий очная форма обучения

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятие/тем/раздел и т.д. дисциплины)	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
8 семестр					
1	2	3	4	5	6
2	1 2 3 4	Текущий контроль	Раздел 1. Угрозы безопасности информационных систем и их классификация	ОПК.7 ОПК.2 УК.2	Защита лабораторной работы
3	5 6 7	Текущий контроль	Раздел 2. Управление информационными рисками	ОПК.7 ОПК.2 УК.2	Защита лабораторной работы
4	8 9 10	Текущий контроль	Раздел 3. Обеспечение конфиденциальности обрабатываемой программой информации	ОПК.7 ОПК.2 УК.2	Защита лабораторной работы
5	11 12	Текущий контроль	Раздел 4. Технология электронной подписи при обработке программой информации	ОПК.7 ОПК.2 УК.2	Защита лабораторной работы

6	14 15 16 17	Текущий контроль	Раздел 5. Технологии и методы аутентификации	ОПК.7 ОПК.2 УК.2	Защита лабораторной работы

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

Описание показателей и критериев оценивания компетенций.
Описание шкал оценивания

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

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

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

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

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	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. Отчет по работе должен содержать полное решение поставленной задачи и ответы на поставленные в ней вопросы	Темы лабораторных работ и требования к их защите
2	Курсовой проект (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 курсовой проект (работу)
3	Конспект	Средство, позволяющее формировать и оценивать способность обучающегося к восприятию, обобщению и анализу информации. Рекомендуется для оценки знаний и умений обучающихся	Темы конспектов по дисциплине
4	Тест	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

		Тестирование проводится два раза за семестр – в середине семестра и за две недели до его окончания	
5	экзамен	Средство, позволяющее оценить знания, умения и владения обучающегося по дисциплине.	экзамен

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

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенции
«отлично»	«зачтено»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
«хорошо»		Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
«удовлетворительно»		Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный
«неудовлетворительно»	«не зачтено»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенция не сформирована

Защита лабораторной работы

Шкала оценивания		Критерии оценивания
«отлично»	«зачтено»	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»	«не зачтено»	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

Курсовая работа

Шкала оценивания	Критерии оценивания
«отлично»	– содержание и оформление курсовой работы соответствует требованиям методических указаний и теме работы; – курсовая работа актуальна, выполнена самостоятельно, имеет творческий характер, отличается определенной новизной; – в курсовой работе дан обстоятельный анализ степени теоретического исследования проблемы, различных подходов к ее решению; – в докладе и ответах на вопросы обучающийся показал знание нормативной базы, учтены последние изменения в законодательстве и нормативных документах по данной проблеме; – проблема раскрыта глубоко и всесторонне, материал изложен логично; – теоретические положения органично сопряжены с практикой; даны представляющие интерес практические рекомендации, вытекающие из анализа проблемы; – в курсовой работе широко используются материалы исследования, проведенного обучающимся самостоятельно или в составе группы (в отдельных случаях допускается опора на вторичный анализ имеющихся данных); – в курсовой работе проведен количественный анализ проблемы, который подкрепляет теорию и иллюстрирует реальную ситуацию, приведены таблицы сравнений, графики, диаграммы, формулы, показывающие умение обучающегося формализовать результаты исследования; – широко представлен список использованных источников по теме работы; – приложения к работе иллюстрируют достижения обучающегося и подкрепляют его выводы; – по своему содержанию и форме курсовая работа соответствует всем предъявленным требованиям
«хорошо»	– содержание и оформление курсовой работы соответствует требованиям методических указаний; – содержание курсовой работы в целом соответствует заявленной теме; – курсовая работа актуальна, написана самостоятельно; – в курсовой работе дан анализ степени теоретического исследования проблемы;

	– в докладе и ответах на вопросы основные положения курсовой работы раскрыты на хорошем или достаточном теоретическом и методологическом уровне; – теоретические положения сопряжены с практикой; – представлены количественные показатели, характеризующие проблемную ситуацию; – практические рекомендации обоснованы; – приложения грамотно составлены и прослеживается связь с положениями курсовой работы; – составлен список использованных источников по теме курсового проекта (работы)
«удовлетворительно»	– содержание и оформление курсовой работы соответствует требованиям методических указаний; – имеет место определенное несоответствие содержания курсовой работы заявленной теме; – в докладе и ответах на вопросы исследуемая проблема в основном раскрыта, но не отличается новизной, теоретической глубиной и аргументированностью, имеются не точные или не полностью правильные ответы; – нарушена логика изложения материала, задачи раскрыты не полностью; – в курсовой работе не полностью использованы необходимые для раскрытия темы научная литература, нормативные документы, а также материалы исследований; – теоретические положения слабо увязаны с управленческой практикой, практические рекомендации носят формальный бездоказательный характер;
«неудовлетворительно»	– содержание и оформление курсовой работы не соответствует требованиям методических указаний; – содержание курсовой работы не соответствует ее теме; – в докладе и ответах на вопросы даны в основном неверные ответы; – курсовая работа содержит существенные теоретико-методологические ошибки и поверхностную аргументацию основных положений; – курсовая работ носит умозрительный и (или) компилятивный характер

Оценочное средство «Тест».

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

Тесты формируются из фонда тестовых заданий по дисциплине. Структура фонда тестовых заданий по дисциплине, структуры тестов по итогам каждого семестра (если дисциплина не является односеместровой) и итогового теста по дисциплине и типовые примеры тестов приведены в разделе 3 данного документа.

Результаты тестирования могут быть использованы при проведении промежуточной аттестации, как в форме зачета, так и в форме экзамена.

Промежуточная аттестация в форме зачета:

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

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 Типовые контрольные задания

«Контроль целостности информации при случайных воздействиях»

Целью работы является изучение различных методов обнаружения ошибок при передаче сообщений и их сравнение.

Введение

Целостность информации может быть нарушена путем ее модификации, уничтожения, замены, повтора или другого типа искажения. Целостность информации может нарушиться либо злоумышленником, либо случайным воздействием внешней и внутренней среды, включая людей.

В контрольной работе рассматриваются методы контроля целостности информации (сообщений) при случайных воздействиях. Предполагается, что одна сторона (отправитель) отправляет сообщение, а другая (получатель) получает его. При передаче в канале связи возможно нарушение целостности сообщения.

Методы контроля целостности информации от случайных воздействий делят на методы обнаружения ошибок (обнаружения самого факта ошибок без определения их положения в сообщении) и методы обнаружения ошибок с определением их положения в сообщении и последующим исправлением. В обоих этих случаях рассматривают одиночную ошибку и случай более одной ошибки.

В контрольной работе рассматриваются методы обнаружения ошибок. Предполагается, что одна сторона (отправитель) отправляет сообщение, а другая (получатель) получает его. При передаче в канале связи возможно нарушение целостности сообщения от случайных воздействий. Получатель должен иметь возможность проверить нарушена или нет целостность информации.

Технология и методы контроля целостности информации

Технология контроля целостности следующая:

1) отправитель, используя метод контроля, формирует контрольное значение для сообщения ($КО_m$), которое передает совместно с сообщением m;

2) получатель, получив сообщение *m* и контрольное значение отправителя $КО_m$, используя тот же метод контроля, создает свое контрольное значение ($КР_m$);

3) получатель сравнивает контрольные значения: $КО_m$= $КР_m$. Если они совпадают, то получатель считает, что целостность информации не нарушена; иначе она нарушена и надо повторить передачу сообщения.

В случае обнаружения одиночной ошибки на практике используются метод контроля четности и метод контрольной суммы.

При использовании метода контроля четности для каждого байта информации резервируется один разряд (бит), который и является контрольным значением. Значение бита четности является результатом сложения по модулю 2 байта сообщения. Например: 10010010 1; 00010100 0.

Напомним, что таблица истинности для сложения по модулю 2 имеет вид: 0(+)0=0; 1(+)0=1; 0(+)1=1; 1(+)1=0. Отличие от обычного сложения заключается в том, что в последней комбинации при сложении по модулю 2 отсутствует единица переноса, что существенно повышает быстродействие этой операции.

Если сообщение представляется двумерной структурой, то бит четности формируется по каждому столбцу, который является также результатом сложения по модулю 2. Совокупность этих битов четности образует контрольное значение, которое называют контрольной суммой (КС). Размерность контрольной суммы определяется размерностью данных в файле. Например: 2-х, 4-х, 8-и байтовое слово. Рассмотрим пример для 2-х байтового слова (рис. 1).

10010100 01100101
10100010 00011101
<u>10000110 00011101</u>
КС 10110000 01100101

Рис. 1. Создание контрольной суммы

Используя операцию сложения по модулю 2, для первого столбца получим 1, для второго 0 и т.д.

Метод контрольной суммы используется в сетевых технологиях, например, в протоколе *TCP* для Интернета. При сетевой передаче сообщение разбивается на пакеты, далее для каждого пакета формируется своя контрольная сумма. Если контрольные суммы отправителя и получателя совпадают, то считается, что целостность пакета не нарушена. Метод контрольной суммы является достаточно быстродействующим, но он обнаруживает одиночную ошибку по каждому столбцу файла. В связи с этим, в настоящее время в сетевых протоколах используется метод циклического контроля (*CRC*), который позволяет обнаруживать более одной ошибки.

При методе *CRC* сообщение рассматривается как *N*-разрядное двоичное число, где *N* – количество битов в сообщении. Далее оно специальным образом делится на простое целое число до получения остатка. Этот остаток иногда по аналогии с методом контрольной суммы называют контрольной суммой.

Остаток является искомым контрольным значением. Его вычисляет как отправитель, так и получатель.

При делении *N*-разрядного числа на простое число (его еще называют полиномом) используется деление по модулю два. Разрядность полинома должна быть на один бит больше, чем разрядность остатка. Для однобайтового остатка рекомендуется полином 100011011 или 10110000 1.

Деление по модулю 2 осуществляется сложением по модулю 2. Рассмотрим этот метод на примере (рис. 2): сообщение 101111001110, полином 10011 (простое число), остаток имеет четыре бита.

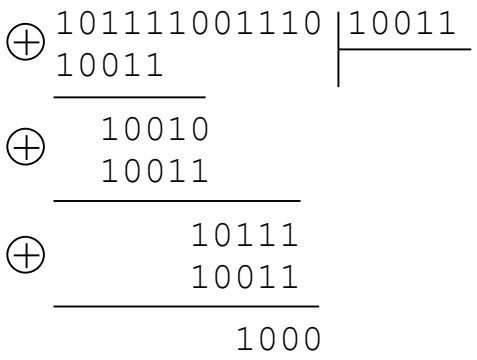

Рис. 2. Деление по модулю 2

Остаток от деления равен 1000. На практике для больших значений *N* при делении используется специально составленная таблица размером 2^nx*n*, где *n* – разрядность остатка (контрольного значения).

Помимо современных сетевых протоколов, метод *CRC*, например, используется при обмене информацией между оперативной и внешней памятью (винчестером).

Список контрольных вопросов

1. Что такое целостность информации.
2. Что понимается под случайным воздействием на информацию.
3. Опишите технологию контроля информации при случайных воздействиях.
4. В чем отличие методов обнаружения ошибок от методов обнаружения и исправления ошибок.
5. Отличие сложения по модулю 2 от обычного сложения.
6. Стандарты информационной безопасности.
7. Характеристика и классификация угроз информационной безопасности.
8. Методы оценки субъективных вероятностей.
9. Управление рисками информационной безопасности.

10.Понятие уязвимости системы защиты информации.

11. Возможные подходы к оценке рисков.

12. Этапы процесса управления рисками.

13. Назначение и функции программных продуктов для аудита информационной безопасности и анализа рисков.

14. Вопросы по методике определения информационных рисков.

Содержание контрольной работы

1. Используя данные своего варианта (табл. 1), записать файл (сообщение m) в виде матрицы, длина строки равна байту, число строк равно четырем. При переходе от 16-ричной системы к двоичной можно использовать таблицу 3.1 из лабораторной работы №3.
2. Найти контрольную сумму отправителя ($КО_m$);
3. Изменить один бит (выбрать самому) в исходном сообщении и найти контрольную сумму получателя ($КР_m$);
4. Убедиться, что контрольные суммы не совпадают;
5. Изменить два бита в одном столбце исходного сообщения;
6. Найти контрольную сумму получателя ($КР_m$) и убедиться, что контрольные суммы отправителя и получателя совпадают. Объяснить почему;
7. Найти остаток от деления по модулю 2 для исходного сообщения (значение полинома имеется в таблице 1) – (ОО);
8. Найти остаток от деления по модулю 2 для сообщения с двумя ошибками – (ОР);
9. Убедиться, что остатки не совпадают. Объяснить почему.

Варианты контрольной работы

Таблица 1

№	Исходное сообщение	Полином
1	A6, BC, 67, 9F	100011011
2	C6, BC, D7, 9F	100011011
3	D6, BC, A5, 3A	100011011
4	B4, B1, 6A, 9E	100011011
5	A6, BE, 62, 8C	100011011
6	A7, CC, DA, 9F	100011011
7	B6, AC, 67, 7E	100011011
8	A6, 4C, 52, 9D	100011011

9	CA, B4, D7, 97	101100001
10	D6, BC, A5, 3A	101100001
11	F4, B1, 6A, 9E	101100001
12	C6, BE, 62, 8C	101100001
13	B7, C5, D1, 9F	101100001
14	E3, AC, 6A, 7E	101100001
15	A2, 4C, C2, 9D	101100001
16	A8, BC, E7, 9F	101100001
17	FA, B4, 37, 97	100011011
18	E6, BC, D7, 3A	100011011
19	A4, B1, 6A, 9E	100011011
20	CB, BE, 62, 8C	101100001

1. Стандарты информационной безопасности.
2. Характеристика и классификация угроз информационной безопасности.
3. Методы оценки субъективных вероятностей.
4. Управление рисками информационной безопасности.
5. Понятие уязвимости системы защиты информации.
6. Возможные подходы к оценке рисков.
7. Этапы процесса управления рисками.
8. Назначение и функции программных продуктов для аудита информационной безопасности и анализа рисков.
9. Вопросы по методике определения информационных рисков.

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

Раздел дисциплины	Тема раздела	Объекты темы	Количество тестовых заданий (ТЗ), типы ТЗ
Раздел 1. Угрозы безопасности информационных систем и их классификация.	Цели и задачи безопасности и защиты программных систем. Основные виды угроз. Характеристика и классификация угроз и атак /Лек/		19 – тип А 17 – тип В
	Проработка лекционного материала: цели и задачи безопасности и защиты программных систем, основные виды угроз, характеристика и классификация угроз и атак /Ср/		

		Итого по разделу	**∑36 19 – тип А 17 – тип В**
Раздел 2. Управление информационными рисками .	Неопределенность и риск. Модели оценки рисков. Трехфакторная модель оценки информационных рисков /Лек/		14 – тип А 22 – тип В
	Проработка лекционного материала: неопределенность и риск, модели оценки рисков, трехфакторная модель оценки информационных рисков /Ср/		
	Подготовка к лабораторному занятию «Контроль целостности информации при случайных воздействиях» / Пр /		
	Контроль целостности информации при случайных воздействиях /Лаб/		
		Итого по разделу	**∑36 14 – тип А 22– тип В**
Раздел 3. Обеспечение конфиденциальности обрабатываемой программой информации.	Основные понятия криптографии. Российский алгоритм криптографического преобразования /Лек/		15– тип В
	Проработка лекционного материала: основные понятия криптографии, российский алгоритм криптографического преобразования /Ср/		
	Двухключевые криптосистемы. Современный протокол шифрования информации /Лек/		5 – тип А 16 – тип В
	Проработка лекционного материала: двухключевые криптосистемы, современный протокол шифрования информации /Ср/		
	Подготовка к лабораторному занятию «Методика определения информационных рисков» /Пр/		

	Методика определения информационных рисков /Лаб/		
Итого по разделу			**∑36 5 – тип А 31 – тип В**
Раздел 4. Технология электронной подписи при обработке программой информации.	Хэш-функции, российский стандарт. Правовое обеспечение электронной подписи /Лек/		20 – тип А 4 – тип В
	Проработка лекционного материала: Хэш-функции, российский стандарт, правовое обеспечение электронной подписи /Ср/		
	Криптографические методы технологии электронной подписи, российский стандарт /Лек/		12 – тип А
	Проработка лекционного материала: криптографические методы технологии электронной подписи, российский стандарт /Ср/		
	Подготовка к Лабораторному занятию «Порядок проведения классификация информационных систем в РФ» / Пр /		
	Порядок проведения классификация информационных систем в РФ /Лаб/		
Итого по разделу			**∑36 32 – тип А 4 – тип В**
Раздел 5. Технологии и методы аутентификации Основные понятия и определения.	Инфраструктура управления открытыми ключами /Лек/		**20– тип А 16 – тип В**
	Проработка лекционного материала: основные понятия и определения, инфраструктура управления открытыми ключами /Ср/		
	Подготовка к лабораторному занятию «Технология применения электронной подписи» / Пр /		
	Технология применения электронной подписи /Лаб/		
Итого по разделу			**∑36 20 – тип А 16 – тип В**
Итого по дисциплине			**∑ 180 106 – тип А 74– тип В**

Тестирование по дисциплине

1) Укажите двухключевую криптосистему:

А) DES

Б) RSA

В) AES

Г) ГОСТ 28147-89

2) Укажите одностороннюю функцию для алгоритма *RSA*:

А) $(e \cdot d) \bmod k = 1; k=p \cdot (q-1);$

Б) $y = a^x \bmod p;$

В) $n = p \cdot q;$

Г) $c = m^e \bmod (n-1);$

3) При зашифровании данных несимметричной криптосистемой, используется:

А) секретный ключ

Б) открытый ключ

В) сначала открытый, а затем секретный ключ

Г) сначала секретный, а затем открытый ключ

4) Размер хэш-образа по российскому стандарту (ГОСТ-2012) равен:

А) 256 бит или 512 бит

Б) 512 бит или 160 бит

В) 160 бит

Г) 320 бит

5) Двухключевая криптосистема по сравнению с одноключевой имеет более высокую производительность при шифровании данных:

А) ДА

Б) НЕТ

6) Современный протокол шифрования данных базируется на совместном применении как симметричной криптосистемы так и несимметричной:

А) ДА

Б) НЕТ

7) Хэш-функция – это криптографическое преобразование информации, переводящее строку битов произвольной длины в строку битов фиксированной длины:

А) ДА

Б) НЕТ

8) В электронном документообороте наилучшим способом контроля целостности данных является:

А) шифрование

Б) электронная цифровая подпись

В) хэширование

9) Увеличение длины ЭЦП в 2 раза по сравнению с хэш-образом это свойство ЭЦП:

А) ДА

Б) НЕТ

10) Размер ЭЦП по российскому стандарту (ГОСТ-2012) равен:

А) 256 бит 512 бит

Б) 512 бит или 1024 бит

В) 1024 бит

Г) 320 бит

11) При шифровании данных несимметричной криптосистемой, используется:

А) секретный ключ

Б) открытый ключ

В) сначала открытый, а затем секретный ключ

Г) сначала секретный, а затем открытый ключ

12) При создании ЭЦП секретный ключ по длине больше, чем открытый:

А) ДА

Б) НЕТ

13) Размер хэш-образа по американскому стандарту *SHA*-1 равен:

А) 256 бит

Б) 512 бит

В) 160 бит

Г) 320 бит

14) В современном протоколе шифрования данных при шифровании сообщений используется двухключевая криптосистема:

А) ДА

Б) НЕТ

15) Размер ЭЦП по американскому стандарту *DSS* равен:

А) 256 бит

Б) 512 бит

В) 1024 бит

Г) 320 бит

16) В электронном документообороте наилучшим способом обеспечения конфиденциальности данных является:

А) шифрование

Б) электронная цифровая подпись

В) хэширование

17) Укажите одностороннюю функцию для алгоритма Эль-Гамаля:

А) $(e \cdot d) \bmod k = 1; k=p \cdot (q-1);$

Б) $y = a^x \bmod p;$

В) $n = p \cdot q;$

Г) $c = m^e \bmod (n-1);$

18) Выберите наиболее эффективную криптосистему для шифрования незначительных по объему данных:

А) RSA

Б) AES

В) DES

Г) ГОСТ 28147-89

19) Двухключевую криптосистему называют криптосистемой с открытым ключом, т.к. при шифровании открытый ключ создает отправитель, а секретный – получатель:

А) ДА

Б) НЕТ

20) Пару ключей при шифровании данных криптосистемой с открытым ключом создает отправитель:

А) ДА

Б) НЕТ

21) Владельцем пары ключей при создании ЭЦП является отправитель:

А) ДА

Б) НЕТ

22) Хэширование сообщения при создании ЭЦП осуществляется, чтобы:

А) обеспечить конфиденциальность информации

Б) увеличить время создания ЭЦП

В) стандартизовать время создания ЭЦП и ее размер

23) Хэш-функция может применяться в следующих случаях:

А) для создания сжатого образа сообщения, используемого в механизме цифровой подписи;

Б) для защиты пароля;

В) при контроле целостности данных;

Г) для сохранения конфиденциальности информации.

24) Коллизия в хэш-функции, это когда разные сообщения имеют одинаковый хэш-образ:

А) ДА

Б) НЕТ

25) В современном протоколе шифрования данных для шифрования секретного ключа симмеричной криптосистемы используется двухключевая криптосистема:

А) ДА

Б) НЕТ

26) Двухключевая криптосистема может применяться в следующих случаях:

А) для шифрования небольших по объему данных;

Б) при создании электронно-цифровой подписи;

В) в задачах аутентификации;

Г) для обеспечения доступности информации.

Перечень тем курсовых работ

1. Информационные технологии, используемые в АИС.
2. Основные угрозы безопасности информации в автоматизированных системах.
3. Модели нарушителя в автоматизированных системах.
4. Методы, способы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем.
5. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.
6. Методы обеспечения информационной безопасности АИС.
7. Методы и этапы проектирования защищенных АИС.
8. Построение комплексной защиты АИС.
9. Основы проектирования комплексной защиты информационной безопасности от НСД.
10. Средства обеспечения надежности защищенных АИС.
11. Технологии создания отказоустойчивых систем.
12. Аттестация АИС по требованиям безопасности.
13. Особенности эксплуатации АИС на объекте защиты.
14. Требования и рекомендации по защите служебной тайны и персональных данных при работе АИС.
15. Порядок обеспечения защиты информации при эксплуатации АИС.
16. Технические и программные средства защиты АИС от несанкционированного доступа.
17. Организация технического обслуживания защищенных АИС.
18. Методы проверки защищенных АИС.
19. Средства диагностирования защищенных АИС.
20. Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств АИС.

21. Технологическое оборудование для ремонта аппаратных средств АИС.
22. Диагностические программы и пакеты диагностических программ, их

назначение, возможности и порядок использования.
23. Аппаратно-программные средства диагностики АИС.
24. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков

Перечень теоретических вопросов к экзамену

1. Информационная безопасность и безопасность информации.
2. Понятия приоритета, охраны и защиты интеллектуальной собственности.
3. Аспекты безопасности информации.
4. Основные виды угроз.
5. Правовое обеспечение интеллектуальной собственности и информационной безопасности. Содержание конфиденциальной информации, определенной Указом Президента РФ.
6. Особенности обработки персональных данных.
7. Виды ИСПДн, уровни защищенности ПДн.
8. Технология и методы контроля целостности информации при случайных воздействиях.
9. Характеристика ФЗ об электронной подписи, виды ЭП.
10. Основные понятия криптографии.
11. Поточное шифрование сообщений.
12. Характеристика блочных симметричных криптосистем.
13. Алгоритм DES и его развитие.
14. Стандарт криптографической защиты AES.
15. Российский алгоритм криптографического преобразования: режимы шифрования.
16. Российский алгоритм криптографического преобразования: режим имитовставки.
17. Несимметричные системы шифрования. Современный протокол шифрования данных.
18. Алгоритм RSA. Сравнение симметричных и несимметричных криптосистем.
19. Определение и назначение хэш-функции, российский стандарт.
20. Электронная подпись: определения, назначение, роль в электронном документообороте.
21. Российский стандарт ЭП: технология создания и проверки.
22. Обмен Диффи-Хеллмана. Назначение мастер-ключа.
23. Биометрическая аутентификация пользователя.
24. Цели, структура и функции системы защиты информации.
25. Инфраструктура управления открытыми ключами.

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/практики.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Тест	Тестирование с применением компьютерных технологий проводится по окончанию каждого семестра и по окончанию изучения дисциплины и (или) в течение года по

	завершению изучения дисциплины (контроль/проверка остаточных знаний, умений, навыков и (или) опыта деятельности). Тесты формируются из фонда тестовых заданий по дисциплине. Структура фонда тестовых заданий по дисциплине, структуры тестов по итогам каждого семестра и итогового теста по дисциплине и типовые примеры тестов приведены в разделе 3 данного документа. Результаты тестирования могут быть использованы при проведении промежуточной аттестации, как в форме зачета, так и в форме экзамена. Описание требований, выполнение которых необходимо для успешного выполнения теста: тематика теста; перечень знать, уметь, владеть; виды и количество предъявляемых обучающемуся тестовых заданий; проходной балл; критерии оценки; норма времени; дополнительные требования, включая необходимость использования справочных таблиц и проч. Тесты для самоконтроля обучающихся по разделам дисциплины, сформированы их из материалов фонда тестовых заданий дисциплины. Требования к тестам для самоконтроля аналогичны требованиям к итоговым тестам по семестрам и дисциплине в целом
Защита лабораторной работы	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Курсовой проект (работа)	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения

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 типовых простых практических заданий к зачету/экзамену для оценки умений;

– перечень типовых практических заданий к зачету/экзамену для оценки навыков и (или) опыта деятельности.

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 и результатами тестирования по материалам, изученным в течении семестра. Оценочные средства и типовые контрольные задания, используемые при текущем контроле, в совокупности с тестированием, позволяют оценить знания, умения и владения навыками/опытом деятельности обучающихся при освоении дисциплины. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок). Время проведения тестирования объявляется обучающимся заранее.

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

Средняя оценка уровня сформированности компетенций	Оценка

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

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

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. Билеты составлены таким образом, что в каждый из них включал в себя теоретические вопросы и практические задания.

Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену; три практических задания: два из них для оценки умений (выбираются из перечня типовых простых практических заданий к экзамену); третье практическое задание для оценки навыков и (или) опыта деятельности (выбираются из перечня типовых практических заданий к экзамену).

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект билетов (25-30 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/задание 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 2020-2021 учебный год	**Экзаменационный билет № 1** **по дисциплине «_____»** ***Специализация/профиль*** **____ семестр**	Утверждаю: Заведующий кафедрой «_____»ИрГУПС _____

1. …….
2. …….
3. ……..
4. ……..
5 ……..…….

Варианты размеров билета:
Билет формата А5 – 148*210мм
Билет формата А4 – 210*297мм