ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

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

Б1.В.ДВ.07.02 Управление информационной безопасностью

рабочая программа дисциплины

Специальность/направление подготовки – 09.04.02 Информационные системы и технологии
Специализация/профиль – Информационные системы и технологии на транспорте
Квалификация выпускника – Магистр
Форма и срок обучения – очная форма 2 года; заочная форма 2 года 5 месяцев
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 4
Часов по учебному плану (УП) – 144
В том числе в форме практической подготовки (ПП) – 10/4
(очная/заочная)

Формы промежуточной аттестации
очная форма обучения:
экзамен 3 семестр
заочная форма обучения:
экзамен 2 курс

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

Семестр	3	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	34/10	**34/10**
– лекции	17	**17**
– практические (семинарские)		
– лабораторные	17/10	**17/10**
Самостоятельная работа	74	**74**
Экзамен	36	**36**
Итого	144/10	**144/10**

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

Курс	2	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	8/4	**8/4**
– лекции	4	**4**
– практические (семинарские)		
– лабораторные	4/4	**4/4**
Самостоятельная работа	118	**118**
Экзамен	18	**18**
Итого	144/4	**144/4**

* В форме ПП – в форме практической подготовки.

ИРКУТСК

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

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – магистратура по направлению подготовки 09.04.02 Информационные системы и технологии, утвержденным Приказом Министерства науки и высшего образования Российской Федерации от 19.09.2017 № 917.

Программу составил(и):
д.т.н., профессор, профессор, Ю.М. Краковский

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

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

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цели дисциплины	
1	формирование у обучающихся важнейших представлений о современных методах защиты информации
2	формирование компетенций в области моделей и методов защиты информации
1.2 Задачи дисциплины	
1	изучение теоретических основ и приобретение практических навыков по созданию и использованию современных средств защиты информации с учетом требований информационной безопасности применительно к ОВС
2	освоить современные методы защиты информации, обеспечивающих целостность, конфиденциальность и доступность информации

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
Блок/часть ОПОП	Блок 1. Дисциплины / Часть, формируемая участниками образовательных отношений
2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины	
1	Дисциплина изучается на начальном этапе формирования компетенции
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б2.О.04(Пд) Производственная - преддипломная практика
2	Б3.01(Д) Выполнение выпускной квалификационной работы
3	Б3.02(Д) Защита выпускной квалификационной работы

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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ПК-3 Способен организовать управление оценкой рисков по комплексной безопасности и планирование надёжности сложных информационных систем	ПК-3.2 Осуществляет управление безопасностью корпоративных информационных системам, включая вопросы целостности, конфиденциальности и доступности информации	Знать: принципы, методы и средства обеспечения качественного режима работы ОВС с учетом информационной безопасности и КМЗИ
		Уметь: осуществлять управление оценкой рисков по комплексной безопасности ИС
		Владеть: средствами обеспечения целостности, конфиденциальности и доступности информации с учетом различных методов защиты, включая КМЗИ

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					Заочная форма					*Код индикатора достижения компетенции
		Семестр	Часы				Курс	Часы				
			Лек	Пр	Лаб	СР		Лек	Пр	Лаб	СР	
1.0	**Раздел 1. Организационно-правовые основы построения открытых вычислительных систем.**											
1.1	Тема 1. Характеристика ОВС. Основные понятия и определения, связанные с информационной безопасностью						2/уст.				16	ПК-3.2
1.2	Тема 2. Организационно-правовое обеспечение безопасности информации. Правовое						2/уст.				14	ПК-3.2

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					Заочная форма					*Код индикатора достижения компетенции
		Семестр	Часы				Курс	Часы				
			Лек	Пр	Лаб	СР		Лек	Пр	Лаб	СР	
	обеспечение электронной подписи											
2.0	**Раздел 2. Средства обеспечения защиты информации применительно к открытым вычислительным системам.**											
2.1	Тема 3. Основные понятия криптографии. Поточное шифрование. Современные алгоритмы криптографического преобразования						2/уст.	2			28	ПК-3.2
2.2	Лабораторная работа «Протокол Диффи-Хеллмана».						2/уст.			2/2		ПК-3.2
2.3	Тема 4. Двухключевые криптосистемы. Технологии шифрования. Национальные стандарты электронной подписи						2/уст.	2			30	ПК-3.2
2.4	Лабораторная работа «Этапы технологии электронной подписи».						2/уст.			2/2		ПК-3.2
3.0	**Раздел 3. Управление информационными рисками для обеспечения защищенности ОВС.**											
3.1	Тема 5. Управление информационными рисками для обеспечения защищенности ОВС						2/уст.				25	ПК-3.2
	Форма промежуточной аттестации – экзамен						2/зимняя	18				ПК-3.2
	Контрольная работа						2/зимняя				5	ПК-3.2
	Итого часов (без учёта часов на промежуточную аттестацию)		17		17/10	74		4		4/4	118	

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

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

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.1.1	Краковский, Ю. М. Методы и средства защиты информации : учебное пособие для вузов / Ю. М. Краковский. — Санкт-Петербург : Лань, 2024. — 272 с. — URL: https://e.lanbook.com/book/385979 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.2	Паршин, К. А. Оценка уровня информационной безопасности на объекте информатизации : учеб. пособие для вузов ж.-д. трансп. / К. А. Паршин. — М. : УМЦ по образованию на ж.-д. трансп., 2015. — 95 с. — Текст : непосредственный.	20
6.1.2 Дополнительная литература		
	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Краковский, Ю. М. Информационная безопасность и защита информации : учеб. пособие / Ю. М. Краковский. Иркутск : ИрГУПС, 2016. - 224с.	93
6.1.2.2	Бутин, А. А. Методы и средства защиты информации от несанкционированного доступа. Программно-аппаратный уровень : учеб. пособие по дисциплинам "Программно-аппаратные средства обеспечения информационной безопасности" и "Программно-аппаратные средства защиты информации" / А. А. Бутин. Иркутск : ИрГУПС, 2015. - 95с.	40
6.1.2.3	Краковский, Ю. М. Методы защиты информации : учебное пособие / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — URL: https://e.lanbook.com/book/156401 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)		
	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.3.1	Краковский Ю.М. Методические указания по изучению дисциплины Б1.В.ДВ.07.02 Управление информационной безопасностью по направлению подготовки 09.04.02 Информационные системы и технологии, профиль Информационные системы и технологии на транспорте / Ю.М. Краковский ; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 12 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_4545_1404_2022_1_signed.pdf	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/	
6.3 Программное обеспечение и информационные справочные системы		
6.3.1 Базовое программное обеспечение		
6.3.1.1	Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.2	Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.3	FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/	
6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/	
6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License	
6.3.2 Специализированное программное обеспечение		
6.3.2.1	Не предусмотрено	
6.3.3 Информационные справочные системы		
6.3.3.1	Не предусмотрены	
6.4 Правовые и нормативные документы		
6.4.1	Не предусмотрены	

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

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л ИрГУПС находится – по адресу г. Иркутск, ул. Лермонтова, д.80

2	Компьютерный класс «Информатика». «Технологии и методы программирования» Д-503 для проведения практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: Специализированная мебель, компьютеры с подключением к сети Интернет, обеспечивающие доступ в электронную информационно-образовательную среду ИрГУПС, учебно-наглядные пособия (презентации, плакаты).
3	Учебная аудитория Д-417 для проведения лекционных и практических занятий, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: Специализированная мебель, мультимедиапроектор, экран, компьютер. Для проведения занятий имеются учебно-наглядные пособия (презентации, плакаты).
4	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507; – помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Лабораторная работа	Основной целью лабораторных работ является теоретическое обоснование, наглядное и/или экспериментальное подтверждение и/или проверка существенных теоретических положений (законов, закономерностей) анализ существующих методик и методов их реализации и т.д. Они занимают преимущественное место при изучении дисциплин

	обязательной части и части, формируемой участниками образовательных отношений Блока 1. Исходя из цели, содержанием лабораторных работ могут быть: - экспериментальная проверка формул, методик расчета; - проведение натурных измерений свойств, рабочих параметров, режимов работы при помощи лабораторного оборудования и/или стендов и макетов; - ознакомление, анализ и теоретические выкладки по устройству, принципу действия и способам обслуживания аппаратов, деталей машин, механизмов, процессов, протекающих в них при этом и т.д.; - наглядная графическая интерпретация чертежей, схем, объемных поверхностей и т.д., воспроизводимых с помощью специализированного программного обеспечения; - имитационное моделирование процессов, протекающих в сложных химических, физических, механических, электрических и пр. объектах; - наглядное представление о работе персонала конкретной организации или подразделения ОАО «РЖД» посредством моделирования штатных и внештатных ситуаций в виртуальных специализированных АРМ (автоматизированных рабочих мест); - установление и подтверждение закономерностей (путем сравнения проведенного эксперимента и рассчитанных значений) и т.д.; - ознакомление с методиками проведения экспериментов, наглядным устройством стенд-макетов и пр.; - установление свойств веществ, их качественных и количественных характеристик; - анализ различных характеристик процессов, в том числе производственных и иных процессов; - расчет параметров различных явлений и процессов, смоделировать которые не возможно в реальных условиях (например, чрезвычайные ситуации и пр.); - наблюдение развития явлений, процессов и др. Допускается иное содержание лабораторных работ, если это будет способствовать реализации целей и задач дисциплины и формированию соответствующих компетенций. По характеру выполняемых лабораторных работ возможны: - ознакомительные работы, используемые для закрепления изученного теоретического материалы; - аналитические работы, используемые для получения новой информации на основе формализованных методов; - творческие работы, ориентированные на самостоятельный выбор подходов решения задач. Прежде, чем приступить к лабораторным занятиям, обучающимся необходимо повторить теоретический материал по теме работы. Каждая лабораторная работа оснащена методическими указаниями, разработанными преподавателями, ведущими дисциплину
Самостоятельная работа	Обучение по дисциплине «Управление информационной безопасностью» предусматривает активную самостоятельную работу обучающегося. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а также указана необходимая учебная литература: обучающийся изучает учебный материал, разбирает примеры и решает разноуровневые задачи в рамках выполнения как общих домашних заданий, так и индивидуальных домашних заданий (ИДЗ) и других видов работ, предусмотренных рабочей программой дисциплины. При выполнении домашних заданий обучающемуся следует обратиться к задачам, решенным на предыдущих практических занятиях, решенным домашним работам, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора. Домашние задания, индивидуальные домашние задания и другие работы, предусмотренные рабочей программой дисциплины должны быть выполнены обучающимся в установленные преподавателем сроки в соответствии с требованиями к оформлению текстовой и графической документации, сформулированным в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль»
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет	

Приложение № 1 к рабочей программе

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

1. Общие положения

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

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

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины;

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

– самоподготовка и самоконтроль обучающихся в процессе обучения.

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

Для оценки уровня сформированности компетенций используется трехуровневая система:

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

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

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

2. Перечень компетенций, в формировании которых участвует дисциплина.
Программа контрольно-оценочных мероприятий.
Показатели оценивания компетенций, критерии оценки

Дисциплина «Управление информационной безопасностью» участвует в формировании компетенций:

ПК-3. Способен организовать управление оценкой рисков по комплексной безопасности и планирование надёжности сложных информационных систем

Программа контрольно-оценочных мероприятий заочная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
2 курс, сессия установочная				
1.0	**Раздел 1. Организационно-правовые основы построения открытых вычислительных систем.**			
1.1	Текущий контроль	Тема 1. Характеристика ОВС. Основные понятия и определения, связанные с информационной безопасностью	ПК-3.2	Собеседование (устно)
1.2	Текущий контроль	Тема 2. Организационно-правовое обеспечение безопасности информации. Правовое обеспечение электронной подписи	ПК-3.2	Собеседование (устно)
2.0	**Раздел 2. Средства обеспечения защиты информации применительно к открытым вычислительным системам.**			
2.1	Текущий контроль	Тема 3. Основные понятия криптографии. Поточное шифрование. Современные алгоритмы криптографического преобразования	ПК-3.2	Тестирование (компьютерные технологии)
2.2	Текущий контроль	Лабораторная работа «Протокол Диффи-Хеллмана».	ПК-3.2	Лабораторная работа (письменно/устно)
2.3	Текущий контроль	Тема 4. Двухключевые криптосистемы. Технологии шифрования. Национальные стандарты электронной подписи	ПК-3.2	Собеседование (устно)
2.4	Текущий контроль	Лабораторная работа «Этапы технологии электронной подписи».	ПК-3.2	Лабораторная работа (письменно/устно)
3.0	**Раздел 3. Управление информационными рисками для обеспечения защищенности ОВС.**			
3.1	Текущий контроль	Тема 5. Управление информационными рисками для обеспечения защищенности ОВС	ПК-3.2	Собеседование (устно)
2 курс, сессия зимняя				
	Текущий контроль	Все разделы	ПК-3.2	Контрольная работа (КР) (письменно)
	Промежуточная аттестация	Все разделы	ПК-3.2	Экзамен (собеседование) Экзамен - тестирование (компьютерные технологии)

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

Описание показателей и критериев оценивания компетенций.
Описание шкал оценивания

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

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

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

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

Текущий контроль

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Контрольная работа (КР)	Средство для проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по разделу дисциплины. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Типовое задание для выполнения контрольной работы по разделам/темам дисциплины
2	Собеседование	Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Может быть использовано для оценки знаний обучающихся	Вопросы для собеседования по темам/разделам дисциплины
3	Тестирование (компьютерные технологии)	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
4	Лабораторная работа	Средство, позволяющее оценить умение обучающегося письменно/устно 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	Образец задания для выполнения лабораторной работы и примерный перечень вопросов для ее защиты

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	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 и практических заданий (образец экзаменационного билета) к экзамену

2	Тест – промежуточная аттестация в форме экзамена	Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине (модулю) с использованием информационно-коммуникационных технологий. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий

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

Шкала оценивания	Критерии оценивания	Уровень освоения компетенции
«отлично»	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»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенция не сформирована

Тест – промежуточная аттестация в форме экзамена

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

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Контрольная работа

Шкалы оценивания	Критерии оценивания

«отлично»	«зачтено»	Обучающийся полностью и правильно выполнил задание контрольной работы. Показал отличные знания и умения в рамках усвоенного учебного материала. Контрольная работа оформлена аккуратно и в соответствии с предъявляемыми требованиями
«хорошо»		Обучающийся выполнил задание контрольной работы с небольшими неточностями. Показал хорошие знания и умения в рамках усвоенного учебного материала. Есть недостатки в оформлении контрольной работы
«удовлетворительно»		Обучающийся выполнил задание контрольной работы с существенными неточностями. Показал удовлетворительные знания и умения в рамках усвоенного учебного материала. Качество оформления контрольной работы имеет недостаточный уровень
«неудовлетворительно»	«не зачтено»	Обучающийся не полностью выполнил задания контрольной работы, при этом проявил недостаточный уровень знаний и умений

Собеседование

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Глубокое и прочное усвоение программного материала. Полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания. Обучающийся свободно справляется с поставленными задачами, может обосновать принятые решения, демонстрирует владение разносторонними навыками и приемами выполнения практических работ
«хорошо»		Знание программного материала, грамотное изложение, без существенных неточностей в ответе на вопрос, правильное применение теоретических знаний, владение необходимыми навыками при выполнении практических задач
«удовлетворительно»		Обучающийся демонстрирует усвоение основного материала, при ответе допускаются неточности, при ответе недостаточно правильные формулировки, нарушение последовательности в изложении программного материала, затруднения в выполнении практических заданий Слабое знание программного материала, при ответе возникают ошибки, затруднения при выполнении практических работ
«неудовлетворительно»	«не зачтено»	Не было попытки выполнить задание

Тестирование

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

Лабораторная работа

Шкалы 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

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

3.1 Типовые контрольные задания для выполнения контрольных работ

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

Ниже приведен образец типовых вариантов заданий для выполнения контрольных работ.

«Методы обнаружения и исправления ошибок»

Цель работы – освоить технологию обнаружения и исправления ошибок на примере кода Хэмминга.

Введение

Код называется кодом с исправлением ошибок, если всегда из неправильного кодового набора можно получить правильный. Главным для исправления ошибок является то, что необходимо уметь обнаруживать и выделять местоположение ошибочных битов. Если местоположение ошибки определено, то ее исправление производится путем замены ошибочного разряда на его инверсию: 0→1, 1→0.

Код, в котором возможно обнаружить и исправить ошибки, называют помехозащищенным или корректирующим.

Одним из первых корректирующих кодов, для которого одиночная ошибка не только обнаруживается, но и исправляется, является код Хэмминга. Рассмотрим основные принципы его построения.

Код Хэмминга

Пусть сообщение имеет n информативных разрядов ($m1, \ldots, mn$) и k контрольных разрядов ($p1, \ldots, pk$), которые используются для контроля целостности сообщения. Пронумеруем позиции каждого из ($n+k$) разрядов расширенного сообщения, начиная со значения 1 для старшего разряда (левый бит) и заканчивая значением ($n+k$) для младшего (правый бит). Контрольные разряды размещаются в позициях с номерами

$$2^{d-1},\ d = 1,2, \ldots, k,\ (1, 2, 4, \ldots). \qquad (1)$$

Отправитель должен сформировать контрольные разряды и вставить их в расширенное сообщение в соответствие с выражением 1). Значения контрольных разрядов определяются с использованием сложения по модулю 2 специальных позиций сообщения.

Получатель, используя полученное расширенное сообщение, формирует k-разрядное контрольное слово, используя сложение по модулю 2 специальных позиций расширенного сообщения. Если все разряды этого слова нулевые, то сообщение является целым (принято без искажения).

В любом другом случае код этого слова указывает номер разряда, в котором произошло искажение бита. Получатель, используя операцию инверсии, исправляет ошибку и делает сообщение целым (без искажения). Чтобы в код из k разрядов можно было записать ($n+k+1$) значений, должно выполняться условие

$$2^k \geq n+k+1. \qquad (2)$$

Так, например, если n=4, то k=3, а контрольное слово будет иметь восемь значений. Номера контрольных разрядов (1): 1, 2, 4; при n=8, учитывая (2), k=4, номера контрольных разрядов: 1, 2, 4, 8.

Опишем способ построения кода Хэмминга при n=4 ($m1$, $m2$, $m3$, $m4$) и k=3 ($p1$, $p2$, $p3$). Для этого приведем перечень комбинаций двоичного кода контрольного слова ($c3c2c1$) при k=3 (N – десятичное представление двоичного кода) (рис. 2.1):

	$c3$	$c2$	$c1$	N
0	0	0	0	(ошибка отсутствует)
	0	0	1	1
	0	1	0	2
	0	1	1	3
	1	0	0	4
	1	0	1	5
	1	1	0	6
	1	1	1	7

Рис. 1. Комбинации контрольного слова

Числа 1–7, представленный на рисунке 1, указывают номера ошибочных разрядов в расширенном сообщении:

1	2	3	4	5	6	7
$p1$	$p2$	$m1$	$p3$	$m2$	$m3$	$m4$

Подгруппы для каждого разряда контрольного слова содержат те номера его комбинаций, которые в данном столбце содержат 1. Например, в столбце для $c1$ единица присутствует в комбинациях с номерами 1, 3, 5, 7. Исходя из этого, получаются следующие подгруппы:

$$c1 – (\underline{1}, 3, 5, 7);\ c2 – (\underline{2}, 3, 6, 7);\ c3 – (\underline{4}, 5, 6, 7). \qquad (3)$$

Как мы видим, каждый контрольный разряд входит в одну из подгрупп, номера их позиций подчеркнуты. При формировании контрольного слова $c3c2c1$ к подгруппам (3) применяется операция сложения по модулю 2. Напомним, что контрольное слово формирует получатель.

Как мы уже указывали, отправитель формирует контрольные разряды и расставляет их в расширенном сообщении в соответствии с выражением (2.1). При этом он использует следующие подгруппы:

$$p1 – (3, 5, 7);\ p2 – (3 ,6, 7);\ p3 – (5, 6, 7). \qquad (4)$$

Подгруппы (4) формируются из подгрупп (3).

Если для нашего примера информативная часть расширенного сообщения равна 0101, то с учетом выражения (4):

$$p1=0,\ p2=1,\ p3=0.$$

Тогда

номера разрядов	1	2	3	4	5	6	7
сообщение			0		1	0	1
отправленное сообщение	0	1	0	0	1	0	1
полученное сообщение	0	1	0	0	1	1	1

Значение контрольного слова (3) (используется операция сложения по модулю 2 подгрупп разрядов)

$$c3=1;\ c2=1;\ c1=0;\ (110=6).$$

Таким образом, ошибочен шестой разряд, поэтому единицу в нем надо изменить на ноль (после этого полученное сообщение совпадет с отправленным).

Заметим, что существуют коды, которые обнаруживают и исправляют более одной ошибки. Подобные коды используются в современных процессорах для обнаружения и исправления возможных ошибок при вычислениях.

Список контрольных вопросов

1. Характеристика и классификация угроз информационной безопасности.
2. Дать определение угрозы и уязвимости.
3. Опишите технологию обнаружения и исправления ошибок на примере кода Хэмминга.
4. В чем отличие методов обнаружения ошибок от методов обнаружения и исправления ошибок.
5. Как определить число контрольных разрядов.
6. Как создается контрольное слово и для чего.
7. Сравнить метод КС и метод Хэмминга.

3.2 Типовые контрольные задания для проведения собеседования

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

Ниже приведены образцы типовых вариантов заданий для проведения собеседований.

«Тема 1. Характеристика ОВС. Основные понятия и определения, связанные с информационной безопасностью ОВС»

1. Дать определение открытой вычислительной системы.
2. Что такое целостность информации.
3. Основные направления по нарушению конфиденциальности информации.
4. Основные виды угроз.

«Тема 2. Организационно-правовое обеспечение безопасности информации. Правовое обеспечение электронной подписи»

1. Основные направления в организационном обеспечение по защите информации и информационной безопасности.
2. Приведите органы государственной власти, обеспечивающих информационную безопасность в Российской Федерации.
3. Основные функции Совета безопасности РФ.
4. Основные функции ФСТЭК.

«Тема 4. Двухключевые криптосистемы. Технологии шифрования. Национальные стандарты электронной подписи»

1. Приведите названия пары ключей для двухключевой криптосистемы.
2. Назначение протокола «Диффи-Хеллмана».
3. Кто является владельцем пары ключей при шифровании двухключевой криптосистемой.
4. Назначение усиленной электронной подписи.

«Тема 5. Управление информационными рисками для обеспечения защищенности ОВС»

1. Что такое информационный риск.
2. Какие факторы входят в трехфакторную модель информационного риска.
3. Что такое управление рисками информационной безопасности.

4. Приведите названия российских программ для управление рисками информационной безопасности.

3.3 Типовые контрольные задания для проведения тестирования

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

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД/РПП	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ПК-3.2	Тема 1. Характеристика ОВС. Основные понятия и определения, связанные с информационной безопасностью ОВС	Знание	10 – ОТЗ 10 – ЗТЗ
ПК-3.2	Тема 2. Организационно-правовое обеспечение безопасности информации. Правовое обеспечение электронной подписи	Умение	10 – ОТЗ 10 – ЗТЗ
ПК-3.2	Тема 3. Основные понятия криптографии. Поточное шифрование. Современные алгоритмы криптографического преобразования	Навыки	10 – ОТЗ 10 – ЗТЗ
ПК-3.2	Тема 4. Двухключевые криптосистемы. Технологии шифрования. Национальные стандарты электронной подписи	Знание	5 – ОТЗ 5 – ЗТЗ
		Умение	5 – ОТЗ 5 – ЗТЗ
ПК-3.2	Тема 5. Управление информационными рисками для обеспечения защищенности ОВС	Навыки	10 – ОТЗ 10 – ЗТЗ
		Итого	50 – ОТЗ 50 – ЗТЗ

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

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

1. В ФЗ № 149 информация это _____
   Ответ: Сведения (сообщение, данные) независимо от формы их представления.
2. Целостность это ____
   Ответ: Неискаженность передаваемой, хранимой или обрабатываемой информации.
3. Угроза это _____
   Ответ: Потенциальное возможное событие, процесс или явление, которые могут привести к нарушению конфиденциальности, целостности или доступности информации.
4. Выберите правильно виды угроз:
   А) **Нарушение конфиденциальности**
   Б) Нарушение симметричности
   В) **Нарушение целостности**
5. Число видов электронной подписи в ФЗ № 63 равно ____
   Ответ: трем
6. В каких приказах ФСТЭК изложена классификация государственных информационных систем _____
   Ответ: Приказ № 17 с учетом приказа № 27.
7. Укажите симметричную криптосистему:
   А) **DES**
   Б) RSA
   В) AES
   Г) **ГОСТ 28147-89**

8. Первый стандарт шифрования данных США имеет наименование:

А) AES

Б) IDEA

В) **DES**

Г) SEAL

9. Размер блока и размер ключа в первом стандарте шифрования данных США имеют следующие значения в битах:

А) 64 и 64

Б) 64 и 256

В) 64 и 48

Г) **64 и 56**

10. Двухключевая криптосистема по сравнению с одноключевой имеет более высокую производительность при шифровании данных:

А) ДА

Б) **НЕТ**

11. 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) $\mathbf{n = p \cdot q}$

Г) $c = m^e \bmod (n-1)$

12. При зашифровании данных асимметричной криптосистемой, используется:

А) закрытый ключ

Б) **открытый ключ**

В) сначала открытый, а затем секретный ключ

Г) сначала секретный, а затем открытый ключ

13. При шифровании данных несимметричной криптосистемой, используется:

А) закрытый ключ

Б) открытый ключ

В) **сначала открытый, а затем закрытый ключ**

Г) сначала секретный, а затем открытый ключ

14. В электронном документообороте наилучшим способом контроля целостности данных является:

А) шифрование

Б) **электронная подпись**

В) хэширование

15. В трехфакторной модели оценки информационных рисков используются следующие факторы: _____

Ответ: вероятность реализации угрозы, вероятность использования уязвимости, затраты.

16. Управление рисками это _____

Ответ: процесс выявления, контроля и минимизации или устранения рисков безопасности, оказывающих влияние на бизнес в рамках допустимых затрат.

17. Для проверки политики информационной безопасности в компании в РФ используются следующие программы:

А) КриптоПро

Б) **КОНДОР+**

В) **Гриф**

18. При оценке информационных рисков используются шкалы для ____ факторов.

Ответ: четырех

3.4 Типовые задания для выполнения лабораторной работы и примерный перечень вопросов для ее защиты

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

Ниже приведены образцы типовых вариантов заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты.

«Лабораторная работа «Протокол Диффи-Хеллмана»

Цель работы – ознакомиться с протоколом «Диффи-Хеллмана», как одним из вариантов создания общего секретного ключа при симметричном шифровании.

Введение

В двухключевых (несимметричных, асимметричных, с открытым ключом) криптосистемах адресатом, которому необходим закрытый (секретный) ключ, создаются два ключа (e, d), связанные между собой математической зависимостью (он их может также заказать). При этом один ключ генерируется, а другой вычисляется (это обеспечивается за счет математической связи между ключами).

Один ключ (e) объявляется открытым (публичным), а другой (d) – закрытым (приватным или секретным). Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Закрытый ключ сохраняется в тайне и находится у его создателя (владельца). В дальнейшем закрытый ключ будет называться секретным или закрытым в зависимости от ситуации.

Обозначение открытого ключа (e) условно, при использовании эллиптических функций открытый ключ – это точка на эллиптической кривой с двумя координатами (x и y).

Ключи всегда создает (заказывает) тот, кому нужен закрытый ключ, поэтому этот ключ никуда не передается в отличие от секретного ключа симметричной криптосистемы. Это важное преимущество двухключевых криптосистем.

Обмен Диффи-Хеллмана

Наиболее эффективным средством защиты конфиденциальной информации при автоматизированной ее обработке является шифрование. С точки скорости шифрования данных более эффективным средством является симметричное шифрование, когда отправитель и получатель пользуются одинаковым секретным ключом. В связи с этим, симметричное шифрование имеет недостаток, связанный с передачей секретного ключа.

Предложены различные технологии решения этой проблемы, одной из которых является выработка общего секретного ключа на основе обмена «Диффи-Хеллмана».

Диффи и Хеллман предложили одностороннюю функцию вида (дискретное возведение в степень)

$$y=a^x mod\ p, \qquad (1)$$

где a и p – открытые числа, обладающие некоторыми свойствами (для повышения криптостойкости p является большим простым числом); x - значение секретного ключа; y – значение открытого ключа, $y<p$. Отправитель и получатель сначала генерируют закрытые ключи, а затем, используя функцию (3.1), вычисляют открытые. Так как функция (1) является односторонней, то злоумышленник не может вычислить закрытый ключ, зная открытый ключ, а также значения a и p.

Обратной функцией является дискретное логарифмирование, вычисление которой является вычислительно трудоемкой задачей.

В настоящий момент рекомендуется размер числа p не менее 1024 битов. Это число имеет более 300 десятичных знаков и это очень и очень большое число.

Считается, что с точки зрения криптостойкости, длина модуля 1024 бита соответствует длине 160 битов секретного ключа симметричной криптосистемы. Напомним, что в российских ГОСТах длина секретного ключа 256 битов.

Обозначим пару ключей отправителя (x_o, y_o), а получателя – (x_n, y_n). Обмен «Диффи-Хеллмана» заключается в следующем:

1. Отправитель (О) и получатель (П) по открытому каналу обмениваются своими открытыми ключами. Отправитель получает ключ y_n, а получатель – y_o.

2. Отправитель выполняет следующее математическое преобразование:

$$k_o=y_n^{xo} mod\ p=a^{xn \cdot xo} mod\ p=k.$$

3. Получатель выполняет следующее математическое преобразование:

$$k_n = y_o^{xn} mod\ p = a^{xn \cdot xo} mod\ p = k.$$

4. Ключ k, который вычислили отправитель и получатель, является сеансовым секретным ключом для симметричной криптосистемы. Его размер определяется размером числа p.

При выполнении этой лабораторной работы проверяются знания по разделу «Криптография – шифрование электронных сообщений». Ниже приведены вопросы для тестирования.

1) Первый стандарт шифрования данных США имеет наименование:

А) AES

Б) IDEA

В) DES

Г) SEAL

2) Размер блока и размер ключа в первом стандарте шифрования данных США имеют следующие значения в битах:

А) 64 и 64

Б) 64 и 256

В) 64 и 48

Г) 64 и 56

3) Режим имитовставки это:

А) Поточный режим шифрования данных

Б) Метод контроля целостности данных средствами симметричной криптосистемы

В) Метод контроля целостности данных средствами несимметричной криптосистемы

Г) Блочный режим шифрования данных

4) Российский алгоритм ГОСТ 28147-89 позволяет:

А) Блочное шифрование данных

Б) Поточное шифрование данных

В) Формировать электронно-цифровую подпись

Г) Осуществлять контроль целостности информации

«Лабораторная работа «Этапы технологии электронной подписи»»

Целью работы является обучение пользователей компонентам этапов в технологии электронной подписи (ЭП), последовательности этапов, а также функциям ЭП.

Основные компоненты технологии:

- исходное сообщение (mA);
- уведомление (mB);
- ключ электронной подписи (dA или dB), предназначенный для создания ЭП;
- ключ проверки электронной подписи (eA или eB);
- электронная подпись (ZmA или ZmB). В российском стандарте по ГОСТ Р 34.10-2012 ЭП состоит из двух чисел равной длины (r, s), длина ЭП равна 512 или 1024 битов;
- результат хэширования (УmA или УmB), для хэширования используется хэш-функция. В российском стандарте по ГОСТ Р 34.11-2012 длина хэш-образа равна 256 или 512 битов;
- отправитель (A), который либо подписывает исходное сообщение (mA), тем самым создает ЭП ZmA, или проверяет подлинность ЭП получателя ZmB;
- получатель (B), который либо проверяет подлинность ЭП отправителя ZmA, либо подписывает уведомление (mB), тем самым создает ЭП ZmB;
- сертификат, электронный документ, содержащий ключ проверки ЭП и другую служебную информацию;
- удостоверяющий центр (УЦ), который создает ключи (dA, eA и dB, eB), а также сертификаты (SeA, SeB). Затем сертификаты УЦ отправляет пользователям.

Описание работы

При запуске программы высвечивается основное окно, содержащее кнопку «Теория» и 5 кнопок практики с названиями этапов.

Внизу имеется поле с выходными результатами:

Время начала и окончания работы;
Сколько этапов Вы выполнили;
Сколько раз Вы обращались к кнопке «Теория»;
Сколько ошибок Вы допустили.
Вы должны в правильной последовательности пройти все 5 этапов.
Для этого:

1. Необходимо внимательно почитать теорию и только после этого обратиться к практике. В каждом окне имеется кнопка «Теория» и Вы можете снова к ней обратиться, но в этом случае Вы возвращаетесь в исходное состояние (этапы необходимо проходить заново).
2. После запуска подготовительного этапа появляется окно с тремя кнопками. Необходимо последовательно их выполнить: «Отправитель» - указать, что делает УдЦентр для отправителя; «Получатель» - указать, что делает УдЦентр для получателя; «Проверить» - осуществляется проверка по этапу.
3. Если Вы правильно действуете, то появляется окно «Верно» и надо подтвердить это. После этого Вы переходите к следующему этапу. Если появляется окно «Не верно», то после подтверждения, Вы возвращаетесь к этапу повторно.
4. После этапов появляются окна для теоретической проверки Ваших знаний. Эти тесты также необходимо пройти.
5. Программа накапливает количество Ваших неверных ответов и количество обращений к кнопке «Теория». Напоминаю, как только Вы обратились к этой кнопке, программа возвращает Вас в исходное состояние (основное окно).

3.5 Перечень теоретических вопросов к экзамену

(для оценки знаний)

1. Характеристика ОВС.
2. Безопасность корпоративных ИС.
3. Аспекты безопасности информации.
4. Организационно-правовое обеспечение безопасности ОВС.
5. Управление рисками информационной безопасности.
6. Аудит состояния информационной безопасности.
7. Программные средства для аудита.
8. Общая схема шифрования.
9. Российский алгоритм криптографического преобразования: режимы шифрования.
10. Российский алгоритм криптографического преобразования: режим имитовставки.
11. Несимметричные системы шифрования. Современный протокол шифрования данных.
12. Алгоритм RSA. Сравнение симметричных и несимметричных криптосистем.
13. Определение и назначение хэш-функции, российский стандарт.
14. Электронная подпись: определения, назначение, роль в электронном документообороте.
15. Российский стандарт ЭП: технология создания и проверки.
16. Обмен Диффи-Хеллмана. Назначение мастер-ключа.
17. Аспекты безопасности информации.
18. Способы формирования ключей для поточного шифрования.
19. Вопросы по поточному шифрованию.

3.6 Перечень типовых простых практических заданий к экзамену

(для оценки умений)

Укажите двухключевую криптосистему:
А) DES
Б) RSA
В) AES
Г) ГОСТ 28147-89
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) $c = m^e \bmod (n-1;$
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
Размер хэш- кода по российскому стандарту (ГОСТ-2012) равен:
А) 256 бит или 512 бит
Б) 512 бит или 160 бит
В) 160 бит
Г) 320 бит

3.7 Перечень типовых практических заданий к экзамену

(для оценки навыков и (или) опыта деятельности)

Двухключевая криптосистема по сравнению с одноключевой имеет более высокую производительность при шифровании данных:
А) ДА
Б) НЕТ
Современный протокол шифрования данных базируется на совместном применении как симметричной криптосистемы так и несимметричной:
А) ДА
Б) НЕТ
Хэш-функция – это криптографическое преобразование информации, переводящее строку битов произвольной длины в строку битов фиксированной длины:
А) ДА
Б) НЕТ
В электронном документообороте наилучшим способом контроля целостности данных является:
А) шифрование
Б) электронная цифровая подпись
В) хэширование

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

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

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Контрольная работа	Преподаватель на установочном занятии доводит до обучающихся: темы, количество заданий в контрольной работе. Контрольная работа должна быть выполнена в установленный срок и в соответствии с правилами к оформлению (текстовой и графической частей), сформулированными в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль» в последней редакции. Выполненная контрольная работа передается для проверки преподавателю в установленные сроки. Если контрольная работа выполнена не в соответствии с указаниями или не в полном объеме, она возвращается на доработку
Собеседование	Собеседование, предусмотренное рабочей программой дисциплины, проводится на практическом занятии. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся тему, вопросы для подготовки к собеседованию. Результаты собеседования преподаватель доводит до обучающихся сразу после завершения собеседования
Тестирование (компьютерные технологии)	Тестирование проводится по результатам освоения тем или разделов дисциплины или по окончанию ее изучения во время практических занятий. Во время проведения тестирования пользоваться учебниками, справочниками, конспектами лекций, тетрадями для практических занятий не разрешено. Преподаватель на практическом занятии, предшествующем занятию проведения теста, доводит до обучающихся: темы, количество заданий в тесте, время выполнения. Результаты тестирования видны обучающемуся на компьютере сразу после прохождения теста
Лабораторная работа	Защита лабораторных работ проводится во время лабораторных занятий. Во время проведения защиты лабораторной работы пользоваться учебниками, справочниками, конспектами лекций, тетрадями не разрешено. Преподаватель на лабораторной работе, предшествующей занятию проведения защиты лабораторной работы, доводит до обучающихся: номер защищаемой лабораторной работы, время на защиту лабораторной работы. Преподаватель информирует обучающихся о результатах защиты лабораторной работы сразу после ее контрольно-оценочного мероприятия

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

Перечень теоретических вопросов и типовые практические задания разного уровня сложности для проведения промежуточной аттестации обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

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

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

При проведении промежуточной аттестации в форме собеседования билеты составляются таким образом, чтобы 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; два практических задания: одно из них для оценки умений (выбирается из перечня типовых простых практических заданий к экзамену); другое 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 фондов оценочных средств.

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

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

Образец экзаменационного билета

ИРГУПС 20__-20__ учебный год	**Экзаменационный билет № 1** **по дисциплине «Комплексная безопасность корпоративных информационных систем»**	Утверждаю: Заведующий кафедрой «ИСиЗИ» ИрГУПС _____
1. Аспекты безопасности информации. 2. Что такое угроза и уязвимость. 3. Хэширование сообщения при создании ЭП осуществляется, чтобы: А) обеспечить конфиденциальность информации Б) увеличить время создания ЭП В) стандартизовать время создания ЭП и ее размер 4. Найдите контрольную сумму, используя операцию сложения по модулю 2^{16} двух слов, заданных в шестнадцатеричной системе счисления: DA9F I+I AFE4		