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.04.01 Защита информации и информационная безопасность

рабочая программа дисциплины

Специальность/направление подготовки – 12.04.01 Приборостроение
Специализация/профиль – Приборы и методы контроля качества и диагностики
Квалификация выпускника – Магистр
Форма и срок обучения – очная форма 2 года
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 3
Часов по учебному плану (УП) – 108
В том числе в форме практической подготовки (ПП) – 34
(очная)

Формы промежуточной аттестации
очная форма обучения:
зачет 2 семестр

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

Семестр	2	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	51/34	**51/34**
– лекции	17	**17**
– практические (семинарские)		
– лабораторные	34/34	**34/34**
Самостоятельная работа	57	**57**
Итого	108/34	**108/34**

* 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 12.04.01 Приборостроение, утвержденным Приказом Министерства науки и высшего образования Российской Федерации от 22.09.2017 № 957.

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

СОГЛАСОВАНО

Кафедра «Физика, механика и приборостроение», протокол от «17» июня 2022 г. № 16

Зав. кафедрой, к. т. н., доцент С.В. Пахомов

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 оптического приборостроения
2	освоить современные методы защиты информации, обеспечивающих ее целостность и конфиденциальность

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	Б1.В.ДВ.01.01 Математическое моделирование в приборных системах
2	Б1.В.ДВ.06.01 Вибрационный и тепловой контроль и диагностика
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б2.О.05(Пд) Производственная - преддипломная практика
2	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
3	Б3.02(Д) Защита выпускной квалификационной работы

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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ПК-1 Способен к научным исследованиям в области оптического приборостроения, оптических материалах и технологий	ПК-1.1 Анализирует научно-техническую информацию по разработке оптотехники, оптических и оптико-электронных приборов и комплексов	Знать: принципы, методы и средства решения стандартных задач в области оптического приборостроения
		Уметь: пользоваться практическим опытом применения нормативной базы с применением информационно-коммуникационных технологий
		Владеть: средствами защиты информации с учетом научно-технической информации по разработке оптотехники
	ПК-1.4 Разрабатывает новые технологии производства оптотехники, оптических и оптико-электронных приборов и комплексов	Знать: организационно-правовые основы применительно к сетям передачи данных
		Уметь: решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности
		Владеть: основными средствами защиты информации при ее передаче

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
1.0	**Раздел 1. Организационно-правовые основы по защите информации и информационной безопасности.**						
1.1	Тема 1. Аспекты безопасности информации, характеристика угроз. Правовое обеспечение защиты информации	2	4			15	ПК-1.1 ПК-1.4
1.2	Лабораторная работа № 1. «Контроль целостности информации при случайных воздействиях»	2			4		ПК-1.1 ПК-1.4
1.3	Тема 2. Организационно обеспечение защиты информации. Управление рисками	2	4			12	ПК-1.1 ПК-1.4
1.4	Лабораторная работа № 2. «Порядок проведения классификации информационных систем в РФ»	2			6		ПК-1.1 ПК-1.4
1.5	Лабораторная работа № 3 «Генерирование секретных ключей для симметричной криптосистемы»	2			4		ПК-1.1 ПК-1.4

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
2.0	**Раздел 2. Средства защиты информации, обеспечивающие ее целостность и конфиденциальность.**						
2.1	Тема 3. Основные понятия криптографии. Поточное шифрование. Российский алгоритм криптографического преобразования	2	4			15	ПК-1.1 ПК-1.4
2.2	Лабораторная работа № 4 «Поточное шифрование»	2			6		ПК-1.1 ПК-1.4
2.3	Лабораторная работа № 5 «Технология обнаружения и исправления ошибок»	2			4		ПК-1.1 ПК-1.4
2.4	Тема 4. Двухключевые криптосистемы. Технологии шифрования. Хэш-функция. Российские стандарты электронной подписи	2	5			15	ПК-1.1 ПК-1.4
2.5	Лабораторная работа № 6. «Протокол Диффи-Хеллмана»	2			6		ПК-1.1 ПК-1.4
2.6	Лабораторная работа №7. «Этапы технологии электронной подписи»	2			4		ПК-1.1 ПК-1.4
	Форма промежуточной аттестации – зачет	2					ПК-1.1 ПК-1.4
	Итого часов (без учёта часов на промежуточную аттестацию)		17		34/34	57	

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	Бутин, А. А. Программно-аппаратные средства защиты информации : учеб. пособие - Изд. 2-е, перераб. и доп. / А. А. Бутин, Н. И. Глухов, С. И. Носков. Иркутск : ИрГУПС, 2022. - 90с.	21
6.1.1.2	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

6.1.2 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	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. - 95с.	17
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.04.01 Защита информации и информационная безопасность по направлению подготовки 12.04.01 Приборостроение, профиль Приборы и методы контроля качества и диагностики / Ю.М. Краковский ; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 11 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_2831_1408_2022_1_signed.pdf	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/	
6.2.2	Научная электронная библиотека eLIBRARY.RU — https://elibrary.ru/	
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	Учебная аудитория Д-521 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, Мультимедиапроектор, экран, (ноутбук переносной)
3	Учебная аудитория А-509 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор (переносной), экран (переносной), компьютер
4	Учебная аудитория А-516 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, Мультимедиапроектор(переносной),экран(переносной),компьютер.
5	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507; – помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей

	области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Лабораторная работа	Основной целью лабораторных работ является теоретическое обоснование, наглядное и/или экспериментальное подтверждение и/или проверка существенных теоретических положений (законов, закономерностей) анализ существующих методик и методов их реализации и т.д. Они занимают преимущественное место при изучении дисциплин обязательной части и части, формируемой участниками образовательных отношений Блока 1. Исходя из цели, содержанием лабораторных работ могут быть: - экспериментальная проверка формул, методик расчета; - проведение натурных измерений свойств, рабочих параметров, режимов работы при помощи лабораторного оборудования и/или стендов и макетов; - ознакомление, анализ и теоретические выкладки по устройству, принципу действия и способам обслуживания аппаратов, деталей машин, механизмов, процессов, протекающих в них при этом и т.д.; - наглядная графическая интерпретация чертежей, схем, объемных поверхностей и т.д., воспроизводимых с помощью специализированного программного обеспечения; - имитационное моделирование процессов, протекающих в сложных химических, физических, механических, электрических и пр. объектах; - наглядное представление о работе персонала конкретной организации или подразделения ОАО «РЖД» посредством моделирования штатных и внештатных ситуаций в виртуальных специализированных АРМ (автоматизированных рабочих мест); - установление и подтверждение закономерностей (путем сравнения проведенного эксперимента и рассчитанных значений) и т.д.; - ознакомление с методиками проведения экспериментов, наглядным устройством стенд-макетов и пр.; - установление свойств веществ, их качественных и количественных характеристик; - анализ различных характеристик процессов, в том числе производственных и иных процессов; - расчет параметров различных явлений и процессов, смоделировать которые не возможно в реальных условиях (например, чрезвычайные ситуации и пр.); - наблюдение развития явлений, процессов и др. Допускается иное содержание лабораторных работ, если это будет способствовать реализации целей и задач дисциплины и формированию соответствующих компетенций.

	По характеру выполняемых лабораторных работ возможны: - ознакомительные работы, используемые для закрепления изученного теоретического материалы; - аналитические работы, используемые для получения новой информации на основе формализованных методов; - творческие работы, ориентированные на самостоятельный выбор подходов решения задач. Прежде, чем приступить к лабораторным занятиям, обучающимся необходимо повторить теоретический материал по теме работы. Каждая лабораторная работа оснащена методическими указаниями, разработанными преподавателями, ведущими дисциплину
Самостоятельная работа	Обучение по дисциплине «Защита информации и информационная безопасность» 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 «Защита информации и информационная безопасность» участвует в формировании компетенций:

ПК-1. Способен к научным исследованиям в области оптического приборостроения, оптических материалах и технологий

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
2 семестр				
1.0	**Раздел 1. Организационно-правовые основы по защите информации и информационной безопасности**			
1.1	Текущий контроль	Тема 1. Аспекты безопасности информации, характеристика угроз. Правовое обеспечение защиты информации	ПК-1.1 ПК-1.4	Собеседование (устно)
1.2	Текущий контроль	Лабораторная работа № 1. «Контроль целостности информации при случайных воздействиях»	ПК-1.1 ПК-1.4	Лабораторная работа (письменно/устно)
1.3	Текущий контроль	Тема 2. Организационно обеспечение защиты информации. Управление рисками	ПК-1.1 ПК-1.4	Собеседование (устно)
1.4	Текущий контроль	Лабораторная работа № 2. «Порядок проведения классификации информационных систем в РФ»	ПК-1.1 ПК-1.4	Лабораторная работа (письменно/устно)
1.5	Текущий контроль	Лабораторная работа № 3 «Генерирование секретных ключей для симметричной криптосистемы»	ПК-1.1 ПК-1.4	Лабораторная работа (письменно/устно)
2.0	**Раздел 2. Средства защиты информации, обеспечивающие ее целостность и конфиденциальность**			
2.1	Текущий контроль	Тема 3. Основные понятия криптографии. Поточное шифрование. Российский алгоритм криптографического преобразования	ПК-1.1 ПК-1.4	Собеседование (устно)
2.2	Текущий контроль	Лабораторная работа № 4 «Поточное шифрование»	ПК-1.1 ПК-1.4	Лабораторная работа (письменно/устно)
2.3	Текущий контроль	Лабораторная работа № 5 «Технология обнаружения и исправления ошибок»	ПК-1.1 ПК-1.4	Лабораторная работа (письменно/устно)
2.4	Текущий контроль	Тема 4. Двухключевые криптосистемы. Технологии шифрования. Хэш-функция. Российские стандарты электронной подписи	ПК-1.1 ПК-1.4	Тестирование (компьютерные технологии)
2.5	Текущий контроль	Лабораторная работа № 6. «Протокол Диффи-Хеллмана»	ПК-1.1 ПК-1.4	Лабораторная работа (письменно/устно)
2.6	Текущий контроль	Лабораторная работа №7. «Этапы технологии электронной подписи»	ПК-1.1 ПК-1.4	Лабораторная работа (письменно/устно)
	Промежуточная аттестация	Все разделы	ПК-1.1 ПК-1.4	Зачет (собеседование)

				Зачет - тестирование (компьютерные технологии)

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

Описание показателей и критериев оценивания компетенций.
Описание шкал оценивания

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

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

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

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

Текущий контроль

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	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
2	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
3	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	Зачет	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий к зачету

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

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

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

Тест – промежуточная аттестация в форме зачета

Шкала оценивания	Критерии оценивания
«зачтено»	Обучающийся верно ответил на 70 % и более тестовых заданий при прохождении тестирования
«не зачтено»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

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 проведения собеседования

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

Ниже приведен образец типовых вариантов заданий для проведения собеседований.

Образец типового варианта вопросов для проведения собеседования

«Тема 1. Аспекты безопасности информации, характеристика угроз. Правовое обеспечение защиты информации»

1. Дать определение информационной системы по ФЗ № 149.
2. Что такое целостность информации.
3. Основные направления по нарушению конфиденциальности информации.
4. Основные виды угроз.
5. Что входит в правовое обеспечение на федеральном уровне.

Образец типового варианта вопросов для проведения собеседования

«Тема 2. Организационно обеспечение защиты информации. Управление рисками»

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.
5. Какие факторы входят в трехфакторную модель информационного риска.

Образец типового варианта вопросов для проведения собеседования

«Тема 3. Основные понятия криптографии. Поточное шифрование. Российский алгоритм криптографического преобразования»

1. Основные понятия криптографии.
2. Классификация криптосистем.
3. Общая схема симметричного шифрования.
4. В чем отличие шифрования от дешифрования.
5. Дать характеристику режимов шифрования российского алгоритма по ГОСТ-89.

Образец типового варианта вопросов для проведения собеседования

«Тема 4. Двухключевые криптосистемы. Технологии шифрования. Хэш-функция. Российские стандарты электронной подписи»

1. Что такое двухключевая криптосистема.
2. Как осуществляется шифрование на основе двухключевой криптосистемы.
3. Назначение обмена Диффи-Хеллмана.
4. Что такое односторонняя функция. Примеры односторонней функции.
5. Перечислить российские стандарты электронной подписи.

3.2 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-1.1 ПК-1.4	Тема 1. Аспекты безопасности информации, характеристика угроз. Правовое обеспечение защиты информации	Знание	4 – ОТЗ 4 – ЗТЗ
ПК-1.1 ПК-1.4	Лабораторная работа № 1. «Контроль целостности информации при случайных воздействиях»	Умение	3 – ОТЗ 3 – ЗТЗ
ПК-1.1 ПК-1.4	Тема 2. Организационно обеспечение защиты информации. Управление рисками	Знание	4 – ОТЗ 4 – ЗТЗ
ПК-1.1 ПК-1.4	Лабораторная работа № 2. «Порядок проведения классификации информационных систем в РФ»	Умение	3 – ОТЗ 3 – ЗТЗ
ПК-1.1 ПК-1.4	Лабораторная работа № 3 «Генерирование секретных ключей для симметричной криптосистемы»	Навыки	3 – ОТЗ 3 – ЗТЗ
ПК-1.1 ПК-1.4	Тема 3. Основные понятия криптографии. Поточное шифрование. Российский алгоритм криптографического преобразования	Знание	4 – ОТЗ 4 – ЗТЗ
ПК-1.1 ПК-1.4	Лабораторная работа № 4 «Поточное шифрование»	Умение	4 – ОТЗ 4 – ЗТЗ
ПК-1.1 ПК-1.4	Лабораторная работа № 5 «Технология обнаружения и исправления ошибок»	Умение	4 – ОТЗ 4 – ЗТЗ
ПК-1.1 ПК-1.4	Тема 4. Двухключевые криптосистемы. Технологии шифрования. Хэш-функция. Российские стандарты электронной подписи	Знание	4 – ОТЗ 4 – ЗТЗ
ПК-1.1 ПК-1.4	Лабораторная работа № 6. «Протокол Диффи-Хеллмана»	Навыки	4 – ОТЗ 4 – ЗТЗ
ПК-1.1 ПК-1.4	Лабораторная работа №7. «Этапы технологии электронной подписи»	Умение	4 – ОТЗ 4 – ЗТЗ
		Итого	41 – ОТЗ 41 – 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.

Раздел 1. Организационно-правовые основы защиты информации и информационной безопасности

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

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

8. Управление рисками это _____

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

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

А) КриптоПро

Б) **КОНДОР+**

В) **Гриф**

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

Ответ: четырех

Раздел 2. Средства защиты информации, обеспечивающие ее целостность и конфиденциальность

11. Укажите симметричную криптосистему:

А) **DES**

Б) RSA

В) AES

Г) **ГОСТ 28147-89**

12. Первый стандарт шифрования данных США имеет наименование:

А) AES

Б) IDEA

В) **DES**

Г) SEAL

13. 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**

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

А) ДА

Б) **НЕТ**

15. 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) $c = m^e \bmod (n-1)$

16. 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

17. 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

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

А) шифрование

Б) **электронная подпись**

В) хэширование

3.3 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 приведен образец типовых вариантов заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 1. «Контроль целостности информации при случайных воздействиях»»

Целью работы является изучение различных методов контроля целостности информации при ее передаче от случайных воздействий.

Метод контрольных сумм

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 КС определяется размерностью данных в файле. Например: 2, 4, 8-байтовое слово. Рассмотрим пример для 2-байтовых слов:

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

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

Метод КС используется в сетевых технологиях, например, в протоколе *TCP* для Интернета. При сетевой передаче сообщение разбивается на пакеты, далее для каждого пакета формируется своя КС. Если КС отправителя и получателя совпадают (1.1), то считается, что целостность пакета не нарушена. Иначе требуется повторная передача этого пакета.

Метод КС является достаточно быстродействующим, но он обнаруживает одиночную ошибку по каждому столбцу пакета. Это является недостатком этого метода.

При создании пакетов число слов в нем выбирают таким образом, чтобы вероятностью более одной ошибки можно было пренебречь (она должна быть маленькой). Пакетная передача позволяет достаточно эффективно передавать сообщения даже по не очень надежным каналам.

С учетом недостатка метода КС его в настоящее время стараются не применять. Чтобы контролировать более одной ошибки используют сложение по модулю 2^n, метод циклического контроля и другие методы. Контрольные значения в этих методах также часто называют контрольными суммами.

Рассмотрим сложение по модулю 2^n.

В этом методе осуществляется обычное сложение, а результатом (КС) являются n младших битов. Как правило n равно длине слова в битах: 16, 32, 256, 512 или другая длина.

Рассмотрим сложение четырех чисел, имеющих 4-х битное представление. Эти числа: 14, 15, 11, 13, сумма этих чисел равна 53. В двоичном представлении это будет: 11 0101.

Проведем сложение по модулю 2^4 в двоичном виде:

1110+1111=1 1101+1011=1 1000+1101=1 0101.

Таким образом, КС=0101.

1. Три аспекта безопасности информации.
2. Что такое конфиденциальность информации.
3. Что такое целостность информации.

4. Что понимается под случайным воздействием на информацию.
5. Опишите технологию контроля информации при случайных воздействиях.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 2. «Порядок проведения классификации информационных систем в РФ»»

Цель работы – освоить порядок проведения классификации информационных систем в соответствии с требованиями Приказа ФСТЭК России от 11 февраля 2013 г. №17 с учетом приказа ФСТЭК от 15.02.2017 г. № 27.

В последнее десятилетие в Российской Федерации государственными регуляторами активно проводятся мероприятия по совершенствованию организационно-правовой базы в сфере защиты информационных систем различного назначения. Можно отметить следующие значимые документы, которые появились в это время:

– приказ ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11.02.2013 № 17;

– приказ ФСТЭК России «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» от 14.03.2014 № 31.

– приказ ФСТЭК от 15.02.2017 г. № 27 в развитие приказа ФСТЭК от 11.02.2013 № 17;

– приказ ФСТЭК от 27.03.2017 г. № 49 в развитие приказа ФСТЭК от 14.03.2014 № 31.

Приказ № 17 с учетом приказа № 27 для защиты государственных ИС предусматривает проведение следующих мероприятий:

– принятие решения о необходимости защиты информации в ИС;

– классификацию ИС по требованиям защиты информации;

– определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации;

– определение требований к системе защиты информации информационной системы.

Приказ №17 с учетом приказа № 27 устанавливает обязательные требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней при обработке указанной информации в государственных и муниципальных информационных системах (ИС).

В документах не рассматриваются требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации.

Требования к системе защиты информации ИС определяются в зависимости от:

1) класса защищенности ИС;

2) угроз безопасности информации, включенных в модель угроз безопасности информации.

1. Особенности обработки персональных данных.
2. Сфера применимости Приказа №17.
3. Виды ИС по масштабу.
4. На основании каких данных формируются требования к системе защиты информации ИС.
5. Перечень мероприятий для обеспечения защиты информации, содержащейся в ИС.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для

их защиты

«Лабораторная работа № 3 «Генерирование секретных ключей для симметричной криптосистемы»»

Цель работы – ознакомиться с технологией генерирования секретных ключей.

Пусть нам необходимо получить значения равномерно распределенной случайной последовательности (РРСП) с элементами

$$x_1, \ldots x_t, \ldots$$

Можно выделить два подхода к получению этой последовательности:

1) создание и реализация алгоритмов, обеспечивающих высокое быстродействие;

2) создание и реализация алгоритмов, обеспечивающих высокую криптостойкость.

Первое направление в большей степени используется в имитационном моделировании, а второе – в криптографии и, в частности, при создании секретных ключей при поточном или блочном шифровании.

Выделяют три типа генераторов РРСП: табличный, физический и программный. Программный генератор РРСП – программа имитации на компьютере реализации РРСП. Имитируемая последовательность называется псевдослучайной, т.к. она вычисляется по детерминированному алгоритму. В тоже время ее статистические свойства «близки» по определенным критериям к свойствам РРСП. Поэтому эти числа называют псевдослучайными (в отличии от настоящих случайных, которые реализуются физическими генераторами).

Важным параметром генераторов РРСП является их период T – длина неповторяющихся (несовпадающих) значений x_t: $x_t=x_{t+T}=x_{t+2T}=\ldots$

Выделяют несколько подходов к построению алгоритмов генерации. Мы рассмотрим конгруэнтный алгоритм как наиболее распространенный метод. Среди конгруэнтных алгоритмов используются линейные, мультипликативные и с простым модулем.

1. Конфиденциальность информации и методы ее защиты.
2. Чем обеспечивается криптостойкость выбранного алгоритма с простым модулем.
3. Какие значения может принимать ключ $k=A(i)$.
4. Что такое период T для генераторов РРСП.
5. Почему величина x_s близка к значению 0,5.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 4 «Поточное шифрование»»

Цель работы – освоить технологию создания ключа для поточного шифрования на основе регистра сдвига с линейной обратной связью.

В современных системах симметричного шифрования информации широкое применение находят системы поточного шифрования.

Необходимо различать процедуру создания поточного ключа и процедуру поточного шифрования (хотя эти процедуры очень связаны и могут выполняться совместно). В связи с этим разделим поточное шифрование на две процедуры:

а) само поточное шифрование;

б) создание ключа для поточного шифрования.

Современные поточные системы при шифровании используют побитное сложение по модулю 2 (операцию *XOR*). Мы ее уже не однократно использовали, например, при контроле целостности информации, когда рассматривали контроль целостности при случайных воздействиях.

Пусть m – исходное электронное сообщение, конфиденциальность которого необходимо обеспечить; c – зашифрованное сообщение, полученное из исходного; K – секретный поточный ключ. Тогда при зашифровании используется следующая операция

$$c_i=m_i(+)K_i, \quad i=1,2,\ldots,I,$$

где m_i – i-й бит исходного сообщения; K_i – i-й бит поточного ключа; c_i – i-й бит зашифрованного сообщения; I – число битов в сообщениях и в ключе; (+) – операция сложения по модулю 2.

При расшифровании используется та же операция

$$m_i=c_i(+)K_i, \quad i=1,2,\ldots,I.$$

Убедимся, что

$$c_i(+)K_i = (m_i(+)K_i)(+)K_i) = m_i(+)(K_i(+)K_i) = m_i.$$

Для поточного шифрования справедливо равенство, которое вытекает из свойства операции сложения по модулю 2

$$K_i = m_i(+)c_i, \quad i=1,2,\ldots,I.$$

Заметим, что в российских национальных стандартах поточное шифрование называют гаммированием, а поточный ключ – гаммой.

1. Способы формирования ключей для поточного шифрования.
2. Какой аспект безопасности обеспечивает шифрование.
3. Что такое отводная последовательность.
4. Как работает РСЛОС.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 5 «Технология 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.

1. Опишите технологию обнаружения и исправления ошибок на примере кода Хэмминга.
2. В чем отличие методов обнаружения ошибок от методов обнаружения и исправления ошибок.

3. Как определить число контрольных разрядов.
4. Как создается контрольное слово и для чего.
5. Сравнить метод КС и метод Хэмминга.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 6. «Протокол Диффи-Хеллмана»»

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

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.

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

5) Укажите блочные криптосистемы с длиной блока 64 бита:

А) RSA
Б) AES
В) DES
Г) ГОСТ 28147-89

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа №7. «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.

1. Назначение электронной подписи.
2. Что такое неотказуемость.
3. Какой ключ используется при создании ЭП.
4. Какой ключ используется при проверки подлинности ЭП.

3.4 Перечень теоретических вопросов к зачету

(для оценки знаний)

1. Информационная безопасность и безопасность информации.
2. Аспекты безопасности информации.
3. Характеристика и классификация угроз.
4. Правовое обеспечение защиты информации.
5. Организационное обеспечение защиты информации.
6. Основные понятия криптографии. Классификация криптосистем.
7. Общая схема шифрования.
8. Способы формирования ключей для поточного шифрования.
9. Вопросы по поточному шифрованию.
10. Что такое угроза и уязвимость.
11. Конфиденциальность информации и методы ее защиты.
12. Российский алгоритм криптографического преобразования: режимы шифрования.
13. Российский алгоритм криптографического преобразования: режим имитовставки.

14. Несимметричные системы шифрования. Современный протокол шифрования данных.
15. Алгоритм RSA. Сравнение симметричных и несимметричных криптосистем.
16. Правовое обеспечение электронной подписи.
17. Определение и назначение хэш-функции, российский стандарт.
18. Электронная подпись: определения, назначение, роль в электронном документообороте.
19. Российский стандарт ЭП: технология создания и проверки.
20. Обмен Диффи-Хеллмана. Назначение мастер-ключа.
21. Управление рисками информационной безопасности.
22. Трехфакторная модель оценки информационных рисков.
23. Аудит состояния информационной безопасности.

3.5 Перечень типовых простых практических заданий к зачету

(для оценки умений)

1. 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

2. Современный протокол шифрования данных базируется на совместном применении как симметричной криптосистемы так и асимметричной:

А) ДА

Б) НЕТ

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

А) ДА

Б) НЕТ

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

А) шифрование

Б) электронная цифровая подпись

В) хэширование

3.6 Перечень типовых практических заданий к зачету

(для оценки навыков и (или) опыта деятельности)

1. Выполните операцию сложения по модулю 2 двух слов, заданных в шестнадцатеричной системе счисления:

14A7(+)2CA8

2. Найдите контрольную сумму, используя операцию сложения по модулю 2^{16} двух слов, заданных в шестнадцатеричной системе счисления:

4A9F I+I 7FE4

3. Найдите контрольную сумму, используя операцию сложения по модулю 2 двух слов, заданных в шестнадцатеричной системе счисления:

CA9F(+)DCB9

4. Выполните операцию сложения по модулю 2 двух слов, заданных в шестнадцатеричной системе счисления:

C4A7(+)BCA8

5. Найдите контрольную сумму, используя операцию сложения по модулю 2^{16} двух слов, заданных в шестнадцатеричной системе счисления:

DA9F I+I AFE4

6. 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

7. При создании ЭЦП секретный ключ по длине больше, чем открытый:

А) ДА

Б) НЕТ

8. В электронном документообороте наилучшим способом обеспечения конфиденциальности данных является:

А) шифрование

Б) электронная цифровая подпись

В) хэширование

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

А) ДА

Б) НЕТ

10. Пару ключей при шифровании данных криптосистемой с открытым ключом создает отправитель:

А) ДА

Б) НЕТ

11. Владельцем пары ключей при создании ЭЦП является отправитель:

А) ДА

Б) НЕТ

12. 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.

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
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 зачета и оценивания результатов обучения

При проведении промежуточной аттестации в форме зачета преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок).

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

Средняя оценка уровня сформированности компетенций по результатам текущего контроля	Шкала оценивания
Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю	«зачтено»

Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю	«не зачтено»

Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета без дополнительного аттестационного испытания, то промежуточная аттестация проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач или в форме компьютерного тестирования.

Промежуточная аттестация в форме зачета с проведением аттестационного испытания проходит на последнем занятии по дисциплине.

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