МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»
Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ
Декан _____ Буднев Н.М.
«22» апреля 2020 г.

Рабочая программа дисциплины

Наименование дисциплины **Б1.Б.08 Криптографические методы защиты информации**

Направление подготовки 10.03.01 Информационная безопасность

Направленность (профиль) подготовки №7 «Техническая защита информации»

Квалификация выпускника бакалавр

Форма обучения очная

Согласовано с УМК физического факультета

Протокол № 25 от «21» апреля 2020 г.
Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 8
От «20» марта 2020 г.
И.О.Зав. кафедрой _____ Колесник С.Н.

Иркутск 2020 г.

Содержание

1. Цели и задачи дисциплины (модуля)

Учебная дисциплина «Криптографические методы защиты информации» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует фундаментализации образования, формирование знаний в области криптографии и навыков применения методов криптографической защиты информации в профессиональной деятельности.

Цели освоения учебной дисциплины «Криптографические методы защиты информации»**:**

1) формирование фундаментальных знаний в области криптографии и способностей, необходимых для решения различных задач шифрования и дешифрирования сообщений;

2) овладение современным аппаратом и методами криптографии для защиты информации от угроз раскрытия и нарушения целостности;

3) формирование личности обучающегося, развитие его интеллекта и способностей к освоению основополагающих способов защиты информации на базе криптографических методов.

4) формирование практических навыков при работе со средствами криптографической защиты информации;

5) формирование у будущих специалистов основных понятий и концепций криптографии и криптоанализа, а также в их применении к анализу конкретных систем шифрования.

Задачи освоения учебной дисциплины**:**

1) изучение математических методов, применяемых для проектирования шифров и анализа криптостойкости алгоритмов;

2) изучение криптографических методов защиты информации, передаваемой по каналам связи и обрабатываемой средствами вычислительной техники;

3) овладение современным математическим аппаратом для дальнейшего использования при решении задач криптоанализа, аргументации стойкости и синтеза криптосистем;

4) изучение концепций построения симметричных и асиммеричных криптографических алгоритмов;

5) изучение основ алгоритмической теории чисел.

2. Место дисциплины в структуре ОПОП

Дисциплина «Криптографические методы защиты информации» является базовой дисциплиной профессионального цикла. Дисциплина является вводной в проблематику

криптографической защиты информации. Взаимосвязь данной дисциплины через компетенции отражена в рабочем учебном плане и матрице компетенций. Дисциплина опирается на знания, полученные в ходе изучения дисциплин «Математический анализ», «Информатика», «Теория вероятностей и математическая статистика», «Дискретная математика» которая должна быть освоена полностью и студенты должны владеть навыками применения криптографических методов защиты информации.

Дисциплина является предшествующей для таких дисциплин профессионального цикла как «Программно-аппаратные средства защиты информации», «Теория информации», «Комплексное обеспечение информационной безопасности автоматизированных систем», а так же для учебной и производственной практики и итоговой государственной аттестации. Изучение данной дисциплины позволяет приобрести первичные навыки, необходимые для изучения принципов обеспечения безопасности автоматизированных систем.

3. Требования к результатам освоения дисциплины (модуля)

Процесс изучения дисциплины (модуля) направлен на формирование следующей компетенции:

ОПК-2. Способность применять соответствующий математический аппарат для решения профессиональных задач.

В результате изучения дисциплины студент должен:

Знать:

- основные требования к шифрам;
- основные характеристики современных криптосистем;
- структуру базовых стандартизированных криптоалгоритмов.

Уметь:

- применять методы криптографической защиты информации в профессиональной деятельности;
- формировать предложения по составу подсистемы криптографической защиты информации;
- применять способы оценки криптостойкости шифров;

Владеть:

- методами применения теоретических знаний и практических навыков при оценке характеристик криптографических систем.
- терминологией в области криптографической защиты информации.
- навыками использования типовых криптографических алгоритмов.

4. Объем дисциплины (модуля) и виды учебной работы

Вид учебной работы	Всего часов / зачетных единиц	Семестры			
		6			
Аудиторные занятия (всего)	80/2,22	80/2,22			
В том числе:	-	-	-	-	-
Лекции	32/0,89	32/0,89			
Практические занятия (ПЗ)	16/0,44	16/0,44			
Семинары (С)					
Лабораторные работы (ЛР)	32/0,89	32/0,89			
КСР	2/0,06	2/0,06			
Контроль					
Самостоятельная работа (всего)	26/0,72	26/0,72			
В том числе:	-	-	-	-	-
Курсовой проект (работа)					
Расчетно-графические работы					
Реферат (при наличии)					
Другие виды самостоятельной работы					
Вид промежуточной аттестации (*зачет, экзамен*)	зачет	зачет			
Контактная работа (всего)	82/2,28	82/2,28			
Общая трудоемкость часы	108	108			
зачетные единицы	3	3			

5. Содержание дисциплины (модуля)

5.1. Содержание разделов и тем дисциплины (модуля). Все разделы и темы нумеруются

РАЗДЕЛ 1 Основы криптографии.

Тема 1.1. Основные понятия и задачи криптографии.

Исторический обзор. Основные задачи и понятия криптографии. Требования к криптосистемам.

Тема 1.2. Классификация шифров, их основные типы и свойства.

Шифры перестановки. Шифры замены.

Тема 1.3. Общая структура криптосистемы, надёжность и криптографическая стойкость шифров.

Принципы построения криптосистем К.Шеннона. Вопросы имитозащиты.

Помехоустойчивость шифров. Оценка криптостойкости различных алгоритмов: простых и многомерных подстановок, гаммирования по ключу.

РАЗДЕЛ 2 Криптографическая защита информации на основе симметричных криптосистем.

Тема 2.1. Одноключевые методы шифрования, элементы теории чисел.

Принципы построения криптографических алгоритмов. Режимы выполнения симметричных криптоалгоритмов. Генераторы псевдослучайных последовательностей и их схемная реализация. Элементы алгоритмической теории чисел.

Тема 2.2. Блочные и потоковые шифры.

Основы построения блочных шифров. Потоковые шифры. Комбинированное шифрование. Режимы шифрования. Сеть Фейстеля.

Тема 2.3. Алгоритмы и стандарты симметричных криптосистем.

Алгоритм DES. Усиления DES. Алгоритм IDEA. Алгоритм AES. Алгоритм ГОСТ 28147-89. Российский алгоритм криптографического преобразования. Национальный стандарт РФ по ГОСТ 34.13-2018.

РАЗДЕЛ 3. Криптографическая защита информации на основе асимметричных криптосистем

Тема 3.1. Двухключевые алгоритмы шифрования и криптосистемы.

Требования к асимметричным криптосистемам. Обмен Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамаля.

Тема 3.2. Современные технологии шифрования.

Криптосистемы на эллиптических кривых. Математические основы. Выбор параметров кривой.

Тема 3.3. Криптоанализ шифров.

Подходы к анализу криптографических алгоритмов. Метод перебора. Частотный анализ. Корреляционный метод анализа поточных шифров. Линейный и дифференциальный методы анализа блочных шифров.

РАЗДЕЛ 4. Криптографические методы защиты электронного документооборота

Тема 4.1. Хеш-функции и их криптографические приложения.

Целостность данных и аутентификация источника данных. Общие сведения о хеш-функциях. Требования к хэш-функциям. Понятие о стойкости хеш-функции. Ключевые и бесключевые хеш-функции. Российский стандарт 2018.

Тема 4.2. Электронная подпись, отечественные и зарубежные стандарты.

Задачи и назначения электронной подписи. Классификация электронных подписей. Примеры цифровых подписей на основе алгоритмов RSA, Эль-Гамаля. Стандарты подписи

ГОСТ 3410 и DSS. Инфраструктура открытых ключей. Правовое обеспечение электронной подписи.

Тема 4.3. Средства криптографической защиты информации.

Средство криптографической защиты информации (СКЗИ) серии Криптон. СКЗИ КриптоПро CSP. Скремблеры.

5.2. Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№№ разделов (тем) данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин
1	Программно-аппаратные средства защиты информации	4 (4.1-4.3)
2	Теория информации	1 (1.1-1.3)
3	Комплексное обеспечение информационной безопасности автоматизированных систем	2 (2.1-2.3) 3 (3.1-3.3)
4	Практика по получению первичных профессиональных умений и навыков	1 (1.1-1.3) 2 (2.1-2.3) 3 (3.1-3.3)
5	Эксплуатационная практика	1 (1.1-1.3) 2 (2.1-2.3) 3 (3.1-3.3)
6	Проектно-технологическая практика	1 (1.1-1.3) 2 (2.1-2.3) 3 (3.1-3.3)

5.3. Разделы и темы дисциплин (модулей) и виды занятий

№ п/п	Наименование раздела	Наименование темы	Виды занятий в часах					
			Лекц.	Практ. зан.	Семин	Лаб. зан.	СРС	Всего
1.	***Раздел 1***	Тема 1.1	2	4			2	8
2.	***Раздел 1***	Тема 1.2	4			4	2	10
3.	***Раздел 1***	Тема 1.3	2			4	2	8

4.	***Раздел 2***	Тема 2.1	2	4			2	8
5.	***Раздел 2***	Тема 2.2	2			4	2	8
6.	***Раздел 2***	Тема 2.3	4			4	2	10
7.	***Раздел 3***	Тема 3.1	4	4			2	10
8.	***Раздел 3***	Тема 3.2	2			4	2	8
9.	***Раздел 3***	Тема 3.3	2			4	2	8
10.	***Раздел 4***	Тема 4.1	2	2			2	6
11.	***Раздел 4***	Тема 4.2	4	2		4	4	14
12.	***Раздел 4***	Тема 4.3	2			4	2	8

6. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)	Оценочные средства	Формируемые компетенции
1	**2**	**3**	**4**	**5**	**6**
1.	***Раздел 1. Тема 1.1.***	ПЗ.1. Математические основы криптографии. ПЗ.2. Математические основы шифров.	4	Тестовый контроль по теме	ОПК-2
2.	***Раздел 1. Тема 1.2.***	Лр.1. Шифры замены.	4	Защита лабораторной работы	ОПК-2
3.	***Раздел 1. Тема 1.3.***	Лр. 2. Шифры перестановки.	4	Защита лабораторной работы	ОПК-2
4.	***Раздел 2. Тема 2.1.***	ПЗ 3. Элементы теории чисел. ПЗ 4. Математические основы симметричных шифров.	4	Тестовый контроль по теме	ОПК-2
5.	***Раздел 2. Тема 2.2.***	Лр. 3. Шифры гаммирования.	4	Защита лабораторной работы	ОПК-2
6.	***Раздел 2. Тема 2.3.***	Лр. 4. Комбинированные шифры.	4	Защита лабораторной работы	ОПК-2
7.	***Раздел 3. Тема 3.1.***	ПЗ 5. Односторонние функции. ПЗ 6. Поля Галуа.	4	Тестовый контроль по теме	ОПК-2
8.	***Раздел 3. Тема 3.2.***	Лр.5. Асимметричные шифры.	4	Защита лабораторной работы	ОПК-2
9.	***Раздел 3. Тема 3.3.***	Лр. 6. Электронные подписи.	4	Защита лабораторной работы	ОПК-2
10.	***Раздел 4. Тема 4.1.***	ПЗ 7. Алгоритмы хэширования и криптоанализа хэш-функций ПЗ 8. Схемы электронных подписей на основе криптографических систем.	4	Тестовый контроль по теме	ОПК-2
11.	***Раздел 4. Тема 4.2.***	Лр. 7. Установка, настройка и эксплуатация средств электронной	4	Защита лабораторн	ОПК-2

		подписи		ой работы	
12.	***Раздел 4. Тема 4.3.***	Лр. 8. Установка, настройка и эксплуатация СКЗИ КриптоПро CSP	4	Защита лабораторной работы	ОПК-2

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-5	**1.1-1.3**	Решение задач к практическим занятиям Подготовка к защите лабораторных работ	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	Учебный сайт	6
6-10	**2.1-2.3**	Решение задач к практическим занятиям Подготовка к защите лабораторных работ	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	Учебный сайт	6
11-15	**3.1-3.3**	Подготовка к защите лабораторных работ	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	Учебный сайт	6
16-20	**4.1-4.3**	Решение задач к практическим занятиям Подготовка к защите лабораторных работ	Повторение и углубленное изучение учебного материала лекции, ПЗ с использовани	Учебный сайт	8

			ем конспекта лекций, литературы, Интернет - ресурсов		
21		Подготовка доклада с презентацией		Учебный сайт	
22		Подведение итогов		Учебный сайт	

6.2. Методические указания по организации самостоятельной работы студентов

Текущая самостоятельная работа по дисциплине «Криптографические методы защиты информации», направленная на углубление и закрепление знаний студента, на развитие практических умений, включает в себя следующие виды работ:

- работа с лекционным материалом;
- подготовка к практическим занятиям;
- выполнение индивидуальных проектов;
- подготовка к лабораторным работам;
- подготовка к зачету.

Творческая проблемно-ориентированная самостоятельная работа по дисциплине «Криптографические методы защиты информации», направленная на развитие интеллектуальных умений, общекультурных и профессиональных компетенций, развитие творческого мышления у студентов, включает в себя следующие виды работ по основным проблемам курса:

- поиск, анализ, структурирование информации;
- выполнение графических работ, обработка и анализ данных;
- участие в конференциях, олимпиадах и конкурсах.

Оценка результатов самостоятельной работы организуется как единство двух форм: самоконтроль и контроль со стороны преподавателя.

Самоконтроль зависит от определенных качеств личности, ответственности за результаты своего обучения, заинтересованности в положительной оценке своего труда, материальных и моральных стимулов, от того насколько обучаемый мотивирован в достижении наилучших результатов. Задача преподавателя состоит в том, чтобы создать условия для выполнения самостоятельной работы (учебно-методическое обеспечение), правильно использовать различные стимулы для реализации этой работы (рейтинговая система), повышать её значимость, и грамотно осуществлять контроль самостоятельной деятельности студента (фонд оценочных средств).

7. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) учебным планом не предусмотрены.

8. Учебно-методическое и информационное обеспечение дисциплины (модуля):

1. Бутакова Н. Г., Федоров Н. В. Криптографические методы и средства защиты информации: Учебное пособие. ИЦ Интермедия, 2020, - 380 с. https://e.lanbook.com/book/161347

2. Лось А. Б. учебник для акад. бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков ; Высш. шк. экономики, Нац. исслед. ун-т. - М. : Юрайт, 2016. - 473 с.

3. Бабенко Л. К. Криптографическая защита информации: симметричное шифрование: учеб. пособие для вузов / Л. К. Бабенко, Е. А. Ищукова; Южный фед. ун-т. - М. : Юрайт, 2018. - 220 с.

4. Каширская Е. Н. Криптографический анализ и методы защиты информации: Учебное пособие. МИРЭА - Российский технологический университет, 2020. – 91 с.

9. Материально-техническое обеспечение дисциплины (модуля)

Компьютерная лаборатория 323б (14 серверов) и лекционная аудитория 225, оснащенные мультимедийными средствами, электронной базой знаний, системой тестирования, выходом в глобальную сеть Интернет. Технические характеристики серверов обеспечивают возможность моделирования необходимого аппаратного обеспечения для работы с современными компьютерными системами хранения и обработки информации.

10. Образовательные технологии

Для достижения планируемых результатов обучения, в дисциплине «Криптографические методы защиты информации» используются различные образовательные технологии:

Информационно-развивающие технологии, направленные на формирование системы знаний, запоминание и свободное оперирование ими.

Используется лекционно-семинарский метод, самостоятельное изучение литературы, применение новых информационных технологий для самостоятельного пополнения знаний, включая использование технических и электронных средств информации.

Деятельностные практико-ориентированные технологии, направленные на формирование системы профессиональных практических умений при проведении экспериментальных исследований, обеспечивающих возможность качественно выполнять профессиональную деятельность.

Используется анализ, сравнение методов проведения химических исследований, выбор метода, в зависимости от объекта исследования в конкретной производственной ситуации и его практическая реализация.

Развивающие проблемно-ориентированные технологии, направленные на формирование и развитие проблемного мышления, мыслительной активности, способности видеть и формулировать проблемы, выбирать способы и средства для их решения. Используются виды проблемного обучения: освещение основных проблем общей и неорганической химии на лекциях, учебные дискуссии, коллективная деятельность в группах при выполнении лабораторных работ, решение задач повышенной сложности. При этом используются первые три уровня (из четырех) сложности и самостоятельности: проблемное изложение учебного материала преподавателем; создание преподавателем проблемных ситуаций, а обучаемые вместе с ним включаются в их разрешение; преподаватель создает проблемную ситуацию, а разрешают её обучаемые в ходе самостоятельной деятельности.

Личностно-ориентированные технологии обучения, обеспечивающие в ходе учебного процесса учет различных способностей обучаемых, создание необходимых условий для развития их индивидуальных способностей, развитие активности личности в учебном процессе. Личностно-ориентированные технологии обучения реализуются в результате индивидуального общения преподавателя и студента при защите лабораторных работ, при выполнении домашних индивидуальных заданий, решении задач повышенной сложности, на еженедельных консультациях.

11. Оценочные средства (ОС):

11.1. Оценочные средства для входного контроля

Не предусмотрено

11.2. Оценочные средства текущего контроля

Вопросы к практическим занятиям (12 тем). Представляют собой перечень вопросов, проверяющих знание теоретического лекционного материала и тем, вынесенных на самостоятельную проработку:

Пз. 1 Найти число x, удовлетворяющее уравнению $3^x = 5(\mathrm{mod} p)$,
где $p - 1 = 2 \cdot 3 \cdot 101 \cdot 103 \cdot 107^2$.
Упрощенный вариант: $p - 1 = 2 \cdot 3 \cdot 101$, или $p - 1 = 2 \cdot 3 \cdot 11 \cdot$

Пз. 2 Определить ключи шифра Цезаря, если известны следующие пары открытый текст – шифротекст: а) АПЕЛЬСИН-САЦЬНВШЮ б) АБРИКОС - ЫЬЛГЕЙМ.

Пз. 3 Используя алгоритм Эвклида и обобщенный алгоритм Эвклида, вычислить наибольшие общие делители d для следующей пары чисел (m,n), дать представление вида $d=mk+nl$: (153, 648),(83, 597),(113, 481),(39, 379),(123, 48),(429, 376), (1526, 748),(439, 817),(356, 499),(15439, 379),(1983, 13675).

Пз. 4 Выполните первый цикл алгоритма шифрования ГОСТ 28147-89 в режиме простой

замены. Для получения 64 бит исходного текста используйте 8 первых букв из своих данных: Фамилии Имени Отчества. Для получения ключа (256 бит) используют текст, состоящий из 32 букв. Первый подключ содержит первые 4 буквы.

Пз. 5 Используя полином $f(x)=x^3+x+1$(неприводимый), $\deg(f(x))=3$, тогда его можно использовать для построения расширенного поля $GF(2^3)=GF(8)$.

Пз.6 Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из первой сотни. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

Пз.7 Найтиде хеш–образ своей Фамилии, используя хеш–функцию $H_i = (H_{i-1} + M_i)^2 \bmod n$, где n = pq, p, q – заданы.

Пз. 8 Используя хеш-образ своей Фамилии, вычислите электронную подпись по схеме RSA. Пусть хеш-образ Фамилии равен 233, а закрытый ключ алгоритма RSA равен (25, 247).

11.3. Оценочные средства для текущего контроля в форме тестирования

Тестовые вопросы для проверки сформированности компетенции

ОПК-2. Способность применять соответствующий математический аппарат для решения профессиональных задач.

1. Укажите двухключевую криптосистему:
А) DES
Б) RSA
В) ГОСТ 28147-89

2. Назовите закон об Электронной подписи?
А) ФЗ-16
Б) ФЗ-63
В) ФЗ-32

3. При применении несимметричной криптосистемы, используется:
А) секретный ключ
Б) открытый ключ
В) сначала открытый, а затем секретный ключ

4. Размер хэш-образа по российскому стандарту (ГОСТ-2012) равен:
А) 256 бит или 512 бит
Б) 320 бит или 160 бит
В) 160 бит

5. Двухключевая криптосистема по сравнению с одноключевой имеет более высокую производительность при шифровании данных:
А) ДА
Б) НЕТ
В) ОДИНАКОВУЮ

6. Современный протокол шифрования данных базируется на совместном применении как симметричной криптосистемы так и несимметричной:
А) ДА
Б) НЕТ
В) ТОЛЬКО СИММЕТРИЧНОЙ

7. Хэш-функция – криптографическое преобразование информации, переводящее ….
А) из данных фиксированной длины в некоторое значение произвольной длины;
Б) строку битов произвольной длины в строку битов фиксированной длины;
В) из данных произвольной длины некоторое значение произвольной длины.

8. Для проверки целостности информации используется:
А) альфа-функция
Б) бета-функция
В) хэш-функция

9. Размер ЭП по российскому стандарту (ГОСТ-2012) равен:
А) 256 бит 320 бит
Б) 512 бит или 1024 бит
В) 320 бит

10. Программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра это?
А) средства записи и чтения;
Б) средства модуляции и детектирования;
В) средства удостоверяющего центра

11. Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите?
А) шифр Цезаря;
Б) шифр Соломона.
В) шифр Хеопса.

12. Прикладная наука о методах и способах преобразования информации с целью ее защиты от незаконных пользователей – это
А) криптозащита;
Б) криптография
В) криптовставка.

13. Уникальная последовательность символов, предназначенная для создания электронной подписи это?
А) ключ электронной подписи
Б) сертификат
В) синхропреамбула.

14. Хэш-функция не применяется:
А) для удаления информации.
Б) для защиты пароля;
В) при контроле целостности данных;

15. Двухключевая криптосистема применяется в следующих случаях (укажите все правильные варианты ответов):
А) для шифрования небольших по объему данных;
Б) при создании электронной подписи;
В) в задачах аутентификации;+

16. Что называется имитовставкой?:

А) специальный набор символов, который добавляется к сообщению и предназначен для обеспечения его целостности и аутентификации источника данных;

Б) набор символов, в котором для шифрования данных используется гаммирование;

В) шифр, в котором процедура шифрования заключается в перестановках элементов исходного текста или их групп, сами элементы при этом остаются неизменными;

17. Шифр Цезаря – это

а) асимметричный шифр

б) шифр биграммами

в) шифр замены со сдвигом

18. Какой алгоритм не используется при симметричном шифровании:

А) поточное шифрование;

Б) побитовое шифрование;

В) алгоритм Эль-Гамаля.

19. Что может указывать на изменение сообщения?

а) Изменился открытый ключ

б) Изменились дайджест сообщения

в) Изменился закрытый ключ

20. Какова длина блока алгоритма шифрования DES:

А) 64 бита;

Б) 56 бит;

В) 5 байт.

21. Сколько всего циклов выполняется операция зашифровывания в алгоритме DES:

А) 10;

Б) 20;

В) 16;

22. Что в переводе с греческого языка означает слово «криптография»?

А) тайнопись

Б) модуляция.

В) детектирование

23. Какой размер ключа в отечественном стандарте симметричного шифрования:

А) 53бит;

Б) 125 бит;

В) 256 бит.

24. Что из перечисленного ниже описывает разницу между алгоритмами DES и RSA?

а) DES – это алгоритм кодирования, а RSA – алгоритм декодирования

б) DES – это алгоритм записи, а RSA – алгоритм чтения.

в) DES – это симметричный алгоритм, а RSA – асимметричный алгоритм

25. Какое из этих утверждений является верным:

А) у S-блоков ГОСТ 4-битовые входы и 8-битовые выходы;

Б) у S-блоков ГОСТ 4-битовые входы и 4-битовые выходы;

В) у S-блоков ГОСТ 8-битовые входы и 4-битовые выходы;

26. Используется ли в отечественном стандарте симметричного шифрования процедура генерации подключей из ключей, как в DES:

А) да, но эта процедура сравнительно проста;

Б) не используется;

В) используется аналогичная по сложности процедура.

27. В отечественном стандарте симметричного шифрования применяется подстановка, основанная на применении S-блоков. Сколько таких блоков используется в ГОСТ:

А) 8;

Б) 12;

В) 14;

28. Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи это?

А) исходный текст;

Б) ключ проверки электронной подписи

В) открытый текст.

29. Выберите правильное утверждение:

А) в DES нет битовых перестановок шифруемого блока.

Б) в отечественном стандарте симметричного шифрования нет начальной и конечной битовых перестановок шифруемого блока, так как они не влияют на стойкость шифра;

В) в DES нет начальной и конечной битовых перестановок шифруемого блока.

30. Что представляет собой операция XOR?

А) интегрирование;

Б) дифференцирование;

В) сложение по модулю 2.

31. К какому классу преобразований относится шифр Цезаря?

А) подстановки;

Б) суммирования.

В) гаммирование.

32. Что в криптографии называют открытым текстом?

А) электронную цифровую подпись

Б) закрытый ключ шифрования

В) исходное сообщение (сообщение до шифрования)

33. **Какой из перечисленных ниже алгоритмов шифрования не является симметричным?**

А) DES;

Б) RSA;

В) IDEA;

34. **Какую длину имеет секретный ключ в алгоритме DES?**

а) 2 бита;

б) 56 бит;

в) 4 бит;

35. Какая архитектура лежит в основе алгоритма DES?

а) сеть Фейстеля;

б) потоковый шифр;

в) сеть Петри;

36. На чем основана криптостойкость метода Диффи-Хэллмана?

а) на вычислении интегралов;

б) на функции возведения в степень;

в) на трудности вычислений дискретных логарифмов.

37. Какая процедура распределения ключей *не* требует использования защищенного канала для передачи ключа адресату?

а) процедура шифрования по алгоритму DES;

б) продедура Диффи-Хэллмана;

в) процедура шифрования Вижинера.

38. Дайджест сообщения (message digest) – это …

а) результат демодуляции;

б) результат кодирования.

в) результат хэширования.

39. Что такое односторонняя хэш-функция?

а) хэш-функция, трудно вычислимая как в прямом, так и обратном направлениях;

б) хэш-функция, легко вычислимая как в прямом, так и обратном направлениях;

в) хэш-функция, легко вычислимая в прямом и трудно вычисляемая в обратном направлении.

40. Чему равен результат вычисления хэш-функции по алгоритму SHA?

а) 160 бит;

б) 127 бит;

в) 63 бита;

41. Какой шифр является симметричными?

а) RSA (Rivest-Shamir-Alderman);

б) DES (DataEncryptionStandart);

в) Эль-Гамаль (ElGamal).

42. Как называется сообщение, полученное после преобразования с использованием любого шифра?

А) ключом

Б) закрытым текстом

В) текстом

43. Математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, называется в криптографии

А) односторонней функцией

Б) функцией Соломона.

В) функцией Фурье

44. Какие из перечисленных ниже алгоритмов являются асимметричными? (укажите все правильные ответы)

а) DES;

б) Эль-Гамаль (El-Gamal);
в) RSA+.

45. Что называется ключом электронной подписи?
А) уникальная последовательность символов, предназначенная для создания электронной подписи.
Б) средство, используемые для оказания услуг доверенной третьей стороной;
В) метка доверенного времени.

46. Что называется электронной подписью?
а) характеристика шифра для криптографического преобразования сообщения;
б) присоединенные к сообщению фамилия, имя и отчество отправителя;
в) информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

47. Виды электронной подписи:
А) простая, неквалифицированная, квалифицированная.
Б) быстрая, сложная, простая.
В) оригинальная, неоригинальная,

48. Программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра это?
А) средства записи и чтения;
Б) средства модуляции и детектирования;
В) средства удостоверяющего центра

49. Какие шифры являются симметричными? (укажите все правильные ответы)
а) DES (DataEncryptionStandart);
б) RSA (Rivest-Shamir-Alderman);
в) ГОСТ 28147-89; +

50. Пространством ключей называют
А) множество всех возможных ключей, доступных для использования в алгоритме.
Б) одинаковые ключи;
В) дублированные ключи.

51. Шифрование речевых сообщений
А) модуляция;
Б) манипуляция;
В) аудиоскремблирование.

52. Название одного из алгоритмов блочного шифрования:
А) «Морж»
Б) «Кузнечик»
В) «Цапля»

53. Какое из нижеперечисленных средств используется для формирования электронной подписи?
а) «Бумеранг»
б) «КриптоПро CSP»
в) «Спрут»

54. Что из нижеперечисленного относится к средствам криптографической защиты информации?

а) «Гранит»

б) «Катран»

в) «КриптоПро CSP»

55. Какой математический аппарат используется в криптографии?

А) поля Ширака;

Б) поля Минтона;

В) поля Галуа;

56. Сложность нахождения секретного ключа системы RSA определяется

а) сложностью разложения числа n на простые множители +

б) сложностью интегрирования;

в) сложностью дифференцирования;

57. Кем было выполнено доказательство существования абсолютно стойких криптографических алгоритмов?

А) Б. Соломоном

Б) К. Шенноном

В) Б. Штанмайером

58. Что определяло надежность алгоритма DES?

а) сложностью интегрирования;

б) размер ключа.

в) вычисление корней алгебраических уравнений.

59. Единственный неуязвимый шифр?

А) одноразовый шифровальный блокнот;

Б) шифр Хэмминга.

В) шифр DES.

60. Стеганографией называют

а) науку о раскрытии шифров;

б) наука (и практика ее применения) о методах и способах вскрытия шифров.

в) совокупность методов и средств защиты информации от несанкционированного доступа путем скрытия факта существования тайного сообщения.

11.4. Оценочные средства для текущего контроля в форме контрольной работы

Демонстрационный вариант контрольной работы №1

1. Какая пара чисел сравнима по mod7 и не сравнима по mod5: (42,47), (–2,12), (19,–6)?

2. Сложите сравнения и определите класс вычетов, содержащий результат:

а) $-9 \equiv 12(\mathrm{mod}7)$, $17 \equiv 3(\mathrm{mod}7)$;

б) $-5 \equiv 12(\mathrm{mod}17)$, $17 \equiv 85(\mathrm{mod}17)$.

3. Какие пары чисел (n,e) можно использовать для построения системы RSA: а) n = 473, e = 289; б) n = 13589, e = 3377; в) n = 38989, e = 4601?

При допустимом наборе определите закрытый ключ d, зашифруйте сообщение x = 128 и затем расшифруйте криптограмму.

4. Докажите, что если $x + k \equiv y(\mathrm{mod}\ 2)$, то $y + k \equiv x(\mathrm{mod}\ 2)$..

5. В алгоритме RSA известно, что $n = p \cdot q = 11102239$, $\phi(n) = 11095560$. Разложите n на множители.

11.5. Оценочные средства для промежуточной аттестации

(в форме зачета).

Проверяется степень усвоения теоретических и практических знаний, приобретенных умений на репродуктивном и продуктивном уровне.

Примерный перечень вопросов и заданий к зачету

Раздел 1. Основы криптографии

Тема 1.1. Основные понятия и задачи криптографии.

1. Аспекты безопасности информации.
2. Основные понятия криптографии.
3. Шифры Цезаря, Вижинера.

Тема 1.2. Классификация шифров, их основные типы и свойства.

1. Общая схема шифрования.
2. Основные требования к шифрам.
3. Шифры перестановки.
4. Шифры замены.

Тема 1.3. Общая структура криптосистемы, надёжность и криптографическая стойкость шифров.

1. Принципы построения криптосистем К.Шеннона.
2. Помехоустойчивость шифров.
3. Надёжность и криптографическая стойкость шифров.

Раздел 2. Криптографическая защита информации на основе симметричных криптосистем

Тема 2.1. Одноключевые методы шифрования, элементы теории чисел.

1. Принципы построения криптографических алгоритмов.
2. Режимы выполнения симметричных криптоалгоритмов.

Тема 2.2. Блочные и поточные шифры.

1. Способы формирования ключей для поточного шифрования.
2. Сеть Фейстеля.
3. Особенности блочных и поточных щифров.

Тема 2.3. Алгоритмы и стандарты симметричных криптосистем.

1. Стандарт криптографической защиты DES.
2. Модификации алгоритма DES.
3. Российский алгоритм криптографического преобразования: режимы шифрования.
4. Российский алгоритм криптографического преобразования: режим имитовставки.
5. Российский алгоритм криптографического преобразования: режим гаммирования.

Раздел 3. Криптографическая защита информации на основе асимметричных криптосистем

Тема 3.1. Двухключевые алгоритмы шифрования и криптосистемы.

1. Обмен Диффи-Хеллмана. Назначение мастер-ключа.
2. Односторонние функции.
3. Дискретное логарифмирование.
4. Несимметричные системы шифрования.
5. Алгоритм RSA.
6. Криптосистема Эль-Гамаля.
7. Сравнение симметричных и несимметричных криптосистем.

Тема 3.2. Современные технологии шифрования.

1. Криптосистемы на эллиптических кривых.
2. Математические основы криптосистем на эллиптических кривых.
3. Выбор параметров кривой.

Тема 3.3. Криптоанализ шифров.

1. Подходы к анализу криптографических алгоритмов.
2. Криптостойкость симметричных криптосистем.
3. Криптостойкость асимметричных криптосистем.
4. Метод перебора.
5. Частотный анализ.
6. Корреляционный метод анализа поточных шифров.
7. Линейный и дифференциальный методы анализа блочных шифров.

Раздел 4. Криптографические методы защиты электронного документооборота.

Тема 4.1. Хеш-функции и их криптографические приложения.

1. Определение и назначение хэш-функции, российский стандарт.
2. Требования к хэш-функциям.
3. Понятие о стойкости хеш-функции.
4. Ключевые и бесключевые хеш-функции.

Тема 4.2. Электронная подпись, отечественные и зарубежные стандарты.

1. Классификация электронных подписей.
2. Российский стандарт ЭП: технология создания и проверки.
3. Электронная подпись: определения, назначение, роль в электронном документообороте.
4. Инфраструктура открытых ключей.
5. Правовое обеспечение электронной подписи.
6. Примеры цифровых подписей на основе алгоритмов RSA, Эль-Гамаля.
7. Стандарты подписи ГОСТ 3410 и DSS.

Тема 4.3. Средства криптографической защиты информации.

1. СКЗИ серии Криптон.
2. СКЗИ КриптоПро CSP.
3. Скремблеры.

Разработчики:

_____	_профессор_____	_Корольков Ю.Д._____
(подпись)	(занимаемая должность)	(Ф.И.О.)

_____	___профессор_____	_Ерохин В.В._____
(подпись)	(занимаемая должность)	(Ф.И.О.)

Программа составлена в соответствии с требованиями ФГОС ВО и учитывает рекомендации ПООП по направлению и профилю подготовки **10.03.01 Информационная безопасность**.

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «20» 03 2020 г. Протокол № 8

И.о.зав. кафедрой  Колесник С.Н.