МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет физико-технический

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Хагуров Т.А.
подпись
«_4_» _мая_ 20_21_г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
ФТД. 02 Современная криптография

Направление подготовки/специальность 09.04.02 Информационные системы и технологии

Направленность (профиль)/ специализация Администрирование информационных систем

Фома обучения очно- заочная

Квалификация магистр

Краснодар 2021

Рабочая программа дисциплины ФТД. 02 Современная криптография составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки/ специальности 09.04.02 Информационные системы и технологии

Программу составил(и):
Е.Н. Тумаев, профессор кафедры теоретической физики и компьютерных технологий,
доктор физ.-мат. наук, доцент _____
подпись

Рабочая программа дисциплины ФТД. 02 Современная криптография утверждена на заседании кафедры теоретической физики и компьютерных технологий
протокол № 8 от 16 апреля 2021 г.
Заведующий кафедрой (выпускающей) В.А. Исаев _____
подпись

Утверждена на заседании учебно-методической комиссии физико-технического факультета
протокол №13 «16» апреля 2021 г.
Председатель УМК факультета Богатов Н.М. _____
подпись

Рецензенты:

Г.Ф. Копытов, заведующий кафедрой радиофизики и нанотехноогий КубГУ, доктор физико-математических наук, профессор

Л.Р. Григорян, генеральный директор ООО НПФ «Мезон»
кандидат физико-математических наук

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины – освоение студентами основных принципов современной криптографии и умение практического применения знаний для защиты информации.

1.2 Задачи дисциплины:

1) дать представления о классических системах шифрование;
2) дать представление о современных симметричных блочных шифров и о методах их взлома;
3) дать представление о современных потоковых шифрах;
4) познакомить с современной ассиметричной криптографией.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Современная криптография» относится к вариативной части факультативного блока учебного плана.

Дисциплина «Современная криптография» учитывает накопленный опыт практической работы магистрантов в образовательных учреждениях, расширяет рамки представлений о сущности образования через освоение подходов к современной классификации наук и месте образования в этой классификации, раскрывает философские проблемы становления человека, методы получения современного научного знания в области образования, а также образовательные инновации, проекты, критерии оценки их эффективности. Изучение дисциплины является основой для последующего изучения дисциплин профессионально-педагогического цикла. Дисциплина базируется на знаниях, полученных при изучении дисциплин «Методы исследования и моделирования информационных процессов и технологий», «Логика и методология науки».

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся профессиональных компетенций (ПК)

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ПК-8	умением проводить разработку и исследование теоретических и экспериментальных моделей объектов профессиональной деятельности в областях: машиностроение, приборостроение, наука,	основную терминологию в области защиты информации	использовать методы и средства защиты информации	основными технологиями построения систем защиты информации

		техника, образование, медицина, административное управление, юриспруденция, бизнес, предпринимательство, коммерция, менеджмент, банковские системы, безопасность информационных систем, управление технологическими процессами, механика, техническая физика, энергетика, ядерная энергетика, силовая электроника, металлургия, строительство, транспорт, железнодорожный транспорт, связь, телекоммуникации, управление инфокоммуникациями, почтовая связь, химическая промышленность, сельское хозяйство, текстильная и легкая промышленность, пищевая промышленность, медицинские и биотехнологии, горное дело, обеспечение безопасности подземных предприятий и производств, геология, нефтегазовая отрасль, геодезия и картография, геоинформационные системы, лесной			

		комплекс, химико-лесной комплекс, экология, сфера сервиса, системы массовой информации, дизайн, медиаиндустрия, а также предприятия различного профиля и все виды деятельности в условиях экономики информационного общества			
2.	ПК-13	способностью прогнозировать развитие информационных систем и технологий	методы прогнозирования проектом информационных систем	проводить исследования характеристик компонентов и информационных систем в целом	навыками составления инновационных проектов

2. Структура и содержание дисциплины.

Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 2 зач.ед. (72 ч.), их распределение по видам работ представлено в таблице

(для студентов ОФО).

Вид учебной работы		Всего часов	Семестры (часы)			
			1			
Контактная работа, в том числе:		24,2	24,2			
Аудиторные занятия (всего):		**24**	**24**			
Занятия лекционного типа		12	12	-	-	-
Занятия семинарского типа (семинары, практические занятия)		12	12	-	-	-
Иная контактная работа:						
Контроль самостоятельной работы (КСР)						
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:		**47,8**	**47,8**			
Проработка учебного (теоретического) материала		27,8	27,8	-	-	-
Реферат		20	20	-	-	-
Подготовка к зачёту				-	-	-
Общая трудоемкость	**час.**	**72**	**72**	-	-	-
	в том числе контактная работа	24,2	24,2			

	зач. ед	**2**	**2**			

Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины. Разделы дисциплины

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Основы теории чисел	12	2	2		7
2.	Числовые сравнения	11	2	2		7
3.	Симметричные и ассиметричные шифры	11	2	2		7
4.	Методы взлома шифров	11	2	2		7
5.	Современные симметричные криптосистемы	11	2	2		7
6.	Отечественный стандарт шифрования данных ГОСТ	9	1	1		7
7.	Цифровая подпись	7,8	1	1		5,8
	Итого по дисциплине:	72,8	12	12		47,8

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

Содержание разделов дисциплины:
Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1.	Основы теории чисел	Делимость. Простые и составные числа.НОД и НОК чисел. Разложение числа на простые множители. Сумма и произведение делителей числа	Опрос
2.	Числовые сравнения	Полная и приведенная системы вычетов. Кольцо вычетов по модулю n. Функция Эйлера, свойство мультипликативности. Теорема Эйлера. Теорема Ферма. Диофантовы уравнения первой степени. Китайская теорема об остатках.	Опрос

3.	Симметричные и ассиметричные шифры	Основные понятия и определения. Шифры перестановки: шифр перестановки «скитала», шифрующие таблицы, применение магических квадратов.	Опрос
4.	Методы взлома шифров	Шифры простой замены: полибианский квадрат, система шифрования Цезаря, аффинная система подстановок Цезаря, система Цезаря с ключевым словом, шифрующие таблицы Трисемуса, биграммный шифр Плейфера, криптосистема Хилла, система омофонов	Опрос
5.	Современные симметричные криптосистемы	Принцип итерирования. Конструкция Фейтстеля.Американский стандарт шифрования данных DES. Область применения алгоритма DES.	Опрос
6.	Отечественный стандарт шифрования данных ГОСТ	режим простой замены, режим гаммирования, режим гаммирования с обратной связью, режим выработки имитовставки.	Опрос
7.	Цифровая подпись	Идентификация и проверка подлинности. Взаимная проверка подлинности пользователей	Опрос

Занятия семинарского типа.

№	Наименование раздела	Тематика практических занятий (семинаров)	Форма текущего контроля
1	2	3	4
1.	Основы теории чисел	Делимость. Простые и составные числа.НОД и НОК чисел. Разложение числа на простые множители. Сумма и произведение делителей числа	Реферат
2.	Числовые сравнения	Полная и приведенная системы вычетов. Кольцо вычетов по модулю n. Функция Эйлера, свойство мультипликативности. Теорема Эйлера. Теорема Ферма. Диофантовы уравнения первой степени. Китайская теорема об остатках.	Задание

3.	Симметричные и ассиметричные шифры	Основные понятия и определения. Шифры перестановки: шифр перестановки «скитала», шифрующие таблицы, применение магических квадратов.	Реферат
4	Методы взлома шифров	Шифры простой замены: полибианский квадрат, система шифрования Цезаря, аффинная система подстановок Цезаря, система Цезаря с ключевым словом, шифрующие таблицы Трисемуса, биграммный шифр Плейфера, криптосистема Хилла, система омофонов	Реферат
5.	Современные симметричные криптосистемы	Принцип итерирования. Конструкция Фейтстеля.Американский стандарт шифрования данных DES. Область применения алгоритма DES.	Задание
6.	Отечественный стандарт шифрования данных ГОСТ	режим простой замены, режим гаммирования, режим гаммирования с обратной связью, режим выработки имитовставки.	Задание
7.	Цифровая подпись	Идентификация и проверка подлинности. Взаимная проверка подлинности пользователей	Реферат

Лабораторные занятия.

Не предусмотрены

Примерная тематика курсовых работ (проектов)

Не предусмотрены

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Курсовая работа, выпускная квалификационная работа	Методические указания предназначены для использования студентами всех направлений по написанию курсовых и выпускных квалификационных работ, утвержденные теоретической физики и компьютерных технологий, протокол №12 от 3.05.17 г.

2	Самоподготовка	Методические рекомендации по самоподготовке, утвержденные кафедрой теоретической физики и компьютерных технологий, протокол №12 от 3.05.17 г.
3	Самостоятельное изучение	Учебно-методическое указания «Численные методы и математическое моделирование», используемые для самостоятельного изучения теоретических основ информационных технологий и утверждённые кафедрой теоретической физики и компьютерных технологий, протокол №12 от 3.05.17 г.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа,

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии.

В процессе преподавания дисциплины для реализации компетентностного подхода предусматривается использование в учебном процессе активных и интерактивных форм проведения занятий, применяются образовательные технологии лекционно-экзаменационной системы обучения и развития креативного мышления. При чтении дисциплины применяются такие виды лекций, как вводная, обзорная, проблемная, лекция-презентация. В течение семестров студенты выполняют самостоятельные работы, контрольные задания и итоговую контрольную работу. Оценка знаний студентов осуществляется на основе рейтинга, сдачи экзаменов.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

4.1. Фонд оценочных средств для проведения текущего контроля.

Опрос по разделам

1. Делимость целых чисел. Основные свойства делимости.
2. Простые и составные числа.
3. НОД и НОК чисел.
4. Числовые сравнения и их свойства.
5. Кольцо Z_n
6. Полна и приведенная система вычетов. Функция Эйлера.
7. Теорема Эйлера и Ферма.

8. Диофантовы уравнений первой степени и способы их решения.
9. Китайская терема об остатках.
10. Основные понятия криптографии.
11. Виды криптографических атак.
12. Шифры перестановки (определение, примеры).
13. Шифры простой замены (определение, примеры).
14. Шифры сложной замены (определение, примеры).
15. Симметричные системы шифрования.
16. Современные блочные шифры (общая схема и пример конкретного шифра с краткой характеристикой)
17. Режимы шифрование блочных шифров.
18. Современные потоковые шифры (общая схема и пример конкретного шифра с краткой характеристикой).
19. Ассиметричные системы шифрования (основные принципы).
20. Комбинированным метод шифрования.
21. Алгоритм RSA.
22. Хеш-функции (определение, примеры).
23. Цифровая подпись (определение, примеры).
24. Криптографические протоколы (определение, примеры)

Перечень части компетенций, проверяемых оценочным средством: ПК-8, ПК-13

Практические задания к разделу«Основы теории чисел»

1. Разложить на простые множители число а) 3551 ; б) 2407; в) 6497
2. Используя решето Эратосфена найти все простые числа из [1;100]
3. Доказать, что в натуральном ряду существуют сколь угодно большие отрезки, не содержащие простых чисел.
4. Найти НОД (99, 162), а также представление НОД через исходные числа.
5. Найти НОД(91427,3960,3360).
6. Найти сумму и число все возможных делителей чисел а) 375; б) 1200; в) 1890
7. Доказать свойства числовых сравнений.
8. Доказать, что число $2^{15}+14^7+5^7$ делится на 9.
9. Найти остаток при делении $22^{25}-23\cdot 14^7+55^{777}$ на 24.
10. Найти две последние цифры числа 203^{203203}
11. Найти функцию Эйлера для чисел а) 720; б) 1200; в) 5^{10}
12. Найти функцию Эйлера для числа $11\cdot 14\cdot 15$
13. Найдите число a, если $\varphi(a)=3600$ и $a=3^{\alpha}5^{\beta}7^{\gamma}$
14. Решить уравнение $\varphi(2x)=\varphi(3x)$
15. Образуют ли полную систему вычетов по модулю 6 числа -40; -45;31;26;-48;-34
16. Образуют ли приведенную систему вычетов по модулю 12 числа 385; -287;-133;--197.
17. Проверить теорему Эйлера для a=24, n=24.
18. Пользуясь теоремой Эйлера, найти остаток от деления 66^{25} на 7.
19. Решить сравнения а) $2x\equiv 3(\mathrm{mod}\,5)$ б) $28x\equiv 40(\mathrm{mod}\,44)$ в) $589x\equiv 101(\mathrm{mod}\,1349)$
20. Найти решения в целых числах $17x+13y=1$
21. Решить систему сравнений $\begin{cases}3x\equiv 7(\mathrm{mod}\,7)\\2x\equiv 3(\mathrm{mod}\,5)\\3x\equiv 3(\mathrm{mod}\,9)\end{cases}$

Практические задания к разделу«Симметричные и ассиметричные шифры»

1. Программа ROT13 (OCUNIX) циклически сдвигает каждую букву латинского алфавита на 13 позиций вправо. Как расшифровать криптограмму , применяя программу ROT13?
2. Пусть кодовый текст ЛЕДЕНЕЦ соответствует фразе открытого текста ПОВЕРНУТЬ КЛЮЧ ВПРАВО НА 90^0

Расшифровать кодовый текс
ЛЕДЕНЕЦ + ЛЕДЕНЕЦ+ ЛЕДЕНЕЦ

3. (Шифр ПОЛИБИЯ) Восстановить тест ЕИЙТДЕФЪЙЭ ФЭКЧЛЫ ДЧФЕЩГЕЩДЕСКЧ ВЯУЬЧ ШЩОМЩЙН_ЧЧ АЧФЫУЧКИКХКУВ_ЯЙ
4. Пусть секретный ключ состоит из одного слова ЗИМА , а открытый текс T=ШИФР_ВИЖЕНЕРА_ДЛЯ_ХАРЕРОВ. Зашифровать текст с помощью таблицы Виженера.
5. Расшифровать сообщение T=FBRNLWUGAJINZTHHXTEPHBNXSW зашифрованное линейным шифрующим преобразованием триграмм 26-буквенного алфавита A-Zсчисловыми эквивалентами 0-25. Известно, что последние три триграммы – это подпись отправителя JAMESBOND. Найти дешифрирующую матрицу и прочитать сообщение.
6. Построить криптосистему RSA для всех трех вариантов и зашифровать текст

T=ПАУК_НА_СУРАНЕН_КЕРЦЕ

Практические задания к разделу«Цифровая подпись»

1. Построить схему установления подлинности адресата на основе криптосистемы RSA(применить его числовой вариант).
2. Пусть два участника А(ключ а) и В (ключ в) решили установить между собой секретную связь без передачи ключей при открытом ключе p=23. Пусть a=5, в=7. Определить секретные ключи из соответствующих сравнений as=9 и вs=19. Зашифровать и подписать сообщение T= НЕ ПИШИТЕ ДЛИННЫЕ ПИСЬМА.
3. Построить криптосистему Эль-Гамаля для p=19 и подписать сообщение T=ВЕРНИСЬ_В_АРЦАХ.

Перечень компетенций, проверяемых оценочным средством: ПК-8, ПК-13

Темы рефератов

История криптографии

1. История криптографии. (Подробное описание развития криптографии с древнейший времен до настоящего времени).
2. История криптографии в России.
3. Криптография во Второй мировой войне.
4. Интересные истории, связанные с криптографией.
5. Стеганография.
6. Современная стеганография (компьютерная).

Шифры ручного шифрования

7. Шифр постой замены.
8. Шифр перестановки.
9. Шифр сложной замены. Шифр Вижинера.
10. Развитие шифра Вижинера.
11. Омофонная замена.
12. Биграммные шифры.
13. Интересные шифры ручного шифрования. И интересные истории, связанные с шифрами.
14. Криптография начала и середины 20 века.
15. Различные устройства для шифрования.
16. Энигма.

Современная криптография

17. История создания алгоритма DES.
18. Алгоритм DES.
19. Алгоритм ГОСТ.
20. Сравнение алгоритма DES и ГОСТ.
21. История конкурса на создания стандарта шифрования США AES.
22. Алгоритмы RC2 и RC5.
23. Режимы шифрования.
24. Потоковые шифры. Регистры сдвига с обратной связью. Регистры сдвига с линейной обратной связью.

Ассиметричная криптография

25. История ассиметричной криптографии.
26. Общая схема ассиметричной криптографии.
27. Алгоритм RSA.
28. Тайная история ассиметричной криптографи
29. Обзор сборников задач по криптографии.
30. Обзор библиотеки книг по криптографии(2010-2017 г).
31. Сайты о криптографии с кратким описанием.
32. Квантовая криптография.

4.2 Фонд оценочных средств для проведения промежуточной аттестации

Вопросы к зачету

25. Делимость целых чисел. Основные свойства делимости.
26. Простые и составные числа.
27. НОД и НОК чисел.
28. Числовые сравнения и их свойства.
29. Кольцо Z_n
30. Полна и приведенная система вычетов. Функция Эйлера.
31. Теорема Эйлера и Ферма.
32. Диофантовы уравнений первой степени и способы их решения.
33. Китайская терема об остатках.
34. Основные понятия криптографии.
35. Виды криптографических атак.
36. Шифры перестановки (определение, примеры).

37. Шифры простой замены (определение, примеры).
38. Шифры сложной замены (определение, примеры).
39. Симметричные системы шифрования.
40. Современные блочные шифры (общая схема и пример конкретного шифра с краткой характеристикой)
41. Режимы шифрование блочных шифров.
42. Современные потоковые шифры (общая схема и пример конкретного шифра с краткой характеристикой).
43. Ассиметричные системы шифрования (основные принципы).
44. Комбинированным метод шифрования.
45. Алгоритм RSA.
46. Хеш-функции (определение, примеры).
47. Цифровая подпись (определение, примеры).
48. Криптографические протоколы (определение, примеры)

Студенты обязаны сдать зачет в соответствии с расписанием и учебным планом. Зачет является формой контроля усвоения студентом учебной программы по дисциплине или ее части, выполнения практических, контрольных, реферативных работ.

Результат сдачи зачета по прослушанному курсу должны оцениваться как итог деятельности студента в семестре, а именно - по посещаемости лекций, результатам работы на практических занятиях, выполнения самостоятельной работы. При этом допускается на очной форме обучения пропуск не более 20% занятий, с обязательной отработкой пропущенных занятий. Студенты у которых количество пропусков, превышает установленную норму, не выполнившие все виды работ и неудовлетворительно работавшие в течение семестра, проходят собеседование с преподавателем, который опрашивает студента на предмет выявления знания основных положений дисциплины.

Для получения положительной оценки зачёта по итогам семестра необходимо минимум выполнение следующих условий: выполнение и успешная защита всех лабораторных работ, а так же посещение 80% лекционных и лабораторных занятий.

Решение о зачете принимается исходя из того, что студент должен был освоить теорию гораздо шире, нежели контролируют эти вопросы тестов, задачи, а так же конфигурирование сети, а экзаменатор руководствуется «положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся в КубГУ».

Оценка «зачтено» выставляется студенту, если от твёрдо знаетматериал, грамотно и по существу излагает его, не допуская существенныхнеточностей, умеет подтвердить теоретические положения примерами изпрактики.

Оценка «не зачтено» выставляется студенту, если он не имеетпредставления о содержании программного материала, либо допускаетсущественные ошибки в изложении материала, не может подтвердитьтеоретические положения примерами.

Студент очной формы обучения к зачету должен выполнить изащитить все лабораторные работы.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине

может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного

документа. Для лиц с

нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).

5.1. Основная литература:

1. Кнауб, Л.В. Теоретико-численные методы в криптографии : учебное пособие / Л.В. Кнауб, Е.А. Новиков, Ю.А. Шитов ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=229582.

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах
«Лань» и «Юрайт».

5.2. Дополнительная литература:

1. Фороузан, Б.А. Математика криптографии и теория шифрования / Б.А. Фороузан. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 511 с. : ил., схем. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 978-5-9963-0242-0 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428998.
2. Гультяева, Т.А. Основы теории информации и криптографии : конспект лекций / Т.А. Гультяева ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2010. - 88 с. : табл., схем. - ISBN 978-5-7782-1425-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=228963
3. Басалова, Г.В. Основы криптографии : курс лекций / Г.В. Басалова ; Национальный Открытый Университет "ИНТУИТ". - Москва : Интернет-Университет Информационных Технологий, 2011. - 253 с. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=233689

6. Перечень ресурсов информационно-телекоммуникационной сети

«Интернет», необходимых для освоения дисциплины (модуля).

1. Современное образование . – URL: https://www.bilim.expert/

2. Центр современного образования. – URL: http://dpocso.ru/mezhregionalnyy-zhurnal-sovremenno

7. Методические указания для обучающихся по освоению дисциплины (модуля).

Рефераты

Реферат предполагает осмысленное изложение содержания наиболее важного и интересного, с точки зрения автора, по предложенной теме. Объем около 20 страниц, традиционная трехчастная структура. Обязательно наличие библиографического списка, оформленного по ГОСТу.

Во введении обосновывается актуальность выбранной темы, формулируются цели работы и основные вопросы, которые предполагается раскрыть в реферате, указываются используемые материалы и дается их краткая характеристика с точки зрения полноты освещения избранной темы. Объем введения не должен превышать1–1,5 страницы.

Основная часть реферата может быть представлена одной или несколькими главами, которые могут включать 2–3 параграфа (подпункта, раздела).

Здесь достаточно полно и логично излагаются главные положения в используемых источниках, раскрываются все пункты плана с сохранением связи между ними и последовательности перехода от одного к другому. Материал в реферате рекомендуется излагать своими словами, не допуская дословного переписывания из литературных источников. В тексте обязательны ссылки на первоисточники. Работа должна быть литературным языком.

Заключение. В этой части обобщается изложенный в основной части материал, формулируются общие выводы с учетом опубликованных в литературе различных точек зрения по проблеме, рассматриваемой в реферате, сопоставления их и личного мнения автора реферата. Заключение по объему не должно превышать 1,5– 2 страниц.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю).

8.1 Перечень информационных технологий.

– Проверка домашних заданий и консультирование посредством электронной почты.

– Использование электронных презентаций при проведении лекционных и практических занятий.

8.2 Перечень необходимого программного обеспечения.

– Программы для демонстрации аудио- и видеоматериалов (проигрыватель «Windows Media Player»).

– Программы для демонстрации и создания презентаций («Microsoft Power Point»).

– Программы для работы с текстом (Microsoft Office (Excel, Word, Access), ABBYY Finereader, AdobeReader).

– Программы-переводчики и электронные словари (ABBYY Lingvo).

– Программы-антивирусы (ESET NOD Antivirus).

– Лицензионное программное обеспечение (Microsoft Windows).

– Программы для доступа в Интернет (Internet Explorer).

8.3Перечень информационных справочных систем:

1. Справочно-правовая система «Консультант Плюс» (http://www.consultant.ru)
2. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)/

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Учебные аудитории для проведения лекционных занятий – ауд. 213, корп. С, вычислительный центр (ул. Ставропольская, 149)
2.	Семинарские занятия	Учебные аудитории для проведения семинарских занятий– ауд. 213, корп. С, вычислительный центр (ул. Ставропольская, 149)
3.	Самостоятельная работа	Аудитория для самостоятельной работы – ауд. 208, корп. С (ул. Ставропольская, 149)

Рецензия

на рабочую программу дисциплины
ФТД.В.02 «Современная криптография»
по направлению подготовки 09.04.02 «Информационные системы и технологии»
(очной формы обучения)

Рабочая программа ФТД.В.02 «Современная криптография» по направлению подготовки 09.04.02 «Информационные системы и технологии» предполагает распределение тем и изучение материала по разделам:

Основы теории чисел
Числовые сравнения
Симметричные и ассиметричные шифры
Методы взлома шифров
Современные симметричные криптосистемы
Отечественный стандарт шифрования данных ГОСТ
Цифровая подпись

Рабочая программа включает разделы:

- цели и задач дисциплины;
- место дисциплины в структуре основной образовательной программы;
- общую трудоемкость дисциплины;
- результаты обучения представлены формируемыми компетенциями;
- образовательные технологии;
- формы промежуточной аттестации;
- содержание дисциплины и учебно-тематический план;
- перечень практических навыков;
- учебно-методическое, информационное и материально-техническое обеспечение дисциплины.

В рабочей программе дисциплины ФТД.В.02 «Современная криптография» по направлению подготовки 09.04.02 «Информационные системы и технологии» указаны примеры оценочных средств для контроля уровня сформированности компетенций; критерии оценки текущего и рубежного контроля. Особый интерес представляют темы: идентификация и проверка подлинности, взаимная проверка подлинности пользователей.

Образовательные технологии обучения представлены по видам учебной работы, характеризуются не только общепринятыми формами (лекции, практическое и лабораторные занятия, семинары), но и интерактивными формами, такими как *участие в научно-практических конференциях, проведение предметных олимпиад и т.д.*

Учебно-методическое и информационное обеспечение содержит перечень основной и дополнительной литературы, программного обеспечения и Интернет-ресурсы.

Материально-техническое обеспечение всех видов учебной работы дисциплины (модуля, практики) отвечают требованиям ФГОС.

Таким образом, рабочая программа дисциплины полностью соответствует ФГОС ВО по направлению подготовки (профиль) 09.04.02 «Информационные системы и технологии» (Информационные системы и технологии) и может быть использована в учебном процессе ФГБОУ ВО «Кубанский государственный университет».

Разработчик РПД: Тумаев Е.Н. док. физ.-мат. наук, профессор кафедры теоретической физики и компьютерных технологий

Заведующий кафедрой физики
и информационных систем
доктор физ.-мат. наук, профессор Богатов Н.М.

Рецензия

на рабочую программу дисциплины
ФТД.В.02 «СОВРЕМЕННАЯ КРИПТОГРАФИЯ»
для магистрантов направления
09.04.02 Информационные системы и технологии
(квалификация «Магистр»)

Факультативная дисциплина «Современная криптография» изучается магистрантами в десятом семестре (семестр А) пятого года обучения, относится к вариативной части блока дисциплин основной образовательной программы, предусматривает получение навыков по анализу стойкости алгоритмов шифрования, разработки надежных протоколов защищенной передачи данных.

Программа в частности содержит следующие разделы:

1. Основы теории чисел.
2. Числовые сравнения.
3. Симметричные и ассиметричные шифры.
4. Методы взлома шифров.
5. Современные симметричные криптосистемы.
6. Отечественный стандарт шифрования данных ГОСТ.
7. Цифровая подпись.

Программой предусмотрено использование современных образовательных технологий, которые необходимо применить во время изучения дисциплины.

В результате магистрант освоит следующие компетенции:

- умением проводить разработку и исследование теоретических и экспериментальных моделей объектов профессиональной деятельности в областях: машиностроение, приборостроение, наука, техника, образование, медицина, административное управление, юриспруденция, бизнес, предпринимательство, коммерция, менеджмент, банковские системы, безопасность информационных систем, управление технологическими процессами, механика, техническая физика, энергетика, ядерная энергетика, силовая электроника, металлургия, строительство, транспорт, железнодорожный транспорт, связь, телекоммуникации, управление инфокоммуникациями, почтовая связь, химическая промышленность, сельское хозяйство, текстильная и легкая промышленность, пищевая промышленность, медицинские и биотехнологии, горное дело, обеспечение безопасности подземных предприятий и производств, геология, нефтегазовая отрасль, геодезия и картография, геоинформационные системы, лесной комплекс, химико-лесной комплекс, экология, сфера сервиса, системы массовой информации, дизайн, медиаиндустрия, а также предприятия различного профиля и все виды деятельности в условиях экономики информационного общества (ПК-8);
- способностью прогнозировать развитие информационных систем и технологий (ПК-13).

Результаты рецензирования рабочей программы показали, что дисциплина ФТД.В.02 «Современная криптография» ООП ВО по направлению 09.04.02 Информационные системы и технологии, разработанная доктором физико-математических наук, профессором кафедры теоретической физики и компьютерных технологий физико-технического факультета ФГБОУ ВО «КубГУ» Тумаевым Евгением Николаевичем, полностью соответствует образовательному стандарту.

Генеральный директор ООО "КПК"
кандидат пед. наук Ю.А. Половодов