Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кубанский государственный университет»
(ФГБОУ ВО «КубГУ»)

Физико-технический факультет

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Хагуров Т.А.
подпись
«27» апреля 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ФТД.В.01 МЕТОДЫ КРИПТОГРАФИИ И ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки 09.03.02 Информационные системы и технологии

Направленность (профиль) Информационные системы и технологии

Программа подготовки академический бакалавриат

Форма обучения очная

Квалификация (степень) выпускника бакалавр

Краснодар 2018

Рабочая программа дисциплины «Методы криптографии и защиты информации» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 09.03.02 Информационные системы и технологии.

Программу составил:
Е. Н. Тумаев, профессор кафедры
теоретической физики и компьютерных
технологий, д. ф.-м. наук, доцент


подпись

Рабочая программа дисциплины «Методы криптографии и защиты информации» утверждена на заседании кафедры теоретической физики и компьютерных технологий
протокол № 9 «29» марта 2018 г.
Заведующий кафедрой (разработчика) Исаев В.А.


подпись

Рабочая программа обсуждена на заседании кафедры теоретической физики и компьютерных технологий
протокол № 9 «29» марта 2018 г.
Заведующий кафедрой (выпускающей) Исаев В.А.


подпись

Утверждена на заседании учебно-методической комиссии физико-технического факультета
протокол № 10 «12» апреля 2018г.
Председатель УМК факультета Богатов Н.М.


подпись

Рецензенты:

Богатов Н.М., доктор физико-математических наук, профессор, заведующий кафедрой физики и информационных систем КубГУ

Половодов Ю.А., кандидат педагогических наук, генеральный директор ООО «КПК»

Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины – подготовка обучающихся посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС ВО, в части представленных ниже знаний, умений и навыков.

1.2 Задачи дисциплины:

1. изучение понятийного аппарата дисциплины, основных теоретических положений и методов
2. формирование умений и привитие навыков применения теоретических знаний для решения практических и прикладных задач

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Методы криптографии и защиты информации» относится к вариативной части факультативного блока учебного плана.

Дисциплина «Методы криптографии и защиты информации» 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 «Основы теории кодирования», «Управление данными», «Теория информационных процессов и систем».

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-25	способностью использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований	основные методы шифрования в области защиты информации	использовать математические методы обработки и средства защиты информации	навыками построения систем защиты информации
2.	ПК-28	способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию	теоретические основы инсталляции и настройки программных и технических средств	организовывать ввод информационных систем в опытную и промышленную эксплуатацию	навыками инсталляции, отладки программных и настройке технических средств для ввода информационных систем в

					опытную и промышленную эксплуатацию
3.	ПК-34	способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию	теоретические основы инсталляции и настройки программных и технических средств	организовывать ввод информационных систем в опытную и промышленную эксплуатацию	навыками инсталляции, отладки программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 1 зач.ед. (36 ч.), их распределение по видам работ представлено в таблице *(для студентов ОФО)*.

Вид учебной работы		Всего часов	Семестры (часы)			
			7			
Контактная работа, в том числе:						
Аудиторные занятия (всего):		**16**	**16**			
Занятия лекционного типа		-	-	-	-	-
Занятия семинарского типа (семинары, практические занятия)		16	16	-	-	-
Иная контактная работа:						
Контроль самостоятельной работы(КСР)						
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:		**19,8**	**19,8**			
Проработка учебного (теоретического) материала		10	10	-	-	-
Реферат		9,8	9,8	-	-	-
Подготовка к зачету		-	-	-	-	-
Общая трудоемкость	**час.**	**36**	**36**	**-**	**-**	**-**
	в том числе контактная работа	16,2	16,2			
	зач. ед	**1**	**1**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины.

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Вне аудиторная работа
			Л	ПЗ	ЛР	СРС

1	2	3	4	5	6	7
1.	Основы теории чисел	4	-	2	-	2
2.	Числовые сравнения	5	-	2	-	3
3.	Симметричные и ассиметричные шифры	5	-	2	-	3
4.	Методы взлома шифров	5	-	2	-	3
5.	Современные симметричные криптосистемы	5	-	2	-	3
6.	Отечественный стандарт шифрования данных ГОСТ	6	-	3	-	3
7.	Цифровая подпись	5,8	-	3	-	2,8
	Итого по дисциплине:	35,8	-	16	-	19,8

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

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

Не предусмотрены

2.3.2 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.	Опрос
3.	Симметричные и ассиметричные шифры	Основные понятия и определения. Шифры перестановки: шифр перестановки «скитала», шифрующие таблицы, применение магических квадратов.	Тест
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.	Реферат
6.	Отечественный стандарт шифрования данных ГОСТ	режим простой замены, режим гаммирования, режим гаммирования с обратной связью, режим выработки имитовставки.	Тест
7.	Цифровая подпись	Идентификация и проверка подлинности. Взаимная проверка подлинности пользователей	Опрос

2.3.3 Лабораторные занятия.

Не предусмотрены

2.3.4 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	Проработка учебного (теоретического) материала	Методические указания по организации аудиторной и самостоятельной работ, утвержденные кафедрой теоретической физики и компьютерных технологий, протокол № 9 от «14» марта 2017г
2	Реферат	1.Методические рекомендации по написанию реферата, утвержденные кафедрой теоретической физики и компьютерных технологий, протокол № 9 от «14» марта 2017г. 2.Бушенева Ю.И. Как правильно написать реферат, курсовую и дипломную работы: Учебное пособие для бакалавров [Электронный ресурс]: учеб. пособие – Электрон. дан. – М.: Дашков и К, 2016. – 140 с. Режим доступа: https://e.lanbook.com/book/93331
3	Подготовка к текущему контролю	Методические рекомендации для подготовки к практическим, семинарским и лабораторным занятиям, утвержденные кафедрой теоретической физики и компьютерных технологий, протокол № 9 от «14» марта 2017г.

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 «Современные проблемы науки и производства» для реализациии 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 промежуточной аттестации.

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 криптографии.

Разное

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.

Фонд оценочных средств для проведения промежуточной аттестации.

Вопросы к зачету

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).

Изучение дисциплины завершается зачетом, который проводится в форме устного опроса по вопросам.

С целью контроля и подготовки студентов к изучению новой темы вначале каждого практического занятия преподавателем проводится индивидуальный или фронтальный устный опрос по выполненным заданиям предыдущей темы.

Критерии оценки:

– правильность ответа по содержанию задания (учитывается количество и характер ошибок при ответе);

– полнота и глубина ответа (учитывается количество усвоенных фактов, понятий и т.п.);

– сознательность ответа (учитывается понимание излагаемого материала);

– логика изложения материала (учитывается умение строить целостный, последовательный рассказ, грамотно пользоваться специальной терминологией);

– рациональность использованных приемов и способов решенияпоставленной учебной задачи (учитывается умение использовать наиболее прогрессивные и эффективные способы достижения цели);

– своевременность и эффективность использования наглядных пособий итехнических средств при ответе (учитывается грамотно и с пользой применять наглядность и демонстрационный опыт при устном ответе);

– использование дополнительного материала (обязательное условие);

– рациональность использования времени, отведенного на задание (не одобряется затянутость выполнения задания, устного ответа во времени, с учетом индивидуальных особенностей студентов).

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. Васильева, И.Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата / И. Н. Васильева. - Москва : Юрайт, 2017. - 349 с. [Электронный ресурс]. - URL: - https://www.biblio-online.ru/book/59BABD78-5536-4ED4-BB9D-55E2F19F80B2.

2. Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М. : Издательство Юрайт, 2018. — 473 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-01530-0. [Электронный ресурс]. - URL: - https://biblio-online.ru/book/27397D56-C8A1-4970-9F39-28E7FA40632A/

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:

Рябко, Б.Я. Криптографические методы защиты информации [Электронный ресурс] : учеб. пособие / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 229 с. — Режим доступа: https://e.lanbook.com/book/5193

6. **Перечень ресурсов информационно-телекоммуникационной сети «Интернет», в том числе современные профессиональные базы данных и информационные справочные системы, необходимые для освоения дисциплины (модуля).**

1. БД Web of Science - главный ресурс для исследователей по поиску и анализу научной литературы, охватывающей около 18000 научных журналов со всего мира. База данных международных индексов научного цитирования http://webofscience.com/
2. zbMATH - полная математическая база данных. Охватывает материалы с конца 19 века. zbMATH содержит около 4000000 документов из более 3000 журналов и 170000 книг по математике, статистике, информатике. https://zbmath.org/
3. БД Kaggle - это платформа для сбора и обработки данных. Является он-лайн площадкой для научного моделирования. https://www.kaggle.com/
4. База данных Научной электронный библиотеки eLIBRARY.RU https://elibrary.ru/
5. База данных Всероссийского института научной и технической информации (ВИНИТИ) РАН http://www2.viniti.ru/
6. «ЭЛЕКТРОННАЯ БИБЛИОТЕКА ДИССЕРТАЦИЙ» Российской Государственной Библиотеки (РГБ) – в настоящее время ЭБД содержит более 800 000 полных текстов диссертаций. https://dvs.rsl.ru
7. Портал открытых данных Российской Федерерации https://data.gov.ru
8. База открытых данных Министерства труда и социальной защиты РФ https://rosmintrud.ru/opendata
9. Федеральный портал единое окно доступа к информационным ресурсам - http://window.edu.ru/
10. Российский фонд фундаментальных исследований предоставляет доступ к информационным наукометрическим базам данных и полнотекстовым научным ресурсами издательств Springer Nature и Elsevier - http://www.rfbr.ru/rffi/ru
11. Федеральный портал "Информационно-коммуникационные технологии в образовании" - http://www.ict.edu.ru/
12. «Лекториум ТВ» – видеолекции ведущих лекторов России. Лекториум – on-line – библиотека, где ВУЗы и известные лектории России презентуют своих лучших лекторов. Доступ к материалам свободный и бесплатный - http://www.lektorium.tv.

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 лицензионного 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).

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

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран) (ауд. 212С, 213С)
2.	Семинарские занятия	Специальное помещение, оснащенное презентационной техникой (проектор, экран) (ауд. 212С, 213С). Компьютерный класс, оборудованный техническими средствами обучения (16 рабочих станций, лаборантская машина и два сервера. Все компьютеры подключены к локальной сети (ауд.212С, 213С))
3.	Текущий контроль, промежуточная аттестация	Аудитория 212С, 213С
4.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета (ауд.212С, 213С)