	Федеральное государственное бюджетное образовательное учреждение высшего образования «Калининградский государственный технический университет» (ФГБОУ ВО «КГТУ») Балтийская государственная академия рыбопромыслового флота (БГАРФ)	
Версия: 1	Рабочая программа дисциплины «Криптографические методы защиты информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем»	стр. 1 из 15

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
Балтийская государственная академия рыбопромыслового флота
ФГБОУ ВО «КГТУ»
БГАРФ

УТВЕРЖДАЮ
И.о. декана РТФ _____ /В.А. Баженов/
27 . марта 2018 г.

Рабочая программа дисциплины

Криптографические методы защиты информации

базовой части образовательной программы
по специальности

10.05.03 Информационная безопасность автоматизированных систем

Специализация программы
«Обеспечение информационной безопасности распределенных информационных систем»

Факультет: Радиотехнический (РТФ)

Кафедра информационной безопасности

Калининград 2018 г.

1. Цель освоения дисциплины.

1.1. Цель изучения дисциплины.

Целью изучения дисциплины «Криптографические методы защиты информации» является освоение студентами основ фундаментальных знаний в области принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

1.2. Задачи изучения дисциплины.

К задачам дисциплины относятся: формирование у обучающихся системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; сформировать умения применять математические методы, используемые в оценке стойкости криптосистем; получить необходимые практические навыки использования типовых криптографических алгоритмов; эффективно использовать отечественные и зарубежные стандарты в области криптографических методов защиты информации в автоматизированных системах.

1.3. Предметом изучения дисциплины являются следующие объекты:
Математический аппарат, применяющийся в криптографии, построение криптографических алгоритмов, современные блочные криптосистемы, стойкость криптосистем, методы синтеза и анализа криптографических алгоритмов.

2. Результаты освоения дисциплины

Таблица 1 - Компетенции, формируемые в результате освоения дисциплины

Коды компетенций	Описание компетенций	Краткое содержание и структура компетенций.
ОПК-1.10	способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач.	**знать:** способы получения новых знаний в предметной области и областях, непосредственно связанных с будущей профессиональной деятельностью; методы и средства познания, связанные с предметной областью: обобщать и систематизировать новые знания в предметной области и выявлять проблемы, используя периодические научные издания, исследовательские сайты в сети Internet; математический аппарат, используемый в своей профессиональной деятельности. **уметь:** самостоятельно получать новые знания по предметной области и в областях, непосредственно примыкающих к объектам будущей профессиональной деятельности; самостоятельно получать знания из смежных областей науки и техники: углублять знания, уточнять по признакам понятий, отделять существенные признаки от несущественных; уточнять гра-

		ницы использования знаний. **владеть:** программными средствами, позволяющими осуществлять формализацию и анализ предметной области; элементами математического аппарата, позволяющими делать вычисления в предметной области.
ОПК-5.3	способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами.	**знать:** направления инновационных решений в области математических методов защиты информации; критерии и показатели инновационных решений в предметной области. **уметь:** классифицировать по степени важности инновационные решения в предметной деятельности; систематизировать показатели эффективности инновационных решений в предметной области. **владеть:** программными средствами, позволяющими делать вычисления в предметной области, основными способами решения прикладных задач; критериями решений задач в предметной области.
ПК-1.12	способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке.	**знать:** классификацию и характеристики информационных баз и хранилищ; информационные базы и хранилища, порядок обращения к ним и поиска информации. **уметь:** определить пути получения научно-технической информации, обобщать и систематизировать информацию; использовать ресурсы информационных баз и хранилищ для поиска, систематизации и обобщения материала в предметной области дисциплины. **владеть:** навыками систематизации, обобщения справочной, нормативно-технической информации; навыками поиска, обобщения, систематизации научно-технической информации, составления кратких отчетов, рефератов.

ПК-13.3	способностью участвовать в проектировании средств защиты информации автоматизированной системы.	**знать:** основные задачи и понятия криптографии; частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки. **уметь:** работать в специализированном ПО, анализировать результаты исследований; анализировать проекты средств защиты информации. **владеть:** навыками использования типовых криптографических алгоритмов; навыками использования ПЭВМ в анализе простейших шифров.
ПК-14.2	способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации.	**знать:** требования к шифрам и основные характеристики шифров; принципы разработки современных блочных и поточных криптосистем. **уметь:** определять работоспособность криптографических средств; использовать отечественные и зарубежные стандарты в области криптографических методов защиты информации в автоматизированных системах. **владеть:** навыками использования ПЭВМ в анализе простейших шифров; статистическими методами анализа криптосистем.

Таблица 2 - Этапы формирования компетенций

Коды компетенций	Этапы формирования компетенций (разделы программы)
ОПК-1.10	Введение в криптографию. Основные классы шифров и их свойства. Методы синтеза и анализа криптографических алгоритмов с секретным ключом. Надежность шифров. Хеш-функции и их криптографические приложения. Методы синтеза и анализа криптографических алгоритмов с открытым ключом.
ОПК-5.3	Методы синтеза и анализа криптографических алгоритмов с секретным ключом. Надежность шифров. Хеш-функции и их криптографические приложения. Методы синтеза и анализа криптографических алгоритмов с открытым ключом.
ПК-1.12	Введение в криптографию. Основные классы шифров и их свой-

	ства. Методы синтеза и анализа криптографических алгоритмов с секретным ключом. Надежность шифров. Хеш-функции и их криптографические приложения. Методы синтеза и анализа криптографических алгоритмов с открытым ключом.
ПК-13.3	Методы синтеза и анализа криптографических алгоритмов с секретным ключом. Надежность шифров. Хеш-функции и их криптографические приложения. Методы синтеза и анализа криптографических алгоритмов с открытым ключом.
ПК-14.2	Основные классы шифров и их свойства. Методы синтеза и анализа криптографических алгоритмов с секретным ключом. Надежность шифров. Хеш-функции и их криптографические приложения. Методы синтеза и анализа криптографических алгоритмов с открытым ключом.

Таблица 3 - Результаты обучения по дисциплине

В результате изучения дисциплины студент должен:	Результаты
знать	основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифрсистемы, асимметричные криптосистемы; модели шифров и математические методы их исследования; криптографические стандарты и их использование в информационных системах;
уметь	эффективно использовать отечественные и зарубежные стандарты в области криптографических методов защиты информации в автоматизированных системах; применять математические методы исследования моделей шифров;
владеть	криптографической терминологией; навыками использования типовых криптографических алгоритмов; навыками использования ПЭВМ при анализе простейших шифров; навыками математического моделирования в криптографии; знаниями из научно-технической литературы в области криптографической защиты.

3. Место дисциплины в структуре образовательной программы

Место дисциплины в структуре ООП специалитета:

Б1.Б.25 Базовая часть. Изучение дисциплины производится в тесной взаимосвязи с базовыми и вариативными математическими и естественнонаучными дисциплинами.

Требования к предварительной подготовке обучающегося:

Для успешного освоения дисциплины студент должен иметь базовую подготовку по основным разделам математического анализа (дифференциальное, интегральное исчисление), ал-

гебры и геометрии (линейная алгебра, аналитическая геометрия), информатики, языкам программирования, теории вероятностей и математической статистики, теории информации.

Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее:

Б1.Б.30 Программно-аппаратные средства обеспечения информационной безопасности,

Б1.Б.34 Информационная безопасность распределенных информационных систем.

4. Содержание дисциплины

Тема 1. Арифметика целых чисел. Модульная арифметика. Система вычетов Z_n. Арифметика целых чисел. Множество целых чисел. Бинарные операции. Простой и расширенный алгоритм Евклида. Вычисление наибольшего общего делителя. Модульная арифметика. Операции по модулю. Система вычетов Z_n. Сравнения в модульной арифметике. Операции в системе вычетов Z_n. Аддитивная и мультипликативная инверсии.

Тема 2. Алгебраические структуры. Группы, кольца, поля. Алгебраические структуры. Группа. Циклические подгруппы. Циклические группы. Кольцо. Поле. Поля $GF(p^n)$.

Тема 3. Понятие шифрования. Шифры подстановки. Понятие шифрования. Криптоанализ. Моноалфавитные шифры. Аддитивный шифр. Мультипликативные шифры. Многоалфавитные шифры. Автоключевой шифр. Шифр Плейфера. Шифр Виженера. Шифр Хилла. Одноразовый блокнот. Роторный шифр.

Тема 4. Ключевые и бесключевые шифры перестановки. Бесключевые шифры перестановки. Ключевые шифры перестановки. Шифр изгороди. Шифр вертикальной перестановки.

Тема 5. Блочный шифр DES. Современные блочные шифры. Подстановка или транспозиция. Блочный шифр и его компоненты. Рассеивание и перемешивание. Составные шифры. Структура DES. Функция DES. Генерация ключей. Слабость в ключе шифра. Многократное применение DES.

Тема 6. Алгоритмы с открытыми ключами. Общие положения криптосистем с открытым ключом. Алгоритм RSA. Однонаправленные хэш-функции. Подпись документа с помощью симметричных криптосистем и посредника. Деревья цифровых подписей. Алгоритм рюкзака. Алгоритм Диффи-Хеллмана. Алгоритм Диффи-Хеллмана на эллиптических кривых ECDH. Сложение точек на эллиптических кривых. Генерация ключа в ECDH. Электронная цифровая подпись. Алгоритм Эль-Гамаля. Алгоритм Эль-Гамаля на эллиптических кривых.

5. Объем (трудоемкость освоения) и структура дисциплины, формы аттестации

Таблица 1 - Объем (трудоемкость освоения) и структура дисциплины, формы аттестации **для очной формы обучения**

Семестр - седьмой (216 час, 6 ЗЕТ).						
Номер и наименование разделов и тем	Объем учебной работы (час.)					
	Лекции	ЛЗ	ПЗ	СРС	Контроль	Всего
Тема 1. Арифметика целых чисел. Модульная арифметика. Система	4	6		6	2	18

вычетов Z_n.						
Тема 2. Алгебраические структуры. Группы, кольца, поля.	6	6		16	8	36
Тема 3. Понятие шифрования. Шифры подстановки.	8	8		14	8	38
Тема 4. Ключевые и бесключевые шифры перестановки.	8	6		12	4	30
Тема 5. Блочный шифр DES.	6	6		14	6	32
Тема 6. Алгоритмы с открытыми ключами.	19	19		16	8	62
Форма аттестации	**Экзамен**					
Всего за семестр:	51	51		78	36	216
Итого по дисциплине	51	51		78	36	216

ЛЗ – лабораторные занятия,
ПЗ – практические занятия,
СРС – самостоятельная работа студента,
КР – курсовая работа,
КП – курсовой проект.

6. Лабораторные занятия (работы)

Таблица 2 - Лабораторные по **очной форме обучения**

№ ЛЗ	Тема дисциплины	Тема и содержание ЛЗ	Кол-во часов ЛЗ
Семестр – седьмой (51 час.).			
1.	**Тема 1.**	Простой и расширенный алгоритм Евклида. Модульная арифметика. Операции в системе вычетов Z_n. Аддитивная и мультипликативная инверсии.	6
2.	**Тема 2.**	Алгебраические структуры. Группа. Циклические подгруппы. Циклические группы. Кольцо. Поле. Поля $GF(p^n)$.	6
3.	**Тема 3.**	Моноалфавитные шифры. Аддитивный, мультипликативный, аффинный шифры. Автоключевой шифр. Шифр Плейфера. Шифр Виженера. Шифр Хилла.	8
4.	**Тема 4.**	Бесключевые шифры перестановки. Ключевые шифры перестановки. Шифр изгороди. Шифр вертикальной перестановки.	6
5.	**Тема 5**.	Пример шифрования с помощью симметричного алгоритма DES.	6

6.	**Тема 6.**	Алгоритм RSA. Алгоритм рюкзака. Алгоритм Диффи-Хеллмана. Алгоритм Диффи-Хеллмана на эллиптических кривых ECDH. Сложение точек на эллиптических кривых. Генерация ключа в ECDH. Электронная цифровая подпись. Алгоритм Эль-Гамаля. Алгоритм Эль-Гамаля на эллиптических кривых.	19
Всего за семестр:			51
Итого по дисциплине			51

7. Практические занятия

Практические занятия по дисциплине учебным планом не предусмотрены.

8. Самостоятельная работа студента

Таблица 3 - Самостоятельная работа студента по **очной форме обучения**

№	Вид (содержание) СРС	Кол-во часов СРС	Форма контроля, аттестации
Семестр – седьмой (78 час.)			
1.	Исторический обзор. Открытые сообщения и их характеристики. Основные задачи и понятия криптографии. Классические ручные шифрсистемы: шифры простой замены, многоалфавитные шифры. Статистические критерии проверки однородности распределений выборок (построение критериев распознавания открытых сообщений). Математическая модель шифра.	6	Текущий опрос, тестирование
2.	Криптоанализ шифра одноалфавитной замены (подготовка к лабораторной работе). Многоалфавитные шифры: диск Альберти, шифр Тритемия, шифр Виженера. Арифметические операции в кольце вычетов Zn. Вычисление обратных элементов. Шифр гаммирования (подготовка к лабораторной работе). Шифры перестановки. Маршрутные перестановки. Повторение раздела алгебры «Матрицы над кольцами вычетов» (подготовка к лабораторной работе). Вычисления обратных матриц в кольце вычетов Zn и определение ключа расшифрова-	16	

	ния для шифра Хилла.		
3.	Принципы построения криптографических алгоритмов. Стандарты блочного шифрования. Режимы шифрования. Линейные рекуррентные последовательности (повторение соответствующего раздела дисциплины «Алгебра»). Методы усложнения линейных рекуррентных последовательностей (работа с лекционным материалом). Методы анализа криптографических алгоритмов.	14	
4.	Теоретическая и практическая стойкость криптосистем. Методика расчета расстояния единственности для шифра простой замены. Имитозащита и шифры не распространяющие искажения.	12	
5.	Криптографические функции хеширования. Конструкции схем аутентификации на основе хеш-функций.	14	
6.	Алгоритмы шифрования: Шамира, RSA, Эль-Гамаля. Алгоритм цифровой подписи ГОСТ Р 34.10-94. Протоколы с нулевым разглашением. Криптографические протоколы распределения ключей.	16	
Всего за семестр		78	
Итого по дисциплине		78	

9. Учебная литература и учебно-методическое обеспечение самостоятельной работы студента

Таблица 4. Основная учебная литература

№ п/п	Автор(ы)	Заглавие	Город, издательство, год издания,
1.	Алферов А. П.	Основы криптографии. Учебное пособие.	– М.: Гелиос АРВ, 2005. 15 экземпляров.
2.	Молдовян Н. А., Молдовян А. А., Еремеев М. А.	Криптография. От примитивов к синтезу алгоритмов. Практическое пособие.	– СПБ.: БХВ-Петербург, 2004. 2 экземпляра.

3.	Рябко Б. Я.	Криптографические методы защиты информации. Учебное пособие.	– М.: Горячая линия - Телеком, 2005. 15 экземпляров.
4.	Никифоров С.Н.	Методы защиты информации. Шифрование данных. Учебное пособие.	– Санкт-Петербург: Лань, 2018. ЭВ.
5.	Воробейкина И.В.	Криптографические методы защиты информации: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем»	– Калининград: Изд-во БГАРФ, 2018. 27 экземпляров.+ ЭВ.

Таблица 5. Дополнительная учебная литература

№ п/п	Автор(ы)	Заглавие	Город, издательство, год издания, кол-во стр.
1.	Романьков В. А.	Введение в криптографию. Курс лекций.	– М.: Форум, 2012. 3 экземпляра.
2.	Зубов А. Ю.	Криптографические методы защиты информации. Совершенные шифры. Учебное пособие.	– М.: Гелиос АРВ, 2005. 1 экземпляр.
3.	Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В.	Введение в теоретико-числовые методы криптографии. Учебное пособие.	– Санкт-Петербург: Лань, 2011. ЭВ.

10. Информационные технологии, программное обеспечение и Интернет-ресурсы дисциплины

Электронная информационная образовательная среда БГАРФ ФГБОУ ВО «КГТУ»: http://83.171.112.16/login/index.php

Интернет-ресурсы

Интернет-ресурсы, применяемые при изучении:

1. http://www.intuit.ru/
2. ЭБС БГАРФ **http://bgarf.ru/academy/biblioteka/elektronnyj-katalog**
3. ЭБС «Лань» **https://e.lanbook.com/**

11. Материально-техническое обеспечение дисциплины

11.1. Общие требования к материально-техническому обеспечению дисциплины

11.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения лекционных занятий используется учебная аудитория № 441.

Состав оборудования: столы учебные – 15 шт., стол преподавательский – 1 шт., стулья учебные – 30 шт., стул преподавательский – 1 шт., трибуна – 1 шт., экран раздвижной PROJECTA – 1 шт.; доска магнитно-маркерная – 1 шт.; мультимедийный проектор TOSHIBA – 1 шт.; ноутбук Acer Extensa – 1 шт.

Стенды: «Комплекс средств автоматизации деятельности оперативного персонала пункта централизованной охраны», «Требования и нормы проектирования по защите объектов от преступных посягательств». Специализированные стенды: СКУД «Стилпост»; «СИНЕРГЕТ» (цифровая система видеонаблюдения и аудиорегистрации).

11.1.2. Материально-техническое обеспечение для лабораторных занятий

Для проведения лабораторных занятий используется лаборатория технической защиты информации № 439.

Состав оборудования: столы учебные – 10 шт., стол преподавательский – 1 шт., стулья учебные – 20 шт., стул преподавательский – 1 шт., доска маркерная – 1 шт.; мультимедийный проектор TOSHIBA – 1 шт.; ноутбук Acer Extensa – 1 шт.

Стенды охранно-пожарной сигнализации – 3 шт.

Стенды со специализированным оборудованием по защите информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок и контроля эффективности защиты (подавитель микрофонов «Шаман», детектор поля ST 007, портативный измеритель частоты и мощности MPF-8000).

Для проведения лабораторных занятий используются компьютерный класс № 248.

Состав оборудования: столы учебные – 19 шт., стол преподавательский – 1 шт., стулья учебные – 23 шт., стул преподавательский – 1 шт., шкаф для учебных пособий – 1 шт., доска маркерная – 1 шт.; мультимедийный проектор ViewSonic – 1 шт.; ноутбук Acer Extensa – 1 шт.; проекционный экран Redleaf – 1 шт.

Компьютер MUSTIFF (системный блок, монитор ASUS, мышка, клавиатура), с установленным лицензионным программным обеспечением: Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription, Kaspersky Total Space Security Russian Edition.

11.1.3. Материально-техническое обеспечение для самостоятельной работы

Для организации самостоятельной работы обучающихся используется библиотечный фонд вуза, библиотека.

Помещение для самостоятельной работы – читальный зал, оснащенный компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду вуза.

11.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов с нарушениями слуха предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов с нарушениями зрениями предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов с нарушениями опорно-двигательного аппарата используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

12. Фонд оценочных средств для проведения аттестации по дисциплине.

Аттестация по дисциплине (итоговая аттестация по дисциплине является промежуточной аттестацией по образовательной программе). Для рабочей программы разработано и утверждено приложение «Фонд оценочных средств для аттестации по дисциплине «Криптографические методы защиты информации».

13. Особенности преподавания и освоения дисциплины

13.1 Под образовательными технологиями будем понимать пути и способы формирования компетенций. В рамках дисциплины предусмотрены:

- лекции;
- лабораторные занятия, во время которых отрабатываются практические навыки, обсуждаются вопросы лекций, домашних заданий, проводятся контрольные и самостоятельные работы и т.д.;
- самостоятельная работа студентов, включающая усвоение теоретического материала, подготовку к практическим занятиям, выполнение индивидуальных заданий, курсовой работы, работа с учебниками, иной учебной и учебно-методической литературой, подготовка к текущему контролю успеваемости, к экзамену;
- тестирование по отдельным темам дисциплины;
- консультирование студентов по вопросам учебного материала.

13.2 Реализация программы предполагает использование интерактивных форм проведения лабораторных занятий. Проведение лабораторных занятий подразумевает обучение, построенное на групповой совместной деятельности студентов, в том числе с использованием персонального компьютера.

14. Методические указания по освоению дисциплины

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно, ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходит углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

- развивающая (повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);

- информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится малорезультативной);
- ориентирующая и стимулирующая (процессу обучения придается профессиональное ускорение);
- воспитывающая (формируются и развиваются профессиональные качества специалиста):
- исследовательская (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводиться с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений студентов;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

- изучить рекомендуемые литературные источники:
- изучить основные понятия, представленные в глоссарии;
- ответить на контрольные вопросы:
- решить предложенные задачи, кейсы, ситуации;
- выполнить контрольные и курсовые работы.

Работа студентов в основном складывается из следующих элементов:

1. Изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам:
2. Выполнение письменных контрольных и курсовых работ;
3. Подготовка и сдача зачетов, курсовых работ, итоговых экзаменов:
4. Написание и защита дипломной работы.

Самостоятельная работа включает такие формы работы, как:

- индивидуальное занятие (домашние занятия) - важный элемент в работе студента по расширению и закреплению знаний;
- конспектирование лекций;
- получение консультаций для разъяснений по вопросам изучаемой дисциплины;
- подготовка ответов на вопросы тестов;
- подготовка к экзамену;
- выполнение контрольных, курсовых и дипломных работ;
- подготовка научных докладов, рефератов, эссе;
- анализ деловых ситуаций (мини кейсов) и др.

Содержание внеаудиторной самостоятельной работы определяется в соответствии с рекомендуемыми видами заданий в соответствии с рабочей программой учебной дисциплины. Распределение объема времени на внеаудиторную самостоятельную работу в режиме дня студента *не* регламентируется расписанием.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференциальный характер, учитывать специфику специальности, изучаемой дисциплины, индивидуальные особенности студента.

Видами заданий для внеаудиторной самостоятельной работы могут быть:

Для овладения знаниями:

- чтение текста (учебника, первоисточника, дополнительной литературы);
- составление плана текста;
- конспектирование текста;
- выписки из текста;
- работа со словарями и справочниками;
- исследовательская работа;
- использование аудио- и видеозаписи;
- работа с электронными информационными ресурсами и ресурсами Internet:

Для закрепления и систематизации знании:

- работа с конспектом лекции (обработка текста);
- повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудио-видеозаписей):
- составление плана и тезисов ответа;
- выполнение тестовых заданий;
- ответы на контрольные вопросы;
- аннотирование, реферирование, рецензирование текста;
- подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов;
- работа с компьютерными программами;
- подготовка к сдаче экзамена;

Для формирования умений:

- решение задач и упражнений по образцу;
- решение вариативных задач и упражнений:
- выполнение расчетно-графических работ;
- решение ситуационных производственных (профессиональных) задач;
- участие в научных и практических конференциях;
- проектирование и моделирование разных видов и компонентов профессиональной деятельности;
- создание проспектов, проектов, моделей;
- экспериментальная работа, участие в НИР;
- рефлексивный анализ профессиональных умений с использованием аудио- видеотехники и компьютерных расчетных программ и электронных практикумов;
- подготовка курсовых и дипломных работ;

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

	Федеральное государственное бюджетное образовательное учреждение высшего образования «Калининградский государственный технический университет» (ФГБОУ ВО «КГТУ») Балтийская государственная академия рыбопромыслового флота (БГАРФ)	
Версия: 1	Рабочая программа дисциплины «Криптографические методы защиты информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем»	стр. 15 из 15

15. Сведения о рабочей программе и ее согласовании

Рабочая программа дисциплины представляет собой компонент образовательной программы специалитета по специальности подготовки 10.05.03 «Информационная безопасность автоматизированных систем» и соответствует учебному плану, утвержденному «31» января 2018 г. и действующему для студентов, принятых на первый курс, начиная с 2014 года.

Автор программы:
ст. преподаватель кафедры информационной безопасности _____ /И.В.Воробейкина/

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры информационной безопасности
(протокол № 9 от 14 июня 2018 г.)

Зав. кафедрой информационной безопасности _____ /Н.Я. Великите/

Рабочая программа дисциплины рассмотрена и одобрена на заседании методической комиссии радиотехнического факультета
(протокол № 6 от 27 июня 2018 г.)

Председатель методической комиссии _____ / А.Г. Жестовский /