БГАРФ	Федеральное агентство по рыболовству ФГБОУ ВО «Калининградский государственный технический университет» Балтийская государственная академия рыбопромыслового флота (БГАРФ)		
	Фонд оценочных средств		
	Версия: 1	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
«24» июня 2018 г.

Фонд оценочных средств для аттестации по дисциплине
(приложение к рабочей программе 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. Результаты освоения дисциплины.

В результате освоения дисциплины «Криптографические методы защиты информации» обучающийся должен получить следующие компетенции:

Таблица 1. Компетенции и уровни их освоения обучающимся.

ОПК-1.10: способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач.	
Знать:	
Уровень 1	способы получения новых знаний в предметной области и областях, непосредственно связанных с будущей профессиональной деятельностью
Уровень 2	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
Уровень 3	предметы и объекты в областях науки и техники, непосредственно связанных с криптографией и защитой информации
Уметь:	
Уровень 1	самостоятельно получать новые знания по предметной области и в областях, непосредственно примыкающих к объектам будущей профессиональной деятельности
Уровень 2	самостоятельно получать знания из смежных областей науки и техники: углублять знания, уточнять по признакам понятий, отделять существенные признаки от несущественных; уточнять границы использования знаний
Уровень 3	самостоятельно получать знания для решения практических задач защиты конфиденциальной информации; применять математический аппарат предметной области для решения стандартных задач в предметной области
Владеть:	
Уровень 1	программными средствами, позволяющими осуществлять формализацию и анализ предметной области
Уровень 2	элементами математического аппарата, позволяющими делать вычисления в пред-
Уровень 3	физико-математическим аппаратом для выполнения анализа и вычислений предметной области
ОПК-5.3: способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами.	
Знать:	
Уровень 1	направления инновационных решений в области математических методов защиты информации
Уровень 2	критерии и показатели инновационных решений в предметной области
Уровень 3	критерии инновационных проектов, методы и средства научного познания, инструментарий научных исследований в предметной области
Уметь:	

Уровень 1	классифицировать по степени важности инновационные решения в предметной деятельности
Уровень 2	систематизировать показатели эффективности инновационных решений в предметной области
Уровень 3	определять направления междисциплинарных связей в предметной области исследований, использовать физико-математический аппарат для решения поставлен-
Владеть:	
Уровень 1	программными средствами, позволяющими делать вычисления в предметной области, основными способами решения прикладных задач
Уровень 2	критериями решений задач в предметной области
Уровень 3	навыками самостоятельного решения задач для исследования междисциплинарных связей 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:	
Уровень 1	классификацию и характеристики информационных баз и хранилищ
Уровень 2	информационные базы и хранилища, порядок обращения к ним и поиска информации
Уровень 3	порядок обработки патентной информации, информации по интеллектуальной собственности
Уметь:	
Уровень 1	определить пути получения научно-технической информации, обобщать и систематизировать информацию
Уровень 2	использовать ресурсы информационных баз и хранилищ для поиска, систематизации и обобщения материала в предметной области дисциплины
Уровень 3	проводить патентный поиск по ключевым словам, выявлять аналоги и прототипы, обобщать и систематизировать научную информацию
Владеть:	
Уровень 1	навыками систематизации, обобщения справочной, нормативно-технической информации
Уровень 2	навыками поиска, обобщения, систематизации научно-технической информации, составления кратких отчетов, рефератов
Уровень 3	Навыками обобщения и систематизации научно-технической информации из предметной области исследований и других областей науки и техники, непосредственно примыкающих к проведенным исследованиям
ПК-13.3 способностью участвовать в проектировании средств защиты информации автоматизированной системы.	
Знать:	

Уровень 1	основные задачи и понятия криптографии
Уровень 2	частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки
Уровень 3	принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах и средствах контроля защищенности автоматизированных систем
Уметь:	
Уровень 1	работать в специализированном ПО, анализировать результаты исследований
Уровень 2	анализировать проекты средств защиты информации
Уровень 3	строить криптографические алгоритмы, использовать средства контроля защищенности автоматизированных систем
Владеть:	
Уровень 1	навыками использования типовых криптографических алгоритмов
Уровень 2	навыками использования ПЭВМ в анализе простейших шифров
Уровень 3	методами синтеза и анализа криптографических алгоритмов при проектировании средств защиты информации и средств контроля защищенности автоматизирован-
ПК-14.2: способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации.	
Знать:	
Уровень 1	требования к шифрам и основные характеристики шифров
Уровень 2	принципы разработки современных блочных и поточных криптосистем
Уровень 3	модели шифров и математические методы их исследования
Уметь:	
Уровень 1	определять работоспособность криптографических средств
Уровень 2	использовать отечественные и зарубежные стандарты в области криптографических методов защиты информации в автоматизированных системах
Уровень 3	применять математические методы исследования моделей шифров при анализе работоспособности криптографических средств защиты информации
Владеть:	
Уровень 1	навыками использования ПЭВМ в анализе простейших шифров
Уровень 2	статистическими методами анализа криптосистем
Уровень 3	подходами к анализу криптографических алгоритмов: метод перебора, корреляционный метод анализа поточных шифров, линейный и дифференциальный методы

Таблица 2. Результаты освоения дисциплины.

3.1	**Знать:**
3.1.1	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;
3.2	**Уметь:**
3.2.1	эффективно использовать отечественные и зарубежные стандарты в области криптографических методов защиты информации в автоматизированных системах; применять математические методы исследования моделей шифров;
3.3	**Владеть:**
3.3.1	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.

2. Перечень оценочных средств.

В перечень оценочных средств **по данной дисциплине** входят:
- опрос на занятиях,
- выполнение лабораторных работ,
- экзамен.

Таблица 3. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код компетенции	Этапы формирования компетенций – Разделы/подразделы теоретического обучения					
	1	2	3	4	5	6
ОПК-1.10	+	+	+	+	+	+
ОПК-5.3			+	+	+	+
ПК-1.12	+	+	+	+	+	+
ПК-13.3			+	+	+	+
ПК-14.2		+	+	+	+	+

Знак «+» означает выполненный этап

2.1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования

Таблица 4. Шкала формирования компетенций обучающимися

Код компетенции по ФГОС	Форма оценивания		
	Текущий контроль		Итоговая аттестация
	Этапы: 1-6	Этапы: 2 - 6	Этапы: 1 - 6
	Опрос	Решение задач	Экзамен (вопросы)

ОПК-1.10	+	+	+
ОПК-5.3	+	+	+
ПК-1.12	+	+	+
ПК-13.3	+	+	+
ПК-14.2	+	+	+

3. Оценочные средства поэтапного формирования результатов освоения дисциплины.

3.1 Текущий контроль.

Фонд оценочных средств для проведения текущего контроля успеваемости включает в себя:
- материалы для проведения текущего контроля успеваемости – варианты заданий;
- перечень компетенций и их элементов, проверяемых на каждом мероприятии текущего контроля успеваемости;
- систему и критерии оценивания по каждому виду текущего контроля успеваемости
- описание процедуры оценивания.

3.1.1. Текущий контроль в форме опроса.

Текущий контроль осуществляется путем опроса по материалу, пройденному на предшествующих лекциях.

Оценивается:
- полнота усвоения пройденного материала,
- качество изложения пройденного материала (устно и письменно)

Таблица 5. Шкала оценок уровня усвоения материала обучающимся

Неудовлетворительный	Пороговый	Углублённый	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Не может ответить на вопросы по пройденному материалу или графически изобразить на доске	Отвечает сбивчиво, путается в определениях и обозначениях, нуждается в помощи других обучающихся	Допускает незначительные ошибки при изложении пройденного материала, не полностью представляет связи между разделами изучаемой дисциплины	Четко отвечает на вопросы, может точно изобразить графическую часть пройденного материала, увязывает последовательность изученных разделов дисциплины

Таблица 6. Шкала оценок уровня освоения дисциплины по экзамену.

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Не знает значительной части программного материала, допускает существенные ошибки, с большими затруднения-	Усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недоста-	Твердо знает программный материал, грамотно и по существу излагает его, не допускает суще-	Глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, гра-

ми выполняет практические задания, задачи.	точно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий.	ственных неточностей в ответе на вопрос, может правильно применять теоретические положения и владеет необходимыми умениями и навыками при выполнении практических заданий.	мотно и логически стройно его изложил, не затрудняется с ответом при видоизменении задания, свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, умеет самостоятельно обобщать и излагать материал, не допуская ошибок.

Таблица 7. Шкала оценок уровня освоения дисциплины по тесту.

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Менее 50% правильных ответов.	50-70% правильных ответов.	71-90% правильных ответов.	91-100% правильных ответов.

4. Критерии оценивания для проведения итоговой аттестации

Итоговая аттестация обучающихся проводится **в форме экзамена**.

Критерии оценивания:

- уровень усвоения материала, предусмотренного программой
- умение выполнять задания, предусмотренные программой
- уровень знакомства с дополнительной литературой
- уровень раскрытия причинно-следственных связей
- уровень раскрытия междисциплинарных связей
- стиль поведения (культура речи, манера общения, убежденность, готовность к дискуссии)
- качество ответа (полнота, правильность, аргументированность, его общая композиция, логичность)

4.1. Вопросы к экзамену:

1. История развития криптографии. Терминология. Предмет криптографии Основные задачи криптографии.
2. Модульная арифметика. Система вычетов Z_n.
3. Простой и расширенный алгоритм Евклида. Вычисление наибольшего общего делителя.
4. Аддитивная и мультипликативная инверсии.
5. Алгебраические структуры. Группы, кольца, поля.
6. Циклические группы. Циклические подгруппы.
7. Поля $GF(p^n)$.
8. Понятие шифрования. Шифры подстановки. Криптоанализ.
9. Моноалфавитные шифры. Аддитивный, мультипликативные, аффинный шифры.
10. Многоалфавитные шифры. Автоключевой шифр.
11. Шифр Плейфера.

12. Шифр Виженера.
13. Шифр Хилла.
14. Одноразовый блокнот. Роторный шифр.
15. Бесключевые шифры перестановки.
16. Ключевые шифры перестановки.
17. Блочный шифр и его компоненты.
18. Рассеивание и перемешивание. Раунды.
19. Структура DES.
20. Функция DES. Генерация ключей.
21. Пример шифрования с помощью симметричного алгоритма DES.
22. Слабость в ключе шифра DES.
23. Алгоритмы с открытыми ключами RSA. Общие положения криптосистем с открытым ключом.
24. Алгоритмы рюкзака.
25. Алгоритм Диффи-Хеллмана.
26. Алгоритм Диффи-Хеллмана на эллиптических кривых ECDH.
27. Сложение точек на эллиптических кривых.
28. Генерация ключа в ECDH.
29. Электронная цифровая подпись.
30. Алгоритм Эль-Гамаля.
31. Алгоритм Эль-Гамаля на эллиптических кривых.

4.2. Комплект тестовых заданий.

1.	***Дайте определение понятия криптография:*** -: Криптография – это наука о защите информации от несанкционированного доступа посторонними лицами +: Криптография – наука о защите информации от прочтения её посторонними лицами, достигаемая путем шифрования, которое делает защищенные данные труднораскрываемыми без знания специальной (ключевой) информации -: Криптография – это наука о защите информации с помощью математических преобразований, которые являются симметричными
2.	***Дайте определение понятия шифр:*** -: Шифр – это совокупность преобразований, с помощью которых осуществляется кодирование информации -: Шифр – это алгоритм преобразования, в котором используется ключ +: Шифр – это совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования
3.	***Соотношение, описывающее процесс образования зашифрованных данных из открытых называется:*** +: Алгоритмом шифрования -: Методом шифрования +: Функцией шифрования +: Уравнением шифрования -: Программой шифрования
4.	***Согласно классификации секретных систем по К. Шеннону существует три общих типа таких систем. Укажите какие.*** -: Системы сокрытия информации +: Системы маскировки

	-: Системы защиты данных +: Тайные системы +: Криптографические системы
5.	***Общей задачей дешифрования называется задача*** -: Вычисления апостериорных вероятностей -: Вычисления ключа секретной системы +: Вычисления априорных вероятностей -: Вычисления алгоритма дешифрования
6.	***Апостериорная вероятность – это*** -: вероятность получения ключа с помощью перехвата +: вероятность того, что шифрограмма будет расшифрована без знания ключа -: вероятность использования системы криптографической защиты в условиях постоянных атак
7.	***Замена смысловых конструкций исходной информации (слов, предложений) кодами называется:*** -: Шифрованием +: Кодированием -: Сжатием -: Дешифрованием
8.	***Методы, позволяющие скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации относятся к методам:*** -: Шифрования -: Кодирования -: Сжатия -: Дешифрования +: Стеганографии
9.	***Процесс дешифрования закрытой информации без знания ключа и, возможно, при отсутствии сведений об алгоритме шифрования называется:*** -: Повторным шифрованием -: Вероятностным дешифрованием +: Криптоанализом -: Обратным шифрованием
10.	***Отметьте те высказывания, которые вы считаете верными:*** +: Стойкость шифра должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей -: Процесс шифрования не должен приводить к увеличению объема сообщения +: Криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа +: Ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации
11.	***Какие побочные эффекты могут возникать при использовании криптографических систем защиты?*** -: Ошибки шифрования для больших объемов информации +: Перегрузка трафика +: Замедление работы операционной системы +: Захват системных ресурсов

12.	***Если противник ничего не знает об источнике сообщений, кроме того, что он создает текст на русском языке, то для сокращения полного перебора он может воспользоваться:*** +: относительными частотами букв в русском языке -: абсолютными частотами букв в русском языке -: методом обратных преобразований +: словарем наиболее часто используемых в русском языке слов
13.	***Расположите указанные системы шифрования в хронологическом порядке их появления*** 1: Шифр Скитала 2: Квадрат Полибия 3: Шифр Цезаря 4: Книжный шифр (они так и располагаются)
14.	***Шифр Цезаря является частным случаем:*** +: Шифра моноалфавитной подстановки -: Шифра полиалфавитной подстановки -: Шифра мультиалфавитной подстановки
15.	***Зашифруйте исходное сообщение «ЗАЩИТА» с помощью шифра Цезаря с ключом 4. Для шифрования рекомендуется использовать следующий алфавит «А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ш Щ Ы Ь Ъ Э Ю Я »*** -: «ИТАЗАЩ» -: «ЩИЗАТА» +: «ЛДЭМЦД» -: «МЕЮНЧЕ»
16.	***По характеру использования ключа все криптосистемы можно разделить на:*** -: Блоковые и потоковые -: Синхронные и асинхронные +: Симметричные и ассиметричные -: Битовые и строковые
17.	***Блоковые шифры являются частным случаем:*** +: Симметричного шифрования -: Ассиметричного шифрования -: Шифров гаммирования -: Шифров перестановки
18.	***Потоковое шифрование является частным случаем:*** +: Симметричного шифрования -: Асимметричного шифрования -: Шифров гаммирования -: Шифров перестановки
19.	***Шифры перестановки являются частным случаем:*** +: Блоковых шифров -: Шифров перестановки -: Шифров гаммирования -: Скремблеров
20.	***В симметричных криптосистемах:*** -: Для шифрования и дешифрования всегда используется один и тот же алгоритм +: Для шифрования и дешифрования может использоваться один и тот же алгоритм +: Как для шифрования, так и для дешифрования применяется один и тот же ключ -: Ключ может быть доступным для всех пользователей

21.	***В асимметричных криптосистемах:*** +: Для шифрования и дешифрования используются разные ключи, связанные между собой некоторой математической зависимостью -: Все ключи являются доступными для всех пользователей +: Один из ключей является доступным для всех пользователей -: Зная закрытый ключ легко можно вычислить открытый ключ
22.	***Наиболее известными представителями асимметричных систем шифрования являются:*** -: Алгоритм Диффи-Хеллмана +: Алгоритм RSA -: Алгоритм Рабина-Миллера -: Алгоритм Хаффмана +: Алгоритм Эль-Гамаля
23.	***В потоковых шифрах основной операцией кодирования являются:*** -: Матричные преобразования -: Преобразования, основанные на вычислениях с плавающей точкой -: Вычисления логарифма в конечном поле +: Операция сложения по модулю два (xor)
24.	***Одним из наиболее распространенных способов задания блочных шифров является*** +: Сеть Фейстела -: Матрица Винжера -: Тест Лемана -: Квадрат Полибия
25.	***Выберите те утверждения, которые вы считаете справедливыми для ассиметричных криптосистем*** +: В асимметричных криптосистемах используется пара ключей – открытый ключ и закрытый ключ +: Между открытым и закрытым ключом существует математическая зависимость -: Зная закрытый ключ можно шифровать и дешифровать сообщения +: Открытый ключ можно не шифровать, он передается по незащищенному каналу связи -: Имея пару открытый текст – зашифрованный текст легко можно вычислить открытый ключ
26.	***Выберите те утверждения, которые вы считаете справедливыми для потоковых шифров*** +: Для получения гаммы чаще всего используются генераторы псевдослучайных чисел +: Имея пару открытый текст - зашифрованный текст всегда легко можно вычислить гамму -: Чем меньше разница длин ключа и исходной информации, тем выше вероятность успешной атаки на шифротекст +: Если ключ короче, чем шифруемая последовательность символов, то шифротекст может быть расшифрован криптоаналитиком статистическими методами исследования
27.	***Маршруты Гамильтона применяются в методах:*** -: Аналитического шифрования +: Перестановки -: Замены

	-: Гаммирования
28.	***Элементы матричной алгебры применяются для шифрования в методах:*** -: Перестановок +: Аналитического шифрования -: Замены по таблице -: Гаммирования
29.	***Проблема неполных последних блоков при использовании методов блокового шифрования решается с помощью следующих способов:*** -: Изменение длины блока таким образом, чтобы длина исходного текста оказалась кратной длине блока +: Отказ от шифрования неполного последнего блока +: Замена недостающих символов последнего блока служебными символами -: Использовании адаптивных алгоритмов шифрования
30.	***Какие режимы использования блочных шифров используются в современной криптографии?*** +: ECB -: CBB +: CBC +: CFB -: AFB +: OFB I: **{{77}}**
31.	***С какой целью применяются различные режимы использования блочных шифров?*** -: С целью повысить криптостойкость системы +: С целью сокрытия структуры закодированного сообщения -: С целью увеличения скорости шифрования -: С целью уменьшения объема зашифрованного сообщения
32.	***Укажите, в основе каких известных стандартов шифрования используется сеть Фейстела?*** +: Стандарт шифрования США DES -: Алгоритм BlowFish -: Алгоритм Rijndael +: Российский стандарт шифрования ГОСТ 28147-89 +: Алгоритм MARS
33.	***На функцию стойкого блочного шифра Z=EnCrypt(X,Key) накладываются следующие условия:*** -: Функция EnCrypt должна быть симметричной +: Функция EnCrypt должна быть обратимой +: Не должно существовать иных методов прочтения сообщения X по известному блоку Z, кроме как полным перебором ключей Key +: Не должно существовать иных методов определения каким ключом Key было произведено преобразование известного сообщения X в сообщение Z, кроме как полным перебором ключей -: Длина ключа Key должна быть не меньше, чем размер шифруемого блока

34.	***Российский стандарт шифрования ГОСТ 28147-89 предусматривает следующие режимы работы*** +: Простая замена -: Простая подстановка +: Гаммирование с обратной связью -: Гаммирование со сцеплением блоков +: Выработка имитовставки
35.	***Какие виды необратимых преобразований используются в современной криптографии с открытыми ключами?*** **+:** Разложение произведения больших простых чисел на сомножители -: Матричные преобразования +: Вычисление логарифма в конечном поле +: Вычисление корней алгебраических уравнений -: Разложение на сомножители больших простых чисел
36.	***Системы с открытым ключом (СОК) могут использоваться по следующим назначениям:*** -: Как общий способ задания блочных шифров -: Как средства идентификации пользователей +: Как самостоятельные средства защиты передаваемых и хранимых данных +: Как средства для распределения ключей +: Как средства аутентификации пользователей
37.	***На основе каких необратимых преобразований базируется алгоритм RSA?*** -: Вычисление логарифма в конечном поле -: Матричные преобразования **+:** Разложение произведения больших простых чисел на сомножители -: Вычисление корней алгебраических уравнений
38.	***На основе каких необратимых преобразований базируется алгоритм Эль-Гамаля?*** -: Матричные преобразования **-:** Разложение произведения больших простых чисел на сомножители -: Вычисление корней алгебраических уравнений +: Вычисление логарифма в конечном поле
39.	**Если число x является простым относительно y, то справедливы следующие утверждения:** -: его можно разложить на сомножители, на которые число y не делится без остатка +: его нельзя разложить на сомножители, на которые число y не делится без остатка -: его нельзя разложить на сомножители, на которые число **y** делится без остатка +: *НОД (x,y)=1*
40.	**Укажите пары чисел, которые являются взаимно простыми** +: 8 и 3 -: 8 и 6 +: 12 и 7 -: 18 и 12 -: 9 и 6
41.	***Для оптимизации вычислений при кодировании по алгоритму RSA используется прием, называемый:*** -: Цепочкой возведения в степень +: Цепочкой сложений -: Цепочкой вычитаний

	-: Цепочкой делений -: Цепочкой умножений
42.	***Для алгоритма Эль-Гамаля справедливы следующие утверждения*** +: Получаемый шифротекст в два раза длиннее открытого текста -: Открытый и закрытый ключ можно менять местами -: В алгоритме Эль-Гамаля не используются простые числа +: При равном значении ключа алгоритмы RSA и Эль-Гамаля имеют одинаковую криптостойкость
43.	***Для алгоритма RSA справедливы следующие утверждения*** -: Получаемый шифротекст в два раза длиннее открытого текста +: Открытый и закрытый ключ можно менять местами +: Пара {d,n} считается закрытым ключом -: В алгоритме RSA не используются простые числа +: При равном значении ключа алгоритмы RSA и Эль-Гамаля имеют одинаковую криптостойкость.
44.	***Электронной цифровой подписью называется*** +: присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения -: зашифрованное сообщение, которое содержит информацию об алгоритме шифрования и ключе -: сообщение, посылаемое в открытом виде получателю сообщения, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения
45.	***Какими из перечисленных свойств должна обладать хеш-функция?*** +: она имеет бесконечную область определения +: она имеет конечную область значений -: она имеет бесконечную область значений -: она имеет конечную область определения +: она необратима
46.	***Криптографический протокол – это*** -: протокол, в котором обмен информацией шифруется с помощью некоторого криптографического алгоритма +: протокол, использующий криптографию, применяемую для предотвращения или обнаружения вредительства и мошенничества +: протокол, использующий криптографию для решения задач аутентификации и идентификации пользователей
47.	***Атака на подпись RSA по выбранному шифротексту базируется на следующем свойстве:*** +: Свойстве мультипликативности при возведении в степень -: Свойстве коммутативности при вычислении логарифма в конечном поле -: Свойстве коммутативности при возведении в степень

БГАРФ	Федеральное агентство по рыболовству ФГБОУ ВО «Калининградский государственный технический университет» Балтийская государственная академия рыбопромыслового флота (БГАРФ)		
	Фонд оценочных средств		
	Версия: 1	дисциплины «Криптографические методы защиты информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем»	стр. 15 из 15

5. Сведения о ФОС и его согласовании

Фонд оценочных средств для аттестации по дисциплине представляет собой приложение к рабочей программе дисциплины «Криптографические методы защиты информации»
(наименование дисциплины)
образовательной программы специалитета по специальности 10.05.03 «Информационная безопасность автоматизированных систем»
утвержденной 27 июня 2018 г.

Автор фонда – ст. преподаватель кафедры информационной безопасности _____ Воробейкина И.В.

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры информационной безопасности

(протокол № 9 от 14 июня 2018 г.)

Зав. кафедрой информационной безопасности _____ Великите Н.Я.

Фонд оценочных средств рассмотрен и одобрен на заседании методической комиссии радиотехнического факультета БГАРФ

(протокол № 6 от 27 июня 2018 г.)

Председатель методической комиссии _____ /А.Г.Жестовский/

Согласовано

Начальник отдела мониторинга и контроля БГАРФ _____ /Борисевич Ю.В./