Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования «Казанский национальный исследовательский
технический университет им. А.Н. Туполева-КАИ»
Институт **Компьютерных технологий и защиты информации**

Кафедра **Компьютерных систем**

УТВЕРЖДАЮ
Ответственный за ОП
_____ И.С. Вершинин
«31» 08 2017 г.
Регистрационный номер 4010-17/п-060

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения промежуточной аттестации обучающихся по дисциплине
«Криптографические методы и средства защиты информации»

(наименование дисциплины, практики)

Индекс по учебному плану: **Б1.В.ДВ.02.01**

Направление подготовки: **09.04.01 «Информатика и вычислительная техника»**

Квалификация: **магистр**

Магистерская программа: **Системное и сетевое администрирование (информатика как вторая компетенция)**

Виды профессиональной деятельности: **научно-исследовательская**

Заведующий кафедрой СИБ И.В. Аникин

Разработчик: доцент каф. СИБ Г.С. Корнилов

Казань 2017 г.

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

«Криптографические методы и средства защиты информации»

(наименование дисциплины)

Содержание фонда оценочных средств (ФОС) соответствует требованиям федерального государственного стандарта высшего образования (ФГОС ВО) по направлению 09.04.01 «Информатика и вычислительная техника», учебному плану специальности 09.04.01 «Информатика и вычислительная техника».

Разработанные ФОС обладают необходимой полнотой и являются актуальными для оценки компетенций, осваиваемых обучающимися при изучении дисциплины «Администрирование безопасности компьютерных систем и сетей». Разработанные ФОС полностью соответствуют задачам будущей профессиональной деятельности обучающихся, установленных ФГОС ВО по направлению 09.04.01 «Информатика и вычислительная техника». В составе ФОС присутствуют оценочные средства в виде тестовых заданий и контрольных вопросов различного уровня сложности, которые позволяют провести оценку порогового, продвинутого и превосходного уровней освоения компетенций по дисциплине.

ФОС обладают необходимой степенью приближенности к задачам будущей профессиональной деятельности обучающихся, связанным со применением перспективных методов исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники и информационных технологий (ПК-7). Существенные недостатки отсутствуют.

Заключение. Учебно-методическая комиссия делает вывод о том, что представленные материалы соответствуют требованиям ФГОС ВО по направлению 09.04.01 «Информатика и вычислительная техника» и рекомендуются для использования в учебном процессе.

Рассмотрено на заседании учебно-методической комиссии института КТЗИ от «31» августа 2017 г., протокол № 8.

Председатель УМК института КТЗИ _____ В.В. Родионов

Содержание

Введение

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Криптографические методы и средства защиты информации» – это комплект методических и контрольно-измерительных материалов, предназначенных для определения уровня сформированности компетенций, оценивания знаний, умений, владений на разных этапах освоения дисциплины для проведения промежуточной аттестации обучающихся по дисциплине.

ФОС ПА является составной частью учебного и методического обеспечения программы магистратуры по направлению 09.04.01 «Информатика и вычислительная техника».

Задачи ФОС по дисциплине «Криптографические методы и средства защиты информации»:

– оценка запланированных результатов освоения дисциплины обучающимися в процессе изучения дисциплины, в соответствии с разработанными и принятыми критериями по каждому виду контроля;

– контроль и управление процессом приобретения обучающимися необходимых знаний, умений, навыков и формирования компетенций, определенных в ФГОС ВО по направлению подготовки

ФОС ПА по дисциплине «Криптографические методы и средства защиты информации» сформирован на основе следующих основных принципов оценивания:

– пригодности (валидности) (объекты оценки соответствуют поставленным целям обучения);

– надежности (использования единообразных стандартов и критериев для оценивания запланированных результатов);

– эффективности (соответствия результатов деятельности поставленным задачам).

ФОС ПА по дисциплине «Криптографические методы и средства защиты информации» разработан в соответствии с требованиями ФГОС ВО по направ-

лению 09.04.01 «Информатика и вычислительная техника» для аттестации обучающихся на соответствие их персональных достижений требованиям поэтапного формирования соответствующих составляющих компетенций и включает контрольные вопросы (или тесты) и типовые задания, необходимые для оценки знаний, умений и навыков, характеризующих этапы формирования компетенций.

1. Формы промежуточной аттестации по дисциплине

Дисциплина «Криптографические методы и средства защиты информации» изучается в 3 семестре при очной форме обучения и завершается промежуточной аттестацией в форме экзамена.

2. Оценочные средства для промежуточной аттестации

Оценочные средства для промежуточной аттестации по дисциплине «Криптографические методы и средства защиты информации» при очной форме обучения.

Таблица 1

Оценочные средства для промежуточной аттестации
(очная форма обучения)

№ п/п	Семестр	Форма промежуточной аттестации	Оценочные средства
1.	3	Экзамен	ФОС ПА

3. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

Перечень компетенций и их составляющих, которые должны быть сформированы при изучении темы соответствующего раздела дисциплины «Криптографические методы и средства защиты информации», представлен в таблице 2.

Таблица 2

Перечень компетенций и этапы их формирования
в процессе освоения дисциплины

№ п/п	Этап формирования (семестр)	Наименование раздела	Код формируемой компетенции (составляющей компетенции)		Форма промежуточной аттестации
1.	3	*Введение, элементы теории чисел, классические симметричные методы шифрования*	ПК-7	ПК-7.З	Экзамен
2.	3	*Симметричные криптосистемы, асимметричные криптосистемы, методы криптоанализа*	ПК-7	ПК-7.З ПК-7.У ПК-7.В	Экзамен
3.	3	*Идентификация и проверка подлинности, Электронная цифровая подпись, управление криптографическими ключами*	ПК-7	ПК-7.З ПК-7.У ПК-7.В	Экзамен

4. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описания шкалы оценивания

Показатели и критерии оценивания сформированности компетенций на зачете, приведены в таблице 3.

Таблица 3

Показатели и критерии оценивания сформированности компетенций на зачете

№ п/п	Этап формирования (семестр)	Код формируемой компетенции (составляющей компетенции)		Критерии оценивания	Показатели оценивания (планируемые результаты обучения)		
					Пороговый уровень	Продвинутый уровень	Превосходный уровень
1.	3	ПК-7	ПК-7.3	Теоретические навыки	Знание перспективных методов исследования и решения профессиональных задач	Знание перспективных методов исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники	Знание перспективных методов исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники и информационных технологий

2.	3	ПК-7	ПК-7.У ПК-7.В	Практические навыки	умение применять перспективные методы исследования и решения профессиональных задач практически выполнять работы по установке, настройке и обслуживанию программных (в том числе криптографических) средств защиты информации. Владеть навыками исследования и решения профессиональных задач Владеть навыками обслуживания программных (в том числе криптографических) средств защиты информации	умение применять перспективные методы исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники практически выполнять работы по установке, настройке и обслуживанию программно-аппаратных (в том числе криптографических) средств защиты информации навыками исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники	умение применять перспективные методы исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники и информационных технологий; практически выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации Владеть навыками исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники и информационных технологий

Формирование оценки при промежуточной аттестации по итогам освоения дисциплины зависит от уровня освоения компетенций, которые обучающийся должен освоить по данной дисциплине. Связь между итоговой оценкой и уровнем освоения компетенций (шкала оценивания) представлена в таблице 4.

Таблица 4

Описание шкалы оценивания

Шкала оценивания		Описание оценки в требованиях к уровню и объему компетенций
Словесное выражение	Выражение в баллах	
отлично	от 86 до 100	Освоен **превосходный** уровень всех компетенций (составляющих компетенций)
хорошо	от 71 до 85	Освоен **продвинутый** уровень всех компетенций (составляющих компетенций)
удовлетворительно	от 51 до 70	Освоен **пороговый** уровень всех компетенций (составляющих компетенций)
неудовлетворительно	до 51	Не освоен **пороговый** уровень всех компетенций (составляющих компетенций)

5. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формирование оценки по результатам текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины «Криптографические методы и средства защиты информации» приведено в таблице 5.

Таблица 5

Формирование оценки по итогам освоения дисциплины

Наименование контрольного мероприятия	Рейтинговые показатели				
	I аттестация	II аттестация	III аттестация	по результатам текущего контроля	по итогам промежуточной аттестации (зачета /экзамена)
Раздел 1. *Введение, элементы теории чисел, классические симметричные методы шифрования*	**10**			**10**	
Тест текущего контроля по разделу	10			10	
Раздел 2. *Симметричные криптосистемы, асимметричные криптосистемы, методы криптоанализа*		**20**		**20**	
Тест текущего контроля по разделу		10		10	
Защита лабораторных работ		10		10	
Раздел 3. *Идентификация и проверка подлинности, Электронная цифровая подпись, управление криптографическими ключами*			**20**	**20**	
Тест текущего контроля по разделу			10	10	
Защита лабораторных работ			10	10	
Промежуточная аттестация (зачет):					**50**
– тест промежуточной аттестации по дисциплине					20
– ответы на контрольные вопросы в письменной форме					30

6 Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины

Тестовые задания

1. Что является целью криптоанализа?

- A. Определение стойкости алгоритма
- B. Увеличение количества функций замещения в криптографическом алгоритме
- C. Уменьшение количества функций подстановкм в криптографическом алгоритме
- D. Определение использованных перестановок

2. Частота применения брутфорс-атак возросла, поскольку:

- A. Возросло используемое в алгоритмах количество перестановок и земещений
- B. Алгоритмы по мере повышения стойкости становились менее сложными и более подверженными атакам
- C. Мощность и скорость работы процессоров возросла
- D. Длина ключа со временем уменьшилась

3. Что из перечисленного ниже не является свойством или характеристикой односторонней функции хэширования?

- A. Она преобразует сообщение произвольной длины в значение фиксированной длины
- B. Имея значение дайджеста сообщения, невозможно получить само сообщение
- C. Получение одинакового дайджеста из двух различных сообщений невозможно, либо случается крайне редко
- D. Она преобразует сообщение фиксированной длины в значение переменной длины

4. Что может указывать на изменение сообщения?

- A. Изменился открытый ключ
- B. Изменился закрытый ключ
- C. Изменился дайджест сообщения
- D. Сообщение было правильно зашифровано

5. Какой из перечисленных ниже алгоритмов является алгоритмом американского правительства, предназначенным для создания безопасных дайджестов соообщений?

- A. Data Encryption Algorithm
- B. Digital Signature Standard
- C. Secure Hash Algorithm
- D. Data Signature Algorithm

6. Что из перечисленного ниже лучше всего описывает отличия между HMAC и CBC-MAC?

- A. HMAC создает дайджест сообщения и применяется для контроля целостности; CBC-MAC используется для шифрования блоков данных с целью обеспечения конфиденциальности
- B. HMAC использует симметричный ключ и алгоритм хэширования; CBC-MAC использует первый блок в качестве контрольной суммы
- C. HMAC обеспечивает контроль целостности и аутентификацию источника данных; CBC-MAC использует блочный шифр в процессе создания MAC
- D. HMAC зашифровывает сообщение на симметричном ключе, а затем передает результат в алгоритм хэширования; CBC-MAC зашифровывает все сообщение целиком

7. В чем преимущество RSA над DSA?

- A. Он может обеспечить функциональность цифровой подписи и шифрования
- B. Он использует меньше ресурсов и выполняет шифрование быстрее, поскольку использует симметричные ключи
- C. Это блочный шифр и он лучше поточного
- D. Он использует одноразовые шифровальные блокноты

8. Многие страны ограничивают использование и экспорт криптографических систем. Зачем они это делают?

- A. Без ограничений может возникнуть большое число проблем совместимости при попытке использовать различные алгоритмы в различных программах
- B. Эти системы могут использоваться некоторыми странами против их местного населения
- C. Криминальные элементы могут использовать шифрование, чтобы избежать обнаружения и преследования
- D. Законодательство сильно отстает, а создание новых типов шифрования еще больше усиливает эту проблему

9. Что используется для создания цифровой подписи?

- A. Закрытый ключ получателя
- B. Открытый ключ отправителя
- C. Закрытый ключ отправителя
- D. Открытый ключ получателя

10. Что из перечисленного ниже лучше всего описывает цифровую подпись?

- A. Это метод переноса собственноручной подписи на электронный документ
- B. Это метод шифрования конфиденциальной информации
- C. Это метод, обеспечивающий электронную подпись и шифрование
- D. Это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения

11. Какова эффективная длина ключа в DES?

- A. 56
- B. 64
- C. 32
- D. 16

12. По какой причине удостоверяющий центр отзывает сертификат?

- A. Если открытый ключ пользователя скомпрометирован
- B. Если пользователь переходит на использование модели PEM, которая использует сеть доверия
- C. Если закрытый ключ пользователя скомпрометирован
- D. Если пользователь переходит работать в другой офис

13. Что из перечисленного ниже лучше всего описывает удостоверяющий центр?

- A. Организация, которая выпускает закрытые ключи и соответствующие алгоритмы
- B. Организация, которая проверяет процессы шифрования
- C. Организация, которая проверяет ключи шифрования
- D. Организация, которая выпускает сертификаты

14. Как расшифровывается аббревиатура DEA?

- A. Data Encoding Algorithm
- B. Data Encoding Application
- C. Data Encryption Algorithm
- D. Digital Encryption Algorithm

15. Кто участвовал в разработке первого алгоритма с открытыми ключами?

- A. Ади Шамир
- B. Росс Андерсон
- C. Брюс Шнайер
- D. Мартин Хеллман

16. Какой процесс обычно выполняется после создания сеансового ключа DES?

- A. Подписание ключа
- B. Передача ключа на хранение третьей стороне (key escrow)
- C. Кластеризация ключа
- D. Обмен ключом

17. Сколько циклов перестановки и замещения выполняет DES?

- A. 16
- B. 32
- C. 64
- D. 56

18. Что из перечисленного ниже является правильным утверждением в отношении шифрования данных, выполняемого с целью их защиты?

- A. Оно обеспечивает проверку целостности и правильности данных
- B. Оно требует внимательного отношения к процессу управления ключами
- C. Оно не требует большого количества системных ресурсов
- D. Оно требует передачи ключа на хранение третьей стороне (escrowed)

19. Как называется ситуация, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст?

- A. Коллизия
- B. Хэширование
- C. MAC
- D. Кластеризация ключей

20. Что из перечисленного ниже является определением фактора трудозатрат для алгоритма?

- A. Время зашифрования и расшифрования открытого текста
- B. Время, которое займет взлом шифрования
- C. Время, которое занимает выполнение 16 циклов преобразований
- D. Время, которое занимает выполнение функций подстановки

21. Что является основной целью использования одностороннего хэширования пароля пользователя?

- A. Это снижает требуемый объем дискового пространства для хранения пароля пользователя
- B. Это предотвращает ознакомление кого-либо с открытым текстом пароля

C. Это позволяет избежать избыточной обработки, требуемой асимметричным алгоритмом

D. Это предотвращает атаки повтора (replay attack)

22. Какой из перечисленных ниже алгоритмов основан на сложности разложения больших чисел на два исходных простых сомножителя?

A. ECC

B. RSA

C. DES

D. Диффи-Хеллман

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

A. DES – это симметричный алгоритм, а RSA – асимметричный

B. DES – это асимметричный алгоритм, а RSA – симметричный

C. Они оба являются алгоритмами хэширования, но RSA генерирует 160-битные значения хэша

D. DES генерирует открытый и закрытый ключи, а RSA выполняет шифрование сообщений

24. Какой из перечисленных ниже алгоритмов использует симметричный ключ и алгоритм хэширования?

A. HMAC

B. 3DES

C. ISAKMP-OAKLEY

D. RSA

25. Генерация ключей, для которой используются случайные значения, называется Функцией генерации ключей (KDF). Какие значения обычно не используются при этом в процессе генерации ключей?

A. Хэши

B. Асимметричные значения

C. Соль

D. Пароли

Вопросы оценки практических навыков

Пример заданий по практической реализации следующих тем:

1. Числа Мерсенна
2. Расширенного алгоритма Евклида
3. Алгоритм ассиметричного шифрования RSA
4. Схема шифрования Эль-Гамаля
5. Цифровая подпись по схеме RSA
6. Алгоритм цифровой подписи Эль-Гамаля
7. ЭЦП ГОСТ Р 34.10-94
8. Слепая цифровая подпись
9. Схема Диффи-Хеллмана

Контрольные вопросы

1. Основные понятия и определения криптографии. Задачи, решаемые криптографией. Принципы построения шифров.
2. Классические симметричные методы шифрования.
3. Классические симметричные методы шифрования. Шифры перестановки.
4. Классические симметричные методы шифрования. Шифры замены.
5. Классические симметричные методы шифрования. Шифрование методом гаммирования.
6. Методы генерации псевдослучайных последовательностей чисел.
7. Симметричные криптосистемы (криптосистемы с секретным ключом).
8. Американский стандарт шифрования данных DES. Основные режимы работы алгоритма DES.
9. Режимы работы алгоритма DES: режим «Электронная кодовая книга».
10. Режимы работы алгоритма DES: режим «Сцепление блоков шифра».
11. Режимы работы алгоритма DES: режим «Обратная связь по шифру».
12. Режимы работы алгоритма DES: режим «Обратная связь по выходу».
13. Алгоритм шифрования данных IDEA.
14. Отечественный стандарт шифрования данных ГОСТ 28147-89. Основные режимы работы алгоритма ГОСТ.
15. Блочные и поточные шифры.
16. Асимметричные криптосистемы (криптосистемы с открытым ключом). Концепция криптосистем с открытым ключом.
17. Однонаправленные функции.
18. Криптосистема шифрования RSA: процедуры шифрования и дешифрования, безопасность и быстродействие криптосистемы.
19. Схема шифрования Эль Гамаля.
20. Методы криптоанализа. Основные методы дешифрования.
21. Методы криптоанализа. Метод тотального опробования ключей.

22. Методы криптоанализа. Статистические модели текстов и шифров.
23. Причины ненадежности криптосистем.
24. Взаимная проверка подлинности пользователей.
25. Протоколы идентификации с нулевой передачей знаний: упрощённая схема идентификации с нулевой передачей знаний, параллельная схема идентификации с нулевой передачей знаний.
26. Электронная цифровая подпись.
27. Проблема аутентификации данных и электронная цифровая подпись.
28. Однонаправленные хэш-функции: хэш-функции на основе симметричных блочных шифров, отечественные стандарты хэш-функций.
29. Алгоритмы электронной цифровой подписи: алгоритм RSA.
30. Алгоритмы электронной цифровой подписи: алгоритм Эль Гамаля.
31. Алгоритмы электронной цифровой подписи: алгоритм DSA.
32. Алгоритмы электронной цифровой подписи: отечественный стандарт цифровой подписи.

Лист регистрации изменений и дополнений

№ п/п	№ страницы внесения изменений	Дата внесения изменения	Краткое содержание изменений (основание)	Ф.И.О., подпись	«Согласовано» заведующий кафедрой, ведущей дисциплину