Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
(ФГБОУ ВО «КГТУ»)

УТВЕРЖДАЮ
И.о. директора института

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 4ae0684d0d529bb9d0248a5b51302ea1
Владелец: Гоконаев Мирослав Валерьевич
Действителен: с 02.08.2024 по 26.10.2025

Фонд оценочных средств
(приложение к рабочей программе модуля)

«МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»

основной профессиональной образовательной программы специалитета
по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ
Специализация
«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

ИНСТИТУТ цифровых технологии
РАЗРАБОТЧИК кафедра информационной безопасности

1. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ. ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ И КРИТЕРИИ ОЦЕНИВАНИЯ

1.1 Результаты освоения дисциплины

Таблица 1 – Планируемые результаты обучения по дисциплине, соотнесенные с установленными индикаторами достижения компетенций

Код и наименование компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями
ОПК-10: Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности.	Методы и средства криптографической защиты информации	Знать: модели шифров и основные задачи криптографии; методы решения криптографических задач. Уметь: использовать математические методы в изучении криптографических алгоритмов; пользоваться средствами криптографии. Владеть: типовыми криптографическими алгоритмами; типовыми средствами для решения задач защиты информации.

1.2. К оценочным средствам текущего контроля успеваемости относятся:

- расчетно-графическая работа;

- тестовые задания открытого и закрытого типов.

К оценочным средствам для промежуточной аттестации относятся:

- экзаменационные задания по дисциплине, представленные в виде тестовых заданий закрытого и открытого типов.

Промежуточная аттестация в форме зачета проходит по результатам прохождения всех видов текущего контроля успеваемости. В отдельных случаях (при не прохождении всех видов текущего контроля) зачет может быть проведен в виде тестирования.

1.3. Критерии оценки результатов освоения дисциплины

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100 – балльную/процентную систему и правило перевода оценок в пятибалльную систему (табл. 2).

Таблица 2 – Система оценок и критерии выставления оценки

Система оценок / Критерий	**2**	**3**	**4**	**5**
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
1. Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно- корректно связывать между собой (только некоторые из которых может связывать между собой)	Обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полнотой знаний и системным взглядом на изучаемый объект
2. Работа с информацией	Не в состоянии находить необходимую информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3. Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	В состоянии осуществлять научно корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задаче данные	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи
4. Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

1.4 Оценивание тестовых заданий закрытого типа осуществляется по системе зачтено/ не зачтено («зачтено» – 41-100% правильных ответов; «не зачтено» – менее 40 % правильных ответов) или пятибалльной системе (оценка «неудовлетворительно» - менее 40 % правильных ответов; оценка «удовлетворительно» - от 41 до 60 % правильных ответов; оценка «хорошо» - от 61 до 80% правильных ответов; оценка «отлично» - от 81 до 100 % правильных ответов).

Тестовые задания открытого типа оцениваются по системе «зачтено/ не зачтено». Оценивается верность ответа по существу вопроса, при этом не учитывается порядок слов в словосочетании, верность окончаний, падежи.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ОПК-10: Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

Тестовые задания открытого типа (7 семестр):

1. Если число *x* является простым относительно *y*, то их наибольший общий делитель:
Ответ: *НОД (x,y)=1*

2. По характеру использования ключа все криптосистемы можно разделить на:
Ответ: симметричные и асимметричные

3. Шифры перестановки являются частным случаем:
Ответ: блоковых шифров

4. Наименьшее число, взаимно простое с 756:
Ответ: 5

5. Количество простых чисел в диапазоне от 20 до 40 равно:
Ответ: 4

6. Наименьшее число, взаимно простое с 9100:
Ответ: 3

7. Расширенный алгоритм Евклида вычисляет:
Ответ: мультипликативную инверсию числа

8. Любой элемент из Z_{n*} имеет:
Ответ: имеет мультипликативную инверсию

9. Число *a* имеет мультипликативную инверсию в Z_n, если:
Ответ: НОД(*a,n*)=*1*

10. Значение выражения *(a + b) mod n* равно:
Ответ: *[(a mod n) + (b mod n)] mod n*

11. Согласно принципу Керкгоффса предполагается, что:

Ответ: ключ должен быть настолько труден, что скрывать алгоритм кодирования/дешифрования нет необходимости

12. При шифровании методом Плейфера фиктивный символ ставится между:
Ответ: стоящими рядом одинаковыми буквами

13. Шифр Цезаря является частным случаем шифра:
Ответ: моноалфавитной подстановки

14. В симметричных криптосистемах ключ шифрования и дешифрования:
Ответ: один и тот же

15. Наибольший общий делитель чисел 574, 273 равен:
Ответ: 7

16. Наибольший общий делитель чисел 115, 253 равен:
Ответ: 23

17. Операция по модулю в криптографии – это:
Ответ: вычисление остатка от деления двух чисел

18. Числа a и b мультипликативно инверсны в Z_n, если:
Ответ: $(a \times b) \bmod n = 1$

19. В шифре Хилла размерность ключевой матрицы зависит от:
Ответ: величины блоков, на которые разбит исходный текст

20. Зашифрованное сообщение ЗАЩИТА с помощью шифра Цезаря с ключом 4 (для шифрования используется алфавит «А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я ») :
Ответ: МДЭНЦД

21. В Z_{23} значение 3^{-1} равно:
Ответ: 8

22. Систематически перемешанный алфавит – это буквы алфавита, записанные:
Ответ: по порядку их следования в алфавите, исключая буквы, использованные в ключевом слове

23. Простой алгоритм Евклида вычисляет:
Ответ: наибольший общий делитель двух чисел

24. Число -17 в системе вычетов Z_{26} равно:
Ответ: 9

25. Числа a и b аддитивно инверсны в Z_n, если:
Ответ: $(a+b) \bmod n = 0$

26. Значение выражения $(12 - 43) \bmod 13 = (-31) \bmod 13$ равно:
Ответ: 8

27. Число 8 в Z_{10} не имеет мультипликативную инверсию, потому что:
Ответ: $НОД(10,8)=2$

28. Согласно принципу Керкгоффса, нужно всегда предполагать, что противник:
Ответ: знает алгоритм кодирования/дешифрования

29. При методе грубой силы противник:
Ответ: пробует все возможные ключи

30. Слову *"crypt"* соответствует числовая последовательность: *x=(2,17,24,15),* которая зашифрована аффинным шифром с ключами (3,5); в результате шифрования получилось сообщение:
Ответ: *LEZY*

Тестовые задания закрытого типа (7 семестр)

1. Аффинный шифр определен:
а. на кольце
б. в группе
в. в поле
г. в циклической подгруппе

2. При статистической атаке противник:
а**.** пробует все возможные ключи
б. **анализирует некоторые свойственные языку исходного текста характеристики**
в. получает доступ к некоторым парам *исходный/зашифрованный текст*
г. пользуется методом обратных преобразований

3. Блоковые шифры являются частным случаем:
а. **симметричного шифрования**
б. асимметричного шифрования
в. шифров перестановки
г. шифра рюкзака

4. Из перечисленных пар чисел взаимно простыми являются:
а. 18, 21
б. **22, 25**
в. 24, 27
г. 25, 100

5. Число 4 имеет мультипликативную инверсию в:
а. Z_{12}
б. $\boldsymbol{Z_{13}}$
в. Z_{14}
г. Z_{26}

6. В Z_{10} ноль:
а. аддитивен единице
б. аддитивен десяти
в. **аддитивен самому себе**
г. аддитивен девяти

7. В Z_{10} число 9:
а. не имеет мультипликативной инверсии
б. мультипликативно единице
в. **мультипликативно самому себе**
г. мультипликативно десяти

8. Криптоанализ – это наука и искусство:

а. создания шифров
б. создания и взламывания шифров
в. **взламывания шифров**
г. обходиться без ключевых шифров

9. Одним из наиболее распространенных способов задания блочных шифров является:

а. **сеть Фейстела** в. квадрат Полибия

б. матрица Виженера г. систематически перемешанный алфавит

10. Преимуществом симметричного шифрования является:

а. высокая скорость выполнения в. высокая стойкость к атакам

б. простота изменения алгоритма г. легкость выбора паролей

Тестовые задания открытого типа (8 семестр):

1. В идеальной криптосистеме один и тот же ключ может использоваться:
Ответ: многократно

2. В российском стандарте электронная подпись к сообщению состоит из чисел *r, s*; число *r* не должно быть равно нулю, т.к. в этом случае:
Ответ: автор сообщения может отказаться от своей подписи

3. Наиболее известными представителями асимметричных систем шифрования является алгоритм:
Ответ: RSA

4. В идеальной системе шифрования найти сообщение без знания ключа:
Ответ: невозможно

5. Шифр Вернама применили для шифрования неизвестного сообщения с ключом 1100 и получили зашифрованное сообщение 1000; неизвестное сообщение:
Ответ: 0100

6. В системе Диффи-Хеллмана используется большое число P, по модулю которого ведется вычисление ключа; это число должно быть:
Ответ: простым

7. При построении электронной подписи используется:
Ответ: хэш-функция

8. В асимметричных криптосистемах для шифрования и дешифрования используются:
Ответ: разные ключи, связанные между собой некоторой математической зависимостью

9. Хэш-функция должна быть:
Ответ: необратимой

10. В шифре RSA сообщение шифруется с использованием:
Ответ: открытого ключа

11. Методы шифрования, использующие пару ключей (открытый и закрытый), называются
Ответ: асимметричными

12. Хэш-функция должна обладать свойством:
Ответ: однонаправленности

13. Система управления ключами это:
Ответ: система, управляющая созданием, распределением и хранением криптографических ключей

14. Для создания цифровых подписей используется алгоритм:
Ответ: RSA

15. Алгоритм гаммирования это:
Ответ: метод шифрования, при котором исходный текст комбинируется (складывается по модулю) с гаммой (случайной последовательностью чисел)

16. Хэш-функция это:
Ответ: алгоритм, который преобразует входные данные произвольной длины в фиксированный размер, обеспечивая целостность данных

17. Электронная подпись это:
Ответ: цифровой аналог подписи, которая используется для подтверждения подлинности электронных документов

18. Задача криптографических протоколов:
Ответ: обеспечение конфиденциальности, целостности и аутентификации передаваемой информации

19. Сертификат в криптографии это:
Ответ: электронный документ, подтверждающий связь между открытым ключом и его владельцем

20. Основные компоненты криптографической системы это:
Ответ: алгоритмы шифрования, ключи и протоколы аутентификации

21. Алгоритм Диффи-Хеллмана позволяет:
Ответ: двум сторонам создать общий секретный ключ через открытый канал связи

22. Передача по открытому каналу это:
Ответ: передача данных без использования защищенных методов шифрования, что делает их уязвимыми для перехвата

23. В алгоритме рюкзака «ограниченный рюкзак» означает, что:
Ответ: каждый предмет можно взять только один раз

24. При формулировке задачи о рюкзаке необходимы параметры:
Ответ: вес, стоимость каждого предмета и общая вместимость рюкзака

25. В шифре RSA сообщение шифруется путем:
Ответ: умножения на секретное число

26. В Российском стандарте электронной подписи используется большое число P, по модулю которого ведутся вычисления; это число должно быть:
Ответ: любым нечетным

27. Секретные параметры пользователя в протоколе Шамира
Ответ: нечетные

28. Шифр Вернама применили для шифрования неизвестного сообщения с ключом 1100 и получили зашифрованное сообщение 1000; неизвестное сообщение:
Ответ: 0100

29. В системе Диффи-Хеллмана используется большое число P, по модулю которого ведется вычисление ключа; это число должно быть:
Ответ: простым

30. В идеальной системе шифрования найти сообщение без знания ключа:
Ответ: невозможно

Тестовые задания закрытого типа (8 семестр)

1. В протоколе шифра Эль-Гамаля сообщение пересылается:

а. **один раз**	в. три раза
б. два раза	г. четыре раза

2. Для асимметричных криптосистем справедливо утверждение:

а. **между открытым и закрытым ключом существует математическая зависимость**	в. имея пару *открытый текст-зашифрованный текст* можно вычислить открытый ключ
б. зная открытый ключ можно шифровать и дешифровать сообщения	г. между открытым и закрытым ключом не существует никакой зависимости

3. В Российском стандарте для электронной подписи используется:

а. **международный стандарт**	в. стандарт Европейского сообщества
б. Российский стандарт	г. стандарт США

4. При использовании криптографических систем защиты могут возникать побочные эффекты:

а. ошибки шифрования для больших объемов информации	в. захват системных ресурсов
б. **замедление работы операционной системы**	г. сбой в работе протокола шифрования

5. Если при использовании методов блокового шифрования последних блок неполон, то проблема решается с помощью следующих способов:

а. изменение длины блока таким образом, чтобы длина исходного текста оказалась кратной длине блока	в. применение других алгоритмов шифрования
б. **замена недостающих символов последнего блока служебными символами**	г. отбрасывание последнего неполного блока

6. Асимметричными являются алгоритмы:

а. алгоритм рюкзака	в. AES
б. DES	**г. RSA**

7. Для генерации ключей используется метод:

а. генерация на основе случайных чисел

в. использование криптографических протоколов

б. использование паролей

г. генерация на основе алгоритмов хэширования

8. Хэш-функция:

а. преобразует данные в фиксированный размер

в. **используется для проверки целостности данных**

б. обеспечивает конфиденциальность данных

г. защищает информацию от атаки грубой силы

9. Гаммирование это:

а. метод шифрования, использующий случайные числа

в. метод перестановки символов по определенны правилам

б. процесс добавления случайных данных к открытым сообщениям

г. удаление пробелов и спецсимволов из исходного текста

10. Основные типы криптографии:

а. симметричная

в. гибридная

б. асимметричная

г. квантовая

3. ТИПОВЫЕ ЗАДАНИЯ НА КОНТРОЛЬНУЮ РАБОТУ, КУРСОВУЮ РАБОТУ/ КУРСОВОЙ ПРОЕКТ, РАСЧЕТНО-ГРАФИЧЕСКУЮ РАБОТУ

Расчетно-графическая работа

Реализация алгоритма Диффи-Хеллмана на эллиптической кривой.

Формулы для операций с точками эллиптической кривой:

Операция	*Поле характеристики p (p≠2 и p≠3)*
Сложение точек $P \neq \pm Q$ $P(x_1, y_1) + Q(x_2, y_2) = R(x_3, y_3)$	$\lambda = \frac{y_2 - y_1}{x_2 - x_1} (mod\ p)$ $x_3 = \lambda^2 - x_1 - x_2\ (mod\ p)$ $y_3 = \lambda(x_1 - x_3) - y_1 (mod\ p)$
Удвоение точки $R(x_3, y_3) = 2\ P(x_1, y_1)$	$\lambda = \frac{3{x_1}^2 + a}{2y_1} (mod\ p)$ $x_3 = \lambda^2 - 2x_1\ (mod\ p)$ $y_3 = \lambda(x_1 - x_3) - y_1 (mod\ p)$
$O + O = O$ $P(x, y) + O = P(x, y)$ $P(x, y) + P(x, -y) = O$	

Сгенерировать общий секретный ключ для двух пользователей по схеме Диффи-Хеллмана, если выбрана эллиптическая кривая $E_{211}(0, -4)$ и точка $P(2, 2)$. Пусть секретный ключ пользователя A будет $K_A = 121$, а пользователя B – $K_B = 203$.

ТЕМЫ И ОБРАЗЦЫ ЗАДАНИЙ ДЛЯ ЛАБОРАТОРНЫХ ЗАНЯТИЙ (семестр 7)

Тема 1. Простой и расширенный алгоритм Евклида. Модульная арифметика. Операции в системе вычетов Zn. Аддитивная и мультипликативная инверсии.

Пример 1.1

Используя алгоритм Евклида, Найти *НОД (2740, 1760), НОД (25, 60).*

Пример 1.2

Используя расширенный алгоритм Евклида, найти мультипликативную инверсию 23 в Z_{100}.

Пример 1.3

Выполните следующие операции:
а. сложить *7* и *14* в Z_{15}
б. вычесть *11* из *7* в Z_{13}
в. умножить *11* на *7* в Z_{20}

Тема 2. Алгебраические структуры.

Пример 2.1

Дана группа $G = <Z_6, +>$, из нее сгенерировать циклические подгруппы.

Пример 2.2

Дана группа $G=<Z_{10^*}, \times>$, найти для нее циклические подгруппы.

Тема 3. Аффинный шифр. Шифр Плейфера. Шифр Виженера. Шифр Хилла

Пример 3.1

С помощью аффинного шифра зашифровать сообщение *cryptography* с ключевой парой *(3,5)* в Z_{26}.

Пример 3.2

С помощью шифра Плейфера зашифровать текст *happy;* ключ шифрования:

Секретный ключ =

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

С помощью шифра Виженера зашифровать сообщение *She is listening*, используя ключевое слово *PASCAL*.

Пример 3.4

С помощью шифра Хилла зашифровать фразу: *без труда не вынешь рыбку из пруда,* записанную в 30-буквенном русском алфавите. Ключевую матрицу выбрать самостоятельно.

Тема 4. Шифр вертикальной перестановки.

Пример 4.1

Зашифровать фразу *вот пример шифра вертикальной перестановки,* используя матрицу *6×7* и числовой ключ *(5,1,4,7,2,6,3).*

Тема 5. Шифрование с помощью симметричного алгоритма DES

Пример 5.1

Зашифровать *64*-битовую последовательность *123456ABCD132536* ключом *AABB09182736CCDD.* Сделать только первый раунд.

Пример 5.2

В примере 5.1 используя ключ шифрования первого раунда сгенерировать ключ шифрования для второго раунда

Тема 6. Усовершенствованный шифр Цезаря

Пример 6.1

Зашифровать усовершенствованным шифром Цезаря (два раунда) слово ЛУНА. Ключ $k1 = 6$, $k2 = 11$. В алфавите 32 буквы (исключить букву Ё)
Таблица замены:
А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я
Р Т М Ф Ы Щ Ъ З Й Ю У Я Г С Э П Ц Н Б К Д Х А Ч Ш В Ь Е Ж О И Л

ТЕМЫ И ОБРАЗЦЫ ЗАДАНИЙ ДЛЯ ЛАБОРАТОНЫХ ЗАНЯТИЙ (семестр 8)

Тема 7. Криптосистемы с открытым ключом: RSA, Шамира, Эль-Гамаля.

Пример 7.1

Для шифра Шамира с параметрами $p = 30803$, $cA = 501$, $cB = 601$ и сообщения $m = 11111$ вычислить dA, dB, $x1$, $x2$, $x3$, $x4$.

Пример 7.2

Для шифра Эль-Гамаля с параметрами $p = 30803$, $g = 2$, $c = 500$, $k = 600$ и сообщения $m = 11111$ вычислить зашифрованное сообщение.

Тема 8. Алгоритм рюкзака.

Пример 8.1

Зашифровать сообщение *АБРАМОВ*, символы которого представить в бинарном виде в соответствии с таблицей кодов символов *Windows 1251*. Сверхвозрастающая последовательность равна *{2, 3, 6, 13, 27, 52, 105, 210}, n=31, m=420.*

Тема 9. Электронная подпись

Пример 9.1

Для системы RSA с параметрами пользователя $P = 131$, $Q = 227$, $d = 3$ и секретного ключа c, найденного в первой лабораторной работе, вычислить подпись для сообщения m = «Happy New Year». Осуществить проверку подписи.

Пример 9.2

В подписанный документ (пример 9.1) внести ошибку (искажение). Еще раз сделать проверку подписи.

Тема 10. Алгоритм Диффи-Хеллмана

Пример 10.1

Сгенерировать секретный ключ. Исходные данные: $p = 23$ – открытое простое число, $g = 5$ – первообразный корень по модулю p (тоже открытое число), $a = 6$ – секретный ключ Алисы, $b = 15$ – секретный ключ Боба.

Пример 10.2

Найти все точки эллиптической кривой $E_7(2,6)$.

Пример 10.3

Найти порядок точки $P(9,4)$ в группе эллиптической кривой $E_{11}(6,3)$.

Пример 10.4

Найти общий ключ для шифрования $K=(x,y)$, используя алгоритм Диффи-Хеллмана на основе эллиптических кривых, если кривая имеет вид $y^2 = x^3 + 2x + 2 \, mod 17$. Примитивный элемент равен $P=(5,1)$. Секретный ключ Алисы $c=3$, секретный ключ Боба $d=10$.

4. СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «Методы и средства криптографической защиты информации» представляет собой компонент основной профессиональной образовательной программы специалитета по специальности 10.05.03 Информационная безопасность. Специализация «Безопасность открытых информационных систем».

Преподаватель-разработчик – старший преподаватель И.В.Воробейкина

Фонд оценочных средств рассмотрен и одобрен методической комиссией института цифровых технологий (протокол №5 от 29 августа 2024 г).

Председатель методической комиссии  О.С. Витренко