СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет ***Математики и информационных технологий***
Кафедра ***Прикладной информатики и программирования***

Оценочные материалы по дисциплине (модулю)

дисциплина ***Методы и средства криптографической защиты информации***

Блок Б1, обязательная часть, Б1.О.28
цикл дисциплины и его часть (обязательная часть или часть, формируемая участниками образовательных отношений)

Направление

10.03.01 ***Информационная безопасность***
код наименование направления

Программа

Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения

Очно-заочная

Для поступивших на обучение в
2021 г.

Разработчик (составитель)
кандидат физико-математических наук, доцент
Перевалова С. Л.
ученая степень, должность, ФИО

Стерлитамак 2022

1. Перечень компетенций, индикаторов достижения компетенций и описание показателей и критериев оценивания результатов обучения по дисциплине (модулю) 3

2. Оценочные средства, необходимые для оценки результатов обучения по дисциплине (модулю).....5

3. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю), описание шкал оценивания 15

1. Перечень компетенций, индикаторов достижения компетенций и описание показателей и критериев оценивания результатов обучения по дисциплине (модулю)

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)	Показатели и критерии оценивания результатов обучения по дисциплине (модулю)				Вид оценочного средства
1	2	3	4				5
			неуд.	удовл.	хорошо	отлично	
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.1.	Обучающийся должен знать: криптографические алгоритмы в современных программных комплексах и корректность их применения.	Отсутствие представления о криптографических алгоритмах в современных программных комплексах и корректности их применения.	Неполные представления о криптографических алгоритмах в современных программных комплексах и корректности их применения.	Сформированные, но содержащие отдельные пробелы представления о криптографических алгоритмах в современных программных комплексах и корректности их применения.	Сформированные систематические представления о криптографических алгоритмах в современных программных комплексах и корректности их применения.	Доклады
	ОПК-9.2.	Обучающийся должен уметь: устанавливать причины, цели и условия изменения свойств	Отсутствие умений устанавливать причины, цели и условия изменения свойств	В целом успешное, но не систематическое умение устанавливать причины, цели и условия	В целом успешное, но содержащее отдельные пробелы в умении устанавливать	Сформированное умение устанавливать причины, цели и условия изменения свойств	Практические работы

		алгоритмов и протоколов применительно к конкретным условиям.	алгоритмов и протоколов применительно к конкретным условиям.	изменения свойств алгоритмов и протоколов применительно к конкретным условиям.	причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям.	алгоритмов и протоколов применительно к конкретным условиям.	
	ОПК-9.3.	Обучающийся должен владеть: навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	Отсутствие навыков реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	В целом успешное, но непоследовательное владение навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	В целом успешное, но содержащее отдельные пробелы владения навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	Успешное и последовательное владение основными навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	Тестирование

2. Оценочные средства, необходимые для оценки результатов обучения по дисциплине (модулю)

Перечень тем докладов

Перечень тем докладов для оценки уровня сформированности компетенции **ОПК-9** на этапе «Знания»

1. Важность проблемы информационной безопасности.
2. Жизненный цикл информационных систем.
3. Доктрина информационной безопасности РФ.
4. Троянская программа.
5. Методы морально психического воздействия.
6. Вредоносное ПО.
7. История «Оранжевой книги».
8. Организационно-правовые методы и средства защиты информации.
9. Инженерно-технические методы и средства защиты информации.
10. Программные и программно-аппаратные методы и средства защиты информации.
11. Методы защиты от несанкционированного доступа к информации.
12. Администрирование средств безопасности.
13. Модель политики безопасности.

Практические работы

Перечень лабораторных работ для оценки уровня сформированности компетенции **ОПК-9** на этапе «Умения»

Тема 1.3 Методы защиты от несанкционированного доступа к информации

Студентами готовятся доклады с презентацией по заявленным темам:

1. парольная аутентификация,
2. модель "рукопожатия",
3. биометрические характеристики,
4. клавиатурный почерк и роспись мышью.

Тема 1.4 Комплексная система защиты информации

Студентами готовятся доклады с презентацией по заявленным темам;

1. организационные-- правовые методы и средства защиты информации;
2. инженерно-технические методы и средства защиты информации;
3. программные и программно-аппаратные методы и средства защиты информации;
4. требования к комплексной системы защиты информации;

Тема 2.1 Требования к алгоритмам симметричного шифрования. Режимы выполнения

Изучение основных криптографических примитивов происходит на алгоритмах донаучного периода:

1. Алгоритм Цезаря
2. Алгоритм Гронефельда
3. Табличная подстановка.

Тема 2.2 Алгоритмы симметричного шифрования ГОСТ 28147-89

Выполните первый цикл алгоритма шифрования ГОСТ 28147 89 в режиме простой замены. Для получения 64 бит исходного текста используйте 8 первых букв из своих данных: Фамилии Имени Отчества. Для получения ключа (256 бит) используют текст, состоящий из 32 букв. Первый подключ содержит первые 4 буквы.

Пример выполнения заданий

Выполните первый цикл алгоритма шифрования ГОСТ 28147-89 в режиме простой замены. Для получения 64 бит исходного текста используйте 8 первых букв из своих данных: Фамилии Имени Отчества. Для получения ключа (256 бит) используют текст, состоящий из 32 букв. Первый подключ содержит первые 4 буквы.

Исходные данные для зашифрования: КОЗИНА Г

Для ключа возьмем последовательность состоящую из 32 букв:

АЛИНа пошла в лес собирать грибы

Для первого подключа X используем первые 4 буквы ключа: АЛИН.

исходный текст

К	11001010
О	11001110
З	11000111
И	11001000
Н	11001101
А	11000000
пробел	00100000
Г	11000011

первый подключ X0

А	1100000
	0
Л	1100101
	1
И	1100100
	0
Н	1100110
	1

Таким образом, первые 64 бита определяют входную последовательность

L0: 11001010 11001110 11000111 11001000

R0: 11001101 11000000 00100000 11000011

следующие 32 бита определяют первый подключ

X0: 11000000 11001011 11001000 11001101

I. Найдем значение функции преобразования f(R0,X0) (см. Приложение А)

1). Вычисление суммы R0 и X0 по mod 2^{32}

R0: 1100 1101 1100 0000 0010 0000 1100 0011

X0: 1100 0000 1100 1011 1100 1000 1100 1101

1000 1110 1000 1011 1110 1001 1001 0000

2). Преобразование в блоке подстановки

Результат суммирования R0+X0 по mod 2^{32}

1000 1110 1000 1011 1110 1001 1001 0000

преобразуем в блоке подстановки (см. Приложение В). Для каждого 4-битного блока вычислим его адрес в таблице подстановки. Номер блока соответствует номеру столбца, десятичное значение блока соответствует номеру строки в таблице. Таким образом, 5-тый блок (1011) заменяется заполнением 11-ой строки и пятого столбца в таблице подстановки (1110).

номера блоков

8	7	6	5	4	3	2	1
1000	1110	1000	1011	1110	1001	1001	0000

соответствующие номера строк в таблице подстановки

8 14 8 11 14 9 9 0

заполнение

9 2 3 14 5 15 3 4

результат

1001 0010 0011 1110 0101 1111 0011 0100

3). Циклический сдвиг результата п.2 на 11 бит влево

1111 0010 1111 1001 1010 0100 1001 0001

Таким образом, нашли значение функции f (R0,X0):

1111 0010 1111 1001 1010 0100 1001 0001

II. Вычисляем R1= f(R0,X0) ⊕L0.

Результат преобразования функции f(R0,X0) складываем с L0 по mod2:

L0:	1100 1010	1100 1110	1100 0111	1100 1000
f(R0,X0):	1111 0010	1111 1001	1010 0100	1001 0001
R1:	0011 1000	0011 0111	0110 0011	0101 1001

Тема 3.1 Алгоритм шифрования RSA

Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из первой сотни. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

Пример выполнения заданий

Сгенерируйте откры-тый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из первой сотни. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

I.Генерация ключей.

Выберем два простых числа $p = 13$ и $q = 19$ (см. Приложение Д).

Тогда модуль

$n = pq = 13*19 = 247$

и функция Эйлера

$\varphi(n) = (p-1)(q-1) = 12*18 = 216$.

Закрытый ключ d выбираем из условий $d < \varphi(n)$ и d взаимно просто с $\varphi(n)$, т.е. d и $\varphi(n)$ не имеют общих делителей.

Пусть $d = 25$.

Открытый ключ e выбираем из условий $e<\varphi(n)$ и $de=1 (mod\ \varphi(n))$: $e<216$,

$25e=1 (mod\ 216)$.

Последнее условие означает, что число $25e-1$ должно делиться на 216 без остатка.

Таким образом, для определения e нужно подобрать такое число k, что

$25e-1 = 216k$.

При $k=14$ получаем $25e=3024+1$ или

$e=121$.

В нашем примере

(121, 247) – открытый ключ,

(25, 247) – секретный ключ.

II. Шифрование.

Представим шифруемое сообщение «КГЛ» как последова-тельность целых чисел. Пусть буква «К» соответствует числу 12, буква «Г» - числу 4 и буква «Л» - числу 13.

Зашифруем сообщение, используя открытый ключ (121, 247):

$C_1 = (12^{121}) \bmod 247 = 12$

$C_2 = (4^{121}) \bmod 247 = 199$

$C_3 = (13^{121}) \bmod 247 = 91$

Таким образом, исходному сообщению (12, 4, 13) соответствует криптограмма (12, 199, 91).

III. Расшифрование

Расшифруем сообщение (12, 199, 91), пользуясь секретным ключом (25,247):

$M_1 = (12^{25}) \bmod 247 = 12$

$M_2 = (199^{25}) \bmod 247 = 4$

$M_3 = (91^{25}) \bmod 247 = 13$

В результате расшифрования было получено исходное сообщение (12, 4, 13), то есть "КГЛ".

Тема 3.2 Функция хеширования

Найти хеш–образ своей Фамилии, используя хеш–функцию $H_i = (H_{i-1} + M_i)^2 \bmod n$, где n = pq.

Пример выполнения заданий

Найти хеш–образ своей Фамилии, используя хеш–функцию $H_i = (H_{i-1} + M_i)^2 \bmod n$, где n = pq, p, q взять из Задания №3.

Хешируемое сообщение «КОЗИНА». Возьмем два простых числа p=13, q=19 (см. Приложение Е). Определим $n=pq$=13*19=247. Вектор инициализации H_0 выберем равным 8 (выбираем случайным образом). Слово «КОЗИНА» можно представить последовательностью чисел (12, 16, 9, 10, 15, 1) по номерам букв в алфавите. Таким образом,

n=247, H_0=8, M_1=12, M_2=16, M_3=9, M_4=10, M_5=15, M_6=1.

Используя формулу

$$H_i = (H_{i-1} + M_i)^2 \bmod n,$$

получим хеш-образ сообщения «КОЗИНА»:

$H_1=(H_0+M_1)^2 \bmod n = (8+12)^2 \bmod 247 = 400 \bmod 247 = 153$

$H_2=(H_1+M_2)^2 \bmod n = (153+16)^2 \bmod 247 = 28561 \bmod 247 = 156$

$H_3=(H_2+M_3)^2 \bmod n = (156+9)^2 \bmod 247 = 27225 \bmod 247 = 55$

$H_4=(H_3+M_4)^2 \bmod n = (55+10)^2 \bmod 247 = 4225 \bmod 247 = 26$

$H_5=(H_4+M_5)^2 \bmod n = (26+15)^2 \bmod 247 = 1681 \bmod 247 = 199$

$H_6=(H_5+M_6)^2 \bmod n = (199+1)^2 \bmod 247 = 40000 \bmod 247 = 233$

В итоге получаем хеш-образ сообщения «КОЗИНА», равный 233.

Тема 3.4. Электронная цифровая подпись

Используя хеш-образ своей Фамилии, вычислите электронную цифровую подпись по схеме RSA.

Схема подписи RSA

Криптосистема с открытым ключом RSA может использоваться не только для шифрования, но и для построения схемы цифровой подписи.

Для создания подписи сообщения M отправитель

1. вычисляет хеш-образ $r = h(M)$ сообщения M с помощью некоторой хеш-функции;
2. зашифровывает полученный хеш-образ r на своем секретном ключе (d,n), т.е. вычисляет значение $s = r^d \bmod n$, которое и является подписью.

Для проверки подписи получатель

1. расшифровывает подпись s на открытом ключе (e,n) отправителя, т.е. вычисляет $r' = s^e \bmod n$ и таким образом восстанавливает предполагаемый хеш-образ r' сообщения M;
2. вычисляет хеш-образ $h(M) = r$ сообщения M с помощью той же самой хеш-функции, которую использовал отправитель;
3. сравнивает полученные значения r и r'. Если они совпадают, то подпись правильная, отправитель действительно является тем, за кого себя выдает, и сообщение не было изменено при передаче.

Пример выполнения заданий

Используя хеш-образ своей Фамилии, вычислите электронную цифровую подпись по схеме RSA.

Пусть хеш-образ Фамилии равен 233, а закрытый ключ алгоритма RSA равен (25, 247). Тогда электронная цифровая подпись сообщения, состоящего из Фамилии, вычисляется по правилу (см. Приложение Ж)

$s = 233^{25} \bmod 247 = 168.$

Для проверки ЭЦП, используя открытый ключ (121, 247), найдем

$H = 168^{121} \bmod 247 = 233.$

Поскольку хеш-образ сообщения совпадает с найденным значением H, то подпись признается подлинной.

Тестовые задания

Перечень тестовых вопросов для оценки уровня сформированности компетенции **ОПК-9** на этапе «Владения»

1. **Алгоритм подстановки заключается в**
   a) Замене символов шифруемого текста другими символами, взятыми из одного или нескольких алфавитов
   b) Перестановке символов шифруемого текста по определенным правилам внутри шифруемого блока символов
   c) посимвольном сложении элементов двух последовательностей – исходного текста и ключевой последовательности
2. **Выберите верное утверждение**
   a) Линейные преобразования являются стойкими
   b) Линейные шифры могут быть вскрыты путем подачи на вход векторов, отличающихся в одном бите
   c) В нелинейном преобразовании изменение одного бита в исходном тексте вызывает изменение одного бита шифрованного текста
3. **Комбинированное использование нескольких различных способов шифрования**
   a) Повышает стойкость шифрования
   b) Понижает стойкость шифрования
   c) Не влияет на стойкость шифрования
4. **В алгоритмах симметричного шифрования секретным должен быть**
   a) Ключ
   b) Весь алгоритм секретного шифрования
   c) Отдельные элементы алгоритма симметричного шифрования (такие как S-box)
5. **Двойной DES не используется, потому что**
   a) Недостаточна длина ключа
   b) Существует атака «встреча посередине», которая позволяет снизить стойкость алгоритма до стойкости простого DES
   c) Слишком увеличивается скорость вычислений
6. **Сеть Фейштеля широко используется при разработке алгоритмов симметричного шифрования, потому что**
   a) Увеличение количества раундов сети Фейштеля приводит к увеличению стойкости алгоритма шифрования
   b) Для обратимости сети Фейштеля не требуется обратимость образующей функции F

c) Сеть Фейштеля достаточно компактна и проста в реализации
d) Других способов реализации алгоритмов симметричного шифрования не существует

7. С увеличением количества раундов стойкость алгоритма

a) Увеличивается
b) Уменьшается
c) Не изменяется

8. В алгоритмах симметричного шифрования используются только следующие операции

a) Операции перестановки и сдвига
b) S-Box и побитовое исключающее или (XOR)
c) Любые из перечисленных выше операций, а также многие другие

9. Криптографическая система считается вычислительно безопасной, если

a) Невозможно расшифровать сообщение без знания ключа шифрования
b) Цена расшифровки сообщения больше цены самого сообщения
c) Время, необходимое для расшифровки сообщения, больше времени жизни сообщения

10. Зависимость между ключами шифрования и дешифрования в алгоритмах симметричного шифрования должна быть следующей

a) Ключи шифрования и дешифрования должны в точности совпадать
b) Ключ дешифрования должен легко получаться из ключа шифрования
c) Между ключами шифрования и дешифрования не должно быть никакой зависимости

11. Криптоанализ – это процесс, при котором

a) Зная зашифрованное сообщение, пытаются узнать незашифрованное сообщение
b) Зная одну или несколько пар (незашифрованное сообщения, зашифрованное сообщение), пытаются узнать ключ
c) Изменяют передаваемое зашифрованное сообщение

12. Выберите правильное утверждение

a) В основе алгоритма DES лежит сеть Фейштеля
b) В алгоритме DES используется S-boxes
c) В алгоритме DES используется умножение по 8 семестр $2^{16} + 1$

13. Различные режимы шифрования предназначены для того, чтобы

a) Обеспечить возможность обрабатывать сообщения, длина которых больше длины шифрования
b) Обеспечить возможность обрабатывать сообщения порциями, меньшими, чем длина блока шифрования
c) Увеличить стойкость алгоритма

14. Последовательность случайных чисел должна быть

a) Монотонно возрастающей
b) Непредсказуемой
c) Иметь равномерное распределение

15. Выберите правильно высказывание

a) Алгоритм ГОСТ 28147 использует постоянные S-boxes
b) Алгоритм ГОСТ 28147 использует переменные S-boxes, зависящие от ключа

c) Алгоритм ГОСТ 28147 не использует S-boxes

16. Длина ключа в алгоритме ГОСТ 28147

a) 56 бит
b) 128 бит
c) 256 бит
d) 448 бит

17. Режим CBC используется для того, чтобы

a) Одинаковые незашифрованные блоки преобразовывались в различные зашифрованные блоки
b) Не было необходимости разбивать сообщение на целое число блоков лостаточно большой длины
c) Увеличить скорость шифрования

18. Для создания подписи следует использовать

a) Свой открытый ключ
b) Закрытый ключ получателя
c) Свой закрытый ключ

19. Задачей факторизации числа является

a) разложение числа на простые сомножители
b) нахождение степени, в которую следует возвести целое число для получения заданного целого числа
c) нахождение степени, в которую следует возвести простое число для получения заданного целого числа

20. Функция Эйлера – это

a) Число положительных чисел, меньших n и взаимно простых с n
b) $a^{\phi(n)} = 1 \; mod \; n$ для всех взаимнопростых a и n, где $\phi(n)$-число положительных чисел, меньших n и взаимно простых с n
c) $a^{n-1} = 1 \; mod \; n$ Если n-простое

21. Для проверки подписи следует использовать

a) Свой открытый ключ
b) Закрытый ключ получателя
c) Свой закрытый ключ

22. Задачей дискретного логарифмирования является

a) Разложение числа на простые сомножители
b) Нахождение степени, в которую следует возвести целое число для получения заданного целого числа
c) Нахождение степени, в которую следует возвести простое число для получения заданного целого числа

23. Теорема Эйлера формулируется следующим образом

a) Если p- простое, то число положительных чисел, меньших p и взаимно простых с p, равно $p - 1$
b) $a^{\phi(n)} = 1 \; mod \; n$ для всех взаимнопростых a и n, где $\phi(n)$ – число положительных чисел, меньших n и взаимно простых с n
c) $a^{n-1} = 1 \; mod \; n$ Если n – простое

24. Для шифрования сообщения следует использовать

a) Свой открытый ключ

b) открытый ключ получателя
c) Свой закрытый ключ

25. Аутентификация сторон в алгоритме Диффи-Хеллмана необходима, потому что

a) В противном случае возможен взлом задачи дискретного логарифмирования
b) В противном случае возможен взлом задачи факторизации числа
c) В противном случае нарушитель может заменить пересылаемые открытые ключи на свой открытый ключ

26. Криптография с использованием эллиптических кривых дает преимущества по сравнению с другими алгоритмами, потому что

a) Принципиально не может быть взломана
b) Обеспечивает эквивалентную защиту при меньшей длине ключа
c) Проще в реализации

27. Задача, которую должен решить атакующий, формулируется следующим образом

a) Даны точки P и Q на эллиптической кривой $E_p(a,b)$. Необходимо найти коэффициент k<p такой, что $P = k \times Q$
b) Даны точка Q на эллиптической кривой $E_p(a,b)$ и целое число k. Необходимо найти такую точку P на кривой, чтобы $P = k \times Q$
c) Даны точка P на эллиптической кривой $E_p(a,b)$ и целое число k. Необходимо найти такую точку Q на кривой, чтобы $P = k \times Q$

28. Шифрование/дешифрование с использованием эллиптических кривых выполняется следующим образом:

a) Участник A выбирает случайное целое положительное число k и вычисляет зашифрованное C_m являющееся точкой на эллиптической кривой $C_m = \{k \times F, P_m + k \times P_8\}$
b) Участник A выбирает случайное целое положительное число k и вычисляет зашифрованное C_m являющееся точкой на эллиптической кривой $C_m = \{P_m + k \times P_8\}$
c) Участник A выбирает случайное целое положительное число k и вычисляет зашифрованное C_m являющееся точкой на эллиптической кривой $C_m = \{k \times G\}$

29. Уравнение эллиптической кривой в общем случае имеет вид

a) $Y^2+axy+by=x^3+cx^2+dx+c$
b) $Y=ax^2+bx+c$
c) $Y^2=ax^2+bx+c$

30. При использовании криптографии на эллиптических кривых в качестве аналога алгоритма Диффи-Хеллмана в уравнении $P_A = \boldsymbol{n_A \times G}$

a) Открытым ключом участника A является P_A, закрытым ключом участника A является n_A
b) Открытым ключом участника A является n_A, закрытым ключом участника A является P_A
c) Открытым ключом участника A является P_A, закрытым ключом участника A является Q

31. Подпись с использование эллиптических кривых имеет

a) Один компонент
b) Два компонента

c) Три компонента

32. Выберите правильное утверждение

a) В криптографии с использованием эллиптических кривых все значения вычисляются по 8 семестр n, где n-произведение двух простых чисел
b) В криптографии с использованием эллиптических кривых все значения вычисляются по 8 семестр простого числа p
c) В криптографии с использованием эллиптических кривых все значения вычисляются по 8 семестр произвольного числа p

33. Нулевым элементом эллиптической кривой считается точка O, которая

a) Имеет координаты (0,0)
b) Является бесконечно удаленной точкой, в которой сходятся все вертикальные прямые
c) Имеет координаты (0,1) или (1,0)

34. Элементами эллиптической кривой являются пары неотрицательных целых чисел, которые меньше простого числа p и удовлетворяют частному виду эллиптической кривой

a) $y \equiv x^2 + ax + b(mod\ p)$
b) $y^2 \equiv x^3 + ax + b(mod\ p)$
c) $y^2 \equiv x^3 + ax^2 + b(mod\ p)$

35. Хэш-функции предназначены для

a) Сжатия сообщения
b) Получения «отпечатков пальцев» сообщения
c) Шифрования сообщения

36. Побитовый XOR блоков нельзя считать криптографической хэш-функцией, потому что

a) Противник может легко подобрать другое сообщение, имеющее тот же хэш=код
b) Побитовый XOR плохо защищает от случайного сбоя
c) Побитовый XOR требует сложных вычислений

37. Выберите правильное высказывание

a) Каждая элементарная функция в алгоритме MD5 получает одно 32-битное слово на входе и создает три 32-битных слова на выходе
b) Каждая элементарная функция в алгоритме MD5 получает три 32-битных слова на входе и создает три 32-битных слова на выходе
c) Каждая элементарная функция в алгоритме MD5 получает три 32-битное слово на входе и создает одно 32-битное слово на выходе

38. Выходом хэш-функции является

a) Сообщение той же длины, что и входное сообщение
b) Сообщение фиксированной длины
c) Сообщение меньшей длины

39. Сильная хэш-функция отличается от слабой наличием следующего свойства

a) У сильной хэш-функции для любого данного значения хэш-кода h вычислительно невозможно найти M такое, что H(M)=h
b) У сильной хэш-функции вычислительно невозможно найти произвольную пару (x,y) такую, что H(y)=H(x)

c) У сильной хэш-функции для любого данного x вычислительно невозможно найти y ≠x, что H(y)=H(x)

40. Хэш-функция должна обладать следующими свойствами:

a) Для любого данного значения хэш-кода h вычислительно невозможно найти M такое, что H(M)=h
b) Хэш-функция H должна применяться к блоку данных фиксированной длины
c) Хэш-функция H создает выход фиксированной длины

41. Длина хэш-кода, создаваемого хэш-функцией MD5, равна

a) 128 бит
b) 160 бит
c) 512 бит

42. Подпись называется рандомизированной, если

a) Для разных сообщений с использованием одного и того же закрытого ключа при каждом подписывании создаются разные подписи
b) Для одного и того же сообщения с использованием одного и того же закрытого ключа при каждом подписывании создаются разные подписи
c) Для одного и того же сообщения с использованием разных закрытых ключей при каждом подписывании создаются разные подписи

43. Подпись, создаваемая ГОСТ 3410, является

a) Детерминированной
b) Рандомизированной

44. В DSS используется следующая хэш-функция

a) MD5
b) SHA-1
c) SHA-2

45. Подпись называется детерминированной, если

a) Для одного и того сообщения с использованием разных закрытых ключей при каждом подписывании создается одна и та же подпись
b) Для разных сообщений с использованием одного и того же закрытого ключа при каждом подписывании создается одна и та же подпись
c) Для одного и того сообщения с использованием одного и того же закрытого ключа при каждом подписывании создается одна и та же подпись

46. Подпись, создаваемая DSS, является

a) Детерминированной
b) Рандомизированной

47. Выберите правильное утверждение

a) Цифровая подпись обеспечивает аутентификацию сообщения
b) Цифровая подпись обеспечивает конфиденциальность сообщения
c) Цифровая подпись обеспечивает целостность сообщения

48. Выберите правильно утверждение

a) Подпись должна быть битовым образцом, который зависит от подписывающего сообщения
b) Подпись должна использовать некоторую уникальную информацию отправителя для предотвращения подделки или отказа
c) Подпись должна обеспечивать невозможность просмотра сообщения

49. Подпись создаваемая RSA является

a) Детерминированной
b) Рандомизированной

50. В стандарте ГОСТ 3410 используется следующая хэш-функция

a) MD5
b) SHA-1
c) ГОСТ 3411

Вопросы к зачету:

1. Основные примитивы криптографии. Подстановки. Перестановки. Гаммирование.
2. Основные примитивы криптографии. Нелинейное преобразование с помощью S-боксов. Комбинированные методы.
3. Основные алгоритмы донаучного периода.
4. Первые криптографические устройства.
5. Алгоритмы симметричного шифрования. Криптография.
6. Сеть Фейштеля.
7. Алгоритмы симметричного шифрования. Криптоанализ.
8. Используемые критерии при разработке алгоритмов симметричного шифрования.
9. Алгоритм DES.
10. Алгоритм ГОСТ 28147.
11. Алгоритм IDEA. Сравнительный анализ с алгоритмом DES.
12. Режимы выполнения алгоритмов симметричного шифрования.
13. Создание случайных чисел.
14. Алгоритмы ассиметричного шифрования. Основные требования к алгоритмам ассиметричного шифрования.
15. Алгоритм RSA.
16. Хэш-функции. Требования к хэш-функциям.
17. Простые хэш-функции.
18. Хэш-функция MD5.
19. Электронная цифровая подпись. Требования к цифровой подписи.
20. Прямая и арбитражная цифровые подписи.
21. Стандарт цифровой подписи DSS.
22. Стандарт цифровой подписи ГОСТ 3410.
23. Криптография с использованием эллиптических кривых. Математические понятия.
24. Аналог алгоритма Диффи-Хеллмана обмена ключами.
25. Алгоритм цифровой подписи на основе эллиптических кривых ECDSA.
26. Шифрование и дешифрование с использованием эллиптических кривых.
27. Использование криптографических алгоритмов в системах защиты информации.

3. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю), описание шкал оценивания

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1				
Текущий контроль			**0**	**20**
Выступление с докладом	10	1	0	10

Выполнение практических работ	10	1	0	10
Рубежный контроль			**0**	**15**
Коллоквиум	15	1	0	15
Модуль 2				
Текущий контроль			**0**	**20**
Выполнение практических работ	5	3	0	15
СРС	5	1	0	5
Рубежный контроль			**0**	**15**
Тестирование	15	1	0	15
Итоговый контроль				**30**
Диф.зачет				30
Итого				**100**
Штрафные баллы за пропущенные занятия				
1. Лекционные занятия				**-6**
2. Практические занятия				**-10**
Поощрительные баллы				
Участие в конференциях с публикацией тезисов/статей				**10**

Объем и уровень сформированности компетенций целиком или на различных этапах у обучающихся оцениваются по результатам текущего контроля количественной оценкой, выраженной в рейтинговых баллах. Оценке подлежит каждое контрольное мероприятие.

При оценивании сформированности компетенций применяется четырехуровневая шкала «неудовлетворительно», «удовлетворительно», «хорошо», «отлично».

Максимальный балл по каждому виду оценочного средства определяется в рейтинг-плане и выражает полное (100%) освоение компетенции.

Уровень сформированности компетенции «хорошо» устанавливается в случае, когда объем выполненных заданий соответствующего оценочного средства составляет 80 - 100%; «удовлетворительно» – выполнено 40 - 80%; «неудовлетворительно» – выполнено 0 - 40%

Рейтинговый балл за выполнение части или полного объема заданий соответствующего оценочного средства выставляется по формуле:

$$\text{Рейтинговый балл} = k \times \text{Максимальный балл}$$
$$\text{Рейтинговыйбалл} = \text{k} \cdot \text{Максимальныйбалл},$$

где k = 0,2 при уровне освоения «неудовлетворительно», $\text{k} = 0{,}6$ k = 0,4 при уровне освоения «удовлетворительно», k = 0,8 при уровне освоения «хорошо» и k = 1 при уровне освоения «отлично».

Оценка на этапе промежуточной аттестации выставляется согласно Положению о модульно-рейтинговой системе обучения и оценки успеваемости студентов БашГУ:

- отлично - при накоплении от 80 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
- хорошо - при накоплении от 60 до 79 рейтинговых баллов,
- удовлетворительно - при накоплении от 45 до 59 рейтинговых баллов,
- неудовлетворительно - при накоплении менее 45 рейтинговых баллов.

Результаты обучения по дисциплине (модулю) у обучающихся оцениваются по итогам текущего контроля количественной оценкой, выраженной в рейтинговых баллах. Оценке подлежит каждое контрольное мероприятие.

При оценивании сформированности компетенций применяется четырехуровневая шкала «неудовлетворительно», «удовлетворительно», «хорошо», «отлично».

Максимальный балл по каждому виду оценочного средства определяется в рейтинг-плане и выражает полное (100%) освоение компетенции.

Уровень сформированности компетенции «хорошо» устанавливается в случае, когда объем выполненных заданий соответствующего оценочного средства составляет 80-100%; «удовлетворительно» – выполнено 40-80%; «неудовлетворительно» – выполнено 0-40%

Рейтинговый балл за выполнение части или полного объема заданий соответствующего оценочного средства выставляется по формуле:

Рейтинговый балл = k × Максимальный балл,

где k = 0,2 при уровне освоения «неудовлетворительно», k = 0,4 при уровне освоения «удовлетворительно», k = 0,8 при уровне освоения «хорошо» и k = 1 при уровне освоения «отлично».

Оценка на этапе промежуточной аттестации выставляется согласно Положению о модульно-рейтинговой системе обучения и оценки успеваемости студентов БашГУ:
На дифференцированном зачете выставляется оценка:

• отлично - при накоплении от 80 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
• хорошо - при накоплении от 60 до 79 рейтинговых баллов,
• удовлетворительно - при накоплении от 45 до 59 рейтинговых баллов,
• неудовлетворительно - при накоплении менее 45 рейтинговых баллов.

При получении на экзамене оценок «отлично», «хорошо», «удовлетворительно», на зачёте оценки «зачтено» считается, что результаты обучения по дисциплине (модулю) достигнуты и компетенции на этапе изучения дисциплины (модуля) сформированы.