МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ

ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Фонды оценочных средств по дисциплине

«КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

1. Формируемые дисциплиной компетенции

ОПК.9 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Индикаторы:

ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации

ОПК.9.2 Анализирует возможности криптографических средств защиты информации

ОПК.9.3 Применяет методы и средства криптографической защиты информации для решения профессиональных задач

2. Планируемые результаты обучения

Коды индикаторов	Планируемый результат
ОПК.9.1	Знать основные методы и средства криптографической защиты информации. Уметь находить информацию о существующих методах и средствах криптографической защиты информации. Владеть навыками поиска, анализа и обобщения информации о существующих методах и средствах криптографической защиты информации.
ОПК.9.2	Знать существующие криптографические средства защиты информации. Уметь анализировать возможности криптографических средств защиты информации. Владеть навыками анализа при выборе криптографических средств защиты информации при решении практических заданий..
ОПК.9.3	Знать существующие средства криптографической защиты информации. Уметь делать выбор средств криптографической защиты информации в соответствии с целями профессиональных задач, и обосновывать его. Владеть навыками применения методов и средств криптографической защиты информации для решения профессиональных задач.

3. Спецификация теста

Тест по дисциплине «Криптографические методы защиты информации» представляет собой перечень примерных вопросов, предлагаемых студентам с учетом тем и заданий контрольных мероприятий, предусмотренных по дисциплине.

Тест по дисциплине «Криптографические методы защиты информации», вариант 1.

1 Какое количество ключей необходимо для взлома DES методом грубой силы?

А) 2^{54} В) 2^{128}

Б) 2^{55} Г) 2^{46}

2 При каком режиме шифрования с использованием шифра «Магма» об исходном тексте сохраняется наибольшее количество информации?

А) CBC В) ECB

Б) OFB Г) CFB

3 Шифр Цезаря является:

А) одноразовым шифром Б) шифром сложной замены В) шифром простой замены Г) шифром перестановки

4 Какой метод не используют при атаке на алгоритмы шифрования, в основе которых лежит сеть Фейстеля?

А) линейный криптоанализ В) дифференциальный криптоанализ

Б) дискретное логарифмирование Г) метод грубой силы

5 В алгоритме шифрования «Кузнечик» функция S-блока представляет собой:

А) функцию перестановки В) функцию сложения по модулю 2

Б) хеш-функцию Г) функцию подстановки

6 При использовании аффинного преобразован ия $aT+b$ (mod N) на коэффициенты a и b накладываются ограничения:

А) b взаимнопростое с N, a и b меньше N В) a взаимнопростое с N, a и b меньше N

Б) a и b любые Г) a и b меньше N

7 К какому классу симметричного шифрования относится шифр Плейфера?

А) однозвучный В) одноалфавитный

Б) это не симметричный шифр Г) полиграммный

8 Протокол Kerberos применяется для аутентификации и распределения ключей ... шифрования:

А) симметричного В) асимметричного

Б) открытого Г) тройного

9 При симметричном шифровании ключ:

А) одинаков для отправителя и получателя и сохраняется в тайне обеими сторонами

В) передается по открытому (незащищенному каналу)

Б) используется два ключа, открытый и зарытый

Г) шифрования знает только отправитель, а дешифрования только получатель

10 Аутентификация основе симметричных криптосистем :

А) невозможна

В) существует и широко используется

Б) возможна только в паре с критосистемой с открытым ключом

Г) возможна, но не используется из-за сложности ее приенения

11 Расшифровать шифротекст RSA 4051753, зная открытый ключ {3, 9173503}

А) 111

В) 11

Б) 11111

Г) 111111

12 Какие данные не входят в сертификат, используемый в инфраструктуре открытых ключей

А) закрытый ключ пользователя

В) данные о пользователе

Б) открытый ключ пользователя

Г) Время действия сертификата

13 Что используется для создания цифровой по дписи Алисой при пересылке сообщения Бобу:

А) закрытый ключ Алисы

В) закрытый ключ Боба

Б) открытый ключ Алисы

Г) открытый ключ Боба

14 При шифровании с использованием схемы Эль-Гамаля в сравнении $g^x=y\ (modp)$ параметр g это:

А) закрытый ключ

В) открытый ключ

Б) первообразный корень

Г) раундовый ключ

15 Какие действия можно производить используя криптосистемы, основанных на эллиптических кривых?

А) шифрование, аутентификацию, обмен ключами

Б) только аутентификацию

В) только шифрование и аутентификацию,

Г) только шифрование и обмен ключами

16 Для взлома шифра RSA достаточно (выберете неверное утверждение)

А) факторизовать модуль

Б) найти функцию Эйлера модуля

В) узнать закрытый ключ

Г) использовать парадокс дней рождений

17 К компонентам инфраструктуры открытых ключей PKI не относится

А) удостоверяющий центр

Б) репозиторий

В) конечный пользователь

Г) компьютерная сеть

18 Какие свойства информации, с точки зрения информационной безопасности, обеспечивает хеш сообщения?

А) целостность и неотказуемость

Б) доступность и неотказуемость

В) конфиденциальность и доступность

Г) конфиденциальность и неотказуемость

19 Для алгоритма Elliptic Curve Digital Signature Algorithm закрытым ключом будет:

А) точка на эллиптической кривой

Б) пара чисел (r,s)

В) натуральное число

Г) сама эллиптическая кривая

20 Для обмена ключами между Алисой и Бобом по протоколу **Диффи — Хеллмана** необходимо чтобы:

А) Алиса Боб имели закрытый канал связи

Б) Алиса и Боб имели каждый свой закрытый ключ

В) Необходим посредник

Г) Алиса и Боб имели каждый свой открытый ключ

Тест по дисциплине «Криптографические методы защиты информации», вариант 2.

1 Какую длину блока и длину ключа имеет шифр “Кузнечик” в соответствии с ГОСТ-34.12-18?

А) Длина блока 64 бит, длина ключа 256 бит.

В) Длина блока 128 бит, длина ключа 256 бит.

Б) Длина блока 64 бит, длина ключа 128 бит.

Г) Длина блока 128 бит, длина ключа 128 бит.

2 Какой из перечисленных ключей не является криптографическим?

А) Симметричный ключ

В) Асимметричный ключ

Б) Блочный ключ

Г) Сеансовый (сессионный) ключ

3 Какой из приведенных алгоритмов шифрования не является симметричным?

А) AES

В) DES

Б) Кузнечик

Г) RSA

4 На каких двух операциях основана SP-сеть?

А) Подстановка, перестановка

В) Сложение по модулю 2, преобразование многочленов над полем Галуа

Б) Сложение по модулю 2, подстановка над полем Галуа, перестановка

Г) Преобразование многочленов

5 Что из перечисленного не относится к компонентам инфраструктуры открытых ключей PKI?

А) Сертификат

В) Удостоверяющий центр

Б) Репозиторий

Г) Протокол TLS

6 При каком режиме шифрования с использованием шифра DES в исходном тексте сохраняется наибольшее количество информации?

А) CBC

В) ECB

Б) OFB

Г) CTR

7 Какое требование не предъявляется к криптографически стойким хеш-функциям?

А) Необратимость

В) Стойкость к коллизиям первого рода

Б) Недетерминированность

Г) Стойкость к коллизиям второго рода

8
Укажите алгоритм, в котором не используется преобразование S-блоков

А) AES Б) DES

В) RSA

Г) ГОСТ 38-12-2018 «Кузнечик»

9 Для чего нельзя использовать VPN? А) Обход ограничений доступа

Б) Объединение компьютеров в сеть

В) Создание защищенного канала между сегментом корпоративной сети и одиночным пользователем, работающим из дома.

Г) Для всего вышеперечисленного VPN использовать можно.

10 Укажите метод факторизации, который основан на поиске таких квадратов чисел, которые равны по модулю факторизуемому числу.

А) Метод квадратичного решета
Б) Метод Ленстры
В) Метод слепой подписи
Г) Перебор делителей

11 Укажите разновидность ЭЦП, особенностью которой является то, что подписывающая сторона не может точно знать содержимое подписываемого документа

А) Неоспоримая подпись
Б) Слепая подпись
В) Разовая подпись
Г) Доверенная подпись

12 Укажите метод криптоанализа, основанный на изучении преобразования разностей между шифруемыми значениями на различных раундах шифрования.

А) Бандитский криптоанализ
Б) Линейный криптоанализ
В) Дифференциальный криптоанализ
Г) Интерполяционный криптоанализ

13 К какому классу криптографических прото ко лов относится шифр “Кузнечик”?

А) Симметричный алгоритм блочного шифрования
Б) Асимметричный алгоритм блочного шифрования
В) Протокол разделения секрета
Г) Протокол групповой подписи

14 Какая из атак по сторонним каналам основан а на осуществлении различных воздействий на шифратор с целью возникновения искажения информации на некоторых этапах шифрования?

А) Атака по времени
В) Атака по ошибкам вычислений

Б) Атака по энергопотреблению

Г) Атака по электромагнитному излучению

15 Каким алгоритмом является алгоритм “Стрибог”, описанный в ГОСТ 34.11-2012?

А) Алгоритм блочного шифрования

В) Алгоритм формирования и проверки электронной цифровой подписи

Б) Алгоритм вычисления хэш-функции для любой последовательности двоичных символов

Г) Алгоритм обмена ключами

16 На какой вычислительно сложной задаче основан алгоритм RSA?

А) Факторизация больших чисел

В) Вычисление дискретных логарифмов в конечных полях

Б) Операции в группе точек эллиптических кривой, определённой над конечным простым полем

Г) Декодирование полных линейных кодов

17 Что, согласно ГОСТ 34.12-18, является изменяемым параметром в виде последовательности символов, определяющим криптографическое преобразование?

А) Шифр

В) Ключ

Б) Шифртекст

Г) Блок

18 К какому типу атак относится атака CRIME?

А) базовая

В) продвинутая

Б) брендовая

Г) атака по сторонним каналам

19 Какие атаки относят к базовым стратегиям?

А) FREAK

В) дифференциальный анализ

Б) DROWN

Г) брутфорс

20 Что не обеспечивает VPN?

А) Анонимность

В) Защиту от вредоносного ПО

Б) Шифрование

Г) Обход блокировок

Ключ к тесту

Вариант 1	Вариант 2
1 б	1 в
2 в	2 б
3 в	3 г
4 б	4 а
5 г	5 г
6 в	6 в
7 г	7 б
8 а	8 в
9 а	9 г
10 в	10 а
11 г	11 б
12 а	12 в
13 а	13 а
14 б	14 в
15 а	15 б
16 г	16 а
17 г	17 в
18 а	18 б
19 в	19 г
20 б	20 в