Минобрнауки России

Бузулукский гуманитарно-технологический институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
«Оренбургский государственный университет»

Кафедра педагогического образования

Фонд
оценочных средств

по дисциплине *«Защита компьютерных систем»*

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
09.03.04 Программная инженерия
(код и наименование направления подготовки)

Разработка программно-информационных систем
(наименование направленности (профиля) образовательной программы)

Квалификация
Бакалавр

Форма обучения
Заочная

Год набора 2024

Фонд оценочных средств предназначен для контроля знаний обучающихся по направлению подготовки *09.03.04 Программная инженерия* по дисциплине *«Защита компьютерных систем»*

Фонд оценочных средств рассмотрен и утвержден на заседании кафедры педагогического образования

наименование кафедры

протокол № 6 от 26.01.2024 г.

Декан факультета _____ О.Н. Григорьева
должность *подпись* *расшифровка подписи*

Исполнитель:
ст. преподаватель _____ С.А. Литвинова
должность *подпись* *расшифровка подписи*

Раздел 1. Перечень компетенций, с указанием этапов их формирования в процессе освоения дисциплины

Формируемые компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Виды оценочных средств/ шифр раздела в данном документе
ПК*-2: Способен использовать методы и инструментальные средства исследования объектов профессиональной деятельности	ПК*-2-В-6 Знает и применяет методы и инструментальные средства исследования информационной безопасности объектов профессиональной деятельности	**Знать:** методы и инструментальные средства исследования информационной безопасности объектов профессиональной деятельности; программно-аппаратные средства защиты	**Блок А –** задания репродуктивного уровня *Тестовые задания, вопросы для опроса*
		Уметь: применять методы и инструментальные средства исследования информационной безопасности объектов профессиональной деятельности и технологии обеспечения безопасности информации в компьютерных системах; разрабатывать компоненты программно-аппаратных средств защиты информации в процессе ее сбора, хранения, обработки, передачи и распространения в компьютерных системах	**Блок В –** задания реконструктивного уровня *Типовые задачи*
		Владеть: инструментами разработки программного обеспечения для реализации мер обеспечения безопасности	**Блок С –** задания практико-ориентированного и/или исследовательского уровня *Дискуссионные вопросы*

Раздел 2. Типовые контрольные задания и иные материалы, необходимые для оценки планируемых результатов обучения по дисциплине (оценочные средства). Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Блок А

А.0 Тестовые задания по дисциплине

1. Чем занимается криптография:
a) составлением алгоритмов шифрования информации;
b) составлением алгоритмов передачи информации;
c) составлением прикладных программ;
d) составлением инструментальных программ;

2. Процесс преобразования открытого текста в шифртекст называется:
a) Enciphering;
b) Deciphering;
c) Cryptanalysis;
d) Algorithm;

3. Процесс преобразования шифрованного текста в исходный называется:
a) Enciphering ;
e) Algorithm;
f) Deciphering;
g) Cryptanalysis;

4. Какая из перечисленных задач не относится к задачам криптографии:
a) Секретность;
b) Целостность;
c) Аутентификация;
d) Системность;

5. Выберите два основных типа криптографических алгоритмов:
a) Симметричные и асимметричные;
b) Симметричные и циклические;
c) Структурные и циклические;
d) Блочные и асимметричные;

6. В каких алгоритмах ключ расшифрования совпадает с ключом зашифрования:
a) Блочных;
b) Циклических;
c) Симметричных;
d) Асимметричных;

7. В современных шифрах применяется принцип:

a) Керкхоффса;
b) Хофмана;
c) Шенона;
d) Эль гаммеля;

8. К основным криптографическим протоколам не относят:
a) обмен ключами;
b) аутентификацию;
c) цифровую подпись;
d) датирование;

9. Что не относится к Сервисам безопасности:
a) идентификация и аутентификация;
b) Шифрование;
c) инверсия паролей;
d) контроль целостности;

10. Что не относится к разделам криптографии:
a) Симметричные криптосистемы;
b) Системы электронной подписи;
c) Управление передачей данных;
d) Управление ключами;

11. Какого шифра не существует:
a) Шифр Цезаря;
b) Шифр Кардано;
c) Шифр Трисемуса;
d) Шифр Хартли;

12. Набор простых логических правил, легко применимых на практике и позволяющих выявить отдельные изъяны криптографических протоколов:
a) Бан-логика;
b) Пан-логика;
c) Ран-логика;
d) Фан-логика;

13. Процесс подтверждения подлинности пользователя – это:
a) Идентификация;
b) Аутентификация;
c) Методология;
d) Интеграция;

14. Каким шифром является DES
a) Симметричным;
b) Асимметричным;
c) Блочным;
d) Каскадным;

14. Сколько ключей надо перебрать для взлома алгоритма шифрования DES, который имеет рабочую длину 56 бит:

a) 256
b) 25
c) 562
d) 26

15. Как по-другому называют ключ шифрования:
a) Сменный шифр;
b) Сменный элемент;
c) Сменная буква;
d) Сменный символ;

16. Каким шифром является RSA:
a) Симметричным;
b) Асимметричным;
c) Блочным;
d) Композиционным;

17. Что не относится к основным аппаратным средствам защиты информации:
a) пластиковые карты;
b) электронные замки;
c) магнитные карты;
d) видео карты;

А.1 Вопросы для опроса:

1 Раскрытие ключа шифрования без привлечения методов криптоанализа называется:

Ответ: Компрометацией

2. Исследование криптографических алгоритмов с целью оценки их стойкости и поиска слабых мест называется:

Ответ: Криптоанализом

3. От какого арабского слова происходит термин шифр?

Ответ: Цифра

4. Как переводится слово криптография?

Ответ: Тайнопись

5. Элемент, позволяющий выбрать одно конкретное преобразование из множества преобразований – это…

Ответ: Ключ

6. Криптографические устройства псевдослучайных чисел – это …

Ответ: Генератор

7. Последовательность шагов, которые предпринимают две или большое количество сторон для совместного решения задачи – это …

Ответ: Протокол

8. Какого типа существуют электронные подписи?

Варианты ответов: DSA; RSA.

9. Вирус, у которого каждая следующая копия в заражённых объектах отличается от предыдущих – это …

Ответ: Призрак

10. Исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения.

Ответ: Вирус

Блок В

В.1 Типовые задачи

Задание №1. Продемонстрировать шифрование методами Цезарь, Атбаш, Виженера.

Вариант ответа:

Дешифровать слово «ИНФОРМАТИКА» с помощью шифра Цезаря.

Ответ: ЛРЧСУПГХЛНГ

Дешифровать слово «ИНФОРМАТИКА» с помощью шифра Атбаш.

Ответ: ЦСКРОТЯМЦФЯ

Дешифровать слово «ИНФОРМАТИКА» с помощью таблицы Виженера, используя в качестве ключа слово «ДЕВА».

Ответ: ЕИТОМЗЮТЕЁЮ

Задание №2. Продемонстрировать алгоритм шифрования RSA.

Вариант ответа:

Зашифруем и расшифруем сообщение "CAB" по алгоритму RSA.

Выберем p=3 and q=11.

Определим n= 3*11=33.

Найдем (p-1)*(q-1)=20. Следовательно, d будет равно, например, 3: (d=3).

Выберем число e по следующей формуле: (e*3) mod 20=1. Значит e будет равно, например, 7: (e=7).

Представим шифруемое сообщение как последовательность чисел в диапазоне от 0 до 32. Буква A =1, B=2, C=3.

Теперь зашифруем сообщение, используя открытый ключ {7,33}

C1 = (3^7) mod 33 = 2187 mod 33 = 9;

C2 = (1^7) mod 33 = 1 mod 33 = 1;

C3 = (2^7) mod 33 = 128 mod 33 = 29;

Теперь расшифруем данные, используя закрытый ключ {3,33}.

M1=(9^3) mod 33 =729 mod 33 = 3(C);

M2=(1^3) mod 33 =1 mod 33 = 1(A);

M3=(29^3) mod 33 = 24389 mod 33 = 2(B);

Данные расшифрованы.

Задание № 3. Шифр Эль-Гамаля. Алгоритм работы.

Вариант ответа:

Сообщение, предназначенное для шифрования, должно быть представлено в виде одного числа или набора чисел, каждое из которых меньше P. Пусть пользователь 1 хочет передать пользователю 2 сообщение m. В этом случае последовательность действий следующая.

1. Первый пользователь выбирает случайное число k, взаимно простое с P-1, и вычисляет числа

$$r = A^k \bmod P, \qquad e = m \times Y_2^k \bmod P$$

где Y_2 – открытый ключ пользователя 2. Число k держится в секрете.

2. Пара чисел (r, e), являющаяся шифротекстом, передается второму пользователю.
3. Второй пользователь, получив (r,e), для расшифрования сообщения вычисляет

$$m = e \times r^{P-1-X_2} \bmod P$$

где X_2 – закрытый ключ пользователя 2. В результате он получает исходное сообщение m.

Если злоумышленник узнает или перехватит P, A, Y_2, r, e, то он не сможет по ним раскрыть m. Это связано с тем, что противник не знает параметр k, выбранный первым пользователем для шифрования сообщения m.

Задание № 4. Определите последовательность из первых четырех чисел, вырабатываемых линейным конгруэнтным генератором псевдослучайных чисел для следующих параметров генератора: a =11, b =7 и c = 16 (k0 принять равным 0).

Вариант ответа:

k1 = 7; k2 = 4; k3=3; k4= 8

Задание № 5. Вычислите последовательность из четырех чисел, генерируемую по методу Фибоначчи с запаздыванием, начиная с ka, при следующих исходных данных: a = 4, b = 2, k0=01; k1=0.7; k2=0.3; k3=0.9.

Вариант ответа:

k4=0.8, k5=0.8, k6=0.5, k7=0.1

Блок С

Дискуссионные вопросы

1 Как работает система защиты электронной почты?

Предполагаемый ответ: Безопасность электронной почты обеспечивается за счет реализации трехэтапного процесса:

Аутентификация - Это процесс, в ходе которого проверяется, действительно ли человек, отправивший вам электронное сообщение, отправил его. Для этого необходимо сверить его имя и цифровую подпись со своими записями.

Шифрование - При этом данные шифруются таким образом, чтобы их могли прочитать только те, кто имеет доступ к закрытому ключу. Это означает, что никто другой не сможет прочитать данные, если только у него нет информации о вашем закрытом ключе.

Защита - Под защитой понимается процесс предохранения от фишинговых атак при нажатии на ссылки в электронных письмах, которые могут скомпрометировать вашу учетную запись или передать конфиденциальную информацию (например, пароли или номера кредитных карт).

2 Укажите типы защиты электронной почты.

Предполагаемый ответ: цифровая (масштабируемая), физическая (изменяемая) и процедурная.

3. Укажите основные объекты защиты информации при виртуализации.

Предполагаемый ответ: К основным объектам защиты при использовании технологий виртуализации относят:

- средства создания и управления виртуальной инфраструктурой;

- виртуальные вычислительные системы;

- виртуальные системы хранения данных;

- виртуальные каналы передачи данных;

- отдельные виртуальные устройства обработки, хранения и передачи данных;

- периметр виртуальной инфраструктуры.

4. Что является основными целями защиты информации в информационных системах?

Предполагаемый ответ: Целями защиты информации являются: предотвращение утечки информации по техническим каналам; предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в системах информатизации

5. Чем отличается квалифицированная электронная подпись от неквалифицированной?

Предполагаемый ответ: Отличие квалифицированной подписи от неквалифицированной заключается в том, что сертификат ключа проверки, квалифицированной ЭП выдается только аккредитованным удостоверяющим центром, а для его создания используются программные средства, соответствующие требованиям № 63-ФЗ «Об электронной подписи» и сертифицированные ФСБ России и другими ведомствами. Усиленная квалифицированная электронная подпись - наиболее защищенный вид электронной подписи.

Блок D

Экзаменационные вопросы.

1. Специфические особенности защиты информации в компьютерных сетях и современные средства защиты информации от НСД.
2. Методы и средства защиты информационно-программного обеспечения на уровне операционных систем.
3. Технологии идентификации и аутентификации в компьютерных сетях
4. Методы защиты внешнего периметра компьютерных сетей.
5. Защита информации при виртуализации.
6. Защищённости информационной системы
7. Понятие криптографии шифра.
8. Задачи и методы криптографии.
9. Основные криптографические протоколы.
10. Электронная цифровая подпись.
11. Задачи и методы криптографии
12. Электронная цифровая подпись
13. Программно-аппаратные средства.
14. Идентификация и аутентификация.
15. Сервисы управления доступом.
16. Протоколирование и аудит.
17. Вирусы. Виды вирусов.
18. Антивирусное программное обеспечение.
19. Защита системы электронной почты.
20. Основные аппаратные и программные средства защиты.

Описание показателей и критериев оценивания компетенций, описание шкал оценивания

4-балльная шкала	*Отлично*	*Хорошо*	*Удовлетворительно*	*Неудовлетворительно*
100 балльная шкала	*85-100*	*70-84*	*50-69*	*0-49*

4-балльная шкала	*Отлично*	*Хорошо*	*Удовлетворительно*	*Неудовлетворительно*
Бинарная шкала	*Зачтено*			*Не зачтено*

Оценивание выполнения практических заданий

4-балльная шкала	*Показатели*	*Критерии*
Отлично	*1. Полнота выполнения практического задания;* *2. Своевременность выполнения задания;* *3. Последовательность и рациональность выполнения задания;* *4. Самостоятельность решения.*	*Задание решено самостоятельно. При этом составлен правильный алгоритм решения задания, в логических рассуждениях, в выборе формул и решении нет ошибок, получен верный ответ, задание решено рациональным способом.*
Хорошо		*Задание решено с помощью преподавателя. При этом составлен правильный алгоритм решения задания, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор формул для решения; есть объяснение решения, но задание решено нерациональным способом или допущено не более двух несущественных ошибок, получен верный ответ.*
Удовлетворительно		*Задание решено с подсказками преподавателя. При этом задание понято правильно, в логическом рассуждении нет существенных ошибок, но допущены существенные ошибки в выборе формул или в математических расчетах; задание решено не полностью или в общем виде.*
Неудовлетворительно		*Задание не решено.*

Оценивание выполнения тестов

4-балльная шкала	*Показатели*	*Критерии*
Отлично	*1. Полнота выполнения тестовых заданий;* *2. Своевременность выполнения;*	*Выполнено 85 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос.*
Хорошо	*3. Правильность ответов на вопросы;* *4. Самостоятельность тестирования.*	*Выполнено 70% заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос; однако были допущены неточности в определении понятий, терминов и др.*
Удовлетворительно		*Выполнено 50 % заданий предложенного теста, в заданиях открытого типа дан неполный ответ на поставленный вопрос, в ответе не присутствуют доказательные примеры, текст со стилистическими и орфографическими ошибками.*
Неудовлетворительно		*Выполнено 49 % заданий предложенного теста, на поставленные вопросы ответ*

4-балльная шкала	Показатели	Критерии
		отсутствует или неполный, допущены существенные ошибки в теоретическом материале (терминах, понятиях).

Оценивание ответа на экзамене

4-балльная шкала	Показатели	Критерии
Отлично	*1. Полнота изложения теоретического материала;* *2. Полнота и правильность решения практического задания;* *3. Правильность и/или аргументированность изложения (последовательность действий);* *4. Самостоятельность ответа;* *5. Культура речи.*	*Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок.*
Хорошо		*Дан развернутый ответ на поставленный вопрос, где студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями.*
Удовлетворительно		*Дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа и решении практических заданий.*
Неудовлетворительно		*Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено,*

4-балльная шкала	*Показатели*	*Критерии*
		т.е студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.

Раздел 3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

В экзаменационный билет включено два теоретических вопроса и практическое задание, соответствующие содержанию формируемых компетенций. Экзамен проводится в устной форме. На ответ и решение задачи студенту отводится 20 минут. За ответ на теоретические вопросы студент может получить максимально 50 баллов, за решение задачи 50 баллов. Перевод баллов в оценку: 5 баллов - 85% - 100%; 4 балла - 70% - 84%; 3 балла - 50% - 69%; 2 балла - менее 50%

По итогам выставляется дифференцированная оценка с учетом шкалы оценивания.

Тестирование проводится с помощью автоматизированной программы «Универсальная система тестирования».

На тестирование отводится 60 минут. Каждый вариант тестовых заданий включает 25 вопросов. За каждый правильный ответ на вопрос дается 4 балла.

Перевод баллов в оценку: 5 баллов - 85% - 100%; 4 балла - 70% - 84%; 3 балла - 50% - 69%; 2 балла - менее 50%