Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра теоретической и прикладной информатики

Паспорт экзамена

по дисциплине «Программные средства защиты информации», 3 семестр

1. Методика оценки

Экзамен проводится в письменной форме, по билетам . Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов (п. 4) 1-55, второй вопрос из диапазона вопросов1-55, третий: 56-77, четвертый: 78-115, пятый-восьмой: *типовые задачи 1-13* . В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма экзаменационного билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет ФПМИ

Билет № __1___
к экзамену по дисциплине «Программные средства защиты информации»

---

1. Что такое защита информации, информационная безопасность, доступность, целостность, конфиденциальность?
2. 4 вида нарушений защиты (атак): привести подробную характеристику. Пассивные и активные атаки.
3. Что такое простое число, взаимно простые числа? Как можно определить, является ли число простым?
4. Аутентификация с привлечением доверенного посредника. Приведите схему, пояснения.
5. Построить LFSR-генератор, заданный многочленом $g(x) = x^5 + x^2 + 1$ и начальным состоянием 11010_2, и получить последовательность, содержащую 12 бит.
6. Найти наибольший общий делитель чисел 4307 и 5183.
7. Алгоритмом Евклида найти в поле Галуа полином $b(x)$ такой, что $a(x) \cdot b(x) \equiv 1 \pmod{m(x)}$, если $a(x) = x^5 + x^4 + x + 1$, $m(x) = x^8 + x^6 + x^4 + x^2 + x$.
8. Найти ключи абонента А и абонента В в алгоритме Диффи-Хеллмана при $n = 31$, $x = 12$, $y = 19$. g – выбрать одно из возможных.

Утверждаю: зав. кафедрой ____ _____ д.т.н.,проф. Чубич В.М.
(подпись)
(дата)

2. **Критерии оценки**

- Ответ на экзаменационный билет считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки, оценка составляет *от 0 до* 19 *баллов.*
- Ответ на экзаменационный билет засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, при решении задачи допускает непринципиальные ошибки, например, вычислительные, оценка составляет *от 20 до 30 баллов.*
- Ответ на экзаменационный билет билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов, явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи, оценка составляет *от 31 до 3*4 *баллов.*
- Ответ на экзаменационный билет билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи, оценка составляет от 35 до 40 *баллов.*

3. **Шкала оценки**

В общей оценке по дисциплине экзаменационные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Вопросы к** экзамену **по дисциплине «**Программные средства защиты информации**»**

Полный перечень вопросов к экзамену

1. Что такое защита информации, информационная безопасность?
2. Что такое доступность, целостность, конфиденциальность?
3. 3 аспекта защиты информации.
4. Что такое идентификация, аутентификация?
5. Что представляет собой сервис безопасности «контроль целостности»?
6. Что представляют собой сервисы безопасности «анализ защищённости» и «обеспечение отказоустойчивости»?
7. Что представляет собой сервис безопасности «обеспечение обслуживаемости»?
8. Что представляет собой сервис безопасности «туннелирование»?
9. Что представляет собой сервис безопасности «управление доступом»? В чём заключается суть ролевого управления доступом?
10. Что представляют собой такие сервисы безопасности, как «протоколирование» и «аудит»? Какие задачи решают?
11. Что представляет собой сервис безопасности «экранирование»? Привести подробную схему.

12. Какие атаки называются активными? 4 группы активных атак.
13. Модель защиты сети. Какие задачи нужно решить при разработке конкретного средства защиты?
14. Характеристики, на основе которых строится классификация криптографических систем.
15. 4 вида нарушений защиты (атак): привести подробную характеристику. Пассивные и активные атаки.
16. Что такое криптология, криптография, открытый текст, шифрование, ключ?
17. Что такое криптоанализ? Типы криптоанализа.
18. 2 критерия защищённости схемы шифрования.
19. Что такое защита информации, информационная безопасность, доступность, целостность, конфиденциальность?
20. Что такое шифрование?
21. Что такое абсолютно стойкий шифр?
22. Необходимые и достаточные условия абсолютной стойкости шифра.
23. Что такое лавинный эффект, диффузия и конфузия?
24. Приведите схему симметричной криптосистемы.
25. Какими свойствами должна обладать последовательность, генерируемая скремблером?
26. Что такое примитивный многочлен степени n? Что такое неприводимый многочлен степени n?
27. Преимущества и недостатки использования однократного гаммирования.
28. Преимущества и недостатки использования скремблера.
29. Алгоритм шифрования AES: преобразования сдвига строк (ShiftRows) и добавление раундового ключа (AddRoundKey).
30. В чём заключаются достоинства и недостатки симметричных криптоалгоритмов?
31. Что такое примитивный многочлен степени n? Что такое неприводимый многочлен степени n?
32. Что такое скремблер, сдвиговый регистр с обратной связью (LFSR)? Приведите схему работы LFSR.
33. Сравните алгоритмы DES и ГОСТ 28147-89. Достоинства и недостатки каждого алгоритма.
34. Распределение ключей при симметричном шифровании.
35. Сценарий централизованного распределения ключей при симметричном шифровании.
36. Сценарий децентрализованного распределения ключей при симметричном шифровании.
37. Сеть Фейстеля. В чём заключаются процессы шифрования и дешифрования?
38. Алгоритм шифрования DES. Общая схема.
39. Алгоритм шифрования DES. В чём заключается функция шифрования f?
40. Алгоритм шифрования DES. Алгоритм получения раундовых ключей.
41. Режим электронной шифровальной книги (ECB). Привести уравнения и нарисовать блок-схему процесса шифрования.
42. Режим сцепление шифрованных блоков (CBC). Привести уравнения и нарисовать блок-схему процесса шифрования.

43. Режим обратная связь по шифротексту (CFB). Привести уравнения и нарисовать блок-схему процесса шифрования.
44. Режим обратная связь по выходу (OFB). Привести уравнения и нарисовать блок-схему процесса шифрования.
45. Схема двойного шифрования. В чём заключается метод двусторонней атаки?
46. 2 схемы тройного шифрования. Привести уравнения и нарисовать блок-схему процесса шифрования. Какая схема лучше и почему?
47. Алгоритм шифрования ГОСТ 28147-89. Общая схема. Описание функции шифрования f.
48. Алгоритм шифрования AES: общий алгоритм.
49. Алгоритм шифрования AES: преобразование замена байт (SubBytes).
50. Алгоритм шифрования AES: преобразование замешивания столбцов (MixColumns).
51. Алгоритм шифрования AES: алгоритм выработки ключей (Key Schedule).
52. Сценарий централизованного распределения ключей при симметричном шифровании.
53. Режим обратная связь по шифротексту (CFB). Привести уравнения и нарисовать блок-схему процесса шифрования.
54. Режим обратная связь по выходу (OFB). Привести уравнения и нарисовать блок-схему процесса шифрования.
55. Что такое простое число, взаимно простые числа? Как можно определить, является ли число простым?
56. Определение и свойства функции Эйлера.
57. Малая теорема Ферма.
58. Теорема Эйлера.
59. Как сгенерировать большое простое число?
60. В чём заключается безопасность обмена ключа по схеме Диффи-Хеллмана?
61. Почему криптосистемы с открытым ключом на практике используются только для шифрования ключа, но не открытого текста?
62. В чём заключаются достоинства и недостатки асимметричных криптоалгоритмов?
63. Приведите схему асимметричной криптосистемы.
64. Приведите схему асимметричной криптосистемы.
65. В чём заключаются достоинства и недостатки асимметричных криптоалгоритмов?
66. Что такое простое число, взаимно простые числа? Как можно определить, является ли число простым?
67. Что означает решить сравнение? Какими методами можно решать сравнение? Общий вид решения сравнения первой степени.
68. Определение и свойства первообразных корней и числа, принадлежащего показателю n.
69. В чём заключается алгоритм Евклида?
70. В чём заключается расширенный алгоритм Евклида?
71. Решение сравнения первой степени способом Эйлера.
72. Алгоритм шифрования RSA.
73. Схема обмена ключами Диффи-Хеллмана.
74. В чём заключается алгоритм Евклида?
75. В чём заключается расширенный алгоритм Евклида?
76. Решение сравнения первой степени с помощью алгоритма Евклида.

77. Решение сравнения первой степени с помощью расширенного алгоритма Евклида.
78. Алгоритм Рабина-Миллера.
79. Распределение открытых ключей в асимметричной криптосистеме: метод «публичное объявление».
80. Распределение открытых ключей в асимметричной криптосистеме: метод «публично доступный каталог».
81. Распределение открытых ключей в асимметричной криптосистеме: метод «авторитетный источник ключей».
82. Распределение открытых ключей в асимметричной криптосистеме: метод «сертификаты открытых ключей». Какие требования существуют для этого метода?
83. Распределение секретных ключей в асимметричной криптосистеме: метод «распределение ключей с обеспечением конфиденциальности и аутентификации».
84. Распределение секретных ключей в асимметричной криптосистеме: метод «простое распределение ключей» (схема Меркла). Приведите пример того, как этот протокол может быть скомпрометирован.
85. 3 способа аутентификации личности.
86. Коды аутентификации сообщений (MAC) с использованием функции хэширования с ключом.
87. Коды аутентификации сообщений (MAC) с использованием алгоритмов блочного шифрования.
88. Алгоритм электронной цифровой подписи RSA.
89. Алгоритм электронной цифровой подписи Эль-Гамаля.
90. Что такое идентификация, аутентификация? Подробное описание 3 видов аутентификации.
91. Взаимная аутентификация. Приведите схему.
92. Аутентификация с помощью пароля: простейший протокол. Приведите схему. Укажите, какие существуют проблемы у данного подхода.
93. Аутентификация с помощью пароля: протокол Нидхема. Приведите схему. Укажите, какие существуют проблемы у данного подхода.
94. Аутентификация с помощью пароля: схема с одноразовыми паролями. Приведите схему. Укажите, какие существуют проблемы у данного подхода.
95. Аутентификация с привлечением доверенного посредника. Приведите схему, пояснения.
96. Механизмы определения свежести сообщения и существования пользователя: стратегии оклик-отзыв – 3 варианта (схемы, пояснения); стандартные варианты этих стратегий (схемы, пояснения).
97. Механизмы определения свежести сообщения и существования пользователя: метка времени – 3 варианта (схемы, пояснения); стандартные варианты этих стратегий (схемы, пояснения).
98. 4 безопасные схемы построения хэш-функций. Привести схемы, пояснения.
99. 3 схемы построения электронной цифровой подписи. Процесс генерации ЭЦП.
100. Приведите схему защиты целостности данных.
101. Приведите определение и примеры применения хэш-функции.
102. Асимметричные методы защиты целостности данных: электронная цифровая подпись. Приведите схему, примеры алгоритмов.
103. Определение и свойства хэш-функции.

104. Электронная цифровая подпись и её свойства.
105. Приведите схему защиты целостности данных.
106. Приведите определение и примеры применения хэш-функции.
107. Что такое биометрия?
108. Физиологические биометрические параметры (перечислить не менее 5 шт.).
109. Поведенческие биометрические параметры (перечислить не менее 4 шт.).
110. (2) Приведите схему биометрической идентификации.
111. Приведите схему биометрической верификации.
112. Сопоставление биометрических образцов. Что такое биометрический шаблон? Приведите схему сопоставления биометрических образцов.
113. Что такое верификация и идентификация в биометрии?
114. 5 свойств биометрических параметров.
115. Какие задачи можно решать с помощью биометрии?

Перечень типовых задач к экзамену

1. Построить LFSR-генератор, заданный многочленом $g(x) = x^5 + x^2 + 1$ и начальным состоянием 11010_2, и получить последовательность, содержащую 12 бит.
2. Найти функцию Эйлера для числа 4725.
3. Найти наибольший общий делитель чисел 4307 и 5183.
4. Умножить полином $a(x) = x^3 + x^2 + x$ на полином $b(x) = x^5 + x^4 + x^2 + x + 1$ в поле Галуа по модулю полинома $m(x) = x^5 + x^2 + 1$.
5. Найти наибольший первообразный корень для числа 50.
6. Решить сравнение 113 $x \equiv 58 \pmod{259}$ способом Эйлера.
7. Найти алгоритмом Евклида элемент d такой, что $e \cdot d \equiv 1 \pmod{n}$, если $e = 88$, $n = 107$.
8. Найти все первообразные корни для числа 6.
9. Решить сравнение 195 $x \equiv 141 \pmod{342}$ алгоритмом Евклида.
10. Алгоритмом Евклида найти в поле Галуа полином $b(x)$ такой, что $a(x) \cdot b(x) \equiv 1 \pmod{m(x)}$, если $a(x) = x^5 + x^4 + x + 1$, $m(x) = x^8 + x^6 + x^4 + x^2 + x$.
11. Найти ключи абонента А и абонента В в алгоритме Диффи-Хеллмана при $n = 31$, $x = 12$, $y = 19$. g – выбрать одно из возможных.
12. Найти открытый и закрытый ключи, зашифровать сообщение $M = 7$ с помощью алгоритма RSA. $p = 3$, $q = 11$, e – выбрать одно из возможных, d – найти одним из методов (не подбором). Привести подробное решение.
13. Найти открытый и закрытый ключи и сгенерировать электронную цифровую подпись по алгоритму Эль-Гамаля для сообщения $M = 14$, если $p = 7$, $g = 6$, $x = 5$.