Вариант I

Задания, ответы и критерии оценивания

Задание 1

В компании используется система электронного документооборота. Все важные документы подписываются электронной подписью. Для хранения закрытых ключей используется аппаратный модуль безопасности (HSM), который имеет следующие характеристики:

- Может хранить до 1000 ключей
- Время генерации одного ключа — 2 минуты
- Время подписи одного документа — 5 секунд
- Время проверки подписи — 3 секунды

В компании работает 50 сотрудников, каждый из которых в среднем подписывает 20 документов в день.

Задания:

1. Определить, хватит ли ёмкости HSM для хранения ключей всех сотрудников на протяжении года, если каждый сотрудник меняет ключ раз в квартал. (Хранение используется для невозможности повторного использования недавних паролей)
2. Рассчитать общее время, которое потребуется на подписание всех документов за месяц
3. Определить, сколько документов можно проверить за 1 рабочий день (8 часов), если проверка идёт непрерывно

В ответ запишите достаточно ли ёмкости HSM, время на подпись документов за месяц в часах, количество документов возможных для проверки за день.

Округления производить до десятых в большую сторону

Решение:

1. Расчёт количества ключей:
   - Каждый сотрудник меняет ключ 4 раза в год
   - Всего сотрудников: 50
   - Необходимое количество ключей в год: 50 × 4 = 200
   - Ёмкость HSM: 1000 ключей
   - Вывод: ёмкости HSM достаточно, так как 200 < 1000
2. Расчёт времени на подписание документов:
   - Подписей в день: 50 сотрудников × 20 документов = 1000 подписей
   - Время на одну подпись: 5 секунд
   - Время в день: 1000 × 5 = 5000 секунд = 83.4 минуты
   - За месяц (30 дней): 83.4 × 30 = 2502 минут = 41.7 часа
3. Расчёт проверки документов:
   - Время работы в день: 8 часов = 28800 секунд
   - Время на одну проверку: 3 секунды
   - Количество проверок в день: 28800 ÷ 3 = 9600 документов

Ответ:

Ёмкость HSM достаточна для хранения ключей всех сотрудников на год
На подписание всех документов за месяц потребуется = 41.7 часа
За рабочий день можно проверить 9600 документов

Баллы	Критерий получения
10	Расчеты и ответ верны.
7	Допущена 1 ошибка в расчётах, но 2 или 3 ответа верны.
4	Допущено 2 ошибки в расчётах, но 2 ответа верны
1	Ответ верен, решение отсутствует
0	Допущено более двух ошибок в расчётах, или верен только 1 ответ

Задание 2

Корпоративная сеть имеет следующие параметры:

- 1000 рабочих станций
- Система обнаружения вторжений (IDS) с вероятностью обнаружения атаки 0.95
- Система предотвращения вторжений (IPS) с эффективностью 0.85
- Вероятность успешной атаки на одну станцию: 0.002
- Время реакции администратора: 15 минут

Атаки производятся с частотой 1 в минуту.

Задания:

1. Рассчитать вероятность успешной атаки на всю сеть (ответ округлить до тысячных)
2. Оценить среднее количество успешных проникновений в час (ответ округлить до десятых)

В ответ запишите вероятность успешной атаки, количество проникновений за час.

Решение:

1. **Вероятность успешной атаки на одну станцию:**

$P_{успех}=P_{атака}\cdot(1-P_{IDS})\cdot(1-P_{IPS})$

$P_{успех}=0.002\cdot(1-0.95)\cdot(1-0.85)$

$P_{успех}=0.002\cdot0.05\cdot0.15=0.000015$

2. **Вероятность успешной атаки на всю сеть:**

$P_{сеть}=1-(1-P\text{успех})^{1000}$

$P_{сеть}=1-(1-0.000015)^{1000}\approx0.015$

3. **Среднее количество успешных проникновений в час:**

$M_{проникновений}=60\cdot1000\cdot P_{успех}=60\cdot1000\cdot0.000015=0.9$

С учетом времени реакции администратора (15 минут):

$M=0.9\cdot\frac{60}{15}=3,6$

Ответ:

Вероятность успешной атаки на сеть: 0.015 = 1,5%

Проникновения в час: 3,6

Баллы	**Критерий получения**
20	Расчеты и ответ верны.
15	Допущена 1 ошибка в расчётах, но ответы верны.
10	Допущено 2 ошибки в расчётах, но 1 ответ верен.
1	Ответ верен, решение отсутствует
0	Допущено более двух ошибок в расчётах, или нет верных ответов.

Задание 3

RSA — это криптосистема с открытым ключом, основанная на сложности факторизации больших чисел.

Основные этапы:

1. Генерация ключей:
   - Выбираются два больших простых числа p и q
   - Вычисляется $n=p\cdot q$
   - Вычисляется функция Эйлера $\phi(n)=(p-1)(q-1)$
   - Выбирается открытый показатель e, взаимно простой с $\phi(n)$
   - Вычисляется закрытый ключ d, такой что $e\cdot d\equiv1(\mathrm{mod}\,\phi(n))$
2. Шифрование: $C=M^e \mathrm{mod} n$
3. Дешифрование: $M=C^d \mathrm{mod} n$

Дано:

- Два простых числа: p=101, q=103
- Открытый ключ: e=7
- Сообщение для шифрования:1754
- Зашифрованный текст:1964

Задание:

1. Сгенерировать закрытый ключ d
2. Зашифровать сообщение
3. Расшифровать сообщение

В ответ запишите значение ключа d, зашифрованное и расшифрованное сообщение.

Решение:

1. Вычисление модуля n:

$n=p\cdot q=101\cdot 103=10403$

2. Вычисление функции Эйлера:

$\phi(n)=(p-1)(q-1)=100\cdot 102=10200$

3. Нахождение закрытого ключа d:

$e\cdot d\equiv 1(\mathrm{mod}\,\phi(n))$

$7\cdot d\equiv 1(\mathrm{mod}10200)$

$d=8743$

4. Шифруем сообщение:

$C\equiv M^e(\mathrm{mod}n)$

$C\equiv 1754^7(\mathrm{mod}10403)$

$C=1775$

5. Дешифрование сообщения:

$M\equiv C^d(\mathrm{mod}n)$

$M\equiv 1964^{8743}(\mathrm{mod}10403)$

$M=5669$

Ответ:

Закрытый ключ: $d=8743$

Зашифрованное сообщение:**1775**

Расшифрованное сообщение: **5669**

Баллы	**Критерий получения**
40	Расчеты и ответ верны.
30	Допущена 1 ошибка в расчётах, но 2 или 3 ответа верны.
15	Допущено 2 ошибки в расчётах, но 2 ответа верны
1	Ответ верен, решение отсутствует
0	Допущено более двух ошибок в расчётах, или верен только 1 ответ

Задание 4

Пароль состоит из 8 символов, включая:

- Строчные и заглавные буквы (английский алфавит – 52 буквы)
- Цифры
- Специальные символы (!@#$%^&*)

Ограничения:

- Пароль должен содержать минимум 2 цифры
- Не может начинаться с цифры
- Не может содержать последовательности из 3 одинаковых символов

Задание:

1. Рассчитать энтропию пароля ($H = \log_2(M^N)$, где M - мощность алфавита, N – длина пароля)
2. Определить количество возможных комбинаций (ответ записать как 2^x, x- высчитать)
3. Оценить время перебора при скорости 1 млн попыток/сек

(дробную часть ответа, если она есть, округлите до десятых в большую сторону)

В ответ запишите энтропию в битах, количество комбинаций, время перебора в годах.

Решение:

Энтропия рассчитывается по формуле:

$H=\log_2(M^N)$

где:

M = 70 (мощность алфавита)

N = 8 (длина пароля)

$H=8\times\log_2(70)=8\times 6.129=49.032$ бит

2. Количество возможных комбинаций
Базовая формула:
$M^N=70^8$=576 480 100 000 000 комбинаций
Учет ограничений:
Первая позиция: 60 символов (без цифр)
Выбор позиций для цифр: $\sum_7^2 C_7^x$ (x – количество цифр в пароле (от 2 до 7)
Итоговая формула: $\sum_7^2(60 * C_7^x * 10^x * 60^{7-x})$
Итоговый результат: 2^{47}
3. Оценка времени перебора
При скорости 1 000 000 попыток/сек:
2^{47} /1 000 000 =1,4 * 10^8 секунд ≈ 4,4 года
Ответ:

- Энтропия: 49,1 бит
- Количество комбинаций: $\mathbf{2^{47}}$
- Время перебора: **4,4 года**

Баллы	**Критерий получения**
30	Расчеты и ответ верны.
20	Допущена 1 ошибка в расчётах, но 2 или 3 ответа верны.
15	Допущено 2 ошибки в расчётах, но 2 ответа верны
1	Ответ верен, решение отсутствует
0	Допущено более двух ошибок в расчётах, или верен только 1 ответ

Вариант I

Задания, ответы и критерии оценивания

Задание 1

Используется шифр простой замены (подстановки) на основе латинского алфавита (26 букв). Ключ - слово МАТН, по которому строится таблица замены:

1. Буквы ключа записываются без повторов: M, A, T, H;
2. Далее идут оставшиеся буквы алфавита в обычном порядке (исключая уже использованные в ключе);
3. Каждая буква открытого текста заменяется на соответствующую из построенной последовательности (A → M, B → A, C → T, D → H, E → B и т. д.).

Необходимо зашифровать слово CODE и расшифровать слово MTBH. Для этого необходимо построить таблицу замены для указанного выше ключа.

В ответ запишите зашифрованное и расшифрованное слово.

Решение:

1. : Строим таблицу замены

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

2. Зашифруем слово CODE, заменяя буквы из первой строчки на букву, стоящую под ней

- C → T
- O → Q
- D → H
- E → B

Результат шифрования: TQHB

3. Расшифруем последовательность MTBH

Используем ту же таблицу, но теперь снизу-вверх.

- **M** → A
- **T** → C
- **B** → E
- **H** → D

Ответ: Зашифрованное слово: TQHB, расшифрованное слово: ACED

Баллы	Критерий получения
10	Расчеты и ответ верны.
7	Допущена 1 ошибка в шифровании или расшифровке
4	Таблица построена не верно, но на её основании шифрование и расшифровка верны
1	Ответ верный, решения нет
0	Допущено более двух ошибок в шифровании или расшифровке

Задание 2

Шифр Виженера — это полиалфавитный шифр подстановки, в котором каждый символ исходного текста шифруется с помощью шифра Цезаря, но с ключом, который меняется в процессе шифрования.

Принцип работы:

- Каждому символу алфавита присваивается число (A=0, B=1, …, Z=25)
- Ключ повторяется циклически по длине сообщения
- Формула шифрования: $C_i=(P_i+K_j)\text{mod}26$
- Формула дешифрования: $P_i=(C_i-K_j+26)\text{mod}26$

Дано:

- Исходный текст: «ATTACK AT DAWN»
- Ключ: «LEMON»

- Алфавит: английский
- Каждый 4-й символ шифрования подвергается дополнительной замене – заменяется на предыдущий символ в алфавите

Задания:

- Выполнить двойное шифрование
- Определить количество возможных комбинаций при таком методе шифрования

В ответ запишите итоговое зашифрованное сообщение и количество комбинаций (принимается вариант как число в степени и полная запись числа (пример: 5^4, 625 – оба варианта правильные))

Решение:

Расшифровка ключа в числовые значения:

- L = 11
- E = 4
- M = 12
- O = 14
- N = 13

Процесс шифрования:

- A(0) + L(11) = L(11)
- T(19) + E(4) = X(23)
- T(19) + M(12) = F(5)
- A(0) + O(14) = O(14)
- C(2) + N(13) = P(15)
- K(10) + L(11) = V(21)
- A(0) + E(4) = E(4)
- T(19) + M(12) = F(5)
- D(3) + O(14) = R(17)
- A(0) + N(13) = N(13)
- W(22) + L(11) = H(7)
- N(13) + E(4) = R(17)

Полученный шифротекст: LXFOPVEFRNHR

Применяем второй этап шифрования:

4-й символ: O → N

8-й символ: F → E

12-й символ: R → Q

Итоговый шифротекст: LXFNPVEERGHQ

Количество комбинаций:

- Длина ключа = 5 символов
- Для каждого символа 26 вариантов
- Общее количество комбинаций ключей: 26^5=11881376

Ответ: LXFNPVEERGHQ, 26^5=11881376

Баллы	**Критерий получения**
20	Расчеты и ответ верны.
15	Допущена 1 ошибка в шифровании или расшифровке, но количество комбинаций верно
13	Допущены 2 ошибки в шифровании или расшифровке, но количество комбинаций верно
7	Допущены 2 ошибки в шифровании или расшифровке и количество комбинаций не верно
1	Ответ верный, решения нет
0	Допущены более 2 ошибок в шифровании или расшифровке и количество комбинаций не верно

Задание 3

В финансовой организации существует комплекс взаимосвязанных угроз:

- DDoS-атаки (вероятность 0.15)
- Фишинг (вероятность 0.25)
- Внутренние угрозы (вероятность 0.1)
- Вирусные атаки (вероятность 0.3)

Угрозы могут комбинироваться:
- DDoS + Фишинг (вероятность 0.05)
- Фишинг + Внутренние (вероятность 0.03)
- Вирусы + DDoS (вероятность 0.04)

Имеющиеся системы защиты:
- Firewall (снижает угрозы вирусов и DDoS-атак на 40%)
- SIEM (снижает комплексные угрозы на 60%)
- Антивирус (снижает вирусные атаки на 80%)
- DLP (снижает внутренние угрозы на 70%)

Ущерб от каждой угрозы различен:
- DDoS: 500 000 руб.
- Фишинг: 700 000 руб.
- Внутренние: 1 000 000 руб.
- Вирусы: 800 000 руб.
- Комбинированные: сумма отдельных ущербов

Задания:
1. Рассчитать ожидаемый годовой ущерб после внедрения защиты (ответ в руб.)
2. Определить наиболее опасный сценарий - угроза, приводящая к самым большим финансовым потерям, уже после внедрения защиты (в ответе укажите её название и сумму ущерба в руб.)
3. Оценить эффективность защиты (ответ дайте в %, округлить до десятых)

В ответ запишите ожидаемый годовой ущерб, наиболее опасный сценарий с указанием ущерба в руб., эффективность защиты системы в %.

Решение:

Расчет остаточных вероятностей после защиты:
- Простые угрозы:
  - DDoS: $P_1' = 0.15 \cdot 0.6 = 0.09$
  - Фишинг: $P_2' = 0.25 \cdot 0.6 = 0.15$
  - Внутренние: $P_3' = 0.1 \cdot 0.3 = 0.03$
  - Вирусы: $P_4' = 0.3 \cdot 0.2 \cdot 0.6 = 0.036$
- Комбинированные угрозы:
  - DDoS + Фишинг: $P_{12}' = 0.05 \cdot 0.6 \cdot 0.4 = 0.012$
  - Фишинг + Внутренние: $P_{23}' = 0.03 \cdot 0.15 \cdot 0.6 = 0.0027$
  - Вирусы + DDoS: $P_{41}' = 0.04 \cdot 0.2 \cdot 0.6 \cdot 0.4 = 0.00192$

Расчет ущерба после защиты:
- DDoS: 500 000 × 0.6 = 300 000
- Фишинг: 700 000 × 0.6 = 420 000
- Внутренние: 1 000 000 × 0.3 = 300 000
- Вирусы: 800 000 × 0.2 × 0.6 = 96 000

Комбинации:
- DDoS + Фишинг: (300 000 + 420 000) × 0.4 = 288 000
- Фишинг + Внутренние: (420 000 + 300 000) × 0.15 = 108 000
- Вирусы + DDoS: (96 000 + 300 000) × 0.08 = 31 680

Ожидаемый годовой ущерб:
- DDoS: 0.09 × 300 000 = 27 000
- Фишинг: 0.15 × 420 000 = 63 000
- Внутренние: 0.03 × 300 000 = 9 000
- Вирусы: 0.036 × 96 000 = 3 456

Комбинации:
- DDoS + Фишинг: 0.012 × 288 000 = 3 456
- Фишинг + Внутренние: 0.0027 × 108 000 = 291.6
- Вирусы + DDoS: 0.00192 × 31 680 = 60.864

Итого: 27 000 + 63 000 + 9 000 + 3 456 + 3 456 + 291.6 + 60.864 = 106 214.464 руб.

Наиболее опасный сценарий: фишинг (420000 руб.)

Эффективность защиты:
- Исходный ожидаемый ущерб (без защиты):
- DDoS: 0.15 × 500 000 = 75 000
- Фишинг: 0.25 × 700 000 = 175 000
- Внутренние: 0.1 × 1 000 000 = 100 000
- Вирусы: 0.3 × 800 000 = 240 000
- Комбинации:
- DDoS + Фишинг: 0.05 × (500 000 + 700 000) = 60 000
- Фишинг + Внутренние: 0.03 × (700 000 + 1 000 000) = 51 000
- Вирусы + DDoS: 0.04 × (800 000 + 500 000) = 52 000

Итого без защиты: 75 000 + 175 000 + 100 000 + 240 000 + 60 000 + 51 000 + 52 000 = 753 000 руб.
Снижение ущерба: 753 000 - 106 214.464 = 646 785.536 руб.
Эффективность защиты: (646 785.536 / 753 000) × 100% = 85.9%

Ответ:

- **Ожидаемый годовой ущерб: 248 760 руб.**
- **Наиболее опасный сценарий: фишинг (420000 руб.)**
- **Эффективность защиты системы: 81.3%**

Баллы	**Критерий получения**
40	Расчеты и ответы верны.
30	В решении допущена одна логическая или расчётная ошибка, и 1 ответ не верный.
15	В решении допущено две логических или расчётных ошибки, но 1 ответ не верный.
1	Ответ верный, решения нет
0	В решении допущено более двух логических или расчетных ошибок, или 2 ответа не верные.

Задание 4

Компания планирует защиту корпоративной сети. Варианты систем:
- Firewall A: стоимость 1 200 000 руб., эффективность 85%, срок службы 3 года
- Firewall B: стоимость 1 800 000 руб., эффективность 92%, срок службы 5 лет
- Firewall C: стоимость 2 500 000 руб., эффективность 95%, срок службы 7 лет

Вероятности атак:
- DDoS: 0.15
- Вирусы: 0.3
- Эксплойты: 0.25
- Фишинг: 0.3

Ущерб от успешной атаки: 3 000 000 руб.
Задания:
1. Рассчитать остаточный риск после внедрения системы
2. Рассчитать TCO (совокупную стоимость владения) для каждого варианта – рассчитывается по формуле:

TCO=T/C+R

где:
C — первоначальная стоимость системы
T — срок службы системы
R — остаточный риск (ожидаемый ущерб после внедрения защиты)

3. Определить ROI (возврат инвестиций) для каждого варианта - рассчитывается по формуле:

$$ROI=\frac{\text{экономия}}{\text{затраты}}=\frac{U-R}{C}$$

где:
U — потенциальный ущерб без защиты
R — ожидаемый ущерб после внедрения защиты (остаточный риск)
C — затраты на систему защиты

4. Выбрать и обосновать оптимальный вариант на основание этих данных

В ответ внести букву варианта системы (например, Ответ - А)

Решение:

1. Расчет совокупного годового риска без защиты

Общая вероятность успешной атаки:

P=0.15+0.3+0.25+0.3=1.0 (с учетом возможной множественности атак)

Ожидаемый годовой ущерб без защиты:

$EU=P\cdot У_{щерб}=1\cdot 3000000=3000000$ руб.

2. Расчет остаточного риска для каждого варианта

- Firewall A:

Остаточный риск: $(1-0.85)\cdot 3000000=0.15\cdot 3000000=450000$ руб.

- Firewall B:

Остаточный риск: $(1-0.92)\cdot 3000000=0.08\cdot 3000000=240000$ руб.

- Firewall C:

Остаточный риск: $(1-0.95)\cdot 3000000=0.05\cdot 3000000=150000$ руб.

3. Расчет TCO (совокупной стоимости владения)

- Firewall A:

$TCO_A=\frac{1200000}{3}+450000=850000$ руб./год

- Firewall B:

$TCO_B=\frac{1800000}{5}+240000=600000$ руб./год

- Firewall C:

$TCO_C=\frac{2500000}{7}+150000=507143$ руб./год

4. Расчет ROI (возврат инвестиций)

- Firewall A:

$ROI_A=\frac{3000000-450000}{1200000}=2.125$ или 212.5%

- Firewall B:

$ROI_B=\frac{3000000-240000}{1800000}=1.533$ или 153.3%

- Firewall C:

$ROI_C=\frac{3000000-150000}{2500000}=1.14$ или 114%

5. **Обоснование выбора:**

Firewall B обеспечивает наилучший баланс между стоимостью владения, эффективностью защиты и сроком службы. Несмотря на более высокую начальную стоимость, он предлагает:

- Разумный годовой TCO
- Достаточную эффективность защиты
- Длительный срок эксплуатации
- Оптимальное соотношение цена/качество

Ответ: B

Баллы	**Критерий получения**
30	Обоснование и ответ верны.
20	В решении допущена одна логическая или расчётная ошибка, но ответ верный.
15	В решении допущено одна логическая или 2 расчётные ошибки, но ответ верный.
1	Ответ верный, решения нет
0	В решении допущено более двух логических или расчётных ошибок или ответ не верный.

Многопрофильная инженерная олимпиада «Звезда»
«Информационная безопасность»

9 классы **Заключительный этап** **2025-2026**

Вариант I

Задания, ответы и критерии оценивания

Требования к оформлению заданий. При проверке заданий учитывается не только ответ, но и само решение. Важно оформлять решения во всех заданиях. Ответы без решения оцениваются не более чем в 1 балл.

Задание 1

В системе безопасности используется матрица доступа 5×5, где:

- Каждая строка – пользователь;
- Каждый столбец – ресурс;
- Элемент матрицы = 1, если доступ разрешен, иначе 0.

Известно:

- У каждого пользователя есть доступ ровно к 3 ресурсам;
- Каждый ресурс используется ровно 3 пользователями;
- Общее число единиц в матрице = 15.

Дополнительно:

- Никакие два пользователя не имеют одинаковый набор ресурсов;
- Никакие два ресурса не доступны одинаковому набору пользователей;
- Перестановки сток и столбцов не учитываются.

Определите количество различных матриц доступа, удовлетворяющих условиям.

Решение:

Сначала выбираем 3 ресурса для первого пользователя: C_5^3=10 способов

Для второго пользователя: $C_2^1 \cdot C_3^2$=2·3=6

Для третьего пользователя: $C_1^1 \cdot C_2^2$=1

Для четвертого и пятого пользователей выбор определяется однозначно

Итоговый результат: 10*6*1*1*1 =60

Ответ: 60 матриц

Баллы	**Критерий получения**
10	Расчеты и ответ верны.
7	В определении количества комбинаций на одной позиции допущена ошибка, или допущена одна ошибка в расчетах.
4	В определении количества комбинаций на двух позициях допущена ошибка.
1	Ответ верный, решение отсутствует
0	Допущено больше двух ошибок в определении количества допустимых символов или все расчеты не верны.

Задание 2

В школьной сети 7 компьютеров (от А до Ж) соединены каналами связи:

А–Б, Б–В, В–Г, Г–Д, Д–Е, Е–Ж, Ж–А, А–Г, Б–Д

Администратор решил ввести дополнительные пароли для групп компьютеров по следующим правилам:

- Если компьютеры соединены в цикл (замкнутый путь без повторения рёбер), они образуют группу и используют один общий пароль;
- Компьютер может входить в несколько групп;
- Если одна группа полностью входит в другую - она не выделяется отдельно.

- Какое минимальное количество различных паролей нужно, чтобы обеспечить безопасность всех таких групп?

Решение:

Находим все простые циклы (без повторения рёбер):
Цикл А-Б-В-Е-Ж-А (длина 6)
Цикл А-Г-Д-Б-А (длина 4)
Цикл Г-Д-Е-Ж-Г (длина 4)
Цикл Б-Д-Е-В-Б (длина 4)
Цикл А-Ж-Е-Д-Г-А (длина 5)
Проверяем, входят ли меньшие циклы в большие:
Цикл А-Г-Д-Б-А входит в А-Б-В-Е-Ж-А
Цикл Г-Д-Е-Ж-Г входит в А-Ж-Е-Д-Г-А
Цикл Б-Д-Е-В-Б не входит ни в один другой
Исключаем вложенные циклы:
Берем большой цикл А-Б-В-Е-Ж-А
Добавляем независимый цикл Б-Д-Е-В-Б
Добавляем оставшийся цикл А-Ж-Е-Д-Г-А
Итого требуется 3 различных пароля.

Ответ: 3

Баллы	**Критерий получения**
20	Расчеты и ответ верны.
15	Ответ верный, но допущена одна ошибка в определении циклов
7	Ответ верный, но допущено две ошибки в определении циклов
1	Ответ верный, решение отсутствует
0	Допущено более двух ошибок или ответ не верный

Задание 3

Цифровой замок открывается 8-битным кодом. Известно, что:
– Код начинается с «1».
– Количество единиц - простое число.
– Код в десятичной системе - чётное число.

Сколько таких кодов существует?

Решение:

8-битный код, начинается с 1 → от 128 до 255 (всего 128 чисел).
Чётное → последний бит = 0.
Значит, биты: 1 _ _ _ _ _ 0 - 6 битов посередине - любые.
Всего таких чисел: 2^6=64.
Проверим условие: количество единиц - простое число. Значит, нужно посчитать, сколько из этих 64 чисел имеют простое количество единиц.
Первый бит = 1, последний = 0.
Количество единиц = 1 + (количество единиц в средних 6 битах).
Пусть k - число единиц в 6 битах, k=0..6.
Тогда общее число единиц: 1+k.
Оно должно быть простым.
Простые числа от 1 до 7: 2, 3, 5, 7.
Значит, 1+k∈{2,3,5,7} → k∈{1,2,4,6}.
Число комбинаций для k единиц в 6 битах: (k из 6)
- k=1: (1 из 6))=6
- k=2: (2 из 6))=15
- k=4: (4 из 6))=15
- k=6: (6 из 6))=1

Сумма: 6+15+15+1=37

Ответ: 37

Баллы	Критерий получения
40	Расчеты и ответ верны.
30	В решении допущена одна логическая ошибка, но расчёты и ответ верны.
20	В решении допущена одна логическая и расчётная ошибка, ответ верный.
10	В решении допущено две логические или расчётные ошибки, но ответ верный.
1	Ответ верный, решение отсутствует
0	В решении допущено более двух логических или расчётных ошибок, или ответ не верный.

Задание 4

В организации используется функция для генерации кода:

H_1=hash(1) - 32-битное число

H_2=hash(2)$\oplus H_1$

H_3=hash(3)$\oplus H_2$

…

H_n=hash(n)$\oplus H_n-1$

где $\oplus$ - побитовое XOR, а hash(k) - случайное 32-битное число, независимое для каждого k.

XOR- Эта операция ставит 1 на бит результата, для которого только один из соответствующих битов операндов равен 1 (но не оба).

Какова вероятность, что H_{10}=0 (все биты нулевые)?

Ответом будет дробь вида $\frac{1}{N}$, в ответ запишите значение N.

Решение:

1. $H_1 = h_1$ - случайное 32-битное число
2. $H_2 = h_2 \oplus h_1$
3. $H_3 = h_3 \oplus h_2 \oplus h_1$

…

Получаем формулу вида:

$H_n = h_1 \oplus h_2 \oplus \cdots \oplus h_n$

Для $H_{10} = \bigoplus_1^{10} h_k$

Каждое h_k - независимое случайное 32-битное число, их XOR - тоже равномерно распределён по всем 32-битным значениям.

Вероятность, что XOR = 0:

$$\frac{1}{2^{32}}$$

$N=2^{32}$=4 294 967 296

Ответ: $N=2^{32}$=4 294 967 296

Баллы	Критерий получения
30	Обоснование и ответ верны.
25	Задача решена методом перебора, но ответ верный.
20	В решении допущена одна расчетная ошибка, но ответ и логика верны.
15	В решении допущено одна логическая ошибка, но ответ и расчеты верны.
1	Ответ верный, решение отсутствует
0	В решении допущено более двух логических ошибок или ответ не верный.

Вариант I

Задания, ответы и критерии оценивания

Задание 1

Администратор просит команду придумать пароль, соответствующий политике безопасности:

- Длина - ровно 6 символов;
- Можно использовать:
  - строчные буквы латинского алфавита (a–z) - 26 букв;
  - цифры (0–9) - 10 цифр;
  - запрещены спецсимволы и пробелы.

Рассматриваются четыре подхода к генерации пароля:

A. Все 6 символов - случайные строчные буквы;

B. Первые 4 символа - буквы, последние 2 – цифры;

C. Пароль состоит из двух одинаковых блоков по 3 символа (например, abcabc), каждый блок - случайные буквы;

D. Пароль - это слово из 6 букв, но с заменой одной буквы на цифру по правилу: o → 0, e → 3, a → 4 (например, p4sswor → длина 7, а у нас 6 - т.к. считаются только буквы).

Какой из вариантов даёт наибольшее количество возможных уникальных паролей?

Решение:

Считаем количество комбинаций для каждого варианта:

A. 6 букв: $26^6=308915776$

B. 4 буквы + 2 цифры: $26^4 \cdot 10^2=456976 \cdot 100=45697600$

C. Два одинаковых блока по 3 буквы:

Первый блок - $26^3=17576$ вариантов

Второй блок - такой же, как первый → не добавляет вариантов

Всего: $26^3=17576$

D. Слово из 6 букв → 26^6 вариантов базовых слов

Но: одна буква заменяется на цифру по правилу: можно заменить o, e, a → но не все слова содержат эти буквы

Кроме того:

- Замена делается только один раз
- И только если такая буква есть

Количество реальных паролей меньше, чем 26^6, потому что:

- Не для всех слов можно сделать замену
- Даже если можно - количество вариантов не превышает 26^6
- На практике - меньше, чем A

Сравним:

- A: 308 915 776
- B: 45 697 600
- C: 17 576
- D: меньше, чем A

Ответ: A

Баллы	Критерий получения
10	Расчеты и ответ верны.
7	В определении количества комбинаций допущена одна ошибка, или допущена одна ошибка в расчетах.
4	В определении количества комбинаций допущено две ошибки, или допущено две ошибки в расчетах.
1	Ответ верный, решение отсутствует

0	Допущено больше двух ошибок в определении количества комбинаций или допущено более двух ошибках в расчётах.

Задание 2

Рассматриваются четыре метода шифрования для сообщения из 6 букв (латинский алфавит, строчные буквы a–z, 26 символов). Нужно определить, какой из методов имеет наибольшее количество возможных ключей.

A. Шифр Цезаря: сдвиг всех букв на фиксированное число позиций (сдвиг от 1 до 25);

B. Перестановка букв: порядок букв в слове меняется по ключу - ключ задаёт перестановку 6 позиций без повтора (например, 2-4-1-6-3-5);

C. Каждая буква шифруется своим сдвигом Цезаря, но шаг сдвига от 1 до 3 (для каждой позиции независимо);

D. Замена только одной буквы в слове: выбирается одна позиция из 6 и одна буква из 25 (не текущую, которую заменяют).

Какой из методов имеет наибольшее количество возможных ключей?

Решение:

A. Шифр Цезаря

Сдвиг от 1 до 25 → 25 ключей

B. Перестановка 6 букв

Количество перестановок: 6! = 720

C. Каждая из 6 букв - свой сдвиг (от 1 до 3)

Для каждой позиции - 3 варианта → 3^6=729

D. Замена буквы

Количество ключей: 6·25=150

Сравним:

- A: 25
- B: 720
- C: 729
- D: 150

Ответ: C

Баллы	**Критерий получения**
20	Расчеты и ответ верны.
15	Выбран верный вариант, но допущена одна ошибка в расчетах
7	Выбран верный вариант, но допущено две ошибки в расчетах
1	Ответ верный, решение отсутствует
0	Допущено более 2 ошибок в расчетах, или выбран не верный вариант

Задание 3

Рассматриваются четыре возможные атаки на школьную систему. Каждая атака состоит из нескольких этапов, и успех атаки требует успеха на всех этапах. Вероятности успеха на этапах - независимы.

A. Фишинг:

- Письмо попадает в почту: 0.9
- Ученик открывает письмо: 0.8
- Ученик вводит пароль: 0.3

B. Подбор пароля:

- Длина пароля - 4 цифры (0–9), повтор возможен
- Злоумышленник делает 1 попытку

C. Атака через USB:

- Ученик находит зараженную флешку: 0.6
- Подключает к компьютеру: 0.5
- Запускает файл: 0.4

D. Социальная инженерия:

- Злоумышленник звонит и представляется учителем: 0.7
- Учитель отвлекается и уходит: 0.5

- Злоумышленник вводит пароль с записки: 0.9

Какая из атак имеет наибольшую вероятность успеха? (округления не производить)

Решение:

Считаем вероятность полного успеха (все этапы подряд):

A. Фишинг:

$0.9 \cdot 0.8 \cdot 0.3 = 0.72 \cdot 0.3 = 0.216$

B. Подбор пароля:

Всего паролей: $10^4 = 10000$

Вероятность угадать за одну попытку 1 правильный пароль:

$1/10000 = 0.0001$

C. USB-атака:

$0.6 \cdot 0.5 \cdot 0.4 = 0.3 \cdot 0.4 = 0.12$

D. Социальная инженерия:

$0.7 \cdot 0.5 \cdot 0.9 = 0.35 \cdot 0.9 = 0.315$

Сравним:

- A: 0.216
- B: 0.0001
- C: 0.12
- D: 0.315

Ответ: D

Баллы	**Критерий получения**
40	Расчеты и ответ верны.
30	В решении допущена одна ошибка в расчётах, но ответ верный.
15	В решении допущено две ошибки в расчётах, но ответ верный.
1	Ответ верный, решение отсутствует
0	В решении допущено более двух ошибок в расчётах или ответ не верный.

Задание 4

Школьный сайт используется для публикации новостей, расписания и для входа в личные кабинеты учеников. Администрация внедрила следующие меры защиты:

1. Все страницы доступны по HTTPS;
2. Для входа в личный кабинет требуется логин и пароль;
3. Пароль должен содержать не менее 8 символов, включая цифру и заглавную букву;
4. После 5 неудачных попыток вход блокируется на 15 минут;
5. Администраторы проверяют журналы доступа раз в неделю;
6. Резервная копия сайта делается раз в сутки в 3:00;
7. Доступ к серверу - только по паролю у администратора;
8. Сервер стоит в запираемом шкафу в кабинете директора.

Рассматриваются угрозы:

A. Злоумышленник подбирает пароль ученика и заходит в его кабинет;
B. Вредоносный скрипт внедряется в сайт через уязвимость в форме обратной связи;
C. Ученик случайно удаляет важную новость - администратор должен восстановить;
D. Злоумышленник крадёт сервер;
E. Происходит утечка пароля администратора;
F. Сайт становится недоступен из-за сбоя - нужно быстро восстановить (менее чем за 6 часов);
G. Злоумышленник использует фишинг, чтобы получить логин и пароль у ученика.

Достаточно ли внедрённых мер для защиты от всех перечисленных угроз? (Каждая угроза должна быть полностью нейтрализована хотя бы одной мерой, в решении напишите какая мера и как устраняет какую угрозу)

Ответ запишите как: «Да» или «Нет».

Решение:

Проанализируем каждую угрозу и есть ли мера, которая её устраняет:

- A. Подбор пароля

Есть ограничение на 5 попыток (мера 4) → замедляет подбор → Да, защищено

- B. Внедрение скрипта (XSS или инъекция)

Ни одна мера не говорит о проверке ввода, фильтрации данных, обновлении ПО → HTTPS и пароли не помогают → Нет защиты → угроза не устранена

- C. Случайное удаление новости

Есть резервная копия раз в сутки (мера 6) → можно восстановить → Да, защищено

- D. Кража сервера

Есть сервер в запираемом шкафу (мера 8) → физическая защита → Да, защищено

- E. Утечка пароля администратора

Пароль администратора становится общедоступным → Нет организационных мероприятий при компрометации пароля → Нет защиты → угроза не устранена

- F. Сбой - нужно восстановить быстро

Резервная копия раз в сутки → возможна потеря до 24 часов данных → Недостаточно по условию→ угроза не устранена

- G. Фишинг

Пароль сложный, но не мешает вводу на поддельном сайте → Нет двухфакторной аутентификации, обучения пользователей → Меры не защищают от фишинга → Не устранено

Вывод: Угрозы B, E, F, G - не защищены

Ответ: Нет

Баллы	**Критерий получения**
30	Обоснование и ответ верны.
20	В решении допущена одна логическая ошибка, но ответ верный.
15	В решении допущено две логических ошибки, но ответ верный.
1	Ответ верный, решение отсутствует
0	В решении допущено более двух логических ошибок или ответ не верный.

Вариант I

Задания, ответы и критерии оценивания

Задание 1

Школьный сейф защищён электронным замком с трёхзначным кодом (каждая цифра от 0 до 9). Чтобы код был надёжным, установлены правила:

- Первая цифра - нечётная (1, 3, 5, 7, 9);
- Вторая цифра - чётная (0, 2, 4, 6, 8);
- Третья цифра - нечётная;
- Нельзя, чтобы все три цифры были одинаковыми (например, 111 или 555 - запрещены);
- Цифры могут повторяться, если это не нарушает предыдущее правило.

Сколько допустимых кодов можно составить по этим правилам?

Решение:

1. Общее число кодов без запрета на одинаковые цифры:
   - Первая цифра (нечётная): 5 вариантов (1, 3, 5, 7, 9).
   - Вторая цифра (чётная): 5 вариантов (0, 2, 4, 6, 8).
   - Третья цифра (нечётная): 5 вариантов.
   - Общее: 5×5×5=125.
2. Вычтем запрещённые коды, где все три цифры одинаковые. Условие: первая и третья - нечётные, вторая - чётная. Чтобы все три цифры были одинаковыми, средняя должна быть и чётной, и нечётной - это невозможно.
3. Вывод: среди всех возможных кодов по правилам нет ни одного, где все три цифры одинаковые. Запрещённых кодов - 0.

Итоговое число допустимых кодов: 125−0=125

Ответ: 125

Баллы	**Критерий получения**
10	Расчеты и ответ верны.
7	В определении количества комбинаций на одной позиции допущена ошибка, или допущена одна ошибка в расчетах.
4	В определении количества комбинаций на двух позициях допущена ошибка.
1	Ответ верный, решение отсутствует
0	Допущено больше двух ошибок в определении количества допустимых символов или все расчеты не верны.

Задание 2

В школе настраивают систему доступа к электронному журналу. Код состоит из двух символов. Есть два варианта формирования кода:

Режим А:

- Первая позиция - буква: A, B или C;
- Вторая позиция - цифра: 1, 2 или 3;
- Все комбинации разрешены.

Режим Б:

- Первая позиция - буква: A, B, C или D;
- Вторая позиция - цифра: 1, 2, 3 или 4;
- Запрещены коды, где буква и цифра “совпадают по номеру”: A1, B2, C3, D4 - запрещены.

Администратор должен выбрать режим с наибольшим количеством разрешённых кодов, чтобы система была и удобной, и устойчивой к перебору.

Какой режим даёт больше разрешённых кодов? В ответе запишите вариант и цифру, означающую количество допустимых кодов (например, А6)

Решение:

Режим А:

Все комбинации разрешены:

3×3=9

Режим Б:

Общее число комбинаций: 4×4=16

Запрещённые: A1, B2, C3, D4 - 4 кода

Разрешённые: 16−4=12

Сравнение:

- Режим А: 9 кодов
- Режим Б: 12 кодов → больше

Ответ: Б12

Баллы	**Критерий получения**
20	Расчеты и ответ верны.
15	Выбран верный вариант, но допущена одна ошибка в расчетах
13	Верный численный ответ, но в ответе выбрана не верная буква
7	Допущено 2 ошибки в расчетах, но выбран верный вариант
1	Ответ верный, решение отсутствует
0	Допущено 2 ошибки в расчетах, но выбран не верный вариант

Задание 3

В школьной сети 7 устройств:

A. Учительский ноутбук (с антивирусом);

B. Принтер (с антивирусом);

C. Компьютер ученика 1 (без антивируса);

D. Компьютер ученика 2 (без антивируса);

E. Сервер с журналом (с антивирусом);

F. Интерактивная доска (без антивируса);

G. Контроллер безопасности (всегда в сети).

Имеются двусторонние соединения: A–B, B–C, C–D, D–F, A–E, E–G, G–F, G–C.

Правила безопасности:

- Как только вирус попадает на любое устройство без антивируса, контроллер G начинает отсчёт:

– Если в течение одного шага вирус не попадает на ещё одно устройство без антивируса, G отключает только первое;

– Если вирус попадает на второе, G отключает все устройства без антивируса до любого следующего шага.

- Контроллер безопасности не подвержен заражению.

Имеется угроза - вирус появился на устройстве C. Сколько устройств в итоге будут заражены?

Решение

1. Вирус на C (без антивируса) → G начинает отсчёт
2. За один шаг:

   – C → D - D заражён (без антивируса) → второе устройство → G отключает C, D, F до следующего шага

3. Обрываются все их связи
4. Кто заражён:
   - C, D
   - B: C → B - не успел, потому что отключение до следующего шага
   - G: C → G - не успел, потому что отключение до следующего шага
   - F: D → F - не успел, потому что отключение до следующего шага
5. Только C и D заражены.

Ответ: 2

Баллы	**Критерий получения**
40	Расчеты и ответ верны.
30	В решении допущена одна логическая ошибка, но ответ верный.
15	В решении допущено две логических ошибки, но ответ верный.
1	Ответ верный, решение отсутствует
0	В решении допущено более двух логических ошибок или ответ не верный.

Задание 4

В школьном кабинете информатики выявлены 6 угроз безопасности:

1. Ученики оставляют компьютеры включёнными после урока - посторонний может зайти и что-то изменить;
2. Ученики подключают личные флешки - возможен занос вируса;
3. Учитель забывает закрыть дверь на ключ - посторонний может войти в кабинет;
4. На компьютерах не установлен пароль - любой может сесть и начать работу;
5. Wi-Fi включён круглосуточно - к сети может подключиться кто-то из коридора или соседнего класса;
6. Кто-то может украсть системный блок - оборудование не закреплено.

Администрация разрешила внедрить только следующие меры защиты (можно выбрать любые):

A. Установить пароль на вход в каждый компьютер;

B. Запретить использование личных флешек, разрешить только школьные с автоматической проверкой на вирусы;

C. Установить дверной замок и вести журнал выдачи ключей уборщице и учителю;

D. Настроить автоматическое выключение всех компьютеров через 10 минут после окончания урока;

E. Отключать Wi-Fi после уроков по расписанию;

F. Закрепить системные блоки на столах стальными тросами;

G. Внедрить централизованную систему управления устройствами (ЦСУ), которая:
   - автоматически выключает компьютеры;
   - блокирует все USB-порты;
   - управляет включением/отключением Wi-Fi.

Важно: ЦСУ работает только если уже внедрены меры A и C. Без них система не активируется.

Какое наименьшее количество мер нужно внедрить, чтобы полностью устранить все 6 угроз?

Решение:

Ключевая мера: G (ЦСУ) решает угрозы 1, 2, 5 - но только если уже внедрены A и C

Остальные меры:

- A → 4
- C → 3
- F → 6

Используем G, чтобы заменить D, B, E. Для этого обязательны A и C. Добавляем F.
Меры: A, C, G, F → 4
Все угрозы устранены.
Без G потребовалось бы 6 мер - выигрыш.
Ответ: 4

Баллы	**Критерий получения**
30	Обоснование и ответ верны.
20	В решении допущена одна логическая ошибка, но ответ верный.
15	В решении допущено две логических ошибки, но ответ верный.
1	Ответ верный, решение отсутствует
0	В решении допущено более двух логических ошибок или ответ не верный.