ПРОФИЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
2025–2026 уч. г.
10–11 КЛАССЫ

Максимальный балл за работу – 100.

Общая часть

1. **Решение:**
   Надо каждую из ветвей алгоритма проверить в обратном направлении (заменяя влево-вправо и вверх-вниз, читая алгоритм снизу вверх и двигаясь от клетки С4)
   1 ветвь (исходная клетка не закрашена):
   вправо Д4
   вверх Д3
   влево С3
   влево В3
   вверх В2
   вправо С2
   Но клктка С2 закрашена - противоречие

   2 ветвь (исходная клетка закрашена):
   вверх С3
   вверх С2
   влево В2
   вниз В3
   влево А3
   вверх А2
   А2 закрашена, это и есть исходная клетка
   Ответ: А2.

2. **Решение:**
   $12_8=10_{10}$
   $11_{16}=17_{10}$
   $11011_2=27_{10}$
   Такого треугольника не существует, т.к. в треугольники сумма двух любых сторон строго больше третьей не выполняется 10+17=27
   Ответ: нет

3. **Решение:**
   Количество информации в битах – это минимум n, при котором выполняется

$2^n \geq$ число сообщений.

Для 500 сообщений: $2^8=256<500$, $2^9=512>500$, значит 9 бит.

Ответ: 9 бит

4. **Решение:**

В этом диапазоне всего 256 IP-адресов (от 0 до 255). Однако, как правило, первый адрес (192.168.1.0) используется для обозначения сети, а последний (192.168.1.255) - для широковещания. Поэтому для устройств остается 256 - 2 = 254 адреса.

Ответ: 254

5. **Решение:**

Если решать, сравнивая каждый элемент с текущим, то можно найти минимальное число за 8 сравнений. Затем можно найти максимальное число среди оставшихся элементов за 7 сравнений. 8+7 = 15 - это не оптимальный способ.

Оптимальный способ:

1. Сравнить элементы по парам (1-5, 3-8, 2-9, 4-7). У нас 4 сравнения.
2. Среди меньших элементов в каждой паре найти минимум (минимум между 1, 3, 2, 4) – это потребует 3 сравнения.
3. Среди больших элементов найти максимум (максимум между 5, 8, 9, 7) – это потребует 3 сравнения.
4. Итого: 4 + 3 + 3 = 7 сравнений. Так как количество элементов нечетное, то последний элемент нужно сравнить и с текущим max, и с текущим min. 7+1+1=9

Ответ: 9

Специальная часть

6. **Решение:**

a) Пароль «School2024» содержит буквы (S, c, h, o, o, l) и цифры (2, 0, 2, 5). Значит, он содержит и буквы, и цифры. Пароль безопасный.

b) Пароль «school25» содержит буквы (s, c, h, o, o, l) и цифры (2, 5). Значит, он содержит и буквы, и цифры. Пароль безопасный.

c) Пароль «12345678» содержит только цифры, ни одной буквы нет. Это нарушает условие. Пароль небезопасный.

Ответ: a, b

7. **Решение:**

Число вариантов положений колес для первого типа сейфов равно 100^6, а для второго – 2^{80}. Для определения того, какой сейф надежнее, надо сравнить эти

числа. Преобразуем первое число к виду 10^{12}, а второе – 16^{20}. Теперь становится очевидно, что первое число меньше, чем второе. Таким образом, получаем, что второй сейф надежнее.

Ответ: Второй сейф надежнее.

8. Ответ: ГАДВАВГВ

9. Решение:

Рассмотрим произвольную букву открытого и шифрованного текстов. Для соответствующих им (по таблице) чисел x и c выполняются равенства $x = y + pz$ и $z = y + qx$, при некоторых y, p и q. При этом по условию $c = r_{32}(z)$. Используя свойство сравнений по модулю целого числа, получим: $x - c = pc - qx \pmod{32}$ или $x(1+q)=c(1+p) \pmod{32}$.

Для дальнейшего решения будем пользоваться следующим свойством: если наибольший общий делитель чисел a и n равен 1, то сравнение $x = y \pmod{n}$ равносильно $ax = ay \pmod{n}$. Используя условие задачи для первой буквы открытого и шифрованного текста, получим равенство $2(1 + q) = 6(1 + p) \pmod{32}$.

Заметим, что сравнение $6t = 2 \pmod{32}$ имеет 2 решения по модулю 32:

$t = 11 \pmod{32}$,

$t = 27 \pmod{32}$.

Тогда получим, что $11\cdot(1 + q) = (1 + p) \pmod{32}$ или $27\cdot(1 + q) = (1 + p) \pmod{32}$ для каждого t. Таким образом, $x = 11c \pmod{32}$ или $x = 27c \pmod{32}$ соответственно. Остается воспользоваться полученными соотношениями для остальных букв. Осмысленное слово получается только при втором варианте. А значит, исходное слово ВЕКТОР.

Ответ: ВЕКТОР

10. Решение:

Чтобы удовлетворить условию (1), первые четыре цифры можно выбрать произвольным образом, тогда пятая может быть найдена двумя способами. Следовательно, имеется $2\cdot10^4$ способов выбрать первые пять цифр. Следующие три цифры (a_6, a_7, a_8) выбираем произвольно, а выполнение условия (2) обеспечивается единственно возможным выбором цифры a_9. Таким образом, количество наборов из 9-ти цифр, удовлетворяющих условиям (1) и (2), равно $2 \cdot 10^4 \cdot 10^3 = 2 \cdot 10^7$.

Ответ: $2 \cdot 10^7$

11. Решение:

Общее количество кадров:

3 минуты =180 секунд

180 секунд · 24 кадра/секунда = 4320 кадров

Общее количество пикселей:

4320 кадров · 100 пикселей · 80 пикселей = 34 560 000 пикселей

Количество битов для скрытия в каждом пикселе:

3 канала (R, G, B) · 1 бит/канал = 3 бита

Общее количество битов для скрытия:

34 560 000 пикселей · 3 бита/пиксель = 103 680 000 бит

Количество символов: $\frac{103\ 680\ 000\ \text{бит}}{8\ \text{бит/символ}} = 12\ 960\ 000$ символов

Ответ в тысячах: 12 960 000 / 1000 = 12 960 тысяч

Ответ: 12 960

12. Решение:

1) Каждый пиксель состоит из трёх цветовых каналов: красного, зелёного и синего (RGB).
2) Один символ текста занимает 8 бит памяти.
3) **Если использовать замену по одному значащему биту на всю интенсивность кадра (то есть заменять во всех 8 битах канала), объём скрываемой информации увеличится в 8 раз.**
4) **Для одного символа потребуется 24 бита (по 8 бит на каждый цветовой канал пикселя).**

Ответ: 3,4

13. Решение:

1 способ:

Перепишем все числа в шестнадцатеричной системе счисления.

Получаем $52_{16} + 106D_{16} + 10BF_{16} = 217E_{16} = 8574_{10}$

2 способ:

Перепишем все числа в восьмиричной системе счисления.

Получаем $122_8 + 10155_8 + 10277_8 = 20576_8 = 8574_{10}$

3 способ:

Перепишем все числа в двоичной системе счисления.

Получаем $1010010_2 + 1000001101101_2 + 1000010111111_2 = 10000101111110_2 = 8574_{10}$

4 способ:

Перепишем все числа в десятичной системе счисления.

Получаем $82_{10} + 4205_{10} + 4287_{10} = 8574_{10}$

Переводим в четверичную систему счисления. Получаем 2011332_4.

Ответ: 2011332_4

14. Решение:

1) Преобразование каждого символа слова «Ryazan» в двоичный код ASCII

Символ	ASCII-код	Двоичное представление (8 бит)
R	82	01010010
y	121	01111001
a	97	01100001
z	122	01111010
a	97	01100001
n	110	01101110

2) Объединение двоичных кодов в одну длинную строку

Соединяем полученные двоичные коды:

01010010 01111001 01100001 01111010 01100001 01101110

Объединяем без пробелов:

010100100111100101100001011110100110000101101110

Длина строки: 6 байт · 8 бит = 48 бит.

3) Разбиение строки на группы по 6 бит

Делим полученную строку на 8 групп по 6 бит:

010100

100111

100101

100001

011110

100110

000101

101110

4) Преобразование каждой 6-битной группы в десятичное число

Двоичное	Десятичное
010100	20
100111	39
100101	37
100001	33
011110	30
100110	38
000101	5
101110	46

5) Замена чисел из таблицы Base64 на соответствующие символы

20 → U

39 → n

37 → l

33 → h

30 → e

38 → m

5 → F

46 → u

Итоговая строка Base64: UnlheFu

Ответ: UnlheFu

15. Решение:

Результат кодирования Base64 всегда короче оригинальных данных.

Base64 используется для кодирования двоичных данных в текстовый формат.

Base64 широко используется для кодирования изображений в формате PNG и JPEG в HTML.

Base64 является методом шифрования и обеспечивает безопасность данных.

Ответ: 2, 3

16. Ответ:

Запрос на подпись сертификата, отправляется в удостоверяющий центр для получения подписанного сертификата.	.rules
Архивные файлы, содержащие Java code, могут содержать вредоносный код.	.csr
Файлы с правилами для систем обнаружения вторжений (IDS) и межсетевых экранов.	.hash
Файлы конфигурации для сетевых устройств и приложений, которые могут содержать настройки безопасности.	.jar
Файлы, содержащие хеш-суммы файлов. Используются для проверки целостности файлов.	.conf

17. Ответ:

Обеспечивает безопасный удаленный доступ к компьютеру или устройству. Шифрует весь трафик, включая пароли.	**Kerberos**
Протокол сетевой аутентификации, использующий тикеты для подтверждения подлинности пользователей и служб.	**SSH**
Протокол аутентификации, авторизации и учета для пользователей, подключающихся к сети через сетевые устройства.	**PGP**
Фреймворк аутентификации, используемый в беспроводных сетях и других типах соединений, поддерживает различные методы аутентификации.	**RADIUS**
Протокол для шифрования и подписи электронной почты и других данных.	**EAP**

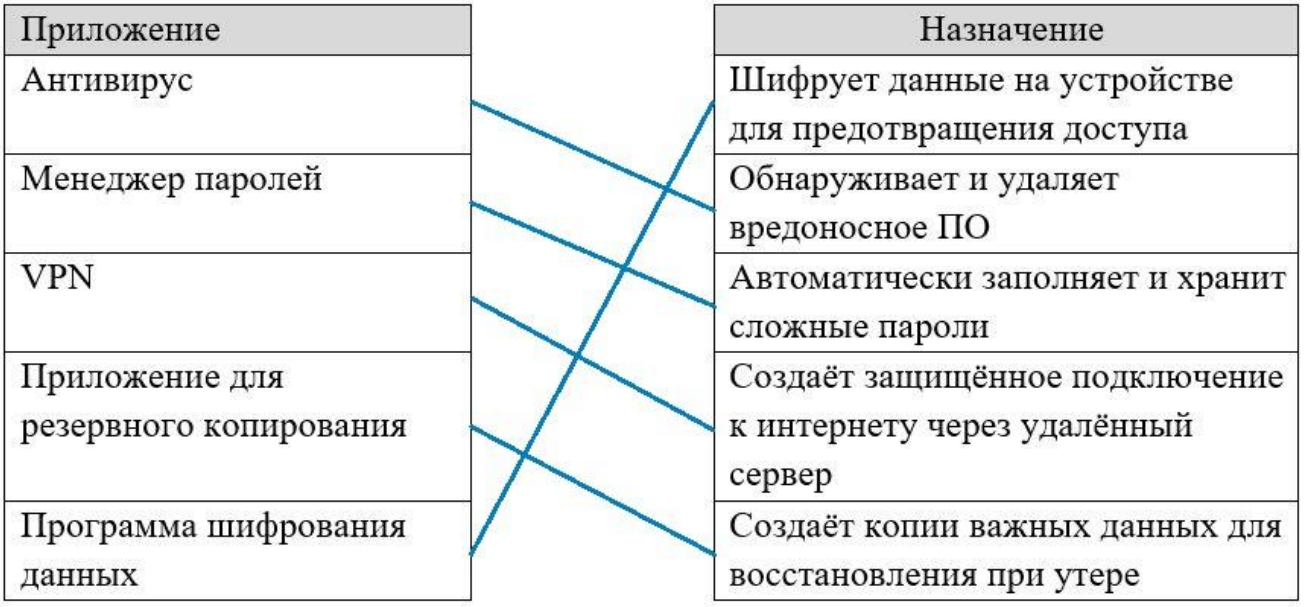
18.Ответ:

Обеспечение конфиденциальности данных (предотвращение несанкционированного доступа к информации).	Шифрование
Подтверждение авторства (аутентификация отправителя и гарантия того, что сообщение не было подделано) и неотказуемость (отправитель не может отрицать факт отправки сообщения).	Криптографические протоколы
Обеспечение целостности данных (обнаружение изменений в информации после ее создания или передачи).	Электронная подпись
Обеспечение безопасной передачи данных по сети.	Хеширование

19.Ответ:

Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).	Обработка персональных данных
Физическое лицо, к которому относятся персональные данные.	Оператор персональных данных
Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными.	Субъект персональных данных
Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.	Конфиденциальность персональных данных
Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.	Персональные данные

20.Ответ:



21.Ответ:

1. 178.248.235.114
2. TLSv1.3
3. 162
4. a