

### Ключи

## МАКСИМАЛЬНЫЙ БАЛЛ ЗА ВСЕ ЗАДАНИЯ – 100.

### Общая часть

#### ЗАДАНИЯ №№ 1-5 ОЦЕНИВАЮТСЯ В 2 БАЛЛА (ставить 0 или 2)

Задание 1.

Обычно промышленные технологии состоят из нескольких частей, которые называются **производственными** технологиями.

Задание 2. **ОТВЕТ ОЦЕНИВАЕТСЯ ПО ОБЩЕМУ СМЫСЛУ**

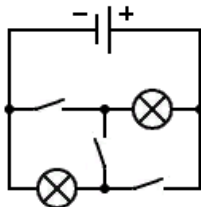
1 – **строительная основа** (оформление стен, пола, потолка)

2 – **предметная наполненность** (мебель, бытовая техника)

Задание 3.

К	О	М	П	О	З	И	Т
---	---	---	---	---	---	---	---

Задание 4.



Задание 5.

– А) 30

– Б) 130

### Специальная часть

#### ЗАДАНИЯ №№ 6-40 ОЦЕНИВАЮТСЯ В 2 БАЛЛА (ставить 0 или 2)

Задание 6. 2.

Задание 7. СОВЕЩАНИЯ

Задание 8. 26316251

Задание 9. – Б) РЕНОВАЦИЯ.

Задание 10. 44

Задание 11. – А) однофакторная аутентификация

Задание 12. – А) доступность похищенных данных

– Б) конфиденциальность похищенных данных

Задание 13. – А) нарушил доступность информации, к которой имели доступ пользователи

Задание 14. – А) доступность данных

– Б) конфиденциальность данных

– В) целостность данных

Задание 15. – А) доступность данных

– В) целостность данных

Задание 16. – Б) конфиденциальность похищенных данных

Задание 17. – Б) конфиденциальность похищенных данных

– В) целостность похищенных данных

Задание 18. – А) доступность хранимых данных

– В) целостность хранимых данных

Задание 19. – А) не нарушили безопасность передаваемой информации

Задание 20. – Б) функции хэширования

Задание 21. – Г) электронная подпись

Задание 22. – А) надежные цифровые водяные знаки

Задание 23. – Б) функции хэширования

– В) хрупкие цифровые водяные знаки

- Задание 24. – Г) \_электронная подпись\_
- Задание 25. – В) \_обеспечение целостности хранимых на сервере файлов\_
- Задание 26. – В) \_пара входных значений, для которых значения функции совпадают\_
- Задание 27. – Б) \_контроль неизменности продуктов, распространяемых по лицензии\_
- Задание 28. – А) \_аутентификация на основе фактора владения\_  
– Г) \_однофакторная аутентификация\_
- Задание 29. – Г) \_биометрическая аутентификация
- Задание 30. – В) \_трёхфакторная аутентификация\_
- Задание 31. – А) \_доступность похищенных данных\_  
– В) \_целостность похищенных данных\_
- Задание 32. – А) \_не нарушили информационную безопасность\_
- Задание 33. – А) \_доступность хранимых данных\_  
– Б) \_конфиденциальность хранимых данных\_  
– В) \_целостность хранимых данных\_
- Задание 34. – Б) \_нарушило конфиденциальность собираемой информации\_
- Задание 35. – Б) \_функции хэширования\_
- Задание 36. – Г) \_проверки электронной подписи\_
- Задание 37. – В) \_осуществить подмену информации, от которой вычислена функция\_

Задание 38. – Г) \_существенное изменение значения функции при внесении изменений во входное значение\_

Задание 39. – В) \_двухфакторная на основе факторов владения и биометрии

Задание 40. – Б) \_двухфакторная биометрическая на основе факторов знания и владения\_

### МАКСИМАЛЬНЫЙ БАЛЛ ЗА ЗАДАНИЕ № 41 – 20.

Задание 41. В ответе могут присутствовать следующие предусмотренные сочетания:

- 1) паспортные данные пассажиров – оптический канал – сканирование паспорта или ввод данных с клавиатуры – скрытая камера, установленная рядом с терминалом (допустимо любое иное устройство, позволяющее подсмотреть информацию с документа или при вводе с клавиатуры) **К1**;
- 2) паспортные данные пассажиров – радиоэлектронный канал – сканирование паспорта или ввод данных с клавиатуры – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу) или его общее описание **К2**;
- 3) паспортные данные пассажиров – акустический канал – ввод данных с клавиатуры – подслушивающее устройство, установленное рядом с терминалом (допустимо любое иное устройство, позволяющее подслушать нажатия клавиш **К3**;
- 4) данные других документов пассажиров – оптический канал – сканирование документа – скрытая камера, установленная рядом с терминалом (допустимо любое иное устройство, позволяющее подсмотреть информацию с документа) **К4**;
- 5) данные других документов пассажиров – радиоэлектронный канал – сканирование документа – устройство перехвата ПЭМИН (побочных

электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу) или его общее описание **К5**;

6) номер, срок действия и владелец карты (напечатаны на лицевой стороне карты) – оптический канал – момент вставки карты в терминал/получения карты из терминала – скрытая камера, установленная рядом с терминалом (допустимо любое иное устройство, позволяющее подсмотреть информацию с лицевой стороны карты) **К6**;

7) номер, срок действия и владелец карты – радиоэлектронный канал – операции с картой через терминал – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу, или его общее описание) **К7**;

8) CVV-код (напечатан на оборотной стороне карты) – оптический канал – момент вставки карты в терминал/получения карты из терминала – скрытая камера, установленная рядом с терминалом (допустимо любое иное устройство, позволяющее подсмотреть информацию с лицевой стороны карты) **К8**;

9) PIN-код – оптический канал – ввод PIN-кода – скрытая камера, установленная рядом с терминалом (допустимо любое иное устройство, позволяющее подсмотреть информацию с клавиатуры) **К9**;

10) PIN-код – акустический канал – ввод PIN-кода – подслушивающее устройство, установленное рядом с терминалом (допустимо любое иное устройство, позволяющее подслушать нажатия клавиш) **К10**;

11) PIN-код – радиоэлектронный канал – ввод PIN-кода – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу) **К11**.

Каждое корректно описанное сочетание – **2 балла** (частичных баллов не предусмотрено, 10 сочетаний из предусмотренных 11 достаточно для получения максимального балла).

Если сумма баллов за корректные сочетания меньше 20, то могут быть начислены бонусные баллы (**К12**):

- за каждое корректное сочетание вне списка предусмотренных – **2 балла**;
- за рассмотрение каждого дополнительного способа или устройства реализации несанкционированного доступа к информации для уже засчитанного сочетания – **1 балл**.

**МАКСИМАЛЬНЫЙ БАЛЛ ЗА ЗАДАНИЕ № 41 – 20.**