ПРОФИЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
2025–2026 уч. г.
9 КЛАСС

Максимальный балл за работу – 100.

Общая часть

1. Какое минимальное количество бит нужно, чтобы закодировать 50 различных сообщений

2. Определите, что будет выведено на экран в результате выполнения следующего алгоритма:

```
x = 15
y = 32
ЕСЛИ x > y ТО
  z = x - y
ИНАЧЕ
  z = y - x
КОНЕЦ ЕСЛИ
ВЫВЕСТИ z
```

3. В сети используются 2 коммутатора, каждый с 48 портами. Первый коммутатор занят 30 портами, второй — 20. Можно ли подключить еще устройства к этим коммутаторам без их замены? Если можно, то сколько портов останутся свободными? Если нельзя подключить еще устройства, то сколько портов не хватает?

4. В компьютерной сети используются IP-адреса из диапазона 192.168.1.0 - 192.168.1.255. Сколько устройств может быть подключено к этой сети?

5. Дан фрагмент таблицы базы данных «Ученики»:

ID	Фамилия	Имя	Класс
1	Иванов	Иван	9А
2	Петров	Петр	9Б
3	Сидоров	Сергей	9А
4	Смирнов	Анна	9В

Какой запрос нужно выполнить, чтобы получить список фамилий учеников из класса 9А? Запишите запрос на простом псевдо-языке.

Специальная часть

6. В магазине имеются сейфы с замками двух типов. Первый открывается, если каждый из восьми его кодовых дисков установить в нужное положение. Каждый диск имеет 100 положений. Второй тип сейфового замка содержит 100 переключателей по два положения у каждого. Сейф открывается только при установке каждого переключателя в нужное положение. Какой сейф надежнее?

7. Выберите все правильные утверждение, касающееся предыдущей задачи.

1) Надежность сейфа определяется общим количеством возможных комбинаций замка. Чем больше комбинаций, тем сложнее подобрать код, и, следовательно, сейф надежнее.
2) Количество комбинаций для первого сейфа (с дисками) равно $8 \cdot 100 = 800$.
3) Для первого сейфа (с дисками) количество комбинаций нужно вычислять как 100^8.
4) Для решения задачи достаточно сравнить основания степеней - чем больше основание, тем надежнее сейф.

8. Для шифрования сообщений Анна и Иван использовали шифр Сцитала: на круглую палочку виток к витку без просветов и нахлёстов наматывалась лента.
При горизонтальном положении палочки на ленту по всей длине стержня построчно записывался текст сообщения без знаков препинания и пробелов. После этого ленту разматывали и, с записанным на ней текстом, посылалась адресату. Иван передал Анне ленту, на которой было написано вот что:

К сожалению, Анна свою палочку потеряла, но она видит, что лента исписана полностью, и знает, что при намотке ленты было сделано целое число оборотов. Помогите ей восстановить сообщение.

9. В Криптограде используется алфавит, состоящий из четырёх латинских букв a,b,c,d. Любая последовательность букв алфавита будет словом криптоградского языка при выполнении единственного ограничения: если в последовательности есть хоть одна буква «a», то тогда в ней обязательно должны встретиться две буквы «a» подряд. Например, последовательности baacda, aabb, ddd, baaacd являются словами, а последовательности bcadda,abba – не являются. Найдите число слов длины 8 в криптоградском языке.

10. Выберите **все** верные утверждения, касающиеся предыдущей задачи.
Утверждения:

1) Если в слове есть только одна буква «а», то его можно отбросить.
2) Все слова, содержащие «аа», нужно включать в ответ
3) Задачу решить аналитически не возможно, решение возможно только программно.
4) С учетом того, что все слова складываются из a, b, c, d и длины 8, то существует только одно слово «аааааааа», которое подходит по условия задачи.

11. Радиопередатчик в течение 20 минут передавал информационное сообщение со скоростью 10 байт в секунду. Сколько символов содержало данное сообщение, если установлено, что использовался алфавит из 33-х символов русского языка и пробела?

12. Злоумышленник планирует внедрить вредоносный код, занимает 4 килобайта, в BMP-изображение. Каждый пиксель представлен в 24-битном формате (8 бит на красный, 8 бит на зеленый, и 8 бит на синий цвет). Хакер использует метод наименее значимого бита (LSB) для скрытия кода, изменяя LSB каждого цветового компонента пикселя. Сколько пикселей хакеру потребуется изменить, чтобы вместить весь код, используя LSB стеганографию? Результат запишите в виде числа.

13. Выберите **все** верные утверждения, относящиеся к предыдущей задаче.
Утверждения:
1) Каждый пиксель изображения позволяет скрыть 1 байт информации.
2) Вредоносный код занимает 32768 бит информации.
3) Для скрытия кода потребуется изменить более 15000 пикселей изображения.
4) Хакер может скрыть код, не изменяя визуально изображение.

14. В тексте, состоящем из 24 букв и записанном без пробелов, буквы переставлены по следующему правилу:
24-я буква поставлена на 1-е место,
1-я буква – на 2-е место,
23-я – на 3-е место,
2-я – на 4-е
22-я – на 5 и так далее (в конце 13-я буква поставлена на 23-е место, 12-я – на 24-е).
Затем такую же процедуру повторили ещё 85 раз. В результате получилось ААЯАНМШСЧЕИИИТФМРСРМТИСЕ. Найдите исходный текст

15. Зашифруйте сообщение ПАРОЛЬ по такому же принципу, как в предыдущем задании:
6-я буква поставлена на 1-е место,
1-я буква – на 2-е место,

5-я – на 3-е место,
2-я – на 4-е место,
4-я – на 5-е место,
3-я - на 6-е место.
Если процедуру повторили 7 раз.

16. Сопоставьте расширения файлов с описанием типов файлов, соответствующих этим расширениям.

Расширения файлов: .bat, .ps1, .dll, .scr, .vbs, .rtf

Библиотека динамической компоновки. Может содержать исполняемый код, используемый другими программами. Злоумышленники могут подменять эти файлы для внедрения вредоносного кода.	.scr
Текстовый файл, содержащий команды, выполняемые операционной системой Windows. Может использоваться для автоматизации задач или, в злонамеренных целях, для причинения вреда системе.	.bat
Экранная заставка Windows. Файлы этого типа могут содержать исполняемый код и использоваться для распространения вредоносного ПО.	.rtf
Скрипт на языке Visual Basic Scripting Edition. Может использоваться для автоматизации задач или выполнения вредоносных действий в Windows.	.dll
Текстовый документ в формате Rich Text Format. Использует форматирование текста с внедрением различных объектов. Является потенциально опасным, так как может содержать вредоносный код, например, эксплойты для программ обработки документов.	.vbs

17. Сопоставьте названия протоколов с их назначениями.

Названия протоколов: SSH, SFTP, SSL/TLS, FTP, IPSec

Протоколы для шифрования соединений; обеспечивают конфиденциальность и целостность трафика.	SSH
Протокол для безопасного удалённого доступа к серверам; шифрует команды и передаваемые данные.	SFTP
Протокол для передачи файлов; незащищённый, риск перехвата файлов и учётных данных.	SSL/TLS
Безопасная версия FTP; шифрует передачу файлов для защиты от прослушки.	FTP

Протокол для шифрования IP-пакетов; используется в VPN для защиты сетевых соединений.	IPSec

18. Установите соответствия между средствами защиты информации и атаками на информационную систему.

Межсетевой экран (файрвол)	Фишинг
Шифрование данных	DDoS-атака
Аутентификация пользователей	Неавторизованный доступ
Регулярное обновление ПО	Атака «человек посередине» (MITM)

19. Установите соответствия между терминами, относящимися к социальной инженерии, и их описаниями.

Термины из социальной инженерии: вишинг, смс-фишинг, предтекстинг, пиггибэкинг.

a) Использование ложной информации для получения данных от жертвы.
b) Отправка мошеннических SMS-сообщений с целью кражи данных.
c) Получение информации о жертве, чтобы создать доверительное отношение.
d) Атака, при которой злоумышленник использует телефон для получения конфиденциальной информации.

20. Выберите **все** верные высказывания об уязвимостях кибербезопасности.

a) Уязвимость в программном обеспечении может быть использована злоумышленниками для получения несанкционированного доступа к системе.
b) Все уязвимости являются результатом недостатков в коде или архитектуре программного продукта.
c) Социальная инженерия не относится к уязвимостям кибербезопасности, так как она не связана с технологиями.
d) Уязвимости могут существовать как в аппаратном, так и в программном обеспечении.

21. Вам представлен скриншот вывода работы консольной утилиты nmap, которая используется для сканирования сетей и определения открытых портов на устройствах. Изучите представленный вывод и ответьте на вопросы.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-17 10:00 MSK
Nmap scan report for 192.168.1.1
Host is up (0.002s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

a) Сколько портов было обнаружено открытыми на устройстве с IP-адресом 192.168.1.1?

b) Какой порт используется для безопасного веб-сервиса? В ответе укажите номер порта.

c) Какой порт может использоваться для удалённого доступа к устройству через командную строку? В ответе укажите номер порта.

d) Что означает статус "Host is up" в выводе nmap?

1) Устройство с указанным IP-адресом недоступно и не отвечает на запросы.
2) Устройство временно отключено от сети.
3) Устройство с указанным IP-адресом доступно и отвечает на запросы.
4) Устройство заблокировано брандмауэром и не может быть обнаружено.

Запишите номер верного варианта ответа.