

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ТЕХНОЛОГИИ
(Муниципальный этап)
ТЕОРЕТИЧЕСКИЙ ТУР

Информационная безопасность

возрастная группа (8 - 9 классы)

Уважаемый участник олимпиады!

Вам предстоит выполнить теоретические и тестовые задания.

Время выполнения заданий теоретического тура 2 академических часа (90 мин.).

Выполнение теоретических (письменных, творческих) заданий целесообразно организовать следующим образом:

- не спеша, внимательно прочитайте задание и определите, наиболее верный и полный ответ;
- отвечая на теоретический вопрос, обдумайте и сформулируйте конкретный ответ только на поставленный вопрос;
- если Вы выполняете задание, связанное с заполнением таблицы или схемы, не старайтесь детализировать информацию, вписывайте только те сведения или данные, которые указаны в вопросе;
- особое внимание обратите на задания, в выполнении которых требуется выразить Ваше мнение с учетом анализа ситуации или поставленной проблемы. Внимательно и вдумчиво определите смысл вопроса и логику ответа (последовательность и точность изложения). Отвечая на вопрос, предлагайте свой вариант решения проблемы, при этом ответ должен быть кратким, но содержать необходимую информацию;
- после выполнения всех предложенных заданий еще раз удостоверьтесь в правильности выбранных Вами ответов и решений.

Выполнение тестовых заданий целесообразно организовать следующим образом:

- не спеша, внимательно прочитайте тестовое задание;
- определите, какой из предложенных вариантов ответа наиболее верный и полный;
- напишите букву или цифру, соответствующую выбранному Вами ответу;
- продолжайте, таким образом, работу до завершения выполнения тестовых заданий;
- после выполнения всех предложенных заданий еще раз удостоверьтесь в правильности ваших ответов;
- если потребуется корректировка выбранного Вами варианта ответа, то неправильный вариант ответа зачеркните крестиком, и рядом напишите новый.

Предупреждаем Вас, что:

- при оценке тестовых заданий, где необходимо определить один правильный ответ, 0 баллов выставляется за неверный ответ и в случае, если участником отмечены несколько ответов (в том числе правильный), или все ответы;
- при оценке тестовых заданий, где необходимо определить все правильные ответы, 0 баллов выставляется, если участником отмечены неверные ответы, большее количество ответов, чем предусмотрено в задании (в том числе правильные ответы) или все ответы.

Задание теоретического тура считается выполненным, если Вы вовремя сдаете его членам жюри.

Максимальная оценка – 60 баллов.

Общая часть

1. Вставьте пропущенные слова.

_____ – это финансовый план, который учитывает и сопоставляет все доходы и расходы семьи за определенный период (месяц, год и др.)

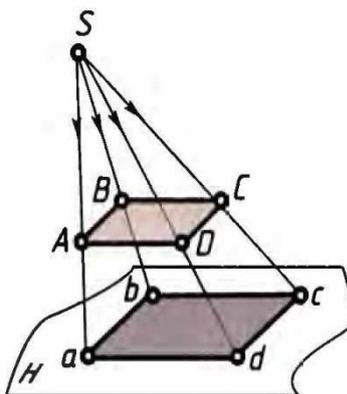
2. По какому специальному признаку разные профессии подразделяют на три общих класса: гностические (познавательные), изыскательские и преобразующие? Приведите не менее чем по два примера профессий для каждого из этих классов.

Ответ:

3. Что означает терминологическое понятие «чистый пар», используемое в сельскохозяйственной земледелии? Объясните его смысл.

Ответ: _____

4. Изображение какого способа (метода) проецирования показано на рисунке и какое специальное название имеет особая точка S в этом методе?



Ответ: _____

5. Каким физическим способом и с помощью каких технических решений, каких устройств, получают основной объем электроэнергии на современной космической орбитальной станции?

Ответ

Специальная часть

1. Авиакомпания N для облегчения пилотирования самолётов устанавливает на них системы автоматического управления (автопилот). Для запуска работы такой системы пилот должен ввести координаты пунктов отправления и назначения, параметры самолёта, а также авторизационные данные для связи с наземными диспетчерскими службами по пути следования. Далее система осуществляет пилотирование по указаниям наземных служб, передавая управление пилоту в случае необходимости принятия решений, возникновении внештатных ситуаций и в иных предусмотренных случаях. Оцените, какие из утверждений являются верными, а какие нет.

- A. Для обеспечения корректного исполнения поступающих от наземных служб указаний требуется обеспечить, в первую очередь, их конфиденциальность. (_____)
- B. Для того, чтобы наземные службы могли постоянно следить за координатами самолёта, требуется обеспечить доступность этих данных. (_____)
- C. Для корректного принятия решений системой пилотирования с учётом параметров самолёта необходимо обеспечить целостность этих данных в памяти программы. (_____)
- D. Пилоты в момент пилотирования могут рассматриваться в качестве потенциальных нарушителей безопасности информации в системе. (_____)
- E. Во время полёта пассажирам может быть запрещено использовать коммуникационные устройства из-за возможности нарушения доступности сигналов от наземных служб при случайном совпадении частот сигналов и внесения искажений. (_____)

За каждый верный ответ – 1 балл.

Максимум за задание – 5 баллов.

2. Вы являетесь специалистом по криптографии в компании «КриптоСекрет Ltd.», которая занимается разработкой криптографических решений. Ваша задача – обеспечить безопасность данных компании и клиентов.

Компания решает разработать свой криптографический алгоритм для защиты данных. Что требуется сделать, чтобы создать надёжный алгоритм шифрования?

- A. Выбрать случайные, никогда ранее не использовавшиеся в шифровании математические операции и создать алгоритм.
- B. Провести анализ существующих криптографических алгоритмов и их уязвимостей.
- C. Попросить сотрудников компании придумать алгоритм, так как они лучше знают служебные данные.
- D. Использовать для построения алгоритма закономерности из других областей знаний – физики, лингвистики, химии и т. п.

За верный ответ – 1 балла.

3. Клиенты «КриптоСекрет Ltd.» хотят зашифровать свои данные перед передачей через открытую сеть. Какой метод шифрования из перечисленных следует рекомендовать?

- A. Симметричное шифрование методом «по модулю».
- B. Асимметричное шифрование с использованием ЭЦП.
- C. Симметричное шифрование с использованием блочного шифра.
- D. Асимметричное шифрование с помощью стеганографии.

За верный ответ – 1 балла.

4. Как часто рекомендуется обновлять ключи шифрования для обеспечения безопасности данных?

- A. Не реже раза в месяц, как и пароли доступа к системе.
- B. С периодом времени, не превышающем половину оценочного времени на подбор криптографического ключа нарушителем.
- C. По разработанному графику, а также при определённых условиях – например, при наличии признаков того, что ключ стал известен нарушителю.
- D. При вводе в действие новых криптографических систем.

За верный ответ – 1 балла.

5. Какие меры защиты из перечисленных наиболее эффективно предпринять для защиты от возможного перебора паролей доступа к системе?

- A. Внедрить механизм двухфакторной аутентификации – требовать при доступе ввода пароля и предъявления электронного ключа
- B. Регулярно менять пароли для всех учётных записей пользователей.
- C. Отключить сетевой доступ к системе
- D. Провести инструктирование пользователей о способах перебора паролей и принципах подбора стойких паролей.

За верный ответ – 1 балла.

6. Расследуя хакерскую атаку, полицейские обнаружили среди файлов нарушителей зашифрованный текст:

Н ЦКЦРПРОДЬЁРЙ КВО ОРЦЦ ОРПНРП ЮВКЦМВРЦ АЗЪБРНДЬ ЧЛЮЩЯЩЬ,
ОЗЛНКЛ ЕЛКУЛК Н ОПРЕКРНРАЛНЛМ ЮВМАР. НХНРЕЭ РТЛ ЩЮ ОЦПЛЭ, МХ
ЧВПВЗЩЮДРМ ПВИЛЦД НОРЙ ОЩОЦРМХ.

По их предположениям, для его шифрования применён шифр простой замены, то есть каждая буква алфавита была заменена во всём тексте какой-то другой буквой того же алфавита. Известно, что в тексте имеется слово «СЕРВЕР».

Как зашифровано слово «СЕРВЕР»?

- A. ЕЛКУЛК
- B. ОРПНРП
- C. ОПРЕКР
- D. ОЗЛНКЛ

За верный ответ – 4 балла.

7. Какое слово зашифровано текстом «АЗЪБРНДЬ»?

- A. ЗАНИМАЕТ
- B. СЕТЕВЫМИ
- C. СИСТЕМАМ
- D. КЛЮЧЕВУЮ

За верный ответ – 4 балла.

8. Определите слово, присутствующее в открытом тексте обнаруженного файла, которое при другом ключе могло бы быть зашифровано так же, как и слово «СЕРВЕР» в приведённом тексте.

- A. ПОНТОН
- B. КЕРНЕР
- C. ДОНЖОН
- D. КОСМОС

За верный ответ – 4 балла.

9. Зашифруйте при помощи использованного ключа замены слово «МАРШРУТИЗАТОР».

- A. МВПГЦДЩЮВЦЛП
- B. РДФЬФЧЦМЛДЦТФ
- C. ЗЭЧБЧЦМЮУЭМКЧ
- D. АЬЛЯЛМПУСЬПОЛ

За верный ответ – 4 балла.

10. Сотрудники полиции столкнулись с новой формой кибермошенничества. Финансовая криптопирамида. Известный хакер Кеша Митников проник в крупную фирму «Мелкомягкие» под видом сетевого специалиста. Для того чтобы собрать доказательства сотрудникам фирмы нужно проанализировать сетевой трафик. Известно, что фирма имеет сеть IPv4 с адресом 54.123.192.0 с маской 255.255.248.0. В этой сети Кеша поступил следующим образом. Разбил исходную сеть на подсети, в которых содержится не менее 100 и не более 200 адресов в каждой, пронумеровав их начиная с 1. Из них каждую сеть с чётным

номером он использовал для нужд фирмы в качестве конспирации, оставшиеся сети (назовём их сети А) он использовал для своих криптофинансовых махинаций. Пронумеровав отдельно сети А, каждую сеть А с чётным номером он разбил на 4 равных подсети (назовём их сети В), а каждую сеть А с нечётным номером он разбил на подсети, в каждой из которых содержится не менее 24 и не более 40 адресов (назовём их сети С). Сети С он разбил на четыре равные части (назовём их сети D), а сети В он разбил на подсети, в которых содержится не менее 6 и не более 10 адресов (назовём их сети Е). В каждой сети Е он запустил по 2 компьютера для майнинга криптовалюты «МиМиМи», для чего без ведома руководства закупил компьютерные комплектующие. Подготовка каждого неучтённого устройства обошлась ему в 75000 рублей. В каждой сети D он также использовал по 2 точно таких же компьютера для майнинга. Для каждой из этих подсетей (D и Е) он закупил (опять же без ведома руководства) крутой роутер фирмы «Кисцо» стоимостью в 100500 рублей.

Каждый компьютер для майнинга генерирует трафик со скоростью 100 Кбит/с.

Пояснение

В терминологии сетей TCP/IP маской сети называют двоичное число, которое показывает, какая часть IP-адреса узла сети относится к адресу сети, а какая – к адресу узла в этой сети. Адрес сети получается в результате применения поразрядной конъюнкции к заданному IP-адресу узла и его маске. Разбиение на подсети происходит путём выделения дополнительных бит для маски сети.

Пример: Дан IPv4-адрес 192.168.1.175. Маска подсети 255.255.255.0 Тогда адрес сети будет 192.168.1.0

Если увеличить маску подсети на 4 бита (255.255.255.240), то адрес сети для искомого адреса будет 192.168.1.160

Определите количество компьютеров, запущенных Кешей для майнинга.

Ответ: _____

За верный ответ – 4 баллов.

11. Определите, какой ущерб (в рублях) Кеша нанёс фирме, закупив лишние компьютеры и роутеры.

Ответ: _____

За верный ответ – 4 баллов.

12. Известно, что Кеша любит тройки ещё со школы, поэтому каждый раз при делении подсетей он заходил в третью подсеть. При последнем делении он выбрал для своего компьютера третий адрес в сети. Определите, какой из IP-адресов принадлежит Кеше.

- A. 54.123.198.117
- B. 54.123.197.53
- C. 54.123.192.17
- D. 54.123.193.83
- E. 54.123.196.111
- F. 54.123.194.51

За верный ответ – 4 баллов.

13. Определите, какое слово зашифровано шифртекстом 36 16 35 16 42 24 46 24 63.

- А. РЕПУТАЦИЯ.
- В. РЕНОВАЦИЯ.
- С. РЕПЕТИЦИЯ**

За верный ответ – 3 балла.

14. Условие (описание ситуации) для заданий №№14-16:

Руководство банка решило усовершенствовать системы информационной безопасности и для этого внедрить новые способы аутентификации. На основе анализа угроз было принято решение защищать как информационные ресурсы организации, так и служебные помещения от несанкционированного доступа.

Для обеспечения контроля пропуски сотрудников была нанята охрана и установлены пропускные турникеты, к которым сотрудники должны прикладывать смарт-карты. Какие типы аутентификации реализованы? Выберите 2 варианта.

- А. однофакторная аутентификация
- В. аутентификация на основе фактора владения
- С. аутентификация по ЭЦП
- Д. двухфакторная аутентификация**

За верный ответ – 3 балла.

15. Перед входом в каждый служебный кабинет стоит робот, который получает уведомление о посетителе и просит его пройти аутентификацию, чтобы войти внутрь. Для этого требуется встать на отмеченную позицию перед роботом и замереть на несколько секунд, пока робот проводит «осмотр» и сопоставляет отсканированную картинку с внутренней базой данных сотрудников. Какой тип аутентификации используется?

- А. биометрическая аутентификация
- В. аутентификация на основе фактора знания
- С. аутентификация по ЭЦП
- Д. аутентификация по GPS**

За верный ответ – 2 балла.

16. Для запуска компьютера на рабочем месте сотрудника руководство установило следующую систему: сначала она требует ввести PIN-код, после его успешного ввода пользователю требуется поднести электронный ключ к считывателю, а если ключ распознан как корректный, то пользователю предлагается приложить палец к сканеру. Укажите, какая система аутентификации реализована.

- А. трёхфакторная аутентификация
- В. однофакторная аутентификация
- С. двухфакторная аутентификация**

За верный ответ – 2 балла.

17. Условие (описание ситуации) для заданий №№ 17-20:

В компании «N» усовершенствовали систему информационной безопасности. После этого информационная система компании стала целью атаки со стороны злоумышленников.

Сначала нарушители решили скомпрометировать системы шифрования компании, для чего осуществили перехват ключа шифрования в момент передачи с аппаратного носителя в систему шифрования. Реализация такой угрозы нарушила

- А. целостность похищенных данных
- В. доступность похищенных данных
- С. конфиденциальность похищенных данных**

За верный ответ – 2 балла.

18. Выберите все правильные ответы. После успешной компрометации ключа шифрования нарушители перехватили несколько передаваемых по сети зашифрованных сообщений и, заблокировав их доставку получателю, прочли их и подменили на собственные, которые затем были отправлены по назначению. Реализация такой угрозы нарушила

- А. целостность похищенных данных
- В. доступность похищенных данных
- С. конфиденциальность похищенных данных

За верный ответ – 2 балла.

19. В другом случае нарушители просто исказили хранимую на сервере в зашифрованном виде информацию таким образом, чтобы при попытке её расшифровать пользователь получал лишь бессмысленный набор символов.. Реализация такой угрозы нарушила

- А. целостность похищенных данных
- В. доступность похищенных данных
- С. конфиденциальность похищенных данных

За верный ответ – 2 балла.

20. Помимо системы шифрования целью атаки стала и система электронной подписи, разработанная компанией. Однако ещё до действий нарушителей отправитель (один из сотрудников компании) ошибся в выборе ключа генерации подписи, в результате чего отправленное сообщение не могло пройти проверку подлинности подписи на стороне получателя. Такие действия отправителя

- А. нарушили целостность передаваемой информации
- В. не нарушили безопасность передаваемой информации
- С. нарушили достоверность передаваемой информации
- Д. нарушили доступность передаваемой информации

За верный ответ – 2 балла.

Максимальный балл за работу – 60.