**ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ТЕХНОЛОГИИ**

**ШКОЛЬНЫЙ ЭТАП**

**ТЕОРЕТИЧЕСКИЙ ТУР**

**7-8 классы**

**Профиль «Информационная безопасность»**

**Уважаемый участник олимпиады!**

Вам предстоит выполнить теоретические и тестовые задания. Время выполнения заданий теоретического тура 2 академических часа (90 минут). 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, 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.

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.

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. (Выберите все правильные ответы) Выберите все РАСТРОВЫЕ графические редакторы

А) Paint

Б) Компас

В) Adobe Photoshop

Г) Adobe Illustrator

Д) Corel DRAW

Е) Corel PHOTO-PAINT

1. Прочитайте высказывание, напишите справа «верно» или «неверно».

 Цифры «46» штрихкода означают, что предприятие зарегистрировано в России

1. Напишите три названия профессий, относящихся к системе «человек – художественный образ»
2. .К направлениям биотехнологии не относится:

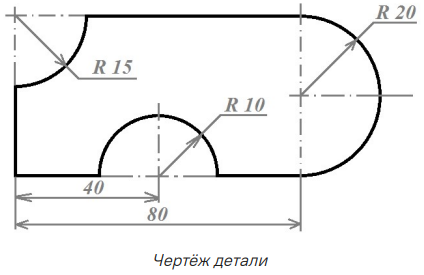
А) генная инженерия;

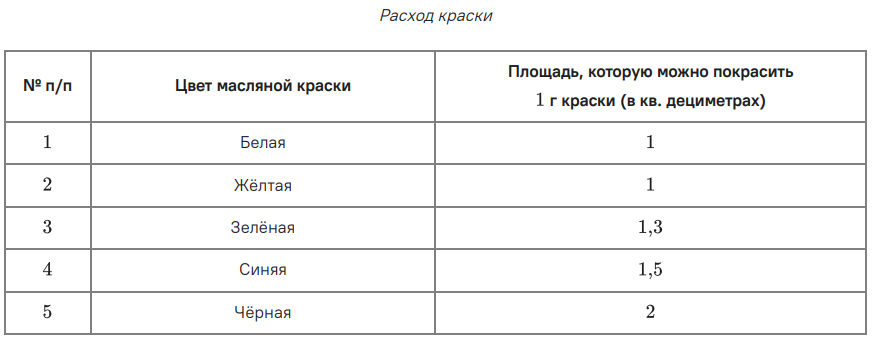
Б) нанотехнология

В) бионика

Г) нейротехнология

1. Определите, сколько краски понадобится (см. расход краски), чтобы покрасить деталь (см. чертеж) с двух сторон желтой масляной краской. Размеры на чертеже указаны в сантиметрах. При расчетах примите π ≈ 3. Ответ дайте в граммах, округлив до целого.





**Специальная часть**

1. .Для удобства продажи железнодорожных билетов на вокзале города N планируют установить терминалы самообслуживания. Пассажиру для приобретения билета потребуется самостоятельно ввести при помощи экранной клавиатуры и встроенного сканера дату отправления и номер поезда, паспортные данные, выбрать место, отсканировать документы, дающие право на приобретение льготного билета, после чего осуществить оплату банковской картой, вставив её в соответствующий разъём терминала и введя PIN-код. Оцените, какие из утверждений являются верными, а какие нет.

А) Отключение терминала от электропитания будет являться нарушением целостности.

Б) Для вводимых данных покупателя потребуется обеспечивать конфиденциальность.

В) Для сведений о поездах и свободных местах потребуется обеспечить доступность.

Г) Пассажиры, покупающие билеты, могут рассматриваться как возможные нарушители информационной безопасности терминалов.

Д) Заклеивая сканер скотчем и оставляя только возможность ввода с клавиатуры, администрация вокзала реализует угрозу нарушения целостности информации.

1. Вас пригласили в компанию «Конфиденциальность Inc.» в качестве специалиста по защите информации. Ваша задача – помочь компании усовершенствовать свои меры по защите конфиденциальных данных. Ваш первый шаг – проведение аудита текущей системы безопасности компании. Выберите наиболее комплексный и корректный вариант действий.

А) Проверить, насколько сложно взломать пароли сотрудников, запуская переборщики паролей.

Б) Выяснить у руководства сведения об информационной системе и на их основе составить план аудита всех аспектов безопасности

В) Провести тестирование на проникновение сетевой инфраструктуры компании.

Г) Провести попытку применения приёмов социальной инженерии к сотрудникам.

Д) Попытаться проникнуть в различные помещения компании.

1. .Вы обнаружили, что многие сотрудники используют слабые пароли. Что лучше всего применить для усиления защиты учётных записей пользователей?

А) Развернуть в системе программное обеспечение, не позволяющее задавать пароли, не отвечающие минимальным требованиям стойкости

Б) Обязать сотрудников сменить пароли в течение суток

В) Ограничить доступ к системе только с определённых IP-адресов.

Г) Оставить ситуацию на усмотрение сотрудников, поскольку это вопрос их удобства работы с системой.

1. При аудите было выявлено, что некоторые компьютеры сотрудников не имеют антивирусного программного обеспечения. Какое решение будет наиболее предпочтительным в такой ситуации?

А) Установить антивирусное программное обеспечение на всех компьютерах за выходной день.

Б) Ознакомить сотрудников с информацией о важности использования антивирусного ПО и предоставить рекомендации по его установке.

В) Запросить согласие руководства компании на выработку и внедрение единой политики установки и использования антивирусного ПО.

Г) Оставить компьютеры без антивирусной защиты, так как это не является критической угрозой, а антивирусное ПО может снизить их производительность.

1. .Как лучше всего организовать обучение сотрудников компании основам информационной безопасности?

А) Организовать встречу с сотрудниками и провести массовое обучение безопасности.

Б) Подготовить обучающие материалы, инструкции и предоставить доступ всем сотрудникам.

В) Провести внезапную проверку безопасности силами приглашённых специалистов, по итогам которой премировать или лишить премий сотрудников, показавших отличные или неудовлетворительные результаты

Г) Разработать программу регулярного информирования, обучения и тестирования сотрудников в области информационной безопасности.

Д) Оставить вопрос на усмотрение самих сотрудников, включив вопрос повышения осведомлённости в вопросах информационной безопасности в их должностные инструкции.

1. .Сотрудники полиции столкнулись с новой хакерской группировкой, которая атакует правительственные сайты. Для того, чтобы раскрыть их, необходимо решить задачу технического характера.

Есть информация о численности группировки и навыках, которыми владеет каждый хакер. При запросе в базе данных для обозначения логической операции «И» используется символ «&», а для логической операции «ИЛИ» символ «|». В таблице приведены запросы и количество найденных по ним записей.

|  |  |
| --- | --- |
| **Запрос** | **Найдено** |
| Социальная инженерия | 715 |
| Технические навыки | 492 |
| Социальная инженерия | технические навыки | 934 |

Разумеется, самыми опасными являются те, кто владеют и социальной инженерией, и техническими навыками. Вычислите их количество.

1. .Расследуя кибератаку, полицейские обнаружили на устройстве предполагаемого нарушителя файл с зашифрованным текстом. На основании анализа других файлов устройства установили, что применён шифр Цезаря – шифр, в котором каждая буква алфавита заменяется буквой того же алфавита с некоторым сдвигом (например, при сдвиге, равном 3, буква «А» будет заменяться на «Г», «Б» – на «Д» и так далее, «Э» – на «А», «Ю» – на «Б», «Я» – на «В»).

Зашифрованный текст выглядит так:

Цчйзетузхещнд н пхнфчузхещнд – учрньтай цфуцуёа цуъхетнчб фехурб ж цйпхйчй. Ирд ёема иеттаъ д фхнсйтдг ж пеьйцчжй фехурд цружу зехетчнд, меэнщхужеттуй цу цижнзус ж уинттеиыечб цнсжуруж. Чеп ут тй ъхетнчцд те пусфбгчйхй ж учпхачус жний, е фхн тйуёъуинсуцчн д жцйзие сузш фуршьнчб йзу цтуже

Определите ключ (величину сдвига), применённый для зашифрования данного текста.

1. .В тексте сообщения имеется слово «фехурб». Какое слово им зашифровали? 

А) всегда 

Б) пароль 

В) хранит 

Г) угроза

1. .Зашифруйте с тем же сдвигом слово «гарантия». 

А) ждфдсцмг 

Б) иёцёушое 

В) зехетчнд 

Г) ёгугрхлв 

Д) йжчжфщпё

1. .Перед специалистом по информационной безопасности поставлена задача обеспечить безопасность сервера компании. Он подготовил перечень возможных угроз, которые относятся к категориям: – угрозы, направленные на нарушение целостности данных на сервере – угрозы, направленные на нарушение доступности данных на сервере Одна и та же угроза может относиться к обеим категориям, только к одной категории или ни к одной из них. Для каждой угрозы выберите соответствующую категорию.

1. DDoS-атака, проводимая конкурентами – это угроза, направленная на нарушение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ данных на сервере.

2. DoS-атака, проводимая хакерской группировкой – это угроза, направленная на нарушение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ данных на сервере.

3. Повреждение кабеля электропитания сервера при проведении ремонтных работ в серверной – это угроза, направленная на нарушение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ данных на сервере.

4. Искажение записей в базе данных, размещённой на сервере – это угроза, направленная на нарушение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ данных на сервере.

5. Искажение и удаление прав доступа к таблицам базы данных определённых пользователей – это угроза, направленная на нарушение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ данных на сервере.

6. Копирование пользователями сведений ограниченного доступа из базы данных на личные носители для продажи конкурентам – это угроза, направленная на нарушение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ данных на сервере.

7. Внедрение в операционную систему сервера вредоносного программного обеспечения, блокирующего таблицы базы данных – это угроза, направленная на нарушение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ данных на сервере.

8. Внедрение в систему управления базой данных вредоносной программы, искажающей записи в таблицах базы данных – это угроза, направленная на нарушение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ данных на сервере.

9. Повреждение и выведение сервера из строя при пожаре – это угроза, направленная на нарушение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ данных на сервере.