Теоретические задания муниципального этапа
всероссийской олимпиады школьников по технологии 2023-24 учебного года
профиль «Информационная безопасность»
10-11 класс
(время выполнения не более 90минут)

Общая часть

1. Документированной информацией, доступ к которой ограничен в соответствии с законодательством РФ, называется
1) Конфиденциальная
2) Персональная
3) Документированная
4) Информация составляющая государственную тайну
5) Информация составляющая коммерческую тайну

2. Информационная безопасность обеспечивает…
1) Блокирование информации
2) Искажение информации
3) Сохранность информации
4) Утрату информации
5) Подделку информации

3. Устройство для идентификации пользователей, представляющее собой мобильное персональное устройство, напоминающие маленький пейджер, не подсоединяемые к компьютеру и имеющие собственный источник питания:
1) Токен
2) Автономный токен
3) USB-токен
4) Устройство iButton
5) Смарт-карта

4. Аппаратные модули доверенной загрузки «Аккорд - АМДЗ» представляют собой…
1) Аппаратный контролер
2) Электронный замок
3) Система контроля
4) Сетевой адаптер
5) Копировальный аппарат

5. Что такое кибербуллинг?
1) мошенничества, совершаемые в сети Интернет
2) размещение в сети Интернет провокационных сообщений с целью вызвать конфликты между участниками беседы
3) любые сообщения или публикации в сети, размещаемые с целью запугать, оскорбить или иначе притеснить другого

Специальная часть

1. Выберите, можно ли в служебных целях использовать электронный адрес (почтовый ящик), зарегистрированный на общедоступном почтовом сервере, таком как gmail.com
1) нет, не при каких обстоятельствах
2) нет, но для отправки срочных и особо важных писем можно

3) можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера

2. Выберите из предложенных вариантов пароля "правильный" (с точки зрения современных требований к паролю) (выберите один правильный вариант ответа):
1) 111222333
2) ИвАнОвА
3) 83466825710
4) 1rR%56ty

3. Вы обнаружили на рабочем столе своего ПК файл "Отчет_(Иванов. А.П)_2017.bat", Иванов А.П. является сотрудником вашей компании. Это файл
1) Отчет (вероятно, Иванова А.П.) в виде документа
2) Отчет (вероятно, Иванова А.П.) в виде архива
3) Файл с вирусом, вредоносной программой
4) Файл с набором неизвестных команд

4. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
1) Чтобы убедиться, что проводится справедливая оценка
2) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
3) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
4) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

5. Процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом:
1) Авторизация
2) Аутентификация
3) Обезличивание
4) Деперсонализация
5) Идентификация

6. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации:
1) Авторизация
2) Обезличивание
3) Деперсонализация
4) Аутентифика́ция
5) Идентификация

7. Выберите наиболее точное определение понятия «Информационная безопасность»
1) Набор программ, которые обеспечивают всестороннюю защиту конфиденциальной корпоративной информации от неправильного использования, несанкционированного доступа, искажения или уничтожения.

2) Набор руководящих документов, которые обеспечивают всестороннюю защиту конфиденциальной корпоративной информации от неправильного использования, несанкционированного доступа, искажения или уничтожения.
3) Набор процедур и инструментов, которые обеспечивают всестороннюю защиту конфиденциальной корпоративной информации от неправильного использования, несанкционированного доступа, искажения или уничтожения.

8. CAPEC, CWE, CVE это
1) Аббревиатуры средств защиты информации и обеспечения контроля доступа в информационных системах
2) Известные системы классификации уязвимостей
3) Известные базы данных уязвимостей
4) Программные инструменты для анализа уязвимостей

9. ФСТЭК – это (выберите один вариант ответа)
1) Федеральная служба по техническому и экспортному контролю, является Регулятором в области защиты информации в Российской федерации
2) Федеральная служба по техническому и экспортному контролю, является Регулятором в области защиты информации в Республике Беларусь
3) Федеральная служба по таможенному и экспортному контролю в области защиты информации в Российской федерации
4) Служба контроля за соблюдением информационной политики и связи в области медицинских персональных данных

10. Можно ли скомпрометировать технологию Блокчейн? Если да, что для этого нужно (один вариант)
1) Нет, так как она является основой построения криптовалюты Биткоин, скомпрометировать её нельзя
2) Можно только расшифровать имеющуюся информацию, если применить методы потоковой криптографии
3) Это альтернативное название криптовалюты Биткоин
4) Можно, для этого необходимо получить контроль над 50% компьютеров, входящих в систему +1 компьютер

11. Хеш-функция это (один ответ)
1) Такое математическое преобразование, которое невозможно однозначно выполнить в обратную сторону
2) Сумма четных бит информации для контроля четности
3) Такое математическое преобразование, которое невозможно однозначно выполнить в прямом направлении и, в результате, хеш-сумма каждый раз будет разная
4) Процесс проверки данных

12. Согласно базовой таблице ASCII вы получили коды символов 85, 114, 105. Что закодировано?
1) Ura
2) Privet
3) Uri
4) Ogo

13. IP-адрес DNS-сервера Yandex 77.88.8.8. Выберите, какой вариант вы укажете, если потребуется ввести данные в двоичном формате
1) 01001101.01011000.00001000.00001000

2) 01001011.01011010.00001000.00001000
3) 01001101.01011000.00100000.00100000
4) 01001101.01111000.00001000.00001000

14. Для передачи конфиденциальной информации по незащищенным каналом какую технологию используют
1) Скремблирования
2) VPN
3) VPS
4) VDS
5) Маскарадинга – «обертывания» IP-пакетов для работы с «серыми» IP-адресами

15. Были перехвачены двоичные данные, которые используются в качестве ключа для архива. Это два двоичных числа 101110101 и 1101101. Известно, что ключ является двоичной суммой этих чисел, а также – если ввести неправильную комбинацию, архив самоуничтожается. Какой ключ выберите для ондократной попытки открыть архив?
1) 111100100
2) 10110101
3) 1101101
4) 111100010
5) 101101101
6) 100001000
7) 011011101
8) 111101010

Кейс-задание

Ваш сотрудник переслал на неизвестный электронный адрес письмо, которая DLP-система заблокировала и отправила системному администратору. В письме был такой текст:
Атбаш: Жцколб
ROT(1-10): Щтфтьт02
И файл samples.exe. При запуске этого .exe файла в «песочнице» - он попросил пароль. Ваш администратор предположил, что пароль должен быть длинным, возможно из двух слов. Но более ничем помочь не смог.
1) Найдите компоненты пароля для открытия файла-архива – запишите их.
2) Кратко опишите, что это за система, которая заблокировала отправку письма.
3) Напишите, чему оказалось равно число в ROT(1-10)?