Теоретические задания муниципального этапа
всероссийской олимпиады школьников по технологии 2024-25 учебного года
профиль «Информационная безопасность»
9 класс

Общая часть

1. Информационная безопасность обеспечивает…
1) блокирование информации
2) искажение информации
3) сохранность информации
4) утрату информации
5) подделку информации

2. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя это:
1) электронное сообщение
2) распространение информации
3) предоставление информации
4) конфиденциальность информации
5) доступ к информации

3. Макровирус. Обычно под этим понятием подразумевают
1) вирусы, имеющие очень большой охват компьютеров по всему миру
2) представляют собой макросы, встраиваемые в табличные или текстовые документы
3) вирусы, имеющие в своем программном коде специальные макросы для исполняемых файлов программ

4. Отношения, связанные с обработкой персональных данных, регулируются законом…
1) «Об информации, информационных технологиях»
2) «О защите информации»
3) Федеральным законом «О персональных данных»
4) Федеральным законом «О конфиденциальной информации»
5) «Об утверждении перечня сведений конфиденциального характера»

5. Последствиями сетевой атаки для Вашего компьютера могут быть (несколько вариантов):
1) неработоспособность программ
2) поломка компьютера
3) кража или уничтожение информации
4) заражение компьютера вредоносными программами

Специальная часть

1. Токен для хранения электронной подписи:
1) специальный носитель – фактически, это флешка, на которую записывается файл цифровой подписи
2) специальный носитель, имеющий в составе криптопроцессор для хранения подписи без возможности её извлечения
3) специальный носитель, имеющий в составе криптопроцессор для хранения подписи с возможностью её извлечения для обновления и перезаписи

2. 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

3. StuxNet это
1) считающийся первым компьютерный вирус, который нанёс повреждения физической инфраструктуре
2) название вирусного ботнета для распределенных сетевых компьютерных атак
3) стек используемых хакерами эксплойтов для проникновения в защищенные информационные веб-системы

4. 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

5. Токен для хранения электронной подписи может быть:
1) только контактным – вставляется в USB-разъём, т.к. для повышения безопасности хранения данных исключается беспроводной канал передачи
2) может быть как контактным, так и беспроводным, при этом используется шифрование трафика
3) специальный носитель, имеющий в составе криптопроцессор для хранения подписи с возможностью её извлечения для обновления и перезаписи

6. Когда говорят о Блокчейн, под этим понимают технологию:
1) выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию.
2) метод потоковой обработки данных
3) это алтьтернативное название криптовалюты Биткоин
4) выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию и хеш-суммы.

7. Можно ли скопировать ключ цифровой подписи с токена, если злоумышленник случайно или целенаправленно получил доступ к токену?
1) да, к сожалению, если есть физический доступ к носителю (токену), то можно его вставить в компьютер и скопировать. Обязательно копировать на другой точно такой же токен;
2) да, достаточно компьютера (например, ноутбука) и простой флешки
3) нет, нельзя скопировать
4) нужна специальная программа

8. Хеш-сумма это
1) результат расчета специальной математической функцией. Основная особенность такой функции – невозможность обратного преобразования
2) сумма четных бит информации для контроля четности
3) сумма нечетных бит информации для контроля четности
4) процесс проверки данных

9. Дефейс – это
1) тип программного обеспечения для раскрытия данных хакеров, в т.ч. тех, которые атакуют рассматриваемый ресурс
2) ошибка при разработке – размещение на ресурсе какого-либо недостоверного сообщения с целью пропаганды и нанесения репутационного ущерба владельцу сайта
3) компьютерная атака – замена содержимого взломанного ресурса и размещением на нем какого-либо вызывающего сообщения с целью пропаганды и нанесения репутационного ущерба владельцу сайта.

10. Ботнет это
1) Сеть из зараженных информационных систем, которая действует в интересах злоумышленников
2) Сеть из людей, которые управляют ботами в Интернет
3) Вирус в системе, распространяющийся по компьютерной сети

11. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет:
1) идентификация
2) аутентификация
3) авторизация
4) экспертиза
5) шифрование

12. Основными рисками информационной безопасности являются (выбрать один):
1) искажение, уменьшение объема, перекодировка информации
2) техническое вмешательство, выведение из строя оборудования сети
3) потеря, искажение, утечка информации

13. Какую технологию используют для организации передачи информации ограниченного доступа по открытым каналам:
1) WWW
2) DICOM
3) VPN
4) FTP
5) XML

14. Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа:
1) антивирус
2) замок
3) брандмауэр
4) криптография
5) экспертная система

15. Комплекс аппаратных и/или программных средств, осуществляющий доверенную загрузку ПК и контролирующий целостность системных файлов:
1. АПКШ
2. МДЗ
3. DLP-система
4. SIEM-система

Кейс-задание

В ходе радиоразведки вы перехватили следующее сообщение
З рциж уиу щиъбсэщчкиые.

По некоторым предположениям, оно сдвиговым шифром. Вам необходимо расшифровать сообщение и определить значение коэффициента сдвига k.