1. Якою формулою пов’язані відкритий y та секретний x ключі в алгоритмі шифрування Ель Гамаля, g, p - відкриті параметри?

а) x = g^ y mod p.

б) x = g^(-y) mod p.

в) y = g^(-x) mod p.

г) y = g^x mod p.

2. Які існують види інформації за порядком доступу?

а) Інформація з обмеженим доступом та службова інформація.

б) Відкрита інформація та інформація з обмеженим доступом.

в) Масова інформація та інформація з обмеженим доступом.

г) Відкрита інформація та закрита інформація, що є власністю держави.

3. Надати функціонально повне визначення терміну «Залишковий ризик», згідно з ДСТУ ІSО/ІЕС 27005:2019.

а) Ризик (частина ризику), що залишається після оброблення ризику.

б) Ризик, що залишається після зміни наслідків ризику.

в) Ризик, що залишається після вилучення джерела ризику.

г) Ризик, що залишається після зміни імовірності виникнення ризику.

4. Чому дорівнює k після виконання наступного фрагменту програми?

int k=0;

for (int i= 0; i<4 ; i++)  { k = k +2; }

а) 4

б) 10

в) 6

г) 8

5. Що відноситься до об’єктів захисту інформації в інформаційно-комунікаційній системі?

а) Апаратні рішення, використані при побудові системи.

б) Технічні рішення, що використовуються для створення апаратури, яка утворює систему.

в) Інформація, що обробляється, та програмне забезпечення, яке призначено для обробки цієї інформації.

г) Алгоритми, що використовуються для функціонування системи.

6. До якого критерія захищеності та основної властивості інформації відносяться послуги: реєстрація, ідентифікація і автентифікація, розподіл обов'язків, самотестування?

а) Спостережність.

б) Конфіденційність.

в) Цілісність.

г) Автентичність.

7. Який з наведених криптографічних алгоритмів заснований на мережі Фейстеля?

а) STRUMOK ДСТУ 8845:2019.

б) Kalyna ДСТУ 7624:2014.

в) Kupyna ДСТУ 7564:2014.

г) Шифр ДСТУ ГОСТ 28147:2009.

8. Яка умова гарантує наявність у числа е (одного з ключів RSA) мультиплікативного оберненого за модулем $φ$(n), де $φ$(n) - функція Ейлера?

а) e просте.

б) e дільник $φ$(n).

в) $φ$(n), просте.

г) e та $φ$(n) взаємно прості.

9. Який мікрофон за своїми параметрами, із наведених нижче, у вібро-акустичному каналі витоку інформації враховує середовище розповсюдження небезпечного сигналу?

а) Електродинамічний.

б) Неспрямований.

в) Вузькосмуговий.

г) Контактний.

10. Які унікальні демаскуючі ознаки мають пристрої, що використовують витік інформації оптичними та оптоелектронними каналами?

а) Відсутність радіочастотного випромінювання.

б) Наявність поверхні, що віддзеркалює.

в) Видимість їх розташування в тепловізорі.

г) Виглядають як елементи декору приміщення.

11. Як розшифровується протокол безпеки прикладного рівня HTTPS?

а) Захищений протокол передачі гіпертексту (HyperText Transfer Protocol Secure).

б) Служба конфіденційного передавання гіпертексту (HyperText Transfer Privacy Service).

в) Протокол служби трансмісії (пересилки) гіпертексту (HyperText Transmission Protocol Service).

г) Захищений протокол транспортування гіпертексту (HyperText Transport Privacy Secure).

12. Яку роль визначає ЗУ «Про інформацію» фізичній особі?

а) Суб'єкт інформаційних відносин.

б) Суб'єкт владних відносин.

в) Об'єкт інформаційних відносин.

г) Об'єкт владних повноважень.

13. При використанні основних теорем теорії чисел визначити, яке число є результатом обчислення  виразу $3^{14}mod21$?

а) 7.

б) 11.

в) 5.

г) 9.

14. Що міститься у контексті процесу?

а) Ідентифікатор процесу.

б) Дані про привілеї процесу.

в) Вміст регістрів процесора, що є доступними для процесу.

г) Ідентифікатор користувача.

15. Який рівень кібербезпеки складових визначає загальну кіберзахищенність ІКС?

а) Найменший.

б) Середній.

в) Сумарний.

г) Найбільший.

16. Що є обов'язковою умовою для використання записів журналу аудиту подій в інформаційно-комунікаційній системі у якості доказів при розслідуванні кіберзлочинів?

а) Синхронізація системних годинників.

б) Копіювання журналу у зовнішню систему.

в) Створення кодів автентифікації подій.

г) Шифрування записів журналу.

17. Що є об’єктом інформаційних відносин відповідно до Закону України «Про інформацію»?

а) Інформація.

б) Фізична особа.

в) Юридична особа.

г) Об'єднання громадян.

18. Що з перелічених процедур є засвідченням чинності відкритого ключа?

а) Формування сертифіката відкритого ключа.

б) Діяльність, пов'язана з обслуговуванням посилених сертифікатів ключів.

в) Документальне засвідчення даних в електронній формі.

г) Створення відкритого ключа підписувачем.

19. Як, відповідно до ЗУ "Про основні засади забезпечення кібербезпеки України", можна назвати процес застосуваннякомунікаційної системи, або її ресурсів та засобів електронних комунікацій для здійснення нападу на інші об'єкти кіберзахисту?

а) Кібератака.

б) Кіберінцидент.

в) Кіберзагроза.

г) Хакерство.

20. Який з названих механізмів призначений для протидії експлуатації можливих уразливостей коду?

а) Рандомізація адресного простору - Address Space Layout Randomization (ASLR).

б) Локальний виклик процедур - Local Procedure Call (LPC).

в) Дискреційне керування доступом - Discretionary Access Control (DAC).

г) Мандатне керування доступом - Mandatory Access Control (MAC).

21. Підприємство запросило у обласному статистичному бюро офіційну інформацію про кількість фірм в регіоні, які виготовляють аналоги споживчіх товарів згідно наданому переліку. Яку відповідь повинно отримати підприємство згідно ЗУ «Про інформацію» ?

а) Відмову в наданні інформації, так як це є інформація з обмеженим доступом.

б) Довідку з офіційною статистичною інформацією, яка відповідає запиту.

в) Повідомлення, що такі відомості не відносяться до статистичних даних.

г) Відповідь, що для отримання інформації слід мати спеціальний дозвіл.

22. Відповідно до Закону України “Про захист інформації в інформаційно-комунікаційних системах” на кого покладається відповідальність за забезпечення захисту інформації в системі?

а) Власника системи.

б) Користувачі.

в) Адміністратора системи.

г) Службу безпеки.

23. Яка криптосхема НЕ належить до асиметричної криптографії?

а) RSA.

б) RC4.

в) Діффі-Хеллмана.

г) DSA.

24. Що називають імітозахистом?

а) Метод використання особливих властивостей форматів файлів для підвищення прихованості повідомлення.

б) Процес ускладнення залежності між секретним ключем і зашифрованим повідомленням.

в) Застосування процедур заміни режимів роботи алгоритмів шифрування.

г) Захист системи зв'язку від спотворень та нав'язування неправдивих даних.

25. Хто, без додаткових договорів або доручень , згідно Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», не є суб'єктами відносин, пов'язаних із захистом інформації в системах?

а) Bолодільці інформації.

б) Bласники системи.

в) Розпорядник системи.

г) Kористувачі.

26. З чим асоційований токен доступу (Access Token) в системі контролю доступом Active Directory?

а) Процесом.

б) Об'єктом.

в) Списком.

г) Записом.

27. Який етап з наведених НЕ відноситься до етапів реагування на інциденти інформаційної безпеки?

а) Контроль та аудит.

б) Виявлення та аналіз.

в) Ліквідація наслідків.

г) Діяльність після інциденту.

28.Які ключі використовують для створення та перевірки електронного цифрового підпису DSA?

а) Для створення - секретний ключ, а для перевірки - відкритий ключ.

б) Для створення - відкритий ключ, а для перевірки - секретний ключ.

в) Використовують один і той самий секретний ключ.

г) Використовують два різних секретних ключа.

29. Яке основне призначення крихких (fragile) ЦВЗ в стеганосистемах?

а) Забезпечення цілісності  контейнеру (мультимедійних даних).

б) Приховання факту наявності вбудованого повідомлення.

в) Забезпечення конфіденційності вбудованого повідомлення.

г) Забезпечення конфіденційності контейнеру (мультимедійних даних).

30. Що є причиною для виникнення явища реверберації?

а) Багаторазове відбиття акустичної хвилі в замкненому просторі.

б) Відбиття хвилі на межі двох середовищ, густини яких приблизно рівні.

в) Спотворення фронту хвилі в відкритому середовищі.

г) Різка зміна параметрів середовища поширення хвилі.

31. Яку методологію можна застосувати до всіх процесів СУІБ відповідно до стандарту ISO/IEC 27005?

а) РDСА «РІаn-Dо-Сheck-Асt» («Плануй-Виконуй-Перевіряй-Дій»).

б) TQM «Total Quality Management» («Всеохоплюючий менеджмент якості»).

в) AQI «Annual Quality Improvement» («Щорічне покращання якості»).

г) QFD «Quality Function Deployment» («Розгортання функції якості»).

32. При розробці КСЗІ для кімнати проведення нарад, яка є частиною контрольованої зони (КЗ), вказано на можливість створення зловмисником радіочастотного каналу витоку інформації – шляхом встановлення технічного засобу розвідки (радіозакладки-мікрофону (РМ)). Визначте необхідний рівень сигналу завади (в дБ), який повинен створити генератор завади на межі КЗ, за умов:

* Коефіцієнт ослаблення конструкції КЗ становить – 20 дБ;
* Потужність випромінювання РМ – 30 мВт;
* Гранична чутливість приймача зловмисника – 100 мкВ/м;
* Розмір КЗ в напрямку місця можливого перебування зловмисника – 300 м

а) -80

б) -60

в) -40

г) -20

33. Який з методів найбільш доцільно застосовувати на початкових етапах роботи з оцінки ризиків?

а) Якісний (qualitative).

б) Кількісний (quantitative).

в) Напівякісний (semi-qualitative).

г) Напівкількісний (semi-quantitative).

34. Яку властивість інформації порушує deface (зміна даних) веб-сайту компанії зловмисником?

а) Доступність.

б) Цілісність**.**

в) Конфіденційність**.**

г) Спостережність**.**

35. При перевірці у приватній газорозподільній компанії виявлено шкідливий програмний засіб, через який відбувався витік персональних даних клієнтів. Кому, крім керівництва компанії, необхідно повідомити про цей кіберінцидент?

а) Урядову команду реагування на комп’ютерні надзвичайні події CERT-UA.

б) Департамент кіберполіції Національної поліції України.

в) Національний координаційний центр кібербезпеки.

г) Службу з питань інформаційної безпеки та кібербезпеки РНБО.

36. Який інструмент аналізує трафік та порти у режимі реального часу, а також виявляє сканування портів, атаки з ідентифікації та переповнення буфера?

а) Snort.

б) Nmap.

в) SIEM.

г) Wireshark.

37. Який з IPsec протоколів забезпечує цілісність віртуального з'єднання (переданих даних), автентифікацію джерела інформації та має додаткову функцію із запобігання повторної передачі пакетів?

а) АН.

б) IKEv2.

в) ISAK MP**.**

г) RADIUS.

38. Нехай сортування даних проводиться від мінімального до максимального значення.

Які основні операції виконуються на кожному етапі алгоритму пухирцевого (бульбашкового) сортування?

а) Переміщення в кінець масиву найбільшого з не відсортованих значень.

б) Переміщення потрібного значення на початок масиву.

в) Спроба знайти найменше значення для переміщення його на початок масиву.

г) Вибір ключового індексу, і далі всі елементи, які більші за ключовий, переміщуються в праву частину масиву, які менші — в ліву.

39. Який параметр Політики резервного копіювання даних визначає періодичність створення резервних копій?

а) Цільова точка відновлення (RPO).

б) Цільовий час відновлення (RTO).

в) Мінімальна ціль неперервності роботи (MBCO).

г) Готовність ІКТ до неперервності роботи (IRBC).

40. Вкажіть суб’єкт управління доменом Active Directory.

а) Робоча стація.

б) Контролер домену.

в) Сайт Active Directory.

г) Web-сервер.

41. До якої мережі належить вузол 168.14.17.254/26?

а) 168.14.17.128/26

б) 168.14.17.192/26

в) 168.14.17.0/26

г) 168.14.0.0/26

42. За принципом функціонування «копіювання полів шляхом зняття індуктивних наводок» розпізнайте канали витоку інформації.

а) Електромагнітні.

б) Віброакустичні.

в) Акустоелектричні.

г) Оптичні.

43. Яка концепція об'єктно-орієнтованого програмування дає можливість одному класові використовувати програмний код іншого класу, доповнюючи його власними деталями реалізації?

а) Поліморфізм.

б) Успадкування.

в) Інкапсуляція.

г) Абстракція.

44. З яких складових формується віртуальна адреса при сторінковому розподілі пам’яті в сучасних ОС?

а) Номера сегмента, номера сторінки та фізичної адреси.

б) Номера сегмента і зсуву.

в) Номера сегмента і номера сторінки.

г) Номера сторінки і зсуву.

45. У процесі ідентифікації ризиків інормаційно-комунікаційної системи отримано числові дані про вартість ресурсів, існуючі загрози та вразливості, можливі втрати від загроз. При якому типі аналізу ризиків визначається очікуваний річний об'єм збитків?

а) Кількісному.

б) Ймовірнісному.

в) Якісному.

г) Витратному.

46. Чому, за можливості, необхідно виключити спільні проходження в одному коробі кабельних силових та сигнальних ліній на об'єктах інформаційної діяльності, де циркулює інформація з обмеженим доступом?

а) Провідники є вторинними антенами.

б) В каналах можуть бути закладні пристрої.

в) Кабельні канали є акустичними резонаторами.

г) Дроти можуть мати електричний потенціал.

47. Який засіб для забезпечення цілісності інформаційного потоку використовує протокол запису (Record Protocol), що входить до SSL/TLS?

а) Електронний цифровий підпис.

б) Код автентифікації повідомлень.

в) Хеш-функцію.

г) Контрольну суму.

48. Що називається неконтрольованим поширенням інформації, яке може призводити до її несанкціонованого  одержання?

а) Друк.

б) Витік.

в) Архівування.

г) Копіювання.

49. Які датчики (сповіщувачі) системи охоронної сигналізації використовують для контролю внутрішнього простору приміщень без вікон?

а) Магнітоконтактні.

б) Пасивні інфрачервоні.

в) Ємнісні.

г) Акустичні.

50. На які основні класи розподіляють сучасні алгоритми шифрування?

а) Симетричні та асиметричні.

б) Одноключові та безключові.

в) Одноалфавітні та багатоалфавітні.

г)  Заміни та перестановки.

51. Що є джерелом інформації, яка зберігається у файлі формату pcap?

а) Мережний трафік.

б) Образ віртуальної машини.

в) Вміст оперативної пам'яті.

г) Завантаженість процесора.

52. В якому режимі працюють менеджери (диспетчери) ресурсів при мікроядерній архітектурі ОС?

а) Ядра.

б) Захищеному.

в) Привілейованому.

г) Користувача.

53. За яким стандартом необхідно здійснювати вибір методики оцінювання ризиків інформаційної безпеки в інформаційних об’єктах критичної інфраструктури?

а) ДСТУ ISO/IEC 27005

б) COBIT 4.1

в) NIST SP 800-53

г) IEC 62443

54. Який з атрибутів дескриптора безпеки об’єкта в сучасних ОС Windows вказує на те, хто та які операції може виконувати з цим об’єктом?

а) Дискреційний список контролю доступу.

б) Системний список управління доступом.

в) Ідентифікатор безпеки власника об’єкта.

г) Ідентифікатор безпеки основної групи об’єкта.

55. Як пов'язані між собою імовірність реалізації ризику, наслідки реалізації ризику та пріоритет (серйозність) ризику?

а) Наслідки залежать від імовірності та пріоритету.

б) Імовірність залежить від наслідків та пріоритету.

в) Пріоритет залежить від імовірності та наслідків.

г) Пріоритет та імовірність залежать від наслідків.

56. Що входить до функціонального профілю захищеності, заданого формулою: КА-2, КО-1, ЦА-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-3, НИ-3, НК-1, НО-2, НЦ-2, НТ-2?

а) Адміністративна цілісність і відкат.

б) Довірча конфіденційність і цілісність при обміні.

в) Аналіз прихованих каналів і автентифікація відправника.

г) Автентифікація одержувача і аналіз прихованих каналів.

57. Який із протоколів передачі файлів забезпечує цілісність і конфіденційність даних?

а) TFTP.

б) FTP.

в) SFTP.

г) FXP.

58. Ha чому заснований послідовний пошук необхідного елемента в масиві?

а) Прямому перегляді елементів.

б) Випадковому виборі елементів.

в) Поділі масиву навпіл.

г) Упорядкуваннi масиву.

59. Відомо, що:

умовна ймовірність реалізації *i*-ої загрози інформації *pЗi*|*Вi* = 0,5;

ймовірність використання *i*-ої загрозою *i*-ої вразливості *pВi*= 0,4;

ймовірність обробки у системі *i*-ої цінної інформації *pЦi*= 0,8;

величина вартості втрат при реалізації *i*-ої загрози *Сi*= 10000 грн.

З урахуванням трьох факторів (загроз, вразливостей, втрат), якою буде величина ризику інформаційної безпеки *Ri* (грн)?

а) 2000.

б) 5000.

в) 3200.

г) 1600.

60. За яких умов існує ризик інформаційної безпеки?

а) Для даної вразливості існує відповідна їй загроза та можливі втрати.

б) Для даної вразливості не існує відповідної для неї загроза.

в) Для даної загрози існує відповідна вразливість, що не породжує втрат.

г) Не знайдено загроз і не знайдено вразливостей.

61. Що підлягає аналізу при обстеженні фізичного середовища функціонування ІТС?

а) Вся інформація, що обробляється, а також зберігається в ІКС.

б) Взаємне розміщення засобів обробки інформації ІКС на ОІД, комунікацій, систем життєзабезпечення і зв’язку, а також режим функціонування цих об’єктів.

в) Види і характеристики каналів зв'язку.

г) Повноваження користувачів щодо допуску до відомостей, які обробляються в ІКС, доступу до ІКС та її окремих компонентів.

62. Який вид віртуалізації операційних систем дозволяє реалізувати пряме керування гостьовими системами в двох режимах root та non-root?

а) Програмна віртуалізація.

б) Апаратна віртуалізація.

в) Контейнерна віртуалізація.

г) Інфраструктурна віртуалізація.

63. Які документи розробляються Державною службою спеціального зв'язку та захисту інформації України для здійснення оцінки стану захищеності інформації в ІКС?

а) План захисту інформації.

б) ТЗ на створення КСЗІ.

в) Програма та методика.

г) Акт обстеження.

64. Як називається додаткова властивість інформаційної системи, що дозволяє фіксувати діяльність користувачів, використання ними пасивних об‘єктів та однозначно встановлювати авторів певних дій в системі?

а) Підзвітність.

б) Достовірність.

в) Не відмовність.

г) Доступність.

65. Скільки виходів має графічний блок розгалуження?

а) 3

б) 2

в) 1

г) 4

66. Яка модель управління кіберінцидентами запропонована у стандартах ISO 27ХХХ?

а) Модель PDCA.

б) Модель Гексада Паркера.

в) Модель СIA.

г) Модель STRIDE.

67. Які послуги захисту повинен в першу чергу забезпечувати комплекс засобів захисту (КЗЗ) інформації об'єктів?

а) Цілісності та керованості.

б) Конфіденційності та доступності.

в) Доступності та спостережності.

г) Спостережності та конфіденційності.

68. На розв’язанні якої математичної задачі заснована криптостійкість схеми генерації спільних секретних ключів Діффі-Хеллмана?

а) Розкладання цілого числа на множники.

б) Дискретне логарифмування.

в) Задача про ранець.

г) Ізоморфізм графів.

69. Задана матриця з оцінками цінності ресурсів СУІБ (0, 1,…,4), імовірностями виникнення загроз та рівнями вразливостей (L - низький, М - середній, H - високий).



Якою буде величнина ризику інформаційної безпеки для ресурсу СУІБ з цінністю 2 при «високій» імовірності реалізації загрози через вразливість з «низьким» рівнем?

а) 4.

б) 5.

в) 6.

г) 7.

70. Який за рівнем функціональності міжмережний екран функціонує на прикладному рівні OSI?

а) Екрануючий транспорт.

б) Екрануючий шлюз.

в) Екрануючий міст.

г) Екрануючий маршрутизатор.

71. Як, за наведеним нижче описом, ранжується зростання рівня кваліфікації порушника щодо способів подолання систем захисту інформації АС?

|  |  |
| --- | --- |
| 1. | Може підслуховувати розмови у приміщеннях та читати документи на чужих робочих місцях. |
| 2. | Використовує пасивні технічні засоби перехоплення без можливості модифікації інформації та компонентів інформаційної системи. |
| 3. | Використовує лише штатні засоби та недоліки системи захисту інформації для її подолання (несанкціоновані дії з використанням дозволених та доступних засобів). |
| 4. | Використовує просунуті технічні засоби активного впливу з метою модифікації інформації та компонентів інформаційної системи. |

а) 2-1-3-4

б) 1-2-3-4

в) 3-1-2-4

г) 4-3-1-2

72. При якому виді резервування (згідно ДСТУ 2860-94. Надійність техніки. Терміни та визначення) використовується здатність компонентів ІКС сприймати додаткові навантаження поверх номінальних?

а) Структурному.

б) Почасовому.

в) Функціональному.

г) Вивантажувальному.

73. Що з наведеного можна назвати «акустичним хвилеводом»?

а) Перфорацію поверхневого шару перегородок між кімнатами.

б) Відкриті хвіртки на вікнах або відчинені двері між кімнатами.

в) Простір між капітальною стелею та шумопоглинаючим матеріалом.

г) Повітропроводи примусової системи вентиляції і кондиціонування.

74. Який шифр отримаємо у випадку, якщо ключ шифру Віженера  складається з одного символу?

а) Шифр Вернама.

б) Шифр Полібія.

в) Шифр Цезаря.

г) Шифр Плейфеєра.

75. Якою є послуга «відкат» згідно з НД ТЗІ 2.5-004-99 ?

а) Автоматизованою.

б) Нормативною.

в) Незалежною.

г) Гарантованою.

76. Який механізм системи SIEM дозволяє об’єднувати дані всередині події, наприклад, при отриманні URL у вигляді різних частин: протокол; домен; URI?

а) Конкатенація.

б) Порівняння полів.

в) Фільтрування джерел.

г) Кореляція за кількома джерелами.

77. Який із підходів оцінювання ризиків відповідно до ISO 13335 має основною метою підбір для організації мінімального набору захисних заходів для захисту всіх або окремих інформаційних систем?

а) Базовий.

б) Неформальний.

в) Детальний.

г) Комбінований.

78. До яких методів захисту інформації від витоку технічними каналами належить екранування?

а) Активних.

б) Акустичних.

в) Електромагнітних.

г) Пасивних.

79. Політики забезпечення яких властивостей оброблюваної інформації мають існувати як складові частини загальної політики безпеки в автоматизованих системах (АС) згідно НД ТЗІ 1.4-001-2000?

а) Цілісності, конфіденційності, доступності.

б) Цілісності, конфіденційності і спостережності.

в) Спостережності, надійності, конфіденційності.

г) Доступності, надійності, цілісності.

80. За негласного отримання інформації, витік мовної інформації може бути здійснений за допомогою мобільних телефонів, диктофонів, спеціальних технічних засобів («жучків»).

Який засіб блокування такого витоку НЕ може бути використано?

а) Трансформатори розділові з екранованою обмоткою, екран приєднано до шини заземлення.

б) Генератори спеціального електромагнітного шуму в діапазонах GSM, CDMA, WI-FI, 802,12.

в) Генератори спеціального акустичного шуму (ультразвукові), впливаючі на мікрофон.

г) Джерела спеціального акустичного шуму, котрі під час передачі інформації змінюють її.

81. Оберіть технологію проактивного захисту, що дозволяє антивірусам на основі аналізу коду виконуваної програми, скрипта або макросу виявити ділянки коду, характерні для вірусів.

а) Співставлення з базою даних.

б) Моніторинг поведінки.

в) Контроль цілісності.

г) Евристичний аналіз.

82. Яка процедура управління інцидентами інформаційної безпеки має за мету визначити потреби у додаткових заходах безпеки?

а) Реагування.

б) Збір доказів.

в) Зіставлення.

г) Виявлення.

83. Яка властивість характеризує методи на основі сигнатур в системах виявлення/попередження вторгнень?

а) Знаходження атак за наперед відомим описом та ознаками.

б) Детектування раніше невідомих атак в потоці подій.

в) Аналізування всіх логів операційних систем для виявлення слідів атак.

г) Виявлення відхилень від передбачуваної поведінки додатків під час атаки.

84. Аналіз яких з перелічених сутностей виконують засоби захисту мережі IDS/IPS?

а) Даних та мережної поведінки.

б) Операційних систем

в) Електронних поштових листів.

г) Драйверів.

85. До якого типу належить гіпервізор VMware ESXi?

а) Тип 1 (автономний гіпервізор).

б) Тип 2 (на основі базової ОС).

в) Тип 1+ (гібридний).

г) Не має аналогів, тому не підпадає під класифікацію.

86. Яка з перелічених інформацій, згідно з ЗУ «Про інформацію», може належити до інформації з обмеженим доступом?

а) Про стан довкілля.

б) Про стан здоров'я населення.

в) Критична технологічна.

г) Про факти порушення прав і свобод людини.

87. Хто з перелічених осіб НЕ має включатись до моделі внутрішніх загроз підприємства під час створення політики безпеки?

а) Начальник охорони.

б) Аутсорсинговий юрист.

в) Інженер.

г) Адміністратор.

88. Які атаки зловмисників найчастіше відбуваються на канальному рівні?

а) Підміна MAC-адреси, атака на ARP і STP протоколи.

б) Підміна локальної адреси, атака на UDP і TCP протоколи.

в) Підміна контрольної суми, атака на DNS і DHCP протоколи.

г) Підміна фізичної адреси, атака на ICMP і IGMP протоколи.

89. Якою може бути довжина ключів в потоковому шифрі STRUMOK ?

а) 256 або 512 байт.

б) 256 або 512 біт.

в) Тільки 256 біт.

г) Тільки 512 біт.

90. Що входить до складу узагальненої моделі стеганосистеми?

а) Демодулятор, спектроаналізатор, кодер.

б) Контейнер, спектроаналізатор, кодер.

в) Детектор, кодер, модулятор.

г) Контейнер, кодер, декодер.

91. Який режим виконання операції введення-виведення сприятиме збільшенню швидкості при роботі програмного модуля?

а) Синхронний.

б) Асинхронний.

в) Пріоритетний.

г) Автоматичний.

92. До яких методів виявлення закладних пристроїв відноситься  перевірка приміщень із використанням нелінійних локаторів?

а) Активних.

б) Пасивних.

в) Візуальних.

г) Оптичних.

93. Коли необхідно виконувати заходи із відновлення функціонування ІКС відносно часу виникнення руйнівних наслідків цільової атаки?

а) Після.

б) До і під час.

в) Під час і після.

г) До, під час і після.

94. З якою метою використовується сертифікат TLS?

а) Шифрування даних під час передачі між сервером і клієнтом.

б) Встановлення безпечного з'єднання між клієнтом і сервером.

в) Забезпечення автентифікації веб-сервера.

г) Забезпечення процесу авторизації служби.

95. Яку задачу виконує процедура авторизації при вході користувача в інформаційну систему?

а) Розпізнавання за ім’ям.

б) Перевірка справжності.

в) Надання повноважень.

г) Реєстрація доступу.

96. В серверній кімнаті, яка знаходиться на п’ятому поверсі багатоповерхової будівлі (висота 16 метрів), порушник зміг встановити радіопередач, який працює на ультракоротких хвилях. Розрахуйте максимальну відстань (в кілометрах) на якій порушник може прийняти сигнал, за умови, що антена приймача знаходиться на висоті 9 метрів.

а) 9.

б) 16.

в) 25.

г) 36.

97. На якому рівні еталонної моделі OSI працює протокол IPSec?

а) Мережний рівень (Network layer).

б) Транспортний рівень (Transport layer).

в) Канальний рівень (Data Link layer).

г) Сеансовий рівень (Session layer).

98. Що є об'єктом інформаційних відносин відповідно до закону України "Про інформацію"?

а) Інформація.

б) Право.

в) Ресурс.

г) Подія.

99. До якого критерію оцінки захищеності інформації належить сукупність послуг: повторне використання об'єктів, аналіз прихованих каналів?

а) Конфіденційність.

б) Доступність.

в) Цілісність.

г) Спостереженість.

100. Яким може бути деструктор класу?

а) Вбудованим (inline), Статичним (static), Віртуальним (virtual).

б) Вбудованим (inline), Статичним (static).

в) Вбудованим (inline), Віртуальним (virtual).

г) Статичним (static), Віртуальним (virtual).