Міністерство освіти і науки України
Хмельницький національний університет

«Затверджую»
Проректор з НПР
_____Матюх С.А.
«30» червня 2021 р.

ПРОГРАМА
фахового вступного іспиту

фахового вступного випробування для навчання
за освітньо-професійною програмою магістра
спеціальності 125 – Кібербезпека

Затверджено на засіданні кафедри кібербезпеки і комп'ютерних систем та мереж
Протокол № 13 від 29 червня 2021 р.

Завідувач кафедри КБКСМ _____
к.т.н., доц. Кльоц Ю.П.

Затверджую
Декан ФПКТС
_____д.т.н., проф. Савенко О.С.

Схвалено Вченою радою ФПКТС
Протокол № 8 від 30 червня 2021 р.

Голова Вченої ради ФПКТС
_____д.т.н., проф. Савенко О.С.

Загальні положення

Фахове вступне випробування проводиться приймальною комісією Хмельницького національного університету – за спеціальністю 125 «Кібербезпека».

Під час виконання завдання перевіряються знання, вміння та навички студентів щодо розв'язання певних завдань з основ інформаційної безпеки, безпеки веб-ресурсів, теорії передачі і захисту даних, програмування (мова С, С++), комплексних систем захисту інформації.

Критерії оцінювання

При тестуванні абітурієнт одержує завдання з 50 тестових питань відповідно на перевірку основних знань і вмінь з теорії передачі інформації, безпеки веб-ресурсів, комп'ютерних систем та мереж, програмування (мова С, С++), захисту інформації в комп'ютерних системах.

Оцінюється тестове завдання за 200-бальною шкалою (від 100 до 200 балів), причому кожне тестове питання оцінюється рівною кількістю балів.

Зміст навчального матеріалу

1 Основи інформаційної безпеки

Основні поняття та визначення: атаки, вразливість, політика безпеки, механізми та сервіси безпеки.

Модель мережної безпеки. Класифікація мережних атак. Модель мережної взаємодії. Сервіси безпеки. Модель безпеки інформаційної системи.

Стиснення інформації як один з методів її захисту. Алгоритми архівації даних.

Огляд основних криптографічних методів захисту інформації. Основні поняття. Класифікація криптографічних методів. Криптографічні методи захисту інформації. Основні поняття криптоаналізу.

Псевдовипадкові числа. Вимоги до випадкових чисел. Генератори псевдовипадкових чисел. Криптографічно створені випадкові числа.

Цифровий підпис. Вимоги до цифрового підпису. Прямий та арбітражний цифрові підписи. Стандарти цифрового підпису.

Хеш-функції та аутентифікація повідомлень. Хеш-функції. Вимоги до хеш-функцій. Прості хеш-функції. Технології аутентифікації. Аутентификация, авторизація та адміністрування дій користувачів.

Основні принципи побудови систем мережної безпеки. Аналіз та керування ризиками. Основні поняття та визначення. Технологія аналізу та керування ризиками. Засоби автоматизації оцінки інформаційних ризиків.

2 Безпека веб-ресурсів

Організація та способи передачі даних мережі Інтернет. Стек протоколів TCP/IP. Система доменних імен DNS. Протоколи Інтернет прикладного рівня.

Основи клієнт-серверних технологій. Web-сервери. Протоколи HTTP та HTTPS. Cookie.

Організація поштових серверів. Принципи організації електронної пошти. Поштові сервери і клієнти. Протоколи передачі електронної пошти (IMAP, POP3, SMTP, UUCP).

Архітектура Web-ресурсів. Основні поняття та термінологія Web-ресурсів. Архітектура "файл-сервер". Архітектура "клієнт-сервер". Архітектура розподілених систем. Архітектура Web-додатків.

Класифікація Web-атак та вразливостей. Аутентифікація. Авторизація. Атаки на клієнтів. Виконання коду. Розголошення інформації. Логічні атаки.

Вимоги до захисту Web-ресурсів. Обробка помилок та їх реєстрація. Обробка вхідних і вихідних даних. Конфігурація та операції. Управління сеансами. Контроль доступу. Відслідковування подій Web-ресурсів. Основні етапи аудиту безпеки Web-ресурсів. Ведення та керування журналами безпеки

3 Комплексні системи захисту інформації.

Загальні положення про комплексні системи захисту інформації. Використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

Основні принципи організації КСЗІ. Принципи організації КСЗІ. Концептуальні підходи до проєктування систем захисту. Порядок проведення робіт із створення КСЗІ в інформаційно-телекомунікаційній системі (ІТС). Етапи створення КСЗІ в ІТС.

Класифікація загроз інформаційній безпеці. Аналіз загроз на об'єкті захисту. Класифікація загроз інформаційній безпеці, ознаки класифікації. Ознаки моделі порушника, як етапу побудови КСЗІ. Категорії порушників. Класифікація порушника. Поняття контрольована зона. Модель загроз для ідентифікації каналів витоку інформації. Джерело загрози. Перелік загроз з визначенням порушень властивостей інформації та ІТС.

Джерела та носії інформації. Характеристика захищеної інформації. Захист інформації як інтегральна проблема та шляхи її вирішення. Специфіка застосування програмно-апаратних засобів захисту в СКЗІ, оцінка результативності якості прийнятих рішень щодо їх застосування. Умови безпеки інформації. Небезпечні сигнали і їх джерела

Типова структура та види технічних каналів витоку інформації (ТКВІ). Загальна характеристика технічного каналу витоку інформації. Класифікація та характеристика технічних каналів витоку інформації. Особливості витоку інформації технічними каналами. Типова структура та види технічних каналів витоку інформації. Схема можливих каналів витоку і несанкціонованого доступу до інформації.

Методи та засоби захисту від витоку інформації. Використання програмних та програмно-апаратних комплексів захисту інформаційних ресурсів. Заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. Принципи блокування ТКВІ. Заходи щодо блокування ТКВІ з використанням активних та пасивних засобів. Задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних методів та засобів криптографічного захисту інформації. Заходи щодо перетворення сигналів у каналах зв'язку.

Системи блокування відеоспостереження. Методи та засоби відеоспостереження. Принципи протидії засобам відеорозвідки. Класифікація візуально-оптичних каналів витоку інформації. Методи захисту інформації

від витоку по візуально-оптичному каналу. Методи і засоби пошуку прихованих відеокамер. Пошук і блокування прихованих пристроїв відеоспостереження, що використовують радіоканал для передачі інформації.

Канали витоку інформації при експлуатації ЕОМ. Види і природа каналів витоку інформації при експлуатації ЕОМ. Способи і методи ЗІ, оброблюваної засобами електронної техніки, від витоку радіочастотним каналу. Механізм виникнення ПЕМВ засобів цифрової електронної техніки. Технічна реалізація пристроїв маскування. Оцінка рівня ПЕМВ. Прилади виявлення ПЕМВ.

Методи та засоби забезпечення систем фізичного доступу та охорони території. Системи фізичного захисту об'єктів. Типова система фізичного доступу. Доглядові системи.. Ручні та арочні металошукачі. Автономні та мережеві системи доступу. Сигналізації.

Організація випробувань КСЗІ. Реалізація КСЗІ відповідно до вимог нормативно-правових документів. Введення КСЗІ в дію. Державна експертиза КСЗІ в ІТС. Супровід КСЗІ.

4. Теорія передачі інформації

Основні положення теорії інформації. Предмет теорії інформації. Основні поняття, визначення і задачі теорії інформації. Вимірювання інформації. Міра Хартлі. Структурні міри інформації. Статистична міра інформації. Імовірність і інформація.

Поняття ентропії. Ентропія як міра невизначеності. Ентропія об'єднаних систем. Ентропія та інформація. Ентропія та надлишковість.

Основні поняття та задачі кодування. Кодування як процес відображення інформації в цифровому вигляді. Ефективне кодування. Завадостійке кодування. Загальні принципи побудови завадостійких кодів. Загальні принципи використання надлишковості. Зв'язок коригувальної здатності коду з кодовою відстанню. Завадостійкі коди та достовірність передачі повідомлень (інформації).

Блокові корегуючі коди. Геометрична інтерпретація блокових корегуючих кодів. Принципи побудови групових завадостійких кодів.

Циклічні коди. Загальні поняття і визначення. Принципи побудови циклічних кодів. Використання циклічних кодів для виявлення і коректування помилок.

Кодування та стиснення інформації у інформаційно-обчислювальних комплексах та мережах. Кодування інформації в ЕОМ. Стиск інформації в ЕОМ. Адресація та кодування даних в мережах ЕОМ з комутацією пакетів.

5 Програмування

Алгоритмічні структури. Основні оператори мови С. Підключення модулів. Оператори порівняння, рівності та логічні. Форматоване введення та виведення інформації в С. Літери-специфікатори функцій printf (), scanf (), scanf_s (). Функції getchar (), gets (), puts(). Значення EOF.

Змінні і базові типи даних мови С. Базові типи та їх розміри в мові програмування С, оголошення. Програми зі змінними, включаючи найпростіші арифметичні операції. Перетворення і приведення типів. Організація циклів у мові С. Цикли while , for , do - while. Складені оператори циклу і оператори відношення, для яких наводяться приклади з повною програмною реалізацією.

Прийняття рішень. Умовні оператори у мові С. Оператори if , if else , if - else if - else , switch - case - default , оператор умови. Оператори переходу break , continue , безумовний оператор переходу goto. Вкладені умовні оператори, логічні умови.

Числові масиви в мові програмування С. Визначення і ініціалізація числових масивів у мові програмування С. Програмні рішення типових прикладів з багатовимірними числовими масивами. Символьні масиви в мові С. Робота з рядками. Завдання і ініціалізацію символьних масивів у мові програмування С, рішення завдань з символьними масивами, базові функції для роботи з рядками.

Вказівники та масиви в мові С. Взаємозв'язок вказівників і масивів, як числових, так і символьних. Допустимі операції з вказівниками і масивами, масиви вказівників і вказівники на вказівники. Динамічний розподіл пам'яті в

мові С. Функції динамічного розподілу пам'яті та їх застосування для числових і символьних масивів, для зберігання даних.

Загальні відомості про функції мови С. Особливості оголошення і визначень функцій, способів завдання формальних параметрів і типів даних, що повертаються, виклик функцій, передача аргументів за значенням і за посиланням. Вказівники та функції в мові програмування С. Програмування функцій, аргументами яких можуть бути вказівники, а також функції, які повертають значення через вказівник.

Файлове введення / виведення у мові С. Базові функції файлової системи мови програмування С. Створення, читання, запис і модифікація файлів.

Структури - похідні типи даних мови С. Створення та використання структур в мові програмування С. Об'єднання і перераховані типи в мові С. Структури і функції мови Сі. Способи передачі структур у функції, Програми на мові С, що складаються з декількох файлів. Звернення до функцій, розташованих в різних файлах.

Рекурсивні алгоритми та функції. Види рекурсії та застосування рекурсивних алгоритмів. Програмування мовою С з використанням рекурсивних функцій. Препроцесор мови С. Властивості препроцесора мови С і приклади типових препроцесорних директив і конструкцій. Використання аргументів командного рядка в С. Способи передачі аргументів командного рядка операційної системи Windows в програму, читання кількості аргументів і вивід імен цих аргументів з можливістю запуску додатків.

Література

1. Технології захисту інформації / Ю. А. Тарнавський – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
2. Інформаційна безпека: навчальний посібник/ [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.] за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.
3. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / Г. І. Ластівка, П. М. Шпатар – Чернівці: Чернівецький національний університет, 2018. - 252 с.
4. Інформаційна безпека держави: навчальний посібник/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с.
5. Комплексні системи захисту інформації: проєктування, впровадження, супровід. / В.В. Гребенніков – Ужгород: Ужгородський національний університет, 2013. – 161 с.
6. Захист інформації в комп'ютерних системах: підручник. / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, О.О. Балюнов – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236 с.
7. Основы информационной безопасности: Учебное пособие. / 3-е изд., стер. СПб, Издательство "Лань", 2017. – 324с.
8. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.
9. Комплексна безпека інформаційних мережевих систем: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. .– Тернопіль: ТНТУ, 2016. – 255 с.
10. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – КІІВіП НУ "ОЮА", 2017. – 128 с.
11. Технології забезпечення безпеки мережевої інфраструктури/ В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
12. Відкритий проект захисту Web-додатків (OWASP). Стандарт оцінювання відповідності безпеки додатків 3.0. – 2015. – 73 с.
13. Основи інформаційної та кібернетичної безпеки. Навчальний посібник/ В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с.
14. Захист Web-сервісів: лабораторний практикум/ І.А. Терейковський, Л.О. Терейковська, К.О. Радченко, С.О. Гнатюк. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 68 с.
15. Professional Pen Testing for Web Applications (Programmer to Programmer)/ Andres Andreu. – Wrox, 2016. – 548 p.
16. Конспект лекцій з дисципліни «Захист інформації у комп'ютерних системах»/ Р.О. Жаровський. – Тернопіль, 2019. – 268 с.
17. The Web Applicaion Hackers's Handbook: Finding and Exploiting Security Flaws/D. Stuttard, M. Pinto. - John Wiley & Sons, Inc, 2011. – 877 p.

18. Комп'ютерні мережі: навчальний посібник/ Ю. І. Лосев, К. М. Руккас, С. І. Шматков. – Х.: ХНУ імені В. Н. Каразіна, 2013. – 248 с.
19. C++: полное руководство. Классическое издание/ Г. Шилдт – Диалектика, 2020. – 800 с.
20. Безопасное программирование на C и C++. 2-е издание / Р. Сикорд. – Williams, 2015. – 496 с.
21. Программирование: принципы и практика с использованием C++, 2-е изд/ Б. Страуструп. – Вильямс, 2019. – 1328 с.
22. Эффективный и современный C++. / С. Мейерс. – Диалектика, 2020. – 304 с.
23. Объектно-ориентированное программирование в C++/ Р. Лафоре. – Питер, 2019. – 928 с.
24. C++ для чайников. 7-е издание/ С.Р. Дэвис. – Диалектика, 2018. – 400 с. Шаблоны C++. Справочник разработчика / Дэвид Вандевурд. – Диалектика, 2018. – 848с.
25. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. – Хмельницький: ХмНУ, 2020. – 196 с.
26. Теорія інформації та обробка сигналів: навчальний посібник (конспект лекцій) / Ю.С. Ямненко, К.С. Клен. – Київ: КПІ ім. Ігоря Сікорського, 2019. – 120с.
27. Введення в теорію інформації: посібник до вивчення дисципліни / А.М. Курко, В.Я. Решетник – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017. – 108 с.
28. Основи теорії інформації та кодування. Конспект лекцій: навчальний посібник / М.І. Романюк, Ю.Г. Савченко. – Київ: КПІ ім. Ігоря Сікорського, 2019. – 70 с.
29. Основи теорії інформації та кодування: лабораторний практикум: навчальний посібник / М.І. Романюк, Г.Г. Власюк. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 81 с.
30. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

Зразок базового тестового завдання

1. Засоби мережної безпеки забезпечують:
   - запобігання порушенням безпеки, які виникають при передачі інформації з мереж
   - пересилання конфіденційної інформації
   - керування віддаленим комп'ютером
   - зміна вмісту повідомлення
   - інша відповідь
2. Для забезпечення безпечної передачі повідомлення:
   - буває необхідна третя довірена сторона
   - необхідно дві компоненти безпеки
   - необхідно захистити передану інформацію від шифрування
   - необхідно отримати хеш-функцію
   - інша відповідь
3. Третя сторона може бути відповідальна:
   - за розподіл між двома учасниками секретної інформації
   - за розподіл між двома учасниками хеш-функції
   - за розподіл між двома учасниками цифрового підпису
   - за розподіл між двома учасниками певного алгоритму
   - інша відповідь
4. Під replay-атакою розуміється:
   - модифікація переданого повідомлення
   - повторне використання переданого раніше повідомлення
   - неможливість одержання сервісу законним користувачем
   - переповнення пам'яті на сервері
   - інша відповідь
5. Що з перерахованого відноситься до механізмів безпеки:
   - хеш-функції
   - цілісність повідомлення
   - неможливість одержання сервісу законним користувачем
   - неможливість відмови від отриманого повідомлення
   - інша відповідь
6. Власник інформації визначає:
   - основні поняття, що відносяться до інформаційної безпеки
   - множину інформаційних цінностей, які повинні бути захищені від різного роду атак
   - основні порушеннями безпеки
   - вразливості ресурсів, що захищаються
   - інша відповідь
7. Супротивники при атаках використовують:
   - основні поняття політики безпеки
   - механізми і сервіси безпеки

- різні вразливості в цінностях що захищаються
- ризики для даного набору інформаційних цінностей
- інша відповідь

8. Основними порушеннями безпеки є:
   - розкриття інформаційних цінностей (втрата конфіденційності)
   - запобігання порушень безпеки, які виникають при передачі інформації з мереж
   - ризики для даних інформаційних цінностей
   - керування віддаленим комп'ютером
   - інша відповідь
9. Вразливість - це:
   - будь-яка дія, що порушує безпеку інформаційної системи
   - імовірність того, що конкретна атака буде здійснена
   - рішення відображене в політиці безпеки
   - надання сервісів безпеки
   - інша відповідь
10. Дешифрування - це:
    - перетворення інформації в шифроване повідомлення за допомогою певних правил
    - перетворення шифрованого повідомлення в інформацію за допомогою певних правил
    - перетворення інформації з шифрованого повідомлення знаючи відкритий ключ
    - перетворення інформації з шифрованого повідомлення не знаючи закритий ключ
    - інша відповідь
11. Що буде виведене на екран при «i» рівному 3?

```
switch(i)
  {
  case 0:
   printf("Змінна дорівнює нулю\n");
   break;
  case 1:
   printf("Змінна дорівнює одиниці\n");
   break;
  default:
   printf("Змінна дорівнює %d\n", i++);
   break;
  }
```

   - змінна дорівнює 4
   - змінна дорівнює 3
   - виникне помилка виконання
   - виникне помилка компіляції

- інша відповідь

12. Що станеться в результаті компіляції і виконання наступного коду:

```
#include <stdio.h>
int main() {
  int a = 5;
  int*b = &a;                    //1
  printf("%d", a**b);          //2
  return 0;
}
```

- буде надруковано деяке ціле число (залежить від адреси змінної b)
- буде надруковано число 25
- виникне помилка компіляції в рядку 1
- виникне помилка компіляції в рядку 2
- інша відповідь.

13. Що надрукує програма:

```
#include <stdio.h>
  typedef struct foo {
    int a:1;
    int b;
    int c;
  };
  int main(void)
  {
    struct foo f;
     f.a = 1;
    f.b = 2;
    f.c = 3;
   printf("%d", f.a);
   return 0;
  }
```

- 1
- -1
- 2
- -2
- інша відповідь.

14. Вкажіть рядки, в яких містяться помилки:

```
    void Test(const int **a)
    {
  a = 0;   // 1
  *a = 0;  // 2
  **a = 0; // 3
  }
```

- 1
- 1, 2

- 2
- 3, 2
- інша відповідь

15. Які з фундаментальних типів С є архітектурно-залежними і мають однакове представлення на усіх платформах?

- int
- unsigned int
- float
- інша відповідь
- long

16. Яке ключове слово у мові С вказує на те, що значення деякої змінної не може бути модифіковане?

- const
- return
- continue
- break
- інша відповідь

17. Які з перерахованих ключових слів не є зарезервованими в С?

- switch
- undo
- enum
- struct
- інша відповідь

18. Виберіть операцію, що не призведе до виходу за межі типу:
int a,b,A,B;
unsigned int c,C;

- A=32768;
- B=-32769;
- C=-50;
- c=50;
- інша відповідь

19. Вкажіть правильне оголошення константного покажчика?

- const* ptrcInt
- const int* const ptrcInt
- const int* ptrcInt
- усі варіанти є правильними
- інша відповідь

20. Чи є у мові С власний редактор?

- тільки в ОС WINDOWS
- так
- тільки в ОС UNIX
- тільки починаючи з С++
- інша відповідь

21. При якій моделі розповсюдження ПЗ відсутня будь-яка оплата або інші умови, що обмежують його використання?

- Freeware
- Trialware
- Nagware
- Cardware
- Інша відповідь

22. Протокол, призначений для реалізації текстового інтерфейсу по мережі – це:

- FTP
- Telnet
- POP3
- HTTPS
- інша відповідь.

23. Якої аутентифікації не існує:

- двофакторної
- однофакторної
- трифакторної
- жодної з перерахованих
- інша відповідь

24. Методи прив'язки до ідентифікатора відносяться до методів захисту:

- апаратних
- програмних
- статичних
- динамічних
- інша відповідь.

25. Базовий протокол керування мережі Internet – це:

- HTTPS
- XMPP
- SMTP
- SNMP
- інша відповідь

26. Whois – це:

- Інтернет-сервіс, що дозволяє отримати інформацію про доменне ім'я в базі даних організації
- шкідлива Інтернет-програма
- Інтернет-сервіс, що дозволяє отримати інформацію про відносні імена в інформаційній системі організації
- пошуковий Інтернет-ресурс
- інша відповідь

27. Web-сайт, що поєднує в собі функції навігаційного сайту та інформаційного ресурсу з різних тем:

- навігаційний сайт
- портал

- інформаційний сайт
- корпоративний сайт
- інша відповідь

28. Програма, що здійснює автоматичне сканування web-ресурсів на предмет появи нових, модифікацію існуючих і видалення старих web-ресурсів – це:

- пошуковий робот
- пошукова система
- пошукова сторінка
- пошуковий сайт
- інша відповідь

29. Вкажіть різновиди протоколів, які використовуються при роботі електронної пошти:

- SMTP, POP-POP3, HTTP
- SMTP, POP-POP3, IMAP
- STMP, POP-POP3, IIMAP
- SMTP, POP-POP3, IMAP, MIME
- інша відповідь

30. Для ідентифікації мережних інтерфейсів не використовуються:

- доменні імена
- мережні адреси
- апаратні адреси
- усі з перерахованих
- інша відповідь

31. Який вид перешкодостійкого коду орієнтований тільки на виявлення однієї помилки:

- жоден варіант не підходить
- Хеммінга
- циклічний
- паритетний з кодуванням за непарністю
- інша відповідь

32. Яку розрядність повинні мати двійкові повідомлення про стан системи, яка з однаковою імовірністю може перебувати у 70 станах:

- 9
- 7
- 6
- 3
- інша відповідь

33. Який вид коду з перелічених є оптимальним (використовується для стиску даних):

- жоден варіант не підходить
- Хеммінга
- циклічний
- Шеннона-Фано
- інша відповідь

34. Яку розрядність повинне мати одне з 35 можливих двійкових повідомлень, що характеризуються однаковою імовірністю надходження:

- 5
- 8
- 9
- 7
- інша відповідь

35. Політика безпеки – це:

- забезпечення безпеки системи і/або переданих даних;
- правила, директиви й практичні навички, які визначають то, як інформаційні цінності обробляються;
- використання вразливості даної інформаційної системи;
- використання одного або більше механізмів безпеки
- інша відповідь

36. Алгоритм DES використовує для дешифрування:

- ті ж ключі, що і для шифрування, але у зворотній послідовності
- ті ж ключі, що і для шифрування, без зміни порядку використання
- інші ключі порівняно з використаними для шифрування
- не використовує ключі шифрування/дешифрування
- інша відповідь

37. Алгоритм подвійний DES використовує для шифрування ключ довжиною:

- 128 біт
- 96 біт
- 112 біт
- 256 біт
- інша відповідь

38. Потрійний DES використовує для шифрування:

- два ключі
- три ключі
- чотири ключі
- вісім ключів
- інша відповідь

39. Стійкість шифру - це:

- здатність шифру застосовувати для шифрування конкретні повідомлення
- здатність шифру застосовувати для шифрування постійний елемент шифрування
- здатність шифру протистояти всіляким методам розкриття
- здатність шифру застосовувати для шифрування змінний елемент шифрування
- інша відповідь

40. Підключем називається:

- ключ шифрування
- ключ дешифрування
- ключ раунду

- ключ шифрування і ключ дешифрування
- інша відповідь

41. Виберіть надійні паролі:
- 12345
- login1
- RE18ZE$NT
- password
- інша відповідь

42. Вкажіть порядок здійснення санкціонованого доступу до ресурсів інформаційної системи:
- ідентифікація, аутентифікація, авторизація
- ідентифікація, авторизація, аутентифікація
- авторизація, ідентифікація, аутентифікація
- послідовність немає значення
- інша відповідь

43. Процес ідентифікації та регулювання на підозрілу діяльність, направлену на обчислювальні чи мережні ресурси – це:
- безпека мережі
- виявлення атак
- методи аутентифікації
- цілісність периметра мережі
- інша відповідь

44. ISO/IES 27001 – це:
- антивірусний програмний пакет
- модуль для виявлення мережевих атак
- міжнародний стандарт інформаційної безпеки
- міжнародний підрозділ боротьби по забезпечення інформаційної безпеки
- інша відповідь

45. Простим способом ідентифікації у комп'ютерної системі є введення ідентифікатора користувача, який має назву:
- токен
- пароль
- логін
- Password
- інша відповідь

46. Процедура визначення та надання прав доступу до ресурсів і управління цим доступом:
- авторизація
- аутентифікація
- ідентифікація
- деперсоналізація
- інша відповідь

47. Процедура перевірки відповідності суб'єкта *і того*, за кого він намагається себе видати, за допомогою якоїсь унікальною інформації:
- авторизація

- аутентифікація
- ідентифікація
- деперсоналізація
- інша відповідь

48. Процес повідомлення суб'єктом свого імені або номера, з метою отримання певних повноважень (прав доступу) на виконання деяких (дозволених йому) дій в системах з обмеженим доступом:
- авторизація
- аутентифікація
- ідентифікація
- деперсоналізація
- інша відповідь

49. До криптографічних засобів протидії загрозам безпеки відносяться:
- спеціальні програми, програмні комплекси і системи захисту інформації в інформаційних системах різного призначення і засобах обробки даних
- спеціальні математичні та алгоритмічні засоби захисту інформації, переданої по мережах зв'язку, збереженої та обробленої на комп'ютерах з використанням методів шифрування
- організація локальних обчислювальних мереж з можливістю перерозподілу ресурсів, у разі виходу з ладу окремих ланок
- розробка норм, що встановлюють відповідальність за комп'ютерні злочини, захист авторських прав програмістів
- інша відповідь

50. Організована сукупність спеціальних установ, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз – це:
- криптографічні засоби протидії безпеці
- система правових заходів захисту інформації
- система захисту інформації
- організація захисту інформації
- інша відповідь