

Міністерство освіти і науки України
Хмельницький національний університет

«Затверджую»
Проректор з НІР
_____ Матюх С.А.
«__» _____ 2020 р.

ПРОГРАМА
фахового вступного іспиту
з галузі знань — 12 «Інформаційні технології»
спеціальності — 125 «Кібербезпека»
для абітурієнтів — випускників коледжів та технікумів
галузі знань «Інформаційні технології»
(освітньо-професійної програми «молодший спеціаліст»)

Затверджено на засіданні кафедри кібербезпеки і комп'ютерних систем та мереж
Протокол №__ від __ січня 2020 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 №__ від _____ 2020 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 захисту інформації в комп'ютерних системах, системного програмного забезпечення, комп'ютерних систем, комп'ютерних мереж, програмування (мова C).

Критерії оцінювання

При тестуванні абітурієнт одержує завдання з 25 тестових питань – відповідно на перевірку основних знань і вмінь з захисту інформації в комп'ютерних системах, системного програмного забезпечення, комп'ютерних систем, комп'ютерних мереж, програмування (мова C).

Оцінюється тестове завдання за 200-бальною шкалою (від 100 до 200 балів), причому кожне тестове питання оцінюється рівною кількістю балів. Для подальшої участі в конкурсі абітурієнт повинен набрати не менше 124 балів.

Зміст навчального матеріалу

1 Захист інформації в комп'ютерних системах

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. Аутентифікація, авторизація та адміністрування дій користувачів.

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

2 Системне програмне забезпечення

Системне програмне забезпечення сучасних операційних систем. Архітектура сучасних операційних систем. Режим «ядра», режим «користувача», рівні привілеїв програмного забезпечення. Системне програмне середовище. Стандартні системні служби. Програмне управління системними службами. Розробка, встановлення, запуск і видалення системних служб.

Процеси і потоки, поняття багатопоточності. Алгоритм «витісняючої» багатозадачності. Створення і запуск потоків. Іменування потоків. Основні і фонові потоки. Обробка помилок та виключень. Система пріоритетів процесів і потоків. Базовий та відносний пріоритет. Керування пріоритетами процесів і потоків. Передача даних в потік. Використання глобальних змінних. Використання сумісних ресурсів потоками одного процесу та різних процесів.

Базові поняття та положення з синхронізації потоків. Планування потоків Вибір об'єкту синхронізації. Вкладені блокування. Примусове розблокування. Поняття стану потоку. Основні методи синхронізації потоків.

Файли та їх властивості. Поняття файлової системи. Іменування файлів. Структура файлу. Типи файлів. Доступ до файлів. Атрибути файлу. Файли, відображувані на адресний простір пам'яті. Каталоги. Реалізація файлової системи. Структура файлової системи. Реалізація файлів. Реалізація каталогів.

3 Комп'ютерні системи

Комп'ютерні системи і паралельна обробка інформації. Класифікація обчислювальних систем обробки даних, структурна організація. Зосередженні та розподілені системи. Функціонування комп'ютерних систем. Основні параметри та характеристики.

Способи організації паралельної обробки інформації: з'єднання в часі етапів рішення різних задач, одночасне рішення різних задач, конвеєрна обробка інформації. Класифікація комп'ютерних систем паралельної обробки інформації.

Метрики комп'ютерних систем: продуктивність, ефективність. Надійність.

Комп'ютерні системи з конвеєрною обробкою інформації. Призначення, принцип побудови. Послідовне ввімкнення операційних блоків конвеєра. Конвеєр даних і команд. Синхронні та асинхронні конвеєрні системи. Ефективність конвеєрних систем. Приклади застосування конвеєрних систем.

Матричні комп'ютерні системи. Призначення, особливості організації і функціонування. Основні параметри матричних комп'ютерних систем. Процесорні елементи в матричних системах. Багатомодальна логіка матричних процесорів. Приклади структурної організації матричних комп'ютерних систем, порівняльна характеристика.

Організація пам'яті в паралельних і розподілених комп'ютерних системах, основні визначення, призначення. Способи організації пам'яті в паралельних комп'ютерних системах. Способи організації пам'яті в розподілених комп'ютерних системах.

Системи введення-виведення даних в комп'ютерних системах. Призначення, структура та функціонування систем введення-виведення даних в комп'ютерних системах. Класифікація. Основні параметри. Системи введення-виведення даних з обліком продуктивності процесорних елементів комп'ютерної системи.

Інтерфейси комп'ютерних систем. Призначення та структура. Основні параметри. Типи інтерфейсів, в залежності від способу організації передачі даних: паралельний інтерфейс, послідовний інтерфейс, зв'язний інтерфейс. Порівняльна характеристика. Сфери застосування різних типів інтерфейсів.

Паралельні та розподілені комп'ютерні системи. Призначення, структурна організація та функціонування. Розподілення функцій між процесорами. Структурний, мікропрограмний та програмний рівні спеціалізації процесорів. Приклади побудови. Основні параметри. Організація обчислювального процесу.

Відмовостійкі паралельні і розподілені комп'ютерні системи. Основні поняття відмовостійкості. Надійнісні характеристики КС: інтенсивність відмовлень, напрацювання на відмовлення, час відновлення, коефіцієнт готовності.

4 Комп'ютерні мережі

Поняття комп'ютерної мережі. Зближення локальних і глобальних мереж. Зв'язок point to point. Найпростіший випадок взаємодії двох комп'ютерів. Мережі відділів. Мережі кампусів. Мережі масштабу підприємства.

Топологія фізичних зв'язків. Адресація вузлів мережі. Комутація й мультиплексування. Комутація каналів і комутація пакетів. Ethernet - приклад стандартної технології комутації пакетів.

Типи ліній зв'язку. Середовище передачі інформації. Провідні лінії зв'язку. Кабельні лінії: кручена пара, коаксіальний кабель, оптоволоконний кабель. Радіоканали наземного та супутникового зв'язку. Апаратури передачі даних. Властивості протоколів каналного рівня.

Загальна характеристика протоколів локальних мереж. Стандартна топологія та поділюване середовище.

Технологія Ethernet. Метод доступу CSMA/CD. MAC - адреси. Етапи доступу до середовища. Виникнення колізій. Час подвійного обороту та розпізнавання колізій. Продуктивність мережі Ethernet. Поняття технології Token Ring. Маркерний доступ до поділюваного середовища.

Стандарти кабелів для будинків і кампусів. Кабелі на основі неекранованої та екранованої звитої пари. Функції та характеристики мережних адаптерів. Класифікація мережних адаптерів. Концентратор Ethernet. Його основні та додаткові функції. Конструктивне виконання концентраторів.

Логічна структуризація за допомогою мостів і комутаторів. Поняття комутатора. Необхідність заміни концентраторів комутаторами Ethernet. Недоліки топології мережі на комутаторах.

Архітектура глобальної мережі (інтермережі). Принципи маршрутизації. Поняття протоколів маршрутизації. Реалізація між мережної взаємодії засобами TCP/IP. Багаторівнева структура стека TCP/IP. Прикладний рівень. Транспортний рівень. Рівень міжмережної взаємодії. Рівень мережних інтерфейсів.

Адресація в IP мережах. Типи адрес в IP - мережах. Форми запису IP адреси. Класи IP- адрес. Особливі IP- адреси. Використання масок при IP - адресації. Централізований розподіл IP - адрес. Автоматизація призначення IP-адрес.

Маршрутизатори. Функціональна модель маршрутизатора. Основні функції маршрутизатора: рівень інтерфейсу; рівень мережного протоколу; рівень протоколів маршрутизації. Додаткові функціональні можливості маршрутизаторів. Фільтрація пакетів за допомогою маршрутизаторів. Класифікація маршрутизаторів по областях застосування. Комутатори 3-го рівня із класичною маршрутизацією.

5 Програмування

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

Змінні і базові типи даних мови C. Базові типи та їх розміри в мові програмування C, оголошення. Програми зі змінними, включаючи найпростіші арифметичні операції. Перетворення і приведення типів. Організація циклів у мові C. 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 C з використанням рекурсивних функцій. Препроцесор мови C. Властивості препроцесора мови C і приклади типових препроцесорних директив і конструкцій. Використання аргументів командного рядка в C. Способи передачі аргументів командного рядка операційної системи Windows в програму, читання кількості аргументів і вивід імен цих аргументів з можливістю запуску додатків.

Література

1. Савенко О.С., Кльоц Ю.П., Лисенко С.М. Системне програмне забезпечення. – Хмельницький: ХНУ, 2016. – 403с.
2. Э. Таненбаум. Современные операционные системы, 3-е издание // СПб: Питер, 2010. 1120стр. ISBN: 978-5-49807-306-4, 978-013006633
3. Таненбаум Э., Бос Х. Современные операционные системы, 4-е издание // СПб: Питер, 2015. - 1120с.
4. Роберт Лав. Ядро Linux: описание процесса разработки. 3-е издание // СПб: Вильямс, 2012. 496 стр. ISBN 978-5-8459-1779-9
5. Ричард Блум, Кристина Бреснахэн. Командная строка Linux и сценарии оболочки. Библия пользователя, 2-е издание // СПб: Диалектика, 2012. 784 стр. ISBN 978-5-8459-1780-5
6. Александр Степанов, Пол Мак-Джонс. Начала программирования // СПб: Вильямс, 2011. 272с. ISBN 978-5-8459-1708-9, 978-0-321-63537-2
7. Колисниченко Денис. Командная строка Linux и автоматизация рутинных задач // СПб: БХВ, 2012. 352 стр. ISBN 978-5-9775-0850-6
8. Брайан Книттель. Windows 7. Скрипты, автоматизация и командная строка // СПб: Питер, 2012. 784 стр. ISBN 978-5-459-00656-8
9. Никлаус Вирт, Юрг Гут кнехт. Разработка операционной системы и компилятора. Проект Обертон // М.: ДМК, 2012. 560 стр. ISBN 978-5-94074-672-0
- 10.Иванов Н.Н. Самоучитель. Программирование в Linux 2-е изд. // СПб: БХВ, 2012. 400 стр. ISBN 978-5-9775-0744-8
- 11.Колисниченко Денис. Разработка Linux-приложений // СПб: БХВ, 2012. 432 стр. ISBN 978-5-9775-0747-9
- 12.Фленов М.Е. Linux глазами хакера // СПб: БХВ, 2012. 480 стр. ISBN 978-5-9775-0547-5
- 13.Эрнст Спиридонов, Михаил Клыков. Операционные системы // Издательство «Либроком», 2010. 352 стр. ISBN 978-5-397-01467-0
- 14.Робачевский А.М. Немнюгин С.А. Стесик О.Л.. Операционная система UNIX // СПб: БХВ, 2010. 656 стр. ISBN 978-5-94157-538-1
- 15.Козловський А.В. Комп'ютерна техніка та інформаційні технології: навч. посіб./ А.В. Козловський, Ю.М. Паночишин, Б.В. Погрішук.-К.: Знання, 2014.- 463с.
16. Проектування комп'ютеризованих систем управління: Опорний конспект лекцій. – Тернопіль, ТНЕУ. // http://dspace.tneu.edu.ua/retrieve/52377/Лекції_ПКСУ.pdf.

17. Чернишенко С.В. Паралельні та розподілені обчислення: навч. посіб./ С.В. Чернишенко, М.М. Ясько, В.С. Чернишенко.-Хмельницький: ХНУ, 2013.-111с.
18. Комп'ютерні системи паралельної обробки даних. Навчальний посібник для студентів напряму підготовки "Комп'ютерна інженерія", В.О. Бойчук, О.В. Огневий, Ю.В. Хмельницький. – Хмельницький: ХНУ, 2013. – 250 с.
19. В.Л. Бройдо В.Л., Ильина О.П. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 4-е изд.-СПб.:Питер,2011.-560с.
20. Вильям Столлингс. Копьютерные системы передачи данных, 6-е издание. М.: Издательский дом «Вильямс», 2010.-1024 с.
21. Мясіщев О.А., Джулій В.М., Красильников С.Р., Чешун В.М. Мережні інформаційні технології: Навчальний посібник з грифом МОНУ. - Хмельницький: ХНУ, 2012. - 422 с.
22. Михайлов Б.М., Халабия Р.Ф. Классификация и организация вычислительных систем. Учебное пособие. - М.: МГУПИ. 2010. - 144 с.
23. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов. 5-е изд. – СПб. Питер, 2016. – 944 с. ил.
24. Танненбаум Э. Компьютерные сети. 5-изд. - СПб. Питер, 2012.
25. Лукас Майкл. FreeBSD. Подробное руководство. – Издательство Символ-Плюс. М., 2010.- 864 с. ил.
26. Брайан Керниган, Деннис Ритчи. Язык программирования Си. — Санкт-Петербург: Невский диалект, 2010. — 352 с. — (Библиотека программиста).
27. Брайан Керниган, Деннис Ритчи. Язык программирования С. — Москва: Вильямс, 2016. — 304 с.
28. П Морган Скиннер. С# 4.0 и платформа .NET 4 для профессионалов. – Вильямс, 2011. -461 с.:ил.
29. Бьерн Страуструп. Язык программирования С++. - Бином, 2015. - 461 с.:ил.
30. Герберт Шилдт. С++ для начинающих. Шаг за шагом – ЭКОМ Паблишерз, 2013. -239 с.:ил.
31. Остапов С. Е. Технології захисту інформації: навч. посіб. - Харків, 2013. - 476 с.
32. Кочарян А. Б. Виховання культури користувача Інтернету. Безпека у всесвітній мережі: навч.-метод. посіб. - Київ, 2011. - 100 с
33. Антонюк А. О. Теоретичні основи моделювання та аналізу систем захисту інформації: [монографія] / А. О. Антонюк, В.В. Жора. - Ірпінь Національний університет ДПС України, 2010. - 310 с.
34. Остапов С. Технології захисту інформації. Посібник. – Родовід, 2014 – 428 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. 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

3. 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

4. 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

5. 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

6. Ризик - це:

- забезпечення безпеки системи і/або переданих даних
- імовірність того, що конкретна атака буде здійснена з використанням конкретної вразливості
- рішення відображене в політиці безпеки
- використання більше одного механізмів безпеки
- інша відповідь.

7. 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

8. 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.

9. 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.

10. 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

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

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

12. Чому дорівнює значення виразу: $x = 0; --x ? --x : x;$

- 0
- 1
- 1
- 2
- інша відповідь.

13. Які з перерахованих ключових слів не є зарезервованими в C?

- switch
- undo
- enum
- struct
- інша відповідь.

14. Що виведе на екран наступний код:

```
#include "stdio.h"  
int dbl(int); // 1
```

```

int main() {
    printf("%d", dbl(5)); // 2
    return 0;
}
int dbl(int a) { // 3
    return a * 2;
}

```

- 100
- помилка компіляції в 1 рядку
- 0
- помилка компіляції в 3, 2 рядку
- інша відповідь

15. Чому дорівнює значення d в наступному виразі `enum { a, b=3, c=5, d }`;

- 7
- 6
- 8
- -7
- інша відповідь.

16. Пріоритетне планування передбачає:

- створення черги, з якої на виконання вибирається процес з найвищим пріоритетом
- створення декількох черг, для кожної з яких виділяються різні кванти часу (перша - один, друга – 2, третя - 4)
- виділення рівних квантів часу процесам, що виконуються циклічно без пріоритетів
- виконання процесу, час завершення якого мінімальний
- інша відповідь

17. Безпріоритетне планування передбачає:

- створення черги, з якої на виконання вибирається процес з найвищим пріоритетом
- виділення рівних квантів часу процесам, що виконуються циклічно без пріоритетів
- створення декількох черг, для кожної з яких виділяються різні кванти часу (перша - один, друга – 2, третя - 4)
- виконання процесу, час завершення якого мінімальний
- інша відповідь

18. На жорсткому диску структури MBR можна створювати не більше чотирьох розділів через:

- обмеженість пропускної здатності шини
- особливості підтримки BIOSa
- обмеженість об'єму жорсткого диску
- обмеженість розміру першого сектора
- інша відповідь

19. В розширеному розділі диску (Extended partition) структури MBR знаходиться інформація про

- активні розділи
- файлові системи розділів
- файлову таблицю розміщення
- встановлену операційну систему
- інша відповідь

20. Що таке маршрутизатор?

- це мережний пристрій, призначений для з'єднання групи комп'ютерів з одними й тими ж мережними адресами
- пристрій, що збирає інформацію про топологію міжмережних з'єднань і на її підставі пересилає пакети мережного рівня в
- мережу призначення
- мережний пристрій, що поєднує комп'ютери, інтерфейсні адаптери яких мають різні MAC адреси
- технічні засоби й програмне забезпечення, що реалізують обмін даними між комп'ютерами за допомогою протоколу TCP/IP
- інша відповідь

21. Продуктивність технічних засобів оцінюється:

- показниками використання пристрою в процесі роботи системи
- продуктивністю технічних засобів з урахуванням простоїв
- набором швидкодій усіх пристроїв
- числом задач, що виконуються системою за одиницю часу
- інша відповідь

22. Недоліки комплексів з загальною шиною:

- відкрита архітектура
- доступ всіх пристроїв до модулів ОЗП
- легко змінювана структура
- порівняно низька вартість
- інша відповідь

23. СОД на основі окремих ЕОМ відносяться :

- до класу паралельних
- до класу послідовних
- до класу зосереджених
- до класу розподілених
- інша відповідь

24. В обчислювальних комплексах прямий зв'язок здійснюється через:

- загальні запам'ятовуючі пристрої
- зовнішні пристрої
- оперативну пам'ять
- інтерфейс прямого керування
- інша відповідь

25. Недоліки комплексів з багатовходовими ОЗП:

- можливість вирішення конфліктів
- ускладнений доступ до інших модулів ОЗП
- кількість входів дорівнює кількості пристроїв
- можливість виділення індивідуальної пам'яті
- інша відповідь

