МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

«ЗАТВЕРДЖУЮ»
Голова приймальної комісії
Олег ГРИГОР
_____
«19» квітня 2024 р.

ПРОГРАМА
фахового вступного іспиту
при вступі на навчання для здобуття
освітньо-наукового ступеня доктора філософії
зі спеціальності 123 – Комп'ютерна інженерія
(освітньо-наукова програма – Комп'ютерні системи та мережі)

Черкаси 2024

1 ПРОГРАМА ВСТУПНИХ ВИПРОБУВАНЬ

Програма вступних випробувань складена відповідно до Порядку прийому на навчання для здобуття вищої освіти в 2024 році, затвердженого наказом Міністерства освіти і науки України № 266 від 06 березня 2024 року, зареєстровано в Міністерстві юстиції України 14 березня 2024 року за № 379/41724 (зі змінами) (далі – Порядок)

1.1 ВИМОГИ ДО РІВНЯ ПІДГОТОВКИ ВСТУПНИКІВ

До участі у конкурсі щодо зарахування на навчання для здобуття освітньо-наукового ступеня доктора філософії **зі спеціальності 123 – Комп'ютерна інженерія (освітньо-наукова програма – Комп'ютерні системи та мережі)** згідно переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого Постановою Кабінету Міністрів України від 29 квітня 2015 року № 266 (зі змінами), допускаються особи, які здобули освітній ступінь магістра або освітньо-кваліфікаційний рівень спеціаліста (*на отримання ОСН доктора філософії*).

Вступник має виявити базові знання з теорії та практики дисциплін, що виносяться на вступне випробування.

1.2 МЕТА ТА ЗАВДАННЯ ВСТУПНИХ ВИПРОБУВАНЬ

Перевірити відповідність знань, умінь, навичок вступників вимогам програм.

Оцінити ступінь підготовки вступників до закладів вищої освіти для навчання та здобуття ступеня доктора філософії **зі спеціальності 123 – Комп'ютерна інженерія (освітньо-наукова програма – Комп'ютерні системи та мережі).**

1.3 ПЕРЕЛІК ДИСЦИПЛІН ТА РОЗДІЛІВ З НИХ, ЯКІ ВИНОСЯТЬСЯ НА ВСТУПНІ ВИПРОБУВАННЯ

На іспит виносяться питання з навчальних програм наступних дисциплін:

1. Комп'ютерні мережі.
2. Операційні системи.
3. Захист інформації в комп'ютерних системах.

4. Діагностика комп'ютерних мереж.

Перелік тем з навчальних дисциплін, що виносяться на іспит:

1.3.1 Дисципліна «Комп'ютерні мережі»

1. КОМП'ЮТЕРНІ МЕРЕЖІ (КМ) ТА ЇХ КЛАСИФІКАЦІЯ. Історія виникнення та класифікація КМ. Стандартизація в комп'ютерних мережах. Джерела стандартів.
2. ЕТАЛОННА МОДЕЛЬ OSI ТА ХАРАКТЕРИСТИКА ЇЇ РІВНІВ. Поняття відкритої системи. Еталонна модель OSI та її загальна характеристика. Характеристика окремих рівнів еталонної моделі OSI. Відповідність між основними протокольними стеками та моделлю OSI.
3. ОСНОВНІ ПРОГРАМНІ ТА АПАРАТНІ КОМПОНЕНТИ МЕРЕЖІ. Складові частини комп'ютерних мереж та операційні системи (ОС). Типи серверів. Класифікація мережних ОС.
4. СЕРЕДОВИЩА ПЕРЕДАВАННЯ ДАНИХ ТА ТОПОЛОГІЯ КМ. Середовища передавання даних та їх основні характеристики. Фізична та логічна топології мереж. Базові топології локальних мереж.
5. МЕТОДИ ДОСТУПУ ТА КОМУТАЦІЇ В МЕРЕЖАХ. Схема ланки передавання даних. Форми передавання даних у каналах КМ. Синхронізація даних. Принцип дії. Передача даних з використанням мережного адаптера. Загальна характеристика та класифікація адаптерів. Будова та складові частини адаптера. Робота адаптера під час приймання та передавання даних.
6. ПРОТОКОЛИ КОМП'ЮТЕРНИХ МЕРЕЖ ТА ЇХ ФУНКЦІЇ. Протокольний стек TCP/IP. Структура мережі протоколу TCP/IP. Мережа Інтернет та її основні сервіси. Адресація в IP–мережах. Служба імен та сервери DNS. Характеристика основних протоколів стеку.
7. МЕРЕЖЕВІ ТЕХНОЛОГІЇ ЛОКАЛЬНИХ МЕРЕЖ ТА ЇХ ХАРАКТЕРИСТИКИ. Мережеві архітектури першого та другого покоління. Архітектура Ethernet та характеристика її різновидів. Формати фреймів Ethernet. Загальна характеристика та історія розвитку.
8. БЕЗДРОТОВІ КОМП'ЮТЕРНІ МЕРЕЖІ. Загальна характеристика та сфери застосування. Класифікація. Переваги та недоліки бездротових мереж. Обладнання для бездротових мереж.

1.3.2 Дисципліна «Операційні системи»

1. ОС, ЇХ ПРИЗНАЧЕННЯ, СКЛАДОВІ ЧАСТИНИ І ФУНКЦІЇ. ОС як інтерфейс між користувачем і ЕОМ. ОС як диспетчер ресурсів. Класифікація ОС.

2. ПОНЯТТЯ ПРОЦЕСУ ЯК МЕТОДУ КОНТРОЛЮ ПРОГРАМ, які виконує процесор, і керування ними. 3 складові процесу. Поняття віртуальної пам'яті. Віртуальна адреса, реальна адреса. Узагальнена модель ієрархічної ОС, її рівні.

3. ХАРАКТЕРИСТИКИ СУЧАСНИХ ОС І ЇХ ОСОБЛИВОСТІ. Основні особливості Windows (стуктурні рівні, модулі виконавчої системи та її структура в рамках моделі клієнт/сервер, типи користувацьких процесів). Традиційні та сучасні системи UNIX, їх короткі характеристики, характеристика Linux.

4. ПРОЦЕСИ І ПОТОКИ. Потоки в Windows. Керування процесами і потоками в Linux.

5. РОБОТА ОС ПО ЗАБЕЗПЕЧЕННЮ ПАРАЛЛЕЛЬНИХ ОБЧИСЛЕНЬ: взаємовиключення і багатозадачність. Принципи паралельних обчислень. Взаємовиключення: апаратний підхід (алгоритм Деккера, алгоритм Петерсона). Апаратна підтримка взаємовиключень в паралельних обчисленнях. Семафори. Монітори. Передача сповіщень. Принципи взаємного блокування. Запобігання взаємоблокуванню. Знищення взаємоблокувань. Алгоритм знаходження взаємоблокувань. Механізми паралельних обчислень в Windows.

6. ПАМ'ЯТЬ. КЕРУВАННЯ ПАМ'ЯТТЮ: вимоги до керування пам'яттю, розподілення пам'яті, сторінкова організація, сегментація. Пам'ять. Віртуальна пам'ять: апаратне забезпечення і керуючі структури. Програмне забезпечення операційної системи. Керування пам'яттю в UNIX та SOLARIS. Керування пам'яттю в Linux. Керування пам'яттю в Windows.

7. ПЛАНУВАННЯ. Планування в однопроцесорних системах: типи планування процесора, алгоритми планування, традиційне планування UNIX. Багатопроцесорне планування і планування реального часу. Планування в Linux.

1.3.3 Дисципліна «Захист інформації в комп'ютерних системах»

1. НАЙПРОСТІШІ ШИФРИ. ШИФРУВАННЯ ДАНИХ.

Шифри простої заміни, перестановок, Цезаря, Віженера, Вернама. Біграмне шифрування. Обладнання шифрування даних.

2. КЛАСИФІКАЦІЯ ШИФРІВ.

Симетричні та асиметричні шифри. Їх порівняння та особливості. Розповсюдження ключів шифрування. Блочні та поточні шифри. Їх порівняння та особливості. Синхронні та асинхронні поточні шифри. Режим зчеплення блоків.

3. МАТЕМАТИЧНІ ОСНОВИ КРИПТОГРАФІЇ (ЗА ШЕННОНОМ).

Абсолютна та умовна стійкість шифру. Вимоги до ключа шифрування даних. Довжина ключа та його статистичні властивості. Розкриття шифру. Випробування ключів. Проблема генерації ключів.

4. СУЧАСНА ПРИКЛАДНА КРИПТОГРАФІЯ.

Області застосування методів криптографічного захисту. Захист від несанкціонованого читання даних, від нав'язування хибних даних, ідентифікація користувачів, контроль цілісності інформації, аутентифікація джерела інформації, електронний цифровий підпис, захист документів та цінних паперів від підробки.

5. КЛАСИФІКАЦІЯ НЕБЕЗПЕЧНИХ ЯВИЩ.

Атаки, види атак. Криптоаналіз на основі шифр-тексту, відкритого тексту, обраного відкритого тексту, обраного шифр-тексту, адаптованого відкритого тексту, адаптованого шифр-тексту, апаратних помилок.

6. СИМЕТРИЧНІ КРИПТОСИСТЕМИ.

Криптографія з закритим ключем. Алгоритм DES. Процедура шифрування. Процедура формування ключів. Режими роботи алгоритму. Гамування та його властивість. Зчеплення блоків. Трек помилки. Криптоалгоритми ДСТУ ГОСТ 28147:2009, AES. Особливості. Криптостійкість. Області застосування. ДСТУ 7624:2014.

7. НЕСИМЕТРИЧНІ КРИПТОСИСТЕМИ.

Криптографія з відкритим ключем. Подвійне гамування. Одностороння функція. Алгоритм RSA. Алгоритми шифрування та формування ключів. Алгоритм Ель-Гамаля. Області застосування. Ідентифікація та аутентифікація. Електронний цифровий підпис.

8. КОМП'ЮТЕРНА СТЕГАНОГРАФІЯ. ПРИХОВАНІ КАНАЛИ.

Поняття стеганографії. Комп'ютерна стеганографія. Приклади застосування. Стеганографічні методи приховування інформації. Приховані канали зв'язку. Використання прихованих каналів для передавання конфіденційної інформації.

9. ГЕНЕРАЦІЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ.

Лінійні та нелінійні генератори ключів. Кільце лишків у кільці цілих чисел, М-послідовності, конгруенц-генератор. Оцінка генераторів. Тести послідовностей. Умови «білизни». Конгруенц-генератор. Рандомізація. Декореляція. Умови криптографічної стійкості генераторів.

10. КОМП'ЮТЕРНІ ВІРУСИ ТА ВІРУСОЛОГІЯ.

Загальні відомості про комп'ютерні віруси: класифікація вірусів; алгоритми функціонування вірусів; технології та засоби створення і розповсюдження комп'ютерних вірусів. Технології захисту комп'ютерних систем від комп'ютерних вірусів: конструктори вірусів; антивірусне програмне забезпечення та сутність його побудови і застосування; методи та технології захисту комп'ютерних систем від вірусів.

11. МЕТОДИ, МЕТОДОЛОГІЇ, ТЕХНОЛОГІЇ І ЗАСОБИ АУТЕНТИФІКАЦІЇ ТА ІДЕНТИФІКАЦІЇ.

Методи і технології ідентифікації користувачів в розподіленнях комп'ютерних системах. методи аутентифікація та ідентифікація суб'єктів на основі симетричних систем шифрування. Поняття майстер ключа та змінного ключа. Електронний цифровий підпис, методи та засоби: встановлення цілісності повідомлень на основі симетричних та асиметричних систем шифрування. Поняття сигнатури повідомлення та цифрового підпису; аутентифікація та ідентифікація суб'єктів в протоколах відкритих замовлень. Поняття електронних чеку та квитанції; багаторівнева організація формування та використання ключів шифрування. Функції майстер-ключа, системного, клієнтського, торгово-касового та сесійного ключів

1.3.4. Дисципліна «Діагностика комп'ютерних мереж»

1. ОСНОВИ ПРОТОКОЛУ OSPFv2 ДЛЯ ОДНІЄЇ ЗОНИ.

Особливості та характеристики OSPF. Пакети OSPF. Принципи роботи OSPF.

2. НАЛАШТУВАННЯ ПРОТОКОЛУ OSPFv2 ДЛЯ ОДНІЄЇ ЗОНИ.

Ідентифікатор маршрутизатора в OSPF. Мережі OSPF типу «точка-точка». Мережі OSPF з множинним доступом. Зміна OSPFv2 для однієї зони. Поширення маршруту за замовчуванням. Перевірка OSPFv2 для однієї зони.

3. ПОНЯТТЯ МЕРЕЖНОЇ БЕЗПЕКИ.

Сучасний стан кібербезпеки. Суб'єкт загрози. Шкідливе ПЗ. Типові мережні атаки. Загрози та вразливості IP. Вразливості TCP та UDP. IP-сервіси. Найкращі практики мережної безпеки. Криптографія.

4. ПРИНЦИПИ РОБОТИ ACL.

Призначення ACL. Шаблонні маски в ACL. Рекомендації щодо створення ACL. Типи ACL для IPv4.

5. ОРГАНІЗАЦІЯ WAN.

Призначення WAN. Принципи роботи WAN. Традиційні WAN-з'єднання. Сучасні WAN-з'єднання. Інтернет- з'єднання.

6. КОНЦЕПЦІЯ QoS.

Якість передавання даних у мережі. Характеристики трафіку. Алгоритми формування черг. Моделі QoS. Технології впровадження QoS.

7. КЕРУВАННЯ МЕРЕЖЕЮ.

Виявлення пристроїв за допомогою протоколу CDP. Виявлення пристроїв за допомогою LLDP. Протокол NTP. Протокол SNMP. Протокол Syslog. Технічне обслуговування файлових систем маршрутизаторів та комутаторів. Керування образами IOS.

8. ПОШУК ТА УСУНЕННЯ НЕСПРАВНОСТЕЙ У МЕРЕЖАХ.

Мережна документація. Процедура пошуку та усунення несправностей. Інструменти для пошуку та усунення несправностей. Ознаки та причини проблем з мережею. Пошук та усунення несправностей IP-з'єднання.

1.4 СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1.4.1 Дисципліна «Комп'ютерні мережі»

1. Odom, W. CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. 2019. 848p.
2. Odom, W. CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press. 2019. 624p.
3. Scott, R. Computer Networking. Russell Scott. 2021. 360 p.
4. Murray, B. Computer Networking: The Complete Guide. Murphy & Moore Publishing. 2022. 244 p.
5. Комп'ютерні мережі. Частина 1. Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 121 «Інженерія програмного забезпечення» та 126 «Інформаційні системи та технології», спеціалізації «Інженерія програмного забезпечення інформаційно управляючих систем» та «Інформаційне забезпечення робототехнічних систем»/ Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 8,6 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с
6. Комп'ютерні мережі : курс лекцій / Ю. В. Волосюк. – Миколаїв : МНАУ, 2019. – 203 с.

1.4.2 Дисципліна «Операційні системи»

7. Федотова-Півень І. М. Операційні системи: навчальний посібник / І.М. Федотова-Півень, І. В. Миронець, О. Б. Півень, С. В. Сисоєнко, Т. В. Миронюк; Черкаський державний технологічний університет; за ред. проф. В. М. Рудницького. – Харків: ТОВ «ДІСІ ПЛЮС», 2019. – 216 с.
8. Булатецький В. В., Булатецька Л. В. Системне програмування та операційні систем : електронний курс навчальної дисципліни, затверджений НМР ВНУ імені Лесі Українки, протокол № 6 від 17.01.2021. Луцьк: ВНУ ім. Лесі Українки, 2021. URL: http://cs.vnu.edu.ua/moodle/course/view.php?id=5
9. William Stallings. Operating Systems: Internals and Design Principles, 9th Edition. – Pearson, 2021. ISBN-13: 9780137516742
10. William Shotts. The Linux Command Line, 2nd Edition: A Complete Introduction. 2019. 504 p.
11. Операційні системи: навч. посіб. / В. Г. Зайцев, І. П. Дробязко; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2019. – 240 с.

12. Andrew S. Tanenbaum, Herbert Bos . Modern Operating Systems, 4th Edition Електронний ресурс. http://indexof.es/Varios2/Modern%20Operating%20Systems%204th%20Edition.pdf

1.4.3 Дисципліна «Захист інформації в комп'ютерних системах»

1. Захист інформації в комп'ютерних системах : підручник для студ. спец. 123 «комп'ютерна інженерія» / уклад. О. М. Гапак, С. І. Балога; рец. : М. І. Глебена. – Ужгород : ПП "АУТДОР-ШАРК, 2021. – 184 с.
2. Новітні технології захисту інформаці: підручник / М. Г. Луцький, В. О. Хорошко, Ю. Є. Хохлачова [та ін.]. – К. : НАУ, 2023. – 312 с
3. Полторак В.П. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах : навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології». – Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с.
4. Інформаційна безпека [Текст] : навч. посіб. / Ю. Я. Бобало [та ін.] ; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого ; Нац. ун-т "Львів. політехніка". - Львів : Вид-во Львів. політехніки, 2019. – 573.
5. Andress J. Foundations of information security: a straightforward introduction. San Francisco : No Starch Press, 2019. 222 p.

1.4.4 Дисципліна «Діагностика комп'ютерних мереж»

1. Stewart J.M., Kinsey D. Network security, firewalls, and VPNs. Burlington : Jones & Bartlett Learning, 2021. 482 p.
2. Odom, W. CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. 2019. 848p.
3. Odom, W. CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press. 2019. 624p.
4. Scott, R. Computer Networking. Russell Scott. 2021. 360 p.
5. Murray, B. Computer Networking: The Complete Guide. Murphy & Moore Publishing. 2022. 244 p.
6. Cisco - Networking, Cloud, and Cybersecurity Solutions. URL: https://cisco.com (date of the request: 15.08.2022).
7. Cisco Networking Academy Builds IT Skills & Education For Future Careers. URL: https://www.netacad.com/ (date of the request: 15.08.2022).

2 ПОЯСНЮВАЛЬНА ЗАПИСКА ДО ВСТУПНИХ ВИПРОБУВАНЬ

Вимоги до вступного іспиту відповідають вимогам чинних навчальних програм згідно стандарту вищої освіти **зі спеціальності 123 – Комп'ютерна інженерія (освітньо - наукова програма – Комп'ютерні системи та мережі).**

Час тестування – 2 астрономічні години (120 хвилин).

Вступні випробування проводяться у формі тестування в письмовій формі.

Тестове завдання містить 25 пунктів (питань).

Для тестового питання подано 4 варіантів відповідей, з яких тільки одна правильна. Тестове питання вважається виконаним правильно, якщо вступник вказав саме правильну відповідь.

Правильність виконання завдань оцінюється відповідно до критеріїв оцінювання знань.

Екзаменатор не зобов'язаний читати розв'язання завдань, що наведені вступником в чернетці.

Оцінка за письмову роботу виставляється як сума балів за кожне завдання і являє собою сумарний рейтинг.

Результати **фахового вступного випробування** оцінюються за шкалою від 0 до 100 балів для здобуття освітньо-наукового ступеня доктора філософії.

Особи, які набрали на вступних випробуваннях менше ніж 24 бали, позбавляються права участі в конкурсі за спеціальністю (освітньо–науковою програмою).

3 КРИТЕРІЇ ОЦІНЮВАННЯ ВСТУПНИХ ВИПРОБУВАНЬ

1. Результати фахового вступного іспиту оцінюються за шкалою від 0 до 100 балів. Оцінка за тест виставляється як сума балів за кожне завдання.

Правила виконання завдань відповідних типів та вимог до запису відповідей вступників наведено в екзаменаційних білетах (тестових завданнях).

Тестове завдання містить 25 пунктів.

Правильна відповідь на кожне тестове питання 1-25 оцінюється у 4 бали, неправильна – 0 балів. Максимальна кількість балів, яку абітурієнт може одержати за відповіді на тести 1-25, складає 100 балів. Вибрану відповідь на тестове питання пояснювати не потрібно.

Якщо відповідь на завдання абітурієнта містить помилки, його оцінка знижується:

- у відповіді *на тести 1-25:* відповідь не позначено або в відповіді на тестове питаня відмічено кілька відповідей відразу – питання оцінюється в 0 балів.

2. Оцінка за тест виставляється як сума балів за кожне завдання.

3. Особи, які набрали на вступних випробуваннях менше ніж 24 бали, позбавляються права участі в конкурсі за спеціальністю (освітньо-науковою програмою).

Голова предметної комісії
зі спеціальності
123 – Комп'ютерна інженерія
(освітньо-наукова
програма – Комп'ютерні
системи та мережі) д.т.н., проф. Віра БАБЕНКО