МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

«ЗАТВЕРДЖУЮ»
Голова приймальної комісії
Олег ГРИГОР
_____
«__22__» ____03____ 2022 р.

ПРОГРАМА

фахових вступних випробувань

при вступі на навчання для здобуття

освітньо-наукового ступеня доктора філософії

зі спеціальності 125 – Кібербезпека

(освітньо - наукова програма – Кібербезпека)

Черкаси 2022

1 ПРОГРАМА ВСТУПНИХ ВИПРОБУВАНЬ

Програма вступних випробувань складена на підставі Умов прийому для здобуття вищої освіти в 2022 році, затверджених Наказом Міністерства освіти і науки України від 13 жовтня 2021 року № 1098, зареєстрованих в Міністерстві юстиції України від 26 листопада 2021 року за № 1542/37164.

1.1 ВИМОГИ ДО РІВНЯ ПІДГОТОВКИ ВСТУПНИКІВ

До участі у конкурсі щодо зарахування на навчання для здобуття освітньо - наукового ступеня доктора філософії **зі спеціальності 125 – Кібербезпека (освітньо – наукова програма – Кібербезпека)** згідно переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету Міністрів України від 29 квітня 2015 року № 266, 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 125 – Кібербезпека (освітньо – наукова програма – Кібербезпека).**

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

На іспит виносяться питання з навчальних програм наступних дисциплін:

1. Забезпечення інформаційної безпеки держави.
2. Інформаційні технології та мови програмування.
3. Операційні системи та системне програмне забезпечення.
4. Програмний захист інформації.
5. Системи інформаційної безпеки.

Перелік тем з навчальних дисциплін, що виносяться на іспит:

1.3.1 Дисципліна «Забезпечення інформаційної безпеки держави»

1. КОНЦЕПТУАЛЬНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ. Сутність забезпечення інформаційної безпеки. Принципи та функції забезпечення інформаційної безпеки.

2. ІНОЗЕМНИЙ ДОСВІД ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ. Спеціальні служби та правоохоронні органи США, які приймають участь у забезпеченні інформаційної безпеки. Структура загальнодержавної системи забезпечення інформаційної безпеки США.

3. ІМІДЖБІЛДІНГ ТА ПІАР-ДІЯЛЬНІСТЬ У ЗАБЕЗПЕЧЕННІ СЕКТОРУ БЕЗПЕКИ. Піар-технології у забезпеченні безпеки держави. Керування іміджем державних служб. Чинники іміджу і антиіміджу в діяльності інститутів сектору безпеки.

4. НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ТА СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ. Загальні положення нормативно-правового регулювання забезпечення інформаційної безпеки України. Структура загальнодержавної системи забезпечення інформаційної безпеки України.

1.3.2. Дисципліна «Інформаційні технології та мови програмування»

1. АЛГОРИТМІЗАЦІЯ ЗАДАЧ. Блок-схеми алгоритмів. Лінійні, розгалужені, циклічні алгоритми.

2. СТРУКТУРА ПРОГРАМИ Pascal ABC. Базові типи даних.

3. ОПЕРАТОРИ МОВИ Pascal ABC. Стандартні процедури і функції мови Pascal ABC. Оператори розгалуження: безумовний та умовний перехід, конструкція типу CASE.

4. ПРОГРАМИ З ЦИКЛАМИ. Цикл з параметром (FOR .. TO .. DO ..). Цикл з передумовою (WHILE .. DO ..). Цикл з постумовою (REPEAT .. UNTIL ..). Вкладені цикли.

5. МАСИВИ. ЗАПИСИ І МНОЖИНИ. Одновимірні, двовимірні масиви, їх опис та обробка. Записи: опис та використання. Множини: опис та використання.

6. ПРОЦЕДУРИ І ФУНКЦІЇ. Звернення до підпрограм. Основні відомості про процедури, функції. Параметри процедур та функцій. Рекурсія. Ряди: їх обробка та використання.

7. ОСНОВНІ ПРИНЦИПИ І ПОНЯТТЯ ОБ'ЄКТНО-ОРІЄНТОВАНОГО ПІДХОДУ. Витоки ООП. Принципи об'єктно-орієнтованого підходу: інкапсуляція, наслідування, поліморфізм. Поняття об'єкту. Організація програми в об'єктно-орієнтованій моделі, повідомлення. Поняття класу. Порівняння процедурного та об'єктно-орієнтованого підходу.

8. ВВЕДЕННЯ ДО ПЛАТФОРМИ MICROSOFT .NET ТА МОВИ C#.

Основні поняття платформи Microsoft .NET та мови C#. Основи мови C#.

9. ОСНОВИ ВИКОРИСТАННЯ МОВИ XML ПІД ЧАС РОЗРОБКИ ДОДАТКІВ ДЛЯ .NET. Основи використання мови XML під час розробки додатків для .Net

10. РЕАЛІЗАЦІЯ ГОЛОВНИХ КОНЦЕПЦІЙ ОБ'ЄКТНО-ОРІЄНТОВАНОГО ПРОГРАМУВАННЯ У МОВІ C#

Основні положення об'єктно-орієнтованого підходу. Класи та об'єкти, співвідношення між ними. Створення та руйнування об'єктів. Реалізація поліморфізму в C#

11. ОСНОВНІ БІБЛІОТЕКИ .NET

Принципи перевантаження операцій. Індексатори та властивості. Обробка виключень. Введення-виведення даних. Колекції. Рядки та регулярні вирази

12. ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ПЛАТФОРМИ .NET ПРИ РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.

Управління пам'яттю та вказівники. Атрибути. Збереження та відновлення стану об'єктів у .NET

1.3.3. Дисципліна «Операційні системи та системне програмне забезпечення»

1. КОМАНДИ. Формати машинних команд. Алгоритми виконання команд. Типи машинних команд. Команди пересилки даних. Арифметичні команди. Логічні команди і команди зсуву. Команди переходів і передач керування. Команди обробки рядків і блоків даних. Команди асемблеру і псевдокоманди. Команди означення даних. Макрозасоби.

2. ПРОГРАМИ. Структура програми. Завантаження сегментних адрес. Зв'язок сегментів усередині програми. Архітектура COM- і EXE- програми. Архітектура COM- програми. Архітектура EXE-програми- Префікс програмного сегмента. Спрощені способи запису програм.

3. СИСТЕМА ПЕРЕРИВАНЬ. Види переривань. Обробка переривання. Вектор переривання. Зразок програми, яка використовує переривання відеоадаптера для виведення рядків символів. Архітектура відеоадаптера. Види відеоадаптерів.

4. КЕРУВАННЯ КЛАВІАТУРОЮ. Рівні керування клавіатурою. Функції для роботи з клавіатурою. Таблиця скен-кодів і розширених кодів. Коди цифрової клавіатури. Призначення деяких кодів ASCII.

5. КЕРУВАННЯ ЕКРАНОМ. Функції керування екраном. Режими роботи екрана. Зображення символів на екрані дисплея. Відеопам'ять. Створення спеціальних символів на екрані.

6. КЕРУВАННЯ ФАЙЛАМИ. Розподіл пам'яті на диску. Розміщення файлів. Організація таблиці розміщення файлів. Каталог диска. Організація файлу. Підготовка до роботи з файлами. Перелік функцій, доступних через переривання 21H, які використовуються при керуванні файлами. Створення і вилучення файлу. Відкриття та закриття файлу. Функції керування файлом за методом дескриптора файлу. Керування каталогом.

7. РЕЗИДЕНТНІ ПРОГРАМИ. Структура TSR-програм. Основні фунції переривань, що обслуговують резидентні програми.

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

9. 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.

10. ХАРАКТЕРИСТИКИ СУЧАСНИХ ОС І ЇХ ОСОБЛИВОСТІ. Основні особливості Windows (структурні 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.

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

12. 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.

1.3.4 Дисципліна «Програмний захист інформації»

1. КАТЕГОРІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. Основні визначення і поняття теорії захисту інформації. Технічний та програмний захист інформації. Історія розвитку. Сфера застосування. Термінологія.

2. ВИЗНАЧЕННЯ ПОЛІТИКИ БЕЗПЕКИ. Абстрактні моделі захисту інформації. Абстрактні моделі та формальні моделі захисту інформації. Особливості моделей Белла-Ла Падуяі та Біба.

3. КЛАСИ БЕЗПЕКИ. КРИТЕРІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ. Класи безпеки інформації та інформаційних систем. Класифікація систем за критеріями інформаційної безпеки. Вимоги стосовно роботи з конфіденційною інформацією. Створення політики інформаційної безпеки. Електромагнітні та електричні канали витоку інформації. Параметричні канали витоку інформації.

4. КЛАСИФІКАЦІЯ КРИПТОАЛГОРИТМІВ. Тайнопис, криптографія з ключем. Симетричні та асиметричні криптоалгоритми.

5. СИСТЕМИ ШИФРУВАННЯ ДАНИХ, ЯКІ ПЕРЕДАЮТЬСЯ В МЕРЕЖАХ. Канальне шифрування. Абонементне шифрування.

6. СУЧАСНА СИТУАЦІЯ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. РІВНІ МЕРЕЖЕВИХ АТАК. Рівні мережевих атак відповідно до моделі OSI. Захист систем передавання інформації.

7. ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ. Системи ідентифікації й аутентифікації користувача (традиційні та біометричні параметри). Система FireWall-1/VPN-1. Система OmniGuard/Enterprise Security Manager компанії Axent. Брандмауери, мережевий екран PIX Firewall. Апаратно-програмний комплекс захисту інформації “ШИП”, “Dallas

Lock". Криптографічний адаптер. Процесор безпеки мережі. Локатори ліній зв'язку. Сканер NetRecon. Аналізатор телефоних ліній SP-18/T "Багер-01". Детектор електромагнітного поля Д-006.

8. ТЕРМІНАЛИ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ. ОТРИМАННЯ ПАРОЛЯ НА ОСНОВІ ПОМИЛОК. Термінали захищеної інформаційної системи. Отримання пароля на основі помилок адміністратора та користувача. Отримання пароля на основі помилок у реалізації. Соціальна психологія й інші способи отримання пароля.

1.3.5 Дисципліна «Системи інформаційної безпеки»

1. КОНЦЕПТУАЛЬНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. Основні поняття та визначення дисципліни. Структура та зміст інформаційної безпеки. Поняття системи інформаційної безпеки.

2. ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ. КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ. Джерела загроз. Канали витоку інформації. Порушники інформаційної безпеки. Класифікація каналів витоку інформації. Канали втрати конфіденційної інформації. Конфіденційна інформація. Джерела й канали втрати конфіденційної інформації. Легальні й нелегальні методи добування інформації. Технічні канали витоку інформації.

3. НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. Нормативні акти, які закріплюють концептуальні положення забезпечення інформаційної безпеки України. Нормативні акти конституційного напрямку, які закріплюють визначальні положення щодо забезпечення інформаційної безпеки України. Нормативні акти вищих та центральних органів виконавчої влади, які регулюють діяльність у сфері забезпечення інформаційної безпеки України. Зарубіжна нормативна база в галузі захисту інформації. "Оранжева книга" безпеки.

4. ДЕРЖАВНА ІНФОРМАЦІЙНА ПОЛІТИКА УКРАЇНИ. ЗАГАЛЬНОДЕРЖАВНА СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. Цивільно-правовий, кримінально-правовий та адміністративно-правовий захист. Стандарти в галузі ІБ. Державна інформаційна політика України. Нормативно-правові акти в галузі ІБ. Цивільно-правовий, кримінально-правовий та адміністративно-правовий захист. Вітчизняне та зарубіжне законодавство в галузі.

5. УПРАВЛІННЯ ІНЦИДЕНТАМИ ТА РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. Основні класи організаційних заходів. Реагування на інциденти ІБ. Основи планування безперервності роботи інформаційних систем. Поняття політики безпеки. Інформаційно-аналітична діяльність. Етапи управління

ризиками. Класифікація ризиків. Методи та засоби оцінки та управління ризиками.

6. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В СИСТЕМІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. Вітчизняне законодавство з питань захисту ПД. Загальні вимоги до обробки ПД.Особливі вимоги до обробки ПД. Державна служба з питань захисту ПД.

7. ІНЖЕНЕРНО-ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ. Фізичні засоби захисту інформації. Охоронні системи, охоронне телебачення, захист елементів будинків і приміщень. Сучасні апаратні та програмні засоби захисту інформації.

8. КРИПТОГРАФІЧНИЙ ТА СТЕГАНОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ. Основні принципи криптографії. Класифікація криптографічних методів та засобів захисту інформації. Класифікація криптоалгоритмів. Симетрична криптографія. Асиметрична криптографія. Конкурси з вибору стандартів шифрування США і Євросоюзу. Основні принципи стеганографії. Класифікація стеганографічних методів та засобів захисту інформації. Хімічні стеганографічні методи захисту інформації. Фізичні стеганографічні методи захисту інформації. Цифрова стеганографія. Лінгвістична стеганографія. Мережева стеганографія. Квантова стеганографія.

1.4 СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1.4.1 Дисципліна «Забезпечення інформаційної безпеки держави»

1. Бакалинський О.О., Петрик В.М., Мельник Д.С., Супрунов Ю.М. Забезпечення інформаційної безпеки України: навч. посіб. - К.: Вид-во ІСЗЗІ НТУУ «КПІ», 2013. - 208 с.
2. ГУардия. Рейтинг самых дорогих корпоративных брендов Украины -2012 [Електронний ресурс]. - Режим доступу: http://kontrakty.ua/rankings/234
3. Гриняев С.Н. Взгляды военных экспертов США на ведение информационного противоборства // Зарубежное военное обозрение. - 2001 - № 8. - С.10-12.
4. Гриняев С.Н. О ходе работ в Министерстве обороны США по реализации основных положений национального Плана защиты информационных систем. —http://www.agentura.ru/equipment/psih/info/pdd63 — 1.03.2003. — 17:10
5. Гриняев С.Н. О ходе реализации плана защиты информационных систем США // Зарубежное военное обозрение. - 2001. - № 9. - С.7-10.
6. Закон України «Про боротьбу з тероризмом» від 20 березня 2003 р.

// Відомості Верховної Ради України. - 2003. - № 25. - Ст. 180.

7. Закон України «Про внесення змін до деяких законів України щодо захисту населення та інформаційного простору від негативного впливу» від 12 січня 2012р. №4316-УІ.

8. Закон України «Про Державну службу спеціального зв'язку та захисту інформації» від 23 лютого 2006 р. // Відомості Верховної Ради України. - 2006. - № ЗО. - Ст. 258.

9. Закон України «Про державну таємницю» від 21 січня 1994 р. // Відомості Верховної Ради України. - 1994. - № 16. - Ст. 93.

10. Закон України «Про електронний цифровий підпис» від 22 травня 2003 р. №852-ІУ // Відомості Верховної Ради України. - 2003. - № 36. - Ст. 276.

11. Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 р. №851-IV // Відомості Верховної Ради України. — 2003. - N 36. - Ст. 275.

12. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31 травня 2005 р. // Відомості Верховної Ради України. - 2006. - №26. - Ст. 347.

13. Закон України «Про інформацію» від 2 жовтня 1992 р. // Відомості Верховної Ради України. - 1992. - №48. - Ст. 650.

14. Закон України «Про контррозвідувальну діяльність» від 26 грудня 2002 р. // Відомості Верховної Ради України. - 2003. - № 12. - Ст. 89.

15. Закон України «Про Національну програму інформатизації» від 4 лютого 1998 р. // Відомості Верховної Ради України. -1998 - №27-28 - Ст. 181.

16. Закон України «Про Раду національної безпеки і оборони України» від 5 березня 1998 року // Відомості Верховної Ради України - 1998 - № 35 - Ст.

17. Закон України «Про Службу безпеки України» від 25 березня 1992 р. // Відомості Верховної Ради. - 1992. - № 27. - Ст. 382.

18. Закон України «Про Службу зовнішньої розвідки України» від 1 грудня 2005р. // Відомості Верховної Ради України. - 2006. - № 8. - Ст.94.

1.4.2 Дисципліна «Інформаційні технології та мови програмування»

1. Ковалюк Т.В. Основи програмування: Підручник для студентів – К., Вид. група ВНУ, 2005. – 384 с.

2. Шикова О.М. Основи програмування мовою Паскаль у прикладах і завданнях : Навчальний посібник / О.М. Шикова; МАУП. – Київ : МАУП, 2004. – 112с.

3. Бєлов Ю.А. Вступ до програмування мовою С++. / Ю.А. Бєлов, Т.О. Карнаух, Ю.В. Коваль, А.Б. Ставровський. – К.: Видавничо-поліграфічний

центр «Київський університет», 2012. – 175 с.

4. Вступ до програмування мовою С++. Організація даних / Т. О. Карнаух, Ю. В. Коваль, М. В. Потієнко, А. Б. Ставровський. – К.: ВПЦ "Київський університет", 2015.

5. Об'єктно-орієнтоване програмування: конспект лекцій для студентів напряму підготовки "Комп'ютерні науки" всіх форм навчання / Ю. Е. Парфьонов, В. М. Федорченко, М. Ю. Лосєв, О. В. Щербаков. – Харків: Вид. ХНЕУ, 2010. – 312 с. (Укр. мов.)

6. Голуб Б. М. C#. Концепція та синтаксис: навч. посібник / Б. М. Голуб. – Львів : Видавничий центр ЛНУ імені Івана Франка, 2006. – 136 с.

1.4.3 Дисципліна «Операційні системи та системне програмне забезпечення»

1. Stallings, William. Operating systems: internals and design principles / William Stallings. – 7th ed. Prentice Hall, New Jersey, 2012, p.769. ISBN-13:978-0-13-230998-1

2. Kusswurm Daniel. Modern X86 Assembly Language Programming/ Daniel Kusswurm. - Apress, 2019. — 604 p.

3. William Stallings. Operating Systems: Internals and Design Principles, 9th Edition. – Pearson, 2018. ISBN-10: 0-13-467095-7 | ISBN-13: 978-0-13-467095-9.

4. Шоттс У. Командная строка Linux. Полное руководство / У. Шоттс - Питер, 2017. – 480 с.

5. Операційні системи : навчальний посібник. [за ред. В. М. Рудницького] / І. М. Федотова-Півень, І. В. Миронець, О. Б. Півень, С. В. Сисоєнко, Т. В. Миронюк; Черкаський державний технологічний університет. – Харків : ТОВ «ДІСА ПЛЮС», 2019. – 216 с. ISBN 978-617-7645-93-0

6. IA-32 Intel® Architecture Software Developer's Manual. Vol. 2. Instruction Set Reference. Intel Corporation, 2002.

7. Richard Blum. Linux Command Line and Shell Scripting. Wiley; 3. Edition. 2015. 816 p.

8. William Shotts. The Linux Command Line, 2nd Edition: A Complete Introduction. 2019. 504 p

9. Jason Cannon. Linux for Beginners: An Introduction to the Linux Operating System and Command Line. 2013. 204 p.

1.4.4 Дисципліна «Програмний захист інформації»

1. Методы и средства защиты информации /Под ред. Ю. С. Ковтанюка. — К.: ЮНИОР, 2003. — 501 с.

2. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 512 с.

3. Ємець В. Сучасна криптографія. Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів : Бак, 2003. – 144с.

4. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Видавнича група BHV, 2009. – 608с.

5. Рибальський О.В. Основи інформаційної безпеки. Підручник для курсантів ВНЗ МВС України / Рибальський О.В., Смаглюк В.М., Хахановський В.Г.– К.: НАВС,2013.– 255 с.

6. Рибальський О.В. Захист інформації в інформаційно-комунікаційних системах. Навчальний посібник для курсантів ВНЗ МВС України / О.В. Рибальський, В.Г. Хахановський, В.А. Кудінов, В.М. Смаглюк. – К.: Вид. Національної академії внутріш. справ, 2013. – 118 с.

1.4.5 Дисципліна «Системи інформаційної безпеки»

1. Богуш В.М., Юдін О.К. Інформаційна безпека держави: навчальний посібник/ В.М. Богуш, О.К. Юдін. – К.: —Мк-Пресс—, 2005. – 432 с., іл..

2. Лужецький В. А. Основи інформаційної безпеки : навчальний посібник / В. А. Лужецький, О. Д. Кожухівській, О. П. Войтович, – Черкаси: ЧДТУ, 2008. – 223 с

3. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем/ М.В.Гайворонський, О.М. Новіков. – К.: Видавнича група BHV,2009. – 608 с., іл.

4. Юдін О.К., Конахович Г.Ф., Корченко О.Г., Захист інформації в мережах передачі даних: підручник/ О.К. Юдін, Г.Ф. Конахович, О.Г. Корченко. – К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714с., іл.

5. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. — Харків: Вид. ХНЕУ, 200’. — 352 с. (Укр. мов.)

6. Скулиш Є. Д., Остроуха Б. В., Петрик Б. М., Присяжнюк М. М. Інформаційна безпека (соціально-правові аспекти). К., 2005. (Укр. Мова)

7. Жарков Я.М., Дзюба М.Т., Замаруєва І.В., ін. Інформаційна безпека особистості, суспільства, держави: Підручник. – К.: Видавничо-поліграфічний центр “Київський університет”, 2008. – 274 с.

8. Хмельницький О.О. Інформаційна культура: Підготовка кадрів до інформаційної роботи: Навчальний посібник. – К.: КНТ, 2007. – 200 с.

9. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. Посібник. – К.: Кондор, 2004. – 384 с. 7.

2 ПОЯСНЮВАЛЬНА ЗАПИСКА ДО ВСТУПНИХ ВИПРОБУВАНЬ

Вимоги до вступного іспиту відповідають вимогам чинних навчальних програм згідно стандарту вищої освіти **зі спеціальності 125 – Кібербезпека (освітньо-наукова програма – Кібербезпека).**

Час тестування – 2 астрономічні години (120 хвилин).

Вступні випробування проводяться у формі тестування в письмовій формі.

Тестове завдання містить 15 пунктів і складається з *двох* блоків.

Блок 1 – 11 завдань (завдання 1-10, 13). *Блок 2* – 4 завдання (завдання 11, 12, 14, 15).

Блок 1 містить завдання закритого типу, *Блок 2* – відкритого типу.

Для тестового *Блоку 1* подано від 3 до 5 варіантів відповідей, з яких тільки одна правильна. Тестове питання вважається виконаним правильно, якщо вступник вказав саме правильну відповідь.

Блок 2 містить 3 завдання практичного типу і 1 завдання теоретичного типу.

Правильність виконання завдань оцінюється відповідно до критеріїв оцінювання знань.

Екзаменатор не зобов'язаний читати розв'язання завдань, що наведені вступником у 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

Результати фахового вступного випробування оцінюються за 100-бальною шкалою.

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

Тестове завдання містить 15 пунктів і складається з *двох* блоків.

Блок 1 – 11 завдань закритого типу (завдання 1-10, 13).

Блок 2 – 4 завдання відкритого типу (завдання 11, 12, 14, 15).

Правильна відповідь на кожне тестове питання 1-10 оцінюється у 4 бали, неправильна – 0 балів. Максимальна кількість балів, яку абітурієнт може одержати за відповіді на тести 1-10, складає 40 балів. Вибрану відповідь на тестове питання пояснювати не потрібно.

Правильна відповідь на кожне завдання 11-13 оцінюються у 10 балів, неправильна – 0 балів. Максимальна кількість балів, яку абітурієнт може одержати за відповіді на завдання 11-13, складає 30 балів. Вибрану відповідь на тестове питання 13 пояснювати не потрібно.

Правильний розв'язок задачі 14 оцінюється у 10 балів, повна правильна відповідь на теоретичне питання 15 оцінюється у 20 балів.

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

1). *У відповіді на тести 1-10:*

- є виправлення – знімається 2 бали;
- відповідь не позначено або в відповіді на тестове питанні відмічено кілька відповідей відразу – знімається 4 бали.

2). *У відповіді для задач 11,12:*

- висновок про дію фрагмента програми повністю невірний – знімається 10 балів;
- правильно описано послідовність дій операторів у фрагменті програми, але зроблено неправильний або дуже розпливчастий висновок про дію фрагмента в цілому – знімається 6 балів;
- є мілкі неточності в описі елементів фрагменту програми, але в цілому формулювання дії фрагменту вірне – знімається 3 бали;
- немає опису дій елементів програми і є розпливчастий, неконкретний висновок – знімається 8 балів.

3). *У відповіді на тест 13:*

- є виправлення – знімається 5 балів;
- відповідь не позначено або в відповіді на тестове питанні відмічено кілька відповідей відразу – знімається 10 балів.

4). *У відповіді на задачу 14:*

- невірний результат із-за технічної помилки в кінці розв'язку – знімається 3 балів;
- невірний результат внаслідок технічної помилки на початку розв'язку – знімається 4 балів;
- правильний хід розв'язку, але відсутній результат – знімається 5 балів;
- правильний підхід до розв'язання задачі, але відсутнє знання технічних елементів процесу розв'язання – знімається 6 балів;
- правильний опис процесу розв'язання, але сам розв'язок відсутній – знімається 7 балів;
- є знання основних елементів процесу розв'язання, але розв'язок відсутній – знімається 8 балів.

5). *У відповіді на теоретичне питання 15:*

- якщо не розкрито питання повністю, знімається 20 балів;
- якщо відповідь розпливчаста, неконкретна, або викладено інформацію, яка мало стосується питання, оцінка знижується на 16 балів;
- якщо відповідь вірна лише на третину, оцінка знижується на 14 балів;
- якщо відповідь вірна лише на половину, оцінка знижується на 10 балів;
- якщо відповідь містить 3-4 незначні неточності, оцінка знижується на 5 балів;
- якщо відповідь містить 1-2 незначні неточності, оцінка знижується на 2 бали;

1. Оцінка за тест (співбесіду) виставляється як сума балів за кожне завдання.

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

Голова предметної комісії
зі спеціальності 125 – Кібербезпека
(освітньо – наукова програма
– Кібербезпека) д.т.н., доцент Віра БАБЕНКО

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

ШИФР_____

Бланк відповідей на тестові завдання
фахових вступних випробувань для здобуття освітньо-наукового ступеня доктора філософії зі спеціальності 125 – Кібербезпека (освітньо-наукова програма – Кібербезпека)

Варіант №_____

УВАГА! Кожне завдання з 1 по 10 включно і завдання 13 містить лише одну правильну відповідь. За виправлення відповідей в завданнях з 1 по 10 включно знімається 2 бали, за виправлення відповідей в завданні 13 знімається 5 балів. За не позначену відповідь або за позначення кількох відповідей відразу в одному завданні з 1 по 10 включно знімаються 4 бали. За не позначену відповідь або за позначення кількох відповідей відразу в завданні 13 знімається 10 балів. Правильна відповідь позначається значком X.

Наприклад: Якщо Ви вважаєте, що на завдання №4 відповідь "b" є правильною, то Ви маєте зробити відмітку у відповідному полі:

	№1	№2	№3	№4
a				
b				X
c				

Завдання 1-10 і 13 мають по декілька варіантів відповідей, з яких тільки ОДНА ПРАВИЛЬНА. Правильна відповідь на кожне тестове питання 1-10 оцінюється у **4** бали, на тестове питання 13 оцінюється у **10** балів. За виконання завдань 1-10 і 13 максимально можливо отримати **50** балів.

	№1	№2	№3	№4	№5	№6	№7	№8	№9	№10	№13
a											
b											
c											
d											
e											
f											
g											
h											

Завдання 11, 12, 14, 15 оформлюються на вкладишах до письмової роботи. Ці завдання передбачають знання і вміння читати і розуміти програмний код (завдання 11,12), вміння створювати блок-схему і власний працюючий код (завдання 14), ґрунтовність теоретичної підготовки (завдання 15). Правильна відповідь на кожне завдання 11,12,14 оцінюються у **10** балів, повна правильна відповідь на теоретичне питання 15 оцінюється у **20** балів. За виконання завдань 11,12, 14,15 можливо отримати максимально **50** балів.

За весь тест можна отримати **100** балів (за шкалою 0-100 балів).

Завдання 1-10 _____, завдання 11,12,13, 14_____

завдання 15_____

Всього: _____(_____)