МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ БІОТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Голова приймальної комісії
В.о. ректора ДБТУ
_____ А.І. Кудряшов
«22» квітня 2024 р.

ПРОГРАМА
фахового вступного випробування
для здобуття ступеня освіти Бакалавр
на основі НРК6 (НРК7)

Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Освітня програма	Кібербезпека та захист інформації

Харків 2024

ЗМІСТ

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Вступ на основі (основа вступу) - раніше здобутий освітній (освітньо-кваліфікаційний) рівень або освітній ступінь та відповідний рівень Національної рамки кваліфікацій (далі - НРК), на основі якого здійснюється вступ для здобуття ступеня вищої освіти.

Фаховий іспит - форма вступного випробування для вступу на основі НРК6 (НРК7), яка передбачає перевірку здатності до опанування освітньої програми певного рівня вищої освіти на основі здобутих раніше компетентностей.

На навчання за програмою підготовки бакалавра за спеціальністю 125 Кібербезпека та захист інформації (освітня програма Кібербезпека та захист інформації) можуть вступати особи, які отримали диплом бакалавра (спеціаліста, магістра) (НРК6, НРК7) з відповідної або іншої спеціальності та продемонстрували достатній рівень знань з тем, перелік яких винесено для оцінювання підготовленості вступника для здобуття вищої освіти.

Для проведення конкурсних фахових вступних випробувань на навчання на здобутих раніш ступенів освіти бакалавр, магістр; освітньо-кваліфікаційного рівня спеціаліст, наказом ректора ДБТУ створюються фахові атестаційні комісії, діяльність яких регламентується Положенням про приймальну комісію вищого навчального закладу, затвердженого наказом Міністерства освіти і науки України від 15 жовтня 2015 року № 1085 та зареєстрованого у Міністерстві юстиції України 4 листопада 2015 року за № 1351/27796.

Фахове вступне випробування проводиться фаховою атестаційною комісією за програмою, затвердженою ректором ДБТУ.

Програма фахового вступного випробування складена для вступників, які вступають на навчання до Державного біотехнологічного університету за освітньо-професійною програмою бакалавр за спеціальністю 125 Кібербезпека та захист інформації та передбачає оцінку базових знань осіб, що мають здобутий освітні ступені бакалавра (магістра), освітньо-кваліфікаційний рівень спеціаліст, за темами фахових дисциплін, які дають можливість оцінити загальний рівень підготовки вступників до навчання за спеціальністю 125 Кібербезпека та захист інформації.

Програма визначає перелік питань, обсяг, складові та технологію оцінювання знань вступників під час вступу на навчання за ступенем освіти магістр за спеціальністю 125 Кібербезпека та захист інформації.

Мета вступного фахового випробування полягає в комплексній перевірці знань вступників, отриманих ними в результаті вивчення

дисциплін та оцінці відповідності цих знань вимогам до навчання за ступенем бакалавр (магістр), освітньо-кваліфікаційний рівень спеціаліст, на спеціальність 125 Кібербезпека та захист інформації та допуску до участі у конкурсному відборі.

Умови проведення вступних випробувань. Фахові вступні випробування проводяться в усній формі, у вигляді іспиту очно або дистанційно. Іспит в усній формі проводиться не менше, ніж двома членами комісії з кожним вступником, яких призначає голова фахової комісії згідно з розкладом у день іспиту. Під час складання іспиту очно члени комісії відмічають правильність відповідей в аркуші усної відповіді, який по закінченні іспиту підписується вступником та членами відповідної комісії. Складання іспиту у дистанційній формі відбувається із застосуванням платформ Zoom (Google Meet). Інформація про результати іспиту оголошується вступникові в день його проведення.

Змістовно-методичне забезпечення вступних випробувань здійснюють науково-педагогічні працівники профільних кафедр.

1. ВИМОГИ ДО РІВНЯ ПІДГОТОВКИ ВСТУПНИКІВ

До проходження фахового вступного випробування допускаються вступники, які виконали повністю навчальний план за освітнім ступенем бакалавра (магістра) або освітньо-кваліфікаційного рівня спеціаліста й отримали диплом за відповідною або іншою спеціальністю.

Вступник повинен знати:

- термінологію, що стосується основних понять за фахом;
- сучасні інформаційно-комунікаційні технології;
- сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
- основи програмування;
- основи законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;
- теорії, моделі та принципи управління доступом до інформаційних ресурсів;
- основи теорії систем управління інформаційною та/або кібербезпекою;
- основні принципи побудови деяких типів комп'ютерних мереж;
- основні різновиди шкідливого програмного забезпечення;
- основні відомості стосовно кібератак;

Вступник повинен вміти:

- вільно володіти термінологією за фахом;
- застосовувати інформаційно-комунікаційні технології при роботі за фахом;
- налагоджувати основні складові програмно-апаратного забезпечення;
- програмувати на сучасній мові високого рівня;
- аналізувати потенційні та реальні загрози інформації;
- здійснювати основний захист свого ПК від інформаційних загроз.

2. ЗМІСТ ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ У РОЗРІЗІ ДИСЦИПЛІН

Програма фахового вступного випробування для зарахування на навчання за ступенем освіти магістр за спеціальністю 125 Кібербезпека та захист інформації містить основні питання за наступними темами:

1. Принципова схема ЕОМ. Поняття інформації.

Принципова схема ЕОМ. Види класифікації ЕОМ. Принципова схема ЕОМ. Основи її роботи. Кодування інформації та її представлення в пристроях комп'ютера в двійковій системі обчислення.

Поняття інформація, дані. Класифікація інформації та її представлення в пристроях комп'ютера. Носій інформації. Інформаційний ресурс. Одиниці виміру даних. Форми подання інформації.

2. Найважливіші терміни, що використовуються в сучасних інформаційних технологіях та кібербезпеці.

Необхідність вивчення термінології. Найважливіші терміни, що відносяться до загальних питань ІТ. Загальні терміни, що відносяться до понять "Інформатика", "Internet" та "Microsoft Office ". Терміни стосовно апаратного та програмного забезпечення ІТ. Терміни стосовно інформаційної безпеки та кібербезпеки. Інші важливі терміни.

3. Програмне забезпечення ПК. Прикладне програмне забезпечення. Загальна характеристика основних складових.

Визначення та структура програмного забезпечення ПК, класифікація програмного забезпечення (ПЗ). Системне ПЗ. Сервісне ПЗ. Системи та засоби автоматизації програмування. Прикладне програмне забезпечення (ППЗ). Основні складові сучасного ППЗ. Назви та характеристики прикладних програм. Поняття інтегрованої системи. Приклади інтегрованих систем. Поняття операційної системи; класифікація операційних систем та їх характеристики; поняття файлу, каталогу; імена дисків. Загальна характеристика операційної системи Windows; структура операційної системи та її можливості.

4. Сутність інформаційних технологій й інформаційних систем.

Сутність інформаційних технологій й інформаційних систем. Інформаційний процес. Збір, обробка, збереження й передача інформації. Інформаційна технологія (ІТ). Автоматизована інформаційна технологія. Класифікаційні ознаки ІТ. Базові інформаційні технології. Представлення базової ІТ трьома рівнями: концептуальним, логічним і фізичним.

Канонічне поняття системи. Інформаційна система. Підсистема. Структура інформаційної системи. Забезпечення ІС. Автоматизована інформаційна система. Класифікація ІС. Масштабність. Сфера застосування. Сфера діяльності. Етапи розвитку інформаційних систем.

5. Системи управління базами даних (СУБД). СУБД MS Access.

Введення в бази даних: поняття «база даних (БД)», «концепція БД», «моделі даних». Поняття про системи управління базами даних (СУБД). Архітектура СУБД. Аналіз функціональних можливостей та порівняння різних СУБД. Етапи проектування структури бази даних. Інформаційно-логічна модель реляційних баз даних.

Призначення, загальна характеристика, особливості та можливості СУБД MS Access. Об'єкти баз даних MS Access. Запуск програми та вихід із неї. Створення та збереження нової бази даних. Графічний інтерфейс СУБД MS Access та структура вікна. Головне меню MS Access і панелі інструментів. Одержання довідкової інформації. Створення шаблонної бази даних у MS Access за допомогою Майстра.

Перегляд і редагування даних у полях таблиці. Виділення полів і записів. Копіювання, переміщення і вилучення даних у таблиці. Зміна ширини стовпців, параметрів шрифту, закріплення та тимчасове закриття окремих полів на екрані. Пошук і заміна даних. Фільтрація даних у таблиці. Побудова фільтрів за виділенням, складних та розширених фільтрів.

6. Мови програмування.

Поняття програми, програмування, мови програмування, машинного коду, алгоритму.

Поняття алгоритму та основні його властивості. Способи побудови алгоритмів. Аналітичні та графічні алгоритми. Поняття лінії потоку, типи символів для побудови графічних алгоритмів. Лінійні, розгалужені, циклічні обчислювальні процеси. Поняття циклу, параметру циклу, цикли з передумовою та післяумовою. Цикли з параметром. Вкладені циклічні процеси. Внутрішні та зовнішні цикли.

Тестування та налагодження програми, типи трансляторів та їх характеристики, покоління мов програмування, огляд сучасних мов програмування, мови програмування баз даних, мови програмування для Інтернету. Інтегровані системи програмування. Рейтинг мов програмування.

7. Основи програмування мовою Visual (Small) Basic. Підпрограми на Visual (Small) Basic. Різновіди Visual Basic.

Загальна характеристика мови Visual Basic та її основні властивості. Основні поняття Visual Basic. Структура головного вікна Visual Basic. Основні прийоми роботи в Visual Basic. Структура програми на мові Visual Basic. Типи даних та операції, що виконуються над даними у Visual Basic. Поняття масиву, індексу елементу масиву, вимірності масиву.

Файли, операції з файлами, режими доступу до файлу.

Підпрограми на Visual Basic. Призначення процедур та їх види. Опис процедур. Виклик процедури. Функції.

Різновидність Visual Basic для роботи з додатками Microsoft Office Visual Basic for Applications (VBA). Різновидність Visual Basic - мова Small Basic та її основні властивості.

8. Історія створення комп'ютерних мереж, їх основні компоненти.

Історія створення комп'ютерних мереж, їх основні компоненти. Типи комп'ютерних мереж. Локальні, регіональні та глобальні комп'ютерні мережі. Протоколи. Основні задачі, що розв'язуються за допомогою локальних комп'ютерних мереж. Протоколи в обчислювальних мережах. Засоби передачі даних у мережі. Характеристики процесу обміну даними в мережі (режим передачі, код передачі, тип синхронізації). Режими передачі даних (симплексний, напівдуплексний, дуплексний). Канали зв’язку в інформаційних мережах. Канали зв’язку на основі кабельного з’єднання. Бездротові канали зв'язку. Супутникові канали зв’язку.

9. Локальні комп'ютерні мережі, їхні типи, інтегровані складові ЛОМ. Основні технології передачі мережних даних. Технологія обробки економічної інформації в ЛОМ.

Клієнт. Сервер. Типи локальних мереж (однорангові, з виділеним сервером). Недоліки і переваги кожного типу. Коротка характеристика основних технологій передачі мережних даних. Розгляд основних інтегрованих складових ЛОМ. Технічні засоби. Мережні програмні засоби. Протоколи та сервіси. Топологія мереж, її види (кільцева, зіркоподібна, шинна). Технологія обробки різноманітної інформації в ЛОМ. Новітні технології зв'язку. Home PNA, RadioEthernet. Передача даних на основі радіосигналів. Мережі на основі електромереж. Бездротові мережі Bluetooth. Стандарт бездротового зв'язку Wi-Fi. Основні режими роботи Wi-Fi. Обладнання для налагодження Wi-Fi зв’язку. Принципи роботи з комплексним бізнес-документом в робочій групі.

10. Історія появи та розвитку Internet. Визначення Internet. Вузлові комп'ютери Internet. Основні сервіси Internet

Зародження глобальної інформаційної мережі Інтернет. Історія появи та становлення Internet. Internet - мережа мереж. Internet як інформаційний простір. Сьогодення та перспективи подальшого розвитку Internet. Сучасний стан Internet в Україні. Пошук інформації в Internet.

Вузлові комп'ютери Internet. Шлюзовий комп’ютер. Схема фрагменту мережі Internet. Сервіси відкладеного доступу (off-line) та інтерактивні сервіси (on-line). Електронна пошта (e-mail). Групи новин. Сервіс FTP. Термінальний режим. Всесвітня павутина (World Wide Web, WWW). Чат (IRC - Internet Relay Chat). Пошукова служба (ICQ). Internet-телефонія (IP-tel). Служба доменних імен (DNS). Система Internet–комерції (CIK).

11. Теоретичні основи Internet. Протоколи TCP/IP. Структура адрес Internet. Інтернет-технології в пошуку учбово-наукової інформації

Теоретичні основи Internet. Рівні взаємодії OSI. Протоколи комп'ютерних мереж. Протоколи TCP/IP. Протокол транспортного рівня (TCP, Transmission Control Protocol) Протокол IP-адресний (IP, Internet Protocol). Протокол зв'язку TCP/IP основа всесвітньої мережі Internet. Структура адрес Internet.

Коротка історія розвитку пошуку інформації в мережі Інтернет. Джерела інформації в мережі Інтернет. Опис основних різновидів джерел інформації. Методологія пошуку інформації в World Wide Web. Що необхідно взагалі для пошуку інформації в Інтернет? Повнота, вірогідність і швидкість пошуку. Планування процесу пошуку. Технологія пошуку інформації в Інтернет. Основні способи, що використовуються для пошуку в Інтернет. Технологія пошуку. Приклад пошуку інформації. Аналіз результатів пошуку.

12. Основи інформаційної безпеки.

Інформаційна безпека: основні підходи до визначення. Основні аспекти інформаційної безпеки. Об'єкти і суб'єкти інформаційної безпеки.

Етапи розвитку інформаційної безпеки.

Інформаційна безпека держави. Інформаційна безпека держави як одна зі складових національної безпеки держави. Об'єкти інформаційної безпеки держави. Модель інформаційної безпеки держави.

13. Види та властивості інформації як предмета захисту.

Види інформації з обмеженим доступом відповідно до законодавства України. Службова інформація. Державна таємниця. Комерційна таємниця. Професійна таємниця. Види професійних таємниць згідно із вітчизняним законодавством.

Персональні дані. Об'єкти захисту. Вимоги до обробки персональних даних.

14. Понятійний апарат кібербезпеки. нормативно-правова база у сфері кібербезпеки. Кіберпростір, Кібербезпека: Поняття і визначення. Кібертероризм.

Понятійний апарат інформаційної безпеки та кібербезпеки. Кіберпростір, кібербезпека: поняття і визначення. Три групи термінів теорії інформаційної безпеки. Взаємозв'язок інформаційного та кіберпросторів. Дійові особи кіберпростору та їхній вплив на інформаційну і кібербезпеку. Способи нанесення збитку інформаційній безпеці.

Інформаційно-телекомунікаційна система. Комп'ютерна система. Автоматизована система. Структура автоматизованої системи. Політика безпеки [інформації]. Конфіденційність. Цілісність. Доступність.

Загрози кібертероризму. Кібервійна.

Нормативно-правова база у сфері кібербезпеки. Закони України «Про інформацію», «Про науково-технічну інформацію», «Про основи національної безпеки України», «Про Державну службу спеціального зв’язку та захисту інформації України», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», «Про основні засади забезпечення кібербезпеки України», «Про державну таємницю», «Про захист персональних даних», «Про критичну інфраструктуру». Основні положення Стратегії кібербезпеки України та Стратегії інформаційної безпеки.

Кібербезпека в умовах розгортання четвертої промислової революції: виклики та можливості для України. Основи міжнародної співпраці з питань забезпечення кібербезпеки.

15. Складові забезпечення інформаційної безпеки та кібербезпеки. джерела загроз інформації.

Складові забезпечення інформаційної безпеки та кібербезпеки. Загальна схема забезпечення інформаційної безпеки. Проблеми розвитку теорії і практики забезпечення інформаційної безпеки та кібербезпеки.

Сутність потенційних та реальних загроз інформації. Два класи загроз: випадкові або ненавмисні, навмисні. Збої й відмови складних систем. Навмисно створювані загрози і їх поділ на групи.

Джерела виникнення загроз та шляхи їх реалізації. Логічний ланцюг взаємодії джерела загроз та вразливості. Шпигунство. Спеціальні технічні засоби негласного знімання інформації. Радіозакладки. Дистанційна відеорозвідка. Термін несанкціонований доступ до інформації (НСД). Системи розмежування доступу (СРД). Чотири класи шкідливих програм залежно від механізму дії.

Класифікація загроз інформації в комп’ютерній системі. Загрози, що обумовлені діями суб'єктів - антропогенні загрози; загрози, що є наслідком відмов та збоїв технічних засобів - техногенні загрози; загрози, викликані стихійними джерелами - природні загрози. Схема загроз комп’ютерній системі.

16. Управління доступом.

Огляд управління доступом. Принципи безпеки. Модель політики безпеки. Правила розмежування доступу. забезпечення доступності, цілісності й конфіденційності ресурсів інформаційного середовища й підтримуючої інфраструктури.

Ідентифікація, аутентифікація, авторизація та підзвітність. Базова схема ідентифікації та аутентифікації. Атаки змагання. Чотири кроки, які необхідно пройти суб'єкту для отримання доступу до об'єкта. Вимоги до ідентифікації. Класифікація методів аутентифікації.

Біометрична ідентифікація й аутентифікація користувача. Біометрія. Основні переваги біометричних методів ідентифікації й аутентифікації

користувача в порівнянні з традиційними. Основні відомі системи біометричної ідентифікації.

Парольні системи аутентифікації. Класифікація парольних систем аутентифікації. Основні загрози безпеки парольних систем. Рекомендації щодо практичної реалізації парольних систем.

17. Інциденти у сфері високих технологій: характерні ознаки та проблемні аспекти.

Інциденти у сфері високих технологій. Комп'ютерні злочини. Способи, що їх використовують зловмисники для здійснення нападу. Загальна схема виникнення інцидентів у сфері високих технологій. Класифікація кібернетичних втручань і загроз. Класифікація джерел інцидентів, а також способів, об'єктів та результатів їхнього впливу.

Модель порушника інформаційної безпеки. Внутрішні порушники (персонал підприємства) та зовнішні порушники (сторонні особи). Класифікація порушників. Хакерство. Види хакерів.

Базові схеми атак та організація каналів витоку інформації. Кібератака. Класифікація кібератак. DoS та DDoS атака. Аналізатори протоколів (sniffers). Mailbombing. Man-in-the-Middle. Узагальнена класифікації кібератак.

Характеристика APT-кібератак як основної форми боротьби в кіберпросторі. APT-кібератака. Приклади APT-кібератак. Життєвий цикл APT-кібератаки. Основні засоби проникнення для APT-кібератак.

18. Шкідливі програми.

Класифікація шкідливого програмного забезпечення. Діаграма зростання кількості шкідливого програмного забезпечення. Класифікація шкідливого програмного забезпечення за механізмами розповсюдження. Класифікація залежно від механізму дії.

Умови існування шкідливих програм та загальні відомості про комп'ютерні віруси. Комп'ютерний вірус. Стелс-вірус. Поліморфні віруси.

Характеристика окремих шкідливих програм. Логічні бомби. Троянські програми. Основні дії, які можуть виконувати різні види троянських програм. Backdoor (Чорний вхід). Trojan-PSW. Trojan-Clicker. Trojan-Downloader. Trojan-Dropper. Trojan-Spy. Rootkit.

Характеристика окремих шкідливих програм. Класичні комп'ютерні віруси. Файлові віруси. Завантажувальні віруси. Макровіруси.

Характеристика окремих шкідливих програм. Бактерії. Мережеві хробаки. Розмноження хробаків.

Характеристика окремих шкідливих програм. Хакерські утиліти та інші шкідливі програми. Tools (HackTool). Exploit. Flooder. Конструктори вірусів і троянських програм. Adware.

19. Антивірусний Захист. Боротьба зі спамом.

Вплив шкідливих програм на комп'ютерну систему. Основні ранні ознаки зараження комп'ютера вірусом. Ознаки активної фази вірусу.

Захист від вірусів. Деякі відомості про антивірусні програми. Загальні засоби захисту. Перелік спеціальних засобів, що допомагають запобігти зараженню комп'ютера. Загальні відомості про антивірусні програми.

Персональний файрвол. Типова схема використання брандмауера в ІТС з підключенням до Інтернету. Класи міжмережевих екранів.

Короткий огляд сучасних антивірусних програм. AVG Internet Security для комплексного захисту ПК. Боротьба зі спамом.

3. КРИТЕРІЇ ОЦІНЮВАННЯ ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

Результати фахового вступного випробування обчислюються (за шкалою від 100 до 200):

Р=П1+П2+П3,

де П1 – оцінка за перше питання (за школою 0-80).

П2 – оцінка за друге питання (за шкалою 0-60).

П3 – оцінка за третє питання (за шкалою 0-60).

Результати фахового вступного випробування оцінюються за шкалою від 100 до 200 балів з урахування рівнів підготовки:

У разі отримання результату фахового вступного випробування від 0 до 99 іспит вважається таким, який не складено і вступник до участі у конкурсному випробуванні не допускається.

Відповідність рейтингових оцінок у балах оцінкам за національною шкалою

Оцінка в балах		**Пояснення**	
100-200	**180-200**	**Відмінно** (відмінне виконання лише з незначною кількістю помилок)	Вступне випробування складено
	150-179	**Добре** (в загальному вірне виконання з певною кількістю суттєвих помилок)	
	100-149	**Задовільно** (непогано, але зі значною кількістю недоліків та задовольняє мінімальним критеріям)	
0-99		**Вступне випробування не складено**	

Оцінювання рівня підготовки, тобто знань і умінь вступника, відбувається на підставі наступних критеріїв:

1. Правильність відповіді;
2. Ступінь усвідомлення програмного матеріалу;
3. Вміння користуватись засвоєним матеріалом.

4. ПОРЯДОК ПРОВЕДЕННЯ ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

Фахове вступне випробування проводиться у формі усного іспиту очно або дистанційно. Для проведення вступного випробування формуються окремі групи вступників в порядку надходження (реєстрації) документів. Список допущених до вступного випробування ухвалюється рішенням приймальної (відбіркової) комісії, про що складається відповідний протокол.

Для проведення вступного випробування головами фахових атестаційних комісій попередньо готуються екзаменаційні білети відповідно до «Програми фахового вступного випробування». Програма фахового вступного випробування оприлюднюється на веб-сайті Університету.

Фахове вступне випробування проводиться у строки, передбачені Правилами прийому до ДБТУ.

На іспиті вступник повинен пред’явити, який посвідчує особу (паспорт громадянина України у вигляді книжечки, ID-картка), при пред'явленні якого він завдання (екзаменаційний білет). Екзаменаційний білет містить завдання з тем, вказаних у програмі фахового вступного випробування. Тривалість іспиту – до 2 астрономічних годин. Користуватися при підготовці друкованими, електронними або іншими інформаційними засобами забороняється.

Результати випробування оцінюються за шкалою від 100 до 200 балів за правилами, вказаними в розділі «Критерії оцінювання фахового вступного випробування». Рівень знань вступника за результатами іспиту заноситься також до екзаменаційної відомості і підтверджується підписами голови та членів комісії. Відомість оформляється і передається до приймальної комісії в день складання фахового вступного випробування.

Розробив к.т.н, доцент кафедри інформаційних технологій, кібернетики та захисту інформації Чалий І. В.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Кащеев Л. Б., Коваленко С.В., Коваленко С.Н. Інформатика. Основи візуального програмування: Навч. посібник. — Харків: Веста, 2011.— 192 с.
2. Анісімов А.В. Інформаційні системи та бази даних: Навчальний посібник для студентів факультету комп'ютерних наук та кібернетики. / Анісімов А.В., Кулябко П.П. − Київ. – 2017. – 110 с.
3. Антоненко В. М. Сучасні інформаційні системи і технології: управління знаннями : навч. посібник / В. М. Антоненко, С. Д. Мамченко, Ю. В. Рогушина. – Ірпінь : Нац. університет ДПС України, 2016. – 212 с.
4. Павлиш В. А. Основи інформаційних технологій і систем: Навчальний посібник. / Павлиш В. А., Гліненко Л. К. - Львів: Видавництво Львівської політехніки, 2013. − 500 с.
5. Інформатика. Комп'ютерна техніка. Комп'ютерні технології [Текст] : підручник для студ. вищ. навч. закл.: затв. МОНУ / В.А. Баженов, П. С. Венгерський, В. С. Гарвона [та ін.]. - 3-тє вид. - К. : Каравела, 2011. - 592 с.
6. Іванов В. Г. Основи інформатики та обчислювальної техніки : підручник / В. Г. Іванов, В. В. Карасюк, М. В Гвозденко. – Х. : Право, 2012. – 312 с.
7. Основи Інтернет-технологій : навч. посіб. / під ред. О.В. Карпухіна. – Х. : Компанія СМІТ, 2010. – 394 с.
8. Дибкова Л. М. Інформатика і комп'ютерна техніка (3-тє видання, доповнене). Навчальний посібник. «Академвидав», – К. 2011. – 464 с. (Альма-матер).
9. Базилевич В. М. Комп'ютерні мережі. Протоколи, технології, обладнання : навч. посіб. для студ. спец. 125 «Кібербезпека» / В.М. Базилевич, Д. Б. Мехед, Ю. М. Ткач. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 108 с. : іл.
10. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В.Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
11. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП Україна», 2015. – 449 с.
12. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок, Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.
13. Гладун А.Я. Англо-український словник термінів з інформаційних технологій та кібербезпеки / А.Я. Гладун, О.О. Пучков, І.Ю. Субач, К.О. Хала. – К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018. – 380 с.

14. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп’ютерних мережах. – К., 2013. – 435 с., іл.160.

15. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.

ДОДАТОК

Зразок «Екзаменаційний білет»

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Державний біотехнологічний університет

	ЗАТВЕРДЖУЮ Голова приймальної комісії В.о. ректора ДБТУ _____ А.І.Кудряшов «_____»_____2024 р.

Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека та захист інформації

ЕКЗАМЕНАЦІЙНИЙ БІЛЕТ № 1
фахового вступного іспиту

1. Інформаційна безпека: основні підходи до визначення.

2. Поняття інформація, дані. Кодування інформації та її представлення в пристроях комп'ютера.

3. Розтлумачте значення термінів " DDoS-атака " та " Керування доступом"

Розробив член фахової атестаційної комісії к.т.н., доцент кафедри інформаційних технологій, кібернетики та захисту інформації Чалий І. В.