МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

ЗАТВЕРДЖУЮ
Ректор_____ О.О.Новомлинець
«____» _____ 2023 р.

ПРОГРАМА

фахового вступного випробування для вступу
на навчання за освітньо-професійною програмою
підготовки **магістра** на основі рівня **бакалавр**
спеціальності 125 – Кібербезпека
з галузі знань 12 – Інформаційні технології

Затверджено на засіданні
кафедри кібербезпеки та
математичного моделювання
Протокол №5 від 18.04 2023 р.

Чернігів 2023

ВСТУП

Фахове вступне випробування – форма вступного випробування для вступу на основі здобутого ступеня бакалавра або освітньо-кваліфікаційного рівня спеціаліста, яка передбачає перевірку здатності до опанування освітньої програми другого (магістерського) рівня вищої освіти на основі здобутих раніше компетентностей. Результати фахового вступного випробування зараховуються для конкурсного відбору осіб, які на основі ступеня бакалавра або освітньо-кваліфікаційного рівня спеціаліста вступають на навчання для здобуття ступеня магістра.

Програма фахового вступного випробування для вступу на навчання за освітньо-професійною програмою підготовки магістра спеціальності 125 – Кібербезпека з галузі знань 12 – Інформаційні технології складена на основі освітньо-професійної програми підготовки бакалаврів з кібербезпеки за спеціальністю 125 – Кібербезпека. Програма розроблена згідно з навчальними програмами навчальних дисциплін спеціальності 125 – Кібербезпека та у відповідності із освітньо-кваліфікаційною характеристикою бакалавра з кібербезпеки за спеціальністю 125 - Кібербезпека.

Фахове вступне випробування з фундаментальної та загально-інженерної підготовки на спеціальність 125 - Кібербезпека приймається екзаменаційною комісією. Фахове вступне випробування здійснюється в письмовій формі / дистанційно.

Вступні випробування охоплюють фахові предмети, які передбачені навчальними планами освітньо-кваліфікаційного рівня бакалавр за спеціальністю 125 - Кібербезпека та складаються із тестових завдань.

МЕТА ТА ЗАВДАННЯ ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

Основною метою проведення фахового вступного випробування з фундаментальної та загально-інженерної підготовки на спеціальність 125 – Кібербезпека є визначення рівня фундаментальної та професійної підготовки абітурієнтів.

Завдання фахового вступного випробування:

- перевірка відповідності знань, умінь та навичок вступників програмовим вимогам;
- виявлення та оцінка рівня навчальних досягнень слухачів;
- оцінка ступеня підготовленості вступників до навчання за спеціальністю 125 - Кібербезпека для здобуття ступеня магістра.

ПОРЯДОК ПРОВЕДЕННЯ ІСПИТУ

Фахове вступне випробування проводиться в письмовій формі. Необхідні для відповіді на питання і розв’язку задачі записи виконуються на папері зі штампом інституту. На кожному листі абітурієнт вказує своє прізвище, ініціали, групу, номер білета. Листи нумеруються, заповнюються з обох сторін. Питання формуються на основі даної програми, яку абітурієнти отримують завчасно.

Основою програми фахового вступного випробування є дисципліни навчального плану спеціальності 125 - Кібербезпека:

- Основи технічного захисту інформації;
- Основи криптографічного захисту інформації;
- Безпека інформації в інформаційно-телекомунікаційних системах;
- Теорія ризиків;
- Комплексні системи захисту інформації.
- Бази даних;
- Операційні системи;
- Архітектура обчислювальних систем;
- Комп'ютерні мережі;
- Основи програмування.

ЗМІСТ ПРОГРАМИ ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

На фахове вступне випробування виноситься матеріал за наступними темами відповідних навчальних дисциплін:

Основи технічного захисту інформації

Види, джерела та носії інформації, що підлягає захисту. Класифікація і структура технічних каналів витоку інформації. Радіо- та електротехнічні канали витоку інформації. Акустичні та віброакустичні канали витоку інформації. Захист від акустичних та віброакустичних каналів витоку інформації. Електричні канали витоку інформації. Захист від електричних каналів витоку інформації. Візуально-оптичні та матеріально-предметні канали витоку інформації. Захист від візуально-оптичних та матеріально-предметних каналів витоку інформації. Канали витоку інформації при експлуатації обчислювальних засобів. Спрямовані мікрофони та їх можливості. Екранування, звукоізоляція та звукопоглинання приміщень. Класифікація закладних пристроїв, їх основні характеристики та застосування. Способи та засоби боротьби із закладними пристроями. Оцінка рівня побічних електромагнітних випромінювань. Методи і засоби технічного захисту. Засоби виявлення каналів витоку інформації. Керівні документи з ТЗІ. Методика розробки системи ТЗІ. Порядок розробки заходів ТЗІ. Основи захисту ВзОД. Типові відомості, які потрібно захищати. Канали витоку предметної форми інформації. Технічні розвідки, їх можливості та застосування. Задачі і способи охорони об'єктів. Принципи створення системи охорони. Засоби охорони та їх характеристики. Принципи дії технічних засобів розвідки. Завдання технічного захисту інформації. Структура та функціонування системи ТЗІ в Україні. Теоретичні та практичні аспекти перекриття можливих технічних каналів витоку інформації та несанкціонованого доступу до інформації. Державні органи системи ТЗІ. Організація контролю ефективності технічного захисту інформації. Способи контролю.

Основи криптографічного захисту інформації

Алгоритм шифрування RSA. Алгоритм шифрування. Обмін конфіденційними повідомленнями за допомогою симетричної криптосистеми. Комбінована криптосистема. Алгоритм цифрового підпису DSA. Забезпечення

практичної неможливості підбору пароля зловмисником. Цифровий підпис повідомлення. Розшифрування повідомлення за допомогою асиметричного криптоалгоритма. Формування коду автентифікації повідомлення. Довжина ключа (в бітах) та кількість раундів криптоалгоритма DES. Довжина ключа (в бітах) та кількість раундів криптоалгоритма ГОСТ 21847-89. Протокол відкритого ключового обміну Діффі-Хеллмана. Шифруюча послідовность, яка генерується синхронним потоковим криптоалгоритмом. Методи криптографії. Основна частина цифрового сертифіката. Протокол Фейге-Фіата-Шаміра. Стійкість криптографічних хеш-функцій до криптоаналізу на основі парадокса дня народження. Схема шифрування Віженера. Умовии створення абсолютно-стійкої криптосистеми. Криптоперетворення на і-тому раунді криптоалгоритма, що реалізований за схемою Фейстеля.

Безпека інформації в інформаційно-телекомунікаційних системах

Кадри «ARP-запит» і «ARP-відповідь». Смуга пропускання і пропускна здатність. Розбиття мережі класу С використовуючи технологію CIDR. Рівні моделі OSI. Логічні топології. Метод доступу «за опитуванням арбітра». Логічні топології. Метод доступу CSMA / CD. Фізична топологія технології Fast Ethernet. Комутатори (switch) для передачі кадрів даних. Смуга пропускання кабелю «вита пара» категорії . Логічна топологія «Зірка». Рівні моделі OSI. Вікно передачі протоколу TCP. Пакети «DNS-запит» і «DNS-відповідь». Повторна передача в протоколі TCP. Відправлений пакет. Повторна передача в протоколі TCP. Вікно передачі. Протокол RIP. Протокол UDP. Сеансовий рівень моделі OSI. Спектр. Фізична топологія «Шина».

Сучасний стан безпеки інформації та методи забезпечення недоступності даних. Протоколи та засоби ідентифікації, авторизації, автентифікації та обліку мережевих ресурсів. Системи захисту обчислювальних мереж. Моделі безпеки комп’ютерних систем. Протоколи безпеки.

Теорія ризиків

Моделювання інформаційних систем в умовах ризику та невизначеності. Формування та формалізація поняття ризику. Ризики, кризи та катастрофи. Методи аналізу та оцінки ризиків. Методи оцінки інформаційних ризиків за міжнародними стандартами. Числові характеристики ризику процесу функціонування інформаційної системи у відносному вираженні. Методики аналізу та оцінки ризиків. Управління інформаційними ризиками. Ризик-менеджмент в управлінні інформаційною безпекою. Аудит інформаційної безпеки.

Комплексні системи захисту інформації

Сутність та задачі комплексної системи захисту інформації. Основні підходи до створення комплексної системи захисту інформації. Поняття комплексної системи захисту інформації. Призначення комплексної системи захисту інформації. Основні стратегії захисту інформації. Розробка політики безпеки. Загальні положення про комплексні системи захисту інформації. Порядок здійснення захисту інформації на об’єктах інформаційної діяльності. Захист

інформації від витоку технічними каналами. Захист інформації під час використання засобів копіювально-розмножувальної техніки.

Бази даних

Бази даних і банки даних. Трирівнева архітектура баз даних. Розподіл обов'язків в системах з базами даних. Основні поняття реляційної моделі даних: відношення, кортежі, атрибути, домени і т. п. Ключі та їх призначення. Нормалізація реляційної моделі даних. Засоби пошуку даних. Запити. Засоби маніпулювання даними. Мова DML. Операції над схемою бази даних.Мова DDL. Індекси. Транзакції.

Операційні системи

Місце операційної системі в програмному забезпеченні ПК. Завдання ОС. Програми в пам'яті. Ядро ОС. Апаратна архітектура (Фон Неймана, Гарвардська, Стекові машини, Lisp Mashine, FPGA та інші). Віртуальна машина. POSIX. Робота ОС з апаратною частиною. Драйвери пристроїв. Час в комп'ютері. Переривання (апаратні, програмні). Схема обробки переривань. Контектси. Домени безпеки. Завантаження ОС. Прошивка. Бінарний інтерфейс додатків(ABI). Асемблер. Адресація пам'яті. Регістри процесора. Стек. Угоди про виклики. Системні виклики. Апаратне управління пам'яттю. Віртуальна пам'ять. Сторінкова організація пам'яті. Сегментна організація пам'яті. Моделі сегментації пам'яті. Програма в пам'яті. Статична пам'ять програми. Динамічна пам'ять програми. Процес. Види процесів. Життєвий цикл процесу. Породження процесу. Завершення процесу. Робота процесу. Планування процесів. Алгоритми планування процесів. Міжпроцесорна взаємодія. Проблема синхронізації. Класичні задачі синхронізації. Алгоритми програмної синхронізації. Апаратні інструкції синхронізації. Системні механізми синхронізації. Спінлок. Семафори. Інтерфейс синхронізації. Проблеми синхронізації. Неблокуюча синхронізація. Файлова система. Файл. Директорія. Схеми розміщення файлів. Оптимізація роботи ФС. Загальні принципи безпеки. Механізми роботи системи безпеки. Реалізація системи безпеки. Основні варіації Unix'ів. GNU/Linux. Ключові рішення Unix. Підтримка GUI в Unix. Принципи розробки під Unix. Критика Unix.Windows NT. Ключові рішення Windows.

Архітектура обчислювальних систем

Основи організації обчислювальних процесів в персональних комп'ютерах та комп'ютерних системах. Поняття обчислювальної системи та обчислювального комплексу. Структура ЕОМ та логічна структура ЕОМ. Архітектура ЕОМ. Архітектура ЕОМ по фон Нейману. Основні принципи фон Неймана. Поняття команди в ЕОМ. Гарвардська архітектура. Класифікація ЕОМ по Фліну. Типи потоку команд. Типи потоку данних. Архітектури ОКОД , ОКМД , МКОД , МКМД. Поняття та загальна характеристика BIOS. Системні плати. Південний та північний міст. Інтерфейси, слоти та роз'єми материнської плати. Порти материнської плати. Комп'ютерні шини. Особливості архітектури системної шини. Поняття головного і другорядного пристрою на шині. Мікропроцесори. Класифікація ЦПП різних архітектур. Види сучасних процесорів, а також особливості їх побудови та функціонування. Процесори з MISC, RISC, CISC та VLIW архітектурою. Покоління процесорів. Багатоядерні процесори. Структурна

схема мікропроцесора. Будова і принципи роботи мікропроцесора. Архітектура системи команд процесора. Робочий цикл процесора. Регістри процесора. Захищений режим процесора. Робота в захищеному режимі. Обробка переривань у захищеному режимі процесора. Означення запам'ятовуючого пристрою. Класифікація ЗП. Оперативна пам'ять. Фізична та віртуальна пам'ять. Основні характеристики пам'яті. Загальні поняття про кешування даних та команд. Основні характеристики кеш. Чисто асоціативний кеш та приклад його реалізації. Кеш з прямим відображенням та схема його побудови. Кеш з множинним доступом. Жорсткий диск. Характеристики жорсткого диска. Флеш-пам'ять. Класифікація систем комп'ютерів. Класифікація та архітектурні особливості суперкомп'ютерів. Класифікація та архітектурні особливості нейрокомп'ютерів. Класифікація та архітектурні особливості трансп'ютерів. Класифікація та архітектурні особливості кластерних комп'ютерів.Мультипроцесорні комп'ютери. Багатомашинні системи. Обчислювальні мережі. Хмарні технології. Грід-системи.

Комп'ютерні мережі

Еволюція комп'ютерних мереж. Принципи побудови комп'ютерних мереж. Узагальнена задача комутації. Комутація каналів і комутація пакетів. Принципи розділення середовища передачі даних. Декомпозиція задачі мережної взаємодії. Модель OSI. Стандартизація мереж. Класифікація та характеристики ліній зв'язку. Модуляція і методи кодування. Мультиплексування і комутація. Безпровідне середовище передавання. Стандартна топологія і розділюване середовище. Стек протоколів локальних мереж. Рівні MAC та LLC. Структура стандартів IEEE 802.x. Формати кадрів та специфікації фізичного середовища Ethernet Загальна характеристика технології Ethernet. MAC-адреси, доступ до середовища і передавання даних. Виникнення колізії. Типи кадрів. Використання різних типів кадрів Ethernet. Стандарти 10Base та волоконно-оптична мережа Ethernet. Технології Fast Ethernet та Gigabit Ethernet, Token Ring та FDDI. Фізичний рівень технології Fast Ethernet. Фізичний рівень технології Token Ring. Типи IP-адрес, доменні імена. Формат IP-адреси, класи IP-адрес. Використання масок під час IP-адресації. Порядок призначення IP-адрес. Формат IP-пакета. Схема IP-маршрутизації. Маршрутизація з використанням масок. Фрагментація IP-пакетів. Призначення і характеристика протоколу ICMP, формат ICMP-пакета. Типи ICMP-повідомлень. Протокол UDP. Формат TCP-сегмента. Логічні з'єднання, порядкові номери та номери підтвердження. Управління вікном прийому. Система DNS, схема роботи DNS. Режими DHCP, алгоритм динамічного призначення адрес. Протокол HTTP. Принципи роботи FTP, FTP-сервер та FTP-клієнт. Протокол SMTP. Ключові команди протоколу SMTP. Організація доступу до поштової скриньки користувача за допомогою протоколу POP3.

Основи програмування

Алгоритми. Змінні. Цикли. Умови. Мова програмування Scratch. Мови C та C++. Ввід та вивід даних. Робота з бібліотеками. Робота з рядками. Функції. Шифрування даних. Сортування та пошук. Робота з текстом в C та C++. Створення багатофайлових проектів. Графічний інтерфейс користувача (GUI).

Особливості створення програмних проектів з GUI. Обробка графічних файлів в C. Зміна розміру зображення та масштабування. Структури даних. Веб-програмування. Однозв’язні списки та хеш-таблиці, префіксні дерева. Робота з текстом в C. Клієнт-серверна модель взаємодії. Мови програмування PHP, JavaScript + HTML/CSS. Створення веб-проектів. Технології Ajax, JSON. Фреймворки.

СТРУКТУРА ЕКЗАМЕНАЦІЙНОГО БІЛЕТА

Завдання для вступного фахового випробування для здобуття освітньо-кваліфікаційного рівня «магістр» на основі освітньо-кваліфікаційного рівня «бакалавр» спеціальності «Кібербезпека» включає: − номер білету; − 20 тестових завдань однакового рівня складності із різними можливими варіантами відповіді (по 5 балів кожне); − шкала оцінювання за 100 бальною шкалою (від 0 до 100 балів).

КРИТЕРІЇ ОЦІНЮВАННЯ ЗНАНЬ АБІТУРІЄНТІВ

За результатами вступних випробувань проводиться оцінка рівня фахових знань за наступними критеріями: кожна правильна відповідь – 5 балів

Загальна кількість балів (максимум 100 балів) визначається шляхом підсумовування балів за виконання окремих тестових завдань.

ЛІТЕРАТУРА

1. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. [Електронний ресурс] / [КорченкоО.Г., Гнатюк С.О., КазмірчукС.В. та ін.]. –К.: Центр навч.-наук. і наук.-пр. видань НАСБ України, 2014. – 190с. – Режим доступу: http://193.178.34.24/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf
2. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. [Електронний ресурс] / [КорченкоО.Г., Гнатюк С.О., КазмірчукС.В. та ін.]. –К.: Центр навч.-наук. та наук.- пр.видань НАСБ України, 2014. – 190 с. – Режим доступу: http://193.178.34.24/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf
3. Белов Е. Б. Основы информационной безопасности : учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М. : Горячая линия-Телеком. 2006. – 544 с., ил.
4. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.
5. Гайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Гайворонський, О.М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с.
6. Дмитриев А. А. Внутренний аудит системы менеджмента информационной безопасности по требованиям ISO/IEC 27001. один из вариантов реализации процесса. Das Management. 2011. № 2. С. 58-64.
7. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
8. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.
9. ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення".
10. Завгородний В. И. Комплексная система защиты в компьютерных системах : Учебное пособие. - М. : Логос; ПБОЮЛ Н. А. Егоров, 2001. – 264 с.

11. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

12. Каторин Ю.Ф. Защита информации техническими средствами: учеб. пособие / Ю.Ф. Каторин, А.В. Разумовский, А.И. Спивак. – СПб: НИУ ИТМО, 2012. – 416 с.

13. Коженевський С.Р. Термінологічний довідник з питань захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков. – К.: ДУІКТ, 2007. – 382 с.

14. Комплексні системи захисту інформації. Проектування, впровадження, супровід / В. Гребенніков. - М.: Издательские решения, 2018. - 303 с.

15. Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 від 08.10.1997.

16. Корченко А., Архипов А., Казмирчук С. Анализ и оценивание рисков информационной безопасности: монография. Киев: ООО «Лазурит-Полиграф», 2013. 275 с.

17. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 510 с.

18. Курило А. П. Аудит информационной безопасности. / [Курило А. П., Зуфиров С. Л., Голованов В. Б. и др.]. – М. : Издательская группа "БДЦ-пресс", 2006. – 304 с.

19. Ленков С. В. Методы и средства защиты информации. В 2-х томах / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. Т.II. Информационная безопасность. – К. : Арий, 2008. – 344 с.

20. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

21. НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі".

22. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.

23. НД ТЗІ 2.7.- 001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.

24. НД ТЗІ 2.7-011-2012 "Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв".

25. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Перед проектні роботи.

26. НД ТЗІ 3.6.-001-2000. Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів механічного захисту інформації від несанкціонованого доступу.

27. НД ТЗІ 3.7.- 002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова).

28. НД ТЗІ 4.7.- 002-2001. Визначення захищеності мовної інформації від витоку акустичним і віброакустичним каналами. Методичні вказівки.

29. Порядок проведення робіт із сертифікації засобів забезпечення технічного захисту інформації загального призначення.

30. Проектування комплексних систем захисту інформації : методичні вказівки, завдання на контрольну та курсову роботи / Уклад. : В. С. Орленко, В. О. Хорошко, Д. В. Чирков. – К. : ДУІКТ, 2005. – 14 с.

31. 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.

32. 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.

33. Руководство по управлению рисками безопасности / Группа разработки решений Майкрософт по безопасности и соответствию, регулятивным нормам; Центр Microsoft security center of excellence, TechNet, Редмонд, США: Корпорация Майкрософт, 2006. URL: http://technet.microsoft.com/ru-ru/library/cc163143.aspx (дата обращения: 29.12.2011].

34. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с.

35. Столлингс В. Криптография и защита сетей. Принципы и практика. - К.: «Вильяме», 2001.-669 с.

36. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.

37. Торокин А.А. Инженерно-техническая защита информации : учеб. пособие для студентов, обучающихся по спеціальностям в обл. информационной безопасности / А.А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.

38. Хорошко В. А. Методы и средства зашиты информации / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с.

39. Шнайер Б. Прикладная криптография: протоколы, алгоритмы, исходные тексты на языке Си. - М.: "Триумф". 2002. - 815 с.

40. «Information technology. Security techniques. Code of practice for information security controls», ISO/IEC 27002:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013. P. 80.

41. «Information technology. Security techniques. Information security management systems implementation guidance», ISO/IEC 27003:2017, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2017. P. 45.

42. «Risk analysis based on IT-Grundschutz», BSI-Standard 100-3, Boon: Bundesamt für Sicherheit in der Informationstechnik, 2008, p. 23.

43. Carla Schroder. Linux Networking Cookbook. M.: O'Reilly Media, 2007.

44. Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley. UNIX and Linux System Administration Handbook (4th Edition). M.: Prentice Hall, 2010.

45. Morgan Guaranty Trust Company Market Risk Research/ New York February 1995 Jacques Longerstaey (1-212) 648-4936 – p. 45.

46. National Vulnerability Database. National Institute of Standards and Technology. Gaithersburg, 2016. URL: https://nvd.nist.gov/home.cfm

47. Tony Bautts, Terry Dawson, Gregor N. Purdy. Linux Network Administrator's Guide. M.: O'Reilly Media, 2005.

Завідувач кафедри кібербезпеки
та математичного моделювання _____ д.п.н., доц. Ткач Ю.М.