МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
ННІ електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

ЗАТВЕРДЖУЮ
Ректор

_____ О. Новомлинець

«__» _____ 2025 р.

ПРОГРАМА

фахового іспиту за другим (магістерським) рівнем освіти
за спеціальністю F5 «Кібербезпека та захист інформації»
за освітньо-професійною програмою «Кібербезпека»

Розглянуто
на засіданні кафедри КБтаММ
протокол № 4 від 22.04.2025

Чернігів – 2025

ЗМІСТ

МЕТА ВСТУПНОГО ФАХОВОГО ІСПИТУ

Основною метою проведення фахового вступного випробування з фундаментальної та загально-інженерної підготовки на спеціальність F5 – Кібербезпека та захист інформації 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 F5 - Кібербезпека та захист інформації для здобуття ступеня магістра.

ХАРАКТЕРИСТИКА ЗМІСТУ ПРОГРАМИ (ОПИС ОСНОВНИХ РОЗДІЛІВ ТА ЇХ КОРОТКИЙ ЗМІСТ)

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

Системи 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 комп’ютерних 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.

Технології 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.

ВИМОГИ ДО ЗДІБНОСТЕЙ І ПІДГОТОВЛЕНОСТІ АБІТУРІЄНТІВ/ВСТУПНИКІВ

Згідно зі стандартом спеціальності F5 «Кібербезпека та захист інформації» рівня підготовки бакалавр вимоги до підготовки абітурієнтів наступні:

- здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки;
- здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки;
- здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах;
- здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;
- здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження;
- здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.);
- здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності;
- здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та

інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки;

- використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
- критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
- діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;
- впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
- виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
- виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах;
- розробляти моделі загроз та порушника
- аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
- використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
- реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
- забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних

інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;

- використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
- застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
- вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
- вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
- реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
- впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
- вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
- аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-

телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;

- здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
- здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
- застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
- вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
- вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
- вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;
- виявляти небезпечні сигнали технічних засобів;
- вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;
- інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик

інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;

- проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
- інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
- забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
- впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
- вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;
- застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
- здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
- вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;

- забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);
- підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;
- вирішувати задачі аналізу програмного коду на наявність можливих загроз.

ПОРЯДОК ПРОВЕДЕННЯ ФАХОВОГО 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 наступні розділи теоретичної та практичної підготовки фахівців спеціальності F5 – Кібербезпека та захист інформації:

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

Структура екзаменаційного білета

Завдання для вступного фахового випробування для здобуття освітньо-кваліфікаційного рівня «магістр» на основі освітньо-кваліфікаційного рівня «бакалавр» спеціальності «Кібербезпека та захист інформації» включає:

− номер білету;

− 40 тестових завдань різного рівня складності із різними можливими варіантами відповіді (по 2 та 3 балів кожне в залежності від складності);

− шкала оцінювання за 100 бальною шкалою (від 0 до 100 балів).

КРИТЕРІЇ ОЦІНЮВАННЯ ФАХОВОГО ІСПИТУ

За результатами вступних випробувань проводиться оцінка рівня фахових знань за наступними критеріями: кожна правильна відповідь – 2 чи 3 балів в залежності від рівня складності питання.

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

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. [Електронний ресурс] / [Корченко О.Г., Гнатюк С.О., Казмірчук С.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. 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.

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

4. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

5. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

6. ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення".

7. 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.

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

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

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

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

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

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

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

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

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

17. 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.

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

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

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

21. 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.

22. 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.

23. 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.

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

25. 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.

26. «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.

27. «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.

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

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

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

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

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

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

34. Про вищу освіту. - Закон України від 01.07.2014р. № 1556-VII // ВВРУ від 19.09.2014р., № 37-38, стор. 2716, стаття 2004. URL: https://zakon.rada.gov.ua/laws/show/1556-18

35. Про освіту. - Закон України від 5 вересня 2017р. № 2145-VIII // ВВРУ від 29.09.2017р., №38-39, стор. 5, стаття 380. URL: https://zakon.rada.gov.ua/laws/show/2145-19

36. Національний класифікатор України: «Класифікатор професій» ДК 003:2010 (Редакція від 25.10.2021). URL: http://zakon.rada.gov.ua/rada/show/va327609-10

37. Національна рамка кваліфікацій. - Постанова КМУ від 23 листопада 2011 р. № 1341 // ОВУ від 06.01.2012р., № 101, стор. 15, ст. 3700, код акта 59774/2011. URL: https://zakon.rada.gov.ua/laws/show/1341-2011-п

38. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти. - Постанова КМУ від 29 квітня 2015р. № 266 // ОВУ від 22.05.2015р., №38, стор. 194, ст. 1147, код акта 76797/2015. URL: https://zakon.rada.gov.ua/laws/show/266-2015-п

39. Ліцензійні умови провадження освітньої діяльності. Постанова КМУ від 30 грудня 2015р. № 1187 // ОВУ від 02.02.2016р., № 7, стор. 23, ст. 345, код акта 80480/2016. URL: https://zakon.rada.gov.ua/laws/show/1187-2015-п

40. Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти. URL: https://naqa.gov.ua/wp-content/uploads/2019/07/Додаток-1.-Стандарти-і-рекомендації-щодо-забезпечення-якості-в-Європейському-просторі-вищої-освіти.pdf

41. Методичні рекомендації щодо розроблення стандартів вищої освіти. Наказ Міністерства освіти і науки України від «01» червня 2017 №600. URL: https://mon.gov.ua/storage/app/media/vishcha-osvita/rekomendatsii-1648.pdf

42. Стандарт вищої освіти України першого (бакалаврського) рівня, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека. Наказ Міністерства освіти і науки України 04.10.2018 р. № 1074 (зі змінами та доповненнями). URL: https://mon.gov.ua/storage/app/media/vishcha-osvita/2022/Standarty.Vyshchoyi.Osvity/Zatverdzheni.Standarty/01/31/125-Kiberbezpeka-bak.31.01.22.pdf