МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖЕНО
Голова Приймальної комісії
Державного університету
інформаційно-комунікаційних
технологій
_____ Володимир ШУЛЬГА

ПРОГРАМА
ФАХОВОГО ІСПИТУ

для здобуття другого (магістерського) рівня вищої освіти

Галузь знань F Інформаційні технології

Спеціальність F5 Кібербезпека та захист інформації

Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

Київ – 2026

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Вступник з кваліфікаційним рівнем **бакалавр** повинен **знати:**

- наукові та практичні основи управління інформаційною безпекою об'єктів різноманітної сфери діяльності;

– структуру діяльності в сфері інформаційної безпеки, ієрархію рівнів організаційної роботи у сфері інформаційної безпеки;

– мету, функціонування і завдання системи забезпечення інформаційної безпеки;

– нормативно-правове забезпечення інформаційної безпеки на рівні держави;

– основи управління інформаційною безпекою підприємства, організації;

– засади побудови системи управління інформаційною безпекою підприємства, організації відповідно до стандартів ISO 27k;

– сутність організаційних заходів з управління інформаційною безпекою підприємства, організації, зокрема створення служби інформаційної безпеки, розробка політики інформаційної безпеки підприємства, забезпечення фізичної безпеки та безпечного поводження з носіями конфіденційних відомостей, дотримання процедур ідентифікації та автентифікації, контролю доступу, вимог операційної та мережевої безпеки тощо;

– основні поняття та визначення теорії захищених інформаційних систем;

– основні процеси та моделі забезпечення безпеки обчислювальних систем;

– основні вимоги до програмного забезпечення, що вирішує завдання захисту інформації;

– зміст національних та міжнародних стандартів безпеки інформаційних технологій;

– типові методи та засоби забезпечення безпеки сучасних інформаційних технологій;

– основні положення криптоаналізу, принципи побудови сучасних криптографічних систем і систем криптографічного захисту інформації;

– побудову та використання систем електронного цифрового підпису

– технічні канали і методи несанкціонованого доступу до інформації:

– типові методи та засоби технічного захисту інформації;

– типові методи та засоби вирішення проблеми комплексного забезпечення інформаційної безпеки в інформаційно-комунікаційних системах та мережах;

– структуру, функції та реалізацію засобів забезпечення безпеки в операційних системах;

– основи безпеки та методи реалізації засобів захисту інформації в системах управління базами даних (СУБД);

– побудову, принципи дії та реалізацію програмно-апаратних засобів забезпечення інформаційної безпеки в розподілених обчислювальних системах та мережах;

– методи та засоби захисту програм та даних від руйнуючих програмних засобів та від програмних засобів, призначених для несанкціонованого перегляду інформації;

– методи та засоби захисту програмного забезпечення від несанкціонованої модифікації та розповсюдження;

– методи та засоби захисту офісних документів від несанкціонованої модифікації та розповсюдження;

– основні напрями розвитку комплексів засобів захисту в інформаційно-комунікаційних системах та мережах;

– основи експлуатації новітніх комплексів засобів захисту в інформаційно-комунікаційних системах та мережах;

– методи забезпечення безпеки інформаційно-комунікаційних систем та процесів їх функціонування в умовах кібернетичного впливу;

– призначення, можливості та принципи побудови інформаційних систем класу SIEM;

– можливості, склад, призначення та функції компонентів програмного комплексу IBM QRadar SIEM;

– основи розгортання, застосування та адміністрування програмного комплексу IBM QRadar SIEM;

– канали та методи несанкціонованого одержання інформації;

– основні методи технічного захисту інформації;

– програмні методи та засоби захисту інформації;

– системи та комплекси технічного захисту інформації;

– порядок розроблення технічного завдання на створення КСЗІ;

– порядок розроблення проектної, робочої та експлуатаційної документації на КСЗІ;

– порядок проведення пусконалагоджувальних робіт, монтажу обладнання і атестації комплексу технічного захисту інформації від витоку технічними каналами;

– порядок проведення інсталяції та ініціалізацію комплексу засобів захисту від несанкціонованого доступу, налагодження всіх механізмів розмежування доступу користувачів до інформації та апаратних ресурсів ІКС, контроль за діями користувачів, формування та актуалізація баз даних захисту, а також контроль цілісності програмного забезпечення та баз даних захисту;

– порядок проведення перевірки працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії;

– порядок проведення дослідної експлуатації КСЗІ;

– порядок організації та проведення державної експертизи КСЗІ;

– порядок організації та проведення супроводу КСЗІ;

– методологічні основи економіки інформаційної безпеки.

вміти:

– планувати й реалізовувати заходи із захисту інформації в інформаційно-комунікаційних системах;

– створювати та забезпечувати функціонування систем інформаційної та кібербезпеки;

– характеризувати основні поняття та визначення теорії захищених інформаційних систем;

– моделювати основні процеси забезпечення безпеки обчислювальних систем;

– обґрунтовувати основні вимоги до програмного забезпечення, що вирішує завдання захисту інформації;

– уміти обґрунтовувати застосування національних та міжнародних стандартів безпеки інформаційних технологій;

– уміти характеризувати особливості забезпечення безпеки сучасних інформаційних технологій;

– характеризувати принципи побудови сучасних криптографічних систем та орієнтуватися в термінології і формулюваннях теоретичних результатів щодо їхньої стійкості;

– надати рекомендації щодо побудови та використання асиметричних криптосистем та основних типів шифрів;

– характеризувати суттєві параметри та потенційні слабкості асиметричних криптосистем та основних типів шифрів;

– надати рекомендації щодо побудови та використання криптографічних протоколів;

– надати рекомендації щодо побудови та використання цифрових підписів на основі еліптичних кривих.

– застосовувати сучасні системи криптографічного захисту інформації;

– виявляти технічні канали витоку інформації;

– використовувати типові методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності;

– використовувати типові методи та засоби вирішення проблеми комплексного забезпечення інформаційної безпеки в інформаційно-комунікаційних системах та мережах.

– характеризувати структуру, функції та реалізацію засобів забезпечення безпеки в операційних системах.

– характеризувати основи безпеки та методи реалізації засобів захисту інформації в системах управління базами даних (СУБД).

– характеризувати побудову, принципи дії та реалізацію програмно-апаратних засобів забезпечення інформаційної безпеки в розподілених обчислювальних системах та мережах.

– реалізувати та експлуатувати методи та засоби захисту програм та даних від руйнуючих програмних засобів та від програмних засобів, призначених для несанкціонованого перегляду інформації.

– реалізувати та експлуатувати методи та засоби захисту програмного забезпечення від несанкціонованої модифікації та розповсюдження.

– реалізувати та експлуатувати методи та засоби захисту офісних документів від несанкціонованої модифікації та розповсюдження.

– характеризувати основні напрями розвитку комплексів засобів захисту в інформаційно-комунікаційних системах та мережах;

– експлуатувати новітні комплекси засобів захисту в інформаційно-комунікаційних системах та мережах;

– створювати моделі об'єктів захисту підприємства (організації), використовуючи системний підхід відповідно до вимог нормативних документів;

– створювати моделі загроз на основі моделювання способів фізичного проникнення зловмисника до об'єктів захисту та моделювання технічних каналів витоку інформації;

– створювати політику безпеки та розробляти вимоги до комплексу засобів захисту;

– проектувати та реалізувати комплексну систему захисту інформації ІКС організації (підприємства) до вимог нормативних документів системи технічного захисту інформації;

– готувати комплексну систему захисту інформації до державної експертизи, розробляти та відпрацьовувати заходи супроводження експлуатації комплексної системи захисту інформації;

– характеризувати системи менеджменту інформаційної безпеки на міжнародному рівні;

– характеризувати системи управління інформаційної безпеки на державному рівні;

– застосовувати системний підхід для побудови системи управління інформаційною безпекою організації (підприємства), яка визначає загальну організацію і класифікацію системи даних, систему доступу, напрямки планування, відповідальність співробітників, використання оцінки ризиків, тощо контексті інформаційної безпеки;

– застосовувати сучасні способи, методи та засоби управління наступними аспектами захисту: політикою безпеки, архітектурою захисту, механізмами захисту та засобами захисту;

– здійснювати оцінку відповідності системи управління інформаційною безпекою своєму призначенню відповідно до вимог діючих стандартів та нормативних документів.

ПРОГРАМА ФАХОВОГО ВИПРОБУВАННЯ

Тема 1. Управління інформаційною безпекою

Теоретичні основи інформаційної безпеки. Поняття інформаційної безпеки та її складових. Інформаційна безпека та кібербезпека. Загрози та джерела загроз інформаційній безпеці. Класифікації загроз інформаційній безпеці. Види

інформації за правовим режимом. Категорії інформації з обмеженим доступом відповідно до українського законодавства. Інформаційні ресурси та інформаційна інфраструктура.

Передумови та основні напрями розвитку менеджменту у сфері інформаційної безпеки. Мета, завдання, передумови та напрями організаційної і управлінської роботи у сфері інформаційної безпеки. Діяльність міжнародних організацій у сфері інформаційної безпеки. Діяльність спеціалізованих міжнародних організацій у сфері інформаційної безпеки. Управління інформаційною безпекою на рівні потужних постачальників інформаційних систем.

Нормативно-правове забезпечення інформаційної безпеки України. Основні положення щодо забезпечення інформаційної безпеки України в Конституції України, Законах України "Про національну безпеку України", "Про інформацію", "Про основні засади забезпечення кібербезпеки України", Указах Президента України "Про Стратегію національної безпеки України", "Про доктрину інформаційної безпеки України", «Про стратегію кібербезпеки України». Механізми правового регулювання і організація захисту персональних даних та інтелектуальної власності в Україні. Правове регулювання боротьби з кіберзлочинністю. Сутність та зміст державно-приватного партнерства у сфері кібербезпеки. Основи національної безпеки, система забезпечення інформаційної безпеки в Україні.

Стандарти у сфері управління інформаційною безпекою та управління безпекою ІТ. Стандарти управління інформаційною безпекою. ITIL. COBIT. Стандарти серії ISO/IEC 27000. Стандарти серії ДСТУ ISO/IEC 13335. НД ТЗІ. Інші стандарти. Гармонізація міжнародних стандартів у сфері управління інформаційною безпекою.

Управління інформаційною безпекою підприємства на основі стандартів серії ISO/IEC 27000. Загальна характеристика стандартів серії ISO/IEC 27000. Огляд стандарту ISO/IEC 27001. Структура стандарту ISO/IEC 27001. Модель системи управління інформаційною безпекою ПВПД (PDCA). Вимоги стандарту і способи їх реалізації.

Розробка та впровадження системи управління інформаційною безпекою. Етапи розробки і впровадження системи управління інформаційною безпекою. Організаційні аспекти впровадження системи управління інформаційною безпекою. Особливості побудови системи управління інформаційною безпекою на основі стандартів серії ISO/IEC 27000. Сертифікація системи управління інформаційною безпекою.

Системний аналіз інформаційної безпеки. Основи системного аналізу інформаційної безпеки. Технології системного аналізу та їх застосування на практиці. Метод експертних оцінок в системному аналізі. Впровадження теорії систем управління в інформаційні системи організації. Моделювання у системному аналізі інформаційної безпеки. Підходи до моделювання процесів створення і оцінки ефективності систем захисту інформації. Сучасні методи й моделі обґрунтування та прийняття рішень.

Управління інформаційною безпекою банку. Особливості захисту банківської інформації. Бізнес-розвідка у банківському секторі. Захист системи електронних банківських платежів. Правове забезпечення захисту інформації у банківській діяльності.

Формування політики інформаційної безпеки на підприємстві (в організації). Структура політики інформаційної безпеки на підприємстві та процес її розробки. Класифікація інформаційних ресурсів підприємства. Методи управління інформаційною безпекою. Заходи забезпечення інформаційної безпеки на адміністративному рівні. Заходи забезпечення інформаційної безпеки на процедурному рівні. Життєвий цикл політики безпеки.

Служба інформаційної безпеки на підприємстві (в організації). Служба інформаційної безпеки як суб'єкт розробки і впровадження системи управління інформаційною безпекою. Організаційна структура служби інформаційної безпеки. Типові завдання служби інформаційної безпеки. Вимоги до фахівця з управління інформаційною бепзекою. Документація з інформаційної безпеки та порядок її ведення.

Вимоги до системи управління інформаційною безпекою відповідно до стандарту ISO/IEC 27002. Заходи фізичної безпеки. Засади автентифікації і безпеки мережі. Правила безпечної роботи в Інтернеті. Правила безпеки користування електронною поштою. Антивірусний захист. Криптографічні заходи. Вимоги безпеки до розробки програмного забезпечення. Типові документи, засновані на вимогах стандарту ISO/IEC 27002.

Управління ризиками інформаційної безпеки підприємства (організації). Аналіз і управління ризиками інформаційної безпеки. Створення реєстру ризиків. Ідентифікація загроз і уразливостей. Оцінка ризиків. Формування паспорту загроз. Управління ризиками.

Управління інцидентами інформаційної безпеки. Поняття інциденту інформаційної безпеки. Виявлення інцидентів. Реагування на інцидент: аналіз інциденту, розслідування інциденту, звіт про інцидент. Запобігання виникненню інцидентів. Усунення наслідків інцидентів.

Аудит інформаційної безпеки на підприємстві (в організації). Поняття аудиту інформаційної безпеки підприємства. Стандарт COBIT. Практика проведення аудиту безпеки. Етапи проведення аудиту: ініціювання процедури аудиту; збирання інформації; аналіз даних аудиту; вироблення рекомендацій; підготовка аудиторського звіту.

Тема 2. Теоретичні основи захищених інформаційних технологій

Основні парадигми формування захищених інформаційних технологій. Основи формування гарантовано захищених інформаційних технологій. Основи розроблення гарантованих систем захисту.

Загальні моделі опису процесів захисту інформації в комп'ютерних системах. Суб'єктно-об'єктна модель опису комп'ютерної системи. Автоматна

суб'єктно-об'єктна модель опису комп'ютерної системи. Підходи до формування моделі загроз. Підходи до формування моделі порушника.

Основи теорії захищених систем. Політики управління доступом. Моделі опису політики безпеки. Моделі забезпечення конфіденційності. Моделі забезпечення цілісності. Моделі забезпечення доступності.

Стандартизовані моделі опису сучасних інформаційних технологій та методи оцінки їх ефективності. Модель, що покладена в основу міжнародних стандартів ISO. Модель, що покладена в основу НД ТЗІ 2.5. Модель, що покладена в основу міжнародного стандарту ISO 15408.

Тема 3. Прикладна криптологія

Основи криптології. Предмет криптології. Роль криптологічних методів в побудові систем захисту інформації. Актуальність побудови надійних систем зв'язку. Проблеми практичної криптології. Загальні типи криптоатак. Практична та теоретична стійкість. Кодування відкритого тексту. Пакування довільних даних для передачі лініями зв'язку.

Розширений алгоритм Евкліда для чисел та многочленів. Методика дешифрування шифру простої заміни.

Порівняння з одним невідомим. Теореми Ейлера і Ферма. Загальний метод розв'язування лінійних порівнянь з одним невідомим. Властивості степеневих порівнянь.

Блокові симетричні криптосистеми.–Загальна характеристика блокових складених шифрів. Принципи побудови блокових шифрів. Компоненти сучасного блокового шифру.

Асиметричні криптосистеми та основні типи шифрів. Задачі криптології, що привели до поняття асиметричних шифрів. Поняття про односторонні функції та односторонні функції з лазівками. Криптосистема RSA, криптосистема Ель-Гамаля, протокол узгодження ключів Діффі-Хеллмана. Поняття геш-функції. Цифровий підпис на основі криптосистеми RSA та криптосистеми Ель-Гамаля.

Генератори псевдовипадкових чисел. Принципи побудови та властивості генераторів псевдовипадкових чисел. Застосування генераторів псевдовипадкових послідовностей при ймовірнісному шифруванні. Приклади криптостійких ГПВЧ: ANSI X9.17, RC4.

Управління ключами. Життєвий цикл ключів. Поняття про ключову систему. Протоколи транспортування та узгодження ключів. Перетворення ключів. Криптоалгоритм RC4. Формування ключів. Алгоритм DES в режимі ECB.

Поняття про електронний цифровий підпис (ЕЦП). Призначення, застосування, властивості і вимоги до ЕЦП. Загальна схема побудови ЕЦП. Схеми електронного цифрового підпису: RSA, Ель-Гамаля; DSA.

Сучасні системи криптографічного захисту інформації. Криптографічний протокол та його основні властивості. Основні принципи побудови і аналізу криптографічних протоколів. Основні класи і види криптопротоколів. Загальна класифікація атак на протоколи. Стандарти

криптопротоколів в Інтернет. Протоколи аутентифікації на основі асиметричної криптосистеми з використанням довіреної особи і на основі доказів з нульовим розголошуванням знання.

Тема 4. Захист інформаційно-комунікаційних систем

Основні положення системи технічного захисту інформації в комп'ютерних системах. Постановка проблеми комплексного забезпечення інформаційної безпеки інформаційних та комунікаційних систем та мереж. Вразливості інформаційно-комунікаційних систем та мереж (ІКСМ) та причини їх виникнення. Основні принципи розробки комплексів засобів (КЗЗ) ІТСМ як розподілених середовищ.

Механізми та засоби захисту операційних систем. Загрози операційним системам. Загальні підходи захисту від атак з метою відмови в обслуговуванні та від атак з метою отримання несанкціонованого доступу до інформації.

Механізми та засоби захисту операційних систем сімейства Microsoft Windows. Особливості моделі захисту операційних систем сімейства Microsoft Windows. Штатні механізми та засоби захисту. Методика використання засобів захисту. Локальні користувачі та групи користувачів. Управління обліковими записами та профілями користувачів. Групова політика безпеки.

Механізми та засоби захисту систем керування базами даних. Причини, види, основні методи порушення конфіденційності в системах керування базами даних (СКБД). Багаторівневі реляційні СКБД. Методи захисту СКБД.

Концепція системи безпеки системи керування базами даних сімейства MS SQL Server. Призначення, традиційна сфера використання та загальнопоширені загрози СКБД сімейства MS SQL Server. Загальна характеристика системи захисту.

Механізми та засоби захисту від шкідливих програмних засобів. Руйнуючі програмні засоби. Програми з потенційно шкідливим впливом та їх властивості. Нормативна та законодавча база в галузі захисту від шкідливих програмних засобів. Основні класи руйнуючих програм. Віруси та „трояни", визначення та класифікація. Засоби розповсюдження. Методи та засоби контролю та протидії вірусам та „троянам".

Загальна характеристика комп'ютерних вірусів. Історична довідка. Визначення комп'ютерного Вірусу. Основні властивості. Класифікація вірусів. Особливості файлових, мережених, загрузочних та макровірусів. Стелс та поліморфні віруси. Шляхи розповсюдження вірусів.

Методи та засоби боротьби з комп'ютерними вірусами. Профілактика зараження вірусами. Використання засобів операційної системи для протидії вірусам. Протидія розповсюдженню вірусів з змінних носіїв інформації (Flash-пам'ять та компакт-диски). Критерії оцінки якості антивірусних програмних комплексів. Сигнатурні методи визначення вірусів. Визначення вірусів за допомогою аналізу подій.

Методи та засоби боротьби з програмами кейлогерами. Призначення програм кейлогерів. Інтернет ресурси в яких представлені кейлогери. Інсталяція та настройка визначеного кейлогера. Визначення програм антикейлогерів.

Технологія захисту від DOS та DDOS атак на комп'ютерні мережі. Поняття DOS та DDOS атак. Мета проведення атаки. Методологія реалізації DOS та DDOS атак.

Захист електронної пошти. Типові загрози для електронної пошти: несанкціонований витік інформації, проникнення вірусів та троянів, засмічення поштового ящика.

Захист Web-серверу Apache. Вітчизняна нормативна база в галузі захисту Web-серверу. Нормативні критерії захищеності Web-серверу. Оцінка захищеності Apache від атаки на відмову в обслуговуванні.

Захист Web-серверу. Вітчизняна нормативна база в галузі захисту Web-серверу. Нормативні критерії захищеності Web-серверу.

Тема 5. SIEM-системи

Методи забезпечення безпеки безпроводових, мобільних та хмарних технологій, які реалізуються в інформаційно-комунікаційних системах. Принципи побудови автоматизованих систем збору та обробки даних про події та потоки в інформаційно-комунікаційних системах. Можливості, склад, призначення та функції компонентів програмного комплексу IBM QRadar SIEM. Основи розгортання, застосування та адміністрування програмного комплексу IBM QRadar SIEM. Поняття «життєвий цикл кібератаки». Зміст етапів процесу кібератаки. Поняття «центр управління кібербезпекою». Призначення та основні завдання SOC. Основні можливості центру управління кібербезпекою. Основні інформаційні технології, які покладені в основу центру управління кібербезпекою. Склад команди та основні функціональні обов'язки фахівців центру управління кібербезпекою. Поняття «SIEM-система». Призначення та основні функції SIEM-системи. Архітектура SIEM-системи. Джерела даних для SIEM-системи.

Тема 6. Основи безпеки комп'ютерних мереж

Загальні принципи побудови та організації комп'ютерних мереж. Розрахунок параметрів IP-адрес. Особливості роботи комутаторів

Мережеві протоколи та обмін даними. Принцип роботи маршрутизаторів. Агрегування каналів в комутованих мережах. Технологія Frame Relay. Статична маршрутизація у мережі на базі маршрутизаторів Cisco. Протокол маршрутизації RIP. Протокол маршрутизації OSPF. Протокол маршрутизації EIGRP. Протокол AAA.

Принципи об'єднання мереж на основі протоколів рівня моделі OSI. Протокол інкапсуляції канального рівня для з'єднань глобальних мереж. Протокол STP/PVST. Засоби протидії атакам на протокол STP/PVST+.

Віртуальні локальні мережі (VLAN). Робота віртуальних локальних мереж. Маршрутизація між VLAN у мережі. Робота протоколу VTP у мережі.

Моніторинг та безпека мережі. Методи та засоби ідентифікації та аутентифікації. Аутентифікація у протоколах канального рівня та у протоколах маршрутизації. Між мережеві захисні екрани. Списки управління доступом (ACL). Віртуальні приватні мережі (VPN). Протокол IPSeci. Засоби протидії атакам MAC-Flooding та MAC-Spoofing.

Тема 7. Методи та засоби захисту інформації

Технічні канали несанкціонованого одержання інформації.

Класифікація каналів витоку інформації. Причини виникнення каналів витоку інформації. *Акустичний* канал витоку інформації. Характеристики каналу та причини його виникнення. *Візуально-оптичний* канал витоку інформації. Характеристики каналу та причини його виникнення. Пристрої візуальних методів нагляду, фотознімання. Класифікація систем прихованого відеонагляду. Основні характеристики, принципи дії та структурні схеми. Особливості застосування. *Електричний* канал витоку інформації. Характеристики каналу та причини його виникнення. Основні характеристики, принцип дії та струкрурні схеми. Особливості застосування та характеристики пристроїв. *Радіотехнічний* канал витоку інформації. Характеристики каналу та причини його виникнення. Витік каналами побічних електромагнітних випромінювань і наводок. Основні характеристики, принцип дії та струкрурні схеми. Особливості застосування та характеристики пристроїв. *Матеріально-речовий* канал витоку інформації. Характеристики каналу та причини його виникнення. Класифікація за фізичним станом, за фізичною природою, за середовищем росповсюдження.

Методи технічного захисту інформації.

Предметна область технічного захисту інформації Концептуальні основи та підходи до створення систем захисту. Класифікація методів та засобів протидії витоку інформації та несанкціонованому її отриманню. Загальні питання захисту інформації від витоку по технічних каналах. Технічні методи захисту інформації. Класифікація технічних методів та засобів захисту інформації. Задачі побудови систем захисту інформації. Підходи до створення комплексних систем захисту інформації.

Програмні методи захисту інформації.

Програмні методи захисту інформації. Основні принципи програмного захисту інформації. Загальні питання побудови систем захисту інформації в автоматизованих системах. Класифікація програмних методів захисту інформації.

Програми зовнішнього захисту. Програми охорони території та приміщень. Програми керування доступом до охороняємої території та приміщень. Програми внутрішнього захисту. Програми розпізнавання користувачів.

Методи розпізнавання автоматизованих систем та її елементів. Проблеми та програми регулювання використання ресурсів. Особливості застосування внутрішнього захисту. Захист програм від копіювання. Програми ядра системи безпеки. Програми реєстрації. Програми знищення та сигналізації. Особливості застосування програм ядра системи безпеки.

Тема 8. Комплексні системи захисту інформації

Загальні положення та вимоги щодо організації робіт із захисту інформації та порядку створення комплексної системи захисту інформації в ІКС. Поняття комплексної системи захисту інформації (КСЗІ) в ІКС. Основні нормативно-правові акти щодо організації робіт із захисту інформації та порядку створення КСЗІ в ІКС. Єдність порядку створення КСЗІ на всіх етапах життєвого циклу ІКС. Процес створення КСЗІ як здійснення комплексу взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в ІКС згідно з вимогами, встановленими нормативно-правовими актами та нормативних документів (НД) у сфері захисту інформації. Порядок створення КСЗІ в ІКС як сукупність впорядкованих у часі, взаємопов'язаних, об'єднаних в окремі етапи робіт, виконання яких необхідне й достатнє для КСЗІ, що створюється.

Основні засоби та заходи, що входять до складу КСЗІ. КСЗІ як заходи та засоби, які реалізують способи, методи, механізми захисту інформації від: витоку технічними каналами, до яких відносяться: канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали; несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів та ін; спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту. Вплив властивостей оброблюваної інформації, класу автоматизованої системи та умов експлуатації ІКС на склад, структуру та вимоги до КСЗІ. Забезпечення режиму секретності, протидії технічним розвідкам та організаційні заходи щодо охорони інформації з обмеженим доступом у процесі проектування, розроблення, виготовлення, експлуатації ІКС. Створення комплексів захисту інформації КЗЗ від витоку технічними каналами. Модульний принцип побудови КСЗІ інтегрованої в ІКС.

Порядок створення, завдання, функції, структура та повноваження служби захисту інформації щодо організації робіт зі створення КСЗІ в ІКС. Загальну положення про службу захисту інформації (СЗІ). Завдання СЗІ. Функції СЗІ: під час створення КСЗІ; під час експлуатації КСЗІ; з організації навчання персоналу з питань забезпечення захисту інформації. Повноваження та відповідальність СЗІ: права СЗІ; обов'язки СЗІ; відповідальність СЗІ; взаємодія СЗІ з іншими підрозділами та зовнішніми організаціями; штатний розклад та структура СЗІ. Організація робіт служби захисту інформації. Фінансування СЗІ.

Обґрунтування необхідності створення КСЗІ. Підстава для визначення необхідності створенні КСЗІ. Вихідні дані для обґрунтування необхідності створення КСЗІ. Прийняття рішення про необхідність створення КСЗІ.

Обстеження середовищ функціонування ІКС. Обстеження обчислювальної системи ІКС. Обстеження інформаційного середовища.

Обстеження фізичного середовища. Обстеження середовища користувачів. Акт обстеження. План захисту інформації в ІКС. Перелік об'єктів захисту. Потенційні загрози для інформації, модель загроз та модель порушника.

Формування завдання на створення КСЗІ. Завдання захисту інформації в ІКС, мета створення КСЗІ, варіант вирішення задач захисту, основні напрями забезпечення захисту. Аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначення переліку суттєвих загроз. Визначення загальної структури та складу КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, допустимі обмеження щодо застосування певних заходів і засобів захисту (обмеження щодо використання засобів активного захисту від витоку інформації каналами ПЕМВН за рахунок використання засобів ЕОТ в захищеному виконанні тощо), інші обмеження щодо середовищ функціонування ІКС, обмеження щодо використання ресурсів ІКС для реалізації задач захисту, припустимі витрати на створення КСЗІ, умови створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальні вимоги до співвідношення та меж застосування в ІКС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ. Оформлення звіту про виконання робіт цієї стадії та оформлення заявки на розробку КСЗІ.

Розробка політики безпеки інформації в ІКС. Вивчення об'єкта, на якому створюється КСЗІ, проведення науково-дослідних робіт. Вибір варіанту КСЗІ. Оформлення політики безпеки.

Розробка технічного завдання на створення КСЗІ. Призначення та основний зміст технічного завдання (ТЗ). Варіанти оформлення ТЗ на КСЗІ. Особливості ТЗ на КСЗІ для інтегрованих ІКС, які будуються за модульним принципом.

Розробка проекту КСЗІ. Порядок розробки проекту КСЗІ. Ескізний проект КСЗІ. Технічний проект КСЗІ. Робочий проект КСЗІ.

Введення КСЗІ в дію та оцінка захищеності інформації в ІКС. Підготовка організаційної структури та розробка розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІКС. Навчання користувачів.

Комплексування КСЗІ. Будівельно-монтажні роботи. Пусконалагоджувальні роботи. Попередні випробування. Дослідна експлуатація. Державна експертиза КСЗІ.

Супроводження КСЗІ. Порядок виконання робіт з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації відповідно до плану захисту та експлуатаційної документації на компоненти КСЗІ, гарантійному та післягарантійному технічному обслуговуванню засобів захисту інформації.

ЛІТЕРАТУРА

1. Закон України “Про інформацію”.
2. Закон України “Про державну таємницю”.
3. Закон України “Про захист персональних даних”.
4. Закон України “Про основні засади забезпечення кібербезпеки України”.
5. Закон України “Про електронні комунікації”.
6. Закон України “Про захист інформації в інформаційно-комунікаційних системах”.
7. Закон України “Про національну безпеку України”.
8. Указ Президента України від 25 лютого 2017 року № 47 “Про рішення Ради нац. безпеки і оборони України від 29 грудня 2016 року “Про Доктрину інформаційної безпеки України”. [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/472017-21374.
9. Указ Президента України від 26 серпня 2021 року № 447/2021 “Про рішення Ради нац.безпеки і оборони України від 14 травня 2021 року “Про Стратегію кібербезпеки України”. [Електронний ресурс]. – Режим доступу: України" https://zakon.rada.gov.ua/laws/show/447/2021#Text.
10. Указ Президента України від 14 вересня 2020 р. № 392/2020 “Про рішення Ради нац. безпеки і оборони України від 14 вересня 2020 року “Про Стратегію національної безпеки України”. [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/3922020-35037.
11. Указ Президента України "Про Положення про технічний захист інформації в Україні" від 27.09.1999 № 1229.
12. Постанова Кабінету Міністрів України від 19.06.2019 № 518 “Про затвердження загальних вимог з кіберзахисту об’єктів критичної інфраструктури”.
13. Постанова Кабінету Міністрів України від 23.12.2020 № 1295 “Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки”.
14. Постанова Кабінету Міністрів України від 29.12.2021 № 1426 “Про затвердження Положення про організаційно-технічну модель кіберзахисту”.
15. Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах”.
16. Постанова Кабінету Міністрів України "Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації" від 21.02.2025 № 205.
17. Наказ Адміністрації Держспецзв’язку від 15.01.2016 № 20 “Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в інтернеті”.
18. Наказ Адміністрації Держспецзв’язку від 26.03.2007 № 45 “Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сферах технічного захисту інформації”.

19. Положення про державну експертизу в сфері технічного захисту інформації. Затверджене наказом ДСТСЗІ СБ України від 16.05.2007 № 93 і зареєстроване в Міністерстві юстиції України 16.07.2007 за № 820/14087.

20. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб. Затверджене наказом ДСТСЗІ СБ України від 18.10.2023 № 899 і зареєстроване в Міністерстві юстиції України 01.12.2021 за № 2091/41147.

21. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT)

22. ДСТУ ISO/IEC 27002:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки (ISO/IEC 27002:2022, IDT)

23. ДСТУ ISO/IEC 27003:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова (ISO/IEC 27003:2017, IDT)

24. ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання (ISO/IEC 27004:2016, IDT)

25. ДСТУ ISO/IEC 27005:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT)

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

27. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 1. Концепції й моделі безпеки IT (ISO/IEC TR 13335-1:1996, IDT)

28. ДСТУ ISO/IEC TR 13335-2:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 2. Керування та планування безпеки IT (ISO/IEC TR 13335-2:1997, IDT)

29. ДСТУ ISO/IEC 15408-1:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки IT. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2022, IDT)

30. ДСТУ ISO/IEC 15408-2:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки IT. Частина 2. Функційні компоненти безпеки (ISO/IEC 15408-2:2022, IDT)

31. ДСТУ ISO/IEC 15408-3:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки IT. Частина 3. Компоненти убезпечення (ISO/IEC 15408-3:2022, IDT)

32. ДСТУ ISO/IEC 15408-4:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки IT. Частина 4. Структура для визначення методів оцінювання та діяльності (ISO/IEC 15408-4:2022, IDT)

33. ДСТУ ISO/IEC 15408-5:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 5. Попередньо визначені пакети вимог до безпеки (ISO/IEC 15408-5:2022, IDT)

34. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

35. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22. (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)

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

37. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000. (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)

38. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. Затверджено наказом ДСТСЗІ СБ України від 09.02.2001 № 2.

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

40. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22. (Зміна № 1 наказ від 28.12.2012 № 806)

41. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22. (Зміна № 1 наказ від 15.10.2008 № 172)

42. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84. (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)

43. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

44. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.

45. НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

46. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації

засобів технічного захисту інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 20.12.2000 № 60. (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)

47. НД ТЗІ 3.6-003-2016. Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації.

48. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22. (Зміна № 1 наказ ДСТСЗІ СБУ від 18.06.2002 № 37, зміна № 2 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)

49. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Затверджено наказом ДСТСЗІ СБ України від 08.11.2005 № 125.

50. Вступ до квантової криптології [Текст]: Навчальний посібник (Для студентів техн. спец. вищ. навч. закл.) / [А.Д. Кожухівський, І.Д. Горбенко, В.К. Задірака, О.М. Хіміч, Ю.І. Горбенко, Г.І. Гайдур, О.А. Кожухівська, В.В. Марченко.]; М-во освіти і науки України, Державний університет телекомунікацій.- К.: ДУТ, 2025. – 691 с.

51. Методи та засоби технічного захисту інформації: Опорний конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: В.М. Луценко, Д.О. Прогонов. – Електронні текстові дані (1 файл: 1,80 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 289 с. https://ela.kpi.ua/bitstreams/1387ecef-b4cb-4554-b55f-7c34e52b3605/download

52. Технічний захист інформації: Навч. погіб. в 2 ч. Ч. 1: Основи технічного захисту інформації / В.М.Богуш, В. Д. Бровко, О.С.Кобус, В.Д. Козюра. Київ: Видавництво Ліра-К, 2022. – 286 с. https://knushop.com.ua/image/catalog/lira20230617/pdf/13054.pdf?srsltid=AfmBOoqRT7snkVTSTjDs_hQJh5fcXTcWSrRXLaQCdYffqFs6whQ8pNvF

53. Котенко А.М. Курс лекцій для студентів з галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека та захист інформації» з дисципліни «Системи контролю та управління доступом на ОІД»/ А.М. Котенко. Державний університет інформаційно-комунікаційних технологій,–К., ДУІКТ, 2024. – 79 с. https://duikt.edu.ua/uploads/l_1372_10715986.pdf

54. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с. https://lira-k.com.ua/preview/12867.pdf?srsltid=AfmBOoqzg23vDnRFvDb9QAjOhJF4yty_1eKmcfB1cF2H8gWrD-P1F2G5

55. Безпека інформації : конспект лекцій / укладач О. С. Кушнерьов. – Суми: Сумський державний університет, 2021. – 99 с. https://essuir.sumdu.edu.ua/bitstream-download/123456789/85989/3/Kushnerov.pdf;jsessionid=DAF96BD511913EA27F430BDEA0BD267F

56. Інформаційна безпека та кібербезпека держави: навчальний посібник / Н.М. Титова, Н.М. Рідей, В.П. Настрадін, М.М. Присяжнюк, С.М. Мамченко, С.В. Артюх, Р.О. Яворська. // К., Вид-во Ліра-К, 2024, 224 с. https://jurkniga.ua/contents/informatsiyna-bezpeka-ta-kiberbezpeka-derzhavi.pdf?srsltid=AfmBOoonlSD1-wrG2YmF-bHwmhdSCi7OHzlEKVrfRyGvvlfca4VA4Sxx

57. О.І. Чобаль, І.І. Трикур, М.П. Самохвалов, В.М. Різак. Методи і засоби захисту інформації: лабораторний практикум. – Ужгород: ДВНЗ „Ужгородський національний університет". – 2023. – 80 с. https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/56222/1/%D0%9F%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA_%D0%9B%D0%B0%D0%B1_%D1%80%D0%BE%D0%B1_%D0%9C%D0%97%D0%97%D0%86_2023.pdf

58. Програмні технології захисту інформації: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти, спеціальності 121 Інженерія програмного забезпечення факультету інформаційних технологій УжНУ / Укладач: д.т.н., доц. Поліщук В.В. – Ужгород: 2023. – 76 с. https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/19693/3/%D0%9A%D0%BE%D0%BD%D1%81%D0%BF%D0%B5%D0%BA%D1%82%20%D0%BB%D0%B5%D0%BA%D1%86%D1%96%D0%B9%20%D0%9F%D0%A2%D0%97%D0%86.pdf

59. Безпека інфокомунікацій та безперервність бізнес-процесів. Електронний навчальний посібник. / Г.В. Косован, Г.І. Ластівка, П.М. Шпатар. // Чернівці, ЧНУ, 2023. 153 с. https://drive.google.com/file/d/1VKk9f3CLavO5ctgWuc-TXOkZKhR1FQOW/view?pli=1

60. Ліцензування, атестація та сертифікація в сфері безпеки об'єктів інформаційної діяльності. Електронний навчальний посібник / Кушнір М.Я., Горбулик В.І. // Чернівці, ЧНУ, 2023. 104 с. https://drive.google.com/file/d/1SdEY2WkJsDj1C4it7YCCHbn_PPynvWPl/view

61. Засоби радіопротидії в інформаційно-телекомунікаційних системах. Електронний навчальний посібник. / Браїловський В.В., Рождественська М.Г., Гресь О.В., Косован Г.В. // Чернівці, ЧНУ, 2021. 130 с. https://drive.google.com/file/d/1PQBSe2ORgpfeYPGvbLiGYTRNexlcVWg9/view

62. Управління інформаційною безпекою. Навчальний посібник / [уклад.: Толюпа С.В., Політанський Л.Ф., Політанський Р.Л., Лесінський В.В.] Чернівці.: Чернівецький нац. ун-т ім. Ю.Федьковича, 2021. – 540 с. https://drive.google.com/file/d/160LvEO5XQnbtZFsQb2L_wA8bJEnjBnch/view

63. Лаптєв О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності Навчальній посібник Київ – 2020. –126 с. https://duikt.edu.ua/uploads/l_2031_50136601.pdf

64. Савченко В.А. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. / Ю. М. Якименко, В. А. Савченко, С. В. Легомінова. Київ: Державний університет телекомунікацій, 2022. 308 с. URL: https://dut.edu.ua/uploads/l_2230_88161692.pdf.

65. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с. https://duikt.edu.ua/uploads/l_1426_56444238.pdf

66. Інформаційна безпека та гібридні загрози: навчальний посібник. Укл. Мухін В.Є., Завгородній В.В., Завгородня Г.А. Київ : ТОВ «ТРОПЕА», 2024. 104 с. https://files.duit.edu.ua/uploads/%D0%A1%D0%B0%D0%B9%D1%82/3_%D0%9D%D0%90%D0%A3%D0%9A%D0%90/scientific-publications/monographs/information_security_and_hybrid_threats.pdf .

67. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с. https://lira-k.com.ua/preview/12867.pdf?srsltid=AfmBOooKlUg0smK991mL4FTTxgPDdWByvtE2XFVfGhLKscRn-MwCT7vt

68. Данілова Е. І. Концепція системного підходу до управління економічною безпекою підприємства: монографія. Вінниця: Європейська наукова платформа, 2020. 342 с. URL: https://ojs.ukrlogos.in.ua/index.php/monograph/article/view/danilova.kontseptsiia-2020/1859.

69. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України. URL: https://zakon.rada.gov.ua/laws/show/v0365500-11.

70. Побудова Системи управління інформаційною безпекою (СУІБ). URL: https://zahyst-ua.com/pobudova-sistemi-upravlinnya-informacijnoju-bezpekoju-suib/.

71. Управління інформаційною безпекою: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1114 Кбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с. http://web.kpi.kharkov.ua/cep/wp-content/uploads/sites/217/2024/01/Upravlinnya-informatsijnoyu-bezpekoyu.pdf

72. П.Г. Сидоркін, С.О. Горліченко, В.С. Некоз, М.В. Шилан. «Методи управління ризиками інформаційної безпеки CRAMM та COBIT 5 FOR RISK». - 2023. https://duikt.edu.ua/uploads/l_2234_89731024.pdf

73. Карпович І.М., Гладка О.М., Калашніков В.І.. «Моделювання процесів аналізу ризиків інформаційної безпеки як спосіб оптимізації витрат». - 2022. https://duikt.edu.ua/uploads/l_2163_29474377.pdf

74. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2024. – 370 с https://profbook.com.ua/index.php?route=product/product/download&product_id=8999&download_id=2047&srsltid=AfmBOopCqtAUcJn81p9V9Tj06MA3Vurf20gX2tJlIve2JhrpPRUdc8Ul

КРИТЕРІЇ ОЦІНЮВАННЯ

Рівень знань	Бали	Критерії оцінювання знань
Початковий	100-107	Вступник називає загрози інформаційній безпеці
	108-115	Вступник називає класифікує загрози інформаційній безпеці; вибирає правильний варіант відповіді на рівні «так-ні»
	116-123	Вступник двома-трьома словами має розповісти про об'єкти захисту інформації
Середній	124-132	Вступник репродуктивно відтворює невелику частину навчального матеріалу, пояснюючи терміни у сфері управління інформаційною безпекою
	133-141	Вступник з допомогою викладача відтворює основний зміст навчальної теми, визначає властивості інформації
	124-150	Вступник самостійно відтворює фактичний матеріал теми, дає стислу характеристику системі управління інформаційною безпекою
Достатній	151-159	Вступник послідовно і логічно відтворює навчальний матеріал теми, виявляє розуміння термінології, характеризує вразливості інформаційної системи (причини, наслідки, значення), відокремлює деякі ознаки явищ та процесів
	160-168	Вступник володіє навчальним матеріалом і використовує знання за аналогією, дає правильні визначення, аналізую можливі загрози інформаційній безпеці, визначає причинно-наслідкові зв'язки між ними
	169-177	Вступник оперує навчальним матеріалом, формує нескладні висновки, обґрунтовуючи їх конкретними фактами; самостійно встановлює причинно-наслідкові зв'язки між вразливостями та загрозами інформаційній безпеці
Високий	178-185	Вступник використовує набуті знання для вирішення нової навчальної проблеми; виявляє розуміння системи управління інформаційною безпекою; робить аргументовані висновки, спираючись на широку джерельну базу

		і визначити шляхи її розв'язання; користується джерелами інформації, аналізує та узагальнює їх.

ПОРЯДОК ПРОВЕДЕННЯ ФАХОВОГО ІСПИТУ

Склад фахової атестаційної комісії визначається наказом ректора Державного університету інформаційно-комунікаційних технологій, робота комісії та порядок проведення вступного випробування регламентуються «Положенням про Приймальну комісію Державного університету інформаційно-комунікаційних технологій» введеного в дію наказом ректора від 21 січня 2026 року № 18.

Завідувач кафедрою
Управління кібербезпекою та
захистом інформації Світлана ЛЕГОМІНОВА