Додаток 13

ЗАТВЕРДЖЕНО
Наказ Державного університету
інформаційно-комунікаційних
технологій
від «18» квітня 2024 р. № 76

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

# ПРОГРАМА
# ФАХОВОГО ІСПИТУ
# ЗІ СПЕЦІАЛЬНОСТІ
# 125 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ
# ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
# «ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА»

для здобуття другого (магістерського) рівня вищої освіти

Київ – 2024

## ПОЯСНЮВАЛЬНА ЗАПИСКА

Програма фахового іспиту для навчання за освітнім ступенем «магістр» галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека та захист інформації» є нормативним документом Державного університету інформаційно-комунікаційних технологій.

Програма розроблена кафедрою Інформаційної та кібернетичної безпеки Навчально-наукового інституту Захисту інформації відповідно до Правил прийому до Державного університету інформаційно-комунікаційних технологій в 2024 році, базується на змісті і вимогах освітньо-кваліфікаційної характеристики та освітньої програми фахівця освітнього ступеня «бакалавр» спеціальності.

В програмі визначено:

- кваліфікаційні вимоги до знань і умінь вступників;
- рівні оцінювання знань і умінь вступників;
- перелік тем фахового іспиту для вступників, які бажають вступити на другий (магістерський) рівень вищої.

## МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО ПРОВЕДЕННЯ ФАХОВОГО ІСПИТУ

Мета фахового іспиту – встановити рівень фахової готовності абітурієнта до навчання за освітнім ступенем «магістр».

Фаховий іспит з спеціальності організує і проводить фахова атестаційна комісія.

Фаховий іспит проводиться таким чином, щоб його тривалість не перевищувала 2 години.

Результати фахового іспиту оцінюється за 200-бальною шкалою, за якими формується рейтинг вступників.

## КВАЛІФІКАЦІЙНІ ВИМОГИ ДО ЗНАНЬ І УМІНЬ ВСТУПНИКІВ

Абітурієнт, який бажає вступити на другий (магістерський) рівень вищої освіти повинен **знати:**

– 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;

– принципи побудови сучасних криптографічних систем;

– основи побудови та використання симетричних криптосистем;

– основи побудови та використання асиметричних криптосистем;
– основні положення криптоаналізу.
– методи побудови та використання криптографічних протоколів;
– побудову та використання систем електронного цифрового підпису
– сучасні системи криптографічного захисту інформації;
– 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 проводження 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;

– основні напрями розвитку системи менеджменту у сфері інформаційної безпеки;

– нормативно-правове забезпечення інформаційної безпеки на рівні держави;

– основи управління інформаційною безпекою підприємства;

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

– сутність організаційних заходів з управління інформаційною безпекою підприємства, 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;

- методологічні основи економіки інформаційної безпеки.

**вміти:**

– 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 ІСПИТУ

### Тема 1. 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 міжнародного стандарту ISO 7498-2. Модель, що покладена в основу НД ТЗІ 2.5. Модель, що покладена в основу міжнародного стандарту ISO 15408.

### Тема 2. 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.

**Модульна арифметика та елементарні шифри.** Лишки за модулем. Відношення порівняння. Розширений алгоритм Евкліда для чисел та многочленів. Модульна арифметика. Шифри заміни, гамування та перестановки. Шифри пропорційної та поліалфавітної заміни. Методика дешифрування шифру простої заміни.

**Порівняння з одним невідомим.** Теореми Ейлера і Ферма. Порядок числа та первісний корінь за модулем. Система лінійних порівнянь та китайська теорема про залишки. Загальний метод розв'язування лінійних порівнянь з одним невідомим. Властивості степеневих порівнянь. Двочленні порівняння вищих степенів за простим модулем.

**Блокові симетричні криптосистеми.** Загальна характеристика блокових складених шифрів. Принципи побудови блокових шифрів. Компоненти сучасного блокового шифру. Атаки на блокові шифри. Блоковий шифр DES. Стандарт криптографічного перетворення даних ГОСТ 28147-89. Стандарт симетричного шифрування AES / Rijndael.

**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 3. 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 4. SIEM-системи

**Методи забезпечення безпеки, 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 5. Основи безпеки комп'ютерних мереж

**Загальні принципи побудови та організації комп'ютерних мереж.** Розрахунок параметрів IP-адрес. Особливості роботи комутаторів та маршрутизаторів. Принцип роботи маршрутизаторів. Агрегування каналів в комутованих мережах.

**Протоколи та алгоритми маршрутизації.** Одномаршрутні та багатомаршрутні алгоритми. Однорівневі та ієрархічні алгоритми**.** Статична та динамічна маршрутизація. Протокол маршрутизації RIP. Протокол маршрутизації OSPF. Протокол маршрутизації BGP. Протокол маршрутизації IGRP/EIGRP.

**Протоколи безпеки на рівнях моделі OSI.** Типи атак на канальному рівні. Протокол інкапсуляції канального рівня для з'єднань глобальних мереж. Протокол STP/PVST. Засоби протидії атакам на протокол STP/PVST+. Протоколи безпеки на мережевому рівні. Протоколи безпеки на транспортному рівні. Керування сеансами TCP. Протокол UDP. Безпека на сеансовому рівні. Протокол

SSL/TLS. Протоколи безпеки прикладного рівня. Шифрування HTTP трафіку (режим HTTPS).

**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. Налаштування служб безпеки AAA. Міжмережеві захисні екрани. Списки управління доступом (ACL). Віртуальні приватні мережі (VPN). Протокол IPSec. Режим тунелювання.

## Тема № 6. Основи захисту конфіденційних даних

**Закони України**. Закон України «Про інформацію», «Про захист персональних даних», «Про доступ до публічної інформації».

**Персональна, власна та конфіденційна інформація.** Персональна інформація. Порівняння персональних та конфіденційних даних. Поняття «комерційна таємниця».

**Особливості доступу до інформації**. Порівняння відкритої інформації та інформації з обмеженим доступом. Поняття таємна та службова інформація. Поняття «запиту на інформацію». Гриф обмеження доступу (гриф конфіденційності). Засекречування та розсекречування носіїв інформації.

## Тема 7. Архітектура захисту інформації

**Механізми захисту інформаційно-комунікаційних систем**

Визначення та зміст керування доступом. Механізми керування доступом. Визначення та зміст довірчого керування доступом (дискреційна модель). Адміністративне керування доступом (мандатна модель). Поняття та зміст ролевої моделі керуванням доступу (RBAC модель). Поняття та зміст керуванням доступом на основы атрибутів керуванням доступу (ABAC модель).

Визначення та зміст автентифікації. Механізми забезпечення автентифікації. Автентифікація на базі протоколу RADIUS. Автентифікація на базі протоколу TACACS+. Автентифікація на базі протоколу LDAP.

Поняття та зміст процедури авторизації користувача. Поняття та зміст процедури ідентифікації користувача.

Поняття та зміст конфіденційності. Механізми забезпечення конфіденційності. Поняття та зміст доступності. Механізми забезпечення доступності. Поняття та зміст цілісності. Механізми забезпечення цілісністі.

Поняття та зміст політики безпеки інформації. Поняття та зміст безпеки інформації. Поняття та зміст захисту інформації в автоматизованих системах.

Поняття та зміст несанкціонованого доступу до інформації. Поняття та зміст захисту від несанкціонованого доступу до інформації.

Поняття та зміст моделі загроз. Поняття та зміст моделі порушника. Поняття та зміст послуги безпеки. Поняття та зміст механізмів захисту. Поняття та зміст моделі політики безпеки.

**Програмно-апаратні комплекси забезпечення захисту інформації.** Системи контролю і керування доступом. Програмні комплекси антивірусного захисту. Призначення, характеристики та особливості застосування мережевих екранів. Системи виявлення вторгнень, призначення, архітектура, функції.

## 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.

**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. 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.

**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 на компоненти КСЗІ, гарантійному та післягарантійному технічному обслуговуванню засобів захисту інформації.

## Тема 9. Управління інформаційною безпекою

**Передумови та основні напрямки розвитку менеджменту у сфері інформаційної безпеки.** Мета, завдання, передумови та напрямки 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.

**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.

**Нормативно-правове забезпечення інформаційної безпеки України.** 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».

**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. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010.

**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.

**Формування політики інформаційної безпеки на підприємстві.** 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.

**Служба інформаційної безпеки на підприємстві**. 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. Робота з персоналом підприємства.

**Управління ризиками інформаційної безпеки підприємства**. Аналіз і управління ризиками інформаційної безпеки. Створення реєстру ризиків. Ідентифікація загроз і уразливостей. Оцінка ризиків. 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**. 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.

## 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 26.08.2021 № 447 “Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року “Про Стратегію кібербезпеки України”.
9. Постанова Кабінету Міністрів України від 19.06.2019 № 518 “Про затвердження загальних вимог з кіберзахисту об’єктів критичної інфраструктури”.
10. Постанова Кабінету Міністрів України від 23.12.2020 № 1295 “Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки”.
11. Постанова Кабінету Міністрів України від 29.12.2021 № 1426 “Про затвердження Положення про організаційно-технічну модель кіберзахисту”.
12. Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах”.
13. Наказ Адміністрації Держспецзв’язку від 15.01.2016 № 20 “Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в інтернеті”.
14. 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”.
15. Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-61 Revision 2. Paul R. Cichonski, Thomas Millar, Timothy Grance, Karen Scarfone [Електронний ресурс]. Режим доступу: https://www.nist.gov/publications/computer-security-incident-handling-guide.
16. Guide to Integrating Forensic Techniques into Incident Response. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-86. Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang [Електронний ресурс]. Режим доступу: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50875.
17. MITRE. 11 Strategies of a World-Class Cybersecurity Operations Center /Carson Zimmerman -The MITRE Corporation, 2022. – 452 p.

18. NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide, August 2012. http://dx.doi.org/10.6028/NIST.SP.800-61r2.

19. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response, August 2006. http://dx.doi.org/10.6028/NIST.SP.800-86 .

20. Горбеноко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: Підручник для вищих навчальних закладів. – Харків: Видавництво «Форт», 2013. – 880с.

21. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. К.: НБУ, 2010.

22. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). [Електронний ресурс] // НБУ – 2010. – Режим доступу до ресурсу: http://s-byte.com/useful/27001.pdf

23. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD). [Електронний ресурс] // НБУ. – 2010. – Режим доступу до ресурсу: http://s-byte.com/useful/27002.pdf

24. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Звід правил для управління інформаційною безпекою. К.: НБУ, 2010.

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

26. ДСТУ ISO/IEC TR 13335-1:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки. К.: Держспоживстандарт України, 2005.

27. ДСТУ ISO/IEC TR 13335-2:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 2. Керування та планування безпеки ІТ. К.: Держспоживстандарт України, 2005.

28. ДСТУ ISO/IEC TR 13335-3:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом ІТ. К.: Держспоживстандарт України, 2005.

29. ДСТУ ISO/IEC TR 13335-4:2005. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 4. Настанови з керування безпекою інформаційних технологій. К.: Держспоживстандарт України, 2005.

30. ДСТУ ISO/IEC TR 13335-5:2005. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 5. Настанови з керування мережною безпекою. К.: Держспоживстандарт України, 2005.

31. Марк Шпеник М., Следж Ор. Керівництво адміністрування даних MS SQL Server.

32. 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.

33. 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.

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

35. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000

36. 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.

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

38. 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.

39. 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.

40. 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.

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

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

43. 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.

44. 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.

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

46. 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.

47. 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.

48. Park Foreman. Vulnerability Management. Second Edition. CRC Press Taylor & Francis Group, 2019. 330 p.

49. Technical Guide to Information Security Testing and Assessment. Recommendations of the National Institute of Standards and Technology. Karen Scarfone. Murugiah Souppaya. Amanda Cody. Angela Orebaugh. NIST Special Publication 800-115. (Sep. 2008). 80 p. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf .

50. Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. Paul Cichonski. Tom Millar. Tim Grance. Karen Scarfone. Special Publication 800-61 Revision 2 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

51. Bertino E., Martino L.D., Paci F., Squicciarini A.C. Security for WEB Services and Service Oriented Architectures Springer, 2010. – 231 p. – ISBN 978-3-540-87741-7.

52. Andrew Hoffman. Web Application Security Exploitation and Countermeasures for Modern Web Applications. 2020. ISBN 9781492053118 .

53. COBIT 2019 Framework: Introduction and Methodology" – "COBIT 2019 Бізнес-модель: Введення та методологія".

54. COBIT 2019 Framework: Governance and Management Objectives – COBIT 2019 Бізнес-модель: Завдання керівництва та управління.

55. «COBIT 2019 DESIGN GUIDE: Designing an Information and Technology Governance Solution – «Проектування рішення щодо керівництва інформацією та технологіями».

56. «COBIT 2019 IMPLEMENTATION GUIDE: Implementing and Optimizing and Information and Technology Governance Solution» — «Впровадження та оптимізація рішення щодо керівництва інформацією та технологіями».

## КРИТЕРІЇ ОЦІНЮВАННЯ

Фаховий іспит складається з 3-х запитанньь (П1, П2, П3), на які абітурієнт письмово надає розширену відповідь. Кожне запитання оцінюється в 200 балів. Розрахунок загального балу (ЗБ):

**ЗБ=(П1+П2+П3)/3.**

| **Рівень знань** | **Бали** | **Критерії оцінювання знань** |
|---|---|---|
| Початковий | 100-107 | Абітурієнт називає загрози інформаційній безпеці |
| | 108-115 | Абітурієнт називає класифікує загрози інформаційній безпеці; вибирає правильний варіант відповіді на рівні «так-ні» |

| | | |
|---|---|---|
| | 116-123 | Абітурієнт двома-трьома словами має розповісти про об’єкти захисту інформації |
| Середній | 124-132 | Абітурієнт репродуктивно відтворює невелику частину навчального матеріалу, пояснюючи терміни у сфері управління інформаційною безпекою |
| | 133-141 | Абітурієнт з допомогою викладача відтворює основний зміст навчальної теми, визначає властивості інформації |
| | 124-150 | Абітурієнт самостійно відтворює фактичний матеріал теми, дає стислу характеристику системі управління інформаційною безпекою |
| Достатній | 151-159 | Абітурієнт 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 | Абітурієнт 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 | Абітурієнт 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 | Абітурієнт використовує набуті знання для вирішення нової навчальної проблеми; виявляє розуміння системи управління інформаційною безпекою; робить аргументовані висновки, спираючись на широку джерельну базу |
| | 168-193 | Абітурієнт володіє глибокими знаннями, може вільно та аргументовано висловлювати власні судження щодо розробки основних документів з питань управління інформаційною безпекою |
| | 194-200 | Абітурієнт системно володіє навчальним матеріалом; виявляє особисту позицію щодо розробки системи управління інформаційною безпекою організації; уміє відокремити проблему 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 від 29.03.2024 року № 62/1 «Про затвердження складу підрозділів Приймальної комісії Державного університету інформаційно-комунікаційних технологій у 2024 році», робота комісії та порядок проведення вступного випробування регламентуються «Положенням про Приймальну комісію Державного університету інформаційно-комунікаційних технологій» введеного в дію наказом від 18 липня 2023 року № 104.

Голова фахової атестаційної комісії Галина ГАЙДУР