МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖЕНО
Голова Приймальної комісії
Державного університету
інформаційно-комунікаційних
технологій
_____Володимир ШУЛЬГА

ПРОГРАМА
ФАХОВОГО ІСПИТУ
ЗІ СПЕЦІАЛЬНОСТІ
F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«ТЕХНІЧНІЧНІ СИСТЕМИ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ»

для здобуття другого (магістерського) рівня вищої освіти

Київ – 2025

ПОЯСНЮВАЛЬНА ЗАПИСКА

Програма фахового іспиту для навчання за освітнім ступенем «магістр» галузі знань «Інформаційні технології» спеціальності F5 «Кібербезпека та захист інформації» є нормативним документом Державного університету інформаційно-комунікаційних технологій.

Програма розроблена кафедрою Систем інформаційного та кібернетичного захисту Навчально-наукового інституту Захисту інформації відповідно до Правил прийому до Державного університету інформаційно-комунікаційних технологій в 2025 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 форми представлення інформації;
- основні об`єкти захисту інформації;
- технічні канали витоку інформації;
- зміст національних та міжнародних стандартів безпеки інформації;
- типові методи та засоби забезпечення безпеки сучасних інформаційних технологій;
- принципи побудови сучасних криптографічних систем;
- класифікацію методів та засобів захисту інформації від витоку технічними каналами;
- основи екранування технічних засобів;
- основи заземлення технічних засобів;
- основи звукоізоляцій приміщень;
- основні положення криптоаналізу;

- принципи фільтрації інформаційних сигналів;
- принципи просторового лінійного зашумлення;
- 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;
- методи та засоби захисту офісних документів від несанкціонованої модифікації та розповсюдження;
- основи експлуатації новітніх комплексів засобів захисту в інформаційно-комунікаційних системах та мережах;
- призначення, можливості та принципи побудови інформаційних систем класу 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 атестації комплексу технічного захисту інформації від витоку технічними каналами;
- порядок проведення дослідної експлуатації КСЗІ;
- порядок організації та проведення державної експертизи КСЗІ;
- порядок організації та проведення супроводу КСЗІ;
- нормативно-правове забезпечення інформаційної безпеки на рівні держави;
- основи управління інформаційною безпекою підприємства;
- засади побудови системи управління інформаційною безпекою підприємства відповідно до стандартів ISO.

вміти:

- виявляти технічні канали витоку інформації;
- моделювати основні процеси забезпечення захисту інформації на об`єктах інформаційної діяльності;
- надати рекомендації щодо побудови та використання електронних цифрових підписів на основі еліптичних кривих.
- застосовувати сучасні системи криптографічного захисту інформації;
- визначити небезпеку витоку інформації технічним каналом;

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

– використовувати типові методи та засоби вирішення проблеми комплексного забезпечення захисту інформації на об`єктах інформаційної діяльності.

– 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 загроз інформації на об'єктах інформаційного захисту підприємств (організацій), використовуючи системний підхід відповідно до вимог нормативних документів;

– створювати моделі порушника інформаційної безпеки 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;

– проектувати технічні засоби захисту інформації;

– застосовувати апаратуру захисту інформації за її функціональним призначенням;

– оцінювати ризики втрати інформації;

– моніторити стан КСЗІ.

ПРОГРАМА ФАХОВОГО ІСПИТУ

Тема 1. Теоретичні основи захищених інформаційних технологій

Загальні моделі опису процесів захисту інформації на об`єктах інформаційної діяльності. Моделі забезпечення захисту акустичної інформації. Моделі забезпечення захисту інформації, представленої в документальній формі. Моделі забезпечення захисту інформації, представленої в електронній формі.

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.

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. 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. 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 технічним каналам. 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 4. 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 на компоненти КСЗІ, гарантійному та післягарантійному технічному обслуговуванню засобів захисту інформації.

Тема 5. Пошукові заходи з виявлення негласних пристроїв отримання мовної інформації

Методи виявлення. Сканування радіоефіру. Спеціальні вимірювання. Дослідження об`єкту інформаційної діяльності. Активні та пасивні методи виявлення радіомікрофонів та апаратури запису мовної інформації. Організаційні заходи підготовки кімнати перемов. Апаратура спеціального призначення та її характеристики.

Заходи протидії перехопленню мовної інформації.Акустичне та просторове зашумлення. Скремблювання. Екранування приміщень. Звукоізоляція об`єкту інформаційної діяльності. Шифрування інформації. Фільтрація інформаційних сигналів. Створення навмисних перешкод. Застосування пристроїв акустичного та віброакустичного захисту та генераторів шумоподібних завад.

Тема 6. Управління інформаційною безпекою

Нормативно-правове забезпечення інформаційної безпеки держави та політика управління інформаційною безпекою на підприємствах. 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.

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. Остапов С.Е., Євсеєв С.П., Король О.Г. Кібербезпека: сучасні технології захисту: Навчальний посібник для студентів вищих навчальних закладів. – Львів: «Новий Світ –2000», 2022. – 678 с.

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

23. 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

24. 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

25. 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.

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. Частина 1. Концепції та моделі безпеки. К.: Держспоживстандарт України, 2005.

28. 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.

29. 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.

30. 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.

31. 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.

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

33. 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.

34. 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.

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

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

37. 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.

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

39. 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.

40. 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.

41. 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.

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

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

44. 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.

45. 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.

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

47. 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.

48. 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.

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

50. 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 .

51. 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.

52. 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.

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

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

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

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

57. «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 екзаменаційної комісії визначається наказом ректора Державного університету інформаційно-комунікаційних технологій «Про затвердження складу підрозділів Приймальної комісії Державного університету інформаційно-комунікаційних технологій у 2025 році», робота комісії та порядок проведення вступного випробування регламентуються «Положенням про Приймальну комісію Державного університету інформаційно-комунікаційних технологій» введеного в дію наказом від 21 березня 2025 року № 102.

Завідувач кафедрою
технічних систем кіберзахисту Олександр ТУРОВСЬКИЙ