ГРОМАДСЬКЕ ОБГОВОРЕННЯ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний аерокосмічний університет
«Харківський авіаційний інститут»

ЗАТВЕРДЖЕНО

вченою радою Національного
аерокосмічного університету
«Харківський авіаційний інститут»
«____» ____ 2025 р., протокол № __

ОСВІТНЯ ПРОГРАМА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ

ФАХІВЕЦЬ З ОЦІНКИ ЗАХОДІВ ЗАХИСТУ ІНФОРМАЦІЇ (КІБЕРБЕЗПЕКИ)

галузі знань: F «Інформаційні технології»
назва відповідно до ліцензії

спеціальність: F5 «Кібербезпека та захист інформації»
код і найменування спеціальності

категорія слухачів: фахівець з оцінки заходів захисту інформації (кібербезпеки), провідний фахівець з оцінки заходів захисту інформації (кібербезпеки)
назва категорії слухачів

Освітня програма підвищення
кваліфікації вводиться в дію
з «____» _____ 2025 р.

В. о. ректора Національного
аерокосмічного університету
«Харківський авіаційний інститут»

_____ Олексій ЛИТВИНОВ
наказ № ___ від «__» _____ 2025 р.

Харків 2025

Розробники програми:

- завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., професор, член-кореспондент НАН України В.С. Харченко;
- учений секретар Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, д.т.н., професор О.К. Юдін;
- старша наукова співробітниця 3-го науково-дослідного відділу 2-го науково-дослідного центру Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, к.т.н., доцентка Л.Г. Черниш
- завідувач кафедри права Національного аерокосмічного університету «ХАІ», д.ю.н., професор В.І. Павликівський;
- професор кафедри комп’ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету «ХАІ», д.т.н., професор Г.В. Фесенко;
- професор кафедри права Національного аерокосмічного університету «ХАІ», к.ю.н., доцент С.Ю. Лукашевич;
- професорка кафедри права Національного аерокосмічного університету «ХАІ», д.ю.н., професорка Н.Є. Філіпенко;
- завідувач кафедри загальної військової підготовки Національного аерокосмічного університету «ХАІ», к.пед.н., доцент В.В. Рютін
- ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету «ХАІ», PhD з комп’ютерних наук К.Є. Лисицький.

Рецензент:

головний науковий співробітник 3-го науково-дослідного відділу 2-го науково-дослідного центру Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, доктор технічних наук, професор С. В. Толюпа.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Освітня програма підвищення кваліфікації «Фахівець з оцінки заходів захисту інформації (кібербезпеки)» розроблена у відповідності до Типової програми підвищення кваліфікації «Фахівець з оцінки заходів захисту інформації (кібербезпеки)», Розділу ІІІ професійного стандарту «Фахівець з оцінки заходів захисту інформації (кібербезпеки)» та Національного класифікатора України ДК 003:2010 «Класифікатор професій» («Фахівець з оцінки заходів захисту інформації (кібербезпеки)» 2139.2), основних положень і вимог визначених законами України «Про освіту», «Про вищу освіту», інших законодавчих і нормативних документів.

Зміст Програми диференційовано за модулями відповідно до визначеної категорії слухачів і розраховано на розвиток їх професійних компетентностей.

Сьогодні інформаційні системи відіграють ключову роль у забезпеченні ефективності роботи державних установ, підприємств та організацій. Державні установи використовують різноманітні інформаційні системи для зберігання, обробки та передачі інформації. Для ефективного захисту інформації у сучасному світі, де цифрові дані є критично важливими, установам необхідний професіонал, який аналізує, розробляє та впроваджує системи для захисту комп'ютерних мереж, даних від кіберзагроз (вірусів, хакерів, витоків) та оцінює їхню ефективність, щоб забезпечити конфіденційність, цілісність та доступність інформації організації, діючи як «цифровий охоронець», а саме фахівець з оцінки заходів захисту інформації (кібербезпеки). Він є ключовим для захисту від хакерів, вірусів та витоків, розробляючи комплексні стратегії та тестуючи системи. У зв’язку з цим актуалізується проблема розвиту професійних компетентностей фахівців з оцінки заходів захисту інформації (кібербезпеки). Фахівці з оцінки заходів захисту інформації (кібербезпеки) мають вільно та ґрунтовно забезпечує надійний захист цифрових активів, балансуючи між доступністю інформації та її безпекою.

ОСНОВНІ ЗАВДАННЯ ПРОГРАМИ

- планувати та проводити огляди авторизації та безпеки;
- розробляти процеси відповідності безпеки та/або аудитів;
- проводити оцінку ефективності засобів контролю безпеки;
- оцінювати всі процеси управління конфігурацією, здійснювати моніторинг;
- виконувати перегляд та аналіз безпеки, визначати недоліки, формувати плани усунення вразливостей, рекомендації для зниження ризиків;
- формувати звіти по результатам аналізу, процедурам проведеного аудиту і моніторингу, надавати рекомендації й пропозиції щодо протидії кіберінцидентам, сприяти підвищенню якості функціонування кібернетичної безпеки, а також інфраструктури організації в цілому.

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ «Фахівець з оцінки заходів захисту інформації (кібербезпеки)»

Загальна інформація	
Повна назва закладу розробника (ків)	Національний аерокосмічний університет «Харківський авіаційний інститут», Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації
Ступінь вищої освіти слухача	особи, які мають ступень вищої освіти бакалавр або вищий за нього
Форма підвищення кваліфікації	змішана (офлайн/онлайн)
Цільова група	фахівець з оцінки заходів захисту інформації (кібербезпеки), провідний фахівець з оцінки заходів захисту інформації (кібербезпеки)
Термін та обсяг Програми	15 днів / 180 год. (6 кредитів ECTS)
Професійна кваліфікація	фахівець з оцінки заходів захисту інформації (кібербезпеки) (трудові функції А, Б, В, Г)
Мета Програми	
Формування у здобувачів курсів системи професійних знань, вмінь та навичок щодо стратегічного управління кіберризиками, забезпечення стійкості та безперервності бізнес-процесів в умовах постійних кіберзагроз. Набуття здобувачами курсів системи теоретичних знань щодо теорії ризиків, нормативно-правової бази в сфері інформаційної безпеки, технічної експертизи. Формування практичних навичок аудиту та тестування, розвиток управлінських та аналітичних компетенцій.	
Функціональна спрямованість	Розвиток складових професійних компетентностей фахівців з оцінки заходів захисту інформації (кібербезпеки) відповідно до комплексного захисту інформації, поєднуючи технічні знання, аналітичні навички та розуміння правового поля
Фокус програми	Акцент на розвиток професійних компетентностей фахівців з оцінки заходів захисту інформації (кібербезпеки) щодо вільного та ґрунтовного забезпечення надійного захисту цифрових активів, балансуючи між доступністю інформації та її безпекою, а саме: планування та проведення оглядів авторизації та безпеки, розробки процесів відповідності безпеки та/або аудитів, проведення оцінки ефективності засобів контролю безпеки, оцінки всіх процесів управління конфігурацією, здійснення моніторингу, виконання переглядів та аналізів безпеки, визначення недоліків, формування планів усунення вразливостей, розроблення рекомендацій для зниження ризиків, формування звітів за результатами аналізу, процедурам проведеного аудиту і моніторингу, надання рекомендацій й пропозиції щодо

	протидії кіберінцидентам, сприяння підвищенню якості функціонування кібернетичної безпеки, а також інфраструктури організації в цілому.
Орієнтація програми	Програма орієнтована на розвиток професійних компетентностей фахівців з оцінки заходів захисту інформації (кібербезпеки)
Особливості програми	Програма підвищення кваліфікації фахівців з оцінки заходів захисту інформації (кібербезпеки) адаптована до національних вимог, зокрема до Професійного стандарту «Фахівець з оцінки заходів захисту інформації (кібербезпеки))», фокусується на оцінці ризиків, аудиту систем безпеки, розробці стратегій захисту та впровадження стандартів (напр., ISO 27001, NIST), розумінні правового поля кібербезпеки, знанні принципів CIA Triad (конфіденційність, цілісність, доступність), вмінні працювати з антивірусами та засобами захисту, а також оцінювати економічну ефективність заходів для забезпечення захищеності інформаційних систем від загроз. Програма складається з 3 модулів / 4 змістовних модулів. Загальний обсяг програми – 180 акад. год. / 6 кредитів ECTS, з яких: *лекції – 64 год., практичні заняття – 10 год., самостійна робота – 96 год., консультації – 2 год., модульний контроль – 8 год.* Вид підсумкового контролю – комп'ютерне оцінювання знань на базі автоматизованої системи тестування
Професійні вимоги (компетенції) та продовження навчання	
Професійні вимоги (компетенції)	Визначаються посадовими інструкціями
Продовження навчання	Освітня Програма передбачає можливість подальшого розширення та поглиблення професійних знань, умінь, навичок у системі неформальної та інформальної освіти.
Програмні компетентності	
Загальні компетентності	**Когнитивна компетентність** Здатність мислити та розвіватися відповідно до змін зовнішнього середовища, безперервного навчання, постійного оновлення і поповнення знань, отримання нового або переосмслення старого досвіту, управління знаннями, самопізнання. **Громаданська компетентність** Здатність діяти активно, відповідально й ефективно реалізовувати громадянські права та обовязки з метою розвитку демократичного громадянського суспільства, усвідомлювати та сповідувати цінності громадянського суспільства.

	Соціальна компетентність Здатність до міжособистностної взаємодії, відкритості, роботі в команді, спілкування с представниками державних установ, підприємств, організацій, представниками органів влади, місцевого самоврядування та ін. **Культурна компетентність** Здатність виявляти повагу та цінувати українську національну культуру, багатоманітність і мультикультурність у суспільстві. **Інноваційна компетентність** Здатність генерувати і втілювати нові ідеї у сферу інформаційної безпеки, що базується на креативності, творчості, відчутті нового, здатності до здорового ризику. **Інформаційно-цифорва компетентність** Здатність ефективно використовувати можливості сучасних інформаційно-комунікативних і цифрових технологій, управління потоками інформації, правильного їх використання у повсякденному і професійному житті.
Фахові (предметно-орієнтовані)	Для фахівця з оцінки заходів захисту інформації (кібербезпеки) потрібні фахові компетентності, що охоплюють: **1. Аудит та оцінка ризиків:** • Проведення комплексної оцінки управлінського, операційного та технічного контролю безпеки. • Виявлення слабких місць та вразливостей в інформаційних системах (ІС). • Аналіз потенційних загроз та їх впливу. • Оцінка ступеня захищеності та ефективності існуючих заходів. **2. Технічні знання:** • Розуміння принципів роботи антивірусного ПЗ та інших засобів захисту. • Знання методів захисту від несанкціонованого доступу та витоку інформації. • Оцінка реалізації послуг безпеки в ІС. **3. Управління безпекою:** • Розробка та контроль виконання заходів для усунення ризиків. • Підвищення рівня безпеки та забезпечення економічної ефективності захисту. • Впровадження стандартів інформаційної безпеки та управління ризиками. **4. Теоретичні основи:**

	• Знання теорії кібербезпеки, класифікації загроз. • Розуміння основних принципів інформаційної безпеки (конфіденційність, цілісність, доступність - CIA Triad). **5. Правові та організаційні аспекти:** • Знання правових аспектів кібербезпеки в Україні. • Розуміння ролі організаційних та технічних заходів захисту інформації
Програмні результати навчання	
Програма підвищення кваліфікації **«Фахівець з оцінки заходів захисту інформації (кібербезпеки)»** спрямовано на досягнення програмних **результатів навчання**, а саме у відповідності до трудових функцій професійного стандарту та визначеної кваліфікації (далі – ТФ):	
ТФ А РН 1	Оцінювання ефективності засобів контролю безпеки, зокрема огляд авторизації безпеки та аудит зовнішніх послуг. Розробка кейсів впевненості та огляд авторизації безпеки.
ТФ Б РН 2	Оцінювання дотримання заходів забезпечення відповідності, у тому числі з аналізом процесів управління конфігураціями та дотриманням встановлених обмежень прикладного програмного забезпечення, мереж або систем.
ТФ Г РН 3	Виконання аналізу системи безпеки та її ризиків, перегляд безпеки архітектури, управління ризиками з наданням відповідних рекомендацій, даних та документів для включення в стратегію зниження ризиків та розробку плану управління ризиками.
ТФ Є РН 4	Нагляд за дотриманням належного опису, оновленню та документуванню діяльності, проектування та розвитку кібербезпеки, зокрема безпеки прикладної системи, системи та мережі, а також керування пакетами документів з акредитації.

2. НАВЧАЛЬНІ МОДУЛІ ПРОГРАМИ

Модуль 1. СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Змістовний модуль 1. Система менеджменту інформаційної безпеки організації.

Основи і принципи побудови СМІБ **(**А2.З1, А2.З3, Б2.З2, Б3.З1, В4.З4, Г4.З1, Г5.З3). Планування та розроблення СМІБ (А2.З6, В1.З5, В2.З8, В3.З2, В4.З6, В4.З7, Г1.З7). Реалізація та функціонування СМІБ (В1.З2, В1.З3, В1.З4, В2.З7, В3.З2, Г2.З1). Моніторинг, аналіз і вдосконалення СМІБ (В2.З5, В3.З1, В3.З4, В4.З3, Г3.З1).

Самостійна робота. Побудувати план розробки та впровадження СМІБ в організації. Сформувати політики інформаційної безпеки різних класів (1-3 рівнів), як складових СМІБ організації. Побудувати таблицю менеджменту інформаційних ресурсів організації. Скласти порядок розрахунку та аналізу ризиків за визначеним методом (кількісний або якісний). Вивчення нормативно-правової бази та передової практики щодо системи менеджменту інформаційної безпеки організації.

Модуль 2. АНАЛІЗ ПРОЦЕСІВ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Змістовний модуль 1. Криптологія та криптоаналіз.

Принципи побудови сучасних криптосистем (А3.З1, Г4.32). Концепція симетричних криптосистем (А3.З1, Г4.32). Концепція криптосистем з відкритим ключем (двоключових криптосистем) (А3.З1, Г4.32). Алгоритми засновані на перетвореннях у групах точок еліптичних кривих (А3.З1, Г4.32).

Самостійна робота. Афінне перетворення алгоритму Rijndael. Рішення задач згідно з індивідуальним завданнями. Проблема автентифікації даних та електронний підпис. Алгоритм RSA, Ель-Гамаля, Рішення задач згідно з індивідуальним завданнями. Математика у групі точок еліптичних кривих. Рішення задач згідно з індивідуальним завданнями. Криптоаналіз асиметричних криптосистем. Рішення задач згідно з індивідуальним завданнями. Вивчення питань стосовно тестування чисел на простоту та побудови великих простих чисел для криптографічних застосувань. Вивчення сучасних тенденцій розвитку криптографії у постквантовий період.

Змістовний модуль 2. Безпечне програмне забезпечення.

Роль безпеки у розробленні програмного забезпечення (А1.37, А1.35, А2.34, Б2.31, Б2.38, В2.32, Б2.35, В2.38, Г3.34). Механізми захисту процесора та операційної системи від переповнення буфера (А1.37, А2.34, Б2.31, Б2.38, В2.34, Г3.34). Цілочисельні переповнення, вразливості форматних рядків (А1.37, В2.38, Б2.38, Г2.34). Потенційно вразливі конструкції в небезпечних мовах програмування (В2.38, Г2.34, Г3.34). Моделі і методи управління безпекою (Б1.35, Б2.37, В3.32, В1.32, Г5.32). Принципи проведення оцінки захищеності мереж

(А2.34, А3.33, Б1.34, В2.36, В3.35, В4.35, Г4.33).

Самостійна робота. Програмна реалізація: переповнення буфера та методи його запобігання, включаючи покращення вихідного коду. Програмна реалізація: цілочисельні та символьні (рядкові) переповнення та методи їх усунення. Сучасні тенденції розробки безпечного програмного забезпечення.

Модуль 3. ПРАВОВІ ТА ПСИХОЛОГІЧНІ ЗАСАДИ ОБІГУ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРБЕЗПЕКИ

Змістовний модуль 1. Правові та психологічні засади обігу інформації, інформаційної безпеки та кібербезпеки інформаційних ресурсів.

Нормативно-правове забезпечення інформаційної безпеки, кібербезпеки та захисту інформації в Україні (Б2.З4, Г6.З1). Нормативно-правове забезпечення кібербезпеки та захисту інформації й захист приватності в кіберпросторі (Г6.З1). Особливості кіберзахисту критичної інфраструктури України (секторальний підхід) та повноваження правоохоронних органів в цій сфері. (В3.З7, Г1.З4, Г6.З2). Загальні засади юридичної відповідальності. Види відповідальності за порушення законодавства у сфері обігу інформації, інформаційної безпеки та кібербезпеки. (Б2.З4, Г1.З4). Кримінальна відповідальність за порушення законодавства у сфері обігу інформації, інформаційної безпеки та кібербезпеки (Б2.З4, Г1.З4). Моральні та психологічні засади захисту інформації та етичного хакінгу. Психологічні основи інформаційної безпеки та кібербезпеки (Г6.З1).

Самостійна робота. Закони, політики та процедури, що стосуються кібербезпеки об’єктів критичної інфраструктури (В3.З7, Г6.З2). Сучасна система нормативно-правового забезпечення побудови та атестації комплексних систем безпеки організацій різних форм власності (В3.З7). Закон України № 4336-IX від 27.03.25р. «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури». Відповідно до повного переліку літератури освітньої програми.

3. НАВЧАЛЬНИЙ ПЛАН ЗА МОДУЛЯМИ ОРІЄНТОВАНИЙ РОЗПОДІЛ ГОДИН ЗА ВИДАМИ НАВЧАННЯ

3.1. Система менеджменту інформаційної безпеки

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	МК	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
Змістовний модуль 1. Система менеджменту інформаційної безпеки організації						
1.1 Основи і принципи побудови СМІБ (А2.З1, А2.З3, Б2.З2, Б3.З1, В4.З4, Г4.З1, Г5.З3). Поняття та значення СМІБ. Цілі, завдання та функції СМІБ. Принципи побудови СМІБ (системний, процесний, ризик-орієнтований підхід). Цикл PDCA (Plan-Do-Check-Act). Взаємозв'язок підходів побудови СМІБ з циклом PDCA. Взаємозв'язок СМІБ із іншими системами менеджменту.	**8**	**4**				**4**
1.2 Планування та розроблення СМІБ (А2.З6, В1.З5, В2.З8, В3.З2, В4.З6, В4.З7, Г1.З7). Визначення контексту організації. Формування політики інформаційної безпеки. Ідентифікація та класифікація інформаційних активів. Оцінювання ризиків інформаційної безпеки. Планування оброблення ризиків. Розроблення структури та документації СМІБ. План розробки та впровадження СМІБ.	**12**	**4**		**2**		**6**
1.3 Реалізація та функціонування СМІБ (В1.З2, В1.З3, В1.З4, В2.З7, В3.З2, Г2.З1). Впровадження політики інформаційної безпеки. Управління доступом і користувачами. Управління технічними та організаційними контролями. Управління ризиками інформаційної безпеки. Моніторинг безпеки та контроль ефективності. Документування та управління записами СМІБ. Навчання, підготовка та підвищення компетентності персоналу. Засоби реалізації та підтримки функціонування СМІБ.	**10**	**4**		**2**		**4**
1.4 Моніторинг, аналіз і вдосконалення СМІБ (В2.З5, В3.З1, В3.З4, В4.З3, Г3.З1). Система моніторингу інформаційної безпеки. Оцінювання результативності та ефективності СМІБ. Внутрішній аудит СМІБ. Управлінський огляд СМІБ. Аналіз невідповідностей і коригувальні дії. Управління змінами та розвиток СМІБ. Постійне вдосконалення СМІБ.	**8**	**4**				**4**
Самостійна робота / практичне завдання						
Самостійна робота 1.1. Побудувати план розробки та впровадження СМІБ в організації.	**1**					**1**
Самостійна робота 1.2. Сформувати політики інформаційної безпеки різних класів (1-3 рівнів), як складових СМІБ організації.	**1**					**1**
Самостійна робота 1.3. Побудувати таблицю менеджменту інформаційних ресурсів організації.	**1**					**1**
Самостійна робота 1.4. Скласти порядок розрахунку та аналізу ризиків за визначеним методом (кількісний або	**1**					**1**

якісний).						
Самостійна робота / теоретична складова						
Самостійна робота 1.5. Вивчення нормативно-правової бази та передової практики щодо системи менеджменту інформаційної безпеки організації	**6**					**6**
Всього годин за модуль 1	**48**	**16**	**0**	**4**	**0**	**28**
Модульна контрольна робота за Частиною 1	**2**	**0**	**0**	**0**	**2**	**0**
Всього годин за Частиною 1	**50**	**16**	**0**	**4**	**2**	**28**

3.2. Аналіз процесів управління інформаційною безпекою.

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	МК	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
Змістовний модуль 1. Криптологія та криптоаналіз						
1.1 Принципи побудови сучасних криптосистем (А3.31, Г4.32). Основні поняття та означення інформаційної безпеки. Актуальність та важливість забезпечення інформаційної безпеки. Типи загроз безпеці автоматизованої системи обробки інформації. Основні поняття та позначення. Структурна схема та математична модель системи КЗІ. Принципи криптографічного захисту інформації. Основні групи шифрів. Криптографія та криптоаналіз, шифрування, розшифрування, ключ, основні типи шифрів, вимоги до шифрів, схема однобічного каналу захищеної передачі інформації.	**8**	**4**				**4**
1.2 Концепція симетричних криптосистем (А3.31, Г4.32). Найпростіші шифри заміни та перестановки. Моноалфавітні та поліалфавітні шифри. Багатоалфавітні криптосистеми. Математичні алгоритми, які найчастіше використовуються в криптографії. Класичні симетричні криптосистеми. Блоковий симетричний шифр DES та режими його роботи. Основні типи перетворень, що використовуються в перспективних симетричних криптосистемах. Блоковий симетричний шифр AES. Структура алгоритму. Генерування ключів. Використання алгоритму в різних режимах.	**10**	**6**				**4**
1.3 Концепція криптосистем з відкритим ключем (двоключових криптосистем) (А3.31, Г4.32). Класичні двоключові Алгоритми RSA та Ель Гамала в режимі шифування. Проблема аутентифікації даних та електронний цифровий підпис. Геш функції. Вимоги до них. Процедура постановки та перевірки підпису. Алгоритми RSA та Ель Гамала в режимі ЕЦП. Загальні відомості відносно методів криптоаналізу двохключових криптосистем. Алгоритми факторизації. Алгоритми Поларда та ρ-1 Поларда. Загальні відомості відносно методів криптоаналізу двохключових криптосистем. Алгоритми факторизації. Алгоритми Ферма та Діксона.	**10**	**4**		**2**		**4**

1.4 Алгоритми засновані на перетвореннях у групах точок еліптичних кривих (А3.31, Г4.32). Поняття про еліптичні криві. Математика у групі точок еліптичних кривих. Види ЕК. Поняття та визначення. Додавання та подвоєння точок. Прядок кривої та порядок точки кривої. Сліди та базиси розширеного поля. Поліноміальний та нормальний базиси. Математика. Надання кривій у різних координатних системах. Оптимальний нормальний базис розширеного поля та його переваги. Перехід від поліноміального базису до нормального. Добуток елементів у нормальному базисі. Переваги нормального базису. Дискретне логарифмування у групі точок ЕК.	**10**	**4**		**2**		**4**
Самостійна робота / практичне завдання						
Самостійна робота 1.1. Афінне перетворення алгоритму Rijndael. Рішення задач згідно з індивідуальним завданнями.	**4**					**4**
Самостійна робота 1.2. Проблема автентифікації даних та електронний підпис. Алгоритм RSA, Ель-Гамаля, Рішення задач згідно з індивідуальним завданнями.	**2**					**2**
Самостійна робота 1.3. Математика у групі точок еліптичних кривих. Рішення задач згідно з індивідуальним завданнями.	**4**					**4**
Самостійна робота 1.4. Криптоаналіз асиметричних криптосистем. Рішення задач згідно з індивідуальним завданнями.	**2**					**2**
Самостійна робота / теоретична складова						
Самостійна робота 1.5. Вивчення питань стосовно тестування чисел на простоту та побудови великих простих чисел для криптографічних застосувань.	**2**					**2**
Самостійна робота 1.6. Вивчення сучасних тенденцій розвитку криптографії у постквантовий період.	**2**					**2**
Всього годин за модулем 1	**54**	**18**	**0**	**4**	**0**	**32**
Змістовний модуль 2. Безпечне програмне забезпечення						
2.1. Роль безпеки у розробленні програмного забезпечення (А1.37, А1.35, А2.34, Б2.31, Б2.38, В2.32, Б2.35, В2.38, Г3.34). Основи безпеки програмного забезпечення (поняття, принципи та значення безпечного програмування). Життєвий цикл розроблення ПЗ з урахуванням безпеки – інтеграція вимог безпеки на всіх етапах створення програм. Типові вразливості програмного забезпечення та способи запобігання їх виникненню. Методи та інструменти забезпечення безпечного коду. Тестування та аудит безпеки програмного забезпечення. Стандарти, політики та найкращі практики безпечного програмування.	**6**	**4**				**2**
2.2. Механізми захисту процесора та операційної системи від переповнення буфера (А1.37, А2.34, Б2.31, Б2.38, В2.34, Г3.34).	**4**	**2**				**2**

Вступ до переповнення буфера та його наслідків (поняття, типи буферних переповнень і їхній вплив на безпеку системи). Апаратні механізми захисту процесора (NX/DEP-біти, сегментація пам'яті, контроль стеку та стекові канарки). Захист на рівні операційної системи (ASLR (Address Space Layout Randomization), контроль доступу до пам'яті, обмеження прав процесів. Комп'ютерні та компіляційні техніки захисту (перевірка розмірів буфера, захищені функції стандартних бібліотек, статичний аналіз коду). Детектування та реагування на атаки (механізми спостереження за переповненням буфера, логування подій та аварійне завершення процесів).						
2.3. Цілочисельні переповнення, вразливості форматних рядків (А1.37, В2.38, Б2.38, Г2.34). Поняття та причини виникнення цілочисельних переповнень. Наслідки цілочисельних переповнень для безпеки програмного забезпечення. Методи виявлення та запобігання цілочисельним переповненням. Вразливості форматних рядків: сутність і принцип дії. Експлуатація вразливостей форматних рядків. Захист від переповнень і вразливостей форматних рядків.	**4**	**2**				**2**
2.4. Потенційно вразливі конструкції в небезпечних мовах програмування (В2.38, Г2.34, Г3.34). Вказівники та арифметика вказівників. Буферні переповнення та робота з рядками (класичні вразливості при використанні небезпечних функцій для копіювання/формування рядків). Керування пам'яттю: вручну виділення і звільнення (помилки use-after-free, double-free, витікання пам'яті і неправильне вирівнювання). Неозначена поведінка та небезпечні перетворення типів. Вразливості, пов'язані з форматними специфікаторами та небезпечними API. Помилки конкурентності, відсутність коректної синхронізації і наслідки для цілісності даних.	**4**	**2**				**2**
2.5. Моделі і методи управління безпекою (Б1.35, Б2.37, В3.32, В1.32, Г5.32). Основи управління інформаційною безпекою (поняття, цілі, принципи та складові системи управління безпекою). Моделі управління доступом. Методи оцінювання ризиків і загроз безпеці. Політики, процедури та стандарти управління безпекою. Моніторинг, аудит і вдосконалення системи безпеки (оцінювання ефективності заходів, аудит подій і безперервне покращення). Організаційні та технічні методи управління безпекою.	**6**	**4**				**2**
2.6. Принципи проведення оцінки захищеності мереж (А2.34, А3.33, Б1.34, В2.36, В3.35, В4.35, Г4.33). Основи оцінювання захищеності мереж (мета, завдання, етапи та ключові поняття процесу оцінки безпеки). Методи аналізу вразливостей мережевої інфраструктури (ручні й автоматизовані підходи до виявлення слабких місць у мережі). Інструменти сканування та тестування мережевої безпеки. Проведення тестів на проникнення (penetration testing) (етапи, техніки, сценарії атак і документування	**8**	**2**		**2**		**4**

результатів). Оцінювання ефективності засобів захисту мережі. Звітність та рекомендації за результатами оцінки.						
Самостійна робота / практичне завдання						
Самостійна робота 2.1. Програмна реалізація: переповнення буфера та методи його запобігання, включаючи покращення вихідного коду.	**4**					**4**
Самостійна робота 2.2. Програмна реалізація: цілочисельні та символьні (рядкові) переповнення та методи їх усунення.	**4**					**4**
Самостійна робота / теоретична складова						
Самостійна робота 2.3. Сучасні тенденції розробки безпечного програмного забезпечення.	**2**					**2**
Всього годин за модулем 2	**42**	**16**	**0**	**2**	**0**	**24**
Модульна контрольна робота за Частиною 2	**2**	**0**	**0**	**0**	**2**	**0**
Всього годин за Частиною 2	**98**	**34**	**0**	**6**	**2**	**56**

3.3. Правові та психологічні засади обігу інформації, інформаційної безпеки та кібербезпеки

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	МК	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
Змістовний модуль 1. Правові та психологічні засади обігу інформації, інформаційної безпеки та кібербезпеки інформаційних ресурсів						
1.1 Нормативно-правове забезпечення інформаційної безпеки, кібербезпеки та захисту інформації в Україні (Б2.З4, Г6.З1).	**3**	**2**				**1**
1.2 Нормативно-правове забезпечення кібербезпеки та захисту інформації й захист приватності в кіберпросторі (Г6.З1).	**4**	**2**				**2**
1.3 Особливості кіберзахисту критичної інфраструктури України (секторальний підхід) та повноваження правоохоронних органів в цій сфері. (В3.З7, Г1.З4, Г6.З2)	**3**	**2**				**1**
1.4 Загальні засади юридичної відповідальності. Види відповідальності за порушення законодавства у сфері обігу інформації, інформаційної безпеки та кібербезпеки. (Б2.З4, Г1.З4)	**3**	**2**				**1**
1.5 Кримінальна відповідальність за порушення законодавства у сфері обігу інформації, інформаційної безпеки та кібербезпеки (Б2.З4, Г1.З4)	**3**	**2**				**1**
1.6 Моральні та психологічні засади захисту інформації та етичного хакінгу.	**3**	**2**				**1**
1.7 Психологічні основи інформаційної безпеки та кібербезпеки (Г6.З1).	**3**	**2**				**1**
Самостійна робота / практичне завдання						
Самостійна робота 1.1. Закони, політики та процедури, що стосуються кібербезпеки об'єктів критичної інфраструктури (**В3.З7, Г6.З2**).	**1**					**1**
Самостійна робота 1.2. Сучасна система нормативно-правового забезпечення побудови та атестації	**1**					**1**

комплексних систем безпеки організацій різних форм власності (**В3.37**).						
Самостійна робота / теоретична складова						
Самостійна робота 1.3. Закон України № 4336-IX від 27.03.25р. «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури».	**1**					**1**
Самостійна робота 1.4. Відповідно до повного переліку літератури освітньої програми.	**1**					**1**
Модульна контрольна робота за Частиною 3	**2**	**0**	**0**	**0**	**2**	**0**
Всього годин за частиною 3	**28**	**14**	**0**	**0**	**2**	**12**
Консультація з контрольної роботи у виді комп'ютерного оцінювання	**2**	**0**	**0**	**0**	**2**	**0**
Контрольна робота у виді комп'ютерного оцінювання	**2**	**0**	**0**	**0**	**2**	**0**
Всього годин за програмою	**180**	**64**	**0**	**10**	**10**	**96**

4. ОСНОВНІ МЕТОДИ НАВЧАННЯ

Під час викладання передбачено застосування наступних форм.

Лекція – логічно довершений, науково обґрунтований та систематизований виклад певного наукового або науково-педагогічного питання, ілюстрований засобами наочності та демонстрацією результатів досліджень.

Лекція є одним із основних видів і, водночас, методів проведення навчальних занять, призначених для засвоєння теоретичного матеріалу. Вона закладає основи наукових знань, визначаючи напрям, основний зміст та характер усіх видів навчальних занять, а також, головним чином, самостійної роботи здобувачів вищої освіти.

Практичне заняття – форма навчального заняття, на якому у здобувача вищої освіти під керівництвом викладача формуються вміння та навички практичного застосування теоретичних положень навчальної дисципліни шляхом виконання здобувачем вищої освіти відповідно сформульованих завдань.

Практичні заняття проводяться в аудиторії, оснащеною комп'ютерною технікою та технічними засобами навчання.

Практичне заняття включає в себе: проведення викладачем контролю знань, вмінь та навичок здобувачів вищої освіти, постановку загальної проблеми (завдання) та її обговорення за участю здобувачів вищої освіти, розв'язування завдань та їх обговорення, виконання контрольних завдань, їх перевірку та оцінювання викладачем.

Консультація – форма навчального заняття, на якому здобувач вищої освіти отримує від викладача відповіді на конкретні запитання або пояснення окремих теоретичних положень та їх використання на практиці.

Самостійна робота забезпечується навчально-методичними засобами, передбаченими для вивчення навчальної дисципліни: підручниками, навчально-

методичними посібниками, конспектами лекцій, практикумами, електронно-обчислювальною технікою тощо.

Самостійна робота над засвоєнням навчального матеріалу може виконуватися в бібліотеці, комп'ютерному класі.

Форми самостійної роботи здобувачів вищої освіти:

- опрацювання теоретичних основ прослуханого лекційного матеріалу;
- вивчення окремих тем або питань, передбачених для самостійного опрацювання;
- виконання різних за формою і змістом завдань;
- підготовка до практичних занять;
- підготовка до поточного, модульного та підсумкового контролю знань;
- пошук та огляд літературних джерел за проблематикою навчальної дисципліни;
- виконання індивідуальних завдань (написання курсової роботи);
- аналітичний розгляд наукової публікації тощо.

Методи навчання:

– під час проведення лекційних занять – лекція-діалог, бесіда, а також наочних методів навчання, зокрема використання мультимедійних презентацій. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії;

– під час проведення практичних занять – використання роздаткового матеріалу, нормативно-правові акти.

5. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Результати навчання можуть оцінюватись за формами:

- стандартною формою;
- комп'ютерне оцінювання знань на базі автоматизованої системи тестування.

5.1 Форма 1. Стандартна форма

Результати навчання слухача з навчальної дисципліни оцінюються за 100-бальною шкалою як сума балів поточного та підсумкового контролю із застосуванням наступних вагових коефіцієнтів, загальна сума яких дорівнює 1:

Вид контролю	Ваговий коефіцієнт
Поточний контроль (К)	**0,6**
Підсумковий контроль (ПК)	**0,4**

Підсумкова семестрова оцінка (ПСО) обчислюється за формулою:
ПСО=К+ПК

5.2. Складниками для обчислення балу поточного контролю є:

Види навчальної діяльності	Мах кількість балів
Частина №1	
Виконання та захист одного практичного заняття *(Для допуску до виконання модульної контрольної роботи здобувач має набрати **не менше 18 балів**)*	15
Усього за частиною №1	30
Частина №2	
Виконання та захист одного практичного заняття *(Для допуску до виконання модульної контрольної роботи здобувач має набрати **не менше 22 балів**)*	12
Усього за частиною №2	36
Частина №3	
Виконання та захист практичного завдання самостійної роботи *(Для допуску до виконання модульної контрольної роботи здобувач має набрати **не менше 8 балів**)*	14
Усього за частиною №3	14
Усього за частинами №1, №2, №3	**80**
Комп'ютерне тестування	**20**
Усього за дисципліною	**100**

Мінімальна кількість балів для допуску до підсумкового контролю 48 балів.

5.3. Шкала оцінювання

Оцінка за шкалою ЄКТС	Оцінка за 100-бальною шкалою	Значення оцінки
A	90-100	*Відмінно – відмінне виконання лише з незначною кількістю помилок.* Здобувач виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили.
B	84-89	*Дуже добре – вище середнього рівня, але з кількома помилками.* Здобувач вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв'язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна
C	75-83	*Добре – загалом правильна робота, але з певною кількістю помилок.* Здобувач вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок.
D	65-74	*Задовільно – непогано, але зі значною кількістю недоліків*. Здобувач відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою

		викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих.
E	60-64	*Достатньо – виконання задовольняє мінімальні вимоги.* Здобувач володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.
FX	35-59	*Незадовільно – потрібна додаткова робота.* Здобувач володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу
F	1-34	*Незадовільно – потрібна значна додаткова робота.* Здобувач володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів.

5.4 Форма 2. Комп'ютерного оцінювання (далі - КО): форма – очна на базі автоматизованої системи тестування (далі – АСТ) мережі Кваліфікаційного центру, формат – електронний.

Для проведення КО побудовано Банк запитань/тестів довжиною 120 запитань у відповідності до узагальненої програми процедури оцінювання з професійної кваліфікації «Фахівець з оцінки заходів захисту інформації (кібербезпеки) (трудові функції А, Б, В, Г)» професійного стандарту «Фахівець з оцінки заходів захисту інформації (кібербезпеки)».

До одного варіанту тесту входить 40 тестових запитань.

Розподіл запитань між змістовними блоками та перекриття усіх трудових функцій професійної кваліфікації представлено у Таблиці 1. У Таблиці 1 параметр «Питома вага розділу» вказує відсоток, який слугує орієнтиром для обрання кількості тестових запитань відповідного розділу. Параметр «Кількість запитань у варіанті тесту» вказує, скільки запитань повинно бути включено до варіанту тесту за відповідною трудовою функцією. Параметр «Кількість запитань у Банку запитань» вказує, скільки запитань з загальної кількості відносяться до певної трудової функції.

При формуванні контрольно-вимірювальних матеріалів відповідно до Порядку присвоєння\підтвердження та цього Регламенту повинно бути забезпечено включення відповідної кількості тестів, які відносяться до кожної трудової функції. Таким чином, забезпечується покриття всіх 100% включених до професійної кваліфікації відповідного стандарту трудових функцій.

Усі завдання з загального Банку завдань мають різний рівень складності (від 1 до 3). На відповідь рівня складності 1 відводиться 1 хвилина, рівня 2 – 3 хвилини, рівня 3 – 5 хвилин.

Варіант тесту складається з 40 запитань. Розподіл запитань за трудовими функціями/змістовними розділами представлено у Таблиці 1. З 40 запитань 24 запитання мають рівень складності 1, 14 запитання рівень складності 2, 3 запитань – рівень складності 3.

На проходження варіанту тесту здобувачеві виділяється 1 година 20 хвилин:

$$23*1+14*3+3*5 = 80 \text{ хв.}$$

Таблиця 1

Відповідність Банку завдань та варіанту тесту професійної кваліфікації

Трудова функція	Найменування розділу	Питома вага розділу	Кількість запитань у варіанті тесту	Кількість запитань у Банку завдань
	Теоретичний модуль тестування знань	**60%**	**24**	**72**
А	Оцінювання ефективності засобів контролю безпеки, зокрема огляд авторизації безпеки та аудит зовнішніх послуг. Розробка кейсів впевненості та огляд авторизації безпеки.	14%	6	18
Б	Оцінювання дотримання заходів забезпечення відповідності, у тому числі з аналізом процесів управління конфігураціями та дотриманням встановлених обмежень прикладного програмного забезпечення, мереж або систем.	15%	6	18
В	Виконання аналізу системи безпеки та її ризиків, перегляд безпеки архітектури, управління ризиками з наданням відповідних рекомендацій, даних та документів для включення в стратегію зниження ризиків та розробку плану управління ризиками.	21%	8	24
Г	Нагляд за дотриманням належного опису, оновленню та документуванню діяльності, проектування та розвитку кібербезпеки, зокрема безпеки прикладної системи, системи та мережі, а також керування пакетами документів з акредитації.	10%	4	12
	Практичний модуль тестування навичок та вмінь	**40%**	**16**	**48**
А	Оцінювання ефективності засобів контролю безпеки, зокрема огляд авторизації безпеки та аудит зовнішніх послуг. Розробка кейсів впевненості та огляд авторизації безпеки.	10%	4	12
Б	Оцінювання дотримання заходів забезпечення відповідності, у тому числі з аналізом процесів управління конфігураціями та дотриманням встановлених обмежень прикладного програмного забезпечення, мереж або систем.	10%	4	12

Трудова функція	Найменування розділу	Питома вага розділу	Кількість запитань у варіанті тесту	Кількість запитань у Банку завдань
В	Виконання аналізу системи безпеки та її ризиків, перегляд безпеки архітектури, управління ризиками з наданням відповідних рекомендацій, даних та документів для включення в стратегію зниження ризиків та розробку плану управління ризиками.	14%	7	21
Г	Нагляд за дотриманням належного опису, оновленню та документуванню діяльності, проектування та розвитку кібербезпеки, зокрема безпеки прикладної системи, системи та мережі, а також керування пакетами документів з акредитації.	6%	1	3
			40	**120**

Система оцінювання. Оцінювання складається з двох частин: Теоретичний модуль (60%) та Практичний модуль (40%). Теоретична частина та практична частина оцінюється одночасно.

Кожне з 40 завдань одного варіанту тесту вважається зарахованим, якщо відповідь вірна та повна, або не зарахованим, якщо відповідь не вірна або неповна.

Оцінювання вважається зараховано за умови не менше 75% правильних відповідей.

За результатами проведених процедур оцінювання комісія ухвалює одне з таких рішень, що відображається у протоколі та подається для затвердження Кваліфікаційним центром інформаційних технологій та кібербезпеки Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації:

- визнати результати навчання, присвоїти/підтвердити повну професійну кваліфікації. Теоретичні знання та практичні навички відповідають критерію не менше 75%;

- відмовити у присвоєнні/підтвердженні повної/часткової професійної кваліфікації. Теоретичні та практичні знання не відповідають критерію - не менше 75%.

6. РЕСУРСНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Основна література:

1. Богуш В. М., Бровко В. Д., Настрадін В. П. Кіберпростір: основи кібербезпеки та кіберзахисту : навч. посіб. У 3 ч. Ч.3. Основи кіберзахисту. Київ : Нац. акад. СБУ, 2020. 72 с.

2. Левченко О. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія. Житомир : Євро-Волинь, 2021. 172 с.

3. Когут Ю. І. Кібервійна та безпека об’єктів критичної інфраструктури : Практ. посібник. Київ : Консалтингова компанія "СІДКОН", 2021. 332 с.

4. Організаційно-правові основи забезпечення кібербезпеки підруч. / М. В. Гуцалюк, А. І. Марущак, Д. С. Мельник [та ін.]; За заг. ред. М. М. Присяжнюка Київ : Наук.-вид. відділ НА СБ України, 2023. 320 с.

Допоміжна література:

5. Бурячок В. Л., Аносов А. О., Семко В. В., Соколов В. Ю., Складанний П. М. Технології забезпечення безпеки мережевої інфраструктури : підруч. Київ : КУБГ, 2019. 218 с.

6. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп’ютерних системах : підруч. Ніжин: ФОП Лук’яненко В. В., ТПК «Орхідея», 2020. 236 с.

7. Козачок В. А., Гайдур Г. І., Гахов С. О., Хмелевський Р. М., Чумак Н. С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів Київ: ДУТ ННІЗІ, 2020. 167 с.

<u>Базові Стандарти</u>

1. ДСТУ ISO\IEC 9000 \ 9001: 2015. Системи менеджменту якості.

2. ДСТУ ISO\IEC 17021. Оцінка відповідності. Вимоги до органів, що здійснюють аудит і сертифікацію систем менеджменту.

3. ДСТУ ISO\IEC 17024. Оцінка відповідності. Загальні вимоги до органів по атестації персоналу. Схема сертифікації персоналу.

4. ДСТУ ISO\IEC 27001.

5. ДСТУ ISO / IEC 27002. Кодекс поведінки для перевірок інформаційної безпеки.

6. ДСТУ ISO / IEC 27003. Керівництво з впровадження СУІБ.

7. ДСТУ ISO / IEC 27004. Управління інформаційною безпекою – вимірювання.

8. ДСТУ ISO / IEC 27005. Управління ризиками інформаційної безпеки.

9. ДСТУ ISO / IEC 27006. Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою.

10. ДСТУ ISO / IEC 27007. Інструкції з перевірки СУІБ.

11. ДСТУ ISO / IEC TR 27008. Рекомендації для аудиторів перевірок інформаційної безпеки.

12. ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології. Методи захисту. Критерії оцінки ч.1-5. Вступ та загальна модель (ISO/IEC 15408-1:2009, IDT).

13. ISO/IEC 15504 Information technology. Process assessment \ Інформаційні технології. Оцінка процесів ч.1-10.

14. COBIT 5 \ SACA. Control Objectives for Information and Related Technology \ Контрольні об’єкти інформаційних та суміжних технологій).

15. ITAF \Information Technology Assurance Framework ISACA. Основні положення професійної практики аудиту та підтвердження довіри до ІС. Стандарт ITAF.

16. ITIL \ IT Infrastructure Library. Бібліотека інфраструктури інформаційних технологій.

17. Prince2 v.3. Проекти в контрольованому середовищі.

Інформаційні ресурси:

1. https://www.mathcad.com/en/education
2. www.zakon.rada.gov.ua
3. http://cert.gov.ua/