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 РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ

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

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

категорія слухачів: молодший фахівець з реагування на інциденти кібербезпеки (трудові функції А, Б, В),
фахівець з реагування на інциденти кібербезпеки (трудові функції А, Б, В, Г, Д, Е),
провідний фахівець з реагування на інциденти кібербезпеки (трудові функції А, Б, В, Г, Д, Е, Є)
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;
- директорка Центру якості освіти, ліцензування та акредитації Національного аерокосмічного університету «ХАІ», к.т.н., доцентка Е.А. Дармофал;
- професор кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету «ХАІ», д.т.н., професор Г.В. Фесенко;
- завідувач кафедри права Національного аерокосмічного університету «ХАІ», д.ю.н., професор В.І. Павликівський;
- 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

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 реагування на інциденти кібербезпеки» розроблена у відповідності до Типової програми підвищення кваліфікації «Фахівець з реагування на інциденти кібербезпеки», Розділу ІІІ професійного стандарту «Фахівець з реагування на інциденти кібербезпеки» та Національного класифікатора України ДК 003:2010 «Класифікатор професій» («Фахівець з реагування на інциденти кібербезпеки»), 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. У сучасному світі, де інформація є цінним активом, фахівець з реагування на інциденти кібербезпеки є професіонал, який аналізує, запобігає та усуває наслідки кібератак; він діє як "кібер-детектив", розслідуючи атаки, збираючи докази, відновлюючи системи та мінімізуючи шкоду, щоб захистити цифрову інфраструктуру та дані від загроз. У зв’язку з цим актуалізується проблема розвиту професійних компетентностей фахівців з реагування на інциденти кібербезпеки. Фахівці з реагування на інциденти кібербезпеки мають вільно та ґрунтовно забезпечувати комплексний захист інформаційних систем, виявляти, аналізувати, локалізувати та усувати кіберзагрози, а також відновлювати нормальну роботу систем після інцидентів. Це включає встановлення патчів, зміну паролів, моніторинг активності зловмисника, розробку сценаріїв протидії та постійний аналіз журналів подій, щоб запобігти повторним атакам та забезпечити цілісність даних.

ОСНОВНІ ЗАВДАННЯ ПРОГРАМИ

– використовувати на практиці нормативні документи в галузі реагування на інциденти кібербезпеки;

– відстежувати, збирати та документувати дані про інциденти кібербезпеки;

– проводити оцінку інцидентів кібербезпеки;

– обробляти інциденти кібербезпеки в режимі реального часу та вживати заходів щодо пом'якшення їх наслідків;

– здійснювати відновлення функціональності системи та процесів до робочого стану після інцидентів кібербезпеки;

– здійснювати моніторинг та оцінку поточного стану кібербезпеки;

– надавати експертну технічну підтримку з управління інцидентами кібербезпеки;

– досліджувати та аналізувати інциденти кібербезпеки.

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ «Фахівець з реагування на інциденти 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	молодший фахівець з реагування на інциденти кібербезпеки (трудові функції А, Б, В), фахівець з реагування на інциденти кібербезпеки (трудові функції А, Б, В, Г, Д, Е), провідний фахівець з реагування на інциденти кібербезпеки (трудові функції А, Б, В, Г, Д, Е, Є)
Термін та обсяг Програми	2 тижні / 180 год. (6 кредитів ECTS)
Професійна кваліфікація	фахівець з реагування на інциденти кібербезпеки (трудові функції А, Б, Г, Д, Е)
Мета Програми	
Формування у здобувачів курсів системи професійних знань, вмінь та навичок щодо організації і супроводу процесів проведення аналізу, оцінки інцидентів кібербезпеки в рамках мережевого середовища та реагування на них. Усунення інцидентів кібербезпеки та пом'якшення їх наслідків. Відстеження, оцінка стану кібербезпеки систем та своєчасне повідомлення про інциденти кібербезпеки. Відновлення функціональності систем і процесів до робочого стану. Дослідження та аналіз заходів реагування, оцінка ефективності та покращення існуючих практик. Накопичення та проведення аналізу даних про кіберзагрози.	
Функціональна спрямованість	Функціональна спрямованість фахівців з реагування на інциденти кібербезпеки полягає в аналізі, оцінці, локалізації та усуненні кібератак і інцидентів, а також відновленні нормальної роботи систем, моніторингу кіберзагроз та постійного вдосконалення захисту для запобігання майбутнім атакам, що охоплює технічну, організаційну та правову складові кіберзахисту. Ці фахівці виконують роль аналітиків, інженерів, розслідувачів та консультантів, працюючи в національних системах обміну інформацією про інциденти, галузевих та корпоративних командах CSIRT.
Фокус програми	Фокус програм фахівців з реагування на інциденти кібербезпеки зосереджений на підготовці експертів, які можуть виявляти, аналізувати, локалізовувати та усувати кіберзагрози, використовуючи технічні знання з

	мережевих протоколів, операційних систем, криптографії та інструментів безпеки, з метою відновлення нормальної роботи систем, збору доказів для розслідування та впровадження профілактичних заходів для захисту інформації.
Орієнтація програми	Програма орієнтована на розвиток професійних компетентностей фахівців з реагування на інциденти кібербезпеки
Особливості програми	Програма підвищення кваліфікації з реагування на інциденти кібербезпеки адаптована до національних вимог, зокрема до Професійного стандарту «Фахівець з реагування на інциденти кібербезпеки», фокусується на підготовці до виявлення, аналізу та нейтралізації атак через комплексні технічні навички, розуміння правових аспектів, розробку політик безпеки та управління інцидентами, поєднуючи як проактивні заходи (моніторинг, сканування вразливостей) та реактивні дії (розслідування, аналіз логів, збір доказів), а також комунікацію та роботу з інструментами (SIEM, EDR). 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)	**1. Технічні компетентності** • Розуміння класифікації та аналізу кіберзагроз, тактик зловмисників (TTPs). • Аналіз мережевого трафіку, робота з технологіями виявлення вторгнень (IDS/IPS). • Здатність аналізувати файли журналів з різних джерел (хостів, мережевих пристроїв). • Сканування та розпізнавання вразливостей в системах. • Знання безпеки операційних систем, програмного забезпечення та комп'ютерних мереж. **2. Операційні та управлінські компетентності** • Вміння керувати життєвим циклом інциденту, від виявлення до відновлення. • Застосування стратегій зниження ризиків. • Автоматизація процесів управління даними про загрози. • Забезпечення неперервності бізнесу під час інциденту. **3. М'які навички (Soft Skills)** • Вміння чітко спілкуватися з різними рівнями керівництва та зацікавленими сторонами, включаючи використання протоколів обміну інформацією (наприклад, TLP). • Співпраця з іншими експертами та командами.

	• Здатність аналізувати складні ситуації та знаходити першопричини. • Здатність діяти ефективно в кризових ситуаціях. **4. Знання нормативної бази** • Розуміння правових аспектів кібербезпеки та національних стандартів
Програмні результати навчання	
Програма підвищення кваліфікації «**Фахівець з реагування на інциденти 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	Відстеження, збір та документування даних про інциденти кібербезпеки з моменту їх виявлення до остаточної ідентифікації статусу події
ТФ Б РН 2	Проведення оцінки інцидентів кібербезпеки
ТФ В РН 3	Оброблення інцидентів кіберзахисту в режимі реального часу та вжиття заходів щодо пом’якшення наслідків кібербезпекових інцидентів, а також відновлення функціональності системи та процесів до робочого стану
ТФ Г РН 4	Моніторинг та оцінка поточного стану кібербезпеки
ТФ Д РН 5	Надання експертної технічної підтримки з управління кіберінцидентами
ТФ Е РН 6	Дослідження та аналіз кіберінцидентів

2. НАВЧАЛЬНІ МОДУЛІ ПРОГРАМИ

Модуль 1. СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Змістовний модуль 1. Система менеджменту інформаційної безпеки організації.

Основи і принципи побудови СМІБ **(**Б1.З1, Б1.З2, Г2.З3, Г2.З5, Д2.З1, Г2.З7, Е1.З1, Е1.З6, Е1.З7**).** Планування та розроблення СМІБ (Б1.З1, Б2.З5, В3.З1, Г1.З5, Е1.З6). Реалізація та функціонування СМІБ (Б2.З5, Б2.З5, В1.З1, В1.З1, В3.З1, Д2.З3, Д2.З4, Е1.З8**).** Моніторинг, аналіз і вдосконалення СМІБ **(**А2.З2, А3.З1, А3.З5, А3.З6, Б1.З6, Д2.З2**).**

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. ОРГАНІЗАЦІЯ ТА ЗАБЕЗПЕЧЕННЯ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

Змістовний модуль 1. Організація управління кіберінцидентами.

Основи управління кіберінцидентами **(**Б1.З7, Б1.З9, Б1.З2**).** Організація процесу реагування на кіберінциденти **(**В1.З3, В2.З3, Д2.З5**)**. Процес реагування на кіберінциденти (Б1.З8, Б1.З9, Б2.З6, В1.З3, В1.З2, В1.З3, В1.З4, В1.З5, В2.З3, Д1.З4, Д2.З4, Д2.З5, Е1.З8**)**. Документування, аналіз і запобігання кіберінцидентам **(**Д1.З6, Е1.З1, Е1.З3, Е1.З4, Е1.З5, Е1.З7, Е1.З8**)**.

Самостійна робота. Скласти план управління кіберінцидентами. Вивчення нормативно-правової бази та передової практики з питань організації управління кіберінцидентами.

Змістовний модуль 2. Експлуатація та моніторинг систем захисту.

Життєвий цикл інформаційної системи (Д1.З1, Д2.З3). Принципи та компоненти архітектури безпеки мереж **(**А1.З2, А1.З3, А1.З4, А1.З5, А1.З7, А2.З1, А2.З3, А2.З4, А2.З5, А3.З2, А3.З7, Б1.З3, Б1.З4, Б1.З5, Б2.З1, Б2.З3, Б2.З4, В1.З4, В2.З2, В2.З3, Г1.З2, Г1.З3, Г1.З4, Г1.З7, Г1.З8, Г2.З1, Г2.З2, Д1.З2, Д1.З3, Д1.З5**).** Практичні аспекти проєктування та реалізації архітектури безпеки мереж **(**А1.З1, А1.З6, А1.З7, А3.З2, А3.З3, А3.З4, А3.З7, В2.З4, В3.З3**).** Безперебійність бізнесу та відновлення після аварій **(**В3.З4**).**

Самостійна робота. Скласти повідомлення про кеіберінцидент. Вивчення нормативно-правової бази та передової практики щодо технологічної основи реагування та відновлення після кіберінцидентів.

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.

Міжнародно-правові акти та українське законодавство в сфері забезпечення інформаційної безпеки, кібербезпеки та захисту інформації України. (Б1.З1, Г2.З5, Є1.З1, Є1.З3). Нормативно-правове забезпечення кібербезпеки та конфіденційності персональних даних в кіберпросторі (Б1.З1, Є1.З1, Є1.З3). Особливості кіберзахисту критичної інфраструктури України (секторальний підхід) та повноваження правоохоронних органів в цій сфері. (Б1.З1, Є1.З3). Загальні засади юридичної відповідальності. Види відповідальності за порушення законодавства у сфері обігу інформації, інформаційної безпеки та кібербезпеки. (Г2.З3). Кримінальна відповідальність за порушення законодавства у сфері обігу інформації, інформаційної безпеки та кібербезпеки. Кримінологічна типологія кіберзлочинців (Г1.З2). Моральні та психологічні засади захисту інформації та етичного хакінгу (Б1.З1). Психологічні основи інформаційної безпеки та кібербезпеки (Б1.З1).

Самостійна робота. Закони, політики та процедури, що стосуються кібербезпеки об’єктів критичної інфраструктури (Б1.З1, Г2.З3, Е1.З6). Сучасна система нормативно-правового забезпечення побудови та атестації комплексних систем безпеки організацій різних форм власності (Б1.З1, Г2.З3, Е1.З6). 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 (Б1.З1, Б1.З2, Г2.З3, Г2.З5, Д2.З1, Г2.З7, Е1.З1, Е1.З6, Е1.З7). 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 (Б1.З1, Б2.З5, В3.З1, Г1.З5, Е1.З6). 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 (Б2.З5, Б2.З5, В1.З1, В1.З1, В3.З1, Д2.З3, Д2.З4, Е1.З8). 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 (А2.З2, А3.З1, А3.З5, А3.З6, Б1.З6, Д2.З2). 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 якісний).	**1**					**1**

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. Організація та забезпечення реагування на кіберінциденти

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	МК	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
Змістовний модуль 1. Організація управління кіберінцидентами						
1.1 Основи управління кіберінцидентами (Б1.37, Б1.39, Б1.32). Поняття інциденту, кіберінциденту, події безпеки. Відмінність між подією та інцидентом, критерії ескалації. Життєвий цикл кіберінциденту (від виявлення до усунення). Класифікація кіберінцидентів. Основні принципи управління інцидентами. Міжнародні підходи (ISO/IEC 27035, NIST SP 800-61, ENISA). Типові ролі в управлінні інцидентами (власник інциденту, аналітик, керівник реагування). Значення управління інцидентами для забезпечення кіберстійкості організації.	**10**	**4**				**6**
1.2 Організація процесу реагування на кіберінциденти (В1.33, В2.33, Д2.35). Місце управління кіберінцидентами у структурі СМІБ (ISO/IEC 27001). Взаємозв'язок процесів: управління ризиками, змінами, аудитами, реагуванням. Політика реагування на кіберінциденти: цілі, обсяг, відповідальність. План управління кіберінцидентами. Розроблення процедур реагування та звітності. Формування команд реагування (CSIRT, CERT, SOC, їх структура та функції). Канали комунікації, ескалація та зовнішня взаємодія (CERT-UA, НКЦК). Підготовка персоналу, тренінги, сценарії реагування.	**10**	**4**				**6**
1.3 Процес реагування на кіберінциденти (Б1.38, Б1.39, Б2.36, В1.33, В1.32, В1.33, В1.34, В1.35, В2.33, Д1.34, Д2.34, Д2.35, Е1.38). Етапи процесу реагування. Методи виявлення інцидентів (моніторинг мереж, систем журналювання, SIEM, IDS/IPS). Критерії пріоритетності реагування та класифікація інцидентів за рівнем впливу. Організаційні дії. Технічні дії (ізоляція активів, вилучення артефактів, усунення шкідливого ПЗ). Розслідування кіберінцидентів. Аналіз джерела інциденту: лог-файли, мережеві трафіки, цифрова форензіка. Взаємодія між технічними фахівцями, адміністрацією та зовнішніми структурами. Приклади сценаріїв реагування: фішинг, злом облікового запису, DDoS, шкідливе ПЗ, витік даних.	**10**	**4**		**2**		**4**

1.4 Документування, аналіз і запобігання кіберінцидентам (Д1.36, Е1.31, Е1.33, Е1.34, Е1.35, Е1.37, Е1.38). Реєстрація інцидентів. Форми та структура звітності (звіт інциденту, протокол, акт розслідування). Документування дій під час інциденту та зберігання цифрових доказів. Постінцидентний аналіз (виявлення кореневих причин). Оцінювання ефективності організаційних заходів реагування в межах СМІБ. Оновлення політик і процедур безпеки за результатами інцидентів. Інтеграція результатів аналізу у процес управління ризиками (ISO/IEC 27005). Проактивне запобігання інцидентам (Threat Intelligence, Threat Hunting, Red/Blue teaming). Підвищення кіберобізнаності персоналу як ключовий фактор профілактики інцидентів.	**10**	**4**		**2**		**4**
Самостійна робота / практичне завдання						
Самостійна робота 1.1. Скласти план управління кіберінцидентами	**2**					**2**
Самостійна робота / теоретична складова						
Самостійна робота 1.2. Вивчення нормативно-правової бази та передової практики з питань організації управління кіберінцидентами	**4**					**4**
Всього годин за модулем 1	**48**	**18**	**0**	**4**		**26**
Змістовний модуль 2. Технологічна основа реагування та відновлення після кіберінцидентів						
2.1 Життєвий цикл інформаційної системи (Д1.31, Д2.33). Управління розробкою програмного забезпечення. Управління якістю програмного забезпечення. Огляд виконавчого керівного комітету. Управління змінами. Управління проектом розробки програмного забезпечення. Огляд життєвого циклу розробки системи. Огляд архітектури даних. Системи підтримки прийняття рішень. Архітектура програми. Централізація проти децентралізації. Електронна комерція. Життєвий цикл інформаційної системи і процес реагування на кіберінциденти	**6**	**2**				**4**
2.2 Принципи та компоненти архітектури безпеки мереж (А1.32, А1.33, А1.34, А1.35, А1.37, А2.31, А2.33, А2.34, А2.35, А3.32, А3.37, Б1.33, Б1.34, Б1.35, Б2.31, Б2.33, Б2.34, В1.34, В2.32, В2.33, Г1.32, Г1.33, Г1.34, Г1.37, Г1.38, Г2.31, Г2.32, Д1.32, Д1.33, Д1.35). Поняття та структура архітектури безпеки мереж. Принципи побудови безпечної мережевої архітектури. Моделі безпеки (Bell-LaPadula, Biba, Zero Trust, Defense in Depth). Загрози, вразливості та кібератаки в мережах (класифікація мережевих атак, основні типи атак, типові вразливості мережевих протоколів (TCP/IP, DNS, HTTP, SMTP), методи виявлення та запобігання кібератакам, роль моделювання загроз (Threat Modeling) у проектуванні архітектури безпеки. Компоненти архітектури безпеки (мережеві екрани, IDS/IPS, VPN, шлюзи, SIEM). Політика						

безпеки та управління доступом. Зонування мереж і моделі довіри. Узагальнені архітектурні підходи (Cisco SAFE, NIST SP 800-207, Microsoft Zero Trust).						
2.3 Практичні аспекти проєктування та реалізації архітектури безпеки мереж (А1.З1, А1.З6, А1.З7, А3.З2, А3.З3, А3.З4, А3.З7, В2.З4, В3.З3). Аналіз ризиків і вимог до безпеки при проєктуванні мережі. Розроблення архітектури безпеки для різних типів мереж (локальні, корпоративні, хмарні, мобільні). Захист на різних рівнях моделі OSI. Інтеграція засобів безпеки: мережеві екрани, VPN, SIEM, NAC, DLP. Безпека маршрутизації, комутації та протоколів (IPSec, SSL/TLS, DNSSEC). Мережева сегментація, VLAN, мікросегментація та Zero Trust. Моніторинг і аудит архітектури безпеки.	**6**	**2**				**4**
2.4 Безперебійність бізнесу та відновлення після аварій (В3.З4). Розуміння п'яти суперечливих дисциплін. Визначення відновлення після катастрофи. Визначення мети безперервності бізнесу. Об'єднання інших планів з безперервністю бізнесу. Розуміння п'яти етапів бізнесу. Розуміння інтересів аудитора в планах BC/DR (Business Continuity/Disaster Recovery).	**6**	**2**				**4**
Самостійна робота / практичне завдання						
Самостійна робота 2.1. Скласти повідомлення про кеіберінцидент	**2**					**2**
Самостійна робота/ теоретична складова						
Самостійна робота 2.2. Вивчення нормативно-правової бази та передової практики щодо технологічної основи реагування та відновлення після кіберінцидентів	**4**					**4**
Всього годин за модулем 2	**48**	**16**	**0**	**2**		**30**
Модульна контрольна робота за Частиною 2	**2**				**2**	
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 Міжнародно-правові акти та українське законодавство в сфері забезпечення інформаційної безпеки, кібербезпеки та захисту інформації України. (Б1.З1, Г2.З5, Є1.З1, Є1.З3).	**3**	**2**				**1**
1.2 Нормативно-правове забезпечення кібербезпеки та конфіденційності персональних даних в кіберпросторі (Б1.З1, Є1.З1, Є1.З3).	**4**	**2**				**2**
1.3 Особливості кіберзахисту критичної інфраструктури України (секторальний підхід) та	**3**	**2**				**1**

повноваження правоохоронних органів в цій сфері. (Б1.З1, Є1.З3)						
1.4 Загальні засади юридичної відповідальності. Види відповідальності за порушення законодавства у сфері обігу інформації, інформаційної безпеки та кібербезпеки. (Г2.З3).	**3**	**2**				**1**
1.5 Кримінальна відповідальність за порушення законодавства у сфері обігу інформації, інформаційної безпеки та кібербезпеки. Кримінологічна типологія кіберзлочинців (Г1.З2)	**3**	**2**				**1**
1.6 Моральні та психологічні засади захисту інформації та етичного хакінгу (Б1.З1).	**3**	**2**				**1**
1.7 Психологічні основи інформаційної безпеки та кібербезпеки (Б1.З1).	**3**	**2**				**1**
Самостійна робота / практичне завдання						
Самостійна робота 1.1. Закони, політики та процедури, що стосуються кібербезпеки об'єктів критичної інфраструктури (**Б1.З1, Г2.З3, Е1.З6**).	**1**					**1**
Самостійна робота 1.2. Сучасна система нормативно-правового забезпечення побудови та атестації комплексних систем безпеки організацій різних форм власності (**Б1.З1, Г2.З3, Е1.З6**).	**1**					**1**
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	Max 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 бали**)*	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 реагування на інциденти кібербезпеки (трудові функції А, Б, В, Г, Д, Е)» професійного стандарту «Фахівець з реагування на інциденти 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 23 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	Відстеження, збір та документування даних про інциденти кібербезпеки з моменту їх виявлення до остаточної ідентифікації статусу події	15%	6	18
Б	Проведення оцінки інцидентів кібербезпеки	15%	6	18
В	Оброблення інцидентів кіберзахисту в режимі реального часу та вжиття заходів щодо пом’якшення наслідків кібербезпекових інцидентів, а також відновлення функціональності системи та процесів до робочого стану	10%	4	12
Г	Моніторинг та оцінка поточного стану кібербезпеки	5%	2	6
Д	Надання експертної технічної підтримки з управління кіберінцидентами	5%	2	6
Е	Дослідження та аналіз кіберінцидентів	10%	4	12
	Практичний модуль тестування навичок та вмінь	**40%**	**16**	**48**
А	Відстеження, збір та документування даних про інциденти кібербезпеки з моменту їх виявлення до остаточної ідентифікації статусу події	10%	4	12
Б	Проведення оцінки інцидентів кібербезпеки	10%	4	12

Трудова функція	Найменування розділу	Питома вага розділу	Кількість запитань у варіанті тесту	Кількість запитань у Банку завдань
В	Оброблення інцидентів кіберзахисту в режимі реального часу та вжиття заходів щодо пом'якшення наслідків кібербезпекових інцидентів, а також відновлення функціональності системи та процесів до робочого стану	5%	2	6
Г	Моніторинг та оцінка поточного стану кібербезпеки	5%	2	6
Д	Надання експертної технічної підтримки з управління кіберінцидентами	5%	2	6
Е	Дослідження та аналіз кіберінцидентів	5%	2	6
			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

Рекомендовані джерела інформації

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/