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

АУДИТОР СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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

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

категорія слухачів: аудитори інформаційних технологій (з кібербезпеки), провідні аудитори інформаційних технологій (з кібербезпеки), аудитори систем менеджменту інформаційної безпеки, провідні аудитори систем менеджменту інформаційної безпеки, керівники команд з аудиту систем менеджменту інформаційної безпеки
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
- асистент кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету «ХАІ» Р.І. Демура;
- асистент кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету «ХАІ» Р.С. Подгорний.

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 «Аудитор систем менеджменту інформаційної безпеки» розроблена у відповідності до Типової програми підвищення кваліфікації «Аудитор систем менеджменту інформаційної безпеки», Розділу ІІІ професійного стандарту «Аудитор інформаційних технологій (з кібербезпеки)» та Національного класифікатора України ДК 003:2010 «Класифікатор професій» («Аудитор інформаційних технологій (з 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 установам необхідна об’єктивна оцінка рівня безпеки інформаційних систем та їх постійне удосконалення. Саме для цих цілей і застосовується аудит інформаційної безпеки або кібераудит. Аудитор систем менеджменту інформаційної безпеки – це ключовий фахівець, який оцінює стан кібербезпеки, дотримується міжнародних стандартів (ISO 27001, NIST, PCI DSS) та законодавчих норм (GDPR, HIPAA), працює в умовах зростання кіберзагроз. У зв’язку з цим актуалізується проблема розвиту професійних компетентностей аудиторів систем менеджменту інформаційної безпеки. Аудитори систем менеджменту інформаційної безпеки мають вільно та ґрунтовно забезпечують стійкість інфраструктури та допомагають у відновленні після інцидентів кібербезпек.

ОСНОВНІ ЗАВДАННЯ ПРОГРАМИ

– використовувати на практиці нормативні документи в галузі аудиту кібернетичної безпеки;

– проводити аудит і сертифікацію (атестацію) систем, підсистем інформаційної безпеки та систем управління інформаційною безпекою;

– визначати рівень якості та проведення контролю інфраструктури на основі критеріїв оцінки, технологій і методологій оцінювання стану кібербезпеки, ефективності функцій захисту інформації та рівня гарантій та їх коректності;

– проводити аналіз та володіти базовими технологіям визначення рівня ефективності систем і процесів інформаційної та кібернетичної безпеки підприємств та організацій;

– формувати звіти по результатам аналізу, процедурам проведеного аудиту і моніторингу, надавати рекомендації й пропозиції щодо протидії кіберінцидентам, підвищенню якості функціонування кібернетичної безпеки, а також інфраструктури організації в цілому.

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ «Аудитор систем менеджменту інформаційної безпеки»

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	аудитори інформаційних технологій (з кібербезпеки), провідні аудитори інформаційних технологій (з кібербезпеки), аудитори систем менеджменту інформаційної безпеки, провідні аудитори систем менеджменту інформаційної безпеки, керівники команд з аудиту систем менеджменту інформаційної безпеки, які прагнуть підвищити кваліфікацію для проведення незалежних аудитів систем менеджменту інформаційної безпеки (СМІБ) згідно з сучасними вимогами та стандартами
Термін та обсяг Програми	15 днів / 180 год. (6 кредитів ECTS)
Професійна кваліфікація	аудитор систем менеджменту інформаційної безпеки (трудові функції А, Б, Г, Є, Ж)
Мета Програми	
Формування у здобувачів курсів системи професійних знань, вмінь та навичок щодо організації і супроводу процесів проведення внутрішнього та зовнішнього аудиту об’єктів інформатизації для надання об’єктивних якісних і кількісних оцінок про поточний стан інформаційної безпеки організації у відповідності з визначеними в нормативно-правовій базі критеріями та показниками безпеки. Формування рекомендацій, на основі наданих оцінок, для посилення системи менеджменту інформаційної безпеки (далі – СМІБ), підтримки планів стійкості, відновлення штатного функціонування інфраструктури організації після інцидентів та нештатних ситуацій. Формування у здобувачів курсів системи спеціальних знань щодо організації та супроводу процесів моніторингу й аудиту кібернетичної безпеки у відповідності до критеріїв і показників якості безпеки, організації і контролю системи мінімізації ризиків, методів та засобів одержання об’єктивних оцінок про поточний стан інформаційної системи та інформаційної інфраструктури організації в цілому.	
Функціональна спрямованість	Розвиток складових професійних компетентностей аудиторів систем менеджменту інформаційної безпеки в умовах діючого законодавства України, міжнародних стандартів (ISO 27001, NIST, PCI DSS) та законодавчих норм (GDPR, HIPAA)

Фокус програми	Акцент на розвиток професійних компетентностей аудиторів систем менеджменту інформаційної безпеки щодо вільного та ґрунтовного забезпечення стійкості інфраструктури та допомоги у відновленні після інцидентів кібербезпек, а саме: використовування на практиці нормативних документів в галузі аудиту кібернетичної безпеки; проведення аудиту і сертифікації (атестації) систем, підсистем інформаційної безпеки та систем управління інформаційною безпекою; визначення рівня якості та проведення контролю інфраструктури на основі критеріїв оцінки, технологій і методологій оцінювання стану кібербезпеки, ефективності функцій захисту інформації та рівня гарантій та їх коректності; проведення аналізу та володіння базовими технологіям визначення рівня ефективності систем і процесів інформаційної та кібернетичної безпеки підприємств та організацій; формування звітів по результатам аналізу, процедурам проведеного аудиту і моніторингу, надання рекомендації й пропозиції щодо протидії кіберінцидентам, підвищення якості функціонування кібернетичної безпеки, а також інфраструктури організації в цілому
Орієнтація програми	Програма орієнтована на розвиток професійних компетентностей аудиторів систем менеджменту інформаційної безпеки
Особливості програми	Програма підвищення кваліфікації аудиторів систем менеджменту інформаційної безпеки адаптована до національних вимог, зокрема до Професійного стандарту «Аудитор інформаційних технологій (з кібербезпеки)», фокусуються на сучасних загрозах кібербезпеки та стандартах (ISO/IEC 27001, ISO 27002), практичний досвід засновано на рівні 6 НРК та включає сучасні інструменти аудиту (наприклад, для управління ризиками), а також підготовку до сертифікації, що дозволяє проводити внутрішні та зовнішні аудити об'єктів інформатизації. 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 аудитора систем менеджменту інформаційної безпеки (СМІБ) потрібні фахові компетентності, що охоплюють: **1. Знання та Розуміння (Knowledge & Understanding):** • **Принципи ІБ:** Конфіденційність, цілісність, доступність (CIA), а також законність та етичні норми. • **Системи менеджменту:** Розуміння принципів та процесів СМІБ (наприклад, ISO 27001). • **Технічні аспекти:** Знання архітектур IT, загроз, вразливостей, механізмів контролю (доступ, мережі).

	• **Правове поле:** Закони та нормативи у сфері кібербезпеки та приватності. • **Методологія аудиту:** Принципи проведення аудиту, моніторингу та оцінки (ISO 19011). **2. Практичні Навички (Skills/Abilities):** • **Планування та проведення аудиту:** Розробка планів, тестування, виявлення ознак інцидентів. • **Аналіз:** Оцінка ризиків, аналіз інформації та виявлення слабких місць. • **Звітність:** Чітке та структуроване формування письмових висновків та звітів. • **Застосування знань:** Здатність застосовувати теорію в реальних ситуаціях. **3. Особистісні Якості (Soft Skills/Competencies):** • **Комунікація:** Ефективна взаємодія в команді, координація дій. • **Аналітичність:** Структурування інформації та формування обґрунтованих висновків. • **Відповідальність: Забезпечення ефективності процедур аудиту.** • **Командна робота:** Співпраця для досягнення спільної мети.
Програмні результати навчання	
Програма підвищення кваліфікації «**Аудитор систем менеджменту інформаційної безпеки**» спрямовано на досягнення програмних **результатів навчання**, а саме у відповідності до трудових функцій професійного стандарту та визначеної кваліфікації (далі – ТФ):	
ТФ А РН 1	Формування (підготовка), впровадження та виконання процедур внутрішнього аудиту інформаційних систем і технологій на основі визначення й прогнозування ризиків з метою забезпечення безпеки інформації та/або кібербезпеки інформаційних ресурсів, виконання стратегічних планів функціонування й розвитку інформаційної інфраструктури організації.
ТФ Б РН 2	Контроль та оцінювання ефективності поточного стану функціонування інформаційної системи, проведення незалежних оглядів (або/чи планових) для оцінювання ефективності сталих інформаційних процесів з метою підтвердження довіри до інформаційних систем і технологій та забезпечення встановленої стратегії і політик безпеки інформації та/або кібербезпеки організації.

ТФ Г РН 3	Розробка планів, впровадження та виконання процедур або/чи відповідних дій контролю для забезпечення управління інцидентами, безперервності сталих операційних процесів, підтримки планів стійкості, відновлення штатного функціонування інфраструктури організації після інцидентів та нештатних ситуацій викликаних реалізацією кібератак різного класу.
ТФ Є РН 4	Формування (підготовка), впровадження та виконання процедур внутрішнього аудиту та/або операційного аудиту систем менеджменту інформаційної безпеки організації, а також об'єктів критичної інфраструктури на основі чинного законодавства, вітчизняної та міжнародної системи стандартизації та кращих світових практик.
ТФ Ж РН 5	Контроль та оцінка ефективності поточного стану функціонування системи менеджменту інформаційної безпеки організації (в т.ч. об'єктів критичної інфраструктури), оцінювання ефективності сталих бізнес-операційних процесів з метою забезпечення встановленої мети, стратегії, політик безпеки різного рівня згідно з вітчизняними та міжнародними вимогами і стандартами.

2. НАВЧАЛЬНІ МОДУЛІ ПРОГРАМИ

Модуль 1. СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Змістовний модуль 1. Система менеджменту інформаційної безпеки організації.

Основи і принципи побудови СМІБ (А1.З6, А2.З5, А3.З6, Є1.З1, Є3.З1). Планування та розроблення СМІБ (А1.З2, А1.З7, А1.З12, А1.З17, А2.З1, А2.З7, А2.З9, Є1.З3, Є3.З1, Є3.З2). Реалізація та функціонування СМІБ (А1.З10, А1.З11, А2.З1, А2.З2, А2.З4, А2.З5, А2.З7, А2.З8, А2.З9, Б1.З1, Б1.З2, Г2.З3, Г2.З6, Ж1.З1, Ж1.З5, Ж2.З1, Є2.З1**).** Моніторинг, аналіз і вдосконалення СМІБ (А1.З7, Б1.З4, Б2З1, Б2.З2, Г1.З3, Ж1.З2, Ж1.З4, Ж2.З1, Ж2.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. ПРОЦЕДУРИ ТА ПОРЯДОК ПРОВЕДЕННЯ АУДИТУ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Змістовний модуль 1. Організація діяльності аудитора та процес аудиту СМІБ.

Організація діяльності аудитора (Є1.З1, Є1.З2, Є1.З3, Є1.З4). Основні положення аудиту та підтвердження довіри до інформаційної системи (Є1.З1, Є1.З2, Є1.З3, Є1.З4). Настанови з аудиту та підтвердження довіри до інформаційної системи (А2.З7, А2.З, Б1.З3, Є1.З1, Є1.З2, Є1.З3, Є1.З4, Ж1.З3). Порядок та управління процедурами аудиту СМІБ (А2.З8, Є1.З3, Є1.З4). Проведення та документування аудиту СМІБ (Є2.З1, Ж1.З3, Ж1.З5, Ж2.З1, Ж2.З2).

Самостійна робота. Розробити пакет документів для проведення внутрішнього аудиту СМІБ. Вивчення нормативно-правової бази та передової практики з питань організації діяльності аудитора та процес аудиту СМІБ.

Змістовний модуль 2. Об’єкти контролю та інструменти аудиту СМІБ.

Життєвий цикл інформаційної системи (А3.З4). Розробка та впровадження інформаційних систем (А1.З6, А1.З7, А2.З3, А2.З8, А3.З1, А3.З6, Ж2.З2, Є1.З4). Архітектура безпеки мережі (А1.З1, А1.З5, А1.З6, А1.З11, А1.З16, А1.З17, А3.З1, А3.З2, А3.З4, А3.З5, А3.З6, Г2.З5, Є1.З4). Захист інформаційних активів (А1.З3, А1.З3, А1.З5, А1.З8, А1.З11, А1.З13, А1.З14, А1.З15, А1.З17, Г1.З3, Г1.З5). Управління інцидентами (Г1.З1, Г1.З2, Г1.З3, Г1.З4, Г1.З5, Г2.З2, Г3.З1, Г3.З2). Безперебійність бізнесу та відновлення після аварій (Г2.З1, Г2.З4).

Самостійна робота. Оформити документацію відповідно до заданого кейсу інциденту. Вивчення нормативно-правової бази та передової практики щодо об’єктів контролю та інструментів аудиту СМІБ.

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 (А1.З12). Нормативно-правове забезпечення системи контролю та аудиту у сфері менеджменту інформаційної безпеки, кібербезпеки та захисту інформації в кіберпросторі держави (А1.З18). Особливості кіберзахисту критичної інфраструктури України (секторальний підхід) та захисту інформаційних ресурсів організацій та підприємств різних форм власності (А1.З18). Загальні засади юридичної відповідальності. Кримінальна відповідальність за порушення законодавства у сфері обігу інформації, інформаційної безпеки та кібербезпеки. Моральні та психологічні засади захисту інформації та етичного хакінгу. Психологічні основи інформаційної безпеки та кібербезпеки.

Самостійна робота. Закони, політики та процедури, що стосуються кібербезпеки об’єктів критичної інфраструктури (Є1.УЗ). Сучасна система нормативно-правового забезпечення побудови та атестації комплексних систем безпеки організацій різних форм власності (Є1.УЗ). 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 (А1.З6, А2.З5, А3.З6, Є1.З1, Є3.З1). 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 (А1.З2, А1.З7, А1.З12, А1.З17, А2.З1, А2.З7, А2.З9, Є1.З3, Є3.З1, Є3.З2). 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 (А1.З10, А1.З11, А2.З1, А2.З2, А2.З4, А2.З5, А2.З7, А2.З8, А2.З9, Б1.З1, Б1.З2, Г2.З3, Г2.З6, Ж1.З1, Ж1.З5, Ж2.З1, Є2.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 (А1.З7, Б1.З4, Б2З1, Б2.З2, Г1.З3, Ж1.З2, Ж1.З4, Ж2.З1, Ж2.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**		**28**
Модульна контрольна робота за Частиною 1	**2**				**2**	
Всього годин за Частиною 1	**50**	**16**	**0**	**4**	**2**	**28**

3.2. Процедури та порядок проведення аудиту системи менеджменту інформаційної безпеки організації

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 діяльності аудитора та процес аудиту СМІБ						
1.1 Організація діяльності аудитора (Є1.31, Є1.32, Є1.33, Є1.34). Розуміння попиту на аудит інформаційних систем. Розуміння політик, стандартів, керівних принципів та процедур, професійної етики та мети аудиту. Розмежування ролей аудитора та об'єкта аудиту. Впровадження стандартів аудиту. Аудитор як керівна посада. Розуміння важливості конфіденційності аудитора. Визначення цінності внутрішніх та зовнішніх аудиторів. Розуміння правила доказів. Визначення осіб, яких необхідно опитати. Розуміння організаційної структури підприємства. Визначення ролей в організаційній структурі підприємства та консалтингової фірми.	**6**	**2**				**4**
1.2 Основні положення аудиту та підтвердження довіри до інформаційної системи (Є1.31, Є1.32, Є1.33, Є1.34). Загальні стандарти (Статут аудиту. Організаційна незалежність. Професійна незалежність. Обґрунтовані очікування. Належна професійна ретельність Професійність. Твердження. Критерії). Стандарти виконання (Планування завдань. Оцінювання ризиків у плануванні. Ефективність і нагляд. Суттєвість. Докази. Залучення інших експертів. Невідповідності та незаконні дії). Стандарти звітування (Звітування. Подальша діяльність).	**8**	**4**				**4**
1.3 Настанови з аудиту та підтвердження довіри до інформаційної системи (А2.37, А2.3, Б1.33, Є1.31, Є1.32, Є1.33, Є1.34, Ж1.33). Основні настанови (Статут аудиту. Організаційна незалежність. Професійна незалежність. Обґрунтовані очікування. Належна професійна ретельність Професійність. Твердження. Критерії). Настанови з виконання (Планування завдань. Оцінювання ризиків у плануванні. Ефективність і нагляд. Суттєвість. Докази.	**8**	**4**				**4**

Залучення інших експертів. Невідповідності та незаконні дії. Вибірка). Настанови щодо звітування (Звітування. Подальша діяльність).						
1.4 Порядок та управління процедурами аудиту СМІБ (А2.З8, Є1.З3, Є1.З4). Розуміння аудиторської програми. Встановлення та затвердження статуту аудиту. Попереднє планування конкретних аудитів. Виконання оцінки аудиторських ризиків. Визначення можливості проведення аудиту.	**10**	**4**		**2**		**4**
1.5 Проведення та документування аудиту СМІБ (Є2.З1, Ж1.З3, Ж1.З5, Ж2.З1, Ж2.З2). Організація проведення аудиту. Збір аудиторських доказів. Проведення перевірки аудиторських доказів. Формування аудиторських висновків. Звіт про результати. Подальші дії (заключна нарада).	**10**	**4**		**2**		**4**
Самостійна робота / практичне завдання						
Самостійна робота 1.1. Розробити пакет документів для проведення внутрішнього аудиту СМІБ.	**2**					**2**
Самостійна робота / теоретична складова						
Самостійна робота 1.2. Вивчення нормативно-правової бази та передової практики з питань організації діяльності аудитора та процес аудиту СМІБ.	**4**					**4**
Всього годин за модулем 1	**48**	**18**	**0**	**4**	**0**	**26**
Змістовний модуль 2. Об'єкти контролю та інструменти аудиту СМІБ						
2.1 Життєвий цикл інформаційної системи (А3.З4). 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.	**6**	**2**				**4**
2.2 Розробка та впровадження інформаційних систем (А1.З6, А1.З7, А2.З3, А2.З8, А3.З1, А3.З6, Ж2.З2, Є1.З4). Розуміння природи ІТ-послуг. Виконання управління ІТ-операціями. Виконання управління продуктивністю. Використання адміністративного захисту. Виконання управління проблемами. Моніторинг стану засобів контролю. Впровадження фізичного захисту.	**6**	**2**				**4**
2.3 Архітектура безпеки мережі (А1.З1, А1.З5, А1.З6, А1.З11, А1.З16, А1.З17, А3.З1, А3.З2, А3.З4, А3.З5, А3.З6, Г2.З5, Є1.З4). Розуміння відмінностей в архітектурі комп'ютерів. Вибір найкращої системи. Вступ до моделі взаємозв'язку відкритих систем. Розуміння фізичної структури мережі. Розуміння топологій мережевих кабелів. Відмінності між типами мережевих кабелів. Підключення мережевих пристроїв. Використання мережевих служб. Розширення мережі. Використання програмного забезпечення як послуги. Основи управління мережею.	**8**	**4**				**4**

2.4 Захист інформаційних активів (А1.33, А1.33, А1.35, А1.38, А1.311, А1.313, А1.314, А1.315, А1.317, Г1.33, Г1.35). Розпізнавання типів загроз та комп'ютерних злочинів. Ідентифікація зловмисників. Розуміння методів атак. Впровадження адміністративного захисту. Класифікація технічного контролю. Контроль програмного забезпечення. Методи автентифікації. Захист доступу до мережі. Методи шифрування. Інфраструктура відкритих ключів. Протоколи мережевої безпеки. Телефонна безпека. Технічне тестування безпеки.	**8**	**4**				**4**
2.5 Управління інцидентами (Г1.31, Г1.32, Г1.33, Г1.34, Г1.35, Г2.32, Г3.31, Г3.32). Розбудова потенціалу реагування на інциденти, пов'язані з комп'ютерною безпекою. Підготовка. Виявлення та аналіз. Стримування, ліквідація наслідків та відновлення. Заходи після інциденту. Контрольний список з управління інцидентами. Обмін детальною інформацією. Рекомендації.	**8**	**2**		**2**		**4**
2.6 Безперебійність бізнесу та відновлення після аварій (Г2.31, Г2.34). 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. Оформити документацію відповідно до заданого кейсу інциденту	**2**					**2**
Самостійна робота/ теоретична складова						
Самостійна робота 2.2. Вивчення нормативно-правової бази та передової практики щодо об'єктів контролю та інструментів аудиту СМІБ	**4**					**4**
Всього годин за модулем 2	**48**	**16**	**0**	**2**	**0**	**30**
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 (А1.312).	**3**	**2**				**1**

1.2 Нормативно-правове забезпечення системи контролю та аудиту у сфері менеджменту інформаційної безпеки, кібербезпеки та захисту інформації в кіберпросторі держави (міжнародні стандарти й національне законодавство у сфері кібербезпеки та захисту інформації державних інформаційних ресурсів України) **(А1.З18).**	**4**	**2**				**2**
1.3 Особливості кіберзахисту критичної інфраструктури України (секторальний підхід) **та захисту інформаційних ресурсів організацій та підприємств різних форм власності (А1.З18).**	**3**	**2**				**1**
1.4 Загальні засади юридичної відповідальності. Дисциплінарна та адміністративна відповідальність за порушення законодавства у сфері обігу інформації, інформаційної безпеки та кібербезпеки.	**3**	**2**				**1**
1.5 Кримінальна відповідальність за порушення законодавства у сфері обігу інформації, інформаційної безпеки та кібербезпеки.	**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.	**3**	**2**				**1**
Самостійна робота / практичне завдання						
Самостійна робота 1.1. Закони, політики та процедури, що стосуються кібербезпеки об'єктів критичної інфраструктури (**Є1.У3).**	**1**					**1**
Самостійна робота 1.2. Сучасна система нормативно-правового забезпечення побудови та атестації комплексних систем безпеки організацій різних форм власності (**Є1.У3**).	**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**				**2**	
Всього годин за частиною 3	**28**	**14**	**0**	**0**	**2**	**12**
Консультація з контрольної роботи у виді комп'ютерного оцінювання	**2**				**2**	
Контрольна робота у виді комп'ютерного оцінювання	**2**				**2**	
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 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 «Аудитор систем менеджменту інформаційної безпеки (трудові функції А, Б, Г, Є, Ж)» професійного стандарту «Аудитор інформаційних технологій (з 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 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	Формування (підготовка), впровадження та виконання процедур внутрішнього аудиту інформаційних систем і технологій на основі визначення й прогнозування ризиків з метою забезпечення безпеки інформації та/або кібербезпеки інформаційних ресурсів, виконання стратегічних планів функціонування й розвитку інформаційної інфраструктури організації	10%	4	12
Б	Контроль та оцінювання ефективності поточного стану функціонування інформаційної системи, проведення незалежних оглядів (або/чи планових) для оцінювання ефективності сталих інформаційних процесів з метою підтвердження довіри до інформаційних систем і технологій та забезпечення встановленої	17,5%	7	21

Трудова функція	Найменування розділу	Питома вага розділу	Кількість запитань у варіанті тесту	Кількість запитань у Банку завдань
	стратегії і політик безпеки інформації та/або кібербезпеки організації			
Г	Розробка планів, впровадження та виконання процедур або/чи відповідних дій контролю для забезпечення управління інцидентами, безперервності сталих операційних процесів, підтримки планів стійкості, відновлення штатного функціонування інфраструктури організації після інцидентів та нештатних ситуацій викликаних реалізацією кібератак різного класу	10%	4	12
Є	Формування (підготовка), впровадження та виконання процедур внутрішнього аудиту та/або операційного аудиту систем менеджменту інформаційної безпеки організації, а також об'єктів критичної інфраструктури на основі чинного законодавства, вітчизняної та міжнародної системи стандартизації та кращих світових практик	10%	4	12
Ж	Контроль та оцінка ефективності поточного стану функціонування системи менеджменту інформаційної безпеки організації (в т.ч. об'єктів критичної інфраструктури), оцінювання ефективності сталих бізнес-операційних процесів з метою забезпечення встановленої мети, стратегії, політик безпеки різного рівня згідно з вітчизняними та міжнародними вимогами і стандартами	12,5%	5	15
	Практичний модуль тестування навичок та вмінь	**40%**	**16**	**48**
А	Формування (підготовка), впровадження та виконання процедур внутрішнього аудиту інформаційних систем і технологій на основі визначення й прогнозування ризиків з метою забезпечення безпеки інформації та/або кібербезпеки інформаційних ресурсів, виконання стратегічних планів функціонування й розвитку інформаційної інфраструктури організації	10%	4	12
Б	Контроль та оцінювання ефективності поточного стану функціонування інформаційної системи, проведення незалежних оглядів (або/чи планових) для оцінювання ефективності сталих інформаційних процесів з метою підтвердження довіри до інформаційних систем	10%	4	12

Трудова функція	Найменування розділу	Питома вага розділу	Кількість запитань у варіанті тесту	Кількість запитань у Банку завдань
	і технологій та забезпечення встановленої стратегії і політик безпеки інформації та/або кібербезпеки організації			
Г	Розробка планів, впровадження та виконання процедур або/чи відповідних дій контролю для забезпечення управління інцидентами, безперервності сталих операційних процесів, підтримки планів стійкості, відновлення штатного функціонування інфраструктури організації після інцидентів та нештатних ситуацій викликаних реалізацією кібератак різного класу	10%	4	12
Є	Формування (підготовка), впровадження та виконання процедур внутрішнього аудиту та/або операційного аудиту систем менеджменту інформаційної безпеки організації, а також об'єктів критичної інфраструктури на основі чинного законодавства, вітчизняної та міжнародної системи стандартизації та кращих світових практик	5%	2	6
Ж	Контроль та оцінка ефективності поточного стану функціонування системи менеджменту інформаційної безпеки організації (в т.ч. об'єктів критичної інфраструктури), оцінювання ефективності сталих бізнес-операційних процесів з метою забезпечення встановленої мети, стратегії, політик безпеки різного рівня згідно з вітчизняними та міжнародними вимогами і стандартами	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.

Базові Стандарти

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/