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 № __

КОНЦЕПЦІЯ ОСВІТНЬОЇ ДІЯЛЬНОСТІ

з підвищення кваліфікації

аудиторів систем менеджменту інформаційної безпеки

зі спеціальності F5 «Кібербезпека та захист інформації»

у сфері післядипломної освіти на основі здобутої вищої освіти

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

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

Харків 2025

ВСТУП

Розроблення Концепції освітньої діяльності з підвищення кваліфікації аудиторів систем менеджменту інформаційної безпеки зі спеціальності F5 «Кібербезпека та захист інформації» у сфері післядипломної освіти для осіб з вищою освітою (далі – Концепція) обумовлена суспільною значимістю та об'єктивною потребою держави в ефективному професійному розвитку аудиторів систем менеджменту інформаційної безпеки на рівні світових аналогів. 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 та вільно та ґрунтовно забезпечують стійкість інфраструктури та допомагають у відновленні після інцидентів кібербезпек.

Концепція регламентує мету та завдання із забезпечення безперервного професійного розвитку та підвищення рівня професійних компетентностей фахівців сфери інформаційної безпеки.

Нормативно-правовою базою розроблення та реалізації Концепції є: Типова програма підвищення кваліфікації «Аудитор систем менеджменту інформаційної безпеки», Розділ ІІІ професійного стандарту «Аудитор інформаційних технологій (з кібербезпеки)», Національний класифікатор України ДК 003:2010 «Класифікатор професій» («Аудитор інформаційних технологій (з кібербезпеки)» 2139.2), основні положення і вимоги визначені законами України «Про освіту», «Про вищу освіту», інші законодавчі і нормативні документи.

1. ОСВІТНЯ ПРОГРАМА З ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ АУДИТОРІВ СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Загальна характеристика

Сфера освіти	Післядипломна освіта для осіб з вищою освітою
Вид основної діяльності	Підвищення кваліфікації
Рівень освіти	Вища освіта
Галузь знань	F «Інформаційні технології»
Спеціальність	F5 «Кібербезпека та захист інформації»
Форма навчання	Змішана (офлайн/онлайн)
Термін та обсяг Програми	15 днів / 180 год. (6 кредитів ECTS)
Мова викладання	Українська
Вид підсумкового контролю	Комп’ютерне оцінювання знань на базі автоматизованої системи тестування

2. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

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

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.

Мета освітньої 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 освітньої програми – 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).

Об'єкт вивчення: процеси управління ІБ, політики, процедури, технічні засоби та людський фактор для оцінки відповідності вимогам стандартів (як ISO/IEC 27001), виявлення вразливостей та ризиків, а об'єктами є вся корпоративна інформація, її інфраструктура (мережі, системи), персонал та документація задля забезпечення конфіденційності, цілісності й доступності.

Цілі навчання: оволодіння принципами та методами аудиту за ISO 27001, розуміння вимог стандарту та ISO 19011, набуття навичок проведення внутрішніх та сертифікаційних аудитів, управління командою аудиторів, аналіз ризиків, оцінку середовища організації та забезпечення відповідності вимогам стейкхолдерів, що дозволяє ефективно оцінювати та покращувати систему менеджменту інформаційної безпеки.

Теоретичний зміст предметної області: глибоке розуміння міжнародних стандартів (ISO/IEC 27001, 27002), методологій аудиту, управлінських процесів захисту інформації, правової бази та технічних аспектів безпеки, з метою оцінки відповідності системі менеджменту інформаційної безпеки вимогам,

виявлення ризиків та надання рекомендацій для безперервного покращення захисту інформаційних активів організації.

Методи, методики та технології: методи документальної та фактичної перевірки, інтерв'ю з персоналом, тестування контрольних процедур та аналіз даних для оцінки відповідності стандартам (як ISO 27001), методики оцінки адміністративних (політики), технічних (засоби захисту), та програмних (СКУД, антивіруси) заходів, інструменти для сканування вразливостей та моніторингу безпеки.

Інструменти та обладнання: документування (чек-листи, опитувальники), інструменти аналізу ризиків (для виявлення слабких місць), спеціалізоване програмне забезпечення (для сканування вразливостей, аналізу мережевого трафіку) та засоби технічного аудиту (обладнання для перевірки фізичної безпеки).

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.

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.

3. 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).

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).

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).

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.

4. ПЕРЕЛІК ОСНОВНИХ КОМПЕТЕНТНОСТЕЙ ТА РЕЗУЛЬТАТІВ НАВЧАННЯ

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) компетентності:

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 ІТ, 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.

5. 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.

6. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Результати навчання можуть оцінюватись за формами:

– стандартною формою;

– комп'ютерне оцінювання знань на базі автоматизованої системи тестування.

6.1 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

6.2. 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.

6.3. 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.

6.4 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:

$$23*1+14*3+3*5 = 80 \text{ хв.}$$

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	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 стратегії і політик безпеки інформації та/або кібербезпеки організації	17,5%	7	21
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	10%	4	12

Трудова функція	Найменування розділу	Питома вага розділу	Кількість запитань у варіанті тесту	Кількість запитань у Банку завдань
	системи стандартизації та кращих світових практик			
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 і технологій та забезпечення встановленої стратегії і політик безпеки інформації та/або кібербезпеки організації	10%	4	12
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	5%	2	6

Трудова функція	Найменування розділу	Питома вага розділу	Кількість запитань у варіанті тесту	Кількість запитань у Банку завдань
	законодавства, вітчизняної та міжнародної системи стандартизації та кращих світових практик			
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%.

7. ЗАБЕЗПЕЧЕННЯ НАЯВНОСТІ НЕОБХІДНИХ ЗАСОБІВ ДЛЯ ОРГАНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ

Освітня програма аудиторів систем менеджменту інформаційної безпеки забезпечена всіма необхідними навчально-методичними матеріалами, електронними ресурсами, сучасним обладнанням, функціональними приміщеннями та відповідає Ліцензійним умовам впровадження освітньої

діяльності (Постанова КМУ «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30.12.2015 р. № 1187 зі змінами).

Усі приміщення відповідають будівельним та санітарним нормам. Наявна соціальна інфраструктура включає спортивний комплекс, пункти харчування, центр творчості, медпункт і базу відпочинку.

Викладання навчальних модулів програми ґрунтуються на індивідуальному особистісному підходу, реалізуються через навчання, творчої спрямованості у формі комбінації лекцій, практичних занять, самостійної роботи з використанням елементів дистанційного навчання та забезпечено компетентними науково-педагогічними працівниками відповідно до Ліцензійних умов впровадження освітньої діяльності (Постанова КМУ «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30.12.2015 р. № 1187 зі змінами).

Внутрішня система забезпечення якості освіти, передбачає постійний моніторинг та вдосконалення, а також дотримання вимог безпеки (техніки безпеки, охорони праці, інформаційної безпеки.