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

фахівців з оцінки заходів захисту інформації (кібербезпеки)

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 фахівців з оцінки заходів захисту інформації (кібербезпеки) 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 фахівців з оцінки заходів захисту інформації (кібербезпеки), які відіграють ключову роль у забезпеченні ефективності роботи державних установ, підприємств та організацій. Фахівці з оцінки заходів захисту інформації (кібербезпеки) є ключовим для захисту від хакерів, вірусів та витоків, розробляючи комплексні стратегії та тестуючи системи та вільно та ґрунтовно забезпечують надійний захист цифрових активів, балансуючи між доступністю інформації та її безпекою.

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 «Фахівець з оцінки заходів захисту інформації (кібербезпеки)», Розділ ІІІ професійного стандарту «Фахівець з оцінки заходів захисту інформації (кібербезпеки)», Національний класифікатор України ДК 003:2010 «Класифікатор професій» («Фахівець з оцінки заходів захисту інформації (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 ФАХІВЦІВ З ОЦІНКИ ЗАХОДІВ ЗАХИСТУ ІНФОРМАЦІЇ (КІБЕРБЕЗПЕКИ)

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 стратегічного управління кіберризиками, забезпечення стійкості та безперервності бізнес-процесів в умовах постійних кіберзагроз. Набуття здобувачами курсів системи теоретичних знань щодо теорії ризиків, нормативно-правової бази в сфері інформаційної безпеки, технічної експертизи. Формування практичних навичок аудиту та тестування, розвиток управлінських та аналітичних компетенцій.

Функціональна спрямованість освітньої програми – розвиток складових професійних компетентностей фахівців з оцінки заходів захисту інформації (кібербезпеки) відповідно до комплексного захисту інформації, поєднуючи технічні знання, аналітичні навички та розуміння правового поля.

Об'єкт вивчення: інформація та інформаційні ресурси (усі види даних, що обробляються, зберігаються, передаються) і інформаційні системи та інфраструктура (апаратне та програмне забезпечення, мережі, що забезпечують їх функціонування), а також процеси управління кібербезпекою та ризиками, з метою забезпечення конфіденційності, цілісності та доступності цих даних.

Цілі навчання: аналіз і оцінку кіберзагроз та інцидентів, розроблення, впровадження та оцінку ефективності систем захисту, управління ризиками, забезпечення неперервності бізнес-процесів, дотримання законодавства та стандартів, а також відновлення функцій систем після атак, комплексне забезпечення кібербезпеки.

Теоретичний зміст предметної області: фундаментальні знання, принципи та теорії кібербезпеки, законодавство та стандарти, методи та моделі захисту, управління ризиками та інцидентами, технології для забезпечення безперервності бізнесу, оцінка ефективності застосованих заходів захисту.

Методи, методики та технології: методи сканування вразливостей, пентести (етичний хакінг), аналіз ризиків та аудит, ґрунтуючись на стандартах типу ISO 27001, методологіях NIST та технологіях управління доступом, шифрування та моніторингу, цілісність та доступність (CIA Triad) інформації.

Інструменти та обладнання: широкий спектр інструментів: від програмних засобів (сканери вразливостей, SIEM-системи, антивіруси, фаєрволи, пісочниці, засоби шифрування) до апаратних рішень (мережеві пристрої, системи контролю доступу), методологій для аналізу загроз, тестування на проникнення (пентест), реагування на інциденти.

Фокус програми: Акцент на розвиток професійних компетентностей фахівців з оцінки заходів захисту інформації (кібербезпеки) щодо вільного та ґрунтовного забезпечення надійного захисту цифрових активів, балансуючи між доступністю інформації та її безпекою, а саме: планування та проведення оглядів авторизації та безпеки, розробки процесів відповідності безпеки та/або аудитів, проведення оцінки ефективності засобів контролю безпеки, оцінки всіх процесів управління конфігурацією, здійснення моніторингу, виконання переглядів та аналізів безпеки, визначення недоліків, формування планів усунення вразливостей, розроблення рекомендацій для зниження ризиків, формування звітів за результатами аналізу, процедурам проведеного аудиту і моніторингу, надання рекомендацій й пропозиції щодо протидії кіберінцидентам, сприяння підвищенню якості функціонування кібернетичної безпеки, а також інфраструктури організації в цілому.

Особливості програми: Програма підвищення кваліфікації фахівців з оцінки заходів захисту інформації (кібербезпеки) адаптована до національних вимог, зокрема до Професійного стандарту «Фахівець з оцінки заходів захисту інформації (кібербезпеки))», фокусується на оцінці ризиків, аудиту систем безпеки, розробці стратегій захисту та впровадження стандартів (напр., ISO 27001, NIST), розумінні правового поля кібербезпеки, знанні принципів CIA Triad (конфіденційність, цілісність, доступність), вмінні працювати з антивірусами та засобами захисту, а також оцінювати економічну ефективність заходів для забезпечення захищеності інформаційних систем від загроз.

3. НАВЧАЛЬНІ МОДУЛІ ПРОГРАМИ

Модуль 1. СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Змістовний модуль 1. Система менеджменту інформаційної безпеки організації.

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

Модуль 2. АНАЛІЗ ПРОЦЕСІВ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Змістовний модуль 1. Криптологія та криптоаналіз.

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

Змістовний модуль 2. Безпечне програмне забезпечення.

Роль безпеки у розробленні програмного забезпечення (А1.37, А1.35, А2.34, Б2.31, Б2.38, В2.32, Б2.35, В2.38, Г3.34). Механізми захисту процесора та операційної системи від переповнення буфера (А1.37, А2.34, Б2.31, Б2.38, В2.34, Г3.34). Цілочисельні переповнення, вразливості форматних рядків (А1.37, В2.38, Б2.38, Г2.34). Потенційно вразливі конструкції в небезпечних мовах програмування (В2.38, Г2.34, Г3.34). Моделі і методи управління безпекою (Б1.35, Б2.37, В3.32, В1.32, Г5.32). Принципи проведення оцінки захищеності мереж (А2.34, А3.33, Б1.34, В2.36, В3.35, В4.35, Г4.33).

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

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

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

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 фахівця з оцінки заходів захисту інформації (кібербезпеки) потрібні фахові компетентності, що охоплюють:

1. Аудит та оцінка ризиків:

Проведення комплексної оцінки управлінського, операційного та технічного контролю безпеки.

Виявлення слабких місць та вразливостей в інформаційних системах (ІС).

Аналіз потенційних загроз та їх впливу.

Оцінка ступеня захищеності та ефективності існуючих заходів.

2. Технічні знання:

Розуміння принципів роботи антивірусного ПЗ та інших засобів захисту.

Знання методів захисту від несанкціонованого доступу та витоку інформації.

Оцінка реалізації послуг безпеки в ІС.

3. Управління безпекою:

Розробка та контроль виконання заходів для усунення ризиків.

Підвищення рівня безпеки та забезпечення економічної ефективності захисту.

Впровадження стандартів інформаційної безпеки та управління ризиками.

4. Теоретичні основи:

Знання теорії кібербезпеки, класифікації загроз.

Розуміння основних принципів інформаційної безпеки (конфіденційність, цілісність, доступність - CIA Triad).

5. Правові та організаційні аспекти:

Знання правових аспектів кібербезпеки в Україні.

Розуміння ролі організаційних та технічних заходів захисту інформації

Програмні результати навчання:

Програма підвищення кваліфікації **«Фахівець з оцінки заходів захисту інформації (кібербезпеки)»** спрямовано на досягнення програмних **результатів навчання**, а саме у відповідності до трудових функцій професійного стандарту та визначеної кваліфікації (далі – ТФ):	
ТФ А РН 1	Оцінювання ефективності засобів контролю безпеки, зокрема огляд авторизації безпеки та аудит зовнішніх послуг. Розробка кейсів впевненості та огляд авторизації безпеки.
ТФ Б РН 2	Оцінювання дотримання заходів забезпечення відповідності, у тому числі з аналізом процесів управління конфігураціями та дотриманням встановлених обмежень прикладного програмного забезпечення, мереж або систем.
ТФ Г РН 3	Виконання аналізу системи безпеки та її ризиків, перегляд безпеки архітектури, управління ризиками з наданням відповідних рекомендацій, даних та документів для включення в стратегію зниження ризиків та розробку плану управління ризиками.
ТФ Є РН 4	Нагляд за дотриманням належного опису, оновленню та документуванню діяльності, проєктування та розвитку кібербезпеки, зокрема безпеки прикладної системи, системи та мережі, а також керування пакетами документів з акредитації.

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

Мінімальна кількість балів для допуску до підсумкового контролю 48 балів.

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 «Фахівець з оцінки заходів захисту інформації (кібербезпеки) (трудові функції А, Б, В, Г)» професійного стандарту «Фахівець з оцінки заходів захисту інформації (кібербезпеки)».

До одного варіанту тесту входить 40 тестових запитань.

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

запитань у Банку запитань» вказує, скільки запитань з загальної кількості відносяться до певної трудової функції.

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

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

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

На проходження варіанту тесту здобувачеві виділяється 1 година 20 хвилин:

$$23*1+14*3+3*5 = 80 \text{ хв.}$$

Таблиця 1

Відповідність Банку завдань та варіанту тесту професійної кваліфікації

Трудова функція	Найменування розділу	Питома вага розділу	Кількість запитань у варіанті тесту	Кількість запитань у Банку завдань
	Теоретичний модуль тестування знань	**60%**	**24**	**72**
A	Оцінювання ефективності засобів контролю безпеки, зокрема огляд авторизації безпеки та аудит зовнішніх послуг. Розробка кейсів впевненості та огляд авторизації безпеки.	14%	6	18
Б	Оцінювання дотримання заходів забезпечення відповідності, у тому числі з аналізом процесів управління конфігураціями та дотриманням встановлених обмежень прикладного програмного забезпечення, мереж або систем.	15%	6	18
В	Виконання аналізу системи безпеки та її ризиків, перегляд безпеки архітектури, управління ризиками з наданням відповідних рекомендацій, даних та документів для включення в стратегію	21%	8	24

Трудова функція	Найменування розділу	Питома вага розділу	Кількість запитань у варіанті тесту	Кількість запитань у Банку завдань
	зниження ризиків та розробку плану управління ризиками.			
Г	Нагляд за дотриманням належного опису, оновленню та документуванню діяльності, проєктування та розвитку кібербезпеки, зокрема безпеки прикладної системи, системи та мережі, а також керування пакетами документів з акредитації.	10%	4	12
	Практичний модуль тестування навичок та вмінь	**40%**	**16**	**48**
А	Оцінювання ефективності засобів контролю безпеки, зокрема огляд авторизації безпеки та аудит зовнішніх послуг. Розробка кейсів впевненості та огляд авторизації безпеки.	10%	4	12
Б	Оцінювання дотримання заходів забезпечення відповідності, у тому числі з аналізом процесів управління конфігураціями та дотриманням встановлених обмежень прикладного програмного забезпечення, мереж або систем.	10%	4	12
В	Виконання аналізу системи безпеки та її ризиків, перегляд безпеки архітектури, управління ризиками з наданням відповідних рекомендацій, даних та документів для включення в стратегію зниження ризиків та розробку плану управління ризиками.	14%	7	21
Г	Нагляд за дотриманням належного опису, оновленню та документуванню діяльності, проєктування та розвитку кібербезпеки, зокрема безпеки прикладної системи, системи та мережі, а також керування пакетами документів з акредитації.	6%	1	3
			40	**120**

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

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

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

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

- визнати результати навчання, присвоїти/підтвердити повну професійну кваліфікації. Теоретичні знання та практичні навички відповідають критерію не менше 75%;
- відмовити у присвоєнні/підтвердженні повної/часткової професійної кваліфікації. Теоретичні та практичні знання не відповідають критерію - не менше 75%.

7. ЗАБЕЗПЕЧЕННЯ НАЯВНОСТІ НЕОБХІДНИХ ЗАСОБІВ ДЛЯ ОРГАНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ

Освітня програма фахівців з оцінки заходів захисту інформації (кібербезпеки) 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.