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 реагування на інциденти 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 реагування на інциденти 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 реагування на інциденти кібербезпеки. У сучасному світі, де інформація є цінним активом, фахівець з реагування на інциденти кібербезпеки є професіонал, який аналізує, запобігає та усуває наслідки кібератак; він діє як "кібер-детектив", розслідуючи атаки, збираючи докази, відновлюючи системи та мінімізуючи шкоду, щоб захистити цифрову інфраструктуру та дані від загроз, забезпечують комплексний захист інформаційних систем.

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 реагування на інциденти кібербезпеки», Розділ ІІІ професійного стандарту «Фахівець з реагування на інциденти кібербезпеки», Національний класифікатор України ДК 003:2010 «Класифікатор професій» («Фахівець з реагування на інциденти кібербезпеки»), 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 РЕАГУВАННЯ НА ІНЦИДЕНТИ 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 організації і супроводу процесів проведення аналізу, оцінки інцидентів кібербезпеки в рамках мережевого середовища та реагування на них. Усунення інцидентів кібербезпеки та пом'якшення їх наслідків. Відстеження, оцінка стану кібербезпеки систем та своєчасне повідомлення про інциденти кібербезпеки. Відновлення функціональності систем і процесів до робочого стану. Дослідження та аналіз заходів реагування, оцінка ефективності та покращення існуючих практик. Накопичення та проведення аналізу даних про кіберзагрози.

Функціональна спрямованість освітньої програми – реагування на інциденти кібербезпеки полягає в аналізі, оцінці, локалізації та усуненні кібератак і інцидентів, а також відновленні нормальної роботи систем, моніторингу кіберзагроз та постійного вдосконалення захисту для запобігання майбутнім атакам, що охоплює технічну, організаційну та правову складові кіберзахисту. Ці фахівці виконують роль аналітиків, інженерів, розслідувачів та консультантів, працюючи в національних системах обміну інформацією про інциденти, галузевих та корпоративних командах CSIRT.

Об'єкт вивчення: реагування на інциденти кібербезпеки кіберінценденти/кібератаки та їхні артефакти на різних рівнях – від мережі та систем до користувачів, процеси виявлення, аналізу, локалізації та усунення цих загроз з метою відновлення безпеки інформаційних систем та захисту даних, вивчення методів зловмисників, інструментів аналізу та протоколів безпеки.

Цілі навчання: підготовка до аналізу, оцінка та усунення кібератак, розробка стратегій захисту, проведення кіберрозслідувань, відновлення систем, застосування сучасних технологій та законодавства для забезпечення стійкості інформаційних систем, захисту критичної інфраструктури від реальних загроз.

Теоретичний зміст предметної області: принципи, теорії та концепції захисту цифрових інтересів від загроз, включаючи методи виявлення, запобігання та нейтралізації кібератак, забезпечення конфіденційності, цілісності та доступності даних, розробку стратегій кіберстійкості для

критичної інфраструктури, ґрунтуючись на законодавстві, стандартах та найкращих практиках, безперервне вдосконалення захисних механізмів.

Методи, методики та технології: комбінація методів, методик, технологій (SIEM, IDS/IPS, EDR), стандартів (NIST, ISO) для швидкого виявлення, аналізу, стримування та ліквідації наслідків кіберінцидентів, безперервний моніторинг.

Інструменти та обладнання: спеціалізовані інструменти (програмні та апаратні) для виявлення, аналізу та реагування на кібератаки, включаючи сканери вразливостей, системи виявлення вторгнень (IDS/IPS), інструменти цифрової форензики, SIEM-системи для моніторингу подій, мережеві аналізатори та засоби для збору образів дисків, спеціалізовані платформи автоматизації (SOAR).

Фокус програми: Фокус програм фахівців з реагування на інциденти кібербезпеки зосереджений на підготовці експертів, які можуть виявляти, аналізувати, локалізовувати та усувати кіберзагрози, використовуючи технічні знання з мережевих протоколів, операційних систем, криптографії та інструментів безпеки, з метою відновлення нормальної роботи систем, збору доказів для розслідування та впровадження профілактичних заходів для захисту інформації.

Особливості програми: Програма підвищення кваліфікації з реагування на інциденти кібербезпеки адаптована до національних вимог, зокрема до Професійного стандарту «Фахівець з реагування на інциденти кібербезпеки», фокусується на підготовці до виявлення, аналізу та нейтралізації атак через комплексні технічні навички, розуміння правових аспектів, розробку політик безпеки та управління інцидентами, поєднуючи як проактивні заходи (моніторинг, сканування вразливостей) та реактивні дії (розслідування, аналіз логів, збір доказів), а також комунікацію та роботу з інструментами (SIEM, EDR).

3. НАВЧАЛЬНІ МОДУЛІ ПРОГРАМИ

Модуль 1. СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Змістовний модуль 1. Система менеджменту інформаційної безпеки організації.

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

Модуль 2. ОРГАНІЗАЦІЯ ТА ЗАБЕЗПЕЧЕННЯ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

Змістовний модуль 1. Організація управління кіберінцидентами.

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

Змістовний модуль 2. Експлуатація та моніторинг систем захисту.

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

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

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

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

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 фахівців з реагування на інциденти кібербезпеки потрібні фахові компетентності, що охоплюють:

1. Технічні компетентності

Розуміння класифікації та аналізу кіберзагроз, тактик зловмисників (TTPs).

Аналіз мережевого трафіку, робота з технологіями виявлення вторгнень (IDS/IPS).

Здатність аналізувати файли журналів з різних джерел (хостів, мережевих пристроїв).

Сканування та розпізнавання вразливостей в системах.

Знання безпеки операційних систем, програмного забезпечення та комп'ютерних мереж.

2. Операційні та управлінські компетентності

Вміння керувати життєвим циклом інциденту, від виявлення до відновлення.

Застосування стратегій зниження ризиків.

Автоматизація процесів управління даними про загрози.

Забезпечення неперервності бізнесу під час інциденту.

3. М'які навички (Soft Skills)

Вміння чітко спілкуватися з різними рівнями керівництва та зацікавленими сторонами, включаючи використання протоколів обміну інформацією (наприклад, TLP).

Співпраця з іншими експертами та командами.

Здатність аналізувати складні ситуації та знаходити першопричини.

Здатність діяти ефективно в кризових ситуаціях.

4. Знання нормативної бази

Розуміння правових аспектів кібербезпеки та національних стандартів

Програмні результати навчання:

Програма підвищення кваліфікації «**Фахівець з реагування на інциденти кібербезпеки**» спрямовано на досягнення програмних **результатів навчання**, а саме у відповідності до трудових функцій професійного стандарту та визначеної кваліфікації (далі – ТФ):	
ТФ А РН 1	Відстеження, збір та документування даних про інциденти кібербезпеки з моменту їх виявлення до остаточної ідентифікації статусу події
ТФ Б РН 2	Проведення оцінки інцидентів кібербезпеки
ТФ В РН 3	Оброблення інцидентів кіберзахисту в режимі реального часу та вжиття заходів щодо пом’якшення наслідків кібербезпекових інцидентів, а також відновлення функціональності системи та процесів до робочого стану
ТФ Г РН 4	Моніторинг та оцінка поточного стану кібербезпеки
ТФ Д РН 5	Надання експертної технічної підтримки з управління кіберінцидентами
ТФ Е РН 6	Дослідження та аналіз кіберінцидентів

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 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 «Фахівець з реагування на інциденти кібербезпеки (трудові функції А, Б, В, Г, Д, Е)» професійного стандарту «Фахівець з реагування на інциденти кібербезпеки».

До одного варіанту тесту входить 40 тестових запитань.

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

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

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

Варіант тесту складається з 40 запитань. Розподіл запитань за трудовими функціями/змістовними розділами представлено у Таблиці 1. З 40 запитань 23 запитання мають рівень складності 1, 14 запитання рівень складності 2, 3 запитань – рівень складності 3.

На проходження варіанту тесту здобувачеві виділяється 1 година 20 хвилин:

$$23*1+14*3+3*5 = 80 \text{ хв.}$$

Таблиця 1

Відповідність Банку завдань та варіанту тесту професійної кваліфікації

Трудова функція	Найменування розділу	Питома вага розділу	Кількість запитань у варіанті тесту	Кількість запитань у Банку завдань
	Теоретичний модуль тестування знань	**60%**	**24**	**72**
А	Відстеження, збір та документування даних про інциденти кібербезпеки з моменту їх виявлення до остаточної ідентифікації статусу події	15%	6	18
Б	Проведення оцінки інцидентів кібербезпеки	15%	6	18
В	Оброблення інцидентів кіберзахисту в режимі реального часу та вжиття заходів щодо пом’якшення наслідків кібербезпекових інцидентів, а також відновлення функціональності системи та процесів до робочого стану	10%	4	12
Г	Моніторинг та оцінка поточного стану кібербезпеки	5%	2	6

Трудова функція	Найменування розділу	Питома вага розділу	Кількість запитань у варіанті тесту	Кількість запитань у Банку завдань
Д	Надання експертної технічної підтримки з управління кіберінцидентами	5%	2	6
Е	Дослідження та аналіз кіберінцидентів	10%	4	12
	Практичний модуль тестування навичок та вмінь	**40%**	**16**	**48**
А	Відстеження, збір та документування даних про інциденти кібербезпеки з моменту їх виявлення до остаточної ідентифікації статусу події	10%	4	12
Б	Проведення оцінки інцидентів кібербезпеки	10%	4	12
В	Оброблення інцидентів кіберзахисту в режимі реального часу та вжиття заходів щодо пом'якшення наслідків кібербезпекових інцидентів, а також відновлення функціональності системи та процесів до робочого стану	5%	2	6
Г	Моніторинг та оцінка поточного стану кібербезпеки	5%	2	6
Д	Надання експертної технічної підтримки з управління кіберінцидентами	5%	2	6
Е	Дослідження та аналіз кіберінцидентів	5%	2	6
			40	**120**

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

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

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

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

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

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

7. ЗАБЕЗПЕЧЕННЯ НАЯВНОСТІ НЕОБХІДНИХ ЗАСОБІВ ДЛЯ ОРГАНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ

Освітня програма фахівців з реагування на інциденти 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.