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 сфери захисту інформації

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 сфери захисту інформації 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 сфери захисту інформації. Фахівець сфери захисту інформації є критично важливим для захисту фінансової та конфіденційної інформації, забезпечення безперервності бізнесу, дотримання законодавчих вимог, підтримання довіри клієнтів, оскільки цифрові технології проникають у всі сфери життя, а кіберзагрози стають дедалі складнішими. Фахівці сфери захисту інформації мають вільно та ґрунтовно забезпечувати комплексний захист інформаційних систем від несанкціонованого доступу, модифікації чи знищення, використовуючи технічні засоби, організаційні заходи, розробку політик безпеки, постійний моніторинг, реагування на кіберзагрози, цілісності та доступності даних.

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 сфери захисту інформації», Розділ ІІІ професійного стандарту «Фахівець сфери захисту інформації», Національний класифікатор України ДК 003:2010 «Класифікатор професій» («Фахівець сфери захисту інформації» 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 СФЕРИ ЗАХИСТУ ІНФОРМАЦІЇ

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 – 58 год., практичні заняття – 16 год., самостійна робота – 96 год., консультації – 2 год., модульний контроль – 8 год.

Мета освітньої програми – формування у здобувачів курсу комплексної системи професійних знань, вмінь та навичок, необхідних для практичного забезпечення захищеності (конфіденційності, цілісності, доступності) інформації, що обробляється та передається в сучасних інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Програма готує фахівця, здатного ефективно протидіяти широкому спектру загроз, зокрема несанкціонованим діям з інформацією, її витоку технічними каналами та спеціальним впливам на засоби обробки. Окремим важливим завданням є формування навичок для захисту інформації, що озвучується на об'єктах інформаційної діяльності, через освоєння всього життєвого циклу комплексних систем захисту.

Функціональна спрямованість освітньої програми – полягає в забезпеченні конфіденційності, цілісності та доступності інформаційних систем шляхом розробки політик, впровадження технічних та організаційних заходів, моніторингу загроз, управління ключами та реагування на інциденти, а також підтримки безпекової культури в організації. Вони охоплюють адміністративну, технічну, програмну та фізичну сторони захисту, працюючи як на стратегічному (політики), так і на операційному рівнях (налаштування, моніторинг, аналіз).

Об'єкт вивчення: інформаційні системи (комп'ютерні, автоматизовані, телекомунікаційні, мережеві) та інформаційні ресурси (дані, потоки, бази даних), технології забезпечення їх безпеки, процеси управління кібербезпекою (ризики, політики, моніторинг), засоби захисту (програмно-апаратні комплекси), правове регулювання та методології захисту від кіберзагроз.

Цілі навчання: забезпечення конфіденційності, цілісності та доступності інформації розробка, впровадження та підтримка системи захисту від кіберзагроз, виявлення вразливостей, проведення аудиту безпеки, реагування на інциденти та розслідування кіберзлочинів, зменшення ризиків несанкціонованого доступу, втрат або пошкодження даних, захист інформаційних систем загалом.

Теоретичний зміст предметної області: охоплює фундаментальні знання, основи кібербезпеки та криптографії, принципи управління безпекою, методи виявлення загроз, технології захисту інформації, захист інформаційних ресурсів від реальних та потенційних загроз у кіберпросторі.

Методи, методики та технології: комплексні методи, методики аналізу, технології VPN, ІРП, "пісочниці" та ін. для забезпечення конфіденційності, цілісності та доступності даних, застосовуючи як програмні, так і технічні та організаційні підходи для захисту від кіберзагроз.

Інструменти та обладнання: комплекс програмних і технічних інструментів: антивіруси, міжмережеві екрани, системи виявлення/запобігання вторгненням, інструменти шифрування, ПЗ для контролю доступу, апаратні засоби для виявлення несанкціонованого прослуховування, спеціалізовані сканери безпеки, інструменти тестування на проникнення (penetration testing), системи SIEM, обладнання для захисту від електромагнітних витоків (TEMPEST) та пристрої для аналізу мережевого трафіку.

Фокус програми: Фокус програми "Фахівці сфери захисту інформації" (Кібербезпека, F5) зосереджений на підготовці експертів для протидії кіберзагрозам та забезпечення конфіденційності й цілісності даних, що охоплює аналіз вразливостей, розробку систем захисту (мережева безпека, криптографія), реагування на інциденти та застосування правових і організаційних методів для захисту інформаційних систем у комерційній та державній сферах.

Особливості програми: Програма підвищення кваліфікації фахівців сфери захисту інформації адаптована до національних вимог, зокрема до Професійного стандарту «Фахівець сфери захисту інформації», фокусується на підготовці професіоналів для забезпечення кібербезпеки, захисту конфіденційності, цілісності та доступності інформації, розробки та впровадження програмно-технічних засобів захисту, управлінні ризиками та створенні комплексних систем інформаційного захисту в умовах сучасних ІТ-загроз, охоплюючи мережеву безпеку, технічні системи та управління безпекою.

3. НАВЧАЛЬНІ МОДУЛІ ПРОГРАМИ

Модуль 1. СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Змістовний модуль 1. Система менеджменту інформаційної безпеки організації.

Основи і принципи побудови СМІБ (А1.З5, А1.З7, А4.З3, А5.З1, А5.З2). Планування та розроблення СМІБ (А1.З4, А3.З1, А7.З4, А7.З7, А8.З3). Реалізація та функціонування СМІБ (А1.З4, А3.З1, А3.З6, А4.З1, А4.З2, А7.З10, А8.З1). Моніторинг, аналіз і вдосконалення СМІБ (А3.З3, А5.З4, Б3.З1, В1.З3, В2.З1, В3.З1, В5.З1, В5.З5).

Модуль 2. ТЕХНІЧНІ ЗАСОБИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Змістовний модуль 1. Основи захисту інформації та технології безпеки.

Основи захисту інформації та криптологія (А1.З1, А1.З2, Б4.З5, А7.З1, А7.З3). Комп'ютерні мережі та їх захист (А1.З3, А6.З18, А6.З19, А7.З2, А7.З8, А7.З9, А7.З10). Архітектура безпеки та інфраструктура (А6.З3, А3.З1, А3.З2, А3.З3, А7.З1, А7.З2, А7.З4, А7.З6). Адміністрування систем та мереж (А8.З1, А8.З2, А8.З3, А8.З4, А7.З5, А7.З7, А7.З11, В2.З2).

Змістовний модуль 2. Експлуатація та моніторинг систем захисту.

Надійність і стійкість систем захисту (В1.З1, В1.З2, В1.З3, В2.З1, В2.З3). Тестування, діагностика та відновлення (В3.З1, В3.З2, В3.З3, В3.З4, В3.З5, В3.З6). Контроль стану систем захисту (В4.З1, В4.З2, В4.З3, В4.З4). Моніторинг загроз і виявлення атак (В5.З1, В5.З2, В5.З3, В5.З4, В5.З5). Сканування та виявлення вразливостей (В6.З1, В6.З2). Спеціальні дослідження та технічні канали витоку інформації (А6.З1, А6.З2, А6.З4, А6.З5, А6.З6, А6.З7, А6.З8, А6.З9, А6.З10, А6.З11, А6.З12, А6.З13, А6.З14, А6.З15, А6.З16, А6.З17). Оцінювання відповідності програмних та апаратних засобів захисту інформації (Г1.З1, Г1.З2, Г1.З3, Г1.З4, Г1.З5, Г1.З6, Г2.З1, Г2.З2, Г2.З3, Г2.З4, Г2.З5, Г2.З6, Г2.З7, Г2.З8).

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.З5, Д1.З2). Нормативно-правове забезпечення кібербезпеки та кріптографічного захисту інформації. (А1.З5, Д1.З2). Особливості кіберзахисту критичної інфраструктури України (секторальний підхід) та повноваження правоохоронних органів в цій сфері. (А1.З5). Загальні засади юридичної відповідальності. Види відповідальності за порушення законодавства у сфері обігу інформації, інформаційної безпеки та кібербезпеки. (А1.З5, Д1.З2). Кримінальна відповідальність за порушення законодавства у сфері обігу інформації, інформаційної безпеки та кібербезпеки (А1.З5, Д1.З2). 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 фахівця сфери захисту інформації потрібні фахові компетентності, що охоплюють:

1. Технічні:

Знання архітектур мереж, ОС, хмарних технологій, апаратного та програмного забезпечення.

Здатність проводити пентести та аналіз вразливостей.

Розуміння криптографічних методів захисту.

Вміння працювати із засобами захисту (Firewalls, IDS/IPS) та фізичними засобами.

2. Аналітичні та процесні:

Оцінка ризиків та загроз інформаційній безпеці.

Розробка політик, стандартів та процедур безпеки.

Управління інцидентами (Incident Response).

Відповідність стандартам та нормативним вимогам.

3. Правові та етичні:

Знання законодавства у сфері захисту даних (GDPR, українське законодавство).

Розуміння етичних принципів використання ІТ та захисту інформації.

4. Комунікативні та організаційні:

Здатність навчати користувачів (підвищення обізнаності).

Презентація результатів аналізів та рекомендацій (звітування).

Координація дій при інцидентах безпеки.

5. Безперервний розвиток:

Адаптуватися до нових технологій та загроз у кіберпросторі, постійно навчатися

Програмні результати навчання:

Програма підвищення кваліфікації «**Фахівець сфери захисту інформації**» спрямовано на досягнення програмних **результатів навчання**, а саме у відповідності до трудових функцій професійного стандарту та визначеної кваліфікації (далі – ТФ):	
ТФ А РН 1	Впровадження систем та комплексів захисту інформації.
ТФ Б РН 2	Оцінювання відповідності систем, комплексів та засобів захисту інформації.
ТФ В РН 3	Експлуатація та обслуговування систем і комплексів захисту інформації, моніторинг та аудит загроз для інформації.
ТФ Г РН 4	Оцінювання відповідності програмних та апаратних засобів технічного та криптографічного захисту інформації.

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 15 балів**)*	12
Усього за частиною №1	24
Частина №2	
Виконання та захист одного практичного заняття *(Для допуску до виконання модульної контрольної роботи здобувач має набрати **не менше 25 балів**)*	7
Усього за частиною №2	42
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 сфери захисту інформації (трудові функції А, Б, В, Г)» професійного стандарту «Фахівець сфери захисту інформації».

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	Впровадження систем та комплексів захисту інформації.	20%	8	24
Б	Оцінювання відповідності систем, комплексів та засобів захисту інформації.	15%	6	18
В	Експлуатація та обслуговування систем і комплексів захисту інформації, моніторинг та аудит загроз для інформації.	15%	6	18
Г	Оцінювання відповідності програмних та апаратних засобів технічного та криптографічного захисту інформації.	10%	4	12
	Практичний модуль тестування навичок та вмінь	**40%**	**16**	**48**
А	Впровадження систем та комплексів захисту інформації.	15%	6	18
Б	Оцінювання відповідності систем, комплексів та засобів захисту інформації.	10%	4	12
В	Експлуатація та обслуговування систем і комплексів захисту інформації, моніторинг та	10%	4	12

Трудова функція	Найменування розділу	Питома вага розділу	Кількість запитань у варіанті тесту	Кількість запитань у Банку завдань
	аудит загроз для інформації.			
Г	Оцінювання відповідності програмних та апаратних засобів технічного та криптографічного захисту інформації.	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 сфери захисту інформації 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.