МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний аерокосмічний університет
«Харківський авіаційний інститут»

ЗАТВЕРДЖЕНО

вченою радою Національного
аерокосмічного університету
«Харківський авіаційний інститут»
«24» грудня 2025 р., протокол № 5

КОНЦЕПЦІЯ ОСВІТНЬОЇ ДІЯЛЬНОСТІ

з підвищення кваліфікації
керівників структурних підрозділів з питань безпеки інформації та кіберзахисту
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 № 614 від 24» грудня 2025 р.

Харків 2025

ВСТУП

Розроблення Концепції освітньої діяльності з підвищення кваліфікації керівників структурних підрозділів з питань безпеки інформації та кіберзахисту 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 керівників структурних підрозділів з питань безпеки інформації та кіберзахисту на рівні світових аналогів. Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту є ключовим фахівцем, оскільки він відповідає за стратегічне управління кібербезпекою, захист критично важливої інформації, розробку політик, управління ризиками та забезпечення безперервності функціонування інформаційних систем, що є критично важливим для функціонування будь-якої організації чи державного органу в сучасному цифровому середовищі.

Концепція регламентує мету та завдання із забезпечення безперервного професійного розвитку та підвищення рівня професійних компетентностей керівників структурних підрозділів з питань безпеки інформації та кіберзахисту.

Нормативно-правовою базою розроблення та реалізації Концепції є: Типова програма підвищення кваліфікації «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту», Розділ ІІІ професійного стандарту «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту», Національний класифікатор України ДК 003:2010 «Класифікатор професій» («Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту» 1239), основні положення і вимоги визначені законами України «Про освіту», «Про вищу освіту», інші законодавчі і нормативні документи.

1. ОСВІТНЯ ПРОГРАМА З ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ КЕРІВНИКІВ СТРУКТУРНИХ ПІДРОЗДІЛІВ З ПИТАНЬ БЕЗПЕКИ ІНФОРМАЦІЇ ТА КІБЕРЗАХИСТУ

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 – 40 год., практичні заняття – 10 год., самостійна робота – 120 год., консультації – 2 год., модульний контроль – 8 год.

Мета освітньої програми – формування у здобувачів курсів системи професійних знань, вмінь та навичок щодо:

– прийняття рішень та визначення перспектив розвитку та забезпечення безпеки інформації та кіберзахисту інформаційних технологій, інформаційних систем/мереж та/або інфраструктури організації в цілому (зокрема критичної інформаційної інфраструктури);

– управління впровадженням стратегії, політик та системи менеджменту інформаційної безпеки та/або кібербезпеки організації в цілому;

– планування та керування розподілом відповідних інформаційних ресурсів, заходами з нейтралізації наслідків кіберінцидентів щодо порушень функціонування встановлених бізнес-операційних процесів та сталого функціонування інформаційних систем/мереж та/або інфраструктури організації в цілому (зокрема критичної інформаційної інфраструктури);

забезпечення обміну інформацією у сфері кібербезпеки та захисту інформації із зовнішніми зацікавленими сторонами.

Функціональна спрямованість освітньої програми – полягає у стратегічному управлінні ризиками, забезпеченні захисту інформаційних ресурсів та інфраструктури від загроз шляхом розробки політик, впровадження комплексних заходів, координації технічних і організаційних процесів, а також реагування на інциденти, що вимагає глибоких знань у галузі кібербезпеки та відповідності законодавству.

Об'єкт вивчення: інформаційні ресурси, їх інфраструктура та процеси управління; загрози й методи захисту від несанкціонованого доступу; пошкодження чи знищення в цифровому та фізичному форматах, що включає аналіз законодавства, впровадження політик, управління ризиками, реагування на інциденти та забезпечення кіберстійкості в умовах постійних кіберзагроз.

Цілі навчання: розвиток стратегічного бачення та практичних навичок для забезпечення кіберстійкості організації, розуміння державної політики у сфері кібербезпеки, ефективного управління ризиками, планування та впровадження комплексних заходів захисту від сучасних кіберзагроз, включаючи реагування на інциденти та захист критичної інфраструктури, задля гарантування конфіденційність, цілісність та доступність інформації.

Теоретичний зміст предметної області: знання законодавства (українського та міжнародних стандартів), принципів кіберзахисту, моделей управління доступом, криптографії, управління ризиками, технологій захисту, реагування на інциденти та розвитку стратегій кібербезпеки, формуючи розуміння управління безпекою, технічного захисту та стратегічного планування в умовах сучасних кіберзагроз.

Методи, методики та технології: методи стратегічного управління ризиками, планування реагування на інциденти, тестування на проникнення (пентести), forensic-аналіз, криптографічні методи, доступ (IAM), безпека хмарних та мобільних рішень, розвиток культури безпеки, використовуючи технології SIEM-систем, EDR/XDR, NGFW, DLP та методики ISO27001, NIST CSF, OWASP Top 10 для захисту інформації та інфраструктури від сучасних кіберзагроз.

Інструменти та обладнання: національні профстандарти, системи моніторингу (SIEM), інструменти для тестування, спеціалізовані тренувальні платформи та тестові стенди для симуляції атак, що готують керівників до стратегічного управління та оперативного реагування.

Фокус програми: Акцент на розвиток професійних компетентностей керівників структурних підрозділів з питань безпеки інформації та кіберзахисту, щодо вільного та ґрунтовного забезпечення розвитку управлінських навичок в умовах кіберзагроз, включаючи стратегічне планування кіберзахисту, управління ризиками, реагування на інциденти, забезпечення комплаєнсу, розробку політик безпеки та лідерство в умовах швидких технологічних змін, щоб забезпечити безперервність бізнесу та захист даних. Керівник повинен вирішувати складні завдання, інтеграцію кібербезпеки в бізнес-процеси та впроваджувати інноваційні рішення.

Особливості програми: Програма підвищення кваліфікації керівника структурного підрозділу з питань безпеки інформації та кіберзахисту адаптована до національних вимог, зокрема до Професійного стандарту «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту», фокусуються на стратегічному управлінні ризиками та інцидентами, розробці політик, відповідності законодавству, практичних тренуваннях з кібергігієни, відповідності національним стандартам, а також ефективно захищати державні й корпоративні ресурси від сучасних кіберзагроз, поєднуючи технічні та організаційні заходи.

3. НАВЧАЛЬНІ МОДУЛІ ПРОГРАМИ

Модуль 1. СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Змістовний модуль 1. Система менеджменту інформаційної безпеки організації.

Основи і принципи побудови СМІБ (А2.З4, А2.З5, Б1.З5). Планування та розроблення СМІБ (А1.З2, А2.З4, А3.З2, Б1.З1, Б1.З4, Б1.З5, В1.З4). Реалізація та функціонування СМІБ (А1.З2, А2.З4, Б1.З1, Б1.З4, Б1.З5, В1.З4). Моніторинг, аналіз і вдосконалення СМІБ (А3.З1, Б1.З5).

Модуль 2. СТРАТЕГІЯ ТА ОПЕРАЦІЙНА ДІЯЛЬНІСТЬ У КІБЕРБЕЗПЕЦІ

Змістовний модуль 1. Технічні та організаційні основи захисту інформаційних систем.

Основи мережевої безпеки (А1.З1, А3.З3, Б1.З3). Класифікація та аналіз кіберзагроз і вразливостей (А3.З4, Б2.З4, Б2.З5, Б4.З3, В1.З1). Організація захисту інформаційних ресурсів (А1.З3, А1.З4, Б3.З1, Б3.З3). Моделі зрілості інформаційно-комунікаційних систем, засобів захисту інформації, систем кібербезпеки та організації в цілому (Б2.З2).

Змістовний модуль 2. Управління, комунікація та контроль у системі кібербезпеки організації.

Засоби аудиту та контролю безпеки інформації та кіберзахисту (В1.З3). Розвиток кадрового потенціалу та комунікація з керівництвом у сфері кібербезпеки (А3.З5, В2.З1, В2.З2, В2.З3, В3.З1). Методологія та етика управління процесами, проєктами та програмами кібербезпеки (А1.З5, Б2.З1, Б2.З3, Б3.З3, Г1.З1, Г1.З2, Г1.З3). Стратегічна взаємодія та комунікація із зацікавленими сторонами в кібербезпеці (Г2.З1, Г3.З1, Г3.З2).

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, захисту інформації та забезпечення приватності даних (А2.З1, А2.З2, Б4.З2). Міжнародні нормативно-правові акти і стандарти, національне законодавство у сфері кібербезпеки та захисту інформаційних ресурсів організацій і підприємств різних форм власності (А1.З6, Б4.З1). Загальні засади юридичної відповідальності. Дисциплінарна, адміністративна та кримінальна відповідальність за порушення законодавства у сфері обігу інформації, інформаційної безпеки та кібербезпеки. Психологічні основи етичного хакінгу, забезпечення приватності даних, інформаційної безпеки та кібербезпеки (Б4.З2, Г1.З2).

4. ПЕРЕЛІК ОСНОВНИХ КОМПЕТЕНТНОСТЕЙ ТА РЕЗУЛЬТАТІВ НАВЧАННЯ

Загальні компетентності:

1. 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.

2. Здатність діяти активно, відповідально й ефективно реалізовувати громадянські права та обовязки з метою розвитку демократичного громадянського суспільства, усвідомлювати та сповідувати цінності громадянського суспільства.

3. Здатність виявляти повагу та цінувати українську національну культуру, багатоманітність і мультикультурність у суспільстві.

4. Здатність генерувати і втілювати нові ідеї у сферу інформаційної безпеки, що базується на креативності, творчості, відчутті нового, здатності до здорового ризику.

Фахові (предметно-орієнтовані) компетентності:

Для керівників структурних підрозділів з питань безпеки інформації та кіберзахисту потрібні фахові компетентності, що охоплюють:

1. *Стратегічне управління та лідерство*: розробка та впровадження політик інфобезпеки; управління кіберризиками (Risk Management) організація робіт з авторизації систем та управління доступом; побудова культури кіберстійкості.

2. *Технічні та операційні знання*: теорія та класифікація кіберзагроз; моніторинг подій та реагування на інциденти (CSIRT); практики захисту мереж, систем та даних; використання антивірусного ПЗ та сучасних засобів захисту.

3. *Нормативно-правова база та стандарти*: знання законодавства України у сфері кібербезпеки; впровадження національних та міжнародних стандартів (ISO 27001, NIST); професійна кваліфікація відповідно до профстандартів (зокрема, «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту»).

4. *Управління персоналом та навчання*: організація тренінгів та інструктажів з кібергігієни; формування команди фахівців з кібербезпеки.

Програмні результати навчання:

Програма підвищення кваліфікації «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту» спрямовано на досягнення програмних результатів навчання, а саме у відповідності до трудових функцій професійного стандарту та визначеної кваліфікації (далі – ТФ):	
ТФ А РН 1	Обґрунтування, визначення, розроблення та формування стратегії, політики, планів та процедур кібербезпеки в організації (підприємстві, установі) або програмі.
ТФ Б РН 2	Керування процесами, процедурами впровадження та супроводження політики і стратегії кібербезпеки в організації (підприємстві, установі) або програмі.
ТФ В РН 3	Консультування вищого керівництва щодо рівня ризику та стану безпеки, аналізу витрат/зисків, програм, політик, процесів, систем та елементів інформаційної безпеки та кібербезпеки.
ТФ Г РН 4	Співпраця із зацікавленими сторонами з метою забезпечення безперервної діяльності організації (підприємства, установи) в рамках програми, стратегії та виконання завдань політики безпеки.

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 оцінювання на базі автоматизованої системи 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 «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту (трудові функції А, Б, В, Г)» професійного стандарту «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту».

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	Обґрунтування, визначення, розроблення та формування стратегії, політики, планів та процедур кібербезпеки в організації (підприємстві, установі) або програмі.	14%	6	18
Б	Керування процесами, процедурами впровадження та супроводження політики і стратегії кібербезпеки в організації (підприємстві, установі) або програмі.	15%	6	18
В	Консультування вищого керівництва щодо рівня ризику та стану безпеки, аналізу витрат/зисків, програм, політик, процесів, систем та елементів інформаційної безпеки та кібербезпеки.	21%	8	24
Г	Співпраця із зацікавленими сторонами з метою забезпечення безперервної діяльності організації (підприємства, установи) в рамках програми, стратегії та виконання завдань політики безпеки.	10%	4	12
	Практичний модуль тестування навичок та вмінь	**40%**	**16**	**48**
А	Обґрунтування, визначення, розроблення та формування стратегії, політики, планів та процедур кібербезпеки в організації (підприємстві, установі) або програмі.	10%	4	12

Трудова функція	Найменування розділу	Питома вага розділу	Кількість запитань у варіанті тесту	Кількість запитань у Банку завдань
Б	Керування процесами, процедурами впровадження та супроводження політики і стратегії кібербезпеки в організації (підприємстві, установі) або програмі.	10%	4	12
В	Консультування вищого керівництва щодо рівня ризику та стану безпеки, аналізу витрат/зисків, програм, політик, процесів, систем та елементів інформаційної безпеки та кібербезпеки.	14%	7	21
Г	Співпраця із зацікавленими сторонами з метою забезпечення безперервної діяльності організації (підприємства, установи) в рамках програми, стратегії та виконання завдань політики безпеки.	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 керівників структурних підрозділів з питань безпеки інформації та кіберзахисту 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.