МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ФОРМУВАННЯ КВАЛІФІКАЦІЙНИХ ВИМОГ ДО ФАХІВЦІВ З КІБЕРБЕЗПЕКИ: АНАЛІЗ ОСНОВНИХ ПІДХОДІВ ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Даниїл КОРОБЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Даниїл КОРОБЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Тетяна МУЖАНОВА
к.держ.упр., доцент Ім’я, ПРІЗВИЩЕ

Рецензент:

Ім’я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Коробенку Даниїлу Олександровичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Формування кваліфікаційних вимог до фахівців з кібербезпеки: аналіз основних підходів”,
керівник кваліфікаційної роботи МУЖАНОВА Тетяна Михайлівна, к.держ.упр., доцент,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51

2. Строк подання кваліфікаційної роботи “12” травня 2026р.
3. Вихідні дані до кваліфікаційної роботи: *кваліфікаційні вимоги до фахівців з кібербезпеки, міжнародні підходи щодо формування кваліфікаційних вимог до кіберфахівців (NICE Framework, EFCS), система формування кваліфікаційних вимог до фахівців з кібербезпеки в Україні.*
4. Перелік питань, які мають бути розроблені:
   4.1. Дослідити теоретичні засади формування кваліфікаційних вимог до фахівців з кібербезпеки.
   4.2. Проаналізувати міжнародні й національні підходи до формування кваліфікаційних вимог до фахівців з кібербезпеки.
   4.3. Визначити напрями вдосконалення системи формування кваліфікаційних вимог до кіберфахівців в Україні й розробити рекомендації на основі кращого міжнародного досвіду.
5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Дослідження теоретичних засад формування кваліфікаційних вимог до фахівців з кібербезпеки.	08.04.2026	
4.	Аналіз міжнародних і національних підходів до формування кваліфікаційних вимог до фахівців з кібербезпеки.	15.04.2026	
5.	Визначення напрямів удосконалення системи формування кваліфікаційних вимог до кіберфахівців в Україні й розробка рекомендацій на основі кращого міжнародного досвіду.	22.04.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	10.06.2026	
10.	Захист в ЕК.	__.06.2026	

Здобувач вищої освіти _____ Даниїл КОРОБЕНКО

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна МУЖАНОВА

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Коробенко Д.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Формування кваліфікаційних вимог до фахівців з кібербезпеки: аналіз основних підходів"

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач КОРОБЕНКО Даниїл у кваліфікаційній роботі дослідив теоретичні засади формування кваліфікаційних вимог до фахівців з кібербезпеки, проаналізував міжнародні й національні підходи до формування кваліфікаційних вимог до фахівців з кібербезпеки, зокрема Рамку NICE та EFCS, визначив напрями вдосконалення засад формування кваліфікаційних вимог до кіберфахівців в Україні й розробив рекомендації на основі кращого міжнародного досвіду.

КОРОБЕНКО Даниїл показав глибоке розуміння проблеми дослідження та різностороннє бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження. Здобувач проявив себе як відповідальний виконавець з високим рівнем самоорганізації і виконавської дисципліни. Результати дослідження апробовані на конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 25 лютого 2026 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача КОРОБЕНКА Даниїла на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) (Ім'я, ПРІЗВИЩЕ)

"____"_____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Коробенко Д.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) (Ім'я, ПРІЗВИЩЕ)

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти КОРОБЕНКА Даниїла

на тему “Формування кваліфікаційних вимог до фахівців з кібербезпеки: аналіз основних підходів”

Актуальність. В умовах швидкої цифровізації усіх сфер життєдіяльності суспільства забезпечення кібербезпеки є нагальним і життєво важливим завданням. Як свідчить статистика, одним із чинників, що ускладнюють досягнення цілей кібербезпеки, є нестача кваліфікованих спеціалістів. Причинами такої ситуації часто є неналежна професійна підготовка. Фахове навчання у сфері кібербезпеки має починатися з формування набору кваліфікаційних вимог до кіберспеціалістів, що є передумовою набуття ними необхідних і затребуваних на ринку праці компетенцій, і, як результат, - заповнення прогалин у забезпеченні галузі кваліфікованою робочою силою.

З огляду на зазначене дослідження засад формування кваліфікаційних вимог до фахівців з кібербезпеки на основі кращих міжнародних підходів є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено міжнародні й національні підходи до формування кваліфікаційних вимог до фахівців з кібербезпеки.

2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді таблиць і рисунків.

3. Автор опрацював достатню джерельну базу, в тому числі англомовні наукові публікації, нормативно-правові документи, професійні стандарти.

4. За результатами дослідження запропоновано рекомендації щодо вдосконалення засад формування кваліфікаційних вимог до кіберфахівців в Україні на основі кращого міжнародного досвіду.

Недоліки.

Доцільно було б приділити більше уваги висвітленню управлінських та інституційних аспектів процесів формування кваліфікаційних вимог до фахівців з кібербезпеки в Україні, зокрема розробки оновлених професійних стандартів.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на високому науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач КОРОБЕНКО Даниїл заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:

_____

підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню засад формування кваліфікаційних вимог до фахівців з кібербезпеки на основі аналізу кращих міжнародних підходів. Робота складається зі вступу, трьох розділів, що містять 9 таблиць і 3 рисунки, висновків і списку використаних джерел із 40 найменувань. Загальний обсяг роботи становить 74 аркуші, з яких 6 аркушів займають перелік умовних скорочень і список використаних джерел.

Метою роботи є дослідження засад формування кваліфікаційних вимог до фахівців з кібербезпеки на основі аналізу кращих міжнародних підходів і розробка рекомендацій щодо вдосконалення системи формування кваліфікаційних вимог до кіберфахівців в Україні.

Об'єктом дослідження є засади формування кваліфікаційних вимог до фахівців у сфері кібербезпеки на основі аналізу кращих міжнародних підходів.

Предмет дослідження – система кваліфікаційних вимог до фахівців у сфері кібербезпеки.

Методи дослідження. Для вирішення означеного наукового завдання в роботі використано методи системного аналізу, порівняльного аналізу, узагальнення, структурно-логічного моделювання, вивчення нормативно-правових документів і наукової літератури.

Як результат у роботі досліджено теоретичні засади формування кваліфікаційних вимог до фахівців з кібербезпеки; проаналізовано міжнародні й національні підходи до формування кваліфікаційних вимог до фахівців з кібербезпеки; визначено напрями вдосконалення системи формування кваліфікаційних вимог до кіберфахівців в Україні й розроблено рекомендації на основі кращого міжнародного досвіду.

Галузь застосування. Напрацювання дослідження й розроблені рекомендації можуть бути використані для оновлення професійних стандартів, вдосконалення освітніх програм зі спеціальності 125 «Кібербезпека», а також для планування програм підвищення кваліфікації та атестації фахівців з кібербезпеки.

Ключові слова: КВАЛІФІКАЦІЙНІ ВИМОГИ ДО ФАХІВЦІВ З КІБЕРБЕЗПЕКИ, NICE FRAMEWORK, EFCS, СИСТЕМА ФОРМУВАННЯ КВАЛІФІКАЦІЙНИХ ВИМОГ ДО ФАХІВЦІВ З КІБЕРБЕЗПЕКИ В УКРАЇНІ.

ABSTRACT

The qualification work is devoted to the study of the principles of formation of qualification requirements for cybersecurity specialists based on the analysis of the best international approaches. The work consists of an introduction, three chapters containing 9 tables and 3 figures, conclusions and a list of references with 40 titles. The total volume of the work is 74 pages, of which 6 pages are occupied by the list of abbreviations and the list of references.

The purpose of the work is to study the principles of formation of qualification requirements for cybersecurity specialists based on the analysis of the best international approaches and to develop recommendations for improving the system of formation of qualification requirements for cyber specialists in Ukraine.

The object the study is the system of formation of qualification requirements for cybersecurity specialists based on the analysis of the best international approaches.

The subject of the study is the system of qualification requirements for cybersecurity specialists.

Research methods. To solve the set scientific task, the methods of system analysis, comparative analysis, generalization, structural-logical modeling, study of normative-legal documents, and scientific literature were used.

As a result, the work investigated the theoretical principles of forming qualification requirements for cybersecurity specialists; analyzed international and national approaches to forming qualification requirements for cybersecurity specialists; identified areas for improving the system of forming qualification requirements for cyber specialists in Ukraine and developed recommendations based on the best international experience.

Field of application. Research results and developed recommendations can be used to update professional standards, improve educational programs in specialty 125 "Cybersecurity", as well as for planning a program of advanced training and certification of cybersecurity specialists.

Keywords: QUALIFICATION REQUIREMENTS FOR CYBERSECURITY SPECIALISTS, NICE FRAMEWORK, EFCS, SYSTEM OF FORMATION OF QUALIFICATION REQUIREMENTS FOR CYBERSECURITY SPECIALISTS IN UKRAINE.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

AI	Artificial Intelligence
CISA	Cybersecurity and Infrastructure Security Agency
DPA	Data Protection Authority
ECSF	European Cybersecurity Skills Framework
ENISA	European Union Agency for Cybersecurity
FSCF	Future Skills and Competences Framework
FSSC	Financial Services Skills Commission
GCI	Global Cybersecurity Index
GDPR	General Data Protection Regulation
ISC²	International Information System Security Certification Consortium
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ML	Machine Learning
NICE	National Initiative for Cybersecurity Education
NIS2	Directive (EU) 2022/2555
NIST	National Institute of Standards and Technology
OT/ICS	Operational Technology / Industrial Control Systems
SFIA	Skills Framework for the Information Age
TKS	Task – Knowledge – Skill
НРК	Національна рамка кваліфікацій

ВСТУП

Актуальність теми. Сучасний розвиток інформаційного суспільства супроводжується стрімким зростанням кіберзагроз, що ставить під питання національну безпеку держав, стабільність критичної інфраструктури та захист персональних даних громадян. За даними ENISA та NIST, щорічно кількість кібератак зростає в геометричній прогресії, а їхня складність і наслідки набувають стратегічного характеру. В умовах повномасштабної російської агресії проти України питання кібербезпеки набуло особливої гостроти: щоденні атаки на державні органи, енергетичну інфраструктуру, фінансову систему та оборонний сектор вимагають наявності висококваліфікованих фахівців, здатних не лише реагувати на інциденти, а й прогнозувати та запобігати їм.

Однак підготовка та підвищення кваліфікації спеціалістів з кібербезпеки в Україні стикається з низкою системних проблем: невідповідність освітніх програм реальним потребам ринку праці, фрагментарність професійних стандартів, недостатня інтеграція міжнародного досвіду та швидке застарівання компетентностей через динаміку розвитку технологій.

З огляду на зазначене, дослідження засад формування кваліфікаційних вимог до фахівців з кібербезпеки на основі передових міжнародних підходів є актуальним і своєчасним науковим завданням.

Метою роботи є дослідження засад формування кваліфікаційних вимог до фахівців з кібербезпеки на основі аналізу кращих міжнародних підходів і розробка рекомендацій щодо вдосконалення системи формування кваліфікаційних вимог до кіберфахівців в Україні.

Об'єктом дослідження є засади формування кваліфікаційних вимог до фахівців у сфері кібербезпеки на основі аналізу кращих міжнародних підходів.

Предмет дослідження – система кваліфікаційних вимог до фахівців у сфері кібербезпеки.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Дослідити теоретичні засади формування кваліфікаційних вимог до

фахівців з кібербезпеки.

2. Проаналізувати міжнародні й національні підходи до формування кваліфікаційних вимог до фахівців з кібербезпеки.

3. Визначити напрями вдосконалення системи формування кваліфікаційних вимог до кіберфахівців в Україні й розробити рекомендації на основі кращого міжнародного досвіду.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використано методи системного аналізу, порівняльного аналізу, узагальнення, структурно-логічного моделювання, вивчення нормативно-правових документів та наукової літератури.

Практичне значення одержаних результатів. Розроблені рекомендації щодо гібридної національної моделі кваліфікаційних вимог (поєднання деталізованої TKS-структури NICE з рольовим підходом ECSF) можуть бути використані для оновлення професійних стандартів Адміністрації Держспецзв'язку України, вдосконалення освітніх програм зі спеціальності 125 «Кібербезпека», а також для планування програм підвищення кваліфікації та атестації фахівців.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 25 лютого 2026 року.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ КВАЛІФІКАЦІЙНИХ ВИМОГ ДО ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

1.1 Проблеми підготовки та підвищення кваліфікації фахівців у галузі кібербезпеки

Сучасний кіберпростір характеризується стрімким зростанням обсягу, складності та руйнівної сили кіберзагроз, які трансформувалися з локальних технічних інцидентів у системні ризики національного та глобального масштабу. За даними Звіту за результатами глобального дослідження щодо прогалин у навичках з кібербезпеки від компанії Fortinet 2025 року (Cybersecurity Skills Gap Global Research Report [1], у 2024 році 86% організацій зазнали щонайменше одного витоку інформації, причому 28% з них 5 і більше інцидентів. Порівняно з 2021 роком, коли лише 19 % організацій повідомляли про 5 і більше порушень безпеки, ситуація значно погіршилася. Більше половини респондентів (52%) зазначили, що наслідки таких інцидентів перевищили 1 млн доларів США. Головними причинами успішних атак залишаються: людський фактор та недостатня обізнаність у питаннях безпеки (56%), брак навичок та підготовки в сфері IT-безпеки (54%) та відсутність відповідних засобів захисту (50%).

У таких умовах традиційна модель підготовки фахівців, яка акцентує увагу переважно на засвоєнні теоретичних знань, демонструє очевидну обмеженість. Сучасні кіберзагрози вимагають від спеціалістів не лише глибоких теоретичних знань, а й розвинених практичних умінь, здатності до швидкого реагування в умовах невизначеності та постійного оновлення компетенцій.

Звіт групи компаній Allianz про стійкість кібербезпеки 2025 року (Cyber Security Resilience Report 2025) [2] прогнозує, що брак IT-навичок до 2026 року коштуватиме світовій економіці близько 5,5 трлн доларів США через затримки проєктів, зниження якості послуг та втрату доходів.

Кожне успішне порушення безпеки, яке спричинене недостатньою підготовкою персоналу, призводить до значних прямих і непрямих втрат. За

даними Fortinet, середній час відновлення після інциденту становить 2,5 місяці, а втрати від кіберінцидентів з порушеннями бізнес-процесів складають понад 50% вартості великих страхових претензій. Окрім цього, Світовий економічний форум (World Economic Forum) у своєму звіті Global Cybersecurity Outlook 2026 [3] зазначає, що 56% керівників організацій з низьким рівнем кіберстійкості вважають саме дефіцит кібернавичок головною перешкодою для підвищення стійкості своїх підприємств.

Саме тому виникає необхідність переходу від традиційного освітнього підходу, орієнтованого переважно на теоретичну підготовку, до моделі, заснованої на навичках (skill-based approach). Відсутність чітко визначених кваліфікаційних вимог можна розглядати як один із суттєвих факторів, що зумовлює зростання кількості та тяжкості кіберінцидентів. Без єдиних стандартів, які б встановлювали чіткі критерії знань, умінь і навичок, неможливо об’єктивно оцінювати рівень підготовки фахівців, планувати їхній професійний розвиток та адаптувати освітні програми до реальних потреб ринку праці та національної безпеки.

Не менш серйозними є проблеми з розробкою освітніх програм і професійних стандартів. Без єдиної рамки кваліфікаційних вимог навчальні плани залишаються розрізненими, а професійні стандарти — фрагментарними та недостатньо деталізованими. Це призводить до дублювання тем, прогалин у ключових компетенціях (наприклад, у сфері AI-безпеки, цифрової криміналістики чи захисту критичної інфраструктури) та відсутності чітких критеріїв оцінювання результатів навчання. У підсумку система освіти не встигає за швидкістю змін у кіберпросторі, а професійні стандарти не стають надійним орієнтиром ні для викладачів, ні для роботодавців.

За даними консорціуму ISC² [4] та компанії Fortinet [1], лише близько 30–35 % випускників кіберспеціальностей одразу можуть виконувати профільні завдання без тривалого донавчання. Така ситуація змушує роботодавців витрачати значні кошти та час на внутрішнє навчання, що знижує конкурентоспроможність як окремих компаній, так і галузі в цілому.

Наслідки такого дефіциту є багатогранними. По-перше, зростає вразливість критичної інфраструктури (енергетика, транспорт, державне управління), що щодня зазнає тисяч кібератак. По-друге, бізнес змушений компенсувати брак кадрів автоматизацією та готовими рішеннями, що знижує ефективність захисту та підвищує залежність від іноземних постачальників. По-третє, ускладнюється виконання міжнародних зобов'язань України, зокрема щодо імплементації Директиви (ЄС) 2022/2555 (NIS2), яка вимагає призначення кваліфікованих менеджерів з кібербезпеки в компаніях.

За оцінками керівництва Адміністрації Держспецзв'язку України [5], дефіцит професійних кадрів у сфері захисту інформації та кіберзахисту може сягати 100 тисяч осіб. При цьому українські заклади вищої освіти щороку випускають тисячі спеціалістів за спеціальністю 125 «Кібербезпека» (з 2025 року - F5 «Кібербезпека та захист інформації», однак більшість із них не мають міжнародно визнаних професійних сертифікатів, що суттєво ускладнює підтвердження їх реальної кваліфікації та працевлаштування на відповідні посади.

За даними Міжнародного союзу електрозв'язку (ITU) [6], кібербезпека залишається одним із найвразливіших напрямів цифрової трансформації країни. Більше 60% українських компаній уже переходять на готові (off-the-shelf) рішення з кібербезпеки саме через гострий брак кваліфікованих фахівців.

Підтвердженням системних прогалин у розвитку кадрового потенціалу є дані Глобального індексу кібербезпеки (Global Cybersecurity Index, GCI) 2024. Як видно з рисунку 1.1, Україна отримала найнижчий бал саме в категорії заходів розвитку спроможностей (Capacity Development Measures) - 14,61 із 20 можливих. Ця категорія безпосередньо стосується освіти, професійної підготовки, підвищення кваліфікації фахівців, програм обізнаності населення та розвитку кадрового потенціалу в галузі кібербезпеки.

Для порівняння, результати України за іншими категоріями GCI виглядають значно сильнішими:

➢ Правові заходи (Legal Measures) - 19,42 балів (один із найвищих показників);

- ➢ Технічні заходи (Technical Measures) - 17,35 балів;
- ➢ Організаційні заходи (Organizational Measures) - 15,97 балів;
- ➢ Заходи зі співпраці (Cooperation Measures) — 16,58 балів.

Така диспропорція яскраво демонструє, що основні проблеми національної системи кібербезпеки України полягають не в законодавстві чи технічній базі, а саме в недостатньому рівні розвитку потенціалу кадрів і безперервного професійного розвитку фахівців. Такий низький показник у категорії заходів розвитку спроможностей яскраво демонструють суттєву відсталість у сфері підготовки та підвищення кваліфікації фахівців з кібербезпеки, яка не відповідає масштабам і складності сучасних кіберзагроз.

Рис. 1.1. Профіль України за GCI 2024 за п’ятьма ключовими категоріями

Війна з Росією суттєво поглибила кадрову проблему. Масова міграція спеціалістів (близько 8 млн осіб виїхали з країни після 2022 року), мобілізація до лав ЗСУ та внутрішнє переміщення населення призвели до значного скорочення пропозиції кваліфікованих кадрів на ринку праці. За оцінками аналітиків, телекомунікаційний і кіберсектор втратили значну частину досвідчених працівників через еміграцію та переорієнтацію на оборонні завдання. Крім того, обмежене фінансування державних програм підготовки та низький рівень

матеріального стимулювання фахівців у державному секторі порівняно з приватним (особливо IT-компаніями, що працюють на експорт) ускладнюють утримання талантів. Стратегія кібербезпеки України на 2021–2025 роки прямо визнавала «невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців» однією з ключових системних проблем, проте повномасштабне вторгнення зробило цю проблему критичною.

Саме ці наслідки є найнебезпечнішими для національної безпеки та захисту критичної інфраструктури. Відсутність чітких вимог до кваліфікації фахівців, які відповідають за безпеку енергетичних об'єктів, транспортних систем, державних реєстрів і банківської сфери, суттєво підвищують вразливість України до кібератак. Насамперед це унеможливлює ефективний відбір, об'єктивну оцінку та планомірне підвищення кваліфікації персоналу. Роботодавці змушені покладатися на суб'єктивні критерії (наявність диплома, стаж роботи, самооцінка кандидата), що часто не відображає реального рівня компетентності. У результаті на ключові посади потрапляють фахівці, які не володіють необхідним набором знань, умінь і навичок, а процес атестації та кар'єрного зростання стає хаотичним і неефективним.

Подолання цих наслідків можливе лише через розробку сучасної, компетентнісно орієнтованої системи кваліфікаційних вимог, яка стане основою для якісної підготовки та безперервного професійного розвитку фахівців з кібербезпеки.

Чітко сформульовані кваліфікаційні вимоги до фахівців з кібербезпеки відіграють роль системоутворюючого елемента, який забезпечує узгодженість між потребами ринку праці, системою освіти та державною політикою у сфері національної безпеки. Вони виступають універсальним інструментом, що дозволяє перейти від хаотичного кадрового забезпечення до цілеспрямованої та ефективної підготовки висококваліфікованих спеціалістів.

Для роботодавців кваліфікаційні вимоги є основою ефективного відбору персоналу, об'єктивної атестації та стратегічного кар'єрного планування. Наявність чітких критеріїв (компетентності, рівні володіння навичками,

необхідні сертифікати) дає можливість проводити структуровані співбесіди, оцінювати кандидатів за єдиними стандартами та зменшувати ризик помилкового найму. Крім того, вони дозволяють будувати чіткі кар'єрні шляхи, планувати внутрішнє навчання та оцінювати ефективність інвестицій у розвиток персоналу. За відсутності таких вимог компанії змушені витрачати значні ресурси на додаткову підготовку працівників або ризикувати безпекою власної інфраструктури.

Для закладів вищої освіти кваліфікаційні вимоги стають фундаментом для розробки сучасних освітніх програм, навчальних планів і матриць компетентності. Вони дозволяють чітко визначити очікувані результати навчання (learning outcomes), інтегрувати практичні компоненти (робота на кіберполігонах, симуляції інцидентів), а також узгодити зміст дисциплін з реальними потребами ринку. Завдяки цьому випускники отримують не лише теоретичні знання, а й практичні уміння та навички, що значно підвищує їхню конкурентоспроможність і зменшує термін адаптації молодих фахівців на робочому місці.

Для держави кваліфікаційні вимоги є ключовим засобом регулювання, сертифікації та розробки професійних стандартів. Вони дозволяють привести національне законодавство у відповідність до міжнародних рамок (NICE, ECSF), забезпечити єдині вимоги до фахівців, які працюють з критичною інфраструктурою, та створити національну систему сертифікації. Крім того, професійні стандарти, побудовані на основі кваліфікаційних вимог, стають обов'язковою підставою для ліцензування діяльності, атестації державних службовців і виконання міжнародних зобов'язань України у сфері кібербезпеки.

Для самого фахівця чіткі кваліфікаційні вимоги надають прозорі орієнтири професійного розвитку та підвищення кваліфікації. Вони дозволяють зрозуміти, яких саме компетенцій бракує для переходу на наступний рівень, спланувати індивідуальну траєкторію навчання, обрати необхідні сертифікації та об'єктивно оцінити власний професійний рівень. Це сприяє мотивації, зменшує ризик професійного вигорання та підвищує мобільність фахівців на ринку праці.

З огляду на це, кваліфікаційні вимоги мають стратегічне значення для всіх зацікавлених сторін. Вони є необхідною передумовою подолання як кількісного, так і якісного дефіциту кадрів у сфері кібербезпеки. Без їх чіткого формулювання неможливо забезпечити ефективну підготовку фахівців, якісне функціонування системи освіти, стабільність ринку праці, а також забезпечення належного рівня кіберзахисту національної критичної інфраструктури й національної безпеки України.

1.2 Сутність, значення та структура кваліфікаційних вимог у сфері кібербезпеки

Кваліфікаційні вимоги у сфері кібербезпеки являють собою систематизований комплекс критеріїв, що визначають мінімально необхідний рівень підготовки фахівця для ефективного виконання професійних завдань у динамічному середовищі кіберзагроз. Вони охоплюють не лише теоретичні знання, а й практичні уміння, навички, компетентності та рівень їхнього застосування в реальних ситуаціях. За визначенням, наведеним у міжнародних дослідженнях, кваліфікаційні вимоги — це формалізований опис очікуваних результатів професійної діяльності, виражений через набір завдань (tasks), знань (knowledge), умінь і навичок (skills & abilities), компетентності (competence), а також відповідні рівні кваліфікації/ фаховості (proficiency levels).

➢ Завдання (tasks) - це конкретні професійні дії або функції, які повинен виконувати фахівець (наприклад, аналіз вразливостей, реагування на кіберінцидент, оцінка ризиків).

➢ Знання (knowledge) - теоретична база, необхідна для розуміння сутності процесів і загроз (криптографія, архітектура мереж, правові аспекти захисту інформації тощо).

➢ Уміння (abilities) - здатність свідомо застосовувати знання для вирішення конкретних завдань.

➢ Навички (skills) - автоматизовані, доведені до високого рівня досконалості дії, які виконуються швидко і ефективно.

➢ Компетентність (competence) - інтегральна характеристика, яка поєднує знання, уміння, навички та особистісні якості фахівця, забезпечуючи його здатність ефективно діяти в реальних, часто нестандартних умовах.

➢ Рівень кваліфікації (proficiency) - шкала володіння, з якою фахівець демонструє певну компетентність, уміння чи навичку

Суттєвою відмінністю кваліфікаційних вимог від традиційних освітніх стандартів є їхня орієнтація на результат професійної діяльності, а не на процес навчання. Якщо освітні стандарти, як правило, фіксують перелік дисциплін, обсяг годин і форми контролю, то кваліфікаційні вимоги акцентують увагу на тому, що саме повинен володіти і бути здатним робити фахівець після завершення підготовки. Вони також відрізняються від професійних кваліфікацій, які часто мають вузькоспеціалізований характер і підтверджуються через сертифікацію (наприклад, CISSP, CISM). Кваліфікаційні вимоги є ширшим поняттям: вони слугують основою як для розробки освітніх програм, так і для створення професійних стандартів і систем сертифікації.

Порівняльний аналіз ключових міжнародних фреймворків компетенцій у сфері кібербезпеки дозволяє не лише виявити спільні та відмінні компоненти структури кваліфікаційних вимог, але й оцінити їх практичну застосовність у різних організаційних і галузевих контекстах.

Рамка навичок для інформаційної епохи (Skills Framework for the Information Age, SFIA) є однією з найзріліших і найпоширеніших глобальних моделей компетенцій у сфері інформаційних технологій, цифрової трансформації та кібербезпеки. Фреймворк був розроблений Фондом SFIA у 2000 році та регулярно оновлюється (актуальна версія - SFIA 9) [7]. Його активно застосовують урядові структури, великі корпорації, освітні установи та консалтингові компанії майже в 200 країнах світу.

Рамка базується на семи рівнях відповідальності (levels of responsibility), які формують основу для опису всіх професійних навичок. Кожен рівень має

керівну фразу (guiding phrase), яка вказує на основну дію, та стислий виклад основної суті рівня (essence of the level). Ці рівні відображають прогресивне зростання автономії, впливу, складності завдань, обсягу знань та бізнес-орієнтованих поведінкових факторів, що дозволяють фахівцю з кібербезпеки еволюціонувати від виконання рутинних технічних операцій під контролем керівника до самостійного стратегічного управління безпекою організації.

Таблиця 1.1.

Рівні відповідальності відповідно до SFIA

Рівень	Керівна фраза	Короткий опис
1.	Виконання за вказівками Follow	Виконує рутинні, стандартні завдання під тісним наглядом і детальним керівництвом. Дотримується чітких інструкцій, потребує постійного контролю та перевірки виконаної роботи. Активно опановує базові знання та навички. Автономія мінімальна, оскільки робота відбувається за конкретними вказівками.
2.	Підтримка Assist	Надає допомогу колегам, працює під рутинним наглядом. Використовує власну розсудливість для вирішення типових, рутинних проблем. Активно навчається через тренінги і практичний досвід. Поступово бере на себе більшу відповідальність за окремі елементи завдань.
3.	Застосування Apply	Застосовує знання та навички для виконання різноманітних завдань, у тому числі складніших і нестандартних, у знайомих ситуаціях. Працює під загальним керівництвом, самостійно планує власну роботу в межах встановлених термінів, проявляє ініціативу та постійно підвищує свою кваліфікацію.

Продовження табл. 1.1.

Рівень	Керівна фраза	Короткий опис
6.	Ініціатива і вплив Initiate and influence	Ініціює зміни, впливає на прийняття рішень і визначення напрямків розвитку в межах організації або великих проєктів. Формує політику та підходи у своїй сфері, активно впливає на зацікавлені сторони.
7.	Розробка стратегії, мотивування, мобілізація Set strategy, inspire, mobilise	Визначає загальну стратегію та бачення на найвищому рівні (організаційному, галузевому чи навіть національному). Надихає людей, мобілізує ресурси, демонструє лідерство та несе повну відповідальність за стратегічні результати та трансформацію.

Сім рівнів відповідальності SFIA створюють чітку ієрархічну основу для визначення та оцінки кваліфікаційних вимог у сфері кібербезпеки. Рівні поступово підвищують вимоги до фахівця: від виконання простих завдань під суворим контролем (рівень 1) до розробки стратегії, лідерства та мобілізації ресурсів на рівні організації чи держави (рівень 7).

Кожен рівень характеризується зростанням автономії, впливу, складності завдань та відповідальності. Завдяки цьому SFIA дозволяє точно описувати, який саме рівень компетентності потрібен для виконання конкретних професійних завдань у кібербезпеці.

Рамка навичок майбутнього 2025 (Future Skills Framework, FSF) є галузево орієнтованою моделлю компетенцій, розробленою Комісією з навичок у галузі фінансових послуг - британською комісією, що об’єднує ключових гравців фінансового сектору Великої Британії. Фреймворк уперше представили у 2021 році з 8 навичками, розширили до 13 у 2022 році, а у 2025 році оновили з урахуванням актуальних викликів цифрової трансформації, зростанням кіберзагроз і регуляторних вимог.

Модель адресована фінансовому сектору, який налічує близько одного мільйона працівників у Великій Британії (72% ролей сьогодні вважаються

висококваліфікованими порівняно з 54% двадцять років тому) [8]. Фінансовий сектор потребує окремого фреймворку через свою високу регуляцію з боку органу із захисту даних DPA, наявність жорстких нормативних вимог відповідно до Загального регламенту про захист даних (GDPR), Директиви NIS2 тощо, критичну залежність від цифрових технологій і підвищену вразливість до кібератак, які можуть спричинити значні фінансові збитки і втрату довіри клієнтів.

Основною метою FSF 2025 є створити спільну мову компетенцій для роботодавців, освітніх установ і працівників, допомогти виявляти прогалини в навичках (skills gaps), формувати програми розвитку персоналу, рекрутингу та навчання, а також забезпечити адаптацію до швидких технологічних змін. Фреймворк підтримує перехід до моделі, заснованої на навичках (skill-based) організації, інтегруючись з інструментами аналізу прогалин і стратегічного планування розвитку кадрів. Він безпосередньо пов’язаний з глобальним дефіцитом кібернавичок, про який свідчать звіти провідних організацій [1-3], де брак підготовки персоналу визнається однією з головних причин успішних атак (людський фактор - 56 %, брак навичок в IT-безпеці - 54 %).

Ключовою особливістю Рамки є цілісний (holistic) підхід, який поєднує 7 технічних і 6 поведінкових компетенцій. Така структура дозволяє розвивати не лише «тверді» цифрові навички, але й м’які поведінкові якості, необхідні для ефективної роботи в умовах постійних змін.

Таблиця 1.2.

Ключові компетенції згідно з Рамкою навичок майбутнього 2025

Компетенція	Категорія	Короткий опис
Цифрова грамотність	технічні	Використання цифрових інструментів для пошуку, оцінки, створення та обмін інформацією
Аналіз даних і статистика	технічні	Етичний і ефективний аналіз даних для прийняття обґрунтованих рішень
Розробка ПЗ	технічні	Розробка, тестування та підтримка ПЗ

Продовження табл. 1.2.

Компетенція	Категорія	Короткий опис
Досвід користувача	технічні	Людино-центричний дизайн для підвищення зручності застосування
Застосування AI/ML	технічні	Розробка та впровадження моделей машинного навчання та штучного інтелекту
Управління змінами	технічні	Циклічне управління змінами з акцентом на швидке тестування та клієнтоорієнтованість
Кібербезпека	технічні	Оцінка, запобігання і захист інтернет-під'єднаних систем від несанкціонованого доступу та атак
Креативне мислення	поведінкові	Генерування нових ідей та перспектив у вирішенні завдань
Наставництво	поведінкові	Сприяння розкриттю потенціалу колег
Емпатія	поведінкові	Застосування емоційного інтелекту для ефективної взаємодії
Адаптивність	поведінкові	Швидка адаптація до змін зі збереженням стійкості
Управління відносинами	поведінкові	Побудова довірливих відносин на основі розуміння потреб
Командна робота	поведінкові	Колективна робота в інклюзивному середовищі

Такий інтегративний характер робить FSF 2025 особливо цінним для високо регульованих галузей з підвищеним рівнем кіберризиків. На відміну від універсального SFIA, який фокусується на рівнях відповідальності в IT загалом, цей фреймворк акцентує увагу на динамічному оновленні компетенцій відповідно до технологічних і регуляторних змін, що відповідає потребам фінансового сектору та може слугувати орієнтиром для адаптації в Україні, зокрема для захисту банківської сфери та критичної інфраструктури.

Модель компетенцій, запропонована австрійськими науковцями Д. Бендлером і М. Федерером [9], є відносно новою академічною розробкою, яка відзначається цілісним, адаптивним та прогресивним характером.

Автори провели якісний контент-аналіз понад 27 існуючих фреймворків і моделей компетенцій у сфері інформаційної безпеки та кібербезпеки. У результаті вони виявили ключові обмеження попередніх підходів, зокрема статичність структури, фрагментарність компонентів, недостатню увагу до нетехнічних аспектів, а також слабку адаптивність до швидкої еволюції ландшафту загроз.

Головною метою запропонованої моделі є створення цілісної та адаптивної рамки кваліфікаційних вимог, яка долає фрагментарність попередніх підходів і сприяє комплексному розвитку фахівця. На відміну від SFIA, орієнтованого переважно на рівні відповідальності, та FSF 2025, який має виражену галузеву (фінансову) специфіку, модель Бендлера-Федерера базується на чотирьох взаємопов’язаних класах компетенцій:

➢ професійні компетенції (Professional competencies) - технічні та предметно-специфічні знання й уміння;

➢ соціальні компетенції (Social competencies) - навички взаємодії з іншими людьми;

➢ особистісні компетенції (Personal competencies) - внутрішні якості та саморегуляція фахівця;

➢ методологічні компетенції (Methodological competencies) - здатність до системного мислення, вирішення проблем і навчання.

Таблиця 1.3.

Структура моделі компетенцій Бендлера-Федерера.

Блок компетенцій	Основні компоненти	Роль у професійній діяльності кіберфахівця
Професійні	Криптографія, хмарна безпека, аналіз загроз і вразливостей, безпека мереж і систем, захист ПЗ, цифрова криміналістика, безпека OT/ICS	Формують технічну основу для виявлення, запобігання і реагування на кіберзагрози. Забезпечують здатність працювати з конкретними технологіями й інструментами
Соціальні	Ефективна комунікація, командна робота, управління ризиками з урахуванням людського фактора, пояснення технічних ризиків керівництву, міждисциплінарна взаємодія	Дозволяють застосовувати технічні знання в реальних організаційних і соціальних контекстах, ефективно взаємодіяти з іншими підрозділами та зацікавленими сторонами
Особистісні	Етичне прийняття рішень, стійкість до стресу та невизначеності, самоконтроль, мотивація до професійного розвитку	Підтримують особисту ефективність фахівця в умовах високого тиску, етичних дилем і постійних змін
Методологічні	Критичне мислення, системний аналіз проблем, швидке навчання, адаптація до змін, рефлексія власної діяльності, технологічне прогнозування (technology watching)	Забезпечують здатність до постійного оновлення компетентнісного профілю, вирішення нестандартних завдань і адаптації до нових загроз (AI-атаки, квантові загрози, хмарні технології)

Модель Бендлера-Федерера не пропонує фіксованої кількості рівнів володіння, а передбачає динамічну структуру, яка дозволяє постійно коригувати набір компетенцій залежно від актуального ландшафту загроз. Це робить її прогресивним доповненням до більш усталених міжнародних фреймворків і відкриває перспективи для адаптації в національних системах кваліфікаційних вимог, зокрема в Україні, де гостро стоїть проблема поєднання глибокої технічної підготовки з розвитком адаптивності, комунікаційних та особистісних якостей фахівців в умовах воєнних загроз і швидкої цифрової трансформації.

Для порівняльного аналізу ключових підходів до формування компетенцій у сфері кібербезпеки розглянуто три фреймворки:

➢ Рамка навичок для інформаційної епохи є найбільш зрілим і універсальним глобальним фреймворком, який відрізняється чіткою ієрархічною структурою з семи рівнів відповідальності. Це забезпечує об’єктивну оцінку компетентності фахівців від виконавчого до стратегічного рівня та дозволяє ефективно використовувати його для кар’єрного планування й атестації в державних структурах та великих організаціях. Водночас SFIA недостатньо акцентує увагу на швидкій адаптації до нових технологічних загроз, таких як AI-безпека чи квантові обчислення.

➢ Рамка навичок майбутнього 2025, розроблений Комісією з навичок в галузі фінансових послуг, є яскравим прикладом галузево орієнтованої моделі. Він поєднує технічні навички (зокрема пріоритетну кібербезпеку) з поведінковими компетенціями та орієнтований на динамічне оновлення навичок у контексті цифрової трансформації та регуляторних вимог. Фреймворк особливо ефективний для високо регульованих секторів, таких як фінансовий, проте його вузька галузева спеціалізація ускладнює перенесення за межі цієї сфери.

➢ На відміну від них, модель Бендлера-Федерера має академічний, цілісний і адаптивний характер. Вона базується на чотирьох класах компетенцій (професійні, соціальні, особистісні й методологічні) і не фіксує жорстку кількість рівнів володіння. Ключовою інновацією моделі є сильний акцент на метакомпетенціях (швидке навчання, адаптація, самоорганізація та рефлексія),

що забезпечує постійну готовність фахівця до еволюції ландшафту загроз, зокрема викликів, пов’язаних зі штучним інтелектом, хмарними технологіями та квантовими обчисленнями. Завдяки цьому модель найкраще підходить для освітнього середовища та розробки сучасних навчальних програм. Крім цього, слід зазначити, що модель враховує положення Зводу знань з кібербезпеки (Cyber Security Body of Knowledge, CyBOK) [10], розробленого для підтримки освіти та професійної підготовки з кібербезпеки.

Таблиця 1.4.

Порівняльний аналіз основних фреймворків компетенцій у галузі кібербезпеки

Характеристика	SFIA	FSF 2025	Модель Бендлера-Федерера
Тип фреймворку	Глобальний, універсальний (IT і кібербезпека)	Галузевий (фінансовий сектор)	Академічний, цілісний і адаптивний
Кількість рівнів	7 рівнів відповідальності	5 рівнів фаховості	Нефіксована, динамічна структура
Основні компоненти	Професійні навички, поведінкові індикатори і загальні атрибути	13 технічних навичок, поведінкові компетенції	Чотири класи компетенцій: професійні, соціальні, особистісні й методологічні
Інтеграція кібербезпеки	Глибока інтеграція з іншими IT-доменами	Інтеграція з AI/ML, управління змінами і цифровою етикою	Повне охоплення CyBOK, синтез технічних і нетехнічних компетенцій
Фокус	Рівні відповідальності, автономія, вплив, складність задач	Швидке оновлення навичок в умовах цифрової трансформації	Адаптивність до нових загроз (AI, хмарні обчислення) і метакомпетенції

Продовження табл. 1.4.

Характеристика	SFIA	FSF 2025	Модель Бендлера-Федерера
Переваги	Висока структурованість, об’єктивна оцінка, широке застосування	Галузева спрямованість, фокус на регуляторних вимогах і прогалинах у навичках	Прогресивність, цілісний підхід, сильний акцент на адаптивності
Обмеження	Менш орієнтований на швидкі технологічні зміни	Обмежений фінансовим сектором	Менш поширений на практиці, потребує подальшої апробації
Найкраще застосування	Великі організації, державні структури, кар’єрне планування	Фінансовий сектор, високо регульовані галузі	Освіта, розробка навчальних програм, наукові дослідження

Стратегічне значення кваліфікаційних вимог у сфері кібербезпеки полягає в їхній здатності слугувати «містком» між системою освіти, ринком праці та державним регулюванням. Вони сприяють подоланню як кількісного, так і якісного дефіциту кадрів, підвищують загальну кіберстійкість організацій і держави, дозволяють оптимізувати витрати на підготовку фахівців та суттєво знижують ризики успішних кібератак, зумовлених людським фактором.

Проведений порівняльний аналіз ключових міжнародних фреймворків (SFIA, FSF 2025 і моделі Бендлера-Федерера) показує, що кожен із них має власні сильні сторони. SFIA забезпечує універсальну ієрархічну структуру рівнів відповідальності, FSF 2025 акцентує на галузевій адаптивності й інтеграції технічних та поведінкових компетенцій, тоді як модель Бендлера-Федерера пропонує цілісний і динамічний підхід, заснований на чотирьох класах

компетенцій (професійні, соціальні, особистісні й методологічні) з особливим акцентом на метакомпетенціях (швидке навчання, адаптація та рефлексія).

Гармонізація таких моделей дає змогу сформувати єдину «міжнародну мову» компетенцій, яка водночас залишає достатній простір для врахування національних особливостей, воєнних загроз і специфіки захисту критичної інфраструктури.

1.3 Основні компоненти кваліфікаційних вимог: компетентності, знання, уміння та навички

У сучасній теорії і практиці кібербезпеки поняття «компетентність» розглядається як інтегральна характеристика фахівця, що відображає його здатність ефективно виконувати професійні завдання в умовах невизначеності, динамічних загроз і швидких технологічних змін. Компетентність не зводиться лише до суми знань чи окремих навичок, а являє собою цілісну якість особистості, яка забезпечує успішне застосування знань, умінь і навичок у реальних професійних ситуаціях.

Згідно з сучасним компетентнісним підходом, компетентність є вищим рівнем у ієрархії компонентів кваліфікаційних вимог. Вона виступає синтезом трьох основних елементів:

- знань (когнітивний компонент),
- умінь (операційно-діяльнісний компонент),
- навичок (практично-автоматизований компонент).

При цьому компетентність завжди має контекстуальний характер — вона проявляється лише в процесі вирішення конкретних професійних завдань і залежить від рівня мотивації, етичних принципів та здатності до самоорганізації фахівця.

Особливе значення компетентності полягає в її ролі ключового критерію оцінки реальної готовності фахівця до професійної діяльності (job-readiness). Якщо традиційний підхід обмежується формальними ознаками (наявність

диплома чи сертифіката), то компетентнісний підхід дозволяє об’єктивно визначити, чи здатен спеціаліст ефективно застосовувати отримані знання в умовах реальних кіберінцидентів, критичних ситуацій та міждисциплінарної взаємодії. Зважаючи на це, компетентність сьогодні розглядається як центральний елемент сучасних кваліфікаційних вимог і слугує концептуальною основою для розробки профілів посад, програм підвищення кваліфікації, систем атестації та сертифікації фахівців з кібербезпеки.

Яскравим прикладом практичної реалізації компетентнісного підходу є зони компетенцій (Competency Areas) у межах NICE Workforce Framework for Cybersecurity від Національного інституту стандартів і технологій (National Institute of Standards and Technology, NIST) [11].

На відміну від традиційного розподілу за робочими ролями, який фокусується на конкретних посадах і професійних завданнях, NISTIR 8355 націлений на реалізацію студенто-центрованого підходу (learner-centric approach) [12], орієнтованого насамперед на потреби, досвід і активну участь фахівця, який навчається або підвищує кваліфікацію, а не просто отримання ним матеріалів від учителя, наставника тощо.

Документ спрямований на розвиток і оцінку конкретних компетентностей у процесі навчання та професійного зростання, незалежно від формальної освіти чи наявного стажу роботи. Кожна компетентнісна область об’єднує пов’язані елементи завдання, знання, навички (Tasks, Knowledge, Skills, TKS) та включає рівні кваліфікації. Такий підхід дозволяє об’єктивно оцінювати рівень підготовки фахівця та формувати індивідуальні освітні траєкторії.

Знання є фундаментальним компонентом кваліфікаційних вимог у сфері кібербезпеки, оскільки становлять теоретичну основу, на якій формуються уміння, навички та професійна компетентність фахівця. У контексті кібербезпеки вони мають яскраво виражений міждисциплінарний характер і забезпечують розуміння причинно-наслідкових зв’язків між загрозами, вразливостями та ефективними контрзаходами.

Водночас, найбільш авторитетним і детально розробленим міжнародним

корпусом знань залишається Звід знань з кібербезпеки CyBOK, представленого у 2021 році. Звід структуровано у 21 зони знань (Knowledge Areas), об'єднані в шість широких категорій [10]. Українські професійні стандарти значною мірою базуються на структурі CyBOK, адаптуючи її до національного законодавства та специфіки актуальних загроз.

Уміння та навички становлять практичну складову кваліфікаційних вимог і відіграють ключову роль у переході від теоретичних знань до реальної професійної діяльності. Хоча ці поняття часто використовуються як синоніми, між ними існує важлива концептуальна відмінність.

➢ Уміння - це свідома здатність виконувати певну дію або операцію на основі отриманих знань, яка передбачає розуміння алгоритму дій (наприклад, проведення аналізу вразливостей за допомогою спеціалізованого сканера).

➢ Навичка - це автоматизована, доведена до високого рівня досконалості дія, яка виконується швидко, точно і з мінімальними витратами уваги (наприклад, оперативне виявлення ознак компрометації в логах SIEM-системи).

Уміння виступає перехідною ланкою між знаннями та навичками, тоді як навички формуються через тривале практичне тренування та досвід. У системі кваліфікаційних вимог вони розглядаються у тісному взаємозв'язку: уміння забезпечують осмислене застосування знань, а навички гарантують оперативність і ефективність дій у критичних ситуаціях.

Яскравим прикладом ефективного формування практичних навичок у вітчизняній практиці є ініціатива «Студентські кібербригади». Як зазначає вітчизняний науковець В. Кальченко [13], участь студентів у таких бригадах дає можливість перейти від теоретичного вивчення кібербезпеки до реального практичного досвіду. Студенти працюють з актуальними інструментами (Wireshark, Splunk, Metasploit, Burp Suite тощо), аналізують реальні або максимально наближені до реальних кіберінциденти, проводять їх розслідування та розробляють заходи захисту.

Такий практико-орієнтований підхід суттєво підвищує рівень практичних навичок, розвиває командну взаємодію та формує здатність швидко приймати

рішення в умовах обмеженого часу. Дослідження свідчать, що студенти, які пройшли практику в кібербригадах, демонструють значно вищий рівень професійної готовності порівняно з тими, хто обмежився лише аудиторними заняттями.

Важливий внесок у розуміння системи формування компетентностей зробили українські дослідники В. Горлинський та Б. Горлинський [14], які виділяють ключові чинники розвитку системи компетентностей фахівців у галузі кібербезпеки, зокрема глобалізацію та євроінтеграційні процеси, стрімкий технологічний прогрес, гібридний характер сучасних війн, необхідність відповідності міжнародним стандартам (НАТО, ЄС).

Автори підкреслюють, що ефективна система кваліфікаційних вимог повинна забезпечувати баланс між технічними навичками (hard skills) та м'якими навичками (soft skills), такими як критичне мислення, комунікація, командна робота та стресостійкість. Особливої актуальності набуває постійне оновлення компетентностей, оскільки термін актуальності технічних знань у сфері кібербезпеки становить у середньому 12-18 місяців.

Таким чином, основними компонентами кваліфікаційних вимог у сфері кібербезпеки є професійна компетентність як інтегральне ядро, а також її складові: знання (когнітивна основа), уміння (свідома дія) та навички (автоматизована дія). Міжнародні підходи, представлені в NIST NICE Framework та CyBOK, у поєднанні з вітчизняними практиками (зокрема, студентськими кібербригадами) свідчать про необхідність комплексного розвитку як технічних, так і нетехнічних компетентностей. Нормативне закріплення цих компонентів у стандартах серії ISO/IEC 27000 робить їх обов'язковими та вимірюваними елементами системи управління інформаційною безпекою.

Висновки до розділу 1

Встановлено, що сучасна підготовка та підвищення кваліфікації фахівців з кібербезпеки стикається з системними проблемами: значним кадровим

дефіцитом, переважанням теоретичної підготовки над практичною, швидким застаріванням компетентностей та недостатньою відповідністю освітніх програм реальним потребам ринку праці й національної безпеки. Аналіз міжнародних і національних підходів показав, що кваліфікаційні вимоги є ключовим системоутворюючим елементом, який забезпечує узгодження інтересів держави, роботодавців, закладів освіти та самих фахівців.

За підсумками дослідження зроблено висновки, що ефективна система кваліфікаційних вимог повинна ґрунтуватися на компетентнісному підході та включати чітку структуру компонентів (завдання, знання, уміння, навички, компетентності та рівні володіння ними). Міжнародні фреймворки (SFIA, FSF 2025, модель Бендлера-Федерера) підтверджують необхідність балансу технічних, соціальних, особистісних і методологічних компетенцій, а також динамічної адаптації до нових загроз (AI, OT/ICS, квантові технології). Саме така структура стає основою для переходу від фрагментарної підготовки до цілісної, практико-орієнтованої моделі розвитку кадрового потенціалу в сфері кібербезпеки.

РОЗДІЛ 2. МІЖНАРОДНІ Й НАЦІОНАЛЬНІ ПІДХОДИ ДО ФОРМУВАННЯ КВАЛІФІКАЦІЙНИХ ВИМОГ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

2.1 Американський підхід до формування кваліфікаційних вимог у сфері кібербезпеки (NICE Framework)

Американський підхід до формування кваліфікаційних вимог у сфері кібербезпеки найповніше представлений Рамкою NICE щодо робочої сили з кібербезпеки, офіційна версія якої представлена у спеціальній публікації NIST SP 800-181 Revision 1 [15], розробленій у співпраці з Агентством кібербезпеки та інфраструктурної безпеки США (Cybersecurity and Infrastructure Security Agency, CISA) та іншими державними й приватними стейкхолдерами.

Виникнення NICE Рамки стало реакцією на стрімке зростання кіберзагроз на початку 2000-х років, коли традиційні моделі підготовки кадрів виявилися недостатньо ефективними для протидії державним і транснаціональним кібератакам. Ключовою передумовою створення фреймворку стало визнання на державному рівні критичної нестачі кваліфікованих фахівців. Так, у 2009 році Президент США Барак Обама ініціював Національну стратегію кібербезпеки, яка згодом трансформувалася в Національну ініціативу з освіти кібербезпеки NICE). Метою ініціативи було формування єдиної національної стратегії розвитку кіберробочої сили шляхом об’єднання зусиль уряду, приватного сектору, академічних установ і громадських організацій. Головним завданням стало подолання розриву між попитом і пропозицією компетентних фахівців у сфері кібербезпеки.

Офіційна версія Рамки NICE вперше з’явилася у 2013 році як Рамка NICE щодо робочої сили з кібербезпеки версія 1.0. Вона започаткувала систематизацію ролей, завдань, знань і навичок у сфері кібербезпеки. У 2017 році NIST опублікував її як NIST SP 800-181. Це була перша офіційна версія від NIST, яка суттєво розширила кількість робочих ролей та запровадила чітку структуру на

основі завдань, знань і навичок (TKS).

Значне оновлення відбулося у листопаді 2020 року з виходом NIST SP 800-181 Revision 1, яка стала основною структурною основою фреймворку. Надалі компоненти Рамки NICE почали підтримувати й оновлювати окремо від основного документа.

Останньою діючою версією є Компоненти Рамки NICE (Framework Components) 2.1.0 від 03 грудня 2025 року [16], які охоплюють 7 категорій робочих ролей, значну кількість робочих ролей, а також 11 зон компетенцій.

NIST виконує роль головного науково-методичного центру, забезпечуючи наукову обґрунтованість фреймворку, його регулярне оновлення та сумісність з іншими національними стандартами. CISA, як операційний орган, відповідає за практичне впровадження Рамки NICE у державних структурах, координацію національних програм підготовки кадрів та моніторинг ефективності його застосування.

Структура Рамки NICE побудована на чіткій ієрархічній моделі, яка дозволяє системно описувати вимоги до фахівців у сфері кібербезпеки. Документ забезпечує єдину мову для роботодавців, освітніх закладів і фахівців, допомагаючи узгоджувати потреби ринку праці з програмами навчання та розвитку кадрів.

Основу Рамки NICE становить чітка ієрархічна модель, побудована за принципом «зверху вниз»: від високого рівня узагальнення до конкретних елементів (Таблиця 2.1).

Слід відзначити, що актуальна версія фреймворку використовує термінологію TKS замість застарілого KSA (Knowledge, Skills, Abilities), оскільки основний акцент зроблено на практичних завданнях, теоретичних знаннях і прикладних навичках.

Таблиця 2.1.

Ієрархічна структура Рамки NICE (2025-2026)

Рівень ієрархії	Назва елемента	Опис	Кількість
Найвищий рівень	Категорії робочих ролей	Високорівневі групи споріднених функцій кібербезпеки	5 категорій
Основний рівень	Робочі ролі	Узагальнені професійні ролі, що описують реальні функції фахівця	понад 40 робочих ролей
Операційний рівень	Завдання	Конкретні професійні дії або завдання	940
Базовий рівень (TKS)	Знання	Теоретична інформація, необхідна для виконання завдань	630
Базовий рівень (TKS)	Навички	Практичні вміння та здатності, набуті через досвід і тренування	530
Додатковий елемент	Зони компетенцій	Групи пов’язаних особистісно-орієнтованих TKS	11 зон компетенцій (NISTIR 8355)

Центральним елементом фреймворку є робочі ролі (Work Roles) - узагальнені професійні ролі, які відображають реальні функції в сфері кібербезпеки. Кожна роль являє собою унікальне поєднання завдань, знань і навичок, необхідних для ефективного виконання професійних обов’язків.

Важливою перевагою Рамки NICE є те, що робочі ролі не прив’язані жорстко до посадових назв. Це забезпечує високу гнучкість: одна й та сама роль може мати різні назви посад у різних організаціях: від державних установ і великих корпорацій до невеликих компаній. Такий підхід дозволяє ефективно

використовувати фреймворк для:

- ➢ розробки посадових інструкцій і профілів компетенцій;
- ➢ створення освітніх програм і курсів;
- ➢ планування кар'єрного зростання фахівців;
- ➢ оцінки та найму персоналу.

Таким чином, американський підхід, втілений у Рамці NICE від NIST, вирізняється високим рівнем деталізації, практичною орієнтацією та гнучкістю, що робить його одним із найвпливовіших інструментів формування кваліфікаційних вимог у сфері кібербезпеки.

2.2 Основні положення Європейської рамки навичок з кібербезпеки (ECSF)

Стрімке зростання кіберзагроз у Європейському Союзі, а також суттєвий дефіцит кваліфікованих фахівців з кібербезпеки зумовили необхідність розробки єдиного європейського підходу до розвитку кібернавичок. Це відповідає стратегічним пріоритетам ENISA [17].

За оцінками Європейського агентства з кібербезпеки ENISA, у 2024–2025 роках дефіцит фахівців у сфері кібербезпеки в ЄС сягав понад 300 тис. осіб [18], а більшість держав-членів стикалися з серйозними труднощами у заповненні вакансій, особливо в секторах критичної інфраструктури. Відсутність спільної рамки кваліфікаційних вимог призводила до фрагментації ринку праці, різного рівня підготовки фахівців у різних країнах та ускладнювала їхню мобільність у межах ЄС. Саме тому ENISA отримало ключову роль у формуванні єдиної політики розвитку кібернавичок.

ENISA відповідає за підвищення рівня кіберстійкості держав-членів, імплементації європейського законодавства у сфері кібербезпеки та координацію зусиль у сфері кібербезпеки. Одним із пріоритетних напрямів діяльності агентства стало створення єдиного інструменту для опису та розвитку компетенцій – Європейської рамки навичок з кібербезпеки (European

Cybersecurity Skills Framework, ECSF) [19].

Розробка ECSF розпочалася у 2019-2020 роках у межах реалізації Європейської стратегії кібербезпеки. Перша концептуальна версія документу була представлена у 2022 році. У 2023-2024 роках ENISA провела широкі консультації з представниками держав-членів, бізнесу, академічних кіл і професійних асоціацій. Актуальна версія ECSF (2025–2026) є результатом цих багатосторонніх зусиль і відображає поточні потреби європейського цифрового ринку.

ECSF тісно пов’язаний з ключовими нормативними документами ЄС. Насамперед це Директива NIS2) [20], яка встановлює жорсткі вимоги до управління ризиками кібербезпеки для життєво важливих (essential) та важливих (important) суб’єктів і прямо вимагає наявності достатньої кількості кваліфікованого персоналу. Крім того, фреймворк інтегровано в Стратегію кібербезпеки ЄС на період 2020-2025 років [21] та Європейську програму розвитку навичок (EU Skills Agenda) [22]. ECSF став практичним інструментом реалізації цих стратегічних документів, забезпечуючи єдину мову опису компетенцій у всіх країнах-членах.

Створення ECSF було обумовлено об’єктивною необхідністю подолання кадрового дефіциту та гармонізації підходів до підготовки фахівців у масштабах усього Європейського Союзу. ENISA як головний розробник забезпечила європейську специфіку фреймворку, орієнтованого на рольові профілі, мобільність кадрів і відповідність вимогам сучасного європейського законодавства у сфері кібербезпеки.

ECSF має чітку, логічну та порівняно компактну архітектуру, яка відрізняється від американського Рамки NICE акцентом на рольовому підході. Загальна архітектура ECSF побудована навколо 12 рольових профілів (role profiles), які є центральним і найважливішим елементом фреймворку. Кожен рольовий профіль представляє собою узагальнений опис типової ролі фахівця з кібербезпеки, що реально існує на європейському ринку праці. На відміну від Рамки NICE, де основою є 41 деталізована робоча роль, ECSF пропонує більш

узагальнений і гнучкий підхід із 12 ключових ролей, які охоплюють більшість практичних потреб організацій (рис. 2.1).

Рис. 2.1. Рольові профілі фахівців з кібербезпеки відповідно до ECSF

Детальна інформація з описом зазначених ролей показана в таблиці 2.2.

Таблиця 2.2.

12 ключових рольових профілів фахівців з кібербезпеки згідно з ECSF

Рольовий профіль	Короткий опис ролі
Директор з інформаційної безпеки (CISO)	Стратегічне керівництво програмою кібербезпеки організації, звітність перед керівництвом
Фахівець з реагування на кіберінциденти	Виявлення, аналіз та реагування на кіберінциденти, управління інцидентами
Фахівець з кіберправа, політики та відповідності	Розробка політики, забезпечення відповідності законодавству та регуляціям у сфері кібербезпеки
Менеджер з управління кіберризиками	Ідентифікація, оцінка та управління кіберризиками організації

Продовження табл.2.2.

Рольовий профіль	Короткий опис ролі
Аудитор кібербезпеки	Проведення аудитів і перевірок систем кібербезпеки
Інструктор з кібербезпеки	Навчання й підвищення кваліфікації фахівців з кібербезпеки
Дослідник кібербезпеки	Проведення наукових досліджень і розробка нових технологій захисту
Експерт з цифрової криміналістики	Збір, аналіз та відновлення цифрових доказів після інцидентів
Тестувальник на проникнення	Симуляція атак для виявлення вразливостей у системах
Інженер-імплементатор кібербезпеки	Розробка, впровадження, інтеграція та підтримка кібербезпекових рішень (систем, ПЗ, заходів) в інфраструктурі організації, включаючи DevSecOps
Спеціаліст з кіберрозвідки	Збір, аналіз та поширення інформації про актуальні кіберзагрози

Кожен рольовий профіль складається з чотирьох основних компонентів:

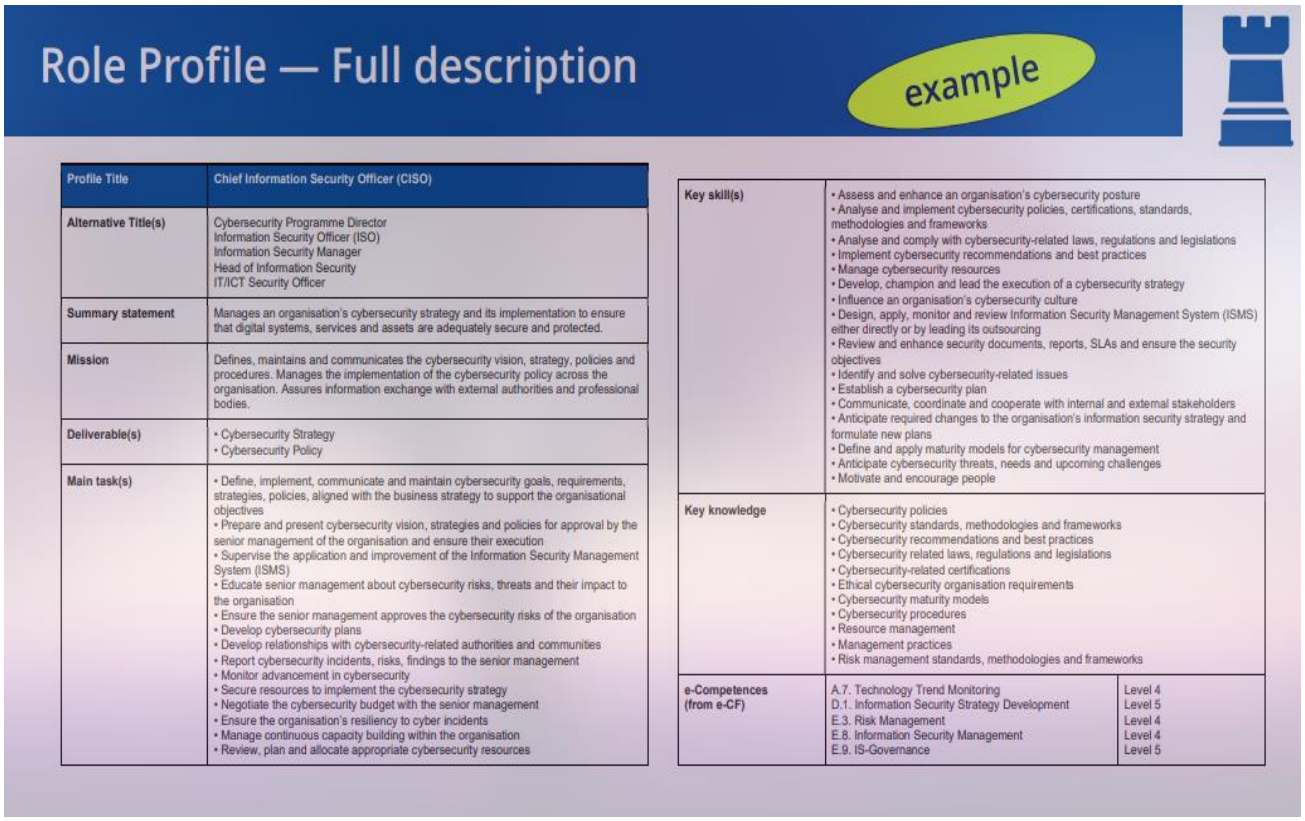
➢ Основні завдання (Main Tasks) - загальні компетенції, які свідчать про здатність виконувати певні функції на високому рівні.

➢ Ключові знання (Key Knowledge) - необхідні для виконання певних функцій теоретичні знання.

➢ Ключові навички (Key Skills) - необхідні для виконання певних функцій практичні уміння.

Для кожної ролі ENISA чітко визначає перелік компетенцій (зазвичай 8–15), а також детально описує, які знання, навички та здібності потрібні для їх реалізації. Це дозволяє створювати профілі посад, які є зрозумілими як для роботодавців, так і для закладів освіти. На рис. 2.3 наведено повний опис

рольового профілю директора з кібербезпеки.



Role Profile — Full description

example

Profile Title	Chief Information Security Officer (CISO)
Alternative Title(s)	Cybersecurity Programme Director Information Security Officer (ISO) Information Security Manager Head of Information Security IT/ICT Security Officer
Summary statement	Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.
Mission	Defines, maintains and communicates the cybersecurity vision, strategy, policies and procedures. Manages the implementation of the cybersecurity policy across the organisation. Assures information exchange with external authorities and professional bodies.
Deliverable(s)	• Cybersecurity Strategy • Cybersecurity Policy
Main task(s)	• Define, implement, communicate and maintain cybersecurity goals, requirements, strategies, policies, aligned with the business strategy to support the organisational objectives • Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organisation and ensure their execution • Supervise the application and improvement of the Information Security Management System (ISMS) • Educate senior management about cybersecurity risks, threats and their impact to the organisation • Ensure the senior management approves the cybersecurity risks of the organisation • Develop cybersecurity plans • Develop relationships with cybersecurity-related authorities and communities • Report cybersecurity incidents, risks, findings to the senior management • Monitor advancement in cybersecurity • Secure resources to implement the cybersecurity strategy • Negotiate the cybersecurity budget with the senior management • Ensure the organisation's resiliency to cyber incidents • Manage continuous capacity building within the organisation • Review, plan and allocate appropriate cybersecurity resources

Key skill(s)	• Assess and enhance an organisation's cybersecurity posture • Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks • Analyse and comply with cybersecurity-related laws, regulations and legislations • Implement cybersecurity recommendations and best practices • Manage cybersecurity resources • Develop, champion and lead the execution of a cybersecurity strategy • Influence an organisation's cybersecurity culture • Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing • Review and enhance security documents, reports, SLAs and ensure the security objectives • Identify and solve cybersecurity-related issues • Establish a cybersecurity plan • Communicate, coordinate and cooperate with internal and external stakeholders • Anticipate required changes to the organisation's information security strategy and formulate new plans • Define and apply maturity models for cybersecurity management • Anticipate cybersecurity threats, needs and upcoming challenges • Motivate and encourage people	
Key knowledge	• Cybersecurity policies • Cybersecurity standards, methodologies and frameworks • Cybersecurity recommendations and best practices • Cybersecurity related laws, regulations and legislations • Cybersecurity-related certifications • Ethical cybersecurity organisation requirements • Cybersecurity maturity models • Cybersecurity procedures • Resource management • Management practices • Risk management standards, methodologies and frameworks	
e-Competences (from e-CF)	A.7. Technology Trend Monitoring D.1. Information Security Strategy Development E.3. Risk Management E.8. Information Security Management E.9. IS-Governance	Level 4 Level 5 Level 4 Level 4 Level 5

Рис. 2.2. Структура рольового профілю CISO згідно з ECSF

На відміну від американської Рамки NICE, яка характеризується високою деталізацією та великою кількістю робочих ролей, ECSF пропонує більш компактну та гнучку архітектуру. Фреймворк акцентує увагу не на максимальній деталізації окремих посад, а на створенні універсальних рольових профілів, які легко адаптувати до національних особливостей держав-членів ЄС. Такий підхід сприяє мобільності фахівців у межах єдиного європейського ринку праці та полегшує гармонізацію систем підготовки кадрів.

Головними перевагами ECSF є:

➢ гармонізація, тобто створення єдиної мови опису кіберкомпетенцій для всіх 27 країн-членів ЄС, що зменшує фрагментацію ринку праці та забезпечує порівнянність кваліфікацій;

➢ мобільність кадрів: фахівці, компетенції яких описані за допомогою ECSF, можуть легше переміщуватися між країнами, оскільки роботодавці та освітні установи користуються спільною системою координат;

➢ формування спільного ринку кібернавичок, оскільки фреймворк сприяє

ефективній взаємодії між попитом і пропозицією на європейському рівні незалежно від національних кордонів.

ECSF тісно інтегрований з ключовими європейськими стратегічними документами, зокрема з Директивою NIS2, Європейською стратегією кібербезпеки, Європейською програмою розвитку навичок (EU Skills Agenda) та Стратегічним планом розвитку кібернавичок (Cybersecurity Blueprint for Skills Development). Рамка ECSF також активно використовується в європейській мережі кіберполігонів (Cyber Ranges) для розробки практичних навчальних програм і сценаріїв тренувань [23].

Методологія ECSF передбачає динамічний характер компетенцій: фреймворк не фіксує раз і назавжди набір знань і навичок, а передбачає їх регулярне оновлення відповідно до еволюції ландшафту загроз і технологічного розвитку. Важливою особливістю є збалансоване поєднання технічних компетенцій з нетехнічними, такими як критичне мислення, комунікація, лідерство та етичне прийняття рішень.

Рамка відображає європейські цінності єдності, гармонізації та орієнтації на людину. Рольовий підхід у поєднанні з інтеграцією в ширші європейські ініціативи робить документ гнучким і перспективним інструментом розвитку кібернавичок на континентальному рівні.

ECSF швидко вийшов за межі теоретичного документа і став практичним інструментом у багатьох державах-членах. Його застосовують для виконання вимог Директиви NIS2, проведення аналізу прогалин у підготовці кіберфахівців, планування програм підвищення кваліфікації та адаптації освітніх програм.

ENISA у 2025 році опублікувала спеціальні настанови щодо зіставлення зобов'язань NIS2 з профілями ролей ECSF (Mapping NIS2 Obligations with ECSF Role Profiles) [24], яке зіставляє кожну ключову вимогу Директиви NIS2 (управління ризиками, реагування на інциденти, аудит тощо) з конкретними рольовими профілями ECSF. Це дозволяє організаціям чітко визначати необхідні компетенції, проводити оцінку наявних кадрів і планувати навчання.

Національні адаптації демонструють високу гнучкість фреймворку. У

Німеччині Федеральне відомство з інформаційної безпеки (BSI) інтегрувало ECSF у національну стратегію «Cybersecurity Made in Germany». У Франції ANSSI активно використовує рольові профілі для акредитації освітніх програм і сертифікації фахівців. Нідерланди та Польща застосовують ECSF для створення національних каталогів компетенцій і програм перепідготовки кадрів.

ECSF є важливою європейською альтернативою американському NIST Рамкою NICE. Порівняльний аналіз, представлений у таблиці 2.3, підтверджує цю тезу [25] Якщо Рамка NICE орієнтована на максимальну деталізацію, операційну точність, то ECSF пропонує більш стратегічну, рольову і гармонізаційну концепцію. Його ключова цінність полягає у створенні єдиної європейської мови опису кіберкомпетенцій на основі 12 рольових профілів, що забезпечує порівнянність кваліфікацій, сприяє професійній мобільності фахівців у межах ЄС і полегшує виконання вимог Директиви NIS2.

Таблиця 2.3.

Порівняльний аналіз ECSF та Рамки NICE

Характеристика	Рамка NICE від NIST	ECSF від ENISA
Кількість основних елементів	41 робоча роль 5 категорій робочих ролей 11 зон компетенцій	12 рольових профілів
Основний підхід	Деталізований, заснований на моделі, що базується на навичках (skills-based)	Орієнтований на ролі (role-based), гармонізаційний, стратегічний
Рівень деталізації	Високий (близько 900–1100 завдань, сотні описів знань і навичок; загалом понад 2100 TKS твердження)	Середній (8–15 компетенцій / ключових елементів на один рольовий профіль)
Основна мета	Операційна точність, вимірюваність компетенцій, практичне застосування в організаціях	Гармонізація компетенцій, мобільність кадрів, відповідність законодавству ЄС

Продовження табл.2.3.

Характеристика	NIST NICE Framework	ECSF від ENISA
Орієнтація	Операційна та організаційна (практичне застосування в компаніях і державних установах)	Стратегічна та європейська (єдиний ринок, гармонізація в межах ЄС)
Гнучкість для інших країн	Середня (орієнтований на американську специфіку, але широко використовується і за межами США)	Висока (легко адаптується до національних контекстів)
Інтеграція з нормативною базою	Національні стратегії та стандарти США (NIST, CISA)	Директива NIS2, Європейська програма розвитку навичок, Стратегічний план розвитку кібернавичок
Система оцінки компетенцій	Детальна, багаторівнева (рівні фаховості, відповідність рівням відповідальності)	Чотирирівнева шкала фаховості, менш деталізована
Актуальність і частота оновлення	Регулярне оновлення (остання версія - v2.1.0, грудень 2025)	Динамічна структура, регулярні консультації та оновлення (2022–2025)
Сильні сторони	Висока деталізація, вимірюваність, операційна ефективність, чіткі TKS твердження	Компактність, гнучкість, сприяння мобільності кадрів та гармонізації
Слабкі сторони	Складність для малих організацій, американська специфіка, більший обсяг даних	Менша деталізація, менш розвинена система оцінки компетенцій

Загальна архітектура ECSF є більш компактною та орієнтованою на

європейські реалії порівняно з американською Рамкою NICE. Вона акцентує увагу не на максимальній деталізації посад, а на створенні універсальних рольових профілів, які легко адаптувати до національних особливостей і які сприяють мобільності фахівців у межах ЄС. В результаті це робить його ефективним інструментом гармонізації кібернавичок на європейському рівні та важливим орієнтиром для країн, які прагнуть наблизити свої системи підготовки кадрів до європейських стандартів.

ECSF не ставить за мету замінити національні системи кваліфікаційних вимог, а пропонує гнучку рамкову структуру, яку кожна держава-член ЄС може адаптувати відповідно до своїх особливостей. Такий підхід робить фреймворк потужним інструментом не лише внутрішньої гармонізації, але й формування єдиного європейського ринку кібернавичок. ECSF успішно інтегрується з ключовими європейськими ініціативами, зокрема з Європейською програмою розвитку навичок, мережею кіберполігонів і настановами щодо зіставлення зобов'язань NIS2 з профілями ролей ECSF, що підтверджує його високу практичну та стратегічну цінність.

Для України ECSF має особливе значення в контексті євроінтеграційного курсу. Національна система підготовки фахівців з кібербезпеки потребує системного наближення до європейських стандартів, особливо з огляду на необхідність імплементації вимог Директиви NIS2, забезпечення захисту критичної інфраструктури та інтеграції у спільний цифровий ринок Європейського Союзу. Використання ECSF дозволить:

➢ гармонізувати українські професійні стандарти та освітні програми з європейськими рольовими профілями;

➢ підвищити міжнародну мобільність українських фахівців на європейському ринку праці;

➢ полегшити визнання українських кваліфікацій на рівні ЄС;

➢ створити основу для спільних освітніх і тренінгових програм з країнами Європейського Союзу.

Водночас пряме перенесення ECSF без відповідної адаптації є

неможливим. Україна має враховувати власні специфічні умови, зокрема воєнний стан, особливості захисту критичної інфраструктури в умовах гібридної війни, обмежені фінансові та кадрові ресурси, а також вже існуючі національні професійні стандарти. Найперспективнішим варіантом видається розробка національного гібридного фреймворку, який поєднає операційну деталізацію та вимірюваність американського Рамки NICE з рольовим і гармонізаційним підходом європейського ECSF.

Таким чином, ECSF від ENISA є важливою європейською альтернативою американському підходу. Орієнтований на єдність, мобільність і стратегічну гармонізацію кібернавичок, ECSF може стати одним із ключових орієнтирів для подальшого розвитку національної системи кваліфікаційних вимог в Україні та її прискореної інтеграції у європейський цифровий простір.

2.3 Національні професійні та освітні стандарти України з кібербезпеки 2024–2026 років

Нормативно-правова база регулювання кваліфікаційних вимог у сфері кібербезпеки України формується на перетині національного законодавства, стратегічних документів та зобов'язань щодо європейської інтеграції. Активний розвиток цієї бази у 2024–2026 роках зумовлений двома ключовими чинниками: інтенсифікацією кіберзагроз в умовах повномасштабної війни та необхідністю гармонізації українського законодавства з *acquis communautaire* ЄС.

Правову основу забезпечення кібербезпеки становить Закон України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року № 2163-VIII [26]. Важливим етапом його розвитку стали зміни, внесені Законом України № 4336-IX від 27 березня 2025 року [27] . Ці зміни суттєво посилили вимоги до кадрового забезпечення суб'єктів кібербезпеки, передбачили створення спеціалізованих підрозділів з кіберзахисту в державних органах, запровадили механізми сертифікації та атестації фахівців, а також сприяли поступовому переходу від традиційної моделі комплексних систем захисту

інформації (КСЗІ) до більш гнучкого підходу на основі профілів безпеки.

Стратегічним документом другого рівня є Стратегія кібербезпеки України, 2021 року [28]. У Стратегії чітко визначено один із ключових викликів — невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з кібербезпеки. Серед пріоритетних стратегічних цілей зазначено проведення докорінної реформи системи професійної освіти і безперервного навчання, а також розробку і впровадження національних професійних стандартів.

У 2024–2025 роках активне формування національної системи професійних стандартів здійснювала Адміністрація Державної служби спеціального зв'язку та захисту інформації України (Адміністрація Держспецзв'язку) - центральний орган, відповідальний за розроблення, затвердження та ведення реєстру професійних стандартів у сфері захисту інформації та кібербезпеки. За цей період було затверджено низку професійних стандартів, які стали першим системним кроком до уніфікації кваліфікаційних вимог до фахівців на національному рівні.

Система професійних стандартів, розроблена Адміністрацією Держспецзв'язку України, ґрунтується на компетентнісному підході та повністю відповідає вимогам Закону України «Про професійні стандарти» [29] та Національної рамки кваліфікацій [30]. Кожен стандарт має уніфіковану структуру, яка включає назву професії, рівень кваліфікації за Національною рамкою кваліфікацій, перелік загальних і професійних компетенцій, а також детальний опис необхідних знань, умінь і навичок (ЗУН) для виконання трудових функцій. Такі стандарти орієнтовані на практичне застосування і слугують основою для розроблення посадових інструкцій, освітніх програм, систем атестації та сертифікації фахівців.

Основні професійні стандарти в галузі кібербезпеки, затверджені Адміністрацією Держспецзв'язку України у 2024–2025 роках, представлені у таблиці 2.4.

Таблиця 2.4.

Основні професійні стандарти у сфері кібербезпеки

Назва професійного стандарту	Основний зміст і акцент компетенцій	Рівень кваліфікації (НРК)
Фахівець з реагування на інциденти кібербезпеки [31]	Виявлення, аналіз, реагування та ліквідація наслідків кіберінцидентів; робота з SIEM-системами, цифрова криміналістика, координація дій та звітність	6–7
Фахівець сфери захисту інформації [32]	Технічний та організаційний захист інформації; нормативно-правова база, оцінка ризиків, впровадження та контроль заходів захисту	6–7
Фахівець з підтримки інфраструктури кіберзахисту [33]	Забезпечення функціонування засобів захисту (фаєрволи, IDS/IPS, захист кінцевих точок тощо); моніторинг, налаштування й обслуговування систем	6
Аудитор інформаційних технологій (з кібербезпеки) [34]	Незалежний аудит систем захисту інформації; планування аудиту, оцінка відповідності ISO/IEC 27001, виявлення вразливостей, аудиторські висновки	7
Фахівець з оцінки заходів захисту інформації (кібербезпеки) [35]	Оцінка ефективності заходів захисту, ризик-орієнтований аналіз, розроблення рекомендацій щодо удосконалення	6–7
Фахівець з технічного захисту інформації [36]	Технічний захист конфіденційної інформації; криптографічний захист, захист від витоку технічними каналами, спеціальні перевірки	6

Продовження табл. 2.4.

Назва професійного стандарту	Основний зміст і акцент компетенцій	Рівень кваліфікації (НРК)
Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту [37]	Стратегічне управління системою кібербезпеки організації; розроблення політики, координація підрозділів, забезпечення нормативної відповідності	7–8

Новий стандарт побудований на компетентнісному підході, відповідає вимогам Національної рамки кваліфікацій та європейським принципам формування освітніх програм. Він чітко розмежовує загальні та фахові компетентності, а також визначає очікувані результати навчання.

Загальні компетентності містять універсальні навички сучасного фахівця (абстрактне мислення, аналіз і синтез, командна робота, комунікація, самоосвіта та етичні норми). Фахові компетентності відображають специфіку спеціальності і охоплюють захист інформації в АС, виявлення вразливостей, реагування на кіберінциденти, оцінку ризиків, криптографічний захист, хмарну безпеку, застосування нормативно-правових актів у сфері кібербезпеки. Особлива увага приділяється практичній підготовці, зокрема навчальним і виробничим практикам.

До сильних сторін українських стандартів слід віднести врахування національної специфіки захисту державної інформації та об’єктів критичної інфраструктури в умовах воєнного стану, чітку орієнтацію на компетентнісний підхід, практичну спрямованість окремих професійних стандартів, а також оперативність їх розробки. Освітній стандарт 2024 року також став помітно прогресивнішим порівняно з версією 2019 року завдяки кращому розмежуванню загальних і фахових компетентностей і більш чіткому визначенню очікуваних результатів навчання.

Водночас порівняння з Рамкою NICE та ECSF висвітлює низку суттєвих недоліків. Найважливішими з них є недостатня деталізація компетенцій, відсутність чітких рівнів кваліфікації, значний дисбаланс на користь теоретичної

підготовки, слабке відображення сучасних технологічних викликів та недостатня інтеграція між освітніми програмами і професійними стандартами. У результаті українські випускники часто потребують тривалого додаткового навчання для відповідності реальним вимогам ринку праці та державного сектору.

Розвиток національної системи кваліфікаційних вимог відбувається в умовах подвійного тиску: гострої потреби в підготовці кадрів для захисту критичної інфраструктури під час повномасштабної війни та необхідності виконання євроінтеграційних зобов'язань, зокрема імплементації Директиви NIS2. Незважаючи на помітний прогрес 2024–2025 років, система залишається фрагментарною і потребує системної гармонізації з європейськими рамками.

Висновки до розділу 2

Встановлено, що підходи, представлені в Рамці NICE, розробленій NIST (США), та європейській Рамці ECSF від ENISA, мають два взаємодоповнюючих вектори формування кваліфікаційних вимог. Рамка NICE вирізняється високою деталізацією (TKS-структура, понад 40 робочих ролей, сотні завдань, знань і навичок), операційною точністю і зручністю для практичного застосування в організаціях. Натомість ECSF пропонує компактніший рольовий підхід (12 рольових профілів), орієнтований на гармонізацію компетенцій, професійну мобільність і відповідність законодавству ЄС, зокрема Директиві NIS2.

Аналіз національного підходу України (професійні та освітні стандарти 2024–2026 рр.) виявив помітний прогрес, але водночас суттєве відставання від міжнародних стандартів за рівнем деталізації, практичної орієнтації, наявності чітких рівнів кваліфікації та інтеграції сучасних компетенцій. За підсумками порівняльного аналізу встановлено, що найбільш перспективним для України є синтез сильних сторін обох вище згаданих міжнародних рамкових документів: деталізованої операційної структури Рамки NICE і стратегічно-гармонізаційного рольового підходу ECSF.

РОЗДІЛ 3. НАПРЯМИ ВДОСКОНАЛЕННЯ ЗАСАД ФОРМУВАННЯ КВАЛІФІКАЦІЙНИХ ВИМОГ ДО КІБЕРФАХІВЦІВ В УКРАЇНІ

3.1 Проблеми та недоліки вітчизняної системи кваліфікаційних вимог до спеціалістів з кібербезпеки

У 2024–2025 роках в Україні відбулися помітні зрушення у формуванні системи кваліфікаційних вимог до фахівців з кібербезпеки. Було затверджено новий Стандарт вищої освіти зі спеціальності F5 «Кібербезпека та захист інформації» (наказ Міністерства освіти і науки України від 29 жовтня 2024 р. № 1547) [38], а також низку професійних стандартів, затверджених Адміністрацією Держспецзв'язку України, зокрема стандарти фахівця з реагування на інциденти кібербезпеки, фахівця сфери захисту інформації, аудитора інформаційних технологій з кібербезпеки, фахівця з підтримки інфраструктури кіберзахисту та інші. Ці документи стали першим системним кроком до уніфікації вимог до знань, умінь і компетенцій спеціалістів у сфері захисту інформації та кібербезпеки.

Проте, незважаючи на певний прогрес, сучасна національна система кваліфікаційних вимог залишається недосконалою і не відповідає масштабам існуючих загроз та реальним потребам держави. Система характеризується фрагментарністю, недостатньою інтеграцією між освітніми та професійними стандартами, слабкою практичною орієнтацією та обмеженою адаптивністю до швидких змін у ландшафті кіберзагроз. Більшість стандартів все ще мають декларативний характер і не забезпечують чіткої вимірюваності рівня компетентності фахівців.

Об'єктивна необхідність критичного аналізу недоліків сучасної системи зумовлена кількома ключовими факторами. По-перше, Україна продовжує зазнавати інтенсивних кібератак, спрямованих переважно на критичну інфраструктуру, державні органи та об'єкти життєзабезпечення. По-друге, зберігається гострий дефіцит кваліфікованих кадрів, який, за оцінками

міжнародних організацій, суттєво перевищує можливості наявної системи підготовки. По-третє, євроінтеграційні зобов'язання України, зокрема імплементація вимог Директиви NIS2, вимагають приведення національних стандартів у відповідність до європейських підходів (ECSF). Без глибокого критичного аналізу наявних недоліків подальший розвиток системи буде малоефективним і не дозволить досягти необхідного рівня кіберстійкості держави.

Сучасна нормативно-правова та інституційна система регулювання кваліфікаційних вимог у сфері кібербезпеки України характеризується значною фрагментарністю та відсутністю єдиної стратегічної рамки. Це є одним із найсерйозніших системних недоліків, який суттєво знижує ефективність усієї кадрової політики у сфері кібербезпеки.

На сьогодні кваліфікаційні вимоги регулюються низкою розрізнених нормативно-правових актів, які не утворюють цілісної системи. Основні документи, серед яких Закон України «Про основні засади забезпечення кібербезпеки України», Стратегія кібербезпеки України, Стандарт вищої освіти зі спеціальності 125 та професійні стандарти Адміністрації Держспецзв'язку України, приймалися в різні періоди і не завжди узгоджені між собою. Відсутня єдина стратегічна рамка, яка б чітко визначала цілі, принципи, механізми формування та оновлення кваліфікаційних вимог на найближчі 5–10 років.

Стратегія кібербезпеки України 2021 року визначає проблему підготовки кадрів як одну з ключових, проте не містить конкретних механізмів її вирішення, чітких показників ефективності та термінів реалізації. У результаті окремі професійні стандарти та освітній стандарт розвиваються майже автономно, без єдиного координаційного центру та єдиної концепції.

Окрім цього, існує суттєва проблема міжвідомчої координації. Головним органом у сфері професійних стандартів є Адміністрація Держспецзв'язку України. Водночас за освітні стандарти відповідає Міністерство освіти і науки (МОН) України, натомість за загальну політику кібербезпеки - Рада національної безпеки і оборони України, Служба безпеки України та інші структури. Відсутність постійного дієвого механізму координації між цими органами

призводить до дублювання функцій, розбіжностей у підходах і запізнілої реакції на нові виклики.

Особливо показовим є приклад Постанови Кабінету Міністрів України «Про внесення змін до Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» [39]. Цією постановою було розширено повноваження Адміністрації Держспецзв'язку України щодо розробки та затвердження професійних стандартів у сфері кібербезпеки. Здавалося б, це позитивний крок. Однак аналіз документа показує його суттєві обмеження:

➢ Постанова посилює роль Адміністрації Держспецзв'язку України лише у сфері технічних і організаційних стандартів захисту інформації, але не наділяє її повноваженнями щодо координації всієї системи кваліфікаційних вимог (включаючи освітні стандарти).

➢ Не передбачено створення міжвідомчої робочої групи чи постійного координаційного органу з участю МОН України, Міністерства цифрової трансформації України, СБУ та інших зацікавлених сторін.

➢ Зміни мають переважно організаційно-технічний характер і не вирішують питання стратегічного планування розвитку кваліфікаційних вимог.

У результаті Адміністрація Держспецзв'язку України залишається основним розробником професійних стандартів, але не має реальних важелів впливу на освітні програми та загальну кадрову політику в сфері кібербезпеки. Це призводить до розриву між тим, чого навчають у вишах, і тим, що вимагають професійні стандарти та ринок праці.

Нормативно-правові та інституційні недоліки є фундаментальною проблемою сучасної системи кваліфікаційних вимог в Україні. Без створення єдиної стратегічної рамки та дієвого механізму міжвідомчої координації подальший розвиток системи буде малоефективним і не дозволить Україні належним чином реагувати на сучасні кіберзагрози та виконувати євроінтеграційні зобов'язання.

Одним із найбільш відчутних недоліків залишається недостатня деталізація та адаптивність затверджених професійних стандартів. Хоча у 2024–

2025 роках Адміністрація Держспецзв'язку України розробила і затвердила низку важливих документів (зокрема, професійні стандарти фахівця з реагування на інциденти кібербезпеки, фахівця сфери захисту інформації, аудитора інформаційних технологій з кібербезпеки, фахівця з підтримки інфраструктури кіберзахисту тощо), вони мають низку системних обмежень.

По-перше, стандарти не передбачають чітких рівнів володіння компетенціями (кваліфікації), що є нормою у міжнародних рамкових документах NICE та ECSF. Рівні кваліфікації за Національною рамкою кваліфікацій (6–8 рівнів) сформульовані досить узагальнено, без градації «junior / middle / senior / expert». Це суттєво ускладнює об'єктивну атестацію фахівців, кар'єрне планування та створення індивідуальних траєкторій професійного розвитку.

По-друге, у стандартах недостатньо відображені сучасні технологічні виклики, такі як безпека штучного інтелекту, DevSecOps, захист кіберфізичних систем (OT/ICS), квантова криптографія та безпека хмарних середовищ. Переважна увага приділяється традиційним технічним і організаційно-правовим аспектам захисту інформації, тоді як практичні навички роботи з SIEM-системами, цифровою криміналістикою, тестування на проникнення та розвідки загроз представлені недостатньо детально. У умовах інтенсивних кібератак на критичну інфраструктуру така невідповідність актуальному ландшафту загроз стає особливо критичною.

По-третє, відсутня комплексна інтеграція між різними стандартами, що не дозволяє формувати цілісні кар'єрні траєкторії. У результаті система залишається фрагментарною і не забезпечує безперервного професійного розвитку фахівців від бакалаврського рівня до керівних посад в галузі кібербезпеки.

Сучасна система формування кваліфікаційних вимог до фахівців з кібербезпеки в Україні характеризується комплексом взаємопов'язаних недоліків: нормативно-правовою фрагментарністю, слабкою міжвідомчою координацією, недостатньою деталізацією та адаптивністю стандартів, дисбалансом між теоретичною підготовкою в закладах вищої освіти та практичними вимогами ринку праці, а також критичним кількісним і якісним

дефіцитом кадрів. Ці проблеми не лише знижують ефективність підготовки фахівців, але й безпосередньо підривають кіберстійкість держави в умовах повномасштабної війни та євроінтеграційних процесів.

Подолання виявлених недоліків вимагає системного підходу, зокрема адаптації кращих практик міжнародних рамкових документів NICE та ECSF з обов'язковим урахуванням національної специфіки (воєнний стан, пріоритет захисту критичної інфраструктури, обмежені ресурси та необхідність швидкого реагування на гібридні загрози).

3.2 Рекомендації щодо адаптації кращих міжнародних практик формування вимог до професійної кваліфікації фахівців з кібербезпеки до українських реалій

Порівняльний аналіз Рамки NICE та ECSF показав, що жоден з них не може бути безпосередньо перенесений в українські реалії без суттєвої адаптації. Рамка NICE вирізняється високою операційною деталізацією, чіткою ієрархічною структурою TKS і орієнтацією на формування готових до виконання за фахом («job-ready») професійних завдань фахівців. Водночас ECSF пропонує більш стратегічний, рольовий підхід, що акцентує увагу на гармонізації компетенцій, професійній мобільності та відповідності європейському законодавству.

У контексті України найбільш перспективним є гібридний підхід, який поєднує сильні сторони обох моделей. Американський фреймворк дозволяє забезпечити необхідну деталізацію та вимірюваність компетенцій, що критично важливо для об'єктивної атестації фахівців, розробки посадових інструкцій та проведення аналізу прогалин. Європейський підхід, у свою чергу, сприяє створенню єдиної «мови» компетенцій, полегшує інтеграцію української системи кваліфікаційних вимог у європейський цифровий ринок праці та безпосередньо підтримує виконання вимог Директиви NIS2.

Переваги гібридної моделі для України полягають у досягненні оптимального балансу між практичною застосовністю та європейською

сумісністю. Поєднання деталізованої структури Рамки NICE з рольовими профілями ECSF дає змогу одночасно вирішувати два стратегічні завдання:

➢ формувати високо підготовлених фахівців, здатних ефективно працювати в умовах реальних кіберзагроз і гібридної війни;

➢ забезпечувати поступову інтеграцію національної системи підготовки кадрів у європейський простір кібернавичок.

Такий підхід повністю відповідає як національним безпековим пріоритетам України (захист критичної інфраструктури, протидія гібридним загрозам, оперативне реагування на кіберінциденти), так і євроінтеграційним зобов'язанням, зокрема імплементації acquis communautaire у сфері кібербезпеки. Гібридна модель дозволяє уникнути крайнощів: надмірної деталізації, характерної для американського підходу, яка може бути складною для впровадження в умовах обмежених ресурсів, та надто узагальненого рольового підходу ECSF, який сам по собі не забезпечує достатньої операційної точності.

Для ефективної адаптації міжнародних фреймворків до українських умов доцільно розробити гібридну національну модель кваліфікаційних вимог. Ця модель має поєднувати операційну деталізацію і вимірюваність американського підходу NICE з рольовою гармонізацією та європейською сумісністю ECSF. Такий синтез дозволяє врахувати специфіку України: умови гібридної війни, захист критичної інфраструктури (OT/ICS), обмежені ресурси та необхідність виконання вимог Директиви NIS2.

Рекомендації щодо інтеграції обох вище згаданих рамкових документів у гібридну національну модель кваліфікаційних вимог України представлені в таблиці 3.1.

Таблиця 3.1.

Впровадження елементів NICE та ECSF в національну модель кваліфікаційних вимог до кіберфахівців

Рамка	Елемент рамки	Практична інтеграція в українську модель	Очікуваний практичний ефект для України
NICE	TKS-структура	Детальний опис кожного професійного стандарту через конкретні завдання, знання та навички (TKS)	Перехід від декларативних до чітко вимірюваних компетенцій; полегшення розробки посадових інструкцій, атестації та gap-аналізу
NICE	Зони компетенцій (11 зон)	Інтеграція актуальних областей (безпека AI, безпека OT, кіберстійкість) у національні стандарти	Посилення захисту кіберфізичних систем об’єктів критичної інфраструктури, підготовка до загроз, пов’язаних з AI
NICE	Рівні кваліфікації	Запровадження системи рівнів кваліфікації через співвіднесення робочих ролей і зон компетенцій NICE із рівнями відповідальності SFIA (7 рівнів)	Об’єктивна оцінка фахівців, чіткі кар’єрні траєкторії (junior, expert), спрощення аналізу прогалин і планування розвитку
ECSF	12 рольових профілів	Використання рольових профілів як основи для назв і змісту національних професійних стандартів	Створення єдиної «мови» компетенцій, полегшення мобільності фахівців і пряма відповідність вимогам Директиви NIS2

Продовження табл. 3.1.

Рамка	Елемент рамки	Практична інтеграція в українську модель	Очікуваний практичний ефект для України
ECSF	Основні завдання, знання, навички	Комбінація з TKS-структурою NICE для кожного рольового профілю	Баланс між стратегічним (рольовим) і операційним (деталізованим) підходом
ECSF	Гармонізація із законодавством ЄС	Зіставлення рольових профілів ECSF з вимогами NIS2 (управління ризиками, реагування на інциденти, аудит, відповідність)	Пряма підтримка імплементації NIS2 та прискорення євроінтеграції у сфері кібербезпеки
Гібридна модель	Адаптація до національної специфіки України	Доповнення моделі елементами захисту критичної інфраструктури в умовах гібридної війни, безпеки OT/ICS, протидії інформаційно-психологічним операціям	Підвищення стійкості енергетики, транспорту, державних систем та об’єктів критичної інфраструктури до реальних загроз воєнного часу

На першому етапі доцільно провести зіставлення чинних українських професійних стандартів з елементами обох фреймворків. Наприклад, стандарт «Фахівець з реагування на інциденти кібербезпеки» доповнюється TKS-компонентами з NICE та рольовим профілем «Cyber Incident Responder» з ECSF.

На другому етапі кожен стандарт отримує:

- ➢ чітку рольову основу (з ECSF);
- ➢ деталізовану TKS-структуру (з NICE);
- ➢ рівні кваліфікації (володіння компетенціями);

➢ національні доповнення (захист OT/ICS, робота в умовах обмеженого енергозабезпечення, протидія гібридним атакам).

Такий підхід дозволяє зберегти гнучкість ECSF для європейської сумісності й отримати високу практичну точність NICE для щоденного застосування в державних органах, на об'єктах критичної інфраструктури та в приватному секторі.

Водночас гібридна модель несе певні ризики, які необхідно враховувати заздалегідь:

1. Інституційні перешкоди, пов'язані з міжвідомчою роз'єднаністю між Адміністрацією Держспецзв'язку України та Міністерством освіти і науки України через різні пріоритети та підходи.

2. Кадровий дефіцит кваліфікованих експертів, здатних здійснювати регулярне оновлення стандартів відповідно до динаміки ландшафту загроз.

3. Обмеженість фінансових ресурсів для оновлення професійних стандартів, навчання викладачів і створення необхідної навчально-методичної бази.

4. Ризик надмірної складності впровадження через деталізацію TKS-структури, що може ускладнити застосування моделі в малих і середніх організаціях.

Таким чином, гібридна модель адаптації міжнародних практик, що поєднує операційну деталізацію та вимірюваність фреймворку NICE з рольовим і гармонізаційним підходом ECSF, є найбільш оптимальним і перспективним варіантом для формування сучасної системи кваліфікаційних вимог до фахівців з кібербезпеки в Україні.

Запровадження гібридної національної моделі кваліфікаційних вимог стане важливим стратегічним кроком на шляху подолання кадрового дефіциту, підвищення якості підготовки фахівців та суттєвого посилення загальної кіберстійкості України. Воно забезпечить не лише відповідність європейським стандартам, але й створення дієвої, адаптивної та практико-орієнтованої системи

розвитку кадрового потенціалу, здатної ефективно протистояти сучасним і перспективним кіберзагрозам.

3.3 Пропозиції щодо оновлення освітніх програм і професійних стандартів в галузі кібербезпеки в Україні

Сучасна система кваліфікаційних вимог до фахівців з кібербезпеки в Україні характеризується фрагментарністю, недостатньою деталізацією компетенцій, слабкою практичною орієнтованістю та обмеженою адаптивністю до швидких змін у ландшафті кіберзагроз. Рекомендації щодо адаптації міжнародних фреймворків NICE та ECSF у межах гібридної національної моделі створюють необхідну концептуальну основу для системного оновлення як професійних стандартів, так і освітніх програм зі спеціальності F5 «Кібербезпека та захист інформації» (125 «Кібербезпека»).

1. Оновлення має ґрунтуватися на компетентнісному та орієнтованому на формування практичних навичок підході. Кваліфікаційні вимоги повинні орієнтуватися не на перелік дисциплін і годин, а на чітко сформульовані результати професійної діяльності: компетентності, знання, уміння, навички та рівні їх володіння (proficiency levels).

2. Ключовим принципом є забезпечення балансу між теоретичною підготовкою та практичними заняттями. Нинішній дисбаланс на користь теорії призводить до того, що лише 30–35 % випускників здатні відразу виконувати профільні завдання. Тому практична складова має становити не менше 50% освітніх програм і професійних стандартів.

3. Оновлення повинно передбачати інтеграцію технічних, нетехнічних і метакомпетенцій. Відповідно до моделі Бендлера-Федерера та підходу ECSF, сучасний фахівець з кібербезпеки потребує не лише глибоких технічних знань, але й розвинених «м’яких» навичок (ефективна комунікація, критичне мислення, етичне прийняття рішень) і метакомпетенцій (адаптивність, здатність до швидкого навчання, стійкість до невизначеності).

4. Усі зміни мають враховувати національну специфіку України: умови повномасштабної війни, необхідність посиленого захисту критичної інфраструктури, протидію гібридним кіберзагрозам, і забезпечувати виконання вимог Директиви NIS2.

5. Система кваліфікаційних вимог повинна бути динамічною: передбачати регулярне оновлення (не рідше одного разу на 12–18 місяців) відповідно до еволюції технологій і ландшафту загроз.

Одним із ключових напрямів вдосконалення системи кваліфікаційних вимог є оновлення професійних стандартів, розроблених Адміністрацією Держспецзв'язку України у 2024–2025 роках. На сьогодні ці стандарти, попри їхню важливість як першого системного кроку, залишаються надто узагальненими, декларативними та недостатньо адаптованими до швидких змін у ландшафті кіберзагроз. Перехід до гібридної національної моделі, дозволяє суттєво підвищити їхню якість, практичну цінність і сумісність з європейськими стандартами.

Основним принципом оновлення має стати перехід від узагальнених компетенцій до чіткої структури гібридної моделі, яка поєднує рольовий підхід ECSF з детальною ієрархічною архітектурою фреймворку NICE. Це передбачає реалізацію таких конкретних заходів:

➢ Введення чітких рівнів кваліфікації (володіння компетенціями). Сучасні професійні стандарти вказують лише рівні Національної рамки кваліфікацій (НРК 6–8) без внутрішньої градації. Рекомендується доповнити кожен стандарт шкалою з чотирьох рівнів: junior, middle, senior та expert (або рівнів на основі NICE). Такий підхід дозволить об'єктивно оцінювати кваліфікацію фахівців, формувати кар'єрні траєкторії та проводити атестацію персоналу на об'єктах критичної інфраструктури.

➢ Розширення блоків TKS за прикладом NICE. Більшість чинних стандартів містять загальні формулювання компетенцій. Необхідно деталізувати їх через конкретні професійні завдання, теоретичні знання та практичні навички. Наприклад, у професійному стандарті «Фахівець з реагування на інциденти

кібербезпеки» доцільно суттєво розширити розділ практичних навичок, включивши детальні завдання з роботи в SIEM-системах, розвідки загроз, створення та застосування збірників сценаріїв (playbooks) реагування на інциденти, цифрової криміналістики та автоматизації процесів реагування.

➢ Інтеграція 12 рольових профілів ECSF як бази для назв і змісту стандартів. Рольові профілі ENISA (зокрема CISO, Cyber Incident Responder, Cybersecurity Risk Manager, Penetration Tester, Cyber Threat Intelligence Specialist, Cybersecurity Architect) можуть стати орієнтиром для оновлення та розробки нових професійних стандартів. Це дозволить забезпечити сумісність з європейськими вимогами, зокрема з Директивою NIS2, та полегшить міжнародне визнання українських кваліфікацій згідно з аналізом (ISC)²

Конкретні пропозиції щодо ключових стандартів включають:

➢ Фахівець з реагування на інциденти кібербезпеки: посилити блоки, пов’язані з сучасними методами виявлення та реагування (SIEM, SOAR, розвідка загроз), а також додати елементи реагування на інциденти з використанням AI.

➢ Фахівець сфери захисту інформації та фахівець з технічного захисту інформації: розширити розділи, присвячені безпеці хмарних середовищ, DevSecOps, захисту кіберфізичних систем (OT/ICS) та безпеки AI.

➢ Аудитор інформаційних технологій з кібербезпеки: доповнити вимогами щодо проведення ризик-орієнтованого аудиту відповідно до ISO/IEC 27001 та оцінки ефективності заходів захисту в умовах гібридних загроз.

➢ Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту: привести у відповідність до рольового профілю CISO, значно посиливши компетенції у сфері стратегічного управління, комунікації з керівництвом, управління ризиками та забезпечення відповідності NIS2.

Для ефективного впровадження запропонованих змін до професійних стандартів і освітніх програм необхідна чітка організаційна та методологічна основа. Реалізація повинна відбуватися поетапно протягом 2026–2028 років.

➢ Етап 1 (2026 рік) - підготовчий: створення постійно діючої міжвідомчої робочої групи під координацією Адміністрації Держспецзв’язку за участю МОН

України, Міністерство цифрової трансформації України, СБУ, представників бізнесу та провідних закладів вищої освіти. Група повинна затвердити детальну дорожню карту, провести повне зіставлення чинних стандартів з гібридною національною моделлю та розробити проекти змін до нормативних документів.

➢ Етап 2 (2026–2027 роки) - пілотне впровадження: оновлення 4–5 пріоритетних професійних стандартів, внесення змін до Стандарту вищої освіти 125, апробація нових навчальних модулів (безпека AI та OT/ICS, DevSecOps) у 3–5 провідних університетах. Важливу роль на цьому етапі відіграє державно-приватне партнерство, зокрема залучення IT-компаній, операторів кіберполігонів [40] і провідних підприємств критичної інфраструктури до розробки практичних програм і надання баз для стажування.

➢ Етап 3 (2027–2028 роки) - масштабування: повне оновлення всіх професійних стандартів, перехід на нові навчальні плани у більшості закладів вищої освіти, запуск національної системи моніторингу компетенцій.

Моніторинг ефективності впровадження пропонується здійснювати за такими ключовими показниками:

1. Відсоток випускників спеціальності F5, готових до виконання профільних завдань без тривалого донавчання (цільовий показник - не менше 60% до 2028 року);
2. Рівень відповідності оновлених стандартів і програм елементам ECSF та NICE;
3. Динаміка зменшення кадрового дефіциту в державному секторі та на об’єктах критичної інфраструктури;
4. Кількість фахівців, які пройшли атестацію за новими стандартами з чіткими рівнями кваліфікації.

Необхідною умовою довгострокової ефективності запропонованих змін є регулярний перегляд і оновлення професійних стандартів та освітніх програм щонайменше раз на 2 роки з урахуванням еволюції ландшафту кіберзагроз, появи нових технологій та динаміки європейського регуляторного середовища.

Перехід до сучасної компетентнісно-орієнтованої системи підготовки

кадрів з кібербезпеки на основі гібридної національної моделі, що поєднує рольовий підхід європейської рамки ECSF з деталізованою ієрархічною структурою фреймворку NICE, дозволить досягти оптимального балансу теоретичних знань і практичних навичок, запровадити чітку вимірюваність компетенцій через рівні кваліфікації, повноцінно врахувати національну специфіку воєнного часу та пріоритети захисту критичної інфраструктури, а також забезпечити виконання євроінтеграційних зобов'язань України.

Реалізація цих пропозицій стане важливим системним кроком у формуванні висококваліфікованої, адаптивної та міжнародно сумісної кадрової складової національної системи кібербезпеки, яка відповідатиме масштабам актуальних і потенційних загроз та суттєво підвищить загальний рівень кіберстійкості Української держави.

Висновки до розділу 3

У розділі 3 проаналізовано сучасну систему формування кваліфікаційних вимог до фахівців з кібербезпеки в Україні та окреслено напрями її вдосконалення. Дослідження показало, що, незважаючи на певний прогрес упродовж 2024-2025 років (затвердження нового освітнього стандарту зі спеціальності 125 «Кібербезпека» і низки професійних стандартів), національна система залишається фрагментарною, недостатньо деталізованою та слабко адаптованою до сучасних реалій. Основними недоліками є відсутність єдиного стратегічного рамкового документу, слабка міжвідомча координація, декларативний характер стандартів, недостатня практична орієнтація і відсутність чітких рівнів володіння компетенціями.

За підсумками дослідження зроблено висновки, що для подолання виявлених проблем найбільш перспективним є гібридний підхід, який поєднує сильні сторони Рамки NICE (операційна деталізація через TKS-структуру) та ECSF (стратегічна гармонізація через рольові профілі), з обов'язковим урахуванням національної специфіки (воєнний стан, захист критичної

інфраструктури OT/ICS та євроінтеграційні зобов’язання щодо NIS2).

Запропоновані рекомендації щодо оновлення професійних стандартів і освітніх програм передбачають впровадження чітких рівнів кваліфікації (junior, middle, senior, expert), розширення практичної складової до рівня не менше 50%, інтеграцію сучасних компетенцій (безпека AI, DevSecOps, кіберстійкість) і поетапне впровадження змін протягом 2026–2028 років.

Реалізація гібридної національної моделі дозволить перейти від фрагментарної системи до цілісної, компетентнісно-орієнтованої та адаптивної моделі підготовки кадрів, що суттєво підвищить якість підготовки кіберфахівців, зменшить кадровий дефіцит та зміцнить загальну кіберстійкість України.

ВИСНОВКИ

У кваліфікаційній роботі проведено комплексне дослідження актуальної проблеми формування кваліфікаційних вимог до фахівців з кібербезпеки в умовах стрімкого зростання кіберзагроз, кадрового дефіциту та євроінтеграційних процесів України.

Проаналізовано теоретичні засади формування кваліфікаційних вимог. Встановлено, що сучасна система підготовки фахівців з кібербезпеки характеризується значним дефіцитом кваліфікованих кадрів, переважанням теоретичної підготовки над практичною і швидким застаріванням компетентностей. Доведено, що кваліфікаційні вимоги є ключовим системоутворюючим елементом, який забезпечує узгодження інтересів ринку праці, системи освіти й державної політики у сфері національної безпеки. Основними компонентами таких вимог є компетентності, знання, уміння, навички та рівні їх володіння.

Дослідження міжнародних підходів до формування кваліфікаційних вимог фахівця з кібербезпеки показало, що американський підхід (Рамка NICE від NIST) відрізняється високою деталізацією TKS-структури, операційною точністю та значною кількістю робочих ролей. Натомість європейський підхід (ECSF від ENISA) орієнтований на рольові профілі, гармонізацію компетенцій і забезпечення мобільності фахівців у межах ЄС. Національний підхід України (професійні та освітні стандарти 2024–2026 рр.) демонструє помітний прогрес, але залишається фрагментарним, недостатньо деталізованим і слабко адаптованим до сучасних технологічних викликів.

Виявлено основні проблеми сучасної системи кваліфікаційних вимог в Україні: нормативно-правову фрагментарність, слабку міжвідомчу координацію, декларативний характер стандартів, відсутність чітких рівнів кваліфікації, дисбаланс між теорією та практикою, а також недостатню інтеграцію сучасних компетенцій (безпека AI, DevSecOps, OT/ICS).

Обґрунтовано доцільність розробки гібридної національної моделі кваліфікаційних вимог, яка поєднує деталізовану TKS-структуру Рамки NICE з рольовим підходом ECSF. Такий синтез дозволяє забезпечити високу операційну точність, європейську сумісність і врахування національної специфіки (воєнний стан, захист критичної інфраструктури в умовах кіберзагроз).

Розроблено практичні рекомендації щодо оновлення професійних стандартів і освітніх програм зі спеціальності F5 «Кібербезпека та захист інформації». Запропоновано впровадити чіткі рівні кваліфікації (junior, middle, senior, expert), розширити практичну складову до 50%, інтегрувати сучасні компетенції та здійснити поетапне впровадження змін протягом 2026–2028 років.

Практичне значення одержаних результатів полягає в тому, що розроблені рекомендації можуть бути використані Адміністрацією Держспецзв’язку України для оновлення професійних стандартів, закладами вищої освіти - для вдосконалення освітніх програм, а також планування програм підвищення кваліфікації й атестації фахівців. Реалізація запропонованої гібридної моделі сприятиме зменшенню кадрового дефіциту, підвищенню якості підготовки кіберфахівців і суттєвому зміцненню кіберстійкості України в сучасних умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Fortinet 2025 Cybersecurity Skills Gap Global Research Report. *Fortinet*. Sunnyvale, 2025. URL: https://www.fortinet.com/content/dam/fortinet/assets/reports/2025-cybersecurity-skills-gap-report.pdf

2. Cyber Security Resilience 2025. *Allianz Commercial*. 2025. URL: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/cyber-security-trends-2025.pdf

3. Global Cybersecurity Outlook 2026. World Economic Forum. Geneva : *WEF*, 2026. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

4. 2025 ISC2 Cybersecurity Workforce Study. *ISC2*. URL: https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study

5. В Україні бракує близько 100 тисяч фахівців з кібербезпеки. *Укрінформ*. 2025. URL: https://www.ukrinform.ua/rubric-society/3975920-v-ukraini-brakue-blizko-100-tisac-fahivciv-z-kiberbezpeki.html

6. Ukraine Digital Development Country Profile 2025. International Telecommunication Union (ITU). Geneva : *ITU*, 2025. URL: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/2025/Final_Ukraine%20Digital%20Development%20Country%20Profile%20version%203.0.pdf

7. Skills Framework for the Information Age (SFIA). Cybersecurity Skills Profile. *SFIA Foundation*. 2025. URL: https://sfia-online.org/en/tools-and-resources/cybersecurity-skills-framework

8. Cyber Security Skills in the UK Labour Market 2025. Department for Science, Innovation and Technology ; *National Cyber Security Centre*. London, 2026. URL: https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2025/cyber-security-skills-in-the-uk-labour-market-2025

9. Competency Models for Information Security and Cybersecurity Professionals: Analysis of Existing Work and a New Model / Bendler D. et al. // *ACM*

Transactions on Computing Education. 2023 (оновлено 2025). Vol. 23, № 2. Art. 25. P. 1–33. URL: https://dl.acm.org/doi/abs/10.1145/3573205

10. The Cyber Security Body of Knowledge (CyBOK) Version 1.1 / The CyBOK Project, *University of Bristol.* 2021. URL: https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

11. NICE Workforce Framework for Cybersecurity (NICE Framework). National Institute of Standards and Technology (NIST). Gaithersburg : *NIST*, 2025. URL: https://niccs.cisa.gov/tools/nice-framework

12. NICE Framework Competency Areas: Preparing a Job-Ready Cybersecurity Workforce (NISTIR 8355). National Institute of Standards and Technology. Gaithersburg : *NIST*, 2023 (оновлено 2025). URL: https://doi.org/10.6028/NIST.IR.8355

13. Кальченко В. Формування компетентностей майбутніх фахівців кібербезпеки завдяки ініціативі «Студентські кібербригади». *Кібербезпека: освіта, наука, техніка*. 2025. № 1. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/1006

14. Горлинський В. В., Горлинський Б. В. Аналіз ключових чинників формування системи компетентностей фахівців у галузі кібербезпеки. *Information Technology and Security*. 2021. Vol. 9, № 2. С. 219–231. URL: https://doi.org/10.20535/2411-1031.2021.9.2.249976

15. NIST Special Publication 800-181 Revision 1. The Workforce Framework for Cybersecurity (NICE Framework). *National Institute of Standards and Technology (NIST)*. URL: https://doi.org/10.6028/NIST.SP.800-181r1

16. NICE Framework Components v2.1.0 (December 3, 2025). *National Institute of Standards and Technology (NIST).* URL: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions

17. ENISA International Strategy 2026. European Union Agency for Cybersecurity (ENISA). Heraklion : *ENISA*, 2026. URL: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20International%20Strategy.pdf

18. Building a Skilled Cyber Security Workforce in Europe. Organisation for

Economic Co-operation and Development (OECD). Paris : *OECD*, 2024. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/02/building-a-skilled-cyber-security-workforce-in-europe_6abaf769/3673cd60-en.pdf

19. European Cybersecurity Skills Framework (ECSF). European Union Agency for Cybersecurity (ENISA). Heraklion : *ENISA*, 2025–2026. URL: https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf

20. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

21. EU Cybersecurity Strategy 2020–2025. Shaping Europe's digital future. *European Commission*. URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

22. EU Skills Agenda. Employment, Social Affairs and Inclusion. *European Commission*. URL: https://employment-social-affairs.ec.europa.eu/policies-and-activities/skills-and-qualifications/european-skills-agenda_en

23. The ENISA Cybersecurity Exercise Methodology. European Union Agency for Cybersecurity (ENISA). Heraklion : *ENISA*, 2026. URL: https://www.enisa.europa.eu/publications/the-enisa-cybersecurity-exercise-methodology

24. Cybersecurity roles and skills for NIS2 essential and important entities. Mapping NIS2 Obligations with ECSF Role Profiles. European Union Agency for Cybersecurity (ENISA). Heraklion : *ENISA*, 2025. URL: https://www.enisa.europa.eu/sites/default/files/2025-06/Mapping%20NIS%202%20obligations%20with%20ECSF%20role%20profiles.pdf

25. Almeida F. Comparative analysis of EU-based cybersecurity skills frameworks. *Computers & Security*. 2025. Vol. 151. Art. 104329. URL: https://www.sciencedirect.com/science/article/pii/S0167404825000185

26. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII (зі змінами, внесеними Законом України від

27.03.2025 № 4336-IX). URL: https://zakon.rada.gov.ua/laws/show/2163-19

27. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20

28. Стратегія кібербезпеки України : затв. Указом Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021

29. Про професійні стандарти : Закон України від 05.07.2012 № 4312-VI (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/4312-17

30. Національна рамка кваліфікацій : затв. Постановою Кабінету Міністрів України від 23.11.2011 № 1341 (в редакції постанови від 16.11.2022 № 1284). URL: https://zakon.rada.gov.ua/laws/show/1341-2011-п

31. Професійний стандарт «Фахівець з реагування на інциденти кібербезпеки». *Адміністрація Держспецзв'язку України*. Київ, 2024. URL: https://register.nqa.gov.ua/uploads/0/571-fahivec_z_reaguvanna_na_incidenti_kiberbezpeki_v_2.pdf

32. Професійний стандарт «Фахівець сфери захисту інформації» : затв. наказом Адміністрації Держспецзв'язку України від 23.01.2024 № 38. URL: https://register.nqa.gov.ua/

33. Професійний стандарт «Фахівець з підтримки інфраструктури кіберзахисту». *Адміністрація Держспецзв'язку України.* Київ, 2024. URL: https://register.nqa.gov.ua/uploads/0/570-fahivec_z_pidtrimki_infrastrukturi_kiberzahistu_v_2.pdf

34. Професійний стандарт «Аудитор інформаційних технологій (з кібербезпеки)». *Адміністрація Держспецзв'язку України*. Київ, 2024. URL: https://register.nqa.gov.ua/uploads/0/578-auditor_informacijnih_tehnologij_z_kiberbezpeki_v_2.pdf

35. Професійний стандарт «Фахівець з оцінки заходів захисту інформації (кібербезпеки)». *Адміністрація Держспецзв'язку України*. Київ, 2024. URL: https://register.nqa.gov.ua/uploads/0/579-

fahivec_z_ocinki_zahodiv_zahistu_informacii_kiberbezpeki_v_2.pdf

36. Професійний стандарт «Фахівець з технічного захисту інформації». *Адміністрація Держспецзв'язку України*. Київ, 2024. URL: https://register.nqa.gov.ua/uploads/0/572-fahivec_z_tehnicnogo_zahistu_informacii_v_2.pdf

37. Професійний стандарт «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту». *Адміністрація Держспецзв'язку України*. Київ, 2024. URL: https://register.nqa.gov.ua/uploads/0/576-kerivnik_strukturnogo_pidrozdilu_z_pitan_bezpeki_informacii_ta.pdf

38. Стандарт вищої освіти зі спеціальності 125 Кібербезпека та захист інформації (перший (бакалаврський) рівень) : затв. наказом Міністерства освіти і науки України від 29.10.2024 № 1547. URL: https://mon.gov.ua/static-objects/mon/uploads/public/675/c15/82e/675c1582e6574702074065.pdf

39. Про внесення змін до Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України : Постанова Кабінету Міністрів України від 04.06.2025 № 669. URL: https://zakon.rada.gov.ua/go/669-2025-п

40. Sánchez J. A framework for designing and certifying ECSF-aligned cybersecurity training through cyber ranges and virtual learning environments. *International Journal of Information Security*. 2026. Vol. 25. Art. 46. URL: https://link.springer.com/article/10.1007/s10207-025-01202-0