

DOI: 10.18372/2310-5461.62.18710
УДК 378.005.94 : 004 (045)

О. К. Юдін, д-р техн. наук., проф.
Державний науково-дослідний інституту технологій кібер-
безпеки та захисту інформації
orcid.org/0000-0002-6417-0768
e-mail: yudin.ok8@gmail.com;

О. Ю. Юдін, канд. техн. наук., проф.
Державний науково-дослідний інституту технологій кібер-
безпеки та захисту інформації
orcid.org/0000-0002-4730-1463
e-mail: yudinalex.ua@gmail.com;

Л. Г. Черниш, канд. техн. наук, доцент
Державний науково-дослідний інституту технологій кібер-
безпеки та захисту інформації
orcid.org/0009-0004-9264-
8863
e-mail: lg4lg666@gmail.com;

В. А. Телющенко
Державний науково-дослідний інституту технологій кібер-
безпеки та захисту інформації
orcid.org/0000-0001-6026-5105
e-mail: telyushchenko@bigmir.net

МЕТОДИ ІМПЛЕМЕНТАЦІЇ ЄВРОПЕЙСЬКОЇ РАМКИ НАВИЧОК З КІБЕРБЕЗПЕКИ ПРИ ФОРМУВАННІ КОНТЕНТУ ПРОФЕСІЙНОГО СТАНДАРТУ «КЕРІВНИК СТРУКТУРНОГО ПІДРОЗДІЛУ З ПИТАНЬ БЕЗПЕКИ ІНФОРМАЦІЇ ТА КІБЕРЗАХИСТУ»

Вступ

Європейська рамка вмінь та навичок у сфері кібербезпеки / European Cybersecurity Skills Framework (ECSF) [1, 2], сформована комітетами Об'єднаного Європейського агентства з кібербезпеки / European Union Agency for Cybersecurity, ENISA). Об'єднане Європейське агентство з кібербезпеки ENISA (далі – Агентство), є Агентством, яке співпрацює з державами-членами та органами ЄС, а також допомагає Європейському суспільству підготуватися до ефективного захисту інформаційних ресурсів кожної країни у кіберпросторі [3].

Тотальна нестача кадрів з кібербезпеки на ринку послуг та недоліки в системі професійної стандартизації й освітніх процесів в країнах Європи, а саме відсутність формалізованої стандартизації знань, вмінь та навичок (зокрема дескрипторів та їх рівнів) є серйозною проблемою, як для економічного розвитку країн, так і для національної безпеки будь-якої держави в цілому. Агенція ENISA формалізувала методики та висвітлила потребу Європи у комплексному підході до формування набору професійних ролей і навичок у сфері кібербезпеки. Зазначені формалізовані набори професійних ролей можна вико-

ристати для зменшення дефіциту сертифікованих фахівців у сфері інформаційних технологій і кібербезпеки та забезпечити зменшення розриву існуючих кваліфікацій сектору індустрії та відповідних їм посад до вимог щодо переліку і контенту знань, вмінь та навичок. Агенція ENISA розробила систему професійної стандартизації та представила Європейську структуру знань, вмінь та навичок з кібербезпеки (далі – ECSF), яка спрямована на зміцнення європейської культури обізнаності у сфері кібербезпеки шляхом надання інтегрованої системи кваліфікацій для спільнот Європи всіх категорій.

Рамка ECSF надає практичний засіб для ідентифікації та формалізації завдань, компетенцій, навичок і знань, які пов'язані з професійними ролями фахівців з кібербезпеки в Європі. Основна мета цієї Рамки полягає в досягненні спільного розуміння між роботодавцями та розробниками освітніх програм різних класів і категорій у країнах-членах Європейського союзу. Європейська Рамка з кібербезпеки є цінним інструментом для подолання відмінностей між вимогами сектору індустрії, професійною стандартизацією та навчальними процесами закладів освіти.

Аналіз останніх досліджень та публікацій

Дослідження в сфері професійних IT-стандартів є актуальним питанням. Дане питання розглядалося різними науковцями, зокрема варто виділити наукову статтю доцента кафедри автоматизованих систем обробки інформації та управління Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» Тетяни Ковалюк (2017 рік). У цій статті обговорюється важливість, концепція та роль професійних та освітніх стандартів у IT-індустрії. Автор описує структуру та зміст таких стандартів в Україні, підкреслює значення аналізу потреб різних зацікавлених сторін при формуванні змісту IT-освіти, а також наголошує на важливості впровадження професійних стандартів (ПС), які надають освітнім закладам необхідну інформацію про напрями та об'єкти професійної діяльності випускників, їхні завдання та потрібні компетенції майбутніх IT-фахівців. [4].

У 2019 році професором кафедри суспільних дисциплін Національного університету водного господарства та природокористування Т. Кристопчук проведено порівняльний аналіз стандартів професійної підготовки фахівців у країнах Європейського Союзу та в Україні. Вона проаналізувала нормативно-правове забезпечення розроблення професійних стандартів у контексті неперервної освіти у європейських країнах та в Україні. [5].

Також питання формування професійних компетентностей фахівців з інформаційних технологій та кібербезпеки розглянуті в наукових збірках Матвійчук-Юдіної О.В. та інших учених.

Постановка проблеми

Метою статті є дослідження сучасних методів та моделей формування контенту професійних стандартів в галузі кібербезпеки на основі методики опису знань, вмінь, навичок та рівнів дескрипторів Європейської рамки навичок з кібербезпеки. Дослідження процесів імплементації проводиться в рамках вимог Національної рамки кваліфікації України (далі – НРК).

Також до мети статті відноситься розробка базових компонентів контенту професійного стандарту «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту» на основі моделі Європейській рамці навичок з кібербезпеки (Далі – Рамки ECSF) та відповідних їй дескрипторів. Автори повинні визначити ключові складові та методи імплементації, які ґрунтуються на Рамки ECSF.

Основні переваги для імплементації Рамки ECSF повинні бути:

- уніфікація термінології, дескрипторів та спільне розуміння в контексті професійних площин серед кіберсуспільства у Європейському союзі;
- визначення формату представлення та формалізованого набору навичок, необхідних для кіберсуспільства, які є базово-критичними для опису кожної професійної площини;
- сприяння гармонізації процесів підготовки та освітньої й професійної атестації кадрів, адаптації освітніх процесів й освітньо-професійних програм кар'єрного зросту фахівців та розвитку системи професійної атестації кадрів.

Виклад основного матеріалу

Європейська рамка вмінь та навичок у сфері кібербезпеки / European cybersecurity skills framework

Структура Європейської рамки описує найважливіші вимоги до професійного робочого місця фахівця, визначаючи набір із 12 можливих типових професійних ролей або 12 фіксованих професійних профілів у сфері кібербезпеки, а саме (зазначені назви представлені на базі офіційного перекладу ENISA): головний фахівець з інформаційної безпеки (CISO); фахівець із реагування на кіберінциденти; фахівець із кіберправових питань, політики та дотримання нормативних вимог (комплаєнсу); фахівець з аналізу кіберзагроз; архітектор із кібербезпеки; аудитор із кібербезпеки; викладач із кібербезпеки; фахівець із впровадження кібербезпеки; дослідник із кібербезпеки; менеджер кібербезпекових ризиків; слідчий із цифрової криміналістики; тестувальник на проникнення (зазначені назви представлені на базі офіційного перекладу ENISA).

Визначені профілі забезпечують загальне розуміння основних професійних площин (так званих – професійних місій) кібербезпеки, а саме завдань і навичок, необхідних у професійному контексті кібербезпеки, що робить їх ідеальним довідником для сектору індустрії. Рамку ECSF було розроблено таким чином, щоб вона була простим для розуміння та достатньо всеосяжним інструментом з метою висвітлення повних відомостей у сфері кібербезпеки. Рамка ECSF повинна бути достатньо гнучка з точки зору методики, щоб дозволити комбінувати професійні профілі відповідно до потреб кожної організації, підприємства або установи різних форм власності. Враховуючи точки зору всіх зацікавлених сторін: підприємств, організацій та громадських об'єд-

нань ця формалізована структура повинна бути застосовна до всіх типів організацій і може бути фундаментом розвитку різних класів професій (комбінація професій на базі зазначених 12) у сфері кібербезпеки.

Дослідження авторів охоплює важливий аспект розробки методів та моделей формування професійних стандартів в галузі кібербезпеки в Україні, зосереджуючись на прикладі створення контенту для стандарту «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту».

Порівняльний аналіз дескрипторів Європейської рамки вмінь та навичок у сфері кібербезпеки та Національної рамки кваліфікації

Рамка EQF [6] включає в себе вісім рівнів, які систематизують результати навчання у категоріях знань, умінь та додатково включають позиції автономії/відповідальності. Зазначені рівні не прив'язані безпосередньо до конкретних типів професійних кваліфікацій. Однак, в контексті Болонського процесу деякі види кваліфікацій фахівці неофіційно пов'язують із певними рівнями результатів навчання та дескрипторів. Зокрема, рівні 6, 7 та 8 часто асоціюються із ступенями бакалавра, магістра та доктора наук відповідно. Деякі країни включають у свої національні рамки кваліфікацій також і ті, що виходять за межі формальної освіти та враховують часткові професійні кваліфікації. Ця різноманітність є надзвичайно важливою, оскільки вона сприяє процесу навчання фахівця протягом усього життя, отримуючи та підтверджуючи результати навчання в рамках неформальної або інформальної освіти.

Однак, як приклад відмінності Рамки EQF, можна привести підтвердження визнання важливості роботи інтеграційних структур світового ІТ суспільства у сфері кібербезпеки, це робота Громадських об'єднань Національної Ініціативи США, а саме груп Робочої Сили та Освіти з Кібербезпеки (National Initiative for Cybersecurity Education's USA/NICE). В рамках проєктів NICE був розроблений освітньо-професійний стандарт NICE NIST 800–181 National Cybersecurity Work force Framework та Індустріальна модель з Кібербезпеки США (Cybersecurity Industry Model USA), яка зараз визнана урядом США і світовою промисловістю як стандарт галузі.

Детально досліджуючи ці стандарти та промислову модель, можна констатувати наявність різних класів компетентностей (9 рівнів) та їх формалізований набір знань, вмінь та навичок, а також відповідні їм дескриптори. За Індустріальною моделлю США, можемо визначити компетентність фахівця за сформованим переліком критично необхідних знань, що формують робочі навички для конкретної професійної категорії.

Такий підхід до формування компетентностей особистості та освітньо-професійних дескрипторів, які розроблені громадськими установами, університетами та ведучими організаціями, визнається світовою кіберспільнотою та державними установами як стандарт освітньо-професійної діяльності галузі.

Згідно зі світовим досвідом і вимогами сектору індустрії та враховуючи освітньо-професійні стандарти галузі, а саме стандарт NICE NIST 800–181\National Cybersecurity Work force Framework, можемо визначити методику формування компетентностей фахівця (знань, вмінь та навичок) з кібербезпеки для формування освітніх і професійних стандартів галузі та відповідних їм дескрипторів.

Класифікація компетентностей за Індустріальною моделлю США та стандартом NICE NIST 800–181 [7] має 1 бакалаврський набір, а саме – так звані фундаментальні компетентності першого освітньо-кваліфікаційного рівня бакалавр:

- Особисті;
- Академічні (замість загальна);
- Фахові (спеціальні);
- Робочого місця.

Класифікація компетентностей за професійним стандартом галузі включає всі чотири попередні та дві Професійні компетентності промисловості (сектор індустрії) у відповідності до другого освітньо-кваліфікаційного рівня магістр, а саме – Професійні компетентності промисловості:

- технічні компетентності;
- функціональні компетентності.

Дескриптори Європейської рамки кваліфікації застосовують наступні визначення згідно EQF:

– “Knowledge/знання” означає результат засвоєння інформації через навчання. Знання – це сукупність фактів, принципів, теорій і практик, які пов'язані зі сферою роботи або навчання. У контексті EQF знання описуються як теоретичні та/або фактичні;

– “Skills/навички” означають здатність застосовувати знання та використовувати новітні технології для виконання завдань та вирішення проблем. У контексті EQF навички описуються як когнітивні (передбачають використання логічного, інтуїтивного та творчого мислення) або практичні (передбачають «ручну спритність» та використання методів, матеріалів, інструментів);

– «Responsibility and autonomy/відповідальність та автономія» означає здатність фахівця

застосовувати знання та навички автономно та з відповідальністю.

Кожен з 8 рівнів Європейської рамки кваліфікації EQF визначається набором дескрипторів, які вказують на результати навчання, що мають відношення до кваліфікації на цьому рівні в будь-якій системі кваліфікацій, будь то інформаційні технології, кібербезпека або медицина. Структура кожного профілю професійної ролі наведена в табл. 1.

Таблиця 1

Структура кожного профілю ролі

Назва профілю	Назва профілю професійної ролі
Альтернативні назви	Перелік назв за профілем
Резюме	Вказує на основне призначення профілю
Місія	Описує обґрунтування профілю
Результат(и)	Список типових результатів профілю, а також пояснення релевантності профілю з неекспертної точки зору
Основні завдання	Перелік типових завдань, які виконує профільна роль
Основні навички	Перелік умінь та навичок, необхідних для виконання робочих функцій і обов’язків за профілем. У деяких випадках навички м’якого спілкування та етика чітко висвітлюються
Основні знання	Перелік основних знань, необхідних для виконання робочих функцій і обов’язків за профілем
е-компетенції (з Системи е-компетенцій e-CF)	Щоб швидко знайти компетенції e-CF, зайдіть на сайт e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer

Профіль для кожної ролі заповнюється набором описових елементів, призначених для надання моментального зрізу функціоналу ролі з точки зору її формалізованого опису завдань, навичок, компетентностей та відповідних їм дескрипторів. Назви та типові альтернативні назви (змішані професійні ролі) можна використовувати як швидкий довідковий інструмент, щоб скерувати користувачів ECSF до найбільш необхідних профілів ролей з метою подальшої розробки їх освітньо-професійних програм [8, 9, 10].

Компоненти профілів ролей можна змінити, щоб краще задовольнити потреби зацікавлених організацій, підприємств та установ різних форм власності, а профілі ролей (з ECSF та інших структур) можна змішувати.

В Україні дескриптори різних рівнів означено змінами протягом деякого часу їх імплементації відповідно до EQF. На даний момент вони виявляються значно ближчими до дескрипторів EQF. У 2017 році, після введення кваліфікацій молод-

шого бакалавра і фахової передвищої освіти, був доданий одинадцятий рівень дескрипторів. У 2020 році рівні були повністю адаптовані до EQF. Рівні Національної рамки кваліфікацій України розроблені з огляду на EQF, однак мають відмінності. Рівні української Національної рамки кваліфікацій є більш деталізованими, та крім базових категорій знання, уміння та навички, відповідальність і автономія, особлива увага приділяється опису категорії – комунікація [11].

Кожен з 8 рівнів визначається набором дескрипторів, що вказують на результати навчання, що мають відношення до кваліфікації на цьому рівні в будь-якій системі кваліфікацій Як приклад візьмемо порівняння дескрипторів 6–8 рівнів Європейської та Національної рамки кваліфікацій (табл. 2).

Нижче представлено порівняльний аналіз дескрипторів рівнів EQF та української Національної рамки кваліфікацій.

Таблиця 2

Порівняльна таблиця дескрипторів Європейської та Національної рамки кваліфікацій 6-8 рівнів

Знання		Навички		Відповідальність і автономність	
Європейська РК	Національна РК	Європейська РК	Національна РК	Європейська РК	Національна РК
Рівень 6 – результати навчання					
Поглиблені знання в галузі роботи або навчання, включно критичне розуміння теорій і принципів	Концептуальні наукові та практичні знання, критичне осмислення теорій, принципів, методів і понять у сфері професійної діяльності та/або навчання	Передові навички, що демонструють майстерність та інновації, необхідні для вирішення складних і непередбачуваних проблем у спеціальній сфері роботи чи навчання	Поглиблені когнітивні та практичні уміння/навички, майстерність та інноваційність на рівні, необхідному для розв'язання складних спеціальних задач і практичних проблем у сфері професійної діяльності або навчання	Керувати складною технічною чи професійною діяльністю чи проектами, беручи на себе відповідальність за прийняття рішень у непередбачуваних умовах роботи чи навчання; брати на себе відповідальність за управління професійним розвитком окремих осіб і груп	Управління складною технічною або професійною діяльністю чи проектами; спроможність нести відповідальність за вироблення та ухвалення рішень у непередбачуваних робочих та/або навчальних контекстах; формування суджень, що враховують соціальні, наукові та етичні аспекти організація та керівництво професійним розвитком осіб та груп; здатність продовжувати навчання із значним ступенем автономії
Рівень 7 – результати навчання					
Вузкоспеціалізовані знання, деякі з яких знаходяться на передньому краї знань у сфері роботи чи навчання, як основа для оригінального мислення та/або дослідження Критичне усвідомлення проблем знань у галузі та на стику між різними галузями	Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у галузі та на межі галузей знань	Спеціалізовані навички вирішення проблем, необхідні в дослідженнях та/або інноваціях, щоб розробити нові знання та процедури та інтегрувати знання з різних галузей	Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур; здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах; здатність розв'язувати проблеми у	Керувати складними, непередбачуваними і потребуючими нових стратегічних підходів контекстами роботи чи навчання та змінювати їх; брати на себе відповідальність за внесок у професійні знання та практику та/або за перегляд стратегічної	Управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів; відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів; здатність продовжувати навчання з високим ступенем автономії

Закінчення табл. 2

Знання		Навички		Відповідальність і автономність	
Європейська РК	Національна РК	Європейська РК	Національна РК	Європейська РК	Національна РК
			нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	діяльності команд	
Рівень 8 – результати навчання					
Знання на найсучаснішому рубежі сфери роботи чи навчання та на стику між галузями	Концептуальні та методологічні знання в галузі чи на межі галузей знань або професійної діяльності	Найдосконаліші та спеціалізовані навички та методи, включно синтез та оцінювання, необхідні для вирішення критичних проблем у дослідженнях та/або інноваціях, а також для розширення та перегляду існуючих знань або професійної практики	Спеціалізовані уміння/навички і методи, необхідні для розв'язання значущих проблем у сфері професійної діяльності, науки та/або інновацій, розширення та переоцінки вже існуючих знань і професійної практики; започаткування, планування, реалізація та коригування послідовного процесу ґрунтового наукового дослідження з дотриманням належної академічної доброчесності; критичний аналіз, оцінка і синтез нових та комплексних ідей	Демонструвати значний авторитет, інноваційність, автономію, наукову та професійну доброчесність і постійну відданість розвитку нових ідей або процесів на передньому краї роботи чи навчання, включно дослідження	Демонстрація значної авторитетності, інноваційності, високий ступінь самостійності, академічна та професійна доброчесність, постійна відданість розвитку нових ідей або процесів у передових контекстах професійної та наукової діяльності; здатність до безперервного саморозвитку та самовдосконалення

В Україні є різні типи кваліфікацій, передбачені Законом «Про освіту»; вони поділяються на освітні та професійні. Освітні кваліфікації, зі свого боку, поділяються на різні типи для: загальної освіти; професійної (професійно-технічної) (включно з післядипломною) та фахової передвищої освіти; вищої освіти.

У сфері загальної освіти, яка охоплює з 1-го по 4-й рівні НРК, видаються такі документи про

освіту [11]: свідоцтво про здобуття базової середньої освіти для осіб з особливими потребами; свідоцтво про здобуття базової середньої освіти; свідоцтво про здобуття повної загальної середньої освіти.

Кваліфікації професійної (професійно-технічної) освіти (далі – ПО, ПТО) відповідають 2–5 рівням НРК. До них входять дипломи кваліфікованих робітників і свідоцтва про присвоєння (під-

вищення) робітничої кваліфікації. На рівні 5 також існує диплом про здобуття фахової передвищої освіти або фахового молодшого бакалавра (раніше – молодший спеціаліст). До кваліфікацій вищої освіти (ВО) належать: рівень 5 – молодший бакалавр, рівень 6 – бакалавр, рівень 7 – магістр, рівень 8 – доктор філософії, доктор мистецтва.

В Україні типи професійних кваліфікацій у відповідності до НПК визначаються у професійних стандартах сфери кібербезпеки. Протягом 2022–2023р.р. в державі були розроблено та введено в дію 21 професійний стандарт з кібербезпеки та захисту інформації, а Національним агентством кваліфікацій у січні 2024 року ці стандарти були внесені до Реєстру професійних стандартів України.

Методика розробки професійних стандартів та відповідність їх рівнів кваліфікацій дескрипторам НПК сформована Національним агентством кваліфікацій (далі – НАК) та передбачає додатково категорії часткової професійної кваліфікації.

Формування контенту професійного стандарту «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту» у відповідності до Європейської рамки вмінь та навичок у сфері кібербезпеки/ECSF

Формування контенту ПС «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту» ґрунтується на формуванні Характеристики фахівця у відповідності до Рамки кваліфікацій з кібербезпеки США / Workforce

Framework for Cybersecurity USA [1, 3] та Європейської рамки вмінь та навичок у сфері кібербезпеки / European Cybersecurity Skills Framework (ECSF). Даний підхід є базовий, оскільки відповідна професійна кваліфікація (професійний профіль) присутня як у Категоріях робочих ролей Workforce Framework for Cybersecurity USA, так і в Європейській рамці вмінь та навичок у сфері кібербезпеки (ECSF).

Згідно з новим переліком професій, внесених до ДК – 003: 2010 у 2021–2022р.р., професійному стандарту «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту» за професійним спрямуванням відповідає:

– професійна категорія: Категорія/Category: Oversee and Govern (OV)/Нагляд та управління і безпосередньо її професійна площина Виконавчий керівник з кібербезпеки/Executive Cyber Leadership у відповідності до NICE NIST Special Publication 800–181;

– професійний профіль: Головний фахівець з інформаційної безпеки (CISO)/Chief Information Security Officer (CISO) згідно з ECSF.

Враховуючи відповідність перекладу зі словосполученням «кіберзахист» Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту/Chief Information Security Officer (CISO), пропонується використовувати в подальшому відповідно до назви Європейської рамки ECSF (табл. 3).

Таблиця 3

Таблиця відповідності назв кваліфікацій

Класифікатор професій України ДК – 003: 201	NICE NIST Special Publication 800–181	Європейська рамка вмінь та навичок у сфері кібербезпеки ECSF
Код ДК: 1239	Код: COG (OV)	Code ESCO : 2529.1
«Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту»	Executive Cyber Leadership	Chief Information Security Officer (CISO)
Назву введено у ДК відповідності до: ECSF ENISA	Категорія / Category: Oversee and Govern (OV) / Нагляд та управління	

Як приклад, розглянемо базові складові контенту керівника з кібербезпеки за Європейською рамкою ECSF: Головний фахівець з інформаційної безпеки (CISO)/ECSF (табл. 4).

Таблиця 4

Базові складові контенту керівника з кібербезпеки за Європейською рамкою ECSF

Назва профілю	Головний фахівець з інформаційної безпеки (Chief information security officer (CISO)/ECSF)	
Альтернативні назви <i>Перелік назв за тим самим профілем</i>	Директор програми з кібербезпеки, Фахівець з інформаційної безпеки (ISO), Керівник відділу інформаційної безпеки, Фахівець з IT-безпеки	
Резюме <i>Вказує основне призначення профілю</i>	Керує стратегією кібербезпеки організації та її реалізацією для належного забезпечення безпеки і захисту цифрових систем, послуг та активів	
Місія <i>Описує обґрунтування профілю</i>	Визначає, обґрунтовує та інформує про бачення, стратегію, політику та процедури кібербезпеки. Керує впровадженням політики кібербезпеки в організації. Забезпечує обмін інформацією із зовнішніми органами та професійними організаціями	
Основні завдання <i>Перелік типових завдань, що їх виконує Головний фахівець з інформаційної безпеки (CISO)</i> <i>Виконує такі завдання:</i>	<ul style="list-style-type: none"> Визначати, впроваджувати, повідомляти і підтримувати цілі, вимоги, стратегії, політику кібербезпеки, узгоджені з бізнес-стратегією для підтримки цілей організації; готувати і представляти бачення, стратегії та політики кібербезпеки для затвердження вищим керівництвом організації, а також забезпечувати їх виконання; контролювати застосування та вдосконалення Системи менеджменту інформаційною безпекою (СМІБ); навчати вище керівництво щодо кібербезпекових ризиків і загроз та їх впливу на організацію; забезпечити узгодження з вищим керівництвом кібербезпекових ризиків організації; розробити плани кібербезпеки; розвивати відносини з органами та громадами, що займаються кібербезпекою; повідомляти вищому керівництву про кібербезпекові інциденти, ризики, висновки; стежити за розвитком кібербезпеки; забезпечувати ресурси для реалізації стратегії кібербезпеки; погоджувати бюджет кібербезпеки з вищим керівництвом; забезпечувати стійкість організації до кіберінцидентів; управляти безперервним нарощуванням потенціалу в організації; переглядати, планувати і розподіляти відповідні ресурси кібербезпеки; 	
Основні знання Перелік основних знань, необхідних для виконання трудових функцій та обов'язків за профілем. (Залежно від рівня) Базове розуміння: Розуміння: Знання: Глибокі знання:	<ul style="list-style-type: none"> знання стандартів кібербезпеки та приватності, засад, політик, положень, законодавства, сертифікацій та найкращих практик; розуміння етичних вимог організації кібербезпеки; знання засобів контролю безпеки; знання моделей зрілості кібербезпеки; знання тактик, прийомів та процедур кібербезпеки; знання методів/принципів управління ресурсами; знання практик управління; знання засад управління ризиками; 	
е-компетенції (з Системи е-компетенцій e-CF) <i>сайт e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer</i>	<ul style="list-style-type: none"> розроблення стратегії інформаційної безпеки; управління ризиками; управління взаємовідносинами; управління інформаційною безпекою; управління ІБ 	Кваліфікація Рівень 5 Рівень 4 Рівень 3 Рівень 4 Рівень 4

Мету діяльності за професією для національного ПК сформовано у відповідності до інтегрованих завдань фахівця, опису місії і резюме за Європейською рамкою ECSF.

Розглянемо як приклад національний ПС. Мета діяльності за професією.

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

Управління впровадженням стратегії, політик та системи менеджменту інформаційної безпеки та/або кібербезпеки організації в цілому. Планування та керування розподілом відповідних інформаційних ресурсів, заходами з нейтралізації наслідків кіберінцидентів щодо порушень функціонування встановлених бізнес-операційних процесів та сталого функціонування інформаційних систем/мереж та/або інфраструктури організації в цілому (зокрема критичної інформаційної інфраструктури). Забезпечення обміну інформацією у сфері кібербезпеки та захисту інформації із зовнішніми зацікавленими сторонами.

Назва професії та код підкласу професії згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій» віднесено до розділу Керівників за кодом – 1239.

Професійну кваліфікацію (кваліфікації) та її рівень визначено у відповідності до рекомендацій НАК згідно з Національною рамкою кваліфікацій (НРК), а саме : «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту» – 7 магістерський рівень НРК.

Висновок

Опрацьовано сучасні методи та моделі формування контенту професійних стандартів в галузі кібербезпеки на основі моделей та методик опису знань, вмінь, навичок та рівнів дескрипторів Європейської рамки навичок з кібербезпеки. Досліджено процеси і методи імплементації, які проводились в рамках вимог Національної рамки кваліфікації України.

Також, сформовано базові компоненти контенту професійного стандарту «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту» на основі розроблених та впроваджених моделей. Авторами визначено ключові етапи та методи імплементації, які ґрунтуються на Європейській рамці навичок з кібербезпеки.

Проаналізовано внесок Європейської рамки навичок з кібербезпеки в процес створення професійних стандартів, що дозволяє врахувати найновіші тенденції та вимоги в цьому сегменті, що стрімко розвивається в нашій країні. Важливо відзначити, що зосередження на конкретних навичках та компетентностях, визначених рамкою,

дозволяє не лише створити ефективний професійний стандарт, адаптований до сектору індустрії, але й сформувані передумови подальшої імплементації професійних стандартів до освітніх процесів підготовки кваліфікованих фахівців у сфері кіберзахисту [12, 13].

ЛІТЕРАТУРА

- [1] European Cybersecurity Skills Framework (ECSF), <https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework> (access data 21.03.2024).
- [2] ESCO The European multilingual classification of Skills, Competences and Occupations, <http://www.es.europa.eu/esco> (access data 21.03.2024).
- [3] ENISA Mandate, Regulation (EU) 2019/881, <https://eur-lex.europa.eu/eli/reg/2019/881/oj> (access data 21.03.2024).
- [4] Ковалюк Т. В. Узгодження вимог професійних та освітніх ІТ-стандартів до компетентностей випускників ІТ-спеціальностей ВНЗ. *Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі.* 2017. № 872. С. 229–240.
- [5] Кристопчук Т. Стандарти професійної підготовки фахівців у країнах Європейського Союзу та в Україні: порівняльний аналіз. *Неперервна професійна освіта: теорія і практика.* 2019. № 2 (59). С. 63–67. doi: 10.28925/1609-8595.2019.2.6367.
- [6] European Qualifications Framework (EQF). URL: https://www.ehea.info/Upload/TPG_A_QF_RO_MK_1_EQF_Brochure.pdf (access data 21.03.2024).
- [7] National Initiative for Cybersecurity Education (2020) NICE Framework Resource Center. URL: <https://www.nist.gov/nice/framework> (access data 21.03.2024).
- [8] European ICT Professional Role Profiles, CWA 16458 EN 16234-1:2019 e-Competence Framework (e-CF), A common European Framework for ICT Professionals in all sectors.
- [9] CEN/TS 17699:2022 Guidelines for developing ICT Professional Curricula as scoped by EN 16234-1 (e-CF).
- [10] CEN/TS 17834:2022 European Professional Ethics Framework for the ICT Profession (EU ICT Ethics).
- [11] Національна рамка кваліфікацій – Україна, URL: https://www.etf.europa.eu/sites/default/files/2021-11/ukraine_ua.pdf (access data 21.03.2024).
- [12] Юдін О. К., Матвійчук-Юдіна О. В. Концепція формування професійних компетентностей фахівців з інформаційних технологій та кібербезпеки. *Наукоємні технології.* 2019. № 3. С. 330–342.
- [13] Спірін О. М., Юдін О. К. Концептуальні питання професійної сертифікації фахівців з інформаційної та кібербезпеки в Україні. *Актуа-*

льні проблеми управління інформаційною безпекою держави. 2018. С. 156–158.

[14] Competency Model Clearinghouse, Cybersecurity Competency Model, <https://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx> (access data 21.03.2024).

[15] Юдін О. К. Концептуальні питання створення національної рамки кваліфікацій з кібербезпеки в Україні. Збірка тез доповідей Міжвідомчої науково-практичної конференції «Посилення спроможностей сектору безпеки і оборони» (12 жовтня 2023 року), м. Київ, Україна. 2023. Київ: НА СБУ. С. 11–14.

**Юдін О. К., Юдін О. Ю., Черниш Л. Г., Телющенко В. А.
МЕТОДИ ІМПЛЕМЕНТАЦІЇ ЄВРОПЕЙСЬКОЇ РАМКИ НАВИЧОК З КІБЕРБЕЗПЕКИ ПРИ
ФОРМУВАННІ КОНТЕНТУ ПРОФЕСІЙНОГО СТАНДАРТУ «КЕРІВНИК
СТРУКТУРНОГО ПІДРОЗДІЛУ З ПИТАНЬ БЕЗПЕКИ ІНФОРМАЦІЇ ТА КІБЕРЗАХИСТУ»**

В роботі проведено аналіз існуючих методів та кращих світових практик щодо створення системи професійної стандартизації у сфері кібербезпеки та захисту інформації.

Показано, що даний час, сформовано новий Перелік професій у відповідності до потреб ринку праці у сфері кібербезпеки та захисту інформації. Уперше, за багато років, за ініціативою комплексної групи фахівців при Держспецзв'язку були внесені зміни та додані нові професії до класифікатора професій ДК – 003:2010 в сфері кібербезпеки та захисту інформації (Зміни #10, Наказ Мінекономіки від 25.10.21 №810; Зміни #11 Наказ Мінекономіки № 5573 від 29.12.22). Згідно внесених Змін на 2024р., загальна кількість професій з напрямку кібербезпеки в Україні складає – 27 професій та 46 кваліфікацій.

Згідно з «Класифікатором професій» ДК 003:2010 та у відповідності до кращих світових практик, зазначений перелік професій був сформований на базі імплементації кращих світових професійних стандартів, а саме з урахуванням Європейської рамки навичок з кібербезпеки, European Cybersecurity Skills Framework (ECSF ENISA, ECSF role profile).

Також, в роботі надано концептуальні та методичні рекомендації формування базової моделі контенту професійних стандартів, а саме створення контенту компетентностей, знань, вмінь та навичок професійного стандарту «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту». Представлений матеріал розглядається з метою здійснення аналізу та надання практичних рекомендацій з методів і процедур імплементації та розроблення (адаптації до вітчизняних вимог) професійних стандартів (далі – ПС) і відповідних їм кваліфікацій згідно з затвердженими Змінами до Національного класифікатора професій «Класифікатор професій» ДК 003:2010 (Зміни № 10, Наказ Мінекономіки від 25.10.2021 № 810; Зміни № 11, Наказ Мінекономіки № 5573 від 29.12.2022). У поданому матеріалі представлений приклад відповідно до European Cybersecurity Skills Framework (ECSF) та згідно з «Класифікатором професій» ДК 003:2010 і Національною рамкою кваліфікацій України.

Ключові слова: рамка кваліфікацій; класифікатор професій; кібербезпека та захист інформації; професійні стандарти; кваліфікації; дескриптори.

**Yudin O. K., Yudin O. Y., Chernysh L., Telyushchenko V.
METHODS OF IMPLEMENTATION OF THE EUROPEAN CYBERSECURITY SKILLS
FRAMEWORK IN THE FORMATION OF THE CONTENT OF THE PROFESSIONAL
STANDARD "HEAD OF THE STRUCTURAL UNIT FOR INFORMATION SECURITY
AND CYBER DEFENCE"**

The paper analyses the existing methods and best international practices for creating a system of professional standardisation in the field of cybersecurity and information protection.

It is shown that at present, a new List of professions has been formed in accordance with the needs of the labour market in the field of cybersecurity and information protection. For the first time in many years, on the initiative of a comprehensive group of specialists at the State Special Communications Service of Ukraine, changes were made and new professions were added to the classifier of professions DK - 003: 2010 in the field of cybersecurity and information protection (Amendments #10, Order of the Ministry of Economy No. 810 dated 25.10.21; Amendments #11, Order of the Ministry of Economy No. 5573 dated 29.12.22). According to the Amendments for 2024, the total number of cybersecurity professions in Ukraine is 27 professions and 46 qualifications.

According to the "Classifier of Occupations" DK 003:2010 and in accordance with the best international practices, the said list of occupations was formed on the basis of the implementation of the best international professional standards, namely, taking into account the European Cybersecurity Skills Framework (ECSF ENISA, ECSF role profile).

Also, the paper provides conceptual and methodological recommendations for the formation of a basic model of the content of professional standards, namely, the creation of the content of competencies, knowledge, skills and abilities of

the professional standard "Head of a structural unit for information security and cyber defence". The material presented is considered with the aim of analysing and providing practical recommendations on methods and procedures for the implementation and development (adaptation to national requirements) of professional standards (hereinafter referred to as PS) and their corresponding qualifications in accordance with the approved Amendments to the National Classifier of Occupations "Classifier of Occupations" DK 003:2010 (Amendments No. 10, Order of the Ministry of Economy No. 810 of 25.10.2021; Amendments No. 11, Order of the Ministry of Economy No. 5573 of 29.12.2022). This material presents an example in accordance with the European Cybersecurity Skills Framework (ECSF) and in accordance with the Classifier of Occupations DK 003:2010 and the National Qualifications Framework of Ukraine.

Keywords: qualifications framework; cybersecurity and information protection; professional standards; qualifications; descriptors.

Стаття надійшла до редакції 25.03.2024 р.
Прийнято до друку 12.06.2024 р.