Прим. № __

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної
служби спеціального зв'язку
та захисту інформації України
23 січня 2024 року № 38

ПРОФЕСІЙНИЙ СТАНДАРТ

КОНСТРУКТОР СИСТЕМ КІБЕРБЕЗПЕКИ

_____

(дата внесення до Реєстру кваліфікацій)

Професійний стандарт розроблено та затверджено згідно з вимогами статті 4^2 Кодексу законів про працю України на підставі:

висновку суб'єкта перевірки – Національного агентства кваліфікацій від 20 грудня 2023 року про дотримання під час підготовки проєкту професійного стандарту вимог Порядку розроблення, введення в дію та перегляду професійних стандартів, затвердженого постановою Кабінету Міністрів України від 31.05.2017 р. № 373;

висновку Профспілки працівників зв'язку України щодо погодження проєкту професійного стандарту «Конструктор систем кібербезпеки» (лист від 16 листопада 2023 року № 01.2-14/136, Постанова Президії Профспілки працівників зв'язку України від 16 листопада 2023 року № П-4-5г).

І. Назва професійного стандарту

Конструктор систем кібербезпеки

ІІ. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Забезпечення ситуації, коли вимоги безпеки зацікавлених сторін, необхідні для захисту місії організації та бізнес-процесів, належним чином ураховуються в усіх аспектах архітектури систем кібербезпеки організації (установи, підприємства), включаючи еталонні моделі, архітектури сегментів та рішень, а також системи для підтримки цих місій та бізнес-процесів.

2. Назва виду (видів) економічної діяльності, секції, розділу, групи, класу економічної діяльності та їх код згідно з Національним класифікатором України ДК 009:2010 «Класифікація видів економічної діяльності»

Секція J	Інформація та телекомунікації	**Розділ 61**	Телекомунікації (електрозв'язок)	**Група 61.1**	Діяльність у сфері проводового електрозв'язку
				Клас 61.10	Діяльність у сфері проводового електрозв'язку
				Група 61.2	Діяльність у сфері безпроводового електрозв'язку
				Клас 61.20	Діяльність у сфері безпроводового електрозв'язку
				Група 61.3	Діяльність у сфері супутникового електрозв'язку
				Клас 61.30	Діяльність у сфері супутникового електрозв'язку
				Група 61.9	Інша діяльність у сфері електрозв'язку
				Клас 61.90	Інша діяльність у сфері електрозв'язку
		Розділ 62	Комп'ютерне програмування, консультування та пов'язана з ними діяльність	**Група 62.0**	Комп'ютерне програмування, консультування та пов'язана з ними діяльність
				Клас 62.01	Комп'ютерне програмування
				Клас 62.02	Консультування з питань інформатизації
				Клас 62.03	Діяльність із керування комп'ютерним устаткуванням
				Клас 62.09	Інша діяльність у сфері інформаційних технологій і комп'ютерних систем

		Розділ 63	Надання інформаційних послуг	**Група 63.1**	Оброблення даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність; веб-портали
				Клас 63.11	Оброблення даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність
				Клас 63.12	Веб-портали
Секція M	Професійна, наукова та технічна діяльність	**Розділ 74**	Інша професійна, наукова та технічна діяльність	**Група 74.9**	Інша професійна, наукова та технічна діяльність, не введенні в інші угрупування
				Клас 74.90	Інша професійна, наукова та технічна діяльність, не введенні в інші угрупування
Секція P	Освіта	**Розділ 85**	Освіта	**Група 85.5**	Інші види освіти
				Клас 85.59	Інші види освіти, не введенні в інші угрупування

3. Назва (назви) професії (професій) та код (коди) підкласу (підкласів) (групи) професії згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій»

Конструктор систем кібербезпеки 2132.2

4. Професійна (професійні) кваліфікація (кваліфікації), її (їх) рівень згідно з Національною рамкою кваліфікацій

Конструктор систем кібербезпеки, 7 рівень НРК

Провідний конструктор систем кібербезпеки, 7 рівень НРК

5. Назва (назви) документа (документів), що підтверджує (підтверджують) професійну кваліфікацію особи

● документ (диплом, сертифікат, тощо), виданий суб’єктом, уповноваженим законодавством на присвоєння/підтвердження та визнання професійної або часткової професійної кваліфікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у відповідності до професійного стандарту «Конструктор систем кібербезпеки»;

● документ (диплом, сертифікат, тощо), виданий суб’єктом, уповноваженим законодавством на присвоєння/підтвердження та визнання професійної або часткової професійної кваліфікації (щодо професійних кваліфікацій, здобутих у інших країнах).

ІІІ. Здобуття професійної кваліфікації та професійний розвиток

1. Здобуття професійної кваліфікації (назва професійної та/або часткової професійної кваліфікації; суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій)

Назва професійної та/або часткової професійної кваліфікації	**Суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
Конструктор систем кібербезпеки	Підготовка за спеціальностями, вказаними у **П.*** на другому (магістерському) рівні вищої освіти або на першому (бакалаврському) рівні вищої освіти за умови наявності стажу роботи за однією з професій відповідного спрямування не менше 2 років.	*не передбачено професійним стандартом*
Провідний конструктор систем кібербезпеки	Підготовка за спеціальностями, вказаними у **П.*** на другому (магістерському) рівні вищої освіти за умови наявності стажу роботи за однією з професій відповідного спрямування не менше 2 років або на першому (бакалаврському) рівні вищої освіти за умови наявності стажу роботи за однією з професій відповідного спрямування не менше 4 років.	*не передбачено професійним стандартом*

П.*

● диплом на першому (бакалаврському) або диплом на другому (магістерському) рівні вищої освіти за спеціальністю:

- 121 «Інженерія програмного забезпечення» галузі знань «Інформаційні технології» (6 або 7 рівень НРК);
- 122 «Комп'ютерні науки» галузі знань «Інформаційні технології» (6 або 7 рівень НРК);
- 123 «Комп'ютерна інженерія» галузі знань «Інформаційні технології» (6 або 7 рівень НРК);
- 124 «Системний аналіз» галузі знань «Інформаційні технології» (6 або 7 рівень НРК);

- 125 «Кібербезпека та захист інформації» галузі знань «Інформаційні технології» (6 або 7 рівень НРК);
- 126 «Інформаційні системи та технології» галузі знань «Інформаційні технології» (6 або 7 рівень НРК);
- 172 «Електронні комунікації та радіотехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (6 або 7 рівень НРК);
- 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (6 або 7 рівень НРК);
- 253 «Військове управління (за видами збройних сил)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону" (6 або 7 рівень НРК);
- 254 «Забезпечення військ (сил)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (6 або 7 рівень НРК);
- 255 «Озброєння та військова техніка» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (6 або 7 рівень НРК);
- 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (6 або 7 рівень НРК).

2. Професійний розвиток

1) з присвоєнням наступної професійної кваліфікації

Назва професійної та/або часткової професійної кваліфікації	**Суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій**	
	Кваліфікаційні Центри	**Суб'єкти освітньої діяльності**
Конструктор систем кібербезпеки	Підвищення кваліфікації для конструктора систем кібербезпеки для отримання професійної кваліфікації "провідний конструктор систем кібербезпеки". Стаж роботи не менше двох років	*не передбачено професійним стандартом*

2) без присвоєння наступної професійної кваліфікації

Підвищення кваліфікації може здійснюватися шляхом неформальної (тренінги, семінари, семінари-практикуми, вебінар, майстер-класи тощо) та інформальної освіти для вдосконалення (підтримання) професійної кваліфікації, в тому числі шляхом набуття нових/додаткових навичок/компетентностей.

Підтвердження наявної та підвищення професійної кваліфікації може бути передбачено відповідними відомчими нормативно-правовими актами та внутрішніми документами підприємств, установ та організацій.

IV. Абревіатури, скорочення

ІТ	інформаційні технології
ІКТ	інформаційно-комунікаційні технології
СК	системи кібербезпеки
ПЗ	програмне забезпечення
ОС	операційна система
DNS	система доменних імен
LAN	внутрішня локальна мережа
PKI	інфраструктура відкритих ключів
TCP/IP	Transmission Control Protocol / Internet Protocol

V. Опис трудових функцій

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
А. Визначення та документальне оформлення вимог до проєктів/ моделей СК з врахуванням наявних спроможностей та потреб організації	**А1.** Здатність перетворювати запропоновані спроможності в технічні вимоги.	**А1.З1.** Принципи кібербезпеки і приватності. **А1.З2.** Закони, нормативні акти, політики і етичні норми, і як вони пов'язані з кібербезпекою і приватністю **А1.З3.** Програми класифікації інформації і процедур розкриття, використовувану в організації (установі, підприємстві) **А1.З4.** Спроможності та прикладні програми мережевого обладнання, включаючи маршрутизатори, комутатори, мости, сервери, засоби передачі і відповідне технічне обладнання	**А1.У1.** Визначати та пріоритезувати суттєві спроможності систем або бізнес-функцій, необхідних для часткового або повного відновлення системи після її повної відмови **А1.У2.** Перекладати функціональні вимоги в потреби захисту (тобто, контролі безпеки) **А1.У3.** Застосовувати принципи кібербезпеки і приватності при формуванні вимог організації (стосовно конфіденційності, цілісності, доступності,	**А1.К1.** Забезпечувати вхідну інформацію стосовно вимог безпеки, які слід включити до звітів про роботу та інших відповідних документів про закупівлі **А1.К2.** Надавати вхідні дані для діяльності процесу загальних принципів управління ризиками та відповідну документацію (наприклад, плани забезпечення життєвого циклу системи, концепція операцій, операційні процедури і навчальні матеріали з технічного обслуговування)	**А1.В1**. Розробляти умови системи безпеки, попередню концепцію проведення операцій з кібербезпеки (CONOPS в абревіатури), і визначати основні вимоги системи безпеки відповідно до прийнятних вимог кібербезпеки

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		А1.З5. ПЗ з підтримкою кібербезпеки **А1.З6.** Багаторівневі типології (наприклад, включаючи ОС сервера і клієнта)	автентифікації і неспростовності)		
	А2. Здатність проектувати архітектури та загальні принципи	**А2.З1.** Прикладні бізнес-процеси і функції в організації–замовника **А2.З2.** Процеси проектування мереж, включаючи розуміння цілей системи безпеки, операційних цілей та компромісів **А2.З3.** Системи баз даних **А2.З4.** Електротехніку, яка використовується в архітектурі комп'ютера (наприклад, друковані плати, процесори, мікросхеми та технічне забезпечення) **А2.З5.** Мікропроцесори **А2.З6.** Обладнання та	**А2.У1.** Проектувати інтеграції апаратних і програмних рішень **А2.У2.** Застосовувати методи проектування **А2.У3.** Документувати та приводити у відповідність інформаційну безпеку організації, архітектуру кібербезпеки та вимоги техніки безпеки системи протягом всього життєвого циклу закупівлі	**А2.К1.** Ідентифікувати та надавати перевагу критичним бізнес-функціям у співпраці із заінтересованими сторонами організації	**А2.В1.** Писати детальні функціональні специфікації, які документують процес розробки архітектури

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		функції апаратного забезпечення мереж **А2.З7.** Операційні системи **А2.З8.** Концепції телекомунікацій (наприклад, комунікаційні канали, бюджетування системних каналів зв'язку, спектральна ефективність, мультиплексування) **А2.З9.** Різні типи комп'ютерних архітектур **А2.З10.** Теорію інформації (наприклад, кодування джерела, канальне кодування, теорія складності алгоритмів і стиснення даних) **А2.З11.** Мережеві протоколи, такі, як TCP/IP, динамічного конфігурування вузлів, системи доменних імен (DNS) і послуг, що	**А2.У4.** Застосовувати інструменти, методи і техніки проектування систем, включаючи інструменти автоматизованого аналізу та проектування систем **А2.У5.** Застосовувати процеси планування захисту програм (наприклад, політики безпеки ланцюжків постачання IT / політика управління ризиками, методи боротьби з підробками та вимоги) **А2.У6.** Застосовувати загальні мережеві протоколи та протоколи		

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		надаються Службою каталогів	маршрутизації (наприклад, TCP/IP), послуги (наприклад, веб-пошти, DNS) та їх взаємодії для забезпечення мережевих зв'язків		
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування.				
Б. Проведення аналізу та технічних розрахунків під час роботи з документацією із проєктування/моделювання систем кібербезпеки	**Б1**. Здатність аналізувати запропоновані архітектури, розподіляти послуги безпеки і обирати механізми безпеки	**Б1.З1**. Процеси управління ризиками (наприклад, методи оцінювання та зниження ризиків) **Б1.З2**. Методи автентифікації, авторизації та контролю доступу **Б1.З3**. Нові і виникаючі ІТ та технології кібербезпеки **Б1.З4**. Методи, принципи і концепції	**Б1.У1.** Застосовувати та інтегрувати ІТ до запропонованих рішень **Б1.У2.** Використовувати моделі систем безпеки (наприклад, модель Белла-Лападули, моделі забезпечення цілісності «Biba» і Кларка-Вілсона)	**Б1.К1.** Аналізувати потреби та вимоги користувачів для планування архітектури **Б1.К2.** Визначити відповідні рівні доступності системи на основі критичних функцій системи та переконатися, що системні вимоги визначають відповідні вимоги відновлення після	**Б1.В1.** Виконувати аналіз системи безпеки, визначати пробіли в архітектурі безпеки

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		комунікацій, які підтримують інфраструктуру мережі **Б1.З5**. Концепції криптографії та управління криптографічними ключами **Б1.З6**. Розділи математики (наприклад, логарифми, тригонометрію, лінійну алгебру, математичний аналіз, статистику і операційний аналіз) **Б1.З7.** Багаторівневі системи безпеки та рішення для захищеного інформаційного обміну між доменами **Б1.З8.** Алгоритми шифрування	**Б1.У3.** Визначати потреби у захисті (тобто, контролях безпеки) інформаційних систем та мережі, а також належним чином їх документувати **Б1.У4.** Використовувати пристрої віртуальних приватних мереж (VPN) і шифрування	аварії та безперервність операцій, включаючи будь-які відповідні вимоги щодо аварійного переходу /альтернативного сайту, вимоги до резервного копіювання та вимоги до забезпечення матеріальної підтримки для відновлення/ реставрації системи	
	Б2. Здатність оцінювати архітектури і проекти безпеки для визначення адекватності проекту та архітектури безпеки, які	**Б2.З1**. Аналіз спроможностей і вимог **Б2.З2.** Безперервність бізнесу та операційних планів відновлення	**Б2.У1.** Моделювати проекти і будувати сценарії їх використання (наприклад,	**Б2.К1**. Надавати консультації щодо витрат на проект, концепцій	**Б2.В1.** Визначати і документувати те, як впровадження нових систем або

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	були запропоновані або надані відповідно до вимог, що містяться в документах про придбання	безперервності після катастроф **Б2.З3.** Корпоративну архітектуру інформаційної безпеки організації **Б2.З4**. Методологію оцінки загальних принципів управління ризиками **Б2.З5**. Інтеграцію цілей і завдань організації в архітектуру **Б2.З6**. Вбудовані системи	універсальною мовою моделювання) **Б2.У2**. Документувати та оновлювати за необхідності усі напрямки діяльності, пов’язані із визначенням архітектури	проектування або змін в проекті	інтерфейсів між системами вплине на стан захищеності діючої інфраструктури
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп’ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування.				
В. Проведення робіт з розроблення та впровадження проєктів/ моделей СК відповідно до	**В1**. Здатність розробляти компоненти архітектури або системних компонент підприємства, необхідні для задоволення потреб користувачів	**В1.З1**. Принципи і методи аналізу прийнятих в галузевих стандартах або в організації **В1.З2.** Основні концепції управління	**В1.У1.** Розробляти контрзаходи для виявлення ризиків безпеки **В1.У2.** Розробляти багаторівневі рішення безпеки/	**В1.К1.** Використовувати цілі і завдання організації при розробці і підтримці архітектури	**В1.В1.** Перевіряти, що придбані або розроблені система (и) та архітектура (и) відповідають

Трудові функції	Компетентності	Результати навчання			
		Знання	Уміння/навички	Комунікація	Відповідальність і автономія
стандартів, норм охорони праці та з врахуванням їх економічної доцільності		безпекою (наприклад, управління версіями, патч-менеджмент) **В1.З3.** Концепції і функції прикладних програм мережевих екранів (наприклад, єдиної точки автентифікації/аудиту/ реалізації політики, сканування повідомлень на наявність шкідливого вмісту, знеособлення даних з метою задоволення вимог стандартів PCI та DII, сканування захисту від втрати даних, прискорених криптографічних операцій, протокол захисту інформації SSL, REST/JSON-обробка) **В1.З4.** Критерії оцінки та підтвердження автентичності, прийнятих в організації	міждоменні рішення **В1.У3.** Застосовувати інструменти, методи і техніки розробки безпечних систем		настановам з архітектури кібербезпеки в організації

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		В1.35. Концепцію паралельних і розподілених обчислень **В1.36.** Концепцію технологій віддаленого доступу **В1.37.** Технологію побудови ПЗ			
	В2. Здатність впроваджувати СК із дотриманням принципів і методів кібербезпеки та приватності, а також організаційних вимог (щодо забезпечення конфіденційності, цілісності, доступності, автентифікації і неспростовності)	**В2.31.** Стандарти безпеки персональних ідентифікаційних даних **В2.32.** Стандарти безпеки даних в сфері платіжних карт **В2.33.** Стандарти безпеки медичних персональних даних **В2.34.** Концепції і протоколи комп'ютерних мереж, а також методологію забезпечення мережевої безпеки **В2.35.** Принципи взаємодії людина-комп'ютер	**В2.У1.** Визначати, як буде функціонувати система безпеки (включаючи її властивості відмовостійкості і надійності), та як зміни умов, операцій або середовища вплинуть на ці результати **В2.У2.** Налаштовувати та використовувати компоненти захисту комп'ютера (наприклад, апаратних	**В2.К1.** Налаштовувати фізичну або логічну підмережу, що відокремлює внутрішню локальну мережу (LAN) від інших ненадійних мереж	**В2.В1.** Розробляти/ інтегрувати проекти з кібербезпеки для систем та мереж із багаторівневими вимогами безпеки або вимогами для обробки кількох рівнів класифікації даних, що застосовуються головним чином до державних організацій (наприклад, некваліфіковані,

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		В2.З6. Вимоги до конфіденційності, цілісності та доступності	брандмауерів, серверів, маршрутизаторів, у відповідних випадках) **В2.У3.** Створювати фізичні або логічні підмережі, які відокремлюють LAN від інших ненадійних мереж		таємні та особливої важливості
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				
Г. Проведення робіт з випробування, експлуатації, удосконалення, модернізації та уніфікації конструйованих СК	**Г1.** Здатність організовувати процеси оцінки стану безпеки і процеси авторизації	**Г1.З1.** Методи тестування та оцінки систем **Г1.З2.** Оцінку систем кіберзахисту і вразливостей, а також їх можливостей **Г1.З3.** Кіберзагрози та вразливості **Г1.З4.** Вразливості прикладних приграм	**Г1.У1**. Застосовувати принципи кібербезпеки і приватності при формуванні організаційних вимог (які стосуються конфіденційності, цілісності, доступності,	**Г1.К1.** Застосовувати методи, стандарти та методики для опису, аналізу та документування архітектури корпоративної інформаційної технології організації (наприклад, The	**Г1.В1.** Застосовувати концепції архітектури безпеки мереж, включаючи топологію, протоколи, компоненти і принципи (наприклад, застосунки з

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		Г1.З5. Методи автентифікації доступу **Г2.З6.** Конкретні операційні наслідки в результаті помилок кібербезпеки	автентифікації і неспростовності) **Г1.У2**. Проводити процедури сканування вразливостей і розпізнавання вразливостей в системах безпеки **Г1.У3**. Готувати плани проведення тестування	Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Framework Architecture Framework [FEAF])	«ешелонованим захистом)
	Г2. Здатність застосовувати сучасні принципи, моделі, інструменти та методи управління системами	**Г2.З1.** Теорію управління потоками в мережах (наприклад, протоколу управління передачею (TCP), протоколу міжмережевого обміну даними (IP), моделі взаємодії відкритих систем (OSI), бібліотеки інфраструктури інформаційних технологій, поточної версії [ITIL]) **Г2.З2.** Управління мережевим доступом,	**Г2.У1.** Налаштовувати і використовувати ПЗ захисту комп'ютерів (наприклад, програмні фільтри, антивірусна програма й антишпигунське ПЗ) **Г2.У2.** Використовувати шифрування PKI та можливості цифрового підпису в програмних додатках	**Г2.К1.** Слугувати основною сполучною ланкою між архітектором підприємства та інженером систем безпеки та співпрацювати з власниками систем, постачальниками загальних контролів та працівниками системи безпеки щодо розподілу контролів безпеки на системні, гібридні або загальні контролі	**Г2.В1.** Застосовувати процеси управління безпечною конфігурацією

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		ідентифікацією, та доступом (наприклад, PKI, автентифікація об'єктів, відкриті ідентифікатори, мова розмітки для контролю захищеності, мова розмітки для надання послуг) **Г2.З3**. Концепції управління послугами для мереж і відповідні стандарти (наприклад, бібліотека інфраструктури інформаційних технологій [ITIL], поточна версія) **Г2.З4.** Методики управління конфігураціями **Г2.З5.** Демілітаризовані зони **Г2.З6.** Технологічні процеси систем	(наприклад, ел.пошта S/MIME, SSL-трафік)	**Г2.К2.** Оцінювати і проектувати функції управління безпекою, пов'язані з кіберпростором	
	Г3. Здатність проводити оптимізацію системи відповідно до вимог	**Г3.З1.** Системи критичної інфраструктури з ІКТ, які були розроблені без	**Г3.У1.** Застосовувати концепції вдосконалення	**Г3.К1.** Виявляти проблеми кібербезпеки і приватності, які	**Г3.В1.** Виявляти системи критичної інфраструктури з

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	продуктивності підприємства	розгляду безпеки системи **ГЗ.З2.** Процедури інсталяції, інтеграції та оптимізації компонентів системи **ГЗ.З3.** Концепції і моделі ІТ архітектури підприємства (наприклад, базовий рівень, затверджений дизайн, цільові архітектури) **ГЗ.З4.** Методологію відмовостійкості систем **ГЗ.З5.** Процеси інтеграції технологій **ГЗ.З6.** Комп'ютерні алгоритми	процесів організації та моделей зрілості процесів (наприклад, і Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions)	виникають при з'єднаннях внутрішніх та зовнішніх замовників та організацій-партнерів	ІКТ, які були спроектовані без урахування безпеки системи
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів відповідно до профілю конструювання; бібліотечні ресурси, архівні матеріали (за потреби); законодавчо-нормативні акти, акти роботодавця відповідного спрямування				
Д. Координація діяльності з розроблення СК	**Д1**. Здатність здійснювати технічне керівництво профільними працівниками,	**Д1.З1**. Керівництва / настанови, інструкції та/чи інші нормативні акти роботодавця, які	**Д1.У1**. Брати участь у координації комплексу робіт із своєчасної та	**Д1.К1**. Готувати та проводити брифінги відповідного спрямування	**Д1.В1.** Розробляти стратегії мінімізації

Трудові функції	Компетентності	Результати навчання			
		Знання	Уміння/навички	Комунікація	Відповідальність і автономія
	задіяними в конструкторській діяльності	застосовуються для організації та координації діяльності з розроблення СК **Д1.З2**. Посадові інструкції на посади розробників СК **Д1.З3**. Основи управління персоналом	якісної підготовки розроблення СК **Д1.У2.** Готувати службові записки та іншу документацію, необхідну для навчання / підвищення кваліфікації підпорядкованих розробників СК відповідного структурного підрозділу підприємства / організації	**Д1.К2**. Комунікувати з керівниками різних рівнів (міжособистісне спілкування, доступність, уміння ефективно сприймати мову виступаючих, відповідно до аудиторії коректувати стиль і мову виступу) **Д1.К3.** Розповсюджувати серед профільних працівників структурного підрозділу**,** керівництва та партнерів останні вітчизняні, зарубіжні та міжнародні досягнення щодо розроблення та застосування стандартів і процедур	ризиків для зменшення витрат, графіку, продуктивності і ризиків безпеки

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
				відповідного спрямування	
	Д2. Здатність взаємодіяти з керівництвом та іншими підрозділами підприємства / організації стосовно технологічних питань відповідного спрямування	**Д2.З1.** Структуру, розподіл функцій між керівниками, підпорядкованість підрозділів підприємства/ організації тощо **Д2.З2**. Положення про структурні підрозділи підприємства/ організації, задіяні в спільному виконанні технологічних та інших функціональних завдань **Д2.З3**. Нормативні акти роботодавця з питань взаємодії з керівництвом, технологічними та іншими підрозділами підприємства/ організації	**Д2.У1.** Узгоджувати повідомлення із заінтересованими структурними підрозділами та відповідальними посадовими особами щодо змін проєктної документації з розроблення СК **Д2.У2**. Готувати іншу документацію, необхідну для забезпечення безперебійної роботи закріпленого структурного підрозділу/ групи / дільниці	**Д2.К1**. Консультувати, тісно співпрацюючи з працівниками системи безпеки, посадових осіб, директорів інформаційних технологій, директорів із інформаційної безпеки та відповідальної посадової особи з управління ризиками/виконав-чого ризику (функції) щодо питань безпеки (наприклад, встановлення периметру системи, оцінки ступеня слабкості та недоліків у системі, планів дій і контрольних точок,	**Д2.В1.** Розробляти посадові інструкції на посади розробників СК, керівництва, інструкції та інші нормативні акти роботодавця, які застосовуються для організації та координації діяльності з розроблення СК **Д2.В2.** Розробляти нормативні акти роботодавця з питань взаємодії з керівництвом та іншими підрозділами підприємства/ організації щодо розроблення СК

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
				підходів до виявлених вразливостей) **Д2.К2**. Готувати, обґрунтовувати та оприлюднювати пропозиції щодо покращення в структурному підрозділі / на підприємстві / в організації розроблення СК	
	Д3. Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень	**Д3.З1**. Основи комунікаційного менеджменту **Д3.З2**. Основи ділової етики **Д3.З3.** Порядок і типові вимоги до проведення ділових / комерційних перемовин **Д3.З4**. Порядок розроблення та виконання договірних робіт для зовнішніх партнерів	**Д3.У1**. Спілкуватися із зовнішніми партнерами стосовно питань розроблення систем кібербезпеки доступними засобами комунікації **Д3.У2**. Брати участь у ділових / комерційних перемовинах із зовнішніми партнерами	**Д3.К1**. Обґрунтовувати та оприлюднювати пропозиції щодо налагодження взаємодії із зовнішніми партнерами **Д3.К2**. Ефективно спілкуватися під час листування	**Д3.В1.** Дотримуватися порядку і типових вимог до проведення ділових / комерційних перемовин; розроблення та виконання договірних робіт для зовнішніх партнерів

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
			ДЗ.УЗ. Супроводжувати договірні роботи із зовнішніми партнерами		
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				

VI. Розподіл трудових функцій та компетентностей за професійними кваліфікаціями

Трудова функція (умовне позначення)	Загальна назва професійної кваліфікації у межах професійного стандарту: конструктор систем кібербезпеки	
	конструктор систем кібербезпеки	провідний конструктор систем кібербезпеки
	повна	повна
А	+	+
Б	+	+
В	+	+
Г	+	+
Д	-	+

VII. Відомості про розроблення та затвердження професійного стандарту

1. Повне найменування розробника професійного стандарту

Адміністрація Державної служби спеціального зв’язку та захисту інформації України.

Склад робочої групи/Учасники робочої групи:

Волкова Ксенія Миколаївна, заступник начальника управління правового співробітництва з міжнародними організаціями Департаменту міжнародного права Міністерства юстиції України;

Горбенко Іван Дмитрович, голова наглядової Ради, головний конструктор ПРАТ «Інститут інформаційних технологій»;

Дівіцький Андрій Сергійович, старший викладач Спеціальної кафедри Інституту спеціального зв’язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;

Дідик Валерія Анатоліївна, керівник напряму з розвитку професійних навичок з кібербезпеки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»;

Дирда Олександр Вікторович, заступник директора департаменту – начальник 4 управління Департаменту захисту інформації Адміністрації Держспецзв'язку;

Жилін Артем Вікторович, начальник 6 управління Державного центру кіберзахисту Держспецзв’язку;

Касаткін Дмитро Юрійович, завідувач кафедри комп'ютерних систем, мереж та кібербезпеки Національного університету біоресурсів і природокористування України;

Ковальчук Людмила Василівна, провідний науковий співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України;

Кожухівський Андрій Дмитрович, професор кафедри інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації Державного університету телекомунікацій;

Конюшок Сергій Миколайович, заступник начальника (з наукової роботи) Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;

Леонов Андрій Олегович, голова Громадської організації «Інститут стандартів та технологій»;

Лукова-Чуйко Наталія Вікторівна, завідувач кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка;

Мазур Наталя Володимирівна, голова Профспілки працівників зв'язку України;

Мельник Сергій Вікторович, консультант напряму з розвитку професійних навичок з кібербезпеки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»;

Одарченко Роман Сергійович, завідувач кафедри телекомунікаційних та радіоелектронних систем факультету аеронавігації, електроніки та телекомунікацій Національного авіаційного університету;

Олексюк Лілія Віталіївна, голова Громадської організації «Всеукраїнська асоціація «Інформаційна безпека та інформаційні технології»;

Охріменко Тетяна Олександрівна, заступник декана з наукової роботи факультету комп'ютерних наук та технологій Національного авіаційного університету;

Педченко Євгеній Миколайович, керівник відділу впровадження систем безпеки ТОВ «ІНТРАСИСТЕМС»;

Сторчак Антон Сергійович, доцент Спеціальної кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;

Четверіков Іван Олександрович, доцент кафедри кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України;

Юдін Олександр Костянтинович, учений секретар Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації.

2. Назва та реквізити документа, яким затверджено професійний стандарт

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23 січня 2024 року № 38.

3. Реквізити висновку суб'єкта перевірки про дотримання вимог Порядку розроблення, введення в дію та перегляду професійних стандартів під час підготовки проєкту професійного стандарту

Висновок суб'єкта перевірки Національного агентства кваліфікацій від 20 грудня 2023 року про дотримання під час підготовки проєкту професійного стандарту «Конструктор систем кібербезпеки» вимог Порядку розроблення, введення в дію та перегляду професійних стандартів, затвердженого постановою Кабінету Міністрів України від 31.05.2017 р. № 373).

4. Реквізити висновку репрезентативних всеукраїнських об'єднань професійних спілок на галузевому рівні про погодження проєкту професійного стандарту

Висновок Профспілки працівників зв'язку України щодо погодження проєкту професійного стандарту «Конструктор систем кібербезпеки» (лист від

16 листопада 2023 року № 01.2-14/136, Постанова Президії ЦК Профспілки працівників зв'язку України від 16 листопада 2023 року № П-4-5г).

VIII. Дата внесення професійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.

Заступник Голови Держспецзв'язку,
керівник комплексної робочої групи
з розробки професійних стандартів Олександр ПОТІЙ