Проєкт

Професійний стандарт

ФАХІВЕЦЬ ІЗ КІБЕРДОСЛІДЖЕНЬ ТА РОЗРОБОК СИСТЕМ БЕЗПЕКИ

_____(дата внесення до Реєстру кваліфікацій)

ЗАТВЕРДЖЕНО:

Адміністрацією Державної служби спеціального зв'язку та захисту інформації України наказ від _____№_____

Професійний стандарт розроблено та затверджено згідно з вимогами статті 42 Кодексу законів про працю України на підставі:

- висновку суб'єкта перевірки – Національного агентства кваліфікацій від _____ 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 від _____ щодо погодження проєкту професійного стандарту

І. Назва професійного стандарту

Фахівець із кібердосліджень та розробок систем безпеки

ІІ. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Дослідження інжинірингу програмного забезпечення та систем, а також програмних систем для розробки нових можливостей, забезпечуючи повне впровадження кібербезпеки. Проведення комплексного дослідження технологій для оцінки потенційних вразливостей в системах кіберпростору. Проєктування, розроблення, тестування та оцінювання безпеки інформаційної системи протягом всього життєвого циклу розробки систем

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 професії та код підкласу професії згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій»

Фахівець із кібердосліджень та розробок систем безпеки, 2139.2

4. Професійна кваліфікація, її рівень згідно з Національною рамкою кваліфікацій (НРК)

Фахівець із кібердосліджень та розробок систем безпеки, 7 рівень НРК

Провідний фахівець із кібердосліджень та розробок систем безпеки, 7 рівень НРК

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

- диплом на другому (магістерському) рівні вищої освіти за спеціальністю:

- 121 «Інженерія програмного забезпечення» галузі знань «Інформаційні технології» (7 рівень НРК);
- 122 «Комп'ютерні науки» галузі знань «Інформаційні технології» (7 рівень НРК);
- 123 «Комп'ютерна інженерія» галузі знань «Інформаційні технології» (7 рівень НРК);
- 124 «Системний аналіз» галузі знань «Інформаційні технології» (7 рівень НРК);
- 125 «Кібербезпека» галузі знань «Інформаційні технології» (7 рівень НРК);
- 126 «Інформаційні системи та технології» галузі знань «Інформаційні технології» (7 рівень НРК);
- 172 «Телекомунікації та радіотехніка» галузі знань 17 «Електроніка та телекомунікації» (7 рівень НРК);

- документ (диплом, сертифікат, тощо), щодо післядипломної освіти та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері кібердосліджень та розробок систем безпеки;
- документ (диплом, сертифікат, тощо), щодо післядипломної освіти та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань в рамках консультаційно-навчальної діяльності у сфері кібердосліджень та розробок систем безпеки;
- документ (диплом, сертифікат, тощо), щодо професійної сертифікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері кібердосліджень та розробок систем безпеки.

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**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
Фахівець із кібердосліджень та розробок систем безпеки, провідний фахівець із кібердосліджень та	Підготовка на другому рівні вищої освіти (магістерському) за спеціальностями вказаними у п.5, галузі знань 12 «Інформаційні технології» та 17 «Електроніка та	

розробок систем безпеки	телекомунікації», стаж роботи за однією з професій відповідного спрямування повинен складати не менше 2 років (аналітик з безпеки інформаційно-телекомунікаційних систем, фахівець з питань безпеки (інформаційно-комунікаційні технології), фахівець сфери захисту інформації тощо)	

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**
Фахівець із кібердосліджень та розробок систем безпеки	Підвищення кваліфікації фахівця із кібердосліджень та розробок систем безпеки для отримання професійної кваліфікації "провідний фахівець із кібердосліджень та розробок систем безпеки ". Стаж роботи не менше двох років на посадах: розробник систем захисту інформації, аналітик з безпеки інформаційно-телекомунікаційних систем, фахівець з питань безпеки (інформаційно-комунікаційні технології), фахівець сфери захисту інформації тощо	

IV. Абревіатури, скорочення

ІТ	інформаційні технології

V. Опис трудових функцій

Трудові функції	**Компетентності**	**Результати навчання**			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
А. Проведення кібердосліджень	**А1**. Здатність досліджувати сучасні технології щоб з розуміти можливості необхідної системи або мережі	**А1.З1.** Технологічні задачі і завдання управління та лідерства пов'язані з організаційними процесами, механізми вирішення проблем **А1.З2**. Концепції і протоколи комп'ютерних мереж, а також методологію забезпечення безпеки мереж (К0001) **А1.З3.** Методики управління ризиками (методи оцінювання та оброблення ризиків) (К0002) **А1.З4**. Закони, нормативні акти,	**А1.У1.** Освоювати досягнення у технологіях захисту інформації для забезпечення їх впровадження у відповідній організації **А1.У2.** Адаптувати технічну інформацію щодо кібердосліджень та їх результатів до рівня розуміння користувача/споживача/ замовника **А1.У3**. Здійснювати моніторинг змін у нормативно-правових	**А1.К1.** Адаптувати технічну інформацію для досліджень до рівня розуміння користувача/споживача / замовника	**А1.В1**. Інтерпретувати та застосовувати закони, нормативні акти, політики, стандарти чи процедури до конкретних питань (Т0131) **А1.В2**. Збирати точні та повні дані з джерел, які використовуються при кібердослідженнях

		політики і етичні норми, та як вони пов'язані з конфіденційністю персональних даних та кібербезпекою (К0003) **А1.З5**. Принципи забезпечення конфіденційності персональних даних та кібербезпеки (К0004) **А1.З6**. Методи автентифікації, авторизації та контролю доступу **А1.З7**. Технології віртуалізації, формування віртуальних машин та їх технічної підтримки **А1.З8**. Нові та ті, що розроблюються технології інформаційної та кібербезпеки (К0059) **А1.З9.** Зовнішні організації і наукові установи, діяльність яких спрямована на дослідження кіберпростору	документах відповідного спрямування **А1.У4.** Формувати й оновлювати базу знайдених матеріалів для подальшого її використання в роботі		

		А1.310. Технологічні вимоги до науково-технічної та іншої дослідницької документації відповідного спрямування **А1.311.** Технічні характеристики й економічні показники кращих вітчизняних і світових розробок із кіберзахисту **А1.312.** Передові світові технологічні тенденції виготовлення продукції у сфері кіберзахисту **А1.313**. Досвід передових вітчизняних і зарубіжних підприємств щодо конструювання кіберпродукції й застосування нових технологій її виробництва			

	А2. Здатність переглядати та затверджувати програми, процеси і вимоги щодо збору та зберігання даних	**А2.З1.** Принципи управління життєвим циклом системи, включаючи забезпечення безпеки та експлуатаційної придатності програмного забезпечення (К0090) **А2.З2**. Методики управління ризиками в ланцюжку постачання (К0126) **А2.З3**. Політики, вимоги і процедури безпеки ланцюжка постачання інформаційних технологій та управління ризиками ланцюжка постачання (К0169) **А2.З4** Методики зворотного інжинірингу технічного обладнання (К0171) **А2.З5** Проміжне програмне забезпечення (шини обслуговування організації і черги	**А2.У1.** Проводити оцінювання ефективності існуючих програм, процесів і вимог щодо збору та зберігання даних **А2.У2**. Здійснювати комплексний аналіз відповідності змісту програм, процесів і вимог щодо збору та зберігання даних встановленим стандартам та регламентам **А2.У3**. Читати й аналізувати схеми й креслення, конструкторську, технологічну та іншу документацію відповідного спрямування **А2.У4.** Працювати з електронними архівами стандартів і технічних умов, які використовуються під час проєктування кіберпродукції	**А2.К1.** Формувати запити на профільну інформацію (Т0707)	**А2.В1.** Виконувати розрахунки технічних, техніко-економічних і функціонально-вартісних показників кіберпродукції, що проєктується

		повідомлень тощо) (К0172) **А2.З6** Мережеві протоколи (К0174) **А2.З7** Методики зворотного інжинірингу програмного забезпечення (К0175) **А2.З8** Схеми розширеної мови розмітки (XML) (К0176) **А2.У9**. Стандарти й технічні умови, використовуються під час проєктування кіберпродукції			
	А3. Здатність визначати стратегії кіберможливостей для розробки програмно-апаратних комплексів	**А3.З1.** Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи (прикладна система ешелонованого захисту тощо) **А3.З2.** Закони, політики, процедури чи корпоративне	**А3.У1.** Надавати визначення та здійснювати опис експериментальних методів дослідження структурних, фізико-механічних і технологічних властивостей матеріалів та	**А3.К1.** Надавати рекомендації щодо структур даних і баз даних з гарантованого забезпечення підготовки коректних і якісних звітних документів (Т0209)	**А3.В1.** Надавати рекомендації щодо нових технологій і архітектур баз даних (Т0210)

		управління, що стосуються кібербезпеки критичних інфраструктур (К0267) **А3.З3.** Архітектуру систем мобільного зв'язку (К0269) **А3.З3.** Структуру та властивості операційної системи (управління процесами, структура каталогів, встановлених застосунків тощо) (К0271) **А3З4.** Експериментальні методології розроблення кіберпродуктів **А3З5.** Основні проблеми й методи **А3З6.** Основні аспекти проєктування кіберпродукції **А3З7.** Методи та ризики, пов'язані з вибором компонентів кіберпродукції	компонентів кіберпродукції **А3.У2.** Визначати стратегії кіберможливостей для розробки програмно-апаратних комплексів для замовника, ґрунтуючись на вимогах місії **А3.У3.** Застосовувати сучасні методи проєктування, конструювання й виробництва кіберпродукції та/чи її компонентів	**А3.К2.** Пояснювати послідовність проєктування, виробництва, випробування та/або сертифікації кіберпродукції та/чи її компонентів **А3.К3.** Пояснювати особливості конструкції та основні аспекти робочих процесів компонентах нових продуктів з кіберзахисту	

	А4. Здатність оцінювати вразливості мережевої інфраструктури, щоб поширити можливості, які розроблюються	**А4.З1.** Класифікацію вразливостей прикладних програм (К0009) **А4.З2**. Кіберзагрози та вразливості (К0005) **А4.З3**. Основні операційні наслідки інцидентів кібербезпеки (К0006) **А4.З4** Системи критичної інфраструктури з інформаційно-комунікаційними технологіями, які були розроблені без розгляду безпеки системи (К0170) **А4.З5.** Криміналістичну процедуру ідентифікації слідів (К0268) **А4.З6.** Інструменти аналізу мереж для виявлення вразливостей у програмному забезпеченні, яке здійснює комунікацію (К0272)	**А4.У1.** Оцінювати вразливості мережевої інфраструктури **А4.У2**. Ураховувати у дослідницькій та проєктній діяльності виявлені вразливості мережевої інфраструктури	**А4.К1.** Проводити моніторинг зауважень, скарг, прокламацій та пропозицій партнерів та користувачів нової кіберпродукції щодо оцінювання наявних вразливості мережевої інфраструктури **А4.К2.** Доповідати безпосередньому керівництву результати моніторингових досліджень щодо наявних вразливості мережевої інфраструктури, готувати пропозиції стосовно їх урахування у дослідницькій та проєктній діяльності	**А4.В1.** Досліджувати і оцінювати наявні технології і стандарти розроблення нової кіберпродукції **А3.В1.** Надавати рекомендації щодо нових технологій і архітектур баз даних (Т0210)

		А4.37. Концепції криптографії та управління криптографічними ключами (К0019) **А4.38.** Концепції і функції прикладних програм мережевих екранів (єдина точка 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 тощо) (К0202) **А4.39.** Методики організації прихованих каналів зв'язку (К0209) **А4.310.** Стандартні галузеві моделі захисту			

	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 кібердосліджень; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції з проведення кібердосліджень				
Б. Проєктування і розроблення нових інструментів/ технологій, стосуються кібербезпеки	**Б1**. Здатність співпрацювати із зацікавленими сторонами для визначення та розроблення відповідної технології рішень	**Б1.З1.** Технології виробництва, комунікації та розповсюдження медійних повідомлень, а також альтернативні способи інформування за допомогою текстових, мовних, візуальних повідомлень **Б1.З2**. Відповідні концепції, процедури, програмне забезпечення, обладнання і прикладні технологічні програми які застосовуються для співпраці із зацікавленими сторонами **Б1.З3.** Методи і способи ефективної комунікації	**Б1.У1**. Розроблювати настанови стосовно впровадження розроблених систем клієнтам або командам впровадження	**Б1.К1.** Розроблювати вказівки і настанови для працівників, залучених до кібердосліджень **Б1.К2.** Комунікувати з керівниками організації різних рівнів, із представниками зацікавлених сторін стосовно організації, проведення та результатів кібердосліджень **Б1.К3.** Проводити робочі зустрічі з партнерами за всім спектром питань розроблення нових кіберпродуктів та проведення кібердосліджень **Б1.К4**. Здійснювати зворотній зв'язок з партнерами, підрядниками	**Б1.В1**. Розроблювати технічну документацію відповідного спрямування

		Б1.З4. Основні бізнес-процеси і місію організації		проєктних та науково-дослідних робіт з розроблення нової кіберпродукції	
	Б2. Здатність дотримуватися стандартів і процедур життєвого програмного забезпечення і інженерії систем	**Б2.З1.** Спроможності, прикладні програми і потенційні вразливості мережевого обладнання, включаючи концентратори, маршрутизатори, комутатори, мости, сервери, носії передачі і супутнє апаратне обладнання (К0296) **Б2.З2.** Стандарти розробки контрзаходів для виявлених ризиків безпеки (К0297) **Б2.З3.** Класифікацію контрзаходів щодо виявлених ризиків безпеки (К0298) **Б2.З4.** Процедуру функціонування системи безпеки (включаючи її можливості відмовостійкості та надійності), а також впливу на неї зміни	**Б2.У1.** Розроблювати і застосовувати в проєктуванні нових інструментів/ технологій, що стосуються кібербезпеки, математичні або статистичні моделі (S0017) **Б2.У2.** Використовувати наукові підходи і методики при вирішенні проблем у проєктуванні та розробленні нових інструментів/ технологій, що стосуються кібербезпеки (S0072) **Б2.У3**. Застосовувати процеси технічної розробки систем (S0140)	**Б2.К1.** Розповсюджувати серед профільних працівників структурного підрозділу, керівництва та партнерів останні вітчизняні, зарубіжні та міжнародні досягнення щодо розроблення та застосування стандартів і процедур відповідного спрямування	**Б2.В1.** Застосовувати у практичній діяльності стандарти і процедури життєвого циклу програмного забезпечення і інженерії систем

		умов, операцій та інфраструктури (К0299) **Б2.35.** Підходи щодо планування мережі і відтворення мереж (К0300)) **Б2.36**. Методи аналізу на пакетному рівні за допомогою відповідних інструментів (Wireshark, tcpdump) (К0301) **Б2.37.** Порядок оформлення технічного завдання на дослідницькі роботи з проєктування кіберпродукції			
	Б3. Здатність розроблювати зворотної інженерії для підвищення спроможностей і виявлення вразливостей	**Б3.31.** Номенклатуру інструментів для сегментування мереж (К0303) **Б3.32.** Технічну документацію відповідного спрямування **Б3.33**. Методологію зламу (К0310)	**Б3.У1.** Проєктувати інтеграцію технологічних процесів і рішень, включаючи застарілі системи і сучасні мови програмування (S0148) **Б3.У2.** Застосовувати та	**Б3.К1.** Ураховувати в обґрунтованому обсязі вимоги керівництва організації під час періодичного розгляду результатів кібердослід-	**Б3.В1**. Розроблювати технічну документацію відповідного спрямування

		Б3.34. Вимоги системи забезпечення якості **Б3.35.** Потенційні вразливості кібербезпеки в галузевих технологіях (К0314) **Б3.36.** Інженерні концепції, що застосовуються до комп'ютерної архітектури і відповідного комп'ютерного обладнання/програмного забезпечення (К0321) **Б3.37.** Принципи, інструменти та методики тестування на проникнення (К0342) **Б3.38**. Безпеку технолог операцій	інтегровувати інформаційні технології до запропонованих рішень (S0005) **Б3.У3.** Застосовувати безпечні методи кодування (S0148)	жень	
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням; приміщення і обладнання; профільна наукова та методична література				

В. Розроблення засобів та методів проведення кібердосліджень	**В1.** Здатність усувати проблеми, що виникають в процесі проєктування прототипів, а також на етапах проектування, розробки і перед запуском продукту	**В1.З1.** Класифікацію вразливостей при експлуатації систем безпеки **В1.З2**. Порядок усунення проблем при проєктуванні та усунення вразливостей при експлуатації систем безпеки **В1.З3.** Прототипи віртуальних машин (Microsoft Hyper-V, VMWare, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud) **В1.З4.** Програмні засоби захисту комп'ютерів (програмні фільтри, антивірусні програми й антишпигунське програмне забезпечення тощо) **В1.З5.** Компоненти системи мережевої безпеки (мережеві екрани, віртуальні приватні мережі, системи виявлення вторгнень тощо)	**В1.У1**. Усувати проблеми, що виникають в процесі проєктування прототипів, а також на етапах проектування, розробки і перед запуском продукту **В1.У2.** Використовувати у процесі проєктування прототипів віртуальні машини **В1.У3.** Налаштовувати і використовувати у процесі проєктування прототипів **В1.У4**. Конфігурувати і використовувати у процесі проєктування прототипів компоненти системи мережевої безпеки **В1.У5**. Використовувати	**В1.К1**. Надавати (доводити до відома) технічну інформацію різним категоріям користувачів **В1.К2.** Встановлювати ефективний зворотний зв’язок з користувачами профільних послуг та партнерами	**В1.В1.** Налаштовувати і використовувати у науковій діяльності програмні засоби захисту комп'ютерів (програмні фільтри, антивірусні програми й антишпигунське програмне забезпечення)

		В1.З6. Сучасні та новітні технології проєктування прототипів **В1.З7.** Порядок застосування в роботі оригінальних форматів відображення інформації	сучасні та новітні технології у процесі проєктування прототипів **В1.У6.** Відображати отримані результати в оригінальних форматах		
	В2. Здатність визначати функціональні властивості і властивості, пов'язані із забезпеченням безпеки, з метою пошуку сприятливих можливостей експлуатації або усунення вразливостей	**В2.З1**. Концепції, процедури, програмне забезпечення, обладнання та/або технологічні прикладні програми, необхідні для визначення функціональних властивостей і властивостей, пов'язаних із забезпеченням безпеки **В2.З2**. Загальнодоступні мережеві інструменти (ping, traceroute, nslookup) **В2.З3.** Командний рядок операційної системи (ipconfig, netstat, dir, nbtstat)	**В2.У1.** Застосовувати концепції, процедури, програмне забезпечення, обладнання та/або технологічні прикладні програми під час визначення функціональних властивостей і властивостей, пов'язаних із забезпеченням безпеки **В2.У2.** Користуватися загальнодоступними мережевими інструментами	**В2.К1.** Сприяти дискусіям у невеликих групах **В2.К2**. Готувати та проводити брифінги з обізнаності результатів кібердосліджень керівництву, персоналу і користувачам	**В2.В1** Керувати різними системами і методами електронної комунікації

		В2.З4. Системами і методами електронної комунікації (електронна пошта, VOIP, IM (миттєві повідомлення), Web-форуми, Direct Video Broadcasts) **В2.З5.** Класифікацію системних проблем безпеки	**В2.У3.** Використовувати командний рядок операційної системи **В2.У4.** Керувати різними системами і методами електронної комунікації		
	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 кібердосліджень; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції з усунення проблем при проєктуванні та усунення вразливостей при експлуатації систем безпеки				
Г. Проєктування та розроблення систем безпеки	**Г1**. Здатність розробляти детальну проєктну документацію з безпеки для специфікацій компонентів та інтерфейсів з метою підтримки проєкту та розроблення системи безпеки	**Г1.З1.** Перелік проєктних обмежень **Г1.З2.** Прийняті в організації правила класифікації інформації щодо рівнів захисту і процедур доступу до неї **Г1.З3**. Методи оцінювання ефективності заходів з кібербезпеки, які використовуються системою (системами)	**Г1.У1.** Аналізувати проєктні обмеження, аналізувати компроміси та детальний проект системи та безпеки, а також розглядати підтримку життєвого циклу (Т0012) **Г1.У2.** Оцінювати ефективність заходів з	**Г1.К1.** Аналізувати потреби та вимоги користувачів з метою планування і проведення розробки системи безпеки (Т0270)	**Г1.В1.** Проєктувати, розробляти, інтегрувати і оновлювати показники захищеності системи, які забезпечують конфіденційність, цілісність, доступність,

		Г1.З4. Джерела і методи збору інформації, її узагальнення, структурування, систематизацію **Г1.З5.** Класифікацію апаратного забезпечення, операційних системи та прикладного програмного забезпечення, необхідного для належного дотримання вимог кібербезпеки **Г1.З6.** Процедури тестування та затвердження системи **Г1.З7.** Вимоги, властивості та обмеження для процедур проєктування та процесів **Г1.З8.** Стандартні операційні процедури адміністрування систем **Г1.З9.** Базові потреби та вимоги користувачів з метою планування і проведення розробки системи безпеки	кібербезпеки, які використовуються системою (системами) (Т0018) **Г1.У3.** Проводити оцінки впливу приватності (PIA) проекту безпеки прикладних програм для відповідних контролів безпеки, що захищає конфіденційність та цілісність персональних ідентифікаційних даних (Т0032) **Г1.У4.** Проєктувати апаратне забезпечення, операційні системи та прикладне програмне забезпечення для належного дотримання вимог кібербезпеки (Т0055) **Г1.У5.** Розроблювати та направляти на		автентифіка-цію і безвідмовність (Т0446) **Г1.В2**. Оцінювати витрати-вигоду, економічний аналіз та аналіз ризиків у процесі прийняття рішень (Т099) **Г1.В3.** Оцінювати ефективність законів, правил, політик, стандартів чи процедур відповідного спрямування (Т0102)

		Г1.З10. Підходи проєктування, розроблення, інтегрування і оновлення показників захищеності системи, які забезпечують конфіденційність, цілісність, доступність, автентифікацію і безвідмовність	розгляд процедури тестування та затвердження системи і документацію (Т0061) **Г1.У6**. Розроблювати та документувати вимоги, властивості та обмеження для процедур проєктування та процесів (Т0062) **Г1.У7.** Розроблювати та документувати стандартні операційні процедури адміністрування систем (Т0063) **Г1.У8.** Визначати та пріоритезувати основні системні функції або підсистеми, необхідні для підтримки основних можливостей або бізнес-функцій з метою відновлення		

			або поновлення після відмови системи або під час відновлення системи на основі загальних системних вимог щодо безперервності та доступності (Т0109)		
	Г2. Здатність проводити ризиків, коли прикладна програма або система зазнають суттєвих змін	**Г2.З1.** Основні небезпеки, ризики і вразливості **Г2.З2**. Процедури сканування (пошуку) вразливостей в системах безпеки **Г2.З3**. Порядок розпізнавання вразливостей в системах безпеки **Г2.З4**. Порядок визначення пропускної здатності, характеристик та продуктивності комунікаційної системи **Г2.З5.** Інструменти мережевого аналізу для визначення	**Г2.У1.** Проводити сканування систем безпеки інформаційних ресурсів на вразливості **Г2.У2.** Аналізувати пропускну здатність, характеристики та продуктивність комунікаційної системи **Г2.У3.** Застосувати принципи забезпечення безпеки інформації – збереження конфіденційності, цілісності та доступності	**Г2.К1.** Здійснювати огляди безпеки та виявляти пробіли в архітектурі безпеки (Т0518)	**Г2.В1.** Розроблювати стратегії зменшення ризиків для усунення вразливостей та рекомендува-ти, у випадку необхідності, зміни заходів безпеки у системі або системних компонентах (Т076)

		вразливостей систем (fuzzing, nmap) **Г2.З6.** Засоби/заходи, що використовують алгоритми побудовані на основі штучного інтелекту для аналізу втручання в роботу інформаційних систем **Г2.З7.** Загрози та вразливості комп'ютерної системи (систем) для розробки профілю ризику безпеки **Г2.З8.** Порядок розроблення стратегій зменшення ризиків для усунення вразливостей та розроблення відповідних рекомендацій **Г2.З9**. Інструкція проведення оглядів без- пеки та виявлення пробілів в архітектурі безпеки	**Г2.У4**. Приймати участь у проведенні сканування та розпізнавання вразливостей в системах безпеки **Г2.У5.** Використовувати інструменти мережевого аналізу для визначення вразливостей систем **Г2.У6.** Застосовувати засоби/заходи, що використовують алгоритми побудовані на основі штучного інтелекту для аналізу втручання в роботу інформаційних систем **Г2.У7.** Оцінювати загрози та вразливості комп'ютерної системи (систем) для розробки		

			профілю ризику безпеки (Т0019) **Г2.У8.** Визначати та скеровувати виправлення технічних проблем, що виникають при тестуванні та впровадженні нових систем (Т0107)		
	Г3. Здатність інтегрувати методології життєвого циклу розробки систем (SDLC) в середовище розробки	**Г3.З1.** Нормативні документи і правила, що забезпечують захист авторських прав, патентування, винаходи **Г3.З2.** Новітні технології, інструменти, процедури, методи та процеси відповідного спрямування **Г3.З3.** Класифікацію технічних та процедурних процесів для безпечного резервного копіювання системи та захищеного зберігання резервних даних **Г3.З4.** Наявні плани аварійного відновлення	**Г3.У1**. Розроблювати або інтегровувати відповідні резервні спроможності у загальні проєкти системи та забезпечувати відповідні технічні та процедурні процеси для безпечного резервного копіювання системи та захищеного зберігання резервних даних (Т0056) **Г3.У2**. Розробляти плани аварійного відновлення та безперервності	**В2.К2**. Готувати та проводити брифінги з обізнаності результатів кібердосліджень керівництву, персоналу і користувачам	**Г3.В1.** Підтверджувати стабільність, сумісність, портативність і/або масштабованість архітектури системи (Т0544)

		та безперервності операцій для систем, що розробляються **Г3.З5.** Процедура тестування систем до їхнього вводу у продуктивне середовище **Г3.З6.** Інструменти управління мережею для аналізу структури мережевого трафіку **Г3.З7.** Аналізатори протоколів **Г3.З8.** Основи реверс-інжинірингу **Г3.З9.** Процедури резервного копіювання та відновлення мережі **Г3.З10.** Чинні вимоги безпеки для забезпечення виконання вимог для всіх систем або прикладних програм	операцій для систем, що розробляються, та забезпечувати тестування систем до їхнього вводу у продуктивне середовище (Т0070) **Г3.У3**. Використовувати інструменти управління мережею для аналізу структури мережевого трафіку **Г3.У4**. Використовувати аналізатори протоколів **Г3.У5**. Застосовувати навички реверс-інжинірингу **Г3.У6**. Переглядати та затверджувати програми, процеси і вимоги щодо збору та зберігання даних (Т0064) **Г3.У7.** Розроблювати та впроваджувати		

			процедури резервного копіювання та відновлення мережі (Т0065) **Г3.У8.** Розроблювати та підтримувати стратегічні плани (Т0066) **Г3.У9.** Розроблювати архітектури або компоненти системи відповідно до технічних умов (Т0067) **Г3.У10.** Розроблювати стандарти даних, політики та процедури (Т0068) **Г3.У11**. Включати рішення щодо вразливості системи у проєкти систем (Т0124) **Г3.У12**. Розроблювати вимоги безпеки для забезпечення виконання вимог		

			для всіх систем або прикладних програм (T0449) **Г3.У13**. Відстежувати системні вимоги з метою проєктування компонентів та виконувати аналіз недоліків розробки (T0541) **Г3.У14.** Проєктувати, впроваджувати, тестувати і оцінювати захищені інтерфейси між інформаційними системами, фізичними системами і/або вбудованими технологіями **Г3.У15.** Розроблювати спеціальні контрзаходи з кібербезпеки та стратегії пом’якшення ризиків для систем		

			та/або прикладних програм (0078) **Г3.У16.** Визначати компоненти чи елементи, розподіляти функції безпеки для цих елементів і описувати взаємозв'язок між елементами (Т0105) **Г3.У17.** Розроблювати детальну проєктну документацію з безпеки для специфікацій компонентів та інтерфейсів з метою підтримки проєкту та розроблення системи безпеки		
	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 проєктування та розроблення систем безпеки; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції з проєктування та розроблення систем безпеки				
Д. Впровад-	**Д1**. Здатність супровод-	**Д1.З1.** Методологію тестування та оцінки	**Д1.У1.** Забезпечувати	**Д1.К1**. Готувати та проводити брифінги	**Д1.В1.** Викону-

жен-ня супроводження систем безпеки	жувати розроблені системи безпеки	систем безпеки та сертифікації **Д1.З2.** Номенклатуру спеціалізованого обладнання та методики каталогізації, документування, вилучення, збирання, упаковки та зберігання цифрових доказів **Д1.З3.** Моделі та симуляції, які застосовуються для аналізу або прогнозування продуктивності системи за різних умов експлуатації **Д1.З4.** Чинні вітчизняні, зарубіжні та міжнародні стратегії мінімізації ризиків для зменшення витрат, графіку, продуктивності і ризиків безпеки **Д1.З5.** Методику оцінки ризиків інформаційної безпеки **А2.З6** Мережеві протоколи (К0174)	заходи щодо тестування та оцінки систем безпеки та сертифікації (Т0231) **Д1.У2**. Використовувати спеціалізоване обладнання та методики каталогізації, документування, вилучення, збирання, упаковки та зберігання цифрових доказів (Т0241) **Д1.У3**. Використовувати моделі та симуляції для аналізу або прогнозування продуктивності системи за різних умов експлуатації (Т0242) **Д1.У4**. Розроблювати стратегії мінімізації ризиків для зменшення витрат, графіку,	відповідного спрямування **Д1.К2**. Комунікувати з керівниками різних рівнів (міжособистісне спілкування, доступність, уміння ефективно сприймати мову виступаючих, відповідно до аудиторії коректувати стиль і мову виступу)	вати оцінку ризиків інфор-маційної без-пеки (Т0509)

		А2.З7 Методики зворотного інжинірингу програмного забезпечення (К0175) **А2.З8** Схеми розширеної мови розмітки (XML) (К0176) **А2.У9**. Стандарти й технічні умови, використовуються під час проєктування кібер-продукції	продуктивності і ризиків безпеки (Т0466)		
	Д2. Здатність забезпечувати дані для планів впровадження і стандартні операційні процедури, стосуються безпеки інформаційних систем	**Д1.З1.** Порядок побудови, тестування та модифікації прототипів кіберпродуктів **Д1.З2.** Підходи до визначення, оцінювання та рекомендування продуктів системи кібербезпеки або продуктів, що сприяють кібербезпеці **Д1.З3.** Загальні принципи управління	**Д2.У1.** Будувати, тестувати та модифікувати прототипи продуктів за допомогою робочих моделей або теоретичних моделей (Т0021) **Д2.У2.** Визначати, оцінювати та рекомендувати продукти системи кібербезпеки або продукти, що	**Д1.К1**. Готувати та проводити брифінги відповідного спрямування	**Д2.В1.** Розвивати розуміння потреб та вимог кінцевих користувачів наукових розробок (Т0060)

		ризиками та відповідну документацію (плани забезпечення життєвого циклу системи, концепція операцій, операційні процедури і навчальні матеріали з технічного обслуговування тощо) **Д1.З4.** Структуру, класифікацію показників та параметрів профільних баз даних **Д1.З5.** Порядок роботи з вхідними даними **А2.З6** Мережеві протоколи (К0174) **А2.З7** Методики зворотного інжинірингу програмного забезпечення (К0175) **А2.З8** Схеми розширеної мови розмітки (XML) (К0176) **А2.У9**. Стандарти й технічні умови, використовуються під час проєк-	сприяють кібербезпеці, для використання в системі, і гарантувати, що рекомендовані продукти відповідають організаційним вимогам щодо їхньої оцінки та затвердження (Т0119) **Д2.У3.** Надавати вхідні дані для діяльності процесу загальних принципів управління ризиками та відповідну документацію (Т0205) **Д2.У4.** Зберігати, відновлювати та обробляти дані для аналізу можливостей системи та вимог (Т0228)		

		тування кіберпродукції			
	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 впровадження та супроводження систем безпеки; бібліотечні ресурси, архівні матеріали (за потреби); профільна наукова та методична література; правила та інструкції з впровадження та супроводження систем безпеки				
Е. Консультування, популяризація оцінювання результатів стосовно застосування на практиці результатів кібердосліджень	**Е1**. Здатність застосовувати принципи навчання дорослих	**Е1.З1.** Методи соціальної інженерії **Е1.З2.** Вимоги і правила дотримання академічної доброчесності **Е1.З3**. Методи і технології підготовки доповідей та презентацій	**Е1.У1**. Використовувати методи соціальної інженерії **Е1.У2**. Ознайомлювати працівників та керівництво з новітніми корпоративними, вітчизняними, зарубіжними та міжнародними напрацюваннями у кіберзахисту	**Е1.К1.** Рекомендувати, за результатами навчання дорослих, керівництву кандидатури працівників до відповідних робочих груп (Т0968) **Д1.К1**. Готувати та проводити брифінги відповідного спрямування	**Е1.В1.** Аналізувати та звітувати перед керівництвом про користування активами і ресурсами управління знаннями (Т0154)
	Е2. Здатність розробляти обґрунтовані і надійні оцінки ре-	**Е2.З1.** Порядок та методи оцінювання результатів навчання	**Е2.У1.** Брати участь у розробленні внутрішніх	**Е2.К1.** Розроблювати тести для визначення рівня обізнаності та участі	**Е2.В1.** Готувати керівництву пропозиції

	зультатів кібердослід-жень та результатів навчання відповідного спря-мування	**Е2.З2.** Класифікацію методів оцінювання та процедуру їх застосування на практиці **Е2.З3.** Методики оцінювання результатів навчання (рубрики, плани оцінювання, тестування, вікторини) **Е2.З4.** Методи та процеси тестування і оцінювання слухачів	регламентів з присвоєння/при-судження кваліфікацій слухачам **Е2.У2.** Приймати участь в оцінюванні в організації результатів кібердосліджень	працівників щодо проведення кібердосліджень **Е2.К2**. Розроблювати критерії оцінювання працівників щодо проведення кібердосліджень **Е2.К3**. Брати участь у розробленні правил оцінювання працівників щодо щодо проведення кібердосліджень	щодо поліпшення в організації роботи з проведення кібердослід-жень, підвищення їх ефектиівності та результатив-ності
	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; лабораторні та навчальні приміщення і обладнання; профільна наукова та методична література правила та інструкції з консультування, популяризації та оцінювання її результатів стосовно застосування на пр результатів кібердосліджень				

VI. Розподіл трудових функцій та компетентностей за професійними кваліфікаціями

Трудова функція (умовне позначення)	**Загальна назва професійної кваліфікації у межах професійного стандарту: фахівець із кібердосліджень та розробок систем безпеки**	
	Фахівець із кібердосліджень та розробок систем безпеки	**провідний фахівець кібердосліджень та робок систем безпеки**
	повна	часткова додаткова
А	+	+
Б	+	+
В	+	+
Г	+	+
Д	+	+
Е	-	+

VII. Відомості про розроблення та затвердження професійного стандарту

1. Повне найменування розробника професійного стандарту

Державної служби спеціального зв’язку та захисту інформації України

Склад робочої групи/Учасники робочої групи:

_____
_____

2. Назва та реквізити документа, яким затверджено професійний стандарт (рішення (може оформлюватися протоколом), наказ, розпорядження).

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 _____ про дотримання під час підготовки проєкту професійного стандарту «фахівець із кібердосліджень та розробок систем безпеки» 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 від _____ щодо погодження проєкту професійного стандарту «фахівець із кібердосліджень та розробок систем безпеки».

VIII. Дата внесення професійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.