Проєкт

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

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

I. Назва професійного стандарту

Фахівець із кібердосліджень та розробок систем безпеки

II. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Концептуалізація, проєктування, розробка технічного завдання для створення та/або закупівлі безпечних систем інформаційних технологій, розвиток систем та/або мереж, оцінювання технологій та процесів інтеграції, забезпечення та підтримка можливості прототипу та/або оцінка його корисності, експлуатація та/або розробка та дослідження програмного забезпечення та систем для набуття нових спроможностей забезпечення кібербезпеки, проведення комплексних технологічних досліджень для оцінювання потенційних вразливостей в інформаційних системах у кіберпросторі. Формування нових гіпотез, теорій, моделей, розробка стандартів, методів (методик) їх реалізації, проведення фундаментальних та прикладних дослідження програмного забезпечення та систем безпеки, сприяння впровадженню інновацій а також систем та/або програмного забезпечення у сфері кібербезпеки.

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 61.9**	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 62.09	Інша діяльність у сфері інформаційних технологій і комп'ютерних систем
Секція M	Професійна, наукова та технічна діяльність	**Розділ 70**	Діяльність головних управлінь (хед-офісів); консультування з питань керування	**Група 70.2**	Консультування з питань керування
				Клас 70.22	Консультування з питань комерційної діяльності й керування

		Розділ 74	Інша професійна, наукова та технічна діяльність	**Група 74.9**	Інша професійна, наукова та технічна діяльності, не введенні в інші угрупування
				Клас 74.90	Інша професійна, наукова та технічна діяльності, не введенні в інші угрупування
Секція Р	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;

Професіонал з кібердосліджень та розробок систем безпеки, 8 рівень НРК.

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

- Диплом на другому (магістерському) та третьому (освітньо-науковому/освітньо-творчому) – рівні вищої освіти за спеціальністю:

- 111 «Математика» галузі знань 11 «Математика та статистика» (7 рівень НРК);
- 112 «Статистика» галузі знань 11 «Математика та статистика» (рівень 7 НРК);
- 113 «Прикладна математика» галузі знань 11 «Математика та статистика» (7 рівень НРК);
- 121 «Інженерія програмного забезпечення» галузі знань 12 «Інформаційні технології» (7, 8 рівні НРК);
- 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології» (7, 8 рівні НРК);
- 123 «Комп'ютерна інженерія» галузі знань 12 «Інформаційні технології» (7, 8 рівні НРК);
- 124 «Системний аналіз» галузі знань 12 «Інформаційні технології» (7, 8 рівні НРК);
- 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційнітехнології» (7,8 рівні НРК);
- 126 «Інформаційні системи та технології» галузі знань 12 «Інформаційні технології» (7, 8 рівні НРК);

- 171 «Електроніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (7, 8 рівні НРК);

- 172 «Електронні комунікації та радіотехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (7, 8 рівні НРК);

- 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (7, 8 рівні НРК);

- 175 «Інформаційно-вимірювальні технології» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (7, 8 рівні НРК);

- 251 «Державна безпека» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7, 8 рівні НРК);

- 252 «Безпека державного кордону» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7, 8 рівні НРК);

- 253 «Військове управління (за видами збройних сил)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7, 8 рівні НРК);

- 255 «Озброєння та військова техніка» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7, 8 рівні НРК);

- 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7, 8 рівні НРК);

- 257 «Управління інформаційною безпекою» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7, 8 рівні НРК).

Додатково (за необхідністю або/чи вимогою суб'єкта, уповноваженого законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій):

- документ (диплом, сертифікат, тощо), щодо післядипломної освіти та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань 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 завдань 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 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	Підготовка на другому рівні вищої освіти (магістерському) за спеціальностями вказаними п. ІІ.5, без вимог до стажу роботи.	*Не передбачено професійним стандартом*
Провідний фахівець із кібердосліджень та розробок систем безпеки	Підготовка на другому рівні вищої освіти (магістерському) за спеціальностями вказаними п. ІІ.5, стаж роботи за однією з професій відповідного спрямування повинен складати не менше 2 років.	*Не передбачено професійним стандартом*
Професіонал з кібердосліджень та розробок систем безпеки	Підготовка на другому (магістерському) та третьому (освітньо-науковому/освітньо-творчому) рівнях вищої освіти за спеціальностями вказаними п. ІІ.5, стаж роботи за однією з професій відповідного спрямування (аналітик з безпеки інформаційно-телекомунікаційних систем, фахівець з питань безпеки (інформаційно-комунікаційні технології), фахівець сфери захисту інформації, аналітик з оцінки вразливостей, фахівець з тестування систем захисту інформації, фахівець з планування	*Не передбачено професійним стандартом*

Назва професійної та/або часткової професійної кваліфікації	Суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
	політики та стратегії кібербезпеки, керівник структурного підрозділу з питань безпеки інформації та кіберзахисту тощо) повинен складати не менше 3 років	

2. Професійний розвиток 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**
Провідний фахівець з кібердосліджень та розробок систем безпеки	Підвищення кваліфікації для отримання професійної кваліфікації «провідний фахівець з кібердосліджень та розробок систем безпеки». Стаж роботи не менше двох років за професійною кваліфікацією «фахівець з кібердосліджень та розробок систем безпеки».	*Не передбачено професійним стандартом*
Професіонал з кібердосліджень та розробок систем безпеки	Підвищення кваліфікації для отримання професійної кваліфікації «професіонал з кібердосліджень та розробок систем безпеки». Стаж роботи не менше року за професійною кваліфікацією «провідний фахівець з кібердосліджень та розробок систем безпеки».	*Не передбачено професійним стандартом*

IV. Абревіатури, скорочення

ІТ	інформаційні технології
ПЗ	програмне забезпечення

PCI DSS	Payment Card Industry Data Security Standard
SSL	Secure Sockets Layer
EBSCO	Elton Bryson Stephens Company
JSTOR	Journal Storage
PIA	Private Internet Access
XML	Extensible Markup Language

V. Опис трудових функцій

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
А. Визначення об'єкту (рамок) інжинірингу програмного забезпечення та систем забезпечення кібербезпеки.	**А1**. Здатність виявляти системи критичної інфраструктури з ІТ, які були спроектовані без врахування безпеки системи.	**А1.З1**. Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи (наприклад, прикладна система ешелонованого захисту. **А1.З2**. 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 стандарту PCI DSS, сканування захисту від втрати даних, прискорених криптографічних операцій, протокол захисту інформації SSL. **А1.З3.**Закони, політики, процедур чи корпоративного	**А1.У1** Досліджувати і оцінювати наявні технології і стандарти з метою задоволення вимог замовника. **А1.У2** Оцінювати ефективність застосованих вимог чинних законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки. **А1.У3** Оцінювати необхідність проведення інжирінгу програмного забезпечення та систем забезпечення кібербезпеки на конкретному об'єкті.	**А1.К1**. Співпрацювати із зацікавленими сторонами, щоб визначити та/або розробити відповідної технології рішень. **А1.К2.** Формувати запити на профільну Інформацію.	**А.В1.** Формування переліку систем критичної інфраструктури з інформаційно-комунікаційними технологіями, які були розроблені без врахування безпеки системи . **А.В2.** Створення переліку об'єктів (визначення границь) інжинірингу програмного забезпечення та систем забезпечення кібербезпеки.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		управління, що стосуються кібербезпеки критичних інфраструктур. **А1.З4**. Діючі закони, нормативно-правових актів парламенту, директив президента, постанов і розпоряджень органів виконавчої влади та/або кодексу і процедур адміністративного/ кримінального права етичних норм, та як вони пов'язані зі забезпечення інформаційної та/або кібербезпеки, а також захисту персональних даних.			
	А2. Здатність оцінювати вразливості мережевої інфраструктури, для покращення ПЗ та систем забезпечення кібербезпеки, що планується розробляти	**А2.З1.** Класифікацію вразливостей прикладних програм. **А2.З2**. Кіберзагрози та вразливості. **А2.З3**. Основні операційні наслідки інцидентів кібербезпеки. **А2.З5.** Криміналістичну процедуру ідентифікації електронних слідів.	**А2.У1**. Враховувати у дослідницькій та проектній діяльності виявлені вразливості мережевої інфраструктури. **А2.У2.** Використовувати інструменти мережевого аналізу	**А2.К1.** Проводити моніторинг зауважень, скарг, прокламацій та пропозицій партнерів та користувачів нових продуктів кіберзахисту щодо оцінювання наявних вразливості	**А2.В1.** Проводити аналіз слабких місць або недоліків, виявлених в системі та її середовищі функціонування, і рекомендувати коригуючі дії для вирішення виявлених вразливостей.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		А2.З6. Інструменти аналізу мереж для виявлення вразливостей у ПЗ комп'ютерних мереж. **А2.З7.** Концепції криптографії та управління криптографічними ключами. **А2.З9.** Методики організації прихованих каналів зв'язку **А2.З10.** Стандартні галузеві моделі захисту.	для визначення вразливостей систем. **А2.У1.** Ідентифікувати вразливості мережевої інфраструктури та ПЗ у сфері кібербезпеки.	мережевої інфраструктури.	
	А3. Здатність оцінювати ризики порушення стану забезпечення кібербезпеки інформаційних ресурсів та систем критичної інформаційної інфраструктури.	**А3.З1.** Методики управління ризиками (методи оцінювання та оброблення ризиків). **А3.З2**. Методики управління ризиками інформаційної та/або кібербезпеки в ланцюжку постачання. **А3.З3.** Оцінювати загрози для комп'ютерної системи (систем) та її вразливості для розробки профілю ризику безпеки.	**А3.У1.** Здійснювати аналіз ризиків, дослідження здійсненності та/або компромісний аналіз для розробки, документування та вдосконалення функціональних вимог та специфікацій. **А3.У2.** Розроблювати і публікувати	**А3.К1.** Приймати участь у розробленні методології кібербезпеки організації та управління ризиком ланцюжка постачання для розробки безперервності операційних планів.	**А3.У1.** Оцінювати загрози та вразливості комп'ютерної системи (систем) для розробки профілю ризику безпеки. **А3.У2.** Розроблювати стратегії зменшення ризиків для усунення вразливостей та рекомендувати, у випадку необхідності, зміни заходів безпеки у

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		А3.З4. Основні небезпеки, ризики і вразливості. **А3.З5.** Методики управління ризиками (методи оцінювання та оброблення ризиків). **А3.З6**. Принципи забезпечення конфіденційності персональних даних та забезпечення їх кібербезпеки. **А3.З7**. Політик, вимог і процедур безпеки ланцюжка постачання ІТ та управління ризиками.	документи щодо управління безпекою ланцюжка постачання та управління ризиками. **А3.У3.** Оцінювати вразливості мережевої інфраструктури, щоб поширити можливості, які розробляються. **А3.У4.** Розроблювати стратегії оцінювання та обробки ризиків з метою усунення вразливостей та рекомендувати, за необхідності, зміни заходів безпеки у системі або системних компонентах. **А3.У5**. Проводити аналіз ризиків, коли прикладна програма або система зазнають суттєвих		системі або системних компонентах. **А3.У3.** Розроблювати стратегії мінімізації ризиків для зменшення витрат, графіку, продуктивності і ризиків безпеки **А3.У4.** Виконувати оцінювання ризиків інформаційної безпеки.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
			змін. **А3.У6**.Здійснювати огляди безпеки та виявляти пробіли в архітектурі безпеки.		
Б. Розроблення методик, методів, алгоритмів, програм, засобів інжинірингу програмного забезпечення та систем забезпечення кібербезпеки.	**Б1.** Здатність розробляти програми, методики дослідження та досліджувати програмне забезпечення та системи забезпечення кібербезпеки.	**Б1.З1.** Новітні технології, інструменти, процедури, методи та процеси відповідного спрямування. **Б1.З2.** Процедури тестування систем до їхнього введення у продуктивне середовище. **Б1.З3.** Спроможності прикладних програм і потенційних вразливостей мережевого обладнання, включаючи концентратори, маршрутизатори, комутатори, мости, сервери, носії передачі інформації і супутнє апаратне обладнання. **Б1.З4.** Інструменти, методи і методики проєктування систем, включаючи	**Б1.У1.** Застосовувати інструменти, методи і техніки проектування систем, включаючи інструменти автоматизованого аналізу та проектування систем. **Б1.У2.** Розроблювати технічну документацію. **Б1.У2.** Розроблювати і документувати стратегію комплексного тестування та оцінювання ПЗ.	**Б1.К1.** Розроблювати вказівки і настанови для працівників, залучених до кібердосліджень. **Б1.К4**. Здійснювати зворотній зв'язок з партнерами, підрядниками проєктних та науково-дослідних робіт з розроблення нових продуктів в сфері кіберзахисту.	**Б1.В1.** Складати алгоритм, програму, методику дослідження з урахуванням специфіки програмного забезпечення та систем забезпечення кібербезпеки, що використовується.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		автоматизовані системи аналізу і інструменти проектування.			
	Б2. Здатність співпрацювати із заінтересованими 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, ПЗ, обладнання і прикладні технологічні програми які застосовуються для співпраці із зацікавленими сторонами. **Б1.З3.** Сучасні/перспективні технологій комунікації. **Б1.З4.** Основні бізнес-процеси і місію організації.	**Б2.У1**. Розроблювати настанови стосовно впровадження розроблених клієнтам або командам впровадження систем. **Б2.У2**. Встановлювати та підтримувати канали зв'язку з зацікавленими сторонами. **Б2.У3**. Переглядати існуючі та перспективні політики із зацікавленими сторонами.	**Б2.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 продуктів у сфері кіберзахисту та проведення кібердосліджень.	**Б2.В1**. Розроблювати технічну документацію відповідного спрямування.
	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);				

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції з проведення кібердосліджень.				
В. Проведення дослідження ПЗ та систем забезпечення кібербезпеки.	**В1.** Здатність проводити дослідження програмного забезпечення та систем забезпечення кібербезпеки, розроблювати обґрунтовані і надійні оцінки результатів кібердосліджень.	**В1.З1.** Вимоги, властивості та обмеження для процедур проєктування. **В1.З2.** Класифікацію апаратного забезпечення, операційних системи та прикладного програмного забезпечення, необхідного для належного дотримання вимог кібербезпеки. **В1.З3.** Стандартні операційні процедури адміністрування систем. **В1.З4**. Підходи до проєктування, розроблення, інтегрування і оновлення показників захищеності системи, які забезпечують конфіденційність, цілісність, доступність, автентифікацію і безвідмовність.	**В1.У1.** Проводити оцінку впливу приватності (PIA) проекту безпеки прикладних програм для відповідних контролів безпеки, що забезпечує конфіденційність та цілісність персональних даних. **В1.У2.** 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	**В1.К1**. Сприяти обміну знаннями між власниками/ користувачами інформації через операційні процеси і системи організації.	**В1.В1.** Готувати керівництву пропозиції щодо поліпшення організації роботи з кібердосліджень, підвищення їх ефективності та результативності.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		В1.З5. Методики зворотного інжинірингу технічного обладнання. **В1.З6.** Процедури сканування (пошуку) вразливостей в системах безпеки. **В1.З7.** Інструкції щодо проведення оглядів безпеки та виявлення пробілів в архітектурі безпеки. **В1.З8.** Засоби/заходи, що використовують алгоритми побудовані на основі штучного інтелекту для аналізу втручання в роботу інформаційних систем. **В1.З9.** Методології зламу. **В1.З10.** Потенційні вразливості кібербезпеки в галузевих технологіях. **В1.З11.** Принципи, інструменти та методики тестування на проникнення. **В1.З12.** Безпеку операцій.	загальних системних вимог щодо безперервності та доступності. **В1.У3.** Приймати участь у проведенні сканування та розпізнавання вразливостей в системах безпеки. **В1.У4.** Аналізувати пропускну здатність, характеристики та продуктивність комунікаційної системи. **В1.У5.** Застосувати принципи забезпечення безпеки інформації, збереження конфіденційності, цілісності та доступності. **В1.У6.** Розроблювати тести для визначення рівня обізнаності та участі працівників		

Трудові функції	Компетентності	Результати навчання			
		Знання	Уміння/навички	Комунікація	Відповідальність і автономія
			щодо кібердосліджень. **В1.У6.** Розроблювати критерії оцінювання працівників щодо кібердосліджень.		

	В2. Здатність визначати стратегії розвитку кіберспроможностей для розробки програмно-апаратних комплексів.	**В2.З1.** Структуру та властивості операційної системи (управління процесами, структура каталогів, встановлених застосунків тощо). **В2.З2.** Експериментальні методології розроблення продуктів, які забезпечують кібербезпеку. **В2.З3.** Основні аспекти проєктування продуктів в сфері кібебезпеки. **В2.З4.** Методи та ризики, пов'язані з вибором компонентів кіберпродукції. **В2.З5.** Інженерні концепції, що застосовуються до комп'ютерної архітектури і відповідного комп'ютерного обладнання/програмного забезпечення.	**В2.У1.** Визначати стратегії розвитку кіберспроможно-стей розробки програмно-апаратних комплексів для замовника. **А3.У2.** Застосовувати сучасні методи проєктування, конструювання й виробництва кіберпродукції та/чи її компонентів. **А3.У2.** Розроблювати та підтримувати стратегічні плани.	**В2.К1.** Надавати рекомендації щодо структур даних і баз даних з метою гарантованого забезпечення підготовки коректних і якісних звітних документів. **В2.К2.** Пояснювати послідовність проєктування, виробництва, випробування та/або сертифікації продуктів, призначених для забезпечення кібербезпеки та/чи її компонентів. **В2.К3.** Пояснювати особливості конструкції та основні аспекти робочих процесів у компонентах нових продуктів з кіберзахисту.	**В2.В1.** Розроблювати стратегії зменшення ризиків для усунення вразливостей та рекомендувати, у випадку необхідності, зміни заходів безпеки у системі або системних компонентах.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	В3. Здатність розроблювати детальну проєктну документацію з безпеки для специфікацій компонентів та інтерфейсів з метою підтримки проєкту та розроблення системи безпеки.	**В3.З1.** Перелік проєктних обмежень. **В3.З2.** Прийняті в організації правила класифікації інформації щодо рівнів захисту і процедур доступу до неї. **В3.З3**. Методи оцінювання ефективності заходів з кібербезпеки, які використовуються системою (системами). **В3.З4.** Джерела і методи збору інформації, її узагальнення, структурування, систематизації. **В3.З5.** Базової потреби та вимог користувачів з метою планування і проведення розробки системи безпеки.	**В3.У1.** Аналізувати проєктні обмеження, аналізувати компроміси та детальний проект системи та безпеки, а також розглядати підтримку життєвого циклу. **В3.У2.** Оцінювати ефективність заходів з кібербезпеки, які використовуються системою (системами). **В3.У3.** Проєктувати апаратне забезпечення, операційні системи та прикладне програмне забезпечення для належного дотримання вимог кібербезпеки. **В3.У4.** Розроблювати та направляти на розгляд процедури	**В3.К1.** Аналізувати потреби та вимоги користувачів з метою планування і проведення розробки системи безпеки.	**В3.В1.** Проєктувати, розроблювати, інтегрувати і оновлювати показники захищеності системи, які забезпечують конфіденційність, цілісність, доступність, автентифікацію і безвідмовність. **В3.В2**. Оцінювати витрати/вигоду, економічний аналіз та аналіз ризиків у процесі прийняття рішень. **В3.В3.** Оцінювати ефективність законів, правил, політик, стандартів чи процедур відповідного спрямування.

Трудові функції	Компетентності	Результати навчання			
		Знання	Уміння/навички	Комунікація	Відповідальність і автономія
			тестування, затвердження системи і документації. **В3.У5**. Розроблювати та документувати вимоги, властивості та обмеження для процедур проєктування та процесів. **В3.У6.** Розроблювати та документувати стандартні операційні процедури адміністрування систем. **В3.У7.** Проєктувати і розроблювати нові інструменти/технології, що стосуються кібербезпеки. **В3.У8.** Розроблювати архітектури або компоненти системи відповідно до технічних умов.		

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
			В3.У9. Розроблювати стандарти даних, політики та процедури. **В3.У10**. Розроблювати вимоги безпеки для забезпечення виконання вимог для всіх систем або прикладних програм. **В3.У11**. Здійснювати комплексний аналіз відповідності змісту програм, процесів і вимог щодо збору та зберігання даних встановленим стандартам та регламентам.		
	В4. Здатність дотримуватися стандартів і процедур життєвого циклу ПЗ і інженерії систем.	**В4.З1.** Основи реверс-інжинірингу ПЗ та технічного обладнання. **В4.З2.** Аналізатори протоколів. **В4.З3.** Інструменти управління мережею для	**В4.У1.** Розроблювати і застосовувати в проєктуванні нових інструментів/ технологій, що стосуються кібербезпеки,	**В4.К1.** Розповсюджувати серед профільних працівників структурного підрозділу, керівництва та партнерів останні	**В4.В1.** Застосовувати у практичній діяльності стандарти і процедури життєвого циклу ПЗ і інженерії систем.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		аналізу структури мережевого трафіку. **В4.З4.** Класифікацію технічних та процедурних процесів для безпечного резервного копіювання системи та захищеного зберігання резервних даних. **В4.З5.** Наявні плани аварійного відновлення та безперервності операцій для систем, що розробляються.	математичні або статистичні моделі. **В4.У2.** Використовувати наукові підходи і методики при вирішенні проблем у проєктуванні та розробленні нових інструментів/ технологій, що стосуються кібербезпеки. **В4.У3**. Застосовувати процеси технічної розробки систем. **В4.У4**. Розроблювати або інтегрувати відповідні спроможності резервування у загальні проєкти, системи та забезпечувати відповідні технічні, процедурні процеси для безпечного резервного копіювання.	вітчизняні, зарубіжні та міжнародні досягнення щодо розроблення та застосування стандартів і процедур відповідного спрямування.	

Трудові функції	Компетентності	Результати навчання			
		Знання	Уміння/навички	Комунікація	Відповідальність і автономія
			системи, а також захищеного зберігання резервних даних. **В4.У5**. Розроблювати плани аварійного відновлення та безперервності операцій для систем, що розробляються, та забезпечувати тестування систем до їхнього вводу у продуктивне середовище. **В4.У6**. Використовувати інструменти управління мережею для аналізу структури мережевого трафіку. **В4.У7**. Використовувати аналізатори протоколів. **В4.У8**. Застосовувати		

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
			навички реверс-інжинірингу. **В4.У9**. Переглядати та затверджувати програми, процеси і вимоги щодо збору та зберігання даних. **В4.У10.** Розроблювати та впроваджувати процедури резервного копіювання та відновлення мережі. **В4.У11**. Відстежувати системні вимоги з метою проєктування компонентів та виконувати аналіз недоліків розробки.		
	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.			

Трудові функції	**Компетентності**	**Результати навчання**			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
Г. Розроблення, впровадження та супроводження нових програмних та технічних рішень забезпечення кібербезпеки.	**Г1.** Здатність визначати функції систем, а також функції, пов'язані з безпекою, для розробки нових спроможностей експлуатації або усунення вразливостей.	**Г1.З1**. Концепції, процедури, ПЗ, обладнання та/або технологічні прикладні програми, необхідні для визначення функціональних властивостей і властивостей, пов'язаних із забезпеченням кібербезпеки. **Г1.З2**. Загальнодоступні мережеві інструменти (ping, traceroute, nslookup тощо). **Г1.З3.** Командний рядок операційної системи (ipconfig, netstat, dir, nbtstat). **Г1.З4.** Порядок розроблювання спеціальних контрзаходів з кібербезпеки та стратегії пом'якшення ризиків для систем та/або прикладних програм.	**Г1.У1.** Застосовувати концепції, процедури, ПЗ, обладнання та/або технологічні прикладні програми під час визначення функціональних властивостей і властивостей, пов'язаних із забезпеченням безпеки. **Г1.У2.** Користуватися загальнодоступ-ними мережевими інструментами. **Г1.У3.** Використовувати командний рядок операційної системи . **Г1.У4.** Користуватися різними системами і методами електронної комунікації.	**Г1.К1.** Співпрацювати із зацікавленими сторонами щодо врегулювання інцидентів в області комп'ютерної безпеки і вимог щодо управління/ усунення вразливостей.	**Г1.В1** Проводити оцінку технічних (оцінка технології) і нетехнічних (оцінка людей і операцій) ризиків і вразливостей пріоритетних технологічних областей (наприклад, локальне комп'ютерне середовище, мережа та інфраструктура, межі закритої групи, допоміжна інфраструктура та прикладні програми).

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
			Г1.У5. Виявляти системні проблеми безпеки на основі аналізу даних вразливостей та конфігурації. **Г1.У6**. Включати рішення щодо управління вразливостями системи у проєкти систем .		
	Г2. Здатність усувати проблеми, що виникають в процесі проєктування прототипів, а також на етапах проектування, розробки і перед запуском продукту.	**Г2.З1.** Класифікацію вразливостей при експлуатації систем безпеки. **Г2.З2.** Порядок усунення проблем при проєктуванні та усунення вразливостей при експлуатації систем безпеки. **Г2.З4.** Програмні засоби захисту комп'ютерів (програмні фільтри, антивірусні програми й антишпигунське програмне забезпечення тощо). **Г2.З5.** Компоненти системи мережевої	**Г2.У1**. Усувати проблеми, що виникають в процесі проєктування прототипів, а також на етапах проектування, розробки і перед запуском продукту. **Г2.У2.** Використовувати у процесі проєктування прототипів віртуальні машини. **Г2.У3.** Налаштовувати і	**Г2.К1**. Надавати (доводити до відома) технічну інформацію різним категоріям користувачів. **Г2.К2.** Встановлювати ефективний зворотній зв’язок з користувачами профільних послуг та партнерами.	**Г2.В1.** Проєктувати, будувати, тестувати та модифікувати прототипи продуктів за допомогою робочих моделей або теоретичних моделей.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		безпеки (мережеві екрани, віртуальні приватні мережі, системи виявлення вторгнень тощо). **Г2.З6.** Стандарти й технічні умови, які використовуються під час проєктування продуктів, що використовуються в сфері кібербезпеки.	використовувати у процесі проєктування прототипи систем кібербезпеки. **Г2.У4**. Конфігурувати і використовувати у процесі проєктування прототипів компоненти системи мережевої безпеки. **Г2.У5**. Використовувати сучасні та новітні технології кіберзахисту в процесі проєктування прототипів. **Г2.У6.** Визначати та/або розробляти засоби зворотної (реверс) інженерії для підвищення спроможностей і виявлення вразливостей. **Г2.У7.** Визначати		

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
			компоненти чи елементи систем безпеки, розподіляти функції безпеки для цих елементів і описувати взаємозв'язок між елементами.		
	ГЗ. Здатність створювати нові спроможності забезпечення кібербезпеки.	**ГЗ.З1** Проміжне програмне забезпечення (шини обслуговування організації і черги повідомлень тощо). **ГЗ.З2** Мережеві протоколи . **ГЗ.З3** Архітектуру систем мобільного зв'язку. **ГЗ.З4** Стандартні галузеві моделей захисту. **ГЗ.З5.** Передові світові технологічні тенденції виготовлення продукції у сфері кіберзахисту. **ГЗ.З6.** Технічні характеристики й економічні показники кращих вітчизняних і	**ГЗ.У1.** Освоювати досягнення у технологіях захисту інформації для забезпечення їх впровадження у відповідній організації. **ГЗ.У2**. Здійснювати моніторинг змін у нормативно-правових документах відповідного спрямування. **ГЗ.У3.** Формувати й оновлювати базу знайдених матеріалів для подальшого її використання в роботі.	**ГЗ.К1.** Адаптувати технічну інформацію для досліджень до рівня розуміння користувача/ споживача/ замовника.	**ГЗ.В1.** Виконувати розрахунки технічних, техніко-економічних і функціонально-вартісних показників продукції, що проєктується. **ГЗ.В2.** Надавати рекомендації щодо нових технологій і архітектур баз даних.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		світових розробок із кіберзахисту. **ГЗ.З7**. Досвід передових вітчизняних і зарубіжних підприємств щодо конструювання кіберпродукції й застосування нових технологій її виробництва. **ГЗ.З8**. Мережеві протоколи. **ГЗ.З9**. Схеми розширеної мови розмітки (XML).	**ГЗ.У4.** Читати й аналізувати схеми й креслення, конструкторську, технологічну та іншу документацію відповідного спрямування. **ГЗ.У5.** Працювати з електронними архівами стандартів і технічних умов, які використовуються під час проєктування продукції сфери кібербезпеки. **ГЗ.У6.** Розроблювати нові можливості управління даними (наприклад, хмарне централізоване управління криптографічними ключами), щоб забезпечити підтримку мобільного персоналу.		

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
			ГЗ.У7. Застосовувати та інтегрувати ІТ до запропонованих рішень. **ГЗ.У8.** Проєктувати інтеграцію технологічних процесів і рішень, включаючи застарілі системи і сучасні мови програмування. **ГЗ.** Застосовувати практики безпечної розробки програмного забезпечення.		
	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.			
Д. Проєктування, розроблення, впровадження нових моделей, сприяння впровадженням	**Д1**. Здатність забезпечувати наявність вхідних даних для планів впровадження і стандартні операційні процедури, які стосуються безпеки інформаційних систем.	**Д1.З1.** Порядок побудови, тестування та модифікації прототипів продуктів в сфері кібербезпеки. **Д1.З2.** Підходи до визначення, оцінювання	**Д1.У1.** Будувати, тестувати та модифікувати прототипи продуктів за допомогою робочих	**Д1.К1.** Готувати та проводити брифінги відповідного спрямування.	**Д1.В1.** Розвивати розуміння потреб та вимог кінцевих користувачів наукових розробок.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
інноваційних програмних та технічних рішень забезпечення кібербезпеки.		та рекомендування продуктів системи кібербезпеки або продуктів, що сприяють кібербезпеці. **Д1.З3.** Загальні принципи управління ризиками та відповідну документацію (плани забезпечення життєвого циклу системи, концепції 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. **Д1.З6.** Мережеві протоколи. **Д1.З7.** Методики зворотного інжинірингу програмного забезпечення. **Д1.З8**. Стандарти й технічні умови, які використовуються під	або теоретичних моделей. **Д1.У2.** Визначати, оцінювати та рекомендувати продукти системи кібербезпеки або продукти, що сприяють кібербезпеці, для використання в системі, і гарантувати, що рекомендовані продукти відповідають організаційним вимогам щодо їхньої оцінки та затвердження. **Д1.У3.** Надавати вхідні дані для діяльності процесу загальних принципів управління ризиками та відповідну документацію. **Д1.У4.** Зберігати, відновлювати та		

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		час проєктування продукції. **Д1.З9**. Технологічні задачі і завдання управління та лідерства пов'язані з організаційними процесами, механізми вирішення проблем. **Д1.З10.** Засоби/заходи, що використовують алгоритми, побудовані на основі штучного інтелекту для аналізу втручання в роботу інформаційних систем.	обробляти дані для аналізу можливостей системи та вимог. **Д1.У5.** Розроблювати і застосування математичні або статистичні моделі.		
	Д2. Здатність супроводжувати розроблені системи безпеки.	**Д2.З1.** Методологію тестування та оцінки систем безпеки та сертифікації. **Д2.З2.** Номенклатуру спеціалізованого обладнання та методики каталогізації, документування, вилучення, збирання, упаковки та зберігання цифрових доказів. **Д2.З3.** Моделі та симуляції, які застосовуються для	**Д2.У1.** Забезпечувати заходи щодо тестування та оцінювання систем безпеки та сертифікації. **Д2.У2**. Використовувати спеціалізоване обладнання та методики каталогізації, документування, вилучення,	**Д2.К1**. Комунікувати з керівниками різних рівнів (міжособистісне спілкування, доступність, уміння ефективно сприймати мову виступаючих, відповідно до аудиторії коректувати стиль і мову виступу).	**Д2.В1.** Виконувати оцінювати ризики інформаційної безпеки. **Д2.В2**. Інтерпретувати та застосовувати закони, нормативні акти, політики, стандарти чи процедури до конкретних питань.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		аналізу або прогнозування продуктивності системи за різних умов експлуатації. **Д2.З4.** Чинні вітчизняні, зарубіжні та міжнародні стратегії мінімізації ризиків для зменшення витрат, графік продуктивності і ризиків безпеки. **Д2.З5.** Методику оцінювання ризиків інформаційної безпеки **Д2.З6** Мережеві протоколи. **Д2.З9**. Стандарти й технічні умови, які використовуються під час проєктування продукції.	збирання, упаковки та зберігання цифрових доказів. **Д2.У3**. Використовувати моделі та симуляції для аналізу або прогнозування продуктивності системи за різних умов експлуатації. **Д2.У4**. Розроблювати стратегії мінімізації ризиків для зменшення витрат, графіку, продуктивності і ризиків безпеки. **Д2.У5.** Визначати та скеровувати виправлення технічних проблем, що виникають при тестуванні та впровадженні нових систем.		
	Д3. Здатність оцінювати результати кібердосліджень та результати навчання відповідного спрямування.	**Д3.З1.** Порядок та методи оцінювання результатів навчання.	**Д3.У1.** Брати участь у розробленні внутрішніх регламентів з	**Д3.К1.** Розроблювати тести для визначення рівня обізнаності та	**Д3.В1.** Готувати керівництву пропозиції щодо поліпшення роботи з

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		ДЗ.З2. Класифікацію методів оцінювання та процедуру їх застосування на практиці. **ДЗ.З3.** Методики оцінювання результатів навчання (рубрики, плани оцінювання, тестування, вікторини). **ДЗ.З4.** Методи та процеси тестування і оцінювання слухачів.	присвоєння/присуд ження кваліфікацій слухачам. **ДЗ.У2.** Приймати участь в оцінюванні результатів кібердосліджень. **ДЗ.У3.** Самостійно проводити експериментальні дослідження в предметній області згідно обраної наукової тематики. **ДЗ.У4.** Застосувати принципи забезпечення безпеки інформації: збереження конфіденційності, цілісності та доступності.	участі працівників щодо проведення кібердосліджень. **ДЗ.К2.** Розроблювати критерії оцінювання працівників щодо проведення кібердосліджень. **ДЗ.К3**. Брати участь у розробленні правил оцінювання працівників щодо проведення кібердосліджень.	проведення кібердосліджень, підвищення їх ефективності та результативності.
	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 практиці результатів кібердосліджень.				
Е. Проведення фундаменталь-них та прикладних	**Е1.** Здатність аналізувати та оцінювати існуючі та перспективні технології,	**Е1.З1** Сучасні методи проведення досліджень у сфері кібербезпеки.	**Е1.У1** Шукати, оброблювати та аналізувати.	**Е.К1** Допомагати стейхолдерам у розробці інноваційних рішень,	**Е.В1** Обирати та застосовувати фреймворки, методи, стандарти,

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
досліджень програмного забезпечення та систем, сприяння впровадженню інновацій у сфері забезпечення кібербезпеки.	рішення, розробки, процеси кібербезпеки.	**Е1.З2.** Методи та системи штучного інтелекту, та шляхи їх використання при вирішенні профільних задачах. **Е1.З3** Методики, методи аналізу та оцінювання технологій, рішень, розробок та процесів кібербезпеки. **Е1.З4** Методики, методи визначення міжгалузевих досягнень кібербезпеки та порядок їх застосування в залежності від контенту або інноваційних підходів та рішень.	інформацію з різних джерел **Е1.У2** Проводити експерименти та готувати докази концепції, "пілотів" і прототипів рішення з кібербезпеки. **Е1.У3** Відслідковувати тенденції й напрями розвитку інформаційної та кібербезпеки, а також суміжних прикладних областей. **Е1.У3.** Використовувати методи фундаментальних і прикладних дисциплін для опрацювання, аналізу й синтезу результатів досліджень. **Е1.У4.** Ефективно здійснювати пошук	пов’язаних з кібербезпекою.	інструменти та протоколи, включаючи створення та тестування концепції для підтримки проектів.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
			та аналіз інформації з різних джерел. **Е1.У5** Проводити дослідження інновації та розробок кібербезпеки. **Е1.У6** Проводити оцінювання результатів кібердосліджень.		
	Е2. Здатність впроваджувати нові технології, рішення, розробки, процеси кібербезпеки.	**Е2.З1**. Концепції і протоколи комп'ютерних мереж, а також методологію забезпечення безпеки мереж. **Е2.З2**. Технології віртуалізації, формування віртуальних машин та їх технічної підтримки. **Е2.З3.** Зовнішні організації і наукові установи, діяльність яких спрямована на дослідження кіберпростору. **Е2.З4.** Технологічні вимоги до науково-технічної та іншої	**Е2.У1** Ефективно поєднувати теорію і практику, задля вирішення науково-прикладних завдань в сфері кібербезпеки з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів. **Е2.У2.** Приймати обґрунтовані рішення, бути здатним їх оцінювати та забезпечувати	**Е2.К1** Обґрунтовувати вибір методів розв'язання науково-прикладних задач та критично оцінювати отримані результати, аргументовано захищаючи прийняті рішення.	**Е2.В1** Проєктувати, розроблювати та модифікувати програмні системи, використовуючи науковий аналіз та математичні моделі для прогнозування та вимірювання результатів та наслідків проєкту.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		дослідницької документації відповідного спрямування. **Е2.З5.** Як планувати та організовувати виконання проєктів управління знаннями.	якість виконуваних робіт. **Е2.У3.** Самостійно досліджувати предметну область згідно обраної наукової тематики.		
	Е3. Здатність очолювати або брати участь в інноваційних процесах і проєктах у сфері забезпечення кібербезпеки.	**Е3.З1** Як використовувати науково-дослідні центри, аналітичні центри, наукові дослідження та промислові системи.	**Е3.З1** Ефективно працювати як індивідуально, так і у складі команди. **Е3.З2** Досліджувати сучасні технології щоб зрозуміти можливості необхідної системи або мережі.	**Е3.К1.** Готовність до проблемно-орієнтованого професійного спілкування.	**Е3.В1.** Керувати та формувати задання для програмістів, проектувальників, технологів і техніків, а також іншому інженерному та науковому персоналу.
	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 практиці результатів кібердосліджень.				
Є. Формування нових гіпотез, теорій, моделей забезпечення	**Є1.** Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють	**Є1.З1.** Розуміння принципів функціонування систем і засобів	**Є1.У1** Досягати розвитку та вдосконалення існуючих рішень,	**Є1.К1.** Вести профільні дискусії і полеміки, здійснювати	**Є1.В1** Проводити наукові дослідження, отримувати та формалізовувати

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
кібербезпеки та розробка, стандартів, методів (методик) їх реалізації, консультування, популяризація та оцінювання відповідних результатів.	нові знання у сфері кібербезпеки.	криптографічного, стеганографічного та технічного захисту інформації, а також систем управління інформаційною безпекою. **Є1.32.** Порядок розроблення стратегій зменшення ризиків для усунення вразливостей та розроблення відповідних рекомендацій. **Є1.33.** Принципи управління життєвим циклом системи, включаючи забезпечення безпеки та експлуатаційної придатності програмного забезпечення.	генерації нових ідей, ефективно застосовувати методи аналізу, математичного моделювання, виконувати натурні та математичні експерименти при проведенні наукових досліджень. **Є.У2** Використовувати методи штучного інтелекту для задач кібербезпеки та глибоке розуміння їх математичного апарату. **Є.У3** Інтегрувати знання з різних дисциплін, застосовувати системний підхід та враховувати нетехнічні аспекти при розв’язанні інженерних задач та проведенні досліджень.	публічні промови, робити повідомлення і доповіді з питань дисертаційного дослідження, аргументовано викладати власну точку зору.	нові знання у галузі кібербезпеки.

Трудові функції	Компетентності	Результати навчання			
		Знання	Уміння/навички	Комунікація	Відповідальність і автономія
			Є.У4. Досліджувати проблеми кібербезпеки критичної інфраструктури. **Є.У5.** Системно мислити та застосовувати творчі здібності до формування принципово нових ідей**.**		

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	Є2. Здатність презентувати та обговорювати результати наукових досліджень та/або інноваційних розробок.	**Є2.З1** Порядок оцінювання систем кіберзахисту і вразливостей, а також їх можливостей. **Є2.З2** Архітектурні концепції та загальні принципи ІТ. **Є2.З3** Вимоги в рамках загальних принципів управління ризиками. **Є2.З4** Розділи математики (наприклад, логарифми, тригонометрію, лінійну алгебру, математичний аналіз, статистику і операційноий аналіз). **Є2.З5**. Нові та ті, що розроблюються, технологій інформаційної та кібербезпеки. **Є2.З6.** Сучасні і перспективні кібертехнології. **Є2.З7.** Фундаментальні кіберконцепції, принципи, обмеження і ефекти.	**Є2.У1** Здатність здійснювати науково-педагогічну діяльність **Є2.У2** Вміти синтезувати науково обґрунтовані рішення щодо кібербезпеки.	**Є2.К1** Допомогати стейкхолдерам в розбудові потенціалу, пов’язаного з кібербезпекою, включаючи підвищення обізнаності, теоретичне навчання, практичне навчання, тестування, наставництво, супервізія та обмін інформацією.	**Є2.В1** Публікувати та презентувати наукові праці та результати досліджень і розробок.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		Є2.38. Стратегії досліджень та управління знаннями. **Є2.39.** Нормативні документи і правила, що забезпечують захист авторських прав, патентування, винаходів.			

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	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 практиці 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 із кібердосліджень та розробок систем безпеки	Професіонал з кібердосліджень та розробок систем безпеки
	повна	повна	повна
А	+	+	+
Б	+	+	+
В	+	+	+
Г	+	+	+
Д	-	+	+
Е	-	-	+
Ж	-	-	+

VII. Відомості про розроблення та затвердження професійного стандарту

1. Повне найменування розробника професійного стандарту

Державної служби спеціального зв'язку та захисту інформації України

2. Склад робочої групи/Учасники робочої групи:

Бакалинський Олександр Олегович, заступник директора департаменту-начальник 2 відділу Департаменту кіберзахисту Адміністрації Держспецзв'язку;

Безштанько Віталій Михайлович, головний спеціаліст 5 відділу Департаменту кіберзахисту Адміністрації Держспецзв'язку;

Бондаренко Іван Дмитрович, доцент кафедри кібербезпеки Науково-навчального інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України;

Гахов Сергій Олександрович, доцент кафедри інформаційної та кібернетичної безпеки, Навчально-науковий інститут захисту інформації, Державний університет телекомунікацій;

Даков Сергій Юрійович, провідний науковий співробітник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

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

Дідусенко Світлана Миколаївна, начальник відділу управління освітньої діяльності Департаменту освіти, науки та спорту Міністерства внутрішніх справ України;

Котетунов Віктор Юрійович, провідний науковий співробітник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

Лазарько Артем Анатолійович, заступник начальника відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

Ліпінський Вадим Володимирович, провідний фахівець сфери захисту інформації відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

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

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

Маковець Сергій Валентинович, директор з технологій ТОВ «ІНФОРМЕЙШН СІСТЕМС СЕК'ЮРІТІ ПАРТНЕРС»;

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

Мохор Володимир Володимирович, директор Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України;

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

Проскуровський Роман Васильович, заступник керівника Центру кіберзахисту Національного банку України;

Толюпа Сергій Васильович, професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка;

Трегубенко Ірина Борисівна, провідний науковий співробітник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

Штомпель Тетяна Миколаївна, віцепрезидент компанії ТОВ «ТЕКЕКСПЕРТ», керівник навчального Центру «Мережні технології»;

Шестаков Валерій Іванович, заступник директора (з навчальної та наукової роботи) Науково-навчального інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України;

Харченко В'ячеслав Сергійович, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Жуковського;

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

3. Назва та реквізити документа, яким затверджено професійний стандарт

(рішення (може оформлюватися протоколом), наказ, розпорядження).

4. 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.