Проєкт

Професійний стандарт

КОНСТРУКТОР СИСТЕМ КІБЕРБЕЗПЕКИ

_____(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

Конструктор систем кібербезпеки

ІІ. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

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

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

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

				Клас 62.03	Діяльність із керування комп'ютерним устаткуванням
				Клас 62.09	Інша діяльність у сфері інформаційних технологій і комп'ютерних систем
		Розділ 63	Надання інформаційних послуг	**Група 63.1**	Оброблення даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність; веб-портали
				Клас 63.11	Оброблення даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність
				Клас 63.12	Веб-портали
Секція M	Професійна, наукова та технічна діяльність	**Розділ 74**	Інша професійна, наукова та технічна діяльність	**Група 74.9**	Інша професійна, наукова та технічна діяльність, не введенні в інші угрупування
				Клас 74.90	Інша професійна, наукова та технічна діяльність, не введенні в інші угрупування
Секція P	Освіта	**Розділ 85**	Освіта	**Група 85.5**	Інші види освіти
				Клас 85.59	Інші види освіти, не введенні в інші угрупування

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

Конструктор систем кібербезпеки 2132.2

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

Конструктор систем кібербезпеки, 7 рівень НРК

Провідний конструктор систем кібербезпеки, 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 конструювання 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 конструювання 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 конструювання 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**
Конструктор систем кібербезпеки, провідний конструктор систем кібербезпеки	Підготовка на другому рівні вищої освіти (магістерському) за спеціальностями вказаними у п.5, галузі знань 12 «Інформаційні технології» та 17 «Електроніка та 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**
Конструктор систем кібербезпеки	Підвищення кваліфікації для конструктора систем кіберзахисту для отримання професійної кваліфікації "провідний конструктор систем кібербезпеки". Стаж роботи не менше двох років	

IV. Абревіатури, скорочення

ІТ	інформаційні технології

V. Опис трудових функцій

Трудові функ	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
А. Проведення аналізу та технічних розрахунків під час роботи з документацією із проєктування/ моделювання систем кібер-захисту	**А1**. Здатність підбирати, систематизувати й аналізувати доступну конструкторську документацію, зокрема інших підприємств/організацій, з метою її використання в процесі проєктування та моделювання систем кіберзахисту	**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.** Аналізувати запропоновані архітектури, розподіляти послуги безпеки і обирати механізми безпеки (Т0307) **А1.У3**. Збирати точні та повні дані з джерел, які використовуються	**А1.К1.** Адаптувати технічну інформацію для конструювання до рівня розуміння користувача/споживача / замовника	**А1.В1**. Інтерпретувати та застосовувати закони, нормативні акти, політики, стандарти чи процедури до конкретних питань (Т0131) **А1.В2**. Оцінювати і проєктувати функції управління безпекою, пов'язані з кіберпростором (Т0556)

		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 моделоювання систем кіберзахисту	при моделюванні систем кіберзахисту **А1.У4**. Здійснювати моніторинг змін у нормативно-правових документах відповідного спрямування **А1.У5.** Формувати й оновлювати базу знайдених матеріалів для подальшого її використання в роботі **А1.У7.** Застосовувати методи, стандарти та методики для опису, аналізу та документування архітектури корпоративної інформаційної технології організації (The Open Group Architecture Framework, Department of Defense Architecture		

		А1.310. Технологічні вимоги до 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/моделювання систем кіберзахисту **А1.314**. Класифікацію кіберзагроз та вразливостей (К0005) **А1.315**. Операційні наслідки в результаті помилок кібербезпеки (К0006) **А1.316**. Методи автентифікації, авторизації та	Framework, Federal Framework Architecture Framework тощо) (А0008)		

		контролю доступу (К0007) **А1.317**. Прикладні бізнес- процеси і функції в організації/підприємстві –замовнику (К0008) **А1.318**. Вразливості прикладних приграм (К0009) **А1.319**. Методи, принципи і концепції комунікацій, які підтримують інфраструктуру мережі (К0010) **А1.320**. Спроможності та прикладні програми мережевого обладнання, включаючи маршрутизатори, комутатори, мости, сервери, засоби передачі і відповідне технічне обладнання (К0011) **А1.321**. Методи аналізу спроможностей і вимог (К0012) **А1.322.** Класифікацію оцінок систем			

		кіберзахисту і вразливостей, а також їх можливостей (К0013) **А1.З23**. Нові та виникаючі інформаційні технології та технології кібербезпеки **А1.З24.** Основні концепції управління безпекою (управління версіями, патч-менеджмент тощо) (К0074)			
	А2. Здатність проводити технічні розрахунки в процесі проєктування/ моделювання систем кіберзахисту, техніко-економічний і функціонально-вартісний аналіз їх ефективності	**А2.З1.** Принципи управління життєвим циклом системи кіберзахисту, включаючи забезпечення безпеки та експлуатаційної придатності програмного забезпечення **А2.З2**. Методики управління ризиками в ланцюжку постачання **А2.З3**. Політики, вимоги і процедури безпеки ланцюжка постачання	**А2.У1**. Здійснювати комплексний аналіз відповідності змісту програм, процесів і вимог щодо архітектури систем кіберзахисту встановленим стандартам та регламентам **А2.У2**. Читати й аналізувати схеми й креслення, конструкторську, технологічну та іншу документацію	**А2.К1.** Формувати запити на профільну інформацію (Т0707) **А2.К2**. Аналізувати потреби та вимоги користувачів для планування архітектури (Т0427)	**А2.В1.** Проводити оцінювання ефективності існуючих програм, процесів і вимог щодо архітектури систем кіберзахисту

		інформаційних технологій та управління ризиками ланцюжка постачання **А2.З4** Методики зворотного інжинірингу технічного обладнання **А2.З5** Проміжне програмне забезпечення (шини обслуговування організації і черги повідомлень тощо) (**А2.З6** Мережеві протоколи **А2.З7** Методики зворотного інжинірингу програмного забезпечення **А2.З8** Схеми розширеної мови розмітки (XML) **А2.У9**. Стандарти й технічні умови, які використовуються під час проєктування/моделювання систем кіберзахисту	відповідного спрямування **А2.У3.** Працювати з електронними архівами стандартів і технічних умов, які використовуються під час роботи **А2.У4**. Виконувати розрахунки технічних, техніко-економічних і функціонально-вартісних показників моделей систем кіберзахисту, що проєктуються про закупівлі (Т0203)		

		А2.З10. Комп'ютерні алгоритми (К0015) **А2.З11.** Алгоритми шифрування (К0018) **А2.З12.** Концепції криптографії та управління криптографічними ключами (К0019)			
	А3. Здатність застосовувати на практиці загальні теоретично-методологічні знання відповідного спрямування	**А3.З1.** Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи (прикладна система ешелонованого захисту тощо) **А3.З2.** Закони, політики, процедури чи корпоративне управління, що стосуються кібербезпеки критичної інфраструктури (К0267) **А3.З3.** Архітектуру систем мобільного зв'язку (К0269)	**А3.У1.** Надавати визначення та здійснювати опис експериментальних методів дослідження структурних, фізико-механічних і технологічних властивостей матеріалів та компонентів кіберпродукції **А3.У2.** Визначати стратегії кіберможливостей для розробки програмно-апаратних	**А3.К1.** Формувати запити на профільну інформацію (Т0707)	**А3.В1.** Проєктувати архітектури та загальні принципи (А0061)

		А3.33. Структуру та властивості операційної системи (управління процесами, структура каталогів, встановлених застосунків тощо) (К0271) **А334.** Експериментальні методології розроблення кіберпродуктів **А335.** Основні проблеми й методи **А336.** Основні аспекти проєктування кіберпродукції **А337.** Методи та ризики, пов'язані з вибором компонентів кіберпродукції **А3.38**. Системи баз даних (К0024) **А3.39**. Правила безперервності бізнесу та операційних планів відновлення безперервності після катастроф (К0026) **А3.310.** Корпоративну архітектуру	комплексів для замовника, ґрунтуючись на вимогах місії **А3.У3.** Застосовувати сучасні методи проєктування та моделювання систем кіберзахисту **А3.У4.** Пояснювати особливості конструкції та основні аспекти робочих процесів у компонентах нових моделей систем кіберхахисту		

		інформаційної безпеки організації/підприємства (К0027) **А3.З11.** Окремі розділи математики (логарифмів, тригонометрії, лінійної алгебри, математичного аналізу, статистики і операційного аналізу) (К0052) **А3.З12.** Концепції технології віддаленого доступу (К0071) **А3.З13.**Технологію побудови програмного забезпечення (К0082)			
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				
Б.	**Б1**. Здатність розроблювати технічні і робочі проєкти/ моделі систем кібер-	**Б1.З1**. Електротехніку, яка використовується в архітектурі комп'ютера (друковані плати, процесори, мікросхеми	**Б1.У1**. Визначати та пріоритезувати суттєві спроможності систем або бізнес-	**Б1.К1.** Розроблювати вказівки і настанови для працівників, залучених до конструювання систем кібербезпеки	**Б1.В1**. Розроблювати технічну документацію

	захисту особливо складної, складної і середньої складності та відповідної допоміжної документації використанням комп'ютерно-інтегрованих технологій	та технічне забезпечення) (К0030) **Б1.З2.** Процедури інсталяції, інтеграції та оптимізації компонентів системи (К0035) **Б1.З3.** Принципів взаємодії людина-комп'ютер (К0036) **Б1.З4.** Процес оцінки стану безпеки і процесу авторизації (К0037) **Б1.З5.** Мікропроцесори (К0055) **Б1.З6.** Управління мережевим доступом, ідентифікацією, та доступом (інфраструктура відкритих ключів, автентифікація об'єктів, відкриті ідентифікатори, мова розмітки для контролю захищеності, мова розмітки для надання послуг тощо) (К0056) **Б1.З7.** Обладнання та функції апаратного забезпечення мереж (К0057)	функцій, необхідних для часткового або повного відновлення системи після її повної відмови (Т0050) **Б1.У2.** Розроблювати умови системи безпеки, попередню концепцію проведення операцій з кібербезпеки (CONOPS), і визначати основні вимоги системи безпеки відповідно до прийнятних вимог кібербезпеки (Т0314) **Б1.У3.** Розроблювати компоненти архітектури або системних компонент підприємства, необхідних для задоволення потреб		відповідного спрямування

		Б1.З8. Процес планування захисту програм (політика безпеки ланцюжків постачання інформаційних технологій/ політика управління ризиками, методи боротьби з підробками та вимоги тощо) (К0264) **Б1.З9.** Концепції і моделі ІТ архітектури організації/підприємства (базовий рівень, затверджений дизайн, цільові архітектури) (К0291) **Б1.З10.** Порядок інтеграції цілей і завдань організації/підприємства в архітектуру (К0293) **Б1.З11.** Мережеві протоколи (TCP/IP, динамічного конфігурування вузлів, системи доменних імен (DNS) і послуг, що надаються службою	користувачів (Т0448) **Б1.У4.** Розроблювати багаторівневі рішення безпеки/міждоменних рішень (S0116)		

		каталогів тощо) (К0332) **Б1.З12.** Процеси проєктування мереж, включаючи розуміння цілей системи безпеки, операційних цілей та компромісів (К0333)			
	Б2. Здатність застосовувати в конструкторській засоби автоматизації проєктування/ моделювання, передовий розроблення/інтеграції конкурентоспроможних систем кіберзахисту	**Б2.З1.** Спроможності, прикладні програми і потенційні вразливості мережевого обладнання, включаючи концентратори, маршрутизатори, комутатори, мости, сервери, носії передачі і супутнє апаратне обладнання **Б2.З2.** Порядок оформлення технічного завдання на роботи з проєктування та моделювання систем кіберзахисту **Б2.З3.** Операційні системи (К0060) **Б2.З4.** Теорію управління потоками в мережах (протокол управління передачею	**Б2.У1.** Використовувати наукові підходи і методики при вирішенні проблем у моделюванні систем кіберзахисту **Б2.У2**. Застосовувати в практичній діяльності процеси технічної розробки систем **Б2.У3.** Застосовувати у практичній діяльності стандарти і процедури життєвого циклу програмного забезпечення і інженерії систем	**Б2.К1.** Розроблювати вказівки і настанови для працівників, залучених до конструювання систем кібербезпеки	**Б2.В1.** Розроблювати і застосовувати в моделюванні систем кіберзахисту технології, що стосуються кібербезпеки, математичні або статистичні моделі

		(TCP), протокол міжмережевого обміну даними (IP), модель взаємодії відкритих систем (OSI), бібліотека інфраструктури інформаційних технологій, поточної версії тощо) (K0061) **Б2.З5.** Концепції паралельних і розподілених обчислень (K0063) **Б2.З6.** Методи тестування та оцінки систем (K0091) **Б2.З7.** Процеси інтеграції технологій (K0092) **Б2.З8.** Концепції телекомунікацій (комунікаційні канали, бюджетування системних каналів зв'язку, спектральна ефективність, мультиплексування тощо) (K0093) **Б2.З9.** Технологічні процеси систем (K0102)	**Б2.У4.** Документувати та оновлювати за необхідності усі напрямки діяльності, пов'язані із визначенням архітектури (T0473) **Б2.У5.** Використовувати моделі системи безпеки (наприклад, модель Белла-Лападули, моделі забезпечення цілісності «Biba» і Кларка-Вілсона) (S0139)		

		Б2.З10. Методи автентифікації доступу (К0336)			
	Б3. Здатність забезпечувати в процесі проєктування/ моделювання систем кіберзахисту відповідність розроблюваних моделей, схем та компонентів технічним завданням, стандартам, нормам охорони праці, вимогам найбільш економної технології виробництва та експлуатації	**Б3.З1.** Номенклатуру інструментів для сегментування мереж **Б3.З2.** Технічну документацію відповідного спрямування **Б3.З3**. Інженерні концепції, що застосовуються до комп'ютерної архітектури і відповідного комп'ютерного обладнання/програмного забезпечення **Б3.З4.** Вимоги системи забезпечення якості **Б3.З5.** Принципи, інструменти та методики тестування на проникнення **Б3.З6.** Безпеку технологічних операцій	**Б3.У1.** Розроблювати/інтегрувати проєкти з кібербезпеки для систем та мереж із багаторівневими вимогами безпеки або вимогами для обробки кількох рівнів класифікації даних, що застосовуються головним чином до державних організацій (наприклад, некваліфіковані, таємні та особливої важливості)(Т0071) **Б3.У2.** Застосовувати та інтегровувати інформаційні технології до запропонованих рішень (S0005)	**Б3.К1.** Ураховувати в обґрунтованому обсязі вимоги керівництва організації під час періодичного перегляду та вдосконалення розвитку конструкторської діяльності в організації	**Б1.В1**. Розроблювати технічну документацію відповідного спрямування

		Б3.З7. Системи критичної інфраструктури з інформаційно-комунікаційними технологіями, які були розроблені без розгляду безпеки системи (К0170) **Б3.З8.** Принципи, моделі, інструменти та методи управління мережевими системами (наскрізний моніторинг продуктивності систем тощо) (К0180) **Б3.З9**. Загальні мережеві протоколи та протоколи маршрутизації (TCP/IP тощо), послуг (веб-пошта, DNS тощо) та їх взаємодію для забезпечення мережевих зв'язків (К0565)	**Б3.У3.** Застосовувати безпечні методи кодування **Б3.У4.** Документувати та приводити у відповідність інформаційну безпеку організації, архітектуру кібербезпеки та вимоги техніки безпеки системи протягом всього життєвого циклу закупівлі(Т0082) **Б3.У5.** Писати детальні функціональні специфікації, які документують процес розробки архітектури (Т0338) **Б3.У6**. Застосовувати принципи кібербезпеки і приватності при формуванні організаційних вимог (які		

			стосуються конфіденційності, цілісності, доступності, автентифікації і неспростовності) (S0367) **Б3.У7**. Застосовувати концепції архітектури безпеки мереж, включаючи топологію, протоколи, компоненти і принципи (застосунки з «ешелонованим захистом тощо) (A0048) **Б3.У8.** Застосовувати інструменти, методи і техніки розробки безпечних систем (A0049) **Б3.У10**. Засто-совувати інстру-менти, методи і техніки проєк-		

			тування систем, включаючи інструменти автоматизованого аналізу та проєктування систем (А0050)		
	Б4. Здатність застосовувати під час проєктування/ моделювання систем кіберзахисту стандартизовані й уніфіковані програми, компоненти та операційні процедури	**Б4.З1**. Принципи і методи аналізу прийнятих в галузевих стандартах або в організації/підприємстві (К0044) **Б4.З2.** Принципи і методи кібербезпеки та приватності, а також організаційні вимоги (щодо забезпечення конфіденційності, цілісності, доступності, автентифікації і неспростовності тощо) (К0044) **Б4.З3.** Концепції вдосконалення процесів організації та моделей зрілості процесів (Capability Maturity Model	**Б4.У1.** Визначити відповідні рівні доступності системи на основі критичних функцій системи та переконатися, що системні вимоги визначають відповідні вимоги відновлення після аварії та безперервність операцій, включаючи будь-які відповідні вимоги щодо аварійного переходу /альтернативного сайту, вимоги до резервного копіювання та	**Б4.К1.** Надавати керівництву пояснення методології з конструювання систем безпеки	**Б4.В1.** Рекомендувати зміни та доповнення кіберполітики організації, приймати участь у координації її перегляду (Т0227) **Б4.В2**. Проводити оптимізацію системи відповідно до вимог продуктивності

		Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions тощо) (K0198) **Б4.З4.** Концепції управління послугами для мереж і в відповідних стандартах (бібліотека інфраструктури інформаційних технологій, поточна версія) (K0200) **Б4.З5.** Концепції і функції прикладних програм мережевих екранів (єдиної точки автентифікації/аудиту/ реалізації політики, сканування повідомлень на наявність шкідливого вмісту, знеособлення даних з метою задоволення вимог стандартів PCI та DII, сканування захисту від втрати даних, прискорених криптографічних операцій, протокол	вимоги до забезпечення матеріальної підтримки для відновлення/ реставрації системи (T0051) **Б4.У2.** Застосовувати процеси управління безпечною конфігурацією (T0084) **Б4.У3.** Оцінювати архітектури і проекти безпеки для визначення адекватності проекту та архітектури безпеки, які були запропоновані або надані відповідно до вимог, що містяться в документах про придбання (T0328) **Б4.У4.** Визначати необхідний рівень складності тесту для конкретної системи (S0026)		підприємства (A0038)

		захисту інформації SSL, REST/JSON-обробка) (К0202) **Б4.З6.** Вимоги до конфіденційності, цілісності та доступності (К02011) **Б4.З7.** Програмне забезпечення з підтримки кібербезпеки (К0212) **Б4.З8.** Методологія оцінки загальних принципів управління ризиками (К0214) **Б4.З9.** Різні типи комп'ютерної архітектури (К0227) **Б4.З10.** Багаторівневі системи безпеки та рішень для захищеного інформаційного обміну між доменами (К0240) **Б4.З11.** Стандарти безпеки персональних ідентифікаційних даних (PII) (К0260) **Б4.З12.** Стандарти безпеки даних в сфері платіжних карт (PCI) (К0261)	**Б4.У5.** Визначати, як буде функціонувати система безпеки (включаючи її властивості відмовостійкості і надійності), та як зміни умов, операцій або середовища вплинуть на ці результати (S0027) **Б4.У6.** Моделювати проєкти і побудову сценаріїв їх використання (наприклад, універсальна мова моделювання) (S0050) **Б4.У7.** Використовувати пристрої віртуальних приватних мереж (VPN) і шифрування (S0059) **Б4.У8.** Готувати плани проведення тестування(S0061)		

		Б4.З13. Стандарти безпеки медичних персональних даних (PHI) (K0262)	**Б4.У9.** Створювати фізичні або логічні підмережі, які відокремлюють внутрішню локальну мережу (LAN) від інших ненадійних мереж (S0168)		
	Б5. Здатність погоджувати проєкти/моделі систем кіберзахисту, що розроблюються, з іншими структурними підрозділами організації, представниками замовника та/чи органів державного нагляду	**Б5.З1.** Технології виробництва, комунікації та розповсюдження медійних повідомлень, а також альтернативні способи інформування за допомогою текстових, мовних, візуальних повідомлень **Б5.З2**. Відповідні концепції, процедури, програмне забезпечення, обладнання і прикладні технологічні програми які застосовуються для співпраці із зацікавленими сторонами	**Б5.У1.** Переконатися, що придбані або розроблені система (и) та архітектура (и) відповідають настановам з архітектури кібербезпеки в організації (T0090) **Б5.У2.** Ідентифікувати та надавати перевагу критичним бізнес-функціям у співпраці з зацікавленими сторонами організації (T0108) **Б5.У3**. Відображати отримані результати в оригінальних форматах	**Б5.К1.** Взаємодіяти з керівниками організації різних рівнів, із представниками зацікавлених сторін стосовно організації, проведення та результатів моделювання систем кіберзахисту **Б5.К2.** Проводити робочі зустрічі з партнерами за всім спектром питань розроблення нових моделей систем кіберзахисту **Б5.К3.** Здійснювати зворотній зв'язок з партнерами, підрядниками профільних проєктних робіт	**Б1.В1**. Розроблювати технічну документацію відповідного спрямування **Б5.В2.** Консультувати посадових осіб, директорів з ІТ, директорів з інформаційної безпеки та відповідальну посадову особу з

		Б5.З3. Методи і способи ефективної комунікації **Б5.З4.** Основні бізнес-процеси і місію організації **Б5.З5**. Порядок застосування в роботі оригінальних форматів відображення інформації **Б5.З6**. Внутрішніх і зовнішніх замовників та партнерських організацій, включаючи їх інформаційні потреби, цілі, структури, можливості тощо (К0376)	**Б5.У4.** Розроблювати настанови стосовно впровадження розроблених моделей систем клієнтам або командам впровадження **Б5.У8.** Виявляти проблеми кібербезпеки і захисту приватності, які виникають при з'єднаннях внутрішніх та зовнішніх замовників та організацій-партнерів (S0374) **Б5.У9.** Використовувати цілі і завдання організації/ підприємства при розробці і підтримці архітектури (А0027) **Б5.У10**. Виступати основною сполучною ланкою		управління ризиками щодо питань безпеки (встановлення периметру системи, оцінки ступеня слабкості та недоліків у системі, дій і контрольних підходів до виявлених вразливостей (А0149)

			між головним конструктором підприємства та інженером систем безпеки та співпрацювати з власниками систем, постачальниками загальних контролів та працівниками системи безпеки щодо розподілу контролів безпеки на системні, гібридні або загальні контролі (A0148)		
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відпов програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових нау журналів (EBSCO, JSTOR) відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабор приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				
B. Проведення робіт з випробування, експлуатації, удосконалення, модернізації	**B1.** Здатність проводити розрахунки ризиків при розробленні нових моделей систем кіберзахисту	**B1.З1.** Класифікацію вразливостей при експлуатації систем безпеки **B1.З2**. Порядок усунення проблем при проєктуванні/моделюванні систем кіберзахисту та	**B1.У1**. Виконувати аналіз системи безпеки, визначати пробіли в архітектурі безпеки і розробляти план управління ризиками (T0177)	**B1.К1**. Надавати (доводити до відома) технічну інформацію різним категоріям користувачів **B1.К2.** Встановлювати ефективний зворотний зв'язок з користувачами	**B1.В1.** Налаштовувати і використовувати у конструкторській діяльності програмні

та уні- фікації конструйованих моделей систем кібер- захисту		усунення вразливостей при експлуатації систем безпеки **В1.З3.** Компоненти системи мережевої безпеки (мережеві екрани, віртуальні приватні мережі, системи виявлення вторгнень тощо) **В1.З4.** Методики управління конфігураціями (К0275) **В1.З5.** Сучасні і перспективні засоби шифрування (система шифрування стовпців і таблиць, шифрування файлів і дисків тощо) в базах даних (вбудовані функції управління криптографічними ключами тощо**)** (К0277) **В1.З6.** Багаторівневі типології (включаючи ОС сервера і клієнта) (К0286) **В1.З7.** Застосовувана в організації/ підприємстві програма класифікації	**В1.У2.** Використовувати у процесі роботи віртуальні машини **В1.У3**. Конфігурувати і використовувати у процесі проєктування/ моделювання компоненти системи мережевої безпеки **В1.У4**. Використовувати сучасні та новітні технології у процесі проєктування/ моделювання **В1.У5**. Надавати вхідні дані для діяльності процесу загальних принципів управління ризиками та відповідну документацію (плани забезпечення життєвого циклу системи, концепція операцій,	профільних послуг та партнерами	засоби захисту комп'ютерів (програмні фільтри, антивірусні програми й антишпигунсь-ке програмне забезпечення)

		інформації і процедур розкриття (К0287)	операційні процедури і навчальні матеріали з технічного обслуговування тощо) (Т0205) **В1.У6**. Визначити потенційні протиріччя, пов'язані з впровадженням будь-яких засобів кіберзахисту (тестування та оптимізація інструментів і підписів тощо) (Т0484) **В1.У7.** Розроблювати контрзаходи для виявлення ризиків безпеки (S0022) **В1.У8.** Перекладати функціональні вимоги в потреби захисту (контроль безпеки тощо) (S0152) **В1.У9.** Налаштовувати та використовувати		

			компоненти захисту комп'ютера (апаратні брандмауери, сервери, маршрутизатори тощо) у відповідних випадках (S 0170) **В1.У10.** Проводити процедури сканування вразливостей і розпізнавання вразливостей в системах безпеки (А0015) **В1.У11**. Виявляти системи критичної інфраст-руктури з ІТ, які спроєктовані без урахування безпеки системи (А0170)		
	В2. Здатність брати участь у роботах з уні-	**В2.З1**. Концепції, процедури, програмне забезпечення, обладнання та/або технологічні прикладні	**В2.У1.** Застосовувати концепції, процедури, програмне	**В2.К1.** Сприяти дискусіям у невеликих групах **В2.К2**. Готувати та проводити брифінги з	**В2.В1** Керувати різними систе-

	фікації конструювання/моделювання систем кіберзахисту та їх компонентів	програми, необхідні для визначення функціональних властивостей і властивостей, пов'язаних із забезпеченням безпеки **В2.32.** Теорію інформації (кодування джерела, канальне кодування, теорія складності алгоритмів і стиснення даних тощо) (К0325) **В2.33.** Демілітаризовані зони (К0326) **В2.34.** Системи і методами електронної комунікації (електронна пошта, VOIP, IM (миттєві повідомлення), Web-форуми, Direct Video Broadcasts) **В2.35**. Класифікацію системних проблем безпеки **В2.36**. Критерії оцінки та підтвердження автентичності,	забезпечення, обладнання та/або технологічні прикладні програми під час визначення функціональних властивостей і властивостей, пов'язаних із забезпеченням безпеки **В2.У2.** Користуватися загальнодоступ-ними мережевими інструментами **В2.У3.** Використовувати командний рядок операційної системи **В2.У4.** Проєктувати інтеграції апаратних і програмних рішень (S0024) **В2.У5.** Керувати різними системами і методами електронної комунікації **В2.У6.** Визначати і документувати те,	обізнаності з конструкторською діяльністю керівництву, персоналу і користувачам	мами і методами елек-тронної кому-нікації (електронна пошта, VOIP, миттєві пові-домлення, форуми, Direct Broadcasts)

		прийнятих в організації (К0320) **В2.37.** Вбудовані системи (К0322) **В2.38.** Методологію відмовостійкості систем (К0323)	як впровадження нових систем або інтерфейсів між системами вплине на стан захищеності діючої інфраструктури (Т0268)		
	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 конструювання; бібліотечні ресурси, архівні матеріали (за потреби); законодавчо-нормативні акти, акти роботодавця відповідного спрямування				
Г. Проведення патентних досліджень, підготовка відгуків і висновків щодо проєктів профільних стандартів, раціоналі ські пропозиції і ви-	**Г1**. Здатність складати заявки на винаходи й промислові зразки моделей систем кіберзахисту	**Г131**. Стандарти й технічні умови, які використовуються під час складання заявок на винаходи й промислові зразки систем кіберзахисту **Г132.** Основи винахідництва щодо конструювання систем кіберзахисту **Г133.** Основи нау технічної, винахідниць раціоналізаторської діял в організаціях/ підприєм	**Г1У1.** Брати участь у розробленні профільних патентних і ліцензійних паспортів **Г1У2**. Готувати замовлення на нове устаткування й заявки на винаходи й промислові зразки відповідного спрямування **Г1У3.** Обґрунтовувати й оцінювати інноваційні проєкти	**Г1.К1**. Готувати та проводити брифінги з обізнаності з патентною діяльністю керівництву, персоналу і користувачам	**Г1.В1**. Оцінювати витрати-вигоду, економічний аналіз та аналіз ризиків у процесі прийняття рішень (Т099) **Г1.В2.** Оцінювати ефективність законів, правил, політик, стандартів чи процедур

находи, пов'язані з моделюванням систем кіберзахисту підприємств/ організацій, задіяних у забезпеченні кібербезпеки		з виробництва с кіберзахисту	у виробництві систем кіберзахисту **Г1У4.** Використовувати сучасні методи виконання винахідницьких завдань, захисту інтелектуальної власності на технічні рішення, створені в процесі професійної діяльності		відповідного спрямування (Т0102)
	Г2. Здатність готувати відгуки й висновки на проєкти стандартів, раціоналізаторські пропозиції й винаходи, які стосуються окремих компонентів нових моделей систем кіберзахисту	**Г23І**. Стандарти й технічні умови, які використовуються під час запровадження на практиці результатів винахідницької й раціоналізаторської діяльності в організаціях/	**Г2У1.** Готувати відгуки й висновки на проєкти стандартів, які стосуються окремих нових елементів систем кіберзахисту **Г2У2.** Готувати відгуки й висновки на раціоналізаторські	**Г1.К1**. Готувати та проводити брифінги з обізнаності з раціоналізаторською діяльністю керівництву, персоналу і користувачам	**Г2.В1**. Розглядати раціоналізаторсь пропозиції вдосконалення технології виробництва систем кіберзахисту

		підприємствах з виробництва систем кіберзахисту **Г232.** Основи науково-технічної, винахідницької раціоналізаторської діяльності в організаціях/ підприємствах з виробництва систем кіберзахисту	пропозиції й винаходи, які стосуються окремих нових елементів систем кіберзахисту **Г2У3**. Брати участь у підготовці висновків про доцільність використання підприємством раціоналізаторських пропозицій щодо вдосконалення технології виробництва систем кіберзахисту		
	Г3. Здатність проводити патентні дослідження у конструювання, моделювання та експлуатації нових систем кіберзахисту	**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.** Основи патентознавства	**Г3.У1**. Проводити патентні дослідження відповідного спрямування **Г3У2**. Проводити розрахунки показників технічного рівня проєктованих об'єктів техніки й технології виробництва нових систем кіберзахисту	**Г3К1.** Брати участь у розробленні профільних патентних і ліцензійних паспортів, замовлень на нове устаткування, заявок на винаходи й промислові зразки нових систем кіберзахисту	**Г3.В1.** Розроблювати стандарти даних, політики та процедури

		Г3.З4. Основи винахідництва щодо конструювання нових систем кіберзахисту **Г3.З5.** Стандарти й технічні умови, які використовуються під час конструювання нових систем кіберзахисту **Г3.З6.** Основи реверс-інжинірингу	**Г3.У3.** Розроблювати архітектури або компоненти системи відповідно до технічних умов **Г3.У4**. Включати рішення щодо вразливості системи у проєкти систем **Г3.У5**. Розроблювати вимоги безпеки для забезпечення виконання вимог для всіх систем або прикладних програм		
	Г4. Здатність визначати показники технічного рівня моделей систем кіберза-хисту, проєктуються/моделюються	**Г4З1.** Характеристики сучасного технологічного обладнання, яке використовується під час створення систем кіберзахисту та їх компонентів **Г4З2.** Технологію створення систем кіберзахисту та їх компонентів	**Г4У1**. Складати технічні вимоги до технологічного обладнання й оснащення, задіяного під час створення систем кіберзахисту та їх компонентів **Г4У2**. Розроблювати техніко-економічне обґрунтування на	**Г4.К1.** Надавати консультації щодо витрат на проєкт, концепцій проєктування або змін в проєкті (Т0196)	**Г4В1**. Склада-ти й погод-жувати внутрішні до-кументи на проєкту-вання й вигo-товлення технологічного

		Г433. Технологічні характеристики сучасного технологічного оснащення, яке використовується при створенні систем кіберзахисту та їх компонентів	придбання/отримання технологічного обладнання й оснащення, задіяного під час створення систем кіберзахисту та їх компонентів **Г4У3**. Складати заявки щодо внесення до плану закупівлі структурним підрозділом технологічного обладнання й оснащення, необхідного для створення систем кіберзахисту та їх компонентів		оснащення, необхідного для створення систем кібер-захисту та їх компонентів
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				
Д. Проведення	**Д1**. Здатність здійснювати	**Д1.З1.** Моделі та симуляції, які	**Д1.У1.** Забезпечувати	**Д1.К1**. Готувати та проводити брифінги	**Д1.В1.** Розроблювати

робіт з адаптації процесів з конструювання систем кіберзахисту до існуючої в організації/ на підприємстві системи менеджменту якості та підвищення загальної ефективності виробництва кіберпродукції та кіберпослуг	технічне керівництво профільними працівниками, заділяними в конструкторській діяльності	застосовуються для аналізу або прогнозування продуктивності системи за різних умов експлуатації **Д1.З2.** Чинні вітчизняні, зарубіжні та міжнародні стратегії мінімізації ризиків для зменшення витрат, графіку, продуктивності і ризиків безпеки	заходи щодо тестування та оцінки систем кіберзахисту та сертифікації **Д1.У2**. Використовувати спеціалізоване обладнання та методики каталогізації, документування, вилучення, збирання, упаковки та зберігання цифрових доказів **Д1.У3**. Використовувати моделі та симуляції для аналізу або прогнозування продуктивності системи кіберзахисту за різних умов експлуатації	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) **Д1.К3.** Розповсюджувати серед профільних працівників структурного підрозділу**,** керівництва та партнерів останні вітчизняні, зарубіжні та міжнародні досягнення щодо розроблення та застосування стандартів і процедур відповідного спрямування	стратегії мінімізації ризиків для зменшення витрат, графіку, продуктивності і ризиків безпеки
	Д2.			**Д1.К1**. Готувати та проводити брифінги відповідного спрямування	**Д2.В1.** Розвивати розуміння потреб та вимог кінцевих

					користувачів інформації (Т0060)
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				

VI. Розподіл трудових функцій та компетентностей за професійними кваліфікаціями

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

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 «конструктор систем кібербезпеки» вимог Порядку розроблення, введення в дію та перегляду професійних стандартів, затвердженого постановою Кабінету Міністрів України від 31.05.2017 р. № 373).

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

Висновок Профспілки працівників зв’язку України від _____ щодо погодження проєкту професійного стандарту «конструктор систем кібербезпеки».

VIII. Дата внесення професійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.