Прим. № __

ЗАТВЕРДЖЕНО

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

ПРОФЕСІЙНИЙ СТАНДАРТ

ФАХІВЕЦЬ З КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

_____

(дата внесення до Реєстру кваліфікацій)

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

висновку суб'єкта перевірки – Національного агентства кваліфікацій від 27 грудня 2023 року про дотримання під час підготовки проєкту професійного стандарту вимог Порядку розроблення, введення в дію та перегляду професійних стандартів, затвердженого постановою Кабінету Міністрів України від 31.05.2017 р. № 373;

висновку Профспілки працівників зв'язку України щодо погодження проєкту професійного стандарту «Фахівець з криптографічного захисту інформації» (лист від 16 листопада 2023 року № 01.2-14/136, постанова Президії Профспілки працівників зв'язку України від 16 листопада 2023 року № П-4-5г).

I. Назва професійного стандарту

Фахівець з криптографічного захисту інформації

II. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Забезпечення криптографічного захисту інформації в інформаційних системах\мережах (або автоматизованих системах, інформаційно-комунікаційних системах, системах електронних комунікацій) на основі перетворень інформації з використанням спеціальних даних (ключових даних) для приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Здійснення оцінки рівня безпеки та контролю стану криптографічного захисту інформації в інформаційних системах\мережах (або автоматизованих системах, інформаційно-комунікаційних системах, системах електронних комунікацій). Дослідження рівня захисту програмних засобів і систем що реалізують криптографічні функції. Супроводження робіт зі створення, впровадження та забезпечення функціонування підсистем криптографічного захисту інформації на всіх етапах життєвого циклу інформаційних систем\мереж в організаціях, підприємствах або установах різних форм власності.

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	Назва секції	№ розділу	Назва розділу	№ групи (класу)	Назва групи (класу)
Секція J	Інформація та телекомунікації	**Розділ 61**	Телекомунікації (електрозв'язок)	**Група 61.1**	Діяльність у сфері проводового електрозв'язку
				Клас 61.10	
				Група 61.2	Діяльність у сфері безпроводового електрозв'язку
				Клас 61.20	
				Група 61.9	Інша діяльність у сфері електрозв'язку
				Клас 61.90	
		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, н.в.і.у
				Клас 74.90	
Секція P	Освіта	**Розділ 85**	Освіта	**Група 85.5**	Інші види освіти
				Клас 85.59	Інші види освіти, не введенні в інші угрупування

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

Фахівець з криптографічного захисту інформації 2139.2.

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

Фахівець з криптографічного захисту інформації (6 рівень НРК).

Провідний фахівець з криптографічного захисту інформації (7 рівень НРК).

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

- документ (диплом, сертифікат, тощо), виданий суб'єктом, уповноваженим законодавством на присвоєння/підтвердження та визнання професійної або часткової професійної кваліфікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у відповідності до професійного стандарту «Фахівець з криптографічного захисту інформації»;
- документ (диплом, сертифікат, тощо), виданий суб'єктом, уповноваженим законодавством на присвоєння/підтвердження та визнання професійної або часткової професійної кваліфікації (щодо професійних кваліфікацій, здобутих у інших країнах)..

III. 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 з криптографічного захисту інформації	Підготовка за спеціальностями, вказаними у **П.*** на першому (бакалаврському) рівні вищої освіти.	*Не передбачено професійним стандартом*
Провідний фахівець з криптографічного захисту інформації	Підготовка за спеціальностями, вказаними у **П.*** на другому (магістерському) рівні вищої освіти за умови наявності стажу роботи за однією з професій відповідного спрямування не менше 3 років.	*Не передбачено професійним стандартом*

П.*

- диплом на першому (бакалаврському) рівні вищої освіти за спеціальністю:

- 111 «Математика» галузі знань 11 «Математика та статистика» (6 рівень НРК);

- 112 «Статистика» галузі знань 11 «Математика та статистика» (6 рівень НРК);

- 113 «Прикладна математика» галузі знань 11 «Математика та статистика» (6 рівень НРК);

- 121 «Інженерія програмного забезпечення» галузі знань 12 «Інформаційні технології» (6 рівень НРК);

- 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології» (6 рівень НРК);

- 123 «Комп'ютерна інженерія» галузі знань 12 «Інформаційні технології» (6 рівень НРК);

- 124 «Системний аналіз» галузі знань 12 «Інформаційні технології» (6 рівень НРК);

- 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» (6 рівень НРК);

- 126 «Інформаційні системи та технології» галузі знань 12 «Інформаційні технології» (6 рівень НРК);

- 254 "Забезпечення військ (сил)" галузі знань 25 "Воєнні науки, національна безпека, безпека державного кордону" (6 рівень НРК);

- 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» (6 рівень НРК).

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

- 111 «Математика» галузі знань 11 «Математика та статистика» (7 рівень НРК);

- 112 «Статистика» галузі знань 11 «Математика та статистика» (7 рівень НРК);

- 113 «Прикладна математика» галузі знань 11 «Математика та статистика» (7 рівень НРК);

- 121 «Інженерія програмного забезпечення» галузі знань 12 «Інформаційні технології» (7 рівень НРК);

- 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології» (7 рівень НРК);

- 123 «Комп'ютерна інженерія» галузі знань 12 «Інформаційні технології» (7 рівень НРК);

- 124 «Системний аналіз» галузі знань 12 «Інформаційні технології» (7 рівень НРК);

- 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» (7 рівень НРК);

- 126 «Інформаційні системи та технології» галузі знань 12 «Інформаційні технології» (7 рівень НРК);

- 254 «Забезпечення військ (сил)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7.рівень НРК)

- 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» (7 рівень НРК);

2. Професійний розвиток

1) з присвоєнням наступної професійної кваліфікації

Назва професійної та/або часткової професійної кваліфікації	**Суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
Фахівець з криптографічного захисту інформації	Підвищення кваліфікації фахівця з криптографічного захисту інформації для отримання професійної кваліфікації провідного фахівця з криптографічного захисту інформації. Стаж роботи за спеціальністю не менше трьох років	*Не передбачено професійним стандартом*

2) без присвоєння наступної професійної кваліфікації

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

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

IV. Абревіатури, скорочення

TCP	Transmission Control Protocol
IP	Internet Protocol
OSI	Open Systems Interconnection
ITIL	Information Technology Infrastructure Library
PL/SQL	Procedural Language / Structured Query Language
TCP/IP	Transmission Control Protocol / Internet Protocol
DNS	Domain Name System
EBSCO	Elton Bryson Stephens Company
JSTOR	Journal Storage
TSCM	Technical Security Counter Measures
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
СУКЗІ	система управління криптографічним захистом інформації
АС	Автоматизована система

ІКС	Інформаційно-комунікаційна система
СЕК	Система електронних комунікацій
ІТ	Інформаційні технології
ІС	Інформаційна система

V. Опис трудових функцій

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
А. Реалізація заходів щодо запровадження в органі (установі, підприємстві, організації) криптографіч-ного захисту інформації	**А1**. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо криптографічного захисту інформації з метою впровадження систем та комплексів захисту інформації	**А1.З1.** Класифікацію інформації, поняття інформації з обмеженим доступом, державних інформаційних ресурсів та інформаційних активів **А1.З2**. Види, криптографічних перетворень інформації, їх сутність та властивості **А1.З3.** Захищені комп'ютерні протоколи, включаючи криптопротоколи **А1.З4**. Вимоги нормативно-правових актів і нормативних документів, що визначають порядок і умови криптографічного захисту інформації **А1.З5**. Принципи, методи та заходи забезпечення кібербезпеки **А1.З6**. Принципи побудови моделей та симуляцій автоматизованих систем і криптосистем, що призначені для аналізу їх	**А1.У1.** Визначати (формулювати) потреби щодо криптографічного захисту інформації на підприємствах, (установах, організаціях) **А1.У2.** Визначати та аналізувати вимоги щодо криптографічного захисту інформації на підприємствах, (установах, організаціях) **А1.У3.** Здійснювати попередню оцінку достатності і коректності вимог і потреб користувачів (замовників) для побудови підсистеми криптографічного захисту інформації з необхідним рівнем безпеки **А1.У4.** Аналізувати потреби та вимоги користувачів з метою планування і проведення	**А1.К1.** Спілкуватися з питань виконання завдань криптографічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **А1.К2** Формувати запити / відповіді в рамках листування з питань криптографічного захисту інформації з державними органами (установами, підприємствами)	**А1.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		вразливостей та прогнозування продуктивності за різних умов експлуатації	розробки системи криптографічної безпеки **А1.У5.** Використовувати моделі та симуляції автоматизованих систем та криптосистем для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації		
	А2. Здатність виявляти, досліджувати (оцінювати), системно аналізувати загрози безпеці криптографічного захисту інформації, аналізувати відповідні ризики безпеки інформації у разі реалізації цих загроз	**А2.З1.** Класифікацію загрози безпеці криптографічного захисту інформації **А2.З2.** Методи (способи) та методики виявлення, дослідження та аналізу загроз безпеці криптографічного захисту інформації **А2.З3.** Вимоги щодо формування моделей загроз та моделі порушника безпеки криптографічного захисту інформації **А2.З4.** Поняття ризиків безпеки інформації та кібербезпеки	**А2.У1.** Виявляти загрози безпеці криптографічного захисту інформації **А2.У2.** Досліджувати (оцінювати) загрози безпеці криптографічного захисту інформації та вразливості автоматизованих систем для розробки функціонального профілю захищеності інформації **А2.У3.** Аналізувати та оцінювати ризики безпеки інформації **А2.У4.** Розробляти моделі загроз та моделі	**А2.К1.** Координувати виконання завдань з криптографічного захисту інформації. **А2.К2** Ефективно співпрацювати з керівниками організації різних рівнів в питаннях захисту інформації.	**А1.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		А2.З5. Класифікацію наслідків для безпеки криптографічного захисту інформації у результаті виникнення кіберінцидентів, дій інсайдерів та помилок персоналу	порушника безпеки криптосистем **А2.У5.** Готувати пропозиції щодо розробки моделі загроз криптосистемам завдяки витоку інформації технічними каналами або внаслідок спеціальних впливів		(установи, організації)
	А3. Здатність аналізувати, розробляти та супроводжувати систему управління безпекою криптографічного захисту інформації на підприємстві (органі, установі)	**А3.З1.** Поняття системи управління безпекою криптографічного захисту на підприємстві (органі, установі) **А3.З2.** Принципи створення систем управління криптографічною безпекою **А3.З3.** Принципи побудови систем криптографічного захисту інформації, що визначені законодавством і стандартами	**А3.У1.** Брати участь у визначенні сфери та меж дії системи управління криптографічним захистом інформації (СУКЗІ) на підприємстві (органі, установі) **А3.У2.** Брати участь у розробці, впровадженні СУКЗІ та забезпеченні її сталого функціонування **А3.У3.** Брати участь у моніторингу стану СУКЗІ та розробці пропозицій щодо її вдосконалення	**А3.К1.** Співпрацювати із зацікавленими сторонами для розробки пропозицій щодо вдосконалення СУКЗІ. **А3.К2** Структурувати інформацію щодо принципів створення та побудови систем криптографічного захисту інформації	**А1.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
	А4. Здатність супроводжувати тематичні дослідження (процеси оцінки відповідності) засобів криптографічного захисту інформації	**А4.З1.** Поняття тематичних досліджень засобів криптографічного захисту інформації **А4.З2.** Архітектуру комп'ютерних систем і мереж, принципи функціонування, класи автоматизованих систем **А4.З3.** Поняття об'єкта інформаційної діяльності **А4.З4.** Поняття стійкості криптосистем та їх інженерно-криптографічних якостей **А4.З5.** Сутність та завдання методики проведення тематичних досліджень засобів криптографічного захисту інформації **А4.З6.** Технічні регламенти, стандарти та нормативні вимоги щодо процедур оцінки відповідності засобів криптографічного захисту інформації **А4.З7.** Математичні основи побудови стійкого шифрування, цифрового	**А4.У1.** Готувати документи (запити, заявки, вихідні дані тощо) для проведення тематичних досліджень (оцінки відповідності) засобів криптографічного захисту інформації **А4.У2.** Використовувати матеріали та звіти за результатами тематичних досліджень (оцінки відповідності) засобів криптографічного захисту інформації для їх раціонального застосування на об'єкті інформаційної діяльності **А4.У3.** Контролювати термін придатності висновків щодо тематичних досліджень (допуску до експлуатації) та оцінки відповідності засобів криптографічного захисту інформації. **А4.У4.** Надавати в необхідних випадка керівництву пропозиції	**А4.К1.** Взаємодіяти з відділами та департаментами для проведення досліджень засобів криптографічного захисту інформації **А4.К2.** Комунікувати з працівниками системи безпеки для розробки регламентів, стандартів та нормативних вимог щодо питань безпеки	**А1.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		підпису, криптопротоколів, систем генерації і тестування ключів та криптоаналізу	щодо укладання договорів на проведення тематичних досліджень (їх окремих складових) та оцінки відповідності засобів криптографічного захисту інформації		
	А5. Здатність опанування (впровадження, інсталяція, налаштування) типовими програмними та апаратними рішеннями (засобами) криптографічного захисту інформації в автоматизованих системах і на об’єктах інформаційної діяльності	**А5.З1.** Поняття криптографічної схеми та основні функції підсистем (модулів) засобу криптографічного захисту **А5.З2.** Принципи і основні вимоги щодо побудови засобів криптографічного захисту інформації та забезпечення їх безпеки **А5.З3**. Державну класифікацію засобів криптографічного захисту інформації **А5.З4.** Методи забезпечення безпеки криптографічних модулів згідно міжнародних стандартів ISO/IEC **А5.З5.** Математичні та методичні основи комп’ютерного	**А5.У1.** Брати учать у реалізації технічних проєктів захищених автоматизованих систем з використанням засобів та комплексів криптографічного захисту інформації **А5.У2.** Використовувати методи комп’ютерного моделювання та проєктування систем для раціонального вибору засобів захисту **А5.У3.** Розробляти та впроваджувати плани і процедури забезпечення безперервності бізнесу, з метою відновлення початкового стану систем у випадку виникнення кіберінцидентів	**А5.К1.** Спілкуватися з відповідних питань (виконання завдань) криптографічного захисту інформації в рамках робочих колективів на підприємстві (органі, установі) **А5.К2** Формувати запитів / відповідей в рамках листування з (відповідних питань) криптографічного захисту інформації з державними органами (установами, підприємствами)	**А5.В1**. Готувати заключний звіт з оцінки безпеки об’єкта інформаційної діяльності **А5.В2.** Виконувати оцінку плану безпеки з метою виявлення раціональних засобів захисту **А1.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		моделювання та проєктування автоматизованих систем **А5.З6.** Порядок розробки та зміст технічних проєктів систем і засобів криптографічного захисту інформації **А5.З7.** Поняття техніко-економічного обґрунтування проєктних рішень **А5.З8.** Процедури активізації (настроювання) програмних механізмів криптографічного захисту інформації в автоматизованих системах **А5.З9.** Особливості застосування та впровадження апаратних засобів криптографічного захисту інформації	**А5.У4.** Аналізувати проєктні обмеження та можливі компроміси безпеки криптографічного захисту інформації **А5.У5.** Розробляти схеми управління ключами криптосистем **А5.У6.** Активізувати (налаштовувати) програмні механізми криптографічного захисту інформації в комп'ютерних системах **А5.У7.** Брати участь у впровадженні програмних та апаратних засобів криптографічного захисту на підприємстві (органі, установі)		
	А6. Здатність розробляти, впроваджувати та аналізувати технічні документи, положення, інструкції щодо систем і	**А6.З1.** Систему технічних документів щодо систем і комплексів криптографічного захисту інформації	**А6.У1.** Брати участь у розробці, впровадженні та аналізі технічних документів, положень, інструкцій щодо систем і комплексів	**А6.К1.** Ефективно співпрацювати в команді та координувати виконання відповідних завдань	**А1.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
	комплексів криптографічного захисту інформації	**А6.З2.** Вимоги до структури та змісту технічних документів щодо систем і комплексів криптографічного захисту інформації **А6.З3.** Вимоги та підходи до розроблення технічних документів положень, інструкцій, методичних матеріалів щодо систем і комплексів криптографічного захисту інформації **А6.З4.** Сучасні підходи до формування вимог до криптографічного захисту інформації в автоматизованих системах і на об'єктах інформаційної діяльності	криптографічного захисту інформації, системи управління криптографічним захистом інформації (СУКЗІ) на підприємстві (установі,/організації)	**А6.К2** Структурувати інформацію та формувати свої висновки щодо вимог криптографічного захисту інформації	порушення в сфері кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)
	Предмети та засоби праці: Нормативно-правові акти, нормативні документи, проєктна документація, протоколи, стандарти та сертифікати відповідного прямування; комп'ютерне, програмне та техніко-технологічне забезпечення; комп'ютерні алгоритми, криптоалгоритми; бази даних; інструменти проєктування та впровадження систем та комплексів криптографічного захисту інформації; засоби вимірювальної техніки відповідного спрямування; програмні та апаратні засоби криптографічного захисту інформації				
Б. Забезпечення нормування, планування,	**Б1.** Здатність забезпечувати контроль (моніторинг) поточного	**Б1.З1**. Вимоги нормативно-правових актів і нормативних документів,	**Б1.У1.** Розробляти плани, програми, інструкції та настанови щодо	**Б1.К1.** Комунікувати з керівництвом організації для	**А1.В1**. Демонструвати обізнаність про

Трудові функції	Компетентності	Результати навчання			
		Знання	Уміння/ навички	Комунікація	Відповідальність і автономія
затвердження, впровадження та поточного оцінювання заходів щодо забезпечення належного рівня безпеки криптографіч-ного захисту інформації в органі (установі, підприємстві)	стану рівня безпеки криптографічного захисту інформації в органі (установі, підприємстві) та оцінку його відповідності вимогам нормативних документів	що визначають порядок контролю стану безпеки криптографічного захисту інформації **Б1.З2.** Поняття експертні та тематичні дослідження, допуск до експлуатації та протидія технічним розвідкам **Б1.З3.** Порядок, умови та організація проведення заходів, пов'язаних із запобіганням вчиненню порушень безпеки інформації в автоматизованих системах, виявленням та усуненням наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, **Б1.З4.** Поняття та загальний зміст методик проведення атестації комплексів криптографічного захисту інформації	контролю рівня безпеки криптографічного захисту інформації в органі (установі, підприємстві) **Б1.У2.** Здійснювати перевірку повноти і відповідності реалізованих заходів із захисту інформації в органі (установі, підприємстві) вимогам нормативних документів з питань криптографічного захисту інформації **Б1.У3.** Брати участь у здійсненні інструментального контролю захищеності інформації на об'єкті інформаційної діяльності від витоку технічними каналами **Б1.У4.** Робити висновки та складати акти за результатами контрольних заходів	забезпечення цілісного підходу стосовно контролю рівня інформаційної безпеки **Б1.К2.** Працювати в команді та співпрацювати з колегами та за потреби із зовнішніми експертами.	законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		Б1.З5. Засоби вимірювальної техніки та методики вимірювань оцінюваних показників комплексів криптографічного захисту інформації **Б1.З6.** Вимоги щодо оформлення документів, що складаються за результатами контрольних заходів			
	Б2. Здатність проводити оцінку безпеки, ефективності та надійності систем генерації, тестування та управління ключами до засобів криптографічного захисту інформації в органі (установі, підприємстві)	**Б2.З1** Вимоги нормативно-правових актів, нормативних документів міжнародних стандартів, що визначають порядок та умови забезпечення безпеки криптографічних ключів на етапах їх життєвого циклу **Б2.З2.** Принципи побудови та функціонування систем генерації, тестування та управління ключами до засобів криптографічного захисту **Б2.З3** Поняття про технології надійного	**Б2.У1.** Складати плани, програми та методичні рекомендації щодо порядку проведення обстежень (поточного контролю) стану безпеки поводження (зберігання і використання) з криптографічними ключами та забезпечення їх безпеки в органі (установі, підприємстві) **Б2.У2.** Робити висновки, розробляти рекомендації і пропозиції, складати акти за результатами контрольних заходів	**Б2.К1.** Готувати звітні документи стосовно стану безпеки поводження з криптографічними ключами. **Б2.К2.** Комунікувати з уповноваженими особами для допомоги забезпечення звітності про діяльність з безпеки	**А1.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		знищення криптографічних ключів на носіях **Б2.З4.** Поняття про особливості генерації і тестування ключів до асиметричних криптосистем **Б2.З5.** Методи управління ключами що мінімізують ризики компрометації інформації та її несанкціонованої модифікації **Б2.З6.** Поняття про методи та заходи щодо забезпечення охорони інформації в приміщеннях, які застосовуються для побудови центрів генерації криптографічних ключів	щодо безпеки криптографічних ключів		(установи, організації)
	Б3. Здатність проводити порівняльний аналіз різних систем та засобів криптографічного захисту інформації з метою їх раціонального вибору та закупівель в рамках тендерних процедур	**Б3.З1.** Поняття процедур оцінки відповідності засобів криптографічного захисту інформації **Б3.З2.** Вимоги технічних регламентів щодо порядку, умов та організації проведення оцінки	**Б3.У1.** Здійснювати оцінку відповідності (брати участь в оцінці відповідності) засобів криптографічного захисту інформації **Б3.У2.** Аналізувати політику безпеки та конфігурації засобів	**Б3.К1.** Співпрацювати з посадовими особами щодо планів закупівлі засобів криптографічного захисту. **Б3.К2.** Формувати запити з питань	**А1.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		відповідності засобів криптографічного	криптографічного захисту інформації, оцінювати їх відповідність нормативним актам і нормативним документам з питань безпеки криптографічного захисту **Б3.У3.** Оцінювати ефективність заходів із захисту інформації, заходів з режиму та управління доступом, заходів з кібербезпеки, які реалізуються системою управління інформаційною безпекою в органі (установі, підприємстві) **Б3.У4.** Робити висновки, готувати рекомендації та пропозиції, оформлювати документи за результатами порівняльного аналізу засобів криптографічного захисту, готувати вихідні	криптографічного захисту інформації зацікавленими сторонами, включаючи клієнтів, керівництво організації.	інформаційної безпеки **А1.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
			дані для проведення тендерів		
	Предмети та засоби праці: Нормативні акти, нормативні документи, проєктна документація, протоколи, стандарти та сертифікати щодо створення та оцінювання відповідності систем, комплексів та засобів захисту інформації; техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності; операційні системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми, алгоритми шифрування; бази даних; інструменти оцінювання відповідності систем, комплексів та засобів захисту інформації; засоби вимірювальної техніки та методики вимірювань оцінюваних показників систем, комплексів та засобів захисту інформації				
В. Реалізація практичних заходів щодо управління безпекою криптографіч-них ключів протягом їхнього життєвого циклу, а також розробка та реалізація інструкцій та заходів з питань відновлення попереднього стану, зруйноваго внаслідок	**В1.** Здатність підтримувати системи та комплекси криптографічного захисту інформації у робочому стані, оцінювати їх надійність та здійснювати контроль їх працездатності та виявлення місць відмов та інцидентів, проблем та подій	**В1.З1.** Загальні положення теорії надійності, методи діагностики працездатності та виявлення місця відмов у комп'ютерних системах, системах і комплексах захисту інформації **В1.З2.** Принципи стійкості та надмірності в комп'ютерних системах і комплексах захисту інформації	**В1.У1.** Здійснювати контроль працездатності комп'ютерних систем, систем і комплексів криптографічного захисту інформації **В1.У2.** Діагностувати несправне апаратне забезпечення системи/сервера **В1.У3.** Застосовувати засоби контролю працездатності та виявлення місця відмов **В1.У4.** Виявляти місця відмов у комп'ютерних системах, системах і комплексах захисту інформації	**В1.К1.**, Консультувати посадових осіб щодо питань криптографічного захисту **В1.К2.** Координувати діяльність працівників систем безпеки для ефективного виконання заходів безпеки	**В1.В1**. Проводити всебічну оцінку застосованих методів захисту **В1.В2.** Забезпечувати контроль працездатності та комплексів криптографічного захисту **А1.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)

Трудові функції	Компетентності	Результати навчання			
		Знання	Уміння/ навички	Комунікація	Відповідальність і автономія
виникнення інцидентів			**В1.У5.** Організовувати (проводити) ремонт та обслуговування апаратних засобів криптографічного захисту інформації		
	Предмети та засоби праці: Протоколи, стандарти, та сертифікати відповідного спрямування; комп'ютерне, програмне та техніко-технологічне забезпечення; операційні системи; прилади та інструменти для діагностування та ремонту несправного апаратного забезпечення системи/сервера, апаратних засобів захисту інформації				
Г. Взаємодія із зацікавленими сторонами з метою забезпечення безперервної діяльності органу (установи, підприємства) у сфері криптографіч-ного захисту інформації	**Г1.** Здатність очолювати робочі групи (підрозділи) органу (установи, підприємства), що тимчасово або постійно виконує завдання в сфері криптографічного захисту	**Г1.З1.** Кодекс законів України про працю, Цивільний кодекс, нормативно-правові акти з питань державної служби, законодавство про захист інформації та кібербезпеку **Г1.З2.** Основи управління персоналом **Г3.З3.** Основи комунікаційного менеджменту **Г3.З4.** Основи ділової етики	**Г1.У1.** Здійснювати керівництво робочою групою (підрозділом) органу (установи, підприємства), що тимчасово (постійно) виконує завдання з криптографічного захисту інформації **Г1.У2.** Координувати роботи з криптографічного захисту інформації в організації (установі, підприємстві) **Г1.У3.** Координувати за дорученням керівництва та надавати експертну підтримку підрозділам	**Г1.К1.** Організовувати опублікування настанов із криптографічного захисту для зацікавлених сторін організації. **Г1.К2.** Співпрацювати з колегами для оцінювати надійності систем криптографічного захисту	**Г1.В1**. Розроблювати вказівки і настанови для працівників з метою підвищення кваліфікації працівників **Г1.В2.** Забезпечувати ефективне виконання завдань в сфері криптографічного захисту

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
			(спеціалістам) органу (установи, підприємства) з питань криптографічного захисту інформації **Г1.У4.** Брати участь в навчанні (підвищенні кваліфікації) працівників органу (установи, підприємства) з питань криптографічного захисту інформації		
	Предмети та засоби праці: Нормативні установчі акти підприємства (організації); структура підприємства (організації); положення про структурні підрозділи підприємства (організації); посадові інструкції керівників та фахівців структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки та нормативні акти роботодавця з організації, координації діяльності та взаємодії структурних підрозділів підприємства (організації); порядок і типові вимоги до проведення ділових (комерційних) перемовин; порядок розроблення та виконання договірних робіт для зовнішніх партнерів				
Д. Проєктування апаратно-програмних комплексів криптографічного захисту.	**Д1.** Здатність проводити оцінку відповідності (державну експертизу) програмних засобів криптографічного захисту інформації	**Д1.З1.** Порядок оцінювання відповідності програмних засобів криптографічного захисту інформації **Д1.З2.** Поняття державної експертизи програмних засобів криптографічного захисту інформації **Д1.З3.** Порядок та організація проведення державної експертизи	**Д1.У1.** Складати програму та методику проведення державної експертизи програмних засобів криптографічного захисту інформації **Д1.У2.** Проводити експертні випробування та дослідження програмних засобів криптографічного	**Д1.К1.** Взаємодіяти із зовнішніми організаціями з метою проведення державної експертизи **Д1.К2.** Співпрацювати з працівниками організації для забезпечення політики безпеки	**Д1.В1**. Готувати звітні документи з проведення експертних випробування програмних засобів криптографічного захисту **Д1.В2.** Здійснювати адміністрування спеціалізованих

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		програмних засобів криптографічного захисту інформації **Д1.З4.** Поняття та загальний зміст програми та методики проведення державної експертизи програмних засобів криптографічного захисту інформації **Д1.З5.** Техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності програмних засобів криптографічного захисту інформації **Д1.З6.** Документи, що оформлюються за результатами державної експертизи програмних засобів криптографічного захисту інформації	захисту інформації (оцінювати функціональні послуги безпеки, оцінювати рівні гарантій коректності реалізації функціональних послуг безпеки) **Д1.У3.** Оцінювати відповідність програмних засобів криптографічного захисту інформації задекларованим характеристикам та вимогам нормативних документів системи криптографічного захисту інформації **Д1.У4.** Виконувати безпечне тестування, огляд та/або оцінку програм, щоб виявити потенційні недоліки в кодах і пом'якшити вразливості **Д1.У5.** Оформлювати протоколи експертних випробувань та експертні висновки за результатами	відповідно до вимог законодавства.	програмних засобів криптографічного захисту.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
			державної експертизи та організовувати їх затвердження і реєстрацію		
	Предмети та засоби праці: Нормативні акти, нормативні документи, проєктна документація, протоколи, стандарти та сертифікати щодо створення та оцінювання відповідності програмних та апаратних засобів криптографічного захисту інформації; техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності; операційні системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми, алгоритми шифрування; бази даних; інструменти оцінювання відповідності програмних та апаратних засобів криптографічного захисту інформації; засоби вимірювальної техніки та методики вимірювань оцінюваних показників апаратних засобів криптографічного захисту інформації				
Е. Консультування вищого керівництва щодо рівнів ризику та рівня безпеки криптографічного захисту інформації в органі (підприємстві, установі, організації)	**Е1.** Здатність аналізувати, інтегрувати і використовувати кращі світові практики, стандарти при розробці нормативних документів системи криптографічного захисту інформації	**Е1.З1.** Системи криптографічного захисту інформації та державну систему кіберзахисту **Е1.З2.** Нормативно-правові акти про криптографічний захист інформації **Е1.З3.** Кращі вітчизняні напрацювання з питань побудови криптосистем. **Е1.З4.** Світовий досвід, міжнародні стандарти в галузі захисту інформації та кібербезпеки	**Е1.У1.** Аналізувати систему нормативних документів (нормативну базу) системи криптографічного захисту інформації **Е1.У2.** Виявляти, ставити та вирішувати проблемні питання щодо системи нормативних документів (нормативної бази) системи криптографічного захисту інформації **Е1.У3.** Проводити системний аналіз світових практик,	**Е1.К1.** Брати участь в якості члена групи з проведення аналізу стандартів захисту за потреби **Е1.К2.** Співпрацювати з уповноваженими особами щодо забезпечення звітності про діяльність з криптографічного захисту інформації	**А1.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
			стандартів із захисту інформації **Е1.У4.** Готувати інформаційно-аналітичні документи в експертній галузі для доповіді керівництву органу (установи, підприємства)		(установи, організації)
	Е2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги криптографічного та організаційного спрямування щодо системи криптографічного захисту інформації	**Е2.З1.** Порядок розробки та впровадження нормативних документів системи криптографічного захисту інформації **Е2.З2.** Порядок актуалізації нормативних документів системи криптографічного захисту інформації	**Е2.У1.** Розробляти (брати участь у розробці) нормативні документи системи криптографічного захисту інформації **Е2.У2.** Писати та публікувати методики та настанови з кіберзахисту та інструктивні матеріали **Е2.У3.** Впроваджувати нормативні документи системи криптографічного захисту інформації **Е2.У4.** Здійснювати актуалізацію нормативних документів системи	**Е2.К1.** Відповідати на запити щодо надання інформації **Е2.К2.** Комунікувати з керівниками всіх рівнів для впровадження нормативних документів.	**А1.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
			криптографічного захисту інформації **Е2.У5.** Використовувати результати аналізу кращих світових практик, стандартів при розробці нормативних документів системи криптографічного захисту інформації		
	Предмети та засоби праці: Нормативні акти, нормативні та технічні документи системи криптографічного захисту інформації; концепції, кращі практики та стандарти розвитку системи криптографічного захисту інформації; нормативні документи з розробки та впровадження нормативних документів системи криптографічного захисту інформації				

VI. Розподіл трудових функцій та компетентностей за професійними кваліфікаціями

Трудова функція (умовне позначення)	Загальна назва професійної кваліфікації у межах професійного стандарту: Фахівець з криптографічного захисту інформації	
	Фахівець з криптографічного захисту інформації	Провідний фахівець з криптографічного захисту інформації
	повна	повна
А	+	+
Б	+	+
В	+	+
Г	+	+
Д	-	+
Е	-	+

VII. Відомості про розроблення та затвердження професійного стандарту

1. Повне найменування розробника професійного стандарту

Адміністрація Державної служби спеціального зв'язку та захисту інформації України

Склад робочої групи/Учасники робочої групи:

Воронов Віктор Романович, провідний консультант 2 відділу 2 управління Департаменту захисту інформації Адміністрації Держспецзв'язку;

Гайдур Галина Іванівна, завідувач кафедри інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації Державного університету телекомунікацій;

Гулак Геннадій Миколайович, професор кафедри інформаційної та кібернетичної безпеки ім. професора Володимира Бурячка факультету інформаційних технологій Київського університету імені Бориса Грінченка;

Давиденко Анатолій Миколайович, провідний науковий співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України;

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

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

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

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

Кононович Володимир Григорович, доцент кафедри кібербезпеки та технічного захисту інформації факультету інформаційних технологій та кібербезпеки Державного університету інтелектуальних технологій і зв'язку;

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

Корнієнко Богдан Ярославович, професор кафедри інформаційних систем та технологій факультету інформатики та обчислювальної техніки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;

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»;

Мельник Сергій Володимирович, доцент кафедри інформаційної безпеки Інституту комп’ютерно-інформаційних технологій та дизайну Міжрегіональної академії управління персоналом;

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

Невара Лілія Михайлівна, керівник навчально-методичного центру, голова профспілкової організації Громадської організації «Українська академія кібербезпеки»;

Пазюк Андрій Валерійович, віцепрезидент Громадської організації «Українська академія кібербезпеки»;

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

Рибка Михайло Сергійович, заступник начальника управління – начальник 1 відділу 5 управління Департаменту захисту інформації Адміністрації Держспецзв’язку;

Супрун Ольга Миколаївна, головний науковий співробітник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації.

2. Назва та реквізити документа, яким затверджено професійний стандарт

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

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

Висновок суб'єкта перевірки Національного агентства кваліфікацій від 27 грудня 2023 року про дотримання під час підготовки проєкту професійного стандарту «Фахівець з криптографічного захисту інформації» вимог Порядку розроблення, введення в дію та перегляду професійних стандартів, затвердженого постановою Кабінету Міністрів України від 31.05.2017 р. № 373).

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

Висновок Профспілки працівників зв'язку України щодо погодження проєкту професійного стандарту «Фахівець з криптографічного захисту інформації» (лист від 16 листопада 2023 року № 01.2-14/136, постанова Президії ЦК Профспілки працівників зв'язку України від 16 листопада 2023 року № П-4-5г).

VIII. Дата внесення професійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.

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