Проєкт

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

Професійний стандарт

ФАХІВЕЦЬ З КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

_____(дата внесення до Реєструкваліфікацій)

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 працюУкраїни на підставі:

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

- висновку Профспілки працівників зв'язку України від _____ щодо погодження проєкту професійного стандарту **.**

І. Назва професійного стандарту

Фахівець з криптографічного захисту інформації

ІІ. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Забезпечення криптографічного захисту інформації в лініях зв'язку та середовищах, включаючи комп'ютерні системи. Здійснення оцінки безпеки та контролю стану криптографічного захисту в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (далі – автоматизовані системи). Дослідження рівня захисту програмних засобів і систем що реалізують криптографічні функції. Супроводження робіт зі створення, впровадження та забезпечення функціонування підсистем криптографічного захисту на етапах життєвого циклу автоматизованих систем.

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

Секція	Назва секції	№ розділу	Назва розділу	№ групи (класу)	Назва групи (класу)
Секція J	Інформація та телекомуніка-ції	**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 устаткованням

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

Фахівець з криптографічного захисту інформації 2139.2.

4. Професійна кваліфікація,її 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

- диплом бакалавра 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);

- диплом магістра 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);

- документ (диплом, сертифікат, тощо), щодо післядипломної освіти та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері криптографічного захисту інформації;

- 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 у сфері криптографічного захисту інформації;

- документ (диплом, сертифікат, тощо), щодо професійної сертифікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері у сфері криптографічного захисту інформації.

ІІІ. Здобуття професійної кваліфікації та професійний розвиток

1. Здобуття професійної кваліфікації

Назва професійної та/або часткової професійної кваліфікації	**Суб'єкти, уповноваженізаконодавством на присвоєння/підтвердження та визнанняпрофесійнихкваліфікацій**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
Фахівець з криптографічного захисту інформації	Підготовка на першому рівні вищої освіти (бакалаврському) за спеціальностями, вказаними у п. 5, галузі знань 11 «Математика та статистика» та 12 «Інформаційні технології»	*Не передбачено професійним стандартом*
Провідний фахівець з криптографічного захисту інформації	Підготовка на першому рівні вищої освіти (магістерському) за спеціальностями, вказаними у п. 5, галузі знань 11 «Математика та статистика» та 12 «Інформаційні технології» та 3 роки досвіду роботи за спеціальністю	*Не передбачено професійним стандартом*

2. Професійний розвиток

1) з присвоєнням наступної професійної кваліфікації

Назва професійної та/або часткової професійної кваліфікації	**Суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнанняпрофесійнихкваліфікацій**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
Фахівець з криптографічного захисту інформації	Підвищення кваліфікації фахівця з криптографічного захисту інформації для отримання професійної кваліфікації провідний фахівця з криптографічного захисту інформації. Стаж	*Не передбачено професійним стандартом*

	роботи за спеціальністю не менше трьох років	

IV. Абревіатури, скорочення

ІТ	інформаційні технології
СУКЗІ	система управління криптографічним захистом інформації
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission

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	**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	**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)

		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 вразливостей та прогнозування продуктивності за різних умов експлуатації	захисту інформації з необхідним рівнем безпеки **А1.У4.** Аналізувати потреби та вимоги користувачів з метою планування і проведення 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	**А2.У1.** Виявляти загрози безпеці криптографічного захисту інформації **А2.У2.** Досліджувати (оцінювати) загрози безпеці криптографічного	**А2.К1.** Спілкуватися з відповідних питань (виконання завдань) криптографічного захисту інформації в рамках робочих колективів на підприємстві	**А2.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та

		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.З5.** Класифікацію наслідків для безпеки криптографічного захисту інформації у результаті виникнення кіберінцидентів, дій інсайдерів та помилок персоналу	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 порушника безпеки криптосистем **А2.У5.** Готувати пропозиції щодо розробки моделі загроз криптосистемам завдяки витоку інформації технічними каналами або внаслідок спеціальних впливів	(установі, організації) **А2.К2** Формувати запити / відповіді в рамках листування з (відповідних питань) криптографічного захисту інформації з державними органами (установами, підприємствами)	інформаційної безпеки **А2.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (органу, установи)
	А3. Здатність аналізувати, розробляти та супроводжувати систему управління безпекою криптографічного захисту	**А3.З1.** Поняття системи управління безпекою криптографічного захисту на	**А3.У1.** Брати участь у визначенні сфери та меж дії системи управління криптографічним захистом інформації	**А3.К1.** Спілкуватися з відповідних питань (виконання завдань) криптографічного захисту інформації в рамках робочих	**А3.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за

	інформації на підприємстві (органі, установі)	підприємстві (органі, установі) **А3.З2.** Принципи створення систем управління криптографічною безпекою **А3.З3.** Принципи побудови систем криптографічного захисту інформації, що визначені законодавством і стандартами	(СУКЗІ) на підприємстві (органі, установі) **А3.У2.** Брати участь у розробці, впровадженні СУКЗІ та забезпеченні її сталого функціонування **А3.У4.** Брати участь у моніторингу стану СУКЗІ та розробці пропозицій щодо її вдосконалення	колективів на підприємстві (органу, установі) **А3.К2** Формувати запити / відповіді в рамках листування з (відповідних питань) криптографічного захисту інформації з державними органами (установами, підприємствами)	порушення в сфері кібербезпеки та інформаційної безпеки **А3.В2.** З~~датність~~ Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (органу, установи)
	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.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	**А4.К1.** Спілкуватися з відповідних питань (виконання завдань) криптографічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **А4.К2.** Формувати запити / відповіді в рамках листування з (відповідних питань) криптографічного захисту інформації з	**А4.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **А4.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця

		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 підпису, криптопротоколів, систем генерації і тестування ключів та криптоаналізу	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 щодо укладання договорів на проведення тематичних досліджень (їх окремих складових) та оцінки відповідності засобів криптографічного захисту інформації	державними органами (установами, підприємствами)	підприємства (установи, організації)

	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 моделювання та проєктування	**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.У4.** Аналізувати проєктні обмеження та можливі компроміси безпеки	**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**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **А5.А1.** ~~Здатність~~ Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (органу, установи)

		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	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,	**А6.З1.** Систему технічних документів щодо систем і комплексів	**А6.У1.** Брати участь у розробці, впровадженні та аналізі технічних	**А6.К1.** Спілкуватися (обговорювати) з відповідних питань (виконання завдань)	**А6.В1**. Демонструвати обізнаність про законодавчо

	інструкції щодо систем і комплексів криптографічного захисту інформації	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	документів, положень, інструкцій щодо систем і комплексів криптографічного захисту інформації, системи управління криптографічним захистом інформації (СУКЗІ) на підприємстві (установі,/організації)	криптографічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **А6.К2** Формувати запити / відповіді в рамках листування з (відповідних питань) криптографічного захисту інформації з державними органами (установами, підприємствами)	визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **А6.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 технічного та криптографічного захисту інформації				

Б. Забезпечення нормування, планування, затвердження, впровадження та поточного оцінювання заходів щодо забезпечення належного рівня безпеки криптографіч-ного захисту інформації в органі (установі, підприємстві)	**Б1.** Здатність забезпечувати контроль (моніторинг) поточного стану рівня безпеки криптографічного захисту інформації в органі (установі, підприємстві) та оцінку його відповідності вимогам нормативних документів	**Б1.З1**. Вимоги нормативно-правових актів і 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	**Б1.У1.** Розробляти плани, програми, інструкції та настанови щодо 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 та технічного 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	**Б1.К1.** Спілкуватися (обговорювати) з відповідних питань (виконання завдань) криптографічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **Б1.К2.** Формувати запити / відповіді в рамках листування з (відповідних питань) криптографічного захисту інформації з державними органами (установами, підприємствами)	**Б1.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **Б1.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)

		якої встановлена законом, **Б1.З4.** Поняття та загальний зміст методик проведення атестації комплексів технічного захисту інформації **Б1.З5. З**асоби вимірювальної техніки та методики вимірювань оцінюваних показників комплексів технічного захисту інформації **Б1.З6.** Вимоги щодо оформлення документів, що складаються за результатами контрольних заходів	акти 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	**Б2.У1.** Складати плани, програми та методичні рекомендації щодо порядку проведення обстежень (поточного контролю) стану безпеки поводження (зберігання і використання) з криптографічними	**Б2.К1.** Спілкуватися (обговорювати) з відповідних питань (виконання завдань) криптографічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації)	**Б2.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки

		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 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 та технічного захисту	ключами та забезпечення їх безпеки в органі (установі, підприємстві) **Б2.У2.** Робити висновки, розробляти рекомендації і пропозиції, складати акти за результатами контрольних заходів щодо безпеки криптографічних ключів	**Б2.К2.** Формувати запити / відповіді в рамках листування з (відповідних питань) криптографічного захисту інформації з державними органами (установами, підприємствами)	**Б2.В2.** ~~Здатність~~ Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)

		інформації в приміщеннях, які застосовуються для побудови центрів генерації криптографічних ключів			
	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 відповідності засобів криптографічного	**Б3.У1.** Здійснювати оцінку відповідності (брати участь в оцінці відповідності) засобів криптографічного захисту інформації **Б3.У2.** Аналізувати політику безпеки та конфігурації засобів 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,	**Б3.К1.** Спілкуватися (обговорювати) з відповідних питань (виконання завдань) криптографічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **Б3.К2.** Формувати запити / відповіді в рамках листування з (відповідних питань) криптографічного захисту інформації з державними органами (установами, підприємствами)	**Б3.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **Б3.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)

			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 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 виникнення інцидентів	**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.У5.** Організовувати (проводити) ремонт та обслуговування апаратних засобів криптографічного захисту інформації	**В3.К1.** Спілкуватися (обговорювати) з відповідних питань (виконання завдань) криптографічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **В3.К2.** Формувати запити / відповіді в рамках листування з (відповідних питань) криптографічного захисту інформації з державними органами (установами, підприємствами)	**В3.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **В3.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)

	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.З3.** Основи управління персоналом **Г3.З4.** Основи комунікаційного менеджменту **Г3.З5.** 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 криптозахисту інформації в органі (установі, підприємстві) **Г1.У3.** Координувати за дорученням керівництва та надавати експертну підтримку підрозділам (спеціалістам) органу (установи, підприємства) з питань криптографічного захисту інформації **Г1.У4.** Брати участь в навчанні (підвищенні кваліфікації) працівників органу (установи, підприємства) з	**Г1.К1.** Спілкуватися (обговорювати) з відповідних питань (виконання завдань) криптографічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **Г1.К2.** Формувати запити / відповіді в рамках листування з (відповідних питань) криптографічного захисту інформації з державними органами (установами, підприємствами)	**Г1.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **Г1.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)

			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 технічного захисту інформації **Д1.З3.** Порядок та організація проведення державної експертизи програмних засобів технічного захисту інформації **Д1.З4.** Поняття та загальний зміст програми та методики проведення державної експертизи програмних засобів технічного захисту інформації **Д1.З5.** Техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності програмних засобів	**Д1.У1.** Складати програму та методику проведення державної експертизи програмних засобів технічного захисту інформації **Д1.У2.** Проводити експертні випробування та дослідження програмних засобів технічного захисту інформації (оцінювати функціональні послуги безпеки, оцінювати рівні гарантій коректності реалізації функціональних послуг безпеки) **Д1.У3.** Оцінювати відповідність програмних засобів технічного захисту інформації задекларованим характеристикам та вимогам нормативних документів системи технічного захисту інформації	**Д1.К1.** Спілкуватися (обговорювати) з відповідних питань (виконання завдань) криптографічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **Д1.К2.** Формувати запити / відповіді в рамках листування з (відповідних питань) криптографічного захисту інформації з державними органами (установами, підприємствами)	**Д1.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **Д1.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)

		технічного захисту інформації **Д1.З6.** Документи, що оформлюються за результатами державної експертизи програмних засобів технічного 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 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 технічного та 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 технічного та криптографічного захисту інформації; засоби вимірювальної техніки та методики вимірювань оцінюваних показників апаратних засобів технічного та 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 та технічного захисту інформації та державну систему кіберзахисту **Е1.З2.** Нормативно-правові акти про криптографічний та технічний 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 та технічного захисту інформації **Е1.У2.** Виявляти, ставити та вирішувати проблемні питання щодо системи нормативних документів (нормативної бази) системи технічного та криптографічного захисту інформації **Е1.У3.** Проводити системний аналіз світових практик, стандартів із захисту інформації **Е1.У4.** Готувати інформаційно-	**Е1.К1.** Спілкуватися (обговорювати) з відповідних питань (виконання завдань) криптографічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **Е1.К2.** Формувати запити / відповіді в рамках листування з (відповідних питань) криптографічного захисту інформації з державними органами (установами, підприємствами)	**Е1.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **Е1.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)

			аналітичні документи в експертній галузі для доповіді керівництву органу (установи, підприємства)		
	Е2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування щодо системи технічного та криптографічного захисту інформації	**Е2.З1.** Порядок розробки та впровадження нормативних документів системи технічного та криптографічного захисту інформації **Е2.З2.** Порядок актуалізації нормативних документів системи технічного та криптографічного захисту інформації	**Е2.У1.** Розробляти (брати участь у розробці) нормативні документи системи технічного та криптографічного захисту інформації **Е2.У2.** Писати та публікувати методики та настанови з кіберзахисту та інструктивні матеріали **Е2.У3.** Впроваджувати нормативні документи системи технічного та криптографічного захисту інформації **Д2.У4.** Здійснювати актуалізацію нормативних документів системи технічного та криптографічного захисту інформації	**Е2.К1.** Спілкуватися (обговорювати)з відповідних питань (виконання завдань) криптографічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **Е2.К2.** Формувати запити / відповіді в рамках листування з (відповідних питань) криптографічного захисту інформації з державними органами (установами, підприємствами)	**Е2.В1**. Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері кібербезпеки та інформаційної безпеки **Е2.В2.** Виконувати відповідні завдання криптографічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)

			Е2.У5. Використовувати результати аналізу кращих світових практик, стандартів при розробці нормативних документів системи технічного та криптографічного захисту інформації		
	Предмети та засоби праці: Нормативні акти, нормативні та технічні документи системи технічного та криптографічного захисту інформації; концепції, кращі практики та стандарти розвитку системи технічного та криптографічного захисту інформації; нормативні документи з розробки та впровадження нормативних документів системи технічного та 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 затвердженняпрофесійного стандарту

1. Повне найменування розробника професійного стандарту

Державної служби спеціального зв’язку та захистуінформації України

Склад робочоїгрупи/Учасникиробочоїгрупи:

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

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

Висновок суб'єкта перевірки Національного агентства кваліфікацій від_____ 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 від _____ щодо погодження проєкту професійного стандарту «фахівець з криптографічного захисту інформації».

VIII. Дата внесення професійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.