Прим. № __

ЗАТВЕРДЖЕНО

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

ПРОФЕСІЙНИЙ СТАНДАРТ

ФАХІВЕЦЬ З ТЕХНІЧНОГО 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 технічного 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).

І. Назва професійного стандарту

Фахівець з технічного захисту інформації

ІІ. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Забезпечення інженерно-технічними та організаційно-технічними заходами та засобами порядку доступу, конфіденційності, цілісності й доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

Захист інформації та безпосередньо її властивостей, спрямований на забезпечення за допомогою нормативно-правових, організаційних та інженерно-технічних заходів та/або програмно-технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації. Супроводження робіт зі створення, впровадження та забезпечення функціонування систем технічного захисту інформації на етапах життєвого циклу інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем (далі – автоматизовані системи).

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 технічного захисту інформації 2139.2.

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

Молодший фахівець з технічного захисту інформації 6 рівень НРК

Фахівець з технічного захисту інформації 7 рівень НРК

Провідний фахівець з технічного 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 технічного 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).

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**
Молодший фахівець з технічного захисту інформації	Підготовка за спеціальностями, вказаними у **П.*** на першому (бакалаврському) рівні вищої освіти	*Не передбачено професійним стандартом*
Фахівець з технічного захисту інформації	Підготовка за спеціальностями, вказаними у **П.*** на першому (бакалаврському) рівні вищої освіти за умови наявності стажу роботи за однією з професій відповідного спрямування не менше 2 років або підготовка за спеціальностями, вказаними у **П.*** на другому (магістерському) рівні вищої освіти	*Не передбачено професійним стандартом*
Провідний фахівець з технічного 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:

- 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);

- 172 «Електронні комунікації та радіотехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (6 рівень НРК);

- 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (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:

- 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);

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

- 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (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 технічного захисту інформації	Підвищення кваліфікації фахівця з технічного захисту інформації для отримання професійної кваліфікації провідн**ог**о фахівця з технічного 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

EBSCO	Elton Bryson Stephens Company
JSTOR	Journal Storage
СУІБ	система управління інформаційною безпекою
NIST SP 800-160	National Institute of Standards and Technology Special Publication 800-160
IP	Internet Protocol
VoIP	Voice over Internet Protocol
IEC	International Electrotechnical Commission
ITIL	Information Technology Infrastructure Library
КСЗІ	комплексна система захисту інформації
АС	Автоматизована система
ІКС	Інформаційно-комунікаційна система
СЕК	Система електронних комунікацій
ІТ	Інформаційні технології
ІС	Інформаційна система
НДР	науково-дослідні роботи
ТЗІ	технічний захист інформації
ОІД	об’єкт інформаційної діяльності
ПМА	програми і методики атестації

V. Опис трудових функцій

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
А. Впровадження та супроводження систем захисту інформації та кіберзахисту інженерно-технічної інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави	**А1**. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації	**А1.З1.** Поняття та класифікацію інформації з обмеженим доступом, державні інформаційні ресурси **А1.З2.** Поняття технічного та криптографічного захисту інформації **А1.З3.** Концепції і протоколи комп'ютерних мереж, методології забезпечення мережевої безпеки та захисту інформації в автоматизованих (інформаційних) системах та на об'єктах інформаційної діяльності **А1.З4**. Методи та процеси управління ризиками (методи оцінки та зниження ризиків)	**А1.У1.** Визначати (формулювати) потреби щодо захисту інформації, що обробляється в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах користувачів (замовників) **А1.У2.** Визначати (формулювати) потреби щодо захисту інформації, що озвучується на об'єктах інформаційної діяльності підприємства (організації) **А1.У3.** Визначати (формулювати) потреби до кібербезпеки в електронних комунікаційних та інформаційно-комунікаційних	**А1.К1.** Спілкуватися з питань виконання завдань технічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **А1.К2.** Формувати запити / відповіді в рамках листування з питань технічного захисту інформації з державними органами (установами, підприємствами)	**А1.В1.** Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері захисту інформації, кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання технічного захисту інформації під контролем провідного фахівця підприємства (установи, організації) **А1.В3.**Використовувати моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		А1.З5. Закони, нормативні акти, нормативні документи, що визначають вимоги із захисту інформації та кіберзахисту **А1.З6.** Політики і етичні норми приватності стосовно безпеки інформації та кібербезпеки **А1.З7**. Принципи та способи захисту інформації, кібербезпеки і приватності **А1.З8**. Класифікацію операційних наслідків в результаті помилок із захисту інформації та кібербезпеки **А1.З9**. Політики, вимоги і процедури безпеки ланцюжка постачання інформаційних технологій та управління ризиками ланцюжка постачання **А1.З10**. Поняття комплексних систем	системах користувачів (замовників) **А1.У4.**Визначати та аналізувати вимоги щодо захисту інформації та кіберзахисту в інформаційно-комунікаційних системах та на об’єктах інформаційної діяльності підприємства (організації) **А1.У5.** Здійснювати попередню оцінку достатності потреб та вимог користувачів (замовників) для забезпечення необхідного рівня захисту інформації та кіберзахисту **А1.У6.**Застосовувативполітики безпеки для досягнення цілей безпеки системи **А1.У7.** Аналізувати потреби та вимоги користувачів з метою планування і проведення		комунікаційних систем для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		захисту інформації та комплексів технічного захисту інформації, їх склад та призначення **А1.З11**. Моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, призначених для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації	розробки системи безпеки **А1.У8.** Відстежувати системні вимоги з метою проєктування компонентів та виконувати аналіз недоліків розробки		
	А2. Здатність виявляти, досліджувати (оцінювати), системно аналізувати загрози для інформації, аналізувати ризики безпеки інформації та кібербезпеки у разі реалізації загроз	**А2.З1.** Класифікацію загроз для інформації та кіберзагроз (загрози від несанкціонованих дій з інформацією, технічні канали витоку інформації, спеціальні впливи на засоби обробки інформації) **А2.З2**. Методи (способи) і методики виявлення, дослідження та	**А2.У1.** Виявляти загрози для інформації та кіберзагрози в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах **А2.У2.** Виявляти загрози для інформації, що озвучується на об’єктах	**А2.К1.** Рекомендувати та обговорювати із зацікавленими сторонами плани дій та етапів або плани відновлення для усунення вразливостей, які були виявлені під час оцінки ризиків, аудиторських та	**А2.В1.** Досліджувати і оцінювати наявні технології і стандарти з метою задоволення вимог замовника. **А1.В1.**Демонструвати обізнаність про законодавчо визначену відповідальність за

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		системного аналізу загроз для інформації та кіберзагроз **А2.З3.** Форми і зміст моделей загроз для інформації, моделі порушника інформації; порядок їх розробки **А2.З4.** Поняття ризиків безпеки інформації та кібербезпеки **А2.З5.** Підходи, методи(способи) оцінки та аналізу ризиків безпеки інформації та кібербезпеки **А2.З6.** Класифікація операційних наслідків, спричинених помилками в системі кібербезпеки **А2.З7.** Поняття спеціальних впливів на засоби обробки інформації з метою знищення (спотворення), блокування інформації	інформаційної діяльності (обґрунтовувати можливість створення певних технічних каналів витоку інформації, що озвучується на конкретному об'єкті інформаційної діяльності) **А2.У3**. Досліджувати (оцінювати) та системно аналізувати загрози для інформації та вразливості комп'ютерної системи (систем) для розробки профілю безпеки **А2.У4**. Оцінювати та аналізувати ризики безпеки інформації та кібербезпеки **А2.У5**. Розробляти модель загроз для інформації від несанкціонованих дій та модель порушника інформації	інспекторських перевірок тощо **А1.К1**. Спілкуватися з питань виконання завдань технічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **А1.К2.** Формувати запити / відповіді в рамках листування з питань технічного захисту інформації з державними органами (установами, підприємствами	порушення в сфері захисту інформації, кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання технічного захисту інформації під контролем провідного фахівця підприємства (установи, організації

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
			А2.У6. Розробляти модель загроз для інформації від витоку технічними каналами **А2.У7**. Розробляти модель загроз для інформації від спеціальних впливів на засоби обробки інформації		
	А3. Здатність формувати стратегію і політики безпеки інформації в інформаційно-комунікаційних системах	**А3.З1.** Поняття стратегії і політики безпеки інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах **А3.З2**. Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи ешелонованого захисту (прикладна система ешелонованого захисту) **А3.З3**. Принципи, моделі, інструменти та	**А3.У1.** Обґрунтовувати та розробляти політику безпеки інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах **А3.У2.** Ураховувати методи управління мережевими системами при обґрунтуванні концепції безпеки інформації **А3.У3.** Ураховувати методи управління ризиками при	**А3.К1.**Застосовувати політики безпеки інформації в інформаційно-комунікаційних системах для досягнення цілей безпеки системи, зокрема при взаємодії із зацікавленими сторонами. **А1.К1.** Спілкуватися з питань виконання завдань технічного захисту інформації в рамках робочих колективів на	**А3.В1** Переглядати стандарти політики та стратегії її впровадження, щоб забезпечити відповідність процедур та настанов політикам кібербезпеки **А1.В1.** Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері захисту інформації, кібербезпеки та

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		методи управління мережевими системами (наскрізний моніторинг продуктивності систем) **А3.З4.** Зміст та порядок розробки політики безпеки інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах **А3.З5.** Поняття профілю безпеки інформації та функціональних послуг безпеки **А3.З6.** Поняття рівня гарантій реалізації функціональних послуг безпеки	обґрунтуванні концепції безпеки інформації **А3.У4.** Визначати (розробляти, обґрунтовувати) профіль безпеки інформації в автоматизованих системах різного класу **А3.У5.** Розробляти групові політики та переліки контролю доступу для забезпечення відповідності стандартам організації, бізнес-правилам та потребам	підприємстві (установі, організації) **А1.К2.** Формувати запити / відповіді в рамках листування з питань технічного захисту інформації з державними органами (установами, підприємствами)	інформаційної безпеки **А1.В2.** Виконувати відповідні завдання технічного захисту інформації під контролем провідного фахівця підприємства (установи, організації
	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				

Трудові функції	Компетентності	Результати навчання			
		Знання	Уміння/ навички	Комунікація	Відповідальність і автономія
Б. Розробка, планування, впровадження та контроль організаційних, підготовчих технічних, технічних заходів для забезпечення і супроводження комплексів технічного захисту інформації з обмеженим доступом від витоку технічними каналами на об’єкті інформаційної діяльності органів державної влади, місцевого самоврядування, військового формування, підприємства, установи та організації	**Б1**. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою підприємства/ організації	**Б1.З1**. Поняття системи управління інформаційною безпекою підприємства/організації **Б1.З2.** Принципи створення систем управління інформаційною безпекою **Б1.З3.** Принципи створення систем інформаційної безпеки	**Б1.У1**. Визначати сферу та межі (брати участь у визначенні сфери та меж) дії СУІБ **Б1.У2.** Брати участь у розробці СУІБ **Б1.У3.** Брати участь у впровадженні СУІБ **Б1.У4.** Брати участь у моніторингу та аналізі СУІБ **Б1.У5.** Брати участь у здійсненні підтримки та вдосконаленні СУІБ **Б1.У6.** Брати участь у створенні систем інформаційної безпеки **Б1.У7.** Застосовувати сервіс-орієнтовані принципи архітектури безпеки, щоб задовольнити вимоги конфіденційності, цілісності та доступності організації	**Б1.К1.** Брати участь у створенні систем інформаційної безпеки із залученням зацікавлених сторін. **А1.К1.** Спілкуватися з питань виконання завдань технічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **А1.К2.** Формувати запити / відповіді в рамках листування з питань технічного захисту інформації з державними органами (установами, підприємствами)	**Б1.В1**. Перетворювати функціональні вимоги в технічні рішення **А1.В1.** Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері захисту інформації, кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання технічного захисту інформації під контролем провідного фахівця підприємства (установи, організації

Трудові функції	Компетентності	Результати навчання			
		Знання	Уміння/ навички	Комунікація	Відповідальність і автономія
	Б2. Здатність виконувати передпроєктні роботи щодо систем та комплексів захисту інформації	**Б2.З1.** Середовища функціонування автоматизованих систем **Б2.З2.** Загальний порядок створення комплексних систем захисту інформації та комплексів технічного захисту інформації **Б2.З3.** Порядок категоріювання об'єктів **Б2.З4**. Порядок та методи (способи) обстеження середовищ функціонування автоматизованих систем та об'єктів інформаційної діяльності **Б2.З5.** Порядок розробки моделей загроз для інформації **Б2.З6.** Порядок розробки та зміст технічних завдань на створення комплексних систем захисту інформації та	**Б2.У1.** Здійснювати категоріювання об'єктів інформаційної діяльності (об'єктів електронно-обчислювальної техніки) **Б2.У2.** Здійснювати обстеження середовищ функціонування автоматизованих систем **Б2.У3.** Здійснювати обстеження об'єктів інформаційної діяльності **Б2.У4.** Розробляти моделі загроз для інформації **Б2.У5.** Розробляти технічні завдання на створення комплексних систем захисту інформації **Б2.У6.** Розробляти технічні завдання на створення комплексів технічного захисту інформації	**Б2.К1.**Здійснювати поглиблене комплексне визначення цілей, планування систем та комплексів захисту інформації із залученням зацікавлених сторін **А1.К1.** Спілкуватис питань виконання за технічного захисту інформації в рамках робочих колективів підприємстві (устан організації) **А1.К2.** Формувати з / відповіді в рамках листування з питань технічного захисту інформації з держав органами (установа підприємствами**)**	**Б2.В1.** Створювати стратегії комплексної експлуатації, які визначають експлуатаційні технічні або операційні вразливості **А1.В1.** Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері захисту інформації, кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання технічного захисту інформації під контролем провідного фахівця підприємства

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		комплексів технічного захисту інформації	**Б2.У7.** Розробляти проекти комплексних систем захисту інформації та комплексів технічного захисту інформації багаторівневими вимогами безпеки або вимогами для обробки кількох рівнів класифікації даних (відкрита інформація, службова інформація, секретна інформація з різними ступенями секретності)		(установи, організації
	Б3.Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності	**Б3.З1.** Поняття спеціальних досліджень засобів обробки інформації, технічних засобів **Б3.З2.** Поняття спеціальних досліджень об'єктів інформаційної діяльності **Б3.З3.** Архітектуру комп'ютера, принципи дії складових електронно-	**Б3.У1.** Проводити спеціальні дослідження засобів обробки інформації, технічних засобів (визначати складові та режими роботи засобів обробки інформації та технічних засобів, визначати тестові сигнали, складати схеми спеціальних досліджень, виявляти та вимірювати	**Б3.К1.**Моніторити та оцінювати ефективність технічних засобів захисту організації з метою гарантованого підтвердження того, що вони забезпечують необхідний рівень захисту.	**Б3.В1**. Тестувати і оцінювати розроблені засоби обробки інформації з метою оперативного використання. **А1.В1.** Демонструвати обізнаність про законодавчо визначену відповідальність за

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		обчислювальної машини, комп'ютерні мережі, класи автоматизованих систем **Б3.З4.** Поняття об'єкта інформаційної діяльності **Б3.З5.** Поняття показників захищеності інформації засобів обробки інформації та показників захищеності мовної інформації на об'єкті інформаційної діяльності **Б3.З6.** Методи вимірювання фізичних величин та принципи роботи сучасних засобів вимірювальної техніки (спектро-аналізаторів, осцилографів, частотомірів, вольтметрів, омметрів, індикаторів поля, віброметрів, шумомірів) **Б3.З7.** Методики спеціальних досліджень засобів обробки	небезпечні (тестові) електричні, електромагнітні та оптичні сигнали, визначати показники захищеності інформації засобів обробки інформації, технічних засобів та можливість (неможливість) створення ними або через них певних технічних каналів витоку інформації) **Б3.У2.** Проводити спеціальні дослідження об'єктів інформаційної діяльності (складати схеми спеціальних досліджень, виявляти та вимірювати небезпечні (тестові) акустичні, віброакустичні, акустоелектричні, акустоелектромаг-нітні, лазерні сигнали, які розповсюджуються різними каналами витоку (повітряним,	**А1.К1.** Спілкуватися з питань виконання завдань технічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **А1.К2.** Формувати запити / відповіді в рамках листування з питань технічного захисту інформації з державними органами (установами, підприємствами)	порушення в сфері захисту інформації, кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання технічного захисту інформації під контролем провідного фахівця підприємства (установи, організації

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		інформації і об’єктів інформаційної діяльності **Б3.38.** Теорію електромагнітного поля (в частині, необхідній для виконання професійних функцій) **Б3.39.** Теорію акустики (в частині, необхідній для виконання професійних функцій) **Б3.310.** Пристрої електротехніки (в частині, що складають архітектуру комп’ютера: друковані плати, мікросхеми, процесори, елементи пам’яті) **Б3.311.** Теорію радіотехнічних ланцюгів та сигналів(в частині, необхідній для виконання професійних функцій) **Б3.312**. Спектри сигналів та методи спектрального аналізу	вібраційним, електроакустичним, оптичним (лазерним), параметричним). Визначати показники захищеності мовної інформації на об’єкті інформаційної діяльності та можливість (неможливість) створення на ОІД певних технічних каналів витоку інформації) **Б3.У3.** Визначати вимоги до показників (характеристик) апаратних засобів технічного захисту інформації, які необхідні для забезпечення захищеності інформації в системі або на об’єкті інформаційної діяльності. **Б3.У4.** Складати протоколи спеціальних досліджень		

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		Б3.З13. Загальні положення теорії інформації та методи кодування **Б3.З14.** Загальні положення теорії ймовірностей та нечітких множин **Б3.З15**. Статистичну радіотехніку (прийом інформаційних сигналів на фоні шумів, оцінка параметрів сигналів, що приймаються на фоні шумів) **Б3.З16**. Методи цифрової обробки зображень та сигналів **Б3.З17**. Математику логарифмів, тригонометрію, лінійну алгебру, математичний аналіз, операційний аналіз, статистику (в частині, необхідній для виконання професійних функцій)	**Б3.У5.** Складати приписи на експлуатацію засобів обробки інформації та об’єктів інформаційної діяльності		

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		Б3.З18. Концепції і протоколи комп'ютерних мереж **Б3.З19**.Передачі голосу по IP (VoIP)			
	Б4. Здатність впроваджувати (активізувати) програмні та апаратні засоби захисту інформації в системах та на об'єктах	**Б4.З1.** Принципи, методи, засоби забезпечення безпеки інформації та інформаційних технологій (програмні засоби (механізми) захисту інформації, мережеві екрани, шифрування) **Б4.З2.** Методології забезпечення мережевої безпеки **Б4.З3.** Способи та апаратні засоби захисту інформації, методи автентифікації, авторизації та контролю доступу **Б4.З4.** Методологічні та математичні основи комп'ютерного проектування та моделювання систем	**Б4.У1.** Використовувати методи комп'ютерного проєктування та моделювання систем для розробки технічних проектів комплексних систем захисту інформації та комплексів технічного захисту інформації **Б4.У2.** Визначати та групувати за пріоритетами основні системні функції або підсистеми, необхідні для підтримки основних можливостей або бізнес-функцій з метою відновлення або поновлення після відмови системи, або під час відновлення системи на основі загальних системних вимог щодо	**Б4.К1.** Залучати представників з зацікавлених сторін до впровадження програмних та апаратних засобів захисту інформації в системах та на об'єктах. **А1.К1.** Спілкуватися з питань виконання завдань технічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **А1.К2.** Формувати запити / відповіді в рамках листування з питань	**Б4.В1.**Оцінювати якість виконаних робіт з впровадження програмних та апаратних засобів захисту інформації в системах та на об'єктах **Б4.В2.** Інтегрувати та застосовувати політику, яка відповідає цілям безпеки в системах

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		Б4.З5. Мови програмування мікроконтролерів та контролерів відповідно до норм IEC 61131-3 Програмовані контролери. Мови програмування **Б4.З6.** Порядок розробки та зміст технічних проектів комплексних систем захисту інформації та комплексів технічного захисту інформації **Б4.З7.** Методи техніко-економічного аналізу та обґрунтування проектних рішень **Б4**.**З8.** Процедури активізації (настроювання) механізмів захисту інформації в інформаційних системах **Б4**.**З9.** Процедури підключення до локальної мережі підприємства	безперервності та доступності **Б4.У3.** Аналізувати проєктні обмеження та можливі компроміси системи безпеки інформації (комплексної системи захисту інформації) **Б4.У4.** Проєктувати, розробляти та модифікувати програмні системи, використовуючи науковий аналіз та математичні моделі для прогнозування та вимірювання результатів та наслідків проекту **Б4.У5.** Розробляти проєкти з кібербезпеки **Б4.У6**. Проєктувати функції управління ключами стосовно сфери кібербезпеки **Б4.У7.** Активізувати (налаштовувати) програмні механізми захисту інформації в	технічного захисту інформації з державними органами (установами, підприємствами)	

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		(організації) та до глобальних мереж та процедури активізації (настроювання) програмних мережевих механізмів захисту інформації **Б4**.**З10.** Концепції управління послугами для мереж і відповідних стандартів (ITIL) **Б4**.**З11.** Способи провадження апаратних засобів захисту інформації **Б4**.**З12.** Процедури активізації (настроювання) програмних мережних механізмів захисту інформації	інформаційних системах, електронних комунікаційних та інформаційно-комунікаційних системах (програмні фільтри, антивірусні програми, антишпигунське програмне забезпечення) **Б4.У8.** Впроваджувати (налаштовувати) програмно-апаратні засоби захисту інформації в інформаційних системах, електронних комунікаційних та інформаційно-комунікаційних системах **Б4.У9.** Впроваджувати (налаштовувати) програмні та програмно-апаратні засоби захисту мережних комунікацій **Б4.У10.** Впроваджувати (налаштовувати) апаратні засоби захисту		

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
			інформації на об’єктах інформаційної діяльності		
	Б5.Здатність розробляти, впроваджувати та аналізувати та обґрунтовувати технічні документи, положення, інструкції щодо систем та комплексів захисту інформації	**Б5.З1.** Систему технічних документів щодо систем та комплексів захисту інформації **Б5.З2**. Вимоги до структури та змісту технічних документів щодо систем та комплексів захисту інформації **Б5.З3**. Вимоги та підходи до розроблення технічних документів положень, інструкцій, методичних матеріалів щодо систем та комплексів захисту інформації **Б5.З4.** Сучасні підходи до формування вимог до захисту інформації в інформаційно-комунікаційних системах та на об’єктах	**Б5.У1.** Формувати (брати участь у формуванні) вимог до захисту інформації в інформаційно-комунікаційних системах та на об’єктах інформаційної діяльності **Б5.У2.** Розробляти (брати участь у розробці) політики безпеки інформації в інформаційно-комунікаційних системах **Б5.У3.** Розробляти (брати участь у розробці) технічної та експлуатаційної документації щодо створення, державної експертизи, (атестації), ведення в експлуатацію, експлуатації систем та	**Б5.К1.** Розробляти та модифікувати системи захисту інформації, їхні прототипи за допомогою робочих моделей або теоретичних моделей, із залученням з зацікавлених сторін. **А1.К1.** Спілкуватися з питань виконання завдань технічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **А1.К2.** Формувати запити / відповіді в рамках листування з питань	**Б5.В1**. Визначати та скеровувати виправлення технічних проблем, що виникають при впровадженні нових систем та комплексів захисту інформації. **А1.В1.** Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері захисту інформації, кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання технічного захисту інформації під контролем провідного фахівця

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		інформаційної діяльності **Б5.З5.** Інструменти, методи і техніки проектування систем, включаючи інструменти автоматизованого аналізу та проектування систем	комплексів захисту інформації **Б5.У4.** Застосовувати інструменти, методи і техніки проектування систем, включаючи інструменти автоматизованого аналізу та проектування систем **Б5.У5.** Розробляти плани аварійного відновлення та безперервності операцій в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах	технічного захисту інформації з державними органами (установами, підприємствами)	підприємства (установи, організації
	Б6. Здатність виявляти закладні пристрої на об’єктах інформаційної діяльності	**Б6.З1.** Поняття закладних пристроїв для зняття інформації, що озвучується та/або обробляється на об’єкті інформаційної діяльності **Б6.З2.** Класифікацію закладних пристроїв	**Б6.У1.** Розробляти методику пошуку, локалізації та виявлення закладних пристроїв на об’єктах інформаційної діяльності **Б6.У2.** Здійснювати пошук, локалізацію та виявлення закладних	**Б6.К1.**Застосовувати визначені правила та особливості проведення контрольно-пошукових робіт у взаємодії з профільними	**Б6.В1.**Здійснювати оцінку захищеності інформації, що циркулює на об’єктах інформаційної діяльності. **А1.В1.**Демонструвати обізнаність про

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		Б6.З3. Принцип дії закладних пристроїв основних класів **Б6.З4.** Методи пошуку, локалізації та виявлення закладних пристроїв на об'єктах інформаційної діяльності	пристроїв на об'єктах інформаційної діяльності **Б6.У3.** Складати акти за результатами пошуку та виявлення закладних пристроїв на об'єктах інформаційної діяльності **Б6.У4.** Здійснювати пошук та локалізації джерел небезпечних радіосигналів	працівниками та партнерами. **А1.К1.** Спілкуватися з питань виконання завдань технічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **А1.К2.** Формувати запити / відповіді в рамках листування з питань технічного захисту інформації з державними органами (установами, підприємствами)	законодавчо визначену відповідальність за порушення в сфері захисту інформації, кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання технічного захисту інформації під контролем провідного фахівця підприємства (установи, організації
	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				

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
В. Розробка, впровадження та супроводження організаційно-технічних заходів з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах, виявлення небезпечних сигналів на об’єктах інформаційної діяльності	**В1.**Здатність проводити всебічну оцінку застосованих в системі технічних заходів безпеки та їх удосконалень для визначення результативності контролів	**В1.З1.**Загальні положення теорії надійності, методи діагностики працездатності та виявлення місця відмов в комп'ютерних системах, системах та комплексах захисту інформації **В1.З2.**Принципи стійкості і надмірності в комп’ютерних системах та комплексах захисту інформації **В1.З3.** Сучасні методи оцінки, впровадження організаційно-технічних заходів. **В1.З4.** Порядок виявлення та усунення несправностей технічних заходів безпеки, що використовують концепції та можливості на основі стандартів. **В1.З5.** Шляхи утворення небезпечних сигналів на	**В1.У1**. Розпізнавати технічну інформацію, яка може бути використана для потенційних клієнтів при проведенні аналізу метаданих. **В1.У2.** Виявляти технічну інформацію, яка може бути використана для розробки цілі, включаючи розробку розвідки **В1.У3.**Тестувати і оцінювати інструменти для впровадження засобів протидії. **В1.У4.** Застосовувати метод синтезу даних з наявних даних для забезпечення нових або продовження проведеного збору інформації **В1.У5.** Визначати комунікаційні мережі цілі.	**В1.К1**. Організовувати спільно з профільними працівниками та партнерами проведення перевірок стану ТЗІ **А1.К1.** Спілкуватися з питань виконання завдань технічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **А1.К2.** Формувати запити / відповіді в рамках листування з питань технічного захисту інформації з державними органами (установами, підприємствами)	**В1.В1.** Перевіряти виконання вимог нормативно-правових актів з питань ТЗІ та в оцінюванні захищеності інформації на об’єкті, де вона циркулюватиме або циркулює. **А1.В1.** Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері захисту інформації, кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання технічного захисту інформації під контролем провідного фахівця підприємства

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		об’єкті інформаційної діяльності. **В1.З6.** Порядок визначення номенклатури вітчизняних засобів обчислювальної техніки та базового програмного забезпечення, оргтехніки, обладнання мереж зв’язку, призначених для оброблення інформації з обмеженим доступом інших засобів забезпечення ТЗІ	**В1.У6.** Оцінювати сучасні технічні засоби з метою визначення необхідності їх подальшого вдосконалення **В1.У7.** Виправляти фізичні та технічні проблеми, що впливають на роботу інформаційно-комунікаційних систем **В1.У8.** Класифікувати порушення з ТЗІ		(установи, організації
	В2.Здатність проводити періодичне обслуговування технічних засобів, комплексних систем захисту інформації та комплексів технічного захисту інформації	**В2.З1**. Загальні положення теорії надійності, методи діагностики працездатності та виявлення місця відмов в комп'ютерних системах, системах та комплексах захисту інформації **В2.З3.** Узагальнені етапи побудови комплексних	**В2.У1.**Здійснювати контроль працездатності комп'ютерних систем, систем та комплексів захисту інформації **В2.У2.** Діагностувати несправне апаратне забезпечення системи/сервера **В2.У3.** Застосовувати засоби контролю	**В2.К1.**Забезпечувати у взаємодії з профільними працівниками та партнерами підтримку, адміністрування та технічне обслуговування, необхідне для забезпечення ефективної та	**В2.В1.**Рекомендувати нові або переглядати існуючі заходи безпеки, стійкості та надійності на основі результатів перевірок **В2.В2**.Застосовувати в інформаційних системах технічні та програмні,

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		систем захисту інформації в автоматизованих системах. **В2.З4.** Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів **В2.З5**. Вимоги до технічних засобів інформації, що використовуються при створенні комплексів технічного захисту інформації **В2.З6**. Методику оцінки захищеності інформації від витоку технічними каналами **В1.З2.**Принципи стійкості і надмірності в комп'ютерних системах та комплексах захисту інформації	працездатності та виявлення місця відмов **В2.У4.** Виявляти місця відмов в комп'ютерних системах, системах та комплексах захисту інформації **В2.У5.**Організовувати (проводити) ремонт апаратних засобів захисту інформації зі складу комплексних систем захисту інформації та комплексів технічного захисту інформації	продуктивної роботи систем захисту **В2.К2**.Застосовувати в інформаційних системах технічні та програмні, організаційні засоби для реалізації заходів захисту	організаційні засоби для реалізації заходів захисту

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю конструювання; бібліотечні ресурси, архівні матеріали (за потреби); законодавчо-нормативні акти, акти роботодавця відповідного спрямування				
Г. Контроль за виконанням заходів ТЗІ та за ефективністю цього захисту інженерно-технічними заходами та засобами з метою забезпечення порядку доступу, конфіденційності, цілісності та доступності (унеможливлення блокування) інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави	**Г1**. Здатність проводити оцінку відповідності (атестацію) комплексів ТЗІ	**Г1.З1.** Поняття атестації комплексів технічного захисту інформації **Г1.З2.** Порядок, умови та організація проведення атестації комплексів технічного захисту інформації **Г1.З3.** Поняття та загальний зміст програми та методики проведення атестації комплексів технічного захисту інформації **Г1.З4.** Техніко-технологічне, комп'ютерне, програмне та інше забезпечення атестації комплексів технічного захисту інформації **Г1.З5.** Засоби вимірювальної техніки та методики вимірювань	**Г1.У1.** Складати програму та методику атестації комплексу ТЗІ **Г1.У2.** Здійснювати перевірку повноти і відповідності реалізованих заходів із захисту інформації вимогам технічного завдання на створення комплексу ТЗІ (або на створення КСЗІ в ІТС в частині вимог до захисту інформації від витоку технічними каналами), нормативно-правових актів та нормативних документів системи ТЗІ **Г1.У3.** Здійснювати інструментальний контроль захищеності інформації на об'єкті інформаційної	**Г1.К1**. Керуватися нормативно-правовими актами та нормативними документами з технічного захисту інформації, що необхідні для проведення робіт з ТЗІ із залученням профільних працівників та партнерів **А1.К1.** Спілкуватися з питань виконання завдань технічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації)	**Г1.В1**. Проводити аналіз та надавати рекомендації щодо вдосконалення заходів з ТЗІ в приміщеннях, в яких циркулює інформація з обмеженим доступом **Г1.В2.** Здійснювати розробку політики безпеки та технічного завдання при проєктуванні КСЗІ

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		оцінюваних показників комплексів технічного захисту інформації **Г1.З6.** Документи, що оформлюються за результатами атестації комплексів технічного захисту інформації	діяльності від витоку технічними каналами **Г1.У4.** Робити висновки щодо відповідності комплексу ТЗІ вимогам технічного завдання на створення комплексу ТЗІ (або на створення КСЗІ в ІТС в частині вимог до захисту інформації від витоку технічними каналами), нормативно-правових актів та нормативних документів системи ТЗІ **Г1.У5.** Оформлювати протоколи інструментального контролю захищеності інформації на об’єкті інформаційної діяльності. **Г1.У6.** Оформлювати акти атестації комплексів ТЗІ та організовувати їх затвердження і реєстрацію	**А1.К2.** Формувати запити / відповіді в рамках листування з питань технічного захисту інформації з державними органами (установами, підприємствами)	

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
	Г2. Здатність проводити оцінку відповідності (державну експертизу) КСЗІ та засобів ТЗІ	**Г2.З1.** Поняття та шляхи проведення державної експертизи КСЗІ та засобів ТЗІ **Г2.З2.** Порядок, умови та організація проведення державної експертизи КСЗІ та засобів ТЗІ **Г2.З3.** Поняття та загальний зміст програми та методики проведення державної експертизи комплексних систем захисту інформації та засобів технічного захисту інформації **Г2.З4.** Методи тестування та оцінки захищеності систем **Г2.З5.** Техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності комплексних систем захисту інформації	**Г2.У1.** Складати програму та методику проведення державної експертизи КСЗІ **Г2.У2.** Проводити попереднє ознайомлення з об'єктом експертизи та поглиблене обстеження об'єкта експертизи **Г2.У3.** Проводити експертні випробування та дослідження КСЗІ (оцінювати функціональні послуги безпеки, оцінювати рівні гарантій коректності реалізації функціональних послуг безпеки, перевіряти наявність зареєстрованого акту атестації комплексу ТЗІ, якщо такий комплекс входить до складу КСЗІ, або проводити його атестацію) **Г2.У4.** Оформлювати протоколи експертних	**Г2.К1.** Виявляти із залученням профільних працівників та партнерів системи критичної інфраструктури з інформаційно-комунікаційними технологіями, які були спроектовані без урахування безпеки системи. **А1.К1.** Спілкуватися з питань виконання завдань технічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації)	**Г2.В1**. Оцінювати ефективність заходів із ТЗІ, які використовуються на об'єкті експертизи. **А1.В1.** Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері захисту інформації, кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання технічного захисту інформації під контролем провідного фахівця підприємства (установи, організації

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		Г2.З6. Засоби ви мірю вальної техніки та методики вимірювань оцінюваних показників комплексних систем захисту інформації та характеристик засобів технічного захисту інформації **Г2.З7.** Документи, що оформлюються за результатами державної експертизи КСЗІ та засобів ТЗІ	випробувань та атестати відповідності КСЗІ **Г2.У5.** Здійснювати експертизу КСЗІ шляхом декларування, оформлювати декларації відповідності КСЗІ та організовувати їх затвердження і реєстрацію **Г2.У6.** Здійснювати експертизу засобів ТЗІ, оформлювати протоколи експертних випробувань засобів ТЗІ та експертні висновки на засоби ТЗІ, організовувати затвердження і реєстрацію експертних висновків		
	Г3. Здатність проводити оцінку відповідності СУІБ	**Г3.З1.** Поняття оцінки відповідності СУІБ **Г3.З2.** Порядок, умови та організація проведення оцінки відповідності СУІБ **Г3.З3.** Документи, що оформлюються за	**Г3.У1.** Здійснювати оцінку відповідності (брати участь в оцінці відповідності) СУІБ відповідно до стандартів ДСТУ ISO/IEC серії 27k **Г3.У2.** Аналізувати політику та конфігурації СУІБ організації та	**Г3.К1.** Використовувати із залученням профільних працівників та партнерів опубліковані нормативні документи,	**Г3.В1.** Проводити процес виконання політики безпеки (знаходити і виправляти слабкі місця в системі інформаційної безпеки).

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		результатами оцінки відповідності СУІБ	оцінювати її відповідність нормативним актам та нормативним документам з питань безпеки інформації та кібербезпеки та нормативним актам та директивам організації **Г3.У3.** Аналізувати проектні обмеження, компроміси та детальний проект СУІБ організації **Г3.У4.** Оцінювати ефективність заходів із захисту інформації, заходів з режиму та управління доступом, заходів з кібербезпеки, які використовуються СУІБ організації **Г3.У5.** Переконуватися, що усі операції з безпеки та їх технічна підтримка належним чином задокументовані та оновлюються в разі необхідності	стандарти для управління інформаційною безпекою **А1.К2.** Формувати запити / відповіді в рамках листування з питань технічного захисту інформації з державними органами (установами, підприємствами)	**А1.В.** Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері захисту інформації, кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання технічного захисту інформації під контролем провідного фахівця підприємства (установи, організації

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
			ГЗ.У6. Переконуватися, що вимоги із захисту інформації та кібербезпеки інтегровані в планування безперервного функціонування системи та/або організації **ГЗ.У7.** Здійснювати технічну оцінку програмного забезпечення прикладних програм, СУІБ чи мережі, а також реалізованих заходів із кіберзахисту вимогам кібербезпеки та можливим вразливостям **ГЗ.У8.** Оформлювати документи за результатами оцінки відповідності СУІБ		
	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				

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
Д. Розробка порядку організації та проведення атестації комплексів ТЗІ, а також проведення робіт із сертифікації засобів забезпечення ТЗІ загального призначення або/чи спеціального призначення	**Д1**. Здатність розробляти, впроваджувати й управляти стратегією організації комплексів ТЗІ	**Д1.З1.** Чинні закони, нормативні акти, директиви, постанови у сфері технічного захисту **Д1.З2.** Нормативні документи на засоби забезпечення ТЗІ, методи їх випробування. **Д1.З3.** Розуміння дестабілізуючих чинників і загроз для інформаційних ресурсів	**Д1.У1.**Здійснювати організацію робіт зі створення і використання комплексів ТЗІ на об’єкті інформаційної діяльності **Д1.У2.**Розробляти технічну документацію відповідного спрямування **Д1.У3.** Проводити роботи з атестації ТЗІ **Д1.У4.** Визначати схему сертифікації засобів забезпечення ТЗІ за поданою заявкою **Д1.У5**. Здійснювати своєчасне виявлення і знешкодження загроз для ресурсів комплексів ТЗІ, причин та умов, які можуть призвести до порушення її функціонування **Д1.У6.** Проводити НДР, пов’язані з пошуком шляхів реалізації	**Д1.К1**. Забезпечувати із залученням профільних працівників та партнерів практичне вирішення проблем ТЗІ **Д1.К1**. Із залученням профільних працівників та партнерів ~~з~~дійснювати своєчасне виявлення і знешкодження загроз для ресурсів комплексів ТЗІ, причин та умов, які можуть призвести до порушення її функціонування	**Д1.В1.** Розробляти звітні документи за результатами проведення робіт із сертифікації засобів забезпечення ТЗІ. **А1.В1.** Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері захисту інформації, кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання технічного захисту інформації під контролем провідного фахівця підприємства (установи, організації

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
			завдання на створення КСЗІ		
	Д2. Здатність аналізувати умови функціонування ОІД, технічну документацію на комплекс ТЗІ, розробляти і оформляти програму та методику атестації (ПМА)	**Д2.З1.** Розуміння основних організаційних процесів ТЗІ **Д2.З2.** Порядок аналізу принципів управління ресурсами. **Д2.З3.** Вимоги до документації, що описує результати створення системи ТЗІ	**Д2.У1.** Проводити випробування відповідно до програми атестації, оформляти протоколи випробування **Д2.У2.**Оформлювати акт атестації комплексів ТЗІ відповідно до нормативних документів **Д2.У3.** Складати висновок щодо відповідності стану ТЗІ, що відповідає вимогам нормативних документів з ТЗІ	**Д2.К1**. Застосовувати на практиці із залученням профільних працівників та партнерів етичні вимоги щодо організації атестації комплексів ТЗІ. **А1.К1.** Спілкуватися з питань виконання завдань технічного захисту інформації в рамках робочих колективів на підприємстві (установі, організації) **А1.К2.** Формувати запити / відповіді в рамках листування з питань технічного захисту	**Д2.В1.** Координувати роботу із своєчасної та якісної підготовки розроблення систем ТЗІ. **А1.В1.** Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері захисту інформації, кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання технічного захисту інформації під контролем провідного фахівця підприємства (установи, організації

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
				інформації з державними органами (установами, підприємствами)	
	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				
Е. Розроблення порядку організації та проведення державної експертизи в сфері ТЗІ, підготовка документів щодо надання експертного висновку та атестата відповідності	**Е1**. Здатність аналізувати, оцінювати апаратні та програмні засоби ТЗІ з метою оцінки їх відповідності вимогам нормативних документів із ТЗІ та можливості їх використання для забезпечення ТЗІ.	**Е1.З1.** Вимоги нормативно-правових актів, що визначають порядок організації робіт із захисту інформації в сфері технічного захисту **Е1.З2**. Вимоги до експлуатаційної документації **Е1.З3.** Перелік засобів ТЗІ, призначений для використання суб'єктами системи ТЗІ під час розроблення, модернізації та	**Е1.У1.** Адаптувати аналіз до необхідних рівнів (наприклад, класифікаційного та організаційного **Е1.У2**. Проводити аналіз, що допомагає при написанні поетапних звітів після проведеного заходу **Е1.У3**. Готувати звітні документи з аудиторської перевірки, які містять технічні та процедурні висновки, а також рекомендувати	**Е1.К1**. Проводити із залученням профільних працівників та партнерів огляди систем ТЗІ для усунення вразливостей, які були виявлені під час перевірки. **А1.К1.** Спілкуватися з питань виконання завдань технічного захисту інформації в рамках робочих колективів на	**Е1.В1.** Здійснювати експлуатацію та підтримку автоматизованих систем для отримання і здійснення доступу до цільових систем **А1.В1.** Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері захисту інформації, кібербезпеки та

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
		впровадження комплексів ТЗІ	коригування стратегій/рішень	підприємстві (установі, організації)	інформаційної безпеки **А1.В2.** Виконувати відповідні завдання технічного захисту інформації під контролем провідного фахівця підприємства (установи, організації
	Е2. Здатність проводити дослідження, перевірку, аналіз, оцінку об'єктів експертизи щодо їх відповідності вимогам нормативних документів із ТЗІ	**Е2.З1.** Програми та методики, згідно з якими може здійснюватися оцінка об'єкта експертизи **Е2.З2.** Критерії оцінки захищеності інформації від несанкціонованого доступу. **Е2.З3.** Порядок організації та проведення державної експертизи у сфері ТЗІ	**Е2.У1.** Уміти якісно та правомірно оформляти результати перевірок для оформлення експертного висновку. **Е2.У2.**Оформлюва-ти розгорнутий висновок щодо відповідності об'єкта експертизи вимогам нормативних документів із ТЗІ **Е2.У3.** Проводити **а**наліз середовища функціонування КСЗІ на відповідність вимогам НД ТЗІ	**Е2.К1**. Оброблювати спільно з профільними працівниками та партнерами зібрані дані для подальшого їх аналізу **А1.К2.** Формувати запити / відповіді в рамках листування з питань технічного захисту інформації з державними органами	**Е2.В1.** Аналізувати політику та конфігурації кіберзахисту організації та оцінювати відповідність нормативним актам та директивам організаці. **А1.В1.** Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері захисту інформації,

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
				(установами, підприємствами)	кібербезпеки та інформаційної безпеки **А1.В2.** Виконувати відповідні завдання технічного захисту інформації під контролем провідного фахівця підприємства (установи, організації)
	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: Фахівець з технічного захисту інформації		
	Молодший фахівець з технічного захисту інформації	Фахівець з технічного захисту інформації	Провідний фахівець з технічного захисту інформації
	повна	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/Учасник 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 Григорійович, 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 технічного 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 технічного 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