ЗАТВЕРДЖЕНО
Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України
29.12.2025 № 865

Професійний стандарт

ФАХІВЕЦЬ ІЗ ЗАХИСТУ ТА СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

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 схваленого рішенням від 17.12.2025 № 6 Національного агентства кваліфікацій (відповідно до протоколу засідання Національного агентства кваліфікацій від 17.12.2025 № 67 (261)) 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 № 373;

висновку Профспілки працівників Збройних Сил України від 10.11.2025 № 54 щодо погодження проєкту професійного стандарту.

1. Назва професійного стандарту.

Фахівець із захисту та стійкості критичної інфраструктури.

2. Загальні відомості про професійний стандарт:

1) мета діяльності за професією

забезпечення безпечного функціонування об'єктів критичної інфраструктури, зокрема налагодження та підтримання функціонування ефективної системи захисту об'єктів критичної інфраструктури, виконання об'єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, оперативне реагування на протиправні дії, фізичні атаки проти об'єкта критичної інфраструктури, а також забезпечення відновлення функціонування об'єктів критичної інфраструктури в разі виникнення аварій та інших небезпечних подій, вчинення протиправних дій;

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» (за потреби);

3) назва (назви) професії (професій) та її (їх) код (коди) згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій».

Фахівець із захисту та стійкості критичної інфраструктури, 2490;

4) узагальнена назва професії (за потреби);

5) назви типових посад (за потреби);

6) назва (назви) професійної (професійних) кваліфікації (кваліфікацій), її (їх) рівень (рівні) згідно з Національною рамкою кваліфікацій.

Фахівець із захисту та стійкості критичної інфраструктури, 6 рівень НРК.

Провідний фахівець із захисту та стійкості критичної інфраструктури, 6 рівень НРК;

7) назва (назви) документа (документів), що підтверджує (підтверджують) професійну кваліфікацію особи:

- сертифікат про присвоєння/підтвердження професійної кваліфікації «Фахівець із захисту та стійкості критичної інфраструктури»;
- сертифікат про присвоєння/підтвердження професійної кваліфікації «Провідний фахівець із захисту та стійкості критичної інфраструктури»;
- інші документи, що підтверджують професійну кваліфікацію.

3. 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)

Назва професійної та/або часткової професійної кваліфікації	**Суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій**	
	кваліфікаційні центри	**суб'єкти освітньої діяльності/інші уповноважені законодавством суб'єкти**
Фахівець із захисту та стійкості критичної інфраструктури	Підготовка на початковому (короткий цикл) рівні вищої освіти за спеціальностями (диплом, сертифікат, тощо), галузями знань: A Освіта; D Бізнес, адміністрування та право; E Природничі науки, математика та статистика; F Інформаційні технології; G Інженерія, виробництво та будівництво; H Сільське, лісове, рибне господарство та ветеринарна медицина; I Охорона здоров'я та соціальне забезпечення; J Транспорт та послуги; K Безпека та оборона. Додатково (за необхідності або/чи вимогою суб'єкта, уповноваженого законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій): - документ (диплом, сертифікат тощо) щодо післядипломної освіти та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері захисту критичної інфраструктури; - документ щодо професійної сертифікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері захисту критичної інфраструктури; - без вимог до стажу роботи.	Не передбачено професійним стандартом

2) професійний розвиток:

з присвоєнням наступного/вищого рівня 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/інші уповноважені законодавством суб'єкти**
Провідний фахівець із захисту та стійкості критичної інфраструктури	Стаж роботи за професійною кваліфікацією «Фахівець із захисту та стійкості критичної інфраструктури» не менше ніж 1 рік	Не передбачено професійним стандартом

без присвоєння наступного/вищого рівня професійної кваліфікації:

для удосконалення (підтримання) професійної кваліфікації, в тому числі шляхом набуття нових/додаткових навичок/компетентностей, удосконалення (підтримання) наявного рівня професійної кваліфікації здійснюється не рідше ніж один раз на 5 (п'ять) років, у тому числі шляхом набуття нових/додаткових навичок/компетентностей (зокрема, але не виключно, безкоштовних онлайн-курсів та інших навчальних заходів, у тому числі організованих із залученням коштів міжнародної технічної допомоги).

4. Абревіатури, скорочення (за потреби)

КІ	критична інфраструктура
НПА	нормативно-правові акти
НСЗКІ	національна система захисту критичної інфраструктури
ОКІ	об'єкт критичної інфраструктури

5. Опис трудових функцій:

Трудові функції (умовне позначення та назва)	Компетентності	Результати навчання			
		знання	**уміння/навички**	**комунікація**	**відповідальність і автономія**
А. Ідентифікація та категоризація ОКІ.	**А1.** Здатність збирати та узагальнювати дані, інформацію, цифровий контент про об'єкти (установи, організації тощо), системи, активи підприємства, визначати їхні критичні послуги/функції та виявляти взаємозалежності з іншими об'єктами або секторами КІ.	**А1.З1.** Законодавство України та НПА у сфері захисту КІ (закони, постанови Кабінету Міністрів України, накази та методичні рекомендації тощо). **А1.З2.** Міжнародні стандарти та найкращі практики з ідентифікації та категоризації КІ. **А1.З3.** Галузева специфіку функціонування сектору КІ. **А1.З4.** Методології (методи, методики), показники та критерії ідентифікації та категоризації ОКІ. **А1.З5.** Принципи надання життєво важливих послуг та/або функцій, та їхній вплив на життєдіяльність	**А1.У1.** Аналізувати та інтерпретувати вимоги НПА щодо ідентифікації та категоризації ОКІ для їх застосування на практиці. **А1.У2.** Збирати інформацію про ОКІ (його структуру, технологічні процеси, послуги, персонал, ІТ-системи, фізичні активи тощо) з різних джерел. **А1.У3.** Визначати рівні негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування ОКІ. **А1.У4.** Виявляти та документувати взаємозалежності між об'єктом, що ідентифікується, та	**А1.К1.** Налагоджувати та підтримувати зв'язки з представниками ОКІ, а також із представниками суб'єктів НСЗКІ. **А1.К2.** Висловлювати думки у письмовій та усній формі, пояснюючи вимоги до збору інформації та результати її аналізу. **А1.К3.** Проводити переговори та опитування з персоналом та керівництвом ОКІ для отримання необхідних даних. **А1.К4.** Обговорювати та узгоджувати з представниками ОКІ зібрану інформацію, її повноту та достовірність.	**А1.В1.** Планувати та організовувати свою діяльність у межах визначених завдань з ідентифікації та збору інформації про ОКІ. **А1.В2.** Нести відповідальність за повноту, достовірність та актуальність зібраної та узагальненої інформації, що є основою для подальшої категоризації та розробки заходів захисту та стійкості. **А1.В3.** Приймати обґрунтовані рішення щодо методів збору даних, цифрового контенту та їхньої верифікації у межах своєї компетенції. **А1.В4.** Взаємодіяти з внутрішніми підрозділами ОКІ, за

Трудові функції (умовне позначення та назва)	Компетентності	Результати навчання			
		знання	**уміння/навички**	**комунікація**	**відповідальність і автономія**
		держави та суспільства. **А1.З6.** Види взаємозалежностей між об'єктами КІ. **А1.З7.** Типи активів підприємства та їхня роль у наданні критичних послуг. **А1.З8.** Секторальні та міжсекторальні показники та критерії оцінки рівнів негативного впливу у разі знищення, пошкодження або порушення функціонування ОКІ. **А1.З9.** Методи збору, систематизації та верифікації даних, інформації та цифрового контенту.	іншими об'єктами або секторами КІ. **А1.У5.** Оцінювати значущість активів ОКІ для надання критичних послуг та їхній внесок у загальну стійкість. **А1.У6.** Систематизувати та узагальнювати великі обсяги інформації. **А1.У7.** Критично оцінювати достовірність отриманої інформації та виявляти потенційні невідповідності або прогалини. **А1.У8.** Працювати з базами даних, цифровим контентом та інформаційними системами, що використовуються для зберігання та управління інформацією про ОКІ.	**А1.К5.** Готувати та презентувати результати ідентифікації та категоризації ОКІ.	необхідності, із зовнішніми зацікавленими сторонами для отримання необхідної інформації. **А1.В5.** Ініціювати коригувальні дії у разі виявлення невідповідностей або неточностей у зібраній інформації. **А1.В6.** Працювати під загальним керівництвом, самостійно обирати шляхи та методи виконання поставлених завдань на підставі власного досвіду та знань. **А1.В7.** Відповідати за дотримання вимог конфіденційності та безпеки при роботі з інформацією з обмеженим доступом.

Трудові функції (умовне позначення та назва)	Компетентності	Результати навчання			
		знання	**уміння/навички**	**комунікація**	**відповідальність і автономія**
			А1.У9. Комунікувати з представниками суб'єктів НСЗКІ, зовнішніми експертами та державними органами для отримання необхідної інформації та обговорення результатів. **А1.У10.** Проводити розрахунки та готувати обґрунтовані пропозиції щодо віднесення ОКІ до однієї з категорій критичності.		
	А2. Здатність визначати категорію критичності ідентифікованого об'єкта відповідно до вимог законодавства України (законів, постанов, відомчих актів).	**А2.З1.** Нормативно-правові акти України, що регулюють сферу захисту КІ, постанови Кабінету Міністрів України, відомчі нормативно-правові документи та методичні рекомендації в частині, що	**А2.У1.** Використовувати документи, що визначають порядок, механізми та процедуру ідентифікації та категоризації ОКІ. **А2.У2.** Визначати показники та критерії категоризації ОКІ.	**А2.К1**. Чітко та аргументовано пояснювати критерії та процес категоризації ОКІ представникам ОКІ та іншим зацікавленим сторонам. **А2.К2**. Надавати роз'яснення щодо законодавчих вимог	**А2.В1.** Відповідати за правильність та обґрунтованість визначення категорії критичності об'єктів відповідно до вимог законодавства. **А2.В2.** Діяти автономно у межах наданих повноважень при застосуванні

Трудові функції (умовне позначення та назва)	Компетентності	Результати навчання			
		знання	**уміння/навички**	**комунікація**	**відповідальність і автономія**
		стосується ідентифікації та категоризації ОКІ. **А2.З2.** Показники та критерії віднесення ОКІ до відповідних категорій, визначені нормативно-правовими актами України. **А2.З3.** Основи ризик-менеджменту у контексті захисту КІ.	**А2.У3.** Узагальнювати та аналізувати інформацію про об'єкт (його послуги, функції та взаємозалежності) для визначення його категорії критичності. **А2.У4.** Формулювати чіткі та обґрунтовані висновки щодо віднесення об'єкта до певної категорії критичності. **А2.У5.** Взаємодіяти з технічними фахівцями та експертами для отримання додаткових даних, необхідних для категоризації. **А2.У6.** Готувати відповідну документацію (протоколи, висновки, обґрунтування) для подання результатів	та наслідків віднесення об'єкта до певної категорії. **А2.К3**. Вести конструктивний діалог під час обговорення спірних питань щодо категоризації, знаходячи консенсус. **А2.К4**. Формулювати висновки щодо категоризації об'єктів у зрозумілій формі для різних аудиторій. **А2.К5**. Готувати презентації та доповіді щодо результатів категоризації.	методологій категоризації та підготовці відповідних висновків. **А2.В3.** Відповідати за дотримання встановлених термінів виконання завдань щодо категоризації об'єктів. **А2.В4.** Ініціювати внесення змін до категорії критичності об'єктів у разі зміни їх функціоналу, взаємозалежностей або нормативно-правової бази. **А2.В5.** Взаємодіяти з уповноваженими державними органами та суб'єктами господарювання з питань категоризації об'єктів, забезпечуючи

Трудові функції (умовне позначення та назва)	Компетентності	Результати навчання			
		знання	**уміння/навички**	**комунікація**	**відповідальність і автономія**
			категоризації до відповідних секторальних органів у сфері захисту КІ.		належний рівень конфіденційності. **А2.В6.** Забезпечувати підтримання актуальність даних про категоризацію об'єктів.
	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 (за потреби); профільна наукова та методична література; правила та інструкції відповідного спрямування.				
Б. Виконання заходів із забезпечення захисту та стійкості ОКІ.	**Б1.** Здатність виконувати заходи із забезпечення захисту та стійкості ОКІ – як фізичних, так і кібернетичних, реагувати на протиправні дії, кризові ситуації, інциденти на ОКІ та ліквідації їх наслідків.	**Б1.З1.** Нормативно-правові акти у сфері захисту КІ, кібербезпеки та фізичного захисту. **Б1.З2.** Принципи та механізми функціонування ОКІ та надання життєво важливих послуг та/або функцій. **Б1.З3.** Методології та інструменти фізичного захисту, включаючи системи контролю доступу,	**Б1.У1.** Організовувати та безпосередньо, у разі потреби, виконувати заходи фізичного захисту, включаючи контроль доступу до об'єкта, моніторинг периметра та реагування на фізичні загрози. **Б1.У2.** Організовувати та безпосередньо, у разі потреби, виконувати заходи кіберзахисту,	**Б1.К1**. Злагоджено взаємодіяти з внутрішніми командами (IT-фахівцями, службою безпеки, операційним персоналом) під час виконання заходів із забезпечення захисту та стійкості ОКІ. **Б1.К2**. Оперативно інформувати керівництво та зацікавлені сторони про виявлені загрози,	**Б1.В1.** Відповідати за своєчасне та ефективне виконання заходів захисту та реагування на інциденти, що можуть призвести до порушення функціонування ОКІ. **Б1.В2.** Діяти автономно при виконанні заходів щодо локалізації загроз та мінімізації їх наслідків.

Трудові функції (умовне позначення та назва)	Компетентності	Результати навчання			
		знання	**уміння/навички**	**комунікація**	**відповідальність і автономія**
		відеоспостереження, периметральну охорону та охоронну сигналізацію. **Б1.З4.** Процедури реагування на інциденти, включаючи ідентифікацію, локалізацію, усунення та відновлення. **Б1.З5.** Методи та засоби ліквідації наслідків кризових ситуацій, відновлення функціонування надання життєво важливих функцій та/або послуг.	зокрема налаштовувати та адмініструвати засоби захисту інформації, контролювати мережевий трафік, аналізувати журнали подій. **Б1.У3.** Оперативно виявляти та ідентифікувати інциденти безпеки та протиправні дії. **Б1.У4.** Своєчасно реагувати на інциденти відповідно до затверджених планів: локалізувати загрозу, мінімізувати збитки та відновлювати нормальне функціонування ОКІ. **Б1.У5.** Проводити базовий аналіз причин та наслідків інцидентів. **Б1.У6.** Забезпечувати безперервність	інциденти та хід реагування. **Б1.К3**. Координувати дії з іншими суб'єктами НСЗКІ під час кризових ситуацій.	**Б1.В3.** Відповідати за дотримання встановлених норм, регламентів та стандартів безпеки. **Б1.В4.** Звітувати про результати виконаних заходів та інцидентів вищому керівництву ОКІ. **Б1.В5.** Проявляти ініціативу в удосконаленні заходів захисту та профілактиці загроз. **Б1.В6.** Нести відповідальність за збереження конфіденційної інформації, отриманої в процесі виконання своїх обов'язків.

Трудові функції (умовне позначення та назва)	Компетентності	Результати навчання			
		знання	**уміння/навички**	**комунікація**	**відповідальність і автономія**
			надання життєво важливих функцій та/або послуг під час та після кризових ситуацій. **Б1.У7.** Використовувати технічні засоби захисту та моніторингу. **Б1.У8.** Документувати хід виконання заходів захисту та реагування на інциденти. **Б1.У9**. Готувати звіти про інциденти та проведені заходи з ліквідації наслідків.		
	Б2. Здатність виконувати заходи щодо відновлення функціонування ОКІ в разі виникнення аварій та інших небезпечних подій, вчинення протиправних дій.	**Б2.З1.** Нормативно-правові акти у сфері реагування на надзвичайні ситуації, ліквідації їх наслідків та відновлення функціонування ОКІ. **Б2.З2**. Принципи та архітектура функціонування ОКІ, їхні ключові системи,	**Б2.У1.** Оперативно активувати та виконувати затверджені плани відновлення функціонування ОКІ після виникнення аварій, небезпечних подій чи протиправних дій.	**Б2.К1.** Взаємодіяти з командою реагування на інциденти, операційним персоналом, ІТ-фахівцями та іншими внутрішніми підрозділами під час відновлювальних робіт.	**Б2.В1.** Відповідати за ефективність та своєчасність виконання заходів щодо відновлення функціонування ОКІ після аварій, небезпечних подій чи протиправних дій. **Б2.В2.** Діяти з високим ступенем

Трудові функції (умовне позначення та назва)	Компетентності	Результати навчання			
		знання	**уміння/навички**	**комунікація**	**відповідальність і автономія**
		компоненти та взаємозалежності, необхідні для швидкого відновлення. **Б2.З3.** Плани безперервності діяльності та плани відновлення після кризових ситуацій, їх структура, зміст та процедури активації. **Б2.З4.** Методи та методики оцінювання збитків та пріоритизації відновлювальних робіт після інцидентів або аварій. **Б2.З5.** Основи безпеки життєдіяльності та охорони праці під час проведення відновлювальних робіт в умовах аварій та надзвичайних подій. **Б2.З6.** Процедури взаємодії з	**Б2.У2.** Швидко оцінювати масштаби пошкоджень та збитків, визначати критичні ділянки для першочергового відновлення. **Б2.У3.** Виконувати дії з відновлення даних та систем, використовуючи резервні копії, альтернативні майданчики або інші методи. **Б2.У4.** Проводити тестування відновлених систем та сервісів для підтвердження їхньої працездатності та відповідності вимогам. **Б2.У5.** Локалізувати подальше поширення збоїв або пошкоджень, запобігаючи каскадним ефектам.	**Б2.К2.** Оперативно інформувати керівництво ОКІ про стан відновлення та прогнозовані терміни відновлення повного функціонування ОКІ. **Б2.К3.** Координувати свої дії з представниками аварійних служб, правоохоронних органів та інших суб'єктів НСЗКІ. **Б2.К4.** Готувати звіти про хід відновлення функціонування ОКІ.	автономії при виконанні завдань, визначених планами відновлення, приймаючи оперативні рішення у динамічних та стресових умовах. **Б2.В3.** Звітувати про хід відновлювальних робіт та їхні результати керівництву ОКІ. **Б2.В4.** Проявляти ініціативу в удосконаленні планів відновлення та підвищенні загальної стійкості ОКІ на основі отриманого досвіду. **Б2.В5.** Відповідати за дотримання вимог безпеки під час проведення відновлювальних робіт.

Трудові функції (умовне позначення та назва)	Компетентності	Результати навчання			
		знання	**уміння/навички**	**комунікація**	**відповідальність і автономія**
		аварійними службами, правоохоронними органами та іншими суб'єктами НСЗКІ під час ліквідації наслідків. **Б2.З7.** Типи та характеристики обладнання, що використовується для відновлювальних робіт.	**Б2.У6.** Взаємодіяти з технічним персоналом та зовнішніми підрядниками, координуючи їхні дії під час відновлювальних робіт. **Б2.У7.** Вести документацію щодо процесу відновлення, фіксувати етапи процесу, виявлені проблеми та прийняті рішення. **Б2.У8.** Проводити пост-інцидентний аналіз для виявлення корінних причин події та розробки заходів щодо запобігання подібним ситуаціям у майбутньому.		
	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 (за потреби); профільна наукова та методична література; правила та інструкції відповідного спрямування.				

Трудові функції (умовне позначення та назва)	**Компетентності**	**Результати навчання**			
		знання	**уміння/навички**	**комунікація**	**відповідальність і автономія**
В. Виконання заходів контролю стану захищеності та стійкості ОКІ.	**В1.** Здатність виконувати заходи щодо реалізації системи контролю стану захищеності та стійкості ОКІ, щодо проведення перевірок стану захищеності та стійкості ОКІ.	**В1.З1.** Нормативно-правові акти у сфері державного контролю, моніторингу та аудиту захисту КІ в частині, що стосується вимог до проведення перевірок, їх періодичності, процедур та повноважень. **В1.З2.** Методології, показники та критерії для оцінювання стану захищеності та стійкості ОКІ, безперервності його діяльності. **В1.З3.** Процедури документування результатів контролю та перевірок (формування актів, протоколів, висновків, пропозицій, рекомендацій тощо).	**В1.У1.** Налаштовувати та адмініструвати елементи системи контролю стану захищеності, включаючи сенсори, агенти, консолі моніторингу та платформи управління вразливостями. **В1.У2.** Проводити планові та позапланові перевірки стану захищеності та стійкості ОКІ за затвердженими методиками, програмами та чек-листами. **В1.У3.** Оцінювати відповідність впроваджених заходів захисту вимогам законодавства, стандартів, галузевих норм та внутрішніх	**В1.К1**. Пояснювати мету, завдання та методологію проведення перевірок та контролю стану захищеності персоналу та керівництву ОКІ. **В1.К2**. Надавати зворотний зв’язок щодо виявлених недоліків та вразливостей, обґрунтовуючи свої висновки та рекомендації. **В1.К3**. Ефективно взаємодіяти з операційним персоналом та керівництвом ОКІ для отримання необхідної інформації та роз’яснень. **В1.К4**. Готувати та презентувати результати перевірок та рекомендації у формі, зрозумілій для	**В1.В1.** Відповідати за об’єктивність, достовірність, неупередженість та повноту результатів моніторингу та проведених перевірок стану захищеності та стійкості ОКІ. **В1.В2.** Діяти автономно у межах затверджених програм та методик контролю, самостійно визначаючи послідовність дій, використання інструментів та пріоритетність завдань. **В1.В3.** Відповідати за своєчасне виявлення критичних вразливостей та потенційних загроз, що можуть вплинути на функціонування ОКІ. **В1.В4.** Ініціювати розробку або

Трудові функції (умовне позначення та назва)	Компетентності	Результати навчання			
		знання	**уміння/навички**	**комунікація**	**відповідальність і автономія**
		В1.З4. Структура та взаємодія суб'єктів НСЗКІ, їхні повноваження щодо контролю та обміну інформацією.	нормативних документів. **В1.У4.** Виявляти та документувати вразливості систем захисту та стійкості ОКІ. **В1.У5.** Формувати висновки та розробляти практичні рекомендації щодо підвищення рівня захищеності та стійкості ОКІ за результатами моніторингу. **В1.У6.** Документувати етапи проведення контролю та перевірок, оформлювати акти, протоколи та детальні звіти. **В1.У7.** Використовувати спеціалізоване програмне забезпечення та інструменти для автоматизації	різних цільових аудиторій. **В1.К5**. Вести ділове листування та складати офіційні документи (листи, запити, акти) за результатами контролю стану захищеності та стійкості ОКІ. **В1.К6**. Представляти результати контролю на зустрічах, нарадах та робочих групах.	удосконалення внутрішніх інструкцій та процедур контролю, а також механізмів реагування на виявлені порушення. **В1.В5.** Звітувати про результати своєї роботи керівництву ОКІ. **В1.В6.** Проявляти високий рівень самодисципліни та уваги при виконанні контрольних функцій, забезпечуючи високу якість роботи. **В1.В7.** Відповідати за дотримання вимог при роботі з інформацією з обмеженим доступом щодо контролю стану захищеності та стійкості ОКІ.

Трудові функції (умовне позначення та назва)	Компетентності	Результати навчання			
		знання	**уміння/навички**	**комунікація**	**відповідальність і автономія**
			процесів моніторингу, аналізу та аудиту.		
	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 (за потреби); профільна наукова та методична література; правила та інструкції відповідного спрямування.				
Г. Документальне забезпечення.	**Г1.** Здатність створювати, систематизувати та підтримувати в актуальному стані внутрішні розпорядчі, нормативні та звітні документи, що регламентують та відображають стан захищеності та стійкості ОКІ.	**Г1.З1.** Нормативно-правові акти у сфері у сфері захисту КІ. **Г1.З2.** Державні стандарти та галузеві нормативи, що регламентують розробку, оформлення та ведення документації з питань захисту та стійкості КІ. **Г1.З3.** Вимоги до внутрішніх розпорядчих документів та їхню юридичну силу. **Г1.З4.** Особливості документування	**Г1.У1.** Розробляти та редагувати внутрішні нормативні та розпорядчі документи, які регламентують захист та стійкість ОКІ, з урахуванням вимог законодавства та специфіки об'єкта. **Г1.У2.** Створювати звітні документи, що об'єктивно відображають стан захищеності та стійкості ОКІ, результати моніторингу, проведених заходів,	**Г1.К1.** Викладати складну технічну та нормативну інформацію у письмовій формі, забезпечуючи її розуміння для різних цільових аудиторій. **Г1.К2.** Взаємодіяти з фахівцями різних підрозділів ОКІ для збору необхідної інформації для документації. **Г1.К3.** Обговорювати та є узгоджувати проекти документів із зацікавленими сторонами та	**Г1.В1.** Відповідати за повноту, достовірність, актуальність та відповідність законодавству всієї розробленої та підтримуваної документації. **Г1.В2.** Діяти автономно у межах своїх функціональних обов'язків щодо розробки та супроводження документації. **Г1.В3.** Відповідати за своєчасне оновлення документів у разі

Трудові функції (умовне позначення та назва)	Компетентності	Результати навчання			
		знання	**уміння/навички**	**комунікація**	**відповідальність і автономія**
		планів реагування на інциденти, планів безперервності діяльності, планів відновлення після кризових ситуацій, результатів оцінки ризиків та вразливостей, аудитів та перевірок. **Г1.З5.** Типи звітних документів та вимоги до їхнього змісту й форми. **Г1.З6.** Методи систематизації та архівації документів, включаючи використання систем електронного документообігу. **Г1.З7.** Правила роботи з інформацією з обмеженим доступом.	інцидентів та їх ліквідації. **Г1.У3.** Систематизувати та класифікувати документацію, забезпечуючи її пошук та доступність для уповноважених осіб. **Г1.У4.** Забезпечувати актуалізацію документації шляхом регулярного перегляду, внесення змін та доповнень відповідно до змін у законодавстві, технологіях, організаційних структурах або виявлених недоліків. **Г1.У5.** Контролювати відповідність розроблених та діючих документів вимогам законодавства та внутрішнім інструкціям.	керівництвом ОКІ, враховуючи їхні зауваження та пропозиції. **Г1.К4.** Готувати презентації щодо важливих документів або звітів для внутрішніх або зовнішніх аудиторій. **Г1.К5.** Відповідати на запити щодо документації, надавати роз’яснення та консультації.	зміни внутрішніх процесів, законодавства або появи нових загроз. **Г1.В4.** Ініціювати розробку нових документів або внесення змін до існуючих за потреби. **Г1.В5.** Працювати під загальним керівництвом, але самостійно визначати пріоритетність завдань з документування. **Г1.В6.** Відповідати за дотримання вимог при роботі з інформацією з обмеженим доступом.

Трудові функції (умовне позначення та назва)	Компетентності	Результати навчання			
		знання	уміння/навички	комунікація	відповідальність і автономія
			Г1.У6. Організовувати зберігання документів з дотриманням вимог безпеки та конфіденційності.		
	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 (за потреби); профільна наукова та методична література; правила та інструкції відповідного спрямування.				

6. Розподіл трудових функцій та компетентностей за професійними кваліфікаціями (за потреби)

Трудова функція (умовне позначення та назва)	**Назва (назви) професійної (професійних) кваліфікації (кваліфікацій) в межах професійного стандарту**	
	фахівець із захисту та стійкості критичної інфраструктури	**провідний фахівець із захисту та стійкості критичної інфраструктури**
	повна	повна
А. Ідентифікація та категоризація ОКІ.	+	+
Б. Виконання заходів із забезпечення захисту та стійкості ОКІ.	+	+
В. Виконання заходів контролю стану захищеності та стійкості ОКІ.	-	+
Г. Документальне забезпечення.	+	+

7. Відомості про розроблення та затвердження професійного стандарту:

1) повне найменування розробника професійного стандарту.

Державна служба спеціального зв'язку та захисту інформації України.

Склад робочої групи/Учасники робочої групи:

БУЧИК Сергій Степанович, професор кафедри кібербезпеки та захисту інформації Київського національного університету ім. Тараса Шевченка;

ВАВІЛЕНКОВА Анастасія Ігорівна, завідувач кафедри кібербезпеки центру кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України;

ВІЛЬЧИНСЬКИЙ Олександр Миколайович, начальник відділу захисту критичної інфраструктури Міністерства енергетики України;

ВІТЮК Олег Володимирович, начальник відділу кібербезпеки та захисту інформації Управління розвитку цифрових трансформацій в аграрному секторі економіки Міністерства аграрної політики та продовольства України;

ГЛУШАК Олег Михайлович, начальник управління мобілізаційної роботи, цивільного захисту та критичної інфраструктури Міністерства внутрішніх справ України;

ДЕНИСЕНКО Артем Сергійович, головний спеціаліст 4 сектору 1 управління Департаменту захисту критичної інфраструктури Адміністрації Держспецзв'язку;

ЗГУРСЬКА Ліна Олексіївна, головний спеціаліст сектору регіональної цифровізації Міністерства цифрової трансформації України;

КОВАЛЬ Володимир Валерійович, провідний консультант (працівник) 2 відділу 2 управління Департаменту захисту критичної інфраструктури Адміністрації Держспецзв'язку;

КРАВЧЕНКО Андрій Андрійович, заступник начальника управління – начальник відділу управління об'єктами державної власності управління державного майна та інвестицій Державного агентства водних ресурсів України Міністерства захисту довкілля та природних ресурсів України;

КРАМСЬКИЙ Антон Євгенович, заступник завідувача Спеціальної кафедри № 1 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;

КУЧЕР Валерій Васильович, провідний фахівець з діяльності профспілки працівників Збройних Сил України;

ЛОЇК Василь Богданович, начальник кафедри цивільного захисту Львівського державного університету безпеки життєдіяльності;

МАРЧЕНКО Олена Михайлівна, начальник 3 управління Департаменту кадрової роботи та управління персоналом Адміністрації Держспецзв'язку;

МІСЮРА Андрій Олександрович, начальник 2 відділу 2 управління Департаменту захисту критичної інфраструктури Адміністрації Держспецзв'язку;

МОХОР Володимир Володимирович, директор Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, член-кореспондент Національної академії наук України;

НІКОЛАЄНКО Богдан Анатолійович, головний спеціаліст 2 відділу 1 управління Департаменту захисту критичної інфраструктури Адміністрації Держспецзв'язку;

ПОДДИМАЙ Андрій Борисович, директор юридичного департаменту Всеукраїнського об'єднання обласних організацій роботодавців, підприємств металургійного комплексу Федерація металургів України;

ПОТЕНКО Олександр Сергійович, старший науковий співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України;

РОМАНЕНКО Євген Олександрович, Президент Громадської організації «Всеукраїнська асамблея докторів наук з державного управління»;

СІРИЙ Олег Вікторович, старший викладач кафедри контррозвідувального захисту об'єктів критичної інфраструктури, Навчально-наукового інституту державної безпеки Національної академії Служби безпеки України;

СКРИНИК Олександр Павлович, начальник Патронатної служби Адміністрації Держспецзв'язку;

ТИМОШЕНКО Ірина Леонідівна, керівник служби з питань безпеки критичної інфраструктури Апарату Ради національної безпеки і оборони України;

ТІЩЕНКО Аліна Анатоліївна, державний експерт експертної групи медичної та критичної інфраструктури Директорату стратегічного планування та координації Міністерства охорони здоров'я України;

ТОЛЮПА Сергій Васильович, професор кафедри кібербезпеки та захисту інформації Київського національного університету ім. Тараса Шевченка;

ТРЕТЬЯКОВ Олег Вальтерович, професор кафедри цивільної та промислової безпеки ім. Героя України Чуба О.С. Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут;

ХАЛМУРАДОВ Батир Данатарович, завідувач кафедри цивільної та промислової безпеки ім. Героя України Чуба О.С. Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут»;

ЧОПОРОВ Сергій Вікторович, начальник управління з питань цифрового розвитку, цифрових трансформацій та цифровізації Міністерства з питань стратегічних галузей промисловості України;

ЮДІН Олександр Костянтинович, учений секретар Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

ЮДІНА Діана Олексіївна, головний спеціаліст 5 відділу Департаменту кіберзахисту Адміністрації Держспецзв'язку;

ЯКОВЧУК Роман Святославович, начальник факультету цивільного захисту Львівського державного університету безпеки життєдіяльності;

2) назва та реквізити документа, яким затверджено професійний стандарт:

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 29.12.2025 № 865;

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 схваленого рішенням від 17.12.2025 № 6 Національного агентства кваліфікацій (відповідно до протоколу засідання Національного агентства кваліфікацій від 17.12.2025 № 67 (261)) про дотримання під час підготовки проєкту професійного стандарту «Фахівець із захисту та стійкості критичної інфраструктури» вимог Порядку розроблення, введення в дію та перегляду професійних стандартів, затвердженого постановою Кабінету Міністрів України від 31.05.2017 № 373;

4) реквізити висновку репрезентативних всеукраїнських об'єднань професійних спілок на галузевому рівні або Спільного представницького органу репрезентативних всеукраїнських об'єднань профспілок на національному рівні про погодження проєкту професійного стандарту.

Висновок Профспілки працівників Збройних Сил України від 10.12.2025 № 54 щодо погодження проєкту професійного стандарту «Фахівець із захисту та стійкості критичної інфраструктури».

8. Рекомендована дата перегляду професійного стандарту:

грудень 2030 року.

_____