Прим. № __

ЗАТВЕРДЖЕНО

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

ПРОФЕСІЙНИЙ СТАНДАРТ

ФАХІВЕЦЬ З РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ

_____

(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 20 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 реагування на інциденти кібербезпеки» (лист від 16 листопада 2023 року № 01.2-14/136, Постанова Президії Профспілки працівників зв'язку України від 16 листопада 2023 року № П-4-5г).

I. Назва професійного стандарту

Фахівець з реагування на інциденти кібербезпеки

II. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Аналіз, оцінка інцидентів кібербезпеки в рамках мережевого середовища та реагування на них. Усунення інцидентів кібербезпеки та пом’якшення їх наслідків. Відстеження, оцінка стану кібербезпеки систем та своєчасне повідомлення про інциденти кібербезпеки. Відновлення функціональності систем і процесів до робочого стану. Дослідження та аналіз заходів реагування, оцінка ефективності та покращення існуючих практик. Накопичення та проведення аналізу даних про кіберзагрози.

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

Секція J	Інформація та телекомунікації	**Розділ 61**	Телекомунікації (електрозв'язок)	**Група 61.9**	Інша діяльність у сфері електрозв'язку
				Клас 61.90	Інша діяльність у сфері електрозв'язку
		Розділ 62	Комп'ютерне програмування, консультування та пов'язана з ними діяльність	**Група 62.0**	Комп'ютерне програмування, консультування та пов'язана з ними діяльність
				Клас 62.02	Консультування з питань інформатизації
				Клас 62.09	Інша діяльність у сфері інформаційних технологій і комп'ютерних систем
Секція M	Професійна, наукова та технічна діяльність	**Розділ 74**	Інша професійна, наукова та технічна діяльність	**Група 74.9**	Інша професійна, наукова та технічна діяльність, не введенні в інші угрупування
				Клас 74.90	Інша професійна, наукова та технічна діяльність, не введенні в інші угрупування

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

Фахівець з реагування на інциденти кібербезпеки, 2139.2

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

Молодший фахівець з реагування на інциденти кібербезпеки, 6 рівень НРК.

Фахівець з реагування на інциденти кібербезпеки, 7 рівень НРК.

Провідний фахівець з реагування на інциденти кібербезпеки, 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 реагування на інциденти кібербезпеки»;
- 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)

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 реагування на інциденти кібербезпеки	Підготовка за спеціальностями, вказаними у **П.*** на першому (бакалаврському) рівні вищої освіти, без вимог до стажу роботи.	*Не передбачено професійним стандартом*
Фахівець з реагування на інциденти кібербезпеки	Підготовка за спеціальностями, вказаними у **П.*** на другому (магістерському) рівні вищої освіти за умови наявності стажу роботи за однією з професій відповідного спрямування не	*Не передбачено професійним стандартом*

Назва професійної та/або часткової професійної кваліфікації	**Суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
	менше 2 років (аналітик з безпеки інформаційно-комунікаційних систем, фахівець з питань безпеки (інформаційно-комунікаційні технології), фахівець сфери захисту інформації тощо)	
Провідний фахівець з реагування на інциденти кібербезпеки	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 (аналітик з безпеки інформаційно-комунікаційних систем, фахівець з питань безпеки (інформаційно-комунікаційні технології), фахівець сфери захисту інформації тощо)	*Не передбачено професійним стандартом*

П.*

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

- 121 «Інженерія програмного забезпечення» галузі знань 12 «Інформаційні технології» (6 рівень НРК);
- 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології» (6 рівень НРК);
- 123 «Комп'ютерна інженерія» галузі знань 12 «Інформаційні технології» (6 рівень НРК);
- 124 «Системний аналіз» галузі знань 12 «Інформаційні технології» (6 рівень НРК);
- 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» (6 рівень НРК);
- 126 «Інформаційні системи та технології» галузі знань 12 «Інформаційні технології» (6 рівень НРК);
- 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);

- 256 «Національна безпека» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (6 рівень НРК).

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

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

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

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

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

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

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

- 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);

- 256 «Національна безпека» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (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**
Молодший фахівець з реагування на інциденти кібербезпеки	Підвищення кваліфікації для отримання професійної кваліфікації "фахівець з реагування на інциденти кібербезпеки". Стаж роботи не менше двох років	*Не передбачено професійним стандартом*

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 реагування на інциденти кібербезпеки	Підвищення кваліфікації для отримання професійної кваліфікації "провідний фахівець з реагування на інциденти кібербезпеки". Стаж роботи 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

IT	інформаційні технології
ПЗ	програмне забезпечення
OSI	Open Systems Interconnection
TCP/IP	Transmission Control Protocol/ Internet Protocol
DNS	Domain Name System
SOC	Security Operations Center
CSIRT	Computer Security Incident Response Team

V. Опис трудових функцій

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
А. Відстеження, збір та документування даних про інциденти кібербезпеки з моменту їх виявлення до остаточної ідентифікації статусу події.	**А1.** Здатність відстежувати та документувати інциденти кібербезпеки з моменту їх виявлення до остаточного вирішення.	**А1.З1.** Модель OSI і базові мережеві протоколи. **А1.З2.** Мережеві протоколи (TCP/IP, динамічного конфігурування вузлів, системи доменних імен (DNS) і послуги, що надаються службою каталогів тощо). **А1.З3.** Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи. **А1.З4.** Мережеві атаки і зв'язок мережевої атаки із загрозами та вразливими місцями. **А1.З5.** Внутрішні компоненти операційних систем, мережеві протоколи та сервіси. **А1.З6.** Фізичні і логічні мережеві пристрої та інфраструктури, зокрема концентратори, комутатори, маршрутизатори, брандмауери. **А1.З7.** Інструменти керування подіями інформаційної безпеки.	**А1.У1.** Розпізнавати та класифікувати типи вразливостей і пов'язаних з ними атак. **А1.У2.** Виявляти вторгнення на хост і мережу за допомогою технологій виявлення вторгнень **А1.У3.** Виявляти вразливості в захищених системах (наприклад, сканування вразливостей і перевірка відповідності). **А1.У4.** Проводити процедури сканування вразливостей і розпізнавання вразливостей в системах безпеки.	**А1.К1.** Писати і публікувати звіти проведених заходів у складі команди.	**А1.В1.** Проводити оцінку процедури відстеження інцидентів кібербезпеки.
	А2. Здатність здійснювати збір артефактів вторгнення і	**А2.З1.** Концепції і протоколи комп'ютерних мереж, а також методології безпеки мережі.	**А2.У1.** Зберігати цілісність доказів відповідно до стандартних оперативних	**А2.К1.** У складі команди готувати звіти, що містять індикатори	**А2.В1.** Здійснювати обмін індикаторами компрометації між

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	використовувати виявлені дані для запобігання потенційним інциденти кібербезпеки в межах підприємства (установи, організації).	**А2.З2.** Механізми контролю доступу до хосту/мережі (список контролю доступу, списки можливостей). **А2.З3.** Методології виявлення вторгнень і способи виявлення вторгнень до хостів і мереж. **А2.З4.** Загальні мережеві протоколи та протоколи маршрутизації, послуги та їх взаємодію для забезпечення мережевих зв'язків. **А2.З5.** Фізичні комп'ютерні компоненти і архітектури, включаючи функції різних компонентів і периферійних пристроїв. **А2.З6.** Методи збору інформації для розслідування інцидентів кібербезпеки. **А2.З7.** Методи соціальної інженерії.	процедур або національних стандартів. **А2.У2.** Застосовувати методики виявлення вторгнень з боку хоста та мережі за допомогою технологій виявлення вторгнень. **А1.У4.** Проводити процедури сканування вразливостей і розпізнавання вразливостей в системах безпеки	компрометації для аналізу поведінки зловмисника та збору артефактів його роботи.	суб'єктами забезпечення кібербезпеки в Україні.
	А3. Здатність проводити аналіз файлів журналу з різних джерел та аналізувати сигнали сповіщення про мережу з метою	**А3.З1.** Методи аналізу мережевого трафіку. **А3.З2.** Внутрішні компоненти операційних систем, мережеві протоколи та сервіси **А3.З3.** Фізичні і логічні мережеві пристрої та інфраструктури, зокрема	**А3.У1.** Працювати з файлами журналів та аналізувати їх. **А3.У2.** Отримувати і аналізувати сигнали сповіщення про мережу від різних джерел всередині організації та визначати можливі	**А3.К1.** Комунікувати з керівниками організації різних рівнів, із представника-ми зацікавлених сторін стосовно проведення аналізу інцидентів кібербезпеки.	**А3.В1.** Періодично переглядати журнали для виявлення доказів минулих вторгнень.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	визначення можливих загроз безпеці мережі.	концентратори, комутатори, маршрутизатори, брандмауери. **А3.34.** Мережеві служби і протоколи взаємодії, які забезпечують мережевий зв'язок. **А3.35.** Методики адміністрування системи, мережі та захисту операційних систем **А3.36.** Методи аналізу на рівні пакетів із використанням відповідних інструментів (Wireshark, tcpdump). **А1.33.** Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи.	причини появи таких сигналів.		
	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 відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); профільна наукова та методична література; нормативні акти, протоколи, стандарти відповідного спрямування; плани та інструкції необхідні для оперативного реагування на інциденти кібербезпеки; програмне та інше техніко-технологічне забезпечення; інструменти збору подій кібербезпеки; інструменти збору артефактів вторгнення.				
Б. Проведення оцінки інцидентів кібербезпеки.	**Б1**. Здатність зіставляти дані про інциденти, для визначення конкретних вразливостей та надання рекомендацій, які дозволять	**Б1.З1.** Закони, нормативні акти, політики і етичні норми, та як вони пов'язані з конфіденційністю персональних даних та кібербезпекою. **Б1.З2.** Принципи забезпечення конфіденційності персональних даних та кібербезпеки.	**Б1.У1.** Використовувати інструменти кореляції подій безпеки. **Б1.У2.** Визначати та пріоритезувати заходи реагування на ризики кібербезпеки. **Б1.У3.** Розробляти або брати участь у	**Б1.К1.** Налаштувати координацію з аналітиками розвідки для кореляції даних оцінки загроз.	**Б1.В1.** Проводити постійну оптимізацію процесів оцінки інцидентів кібербезпеки.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	швидко їх усунути.	**Б1.З3.** Кіберзагрози та вразливості. **Б1.З4.** Різні класи атак. **Б1.З5.** Методи і техніки атак. **Б1.З6.** Аналіз на рівні пакетів. **Б1.З7.** Інструменти кореляції подій безпеки. **Б1.З8.** Методологію опрацювання інцидентів кібербезпеки. **Б1.З9.** Системи збору та кореляції подій кібербезпеки.	розробці порядку проведення оцінки інцидентів кібербезпеки. **Б1.У4.** Проводити оцінку дій противника та його методів, виявляти техніки, тактики та процедури нападу.		
	Б2. Здатність виконувати сортування інцидентів кібербезпеки , включаючи визначення масштабу, терміновості та потенційного впливу, визначати конкретні вразливості та надавати рекомендації, які дозволять швидко	**Б2.З1.** Принципи кібербезпеки та конфіденційності, а також організаційні вимоги (щодо конфіденційності, цілісності, доступності, автентифікації, невідмовності). **Б2.З2.** Конкретні операційні наслідки інцидентів кібербезпеки. **Б2.З3.** Вразливості прикладних програм. **Б2.З4.** Сценарії реалізації загроз. **Б2.З5.** Процеси управління ризиками, а саме, методи оцінки та пом’якшення ризиків. **Б2.З6**. Категорії інцидентів, процедур і терміни реагування на інциденти кібербезпеки.	**Б2.У1.** Проводити оцінку збитків. **Б2.У2.** Проводити оцінку впливу/ризику. **Б2.У3.** Виконувати накопичення і перевірку артефактів з метою визначення можливих заходів щодо зниження/усунення несправностей в системах підприємства (установи, організації). **Б2.У4.** Визначати зв’язки та закономірності між подіями кібербезпеки.	**Б2.К1.** Надавати рекомендації для усунення або пом’якшення наслідків інцидентів кібербезпеки на основі проведеної оцінки.	**Б2.В1.** Оцінювати ефективність процедур відповідного спрямування.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	виправити ситуацію.				
	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 відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); профільна наукова та методична література; нормативні акти, протоколи, стандарти відповідного спрямування; плани та інструкції, необхідні для оперативного реагування на інциденти кібербезпеки; програмне та інше техніко-технологічне забезпечення; інструменти збору та кореляції подій кібербезпеки.				
В. Оброблення інцидентів кіберзахисту в режимі реального часу та вжиття заходів щодо пом'якшення наслідків інцидентів кібербезпеки, а також відновлення функціональності системи та процесів до робочого стану.	**В1.** Здатність виконувати завдання з обробки інцидентів кібербезпеки в режимі реального часу з метою підтримки розгорнутих груп реагування на інциденти.	**В1.З1.** Практики та інструменти опрацювання інцидентів кібербезпеки. **В1.З2.** Методології реагування та обробки інцидентів кібербезпеки. **В1.З3.** Етапи здійснення кібератак (розвідка, сканування, перерахування, отримання доступу, ескалація привілеїв, підтримка доступу, використання мережі, приховування слідів). **В1.З4.** Методологію опрацювання інцидентів кібербезпеки. **Б2.З6**. Категорії інцидентів, процедур і терміни реагування на інциденти кібербезпеки.	**В1.У1.** Ідентифікувати, захоплювати, стримувати та звітувати про зловмисне ПЗ. **В1.У2.** Захищати мережеві комунікації. **В1.У3.** Забезпечувати захист мережі від зловмисного програмного забезпечення. **В1.У4.** Реагувати і проводити локальні заходи у відповідь на сигнали сповіщення про загрозу, що поширені постачальниками послуг.	**В1.К1.** Документувати та передавати інциденти, які можуть спричинити постійний і негайний вплив на навколишнє середовище.	**В1.В1.** Приймати участь у розробленні плану реагування на інциденти кібербезпеки та плану відновлення функціональності систем і процесів до робочого стану. **В1.В2.** Проводити на постійній основі тестування та оцінку відпрацювання інцидентів кібербезпеки.
	В2. Здатність забезпечувати своєчасне виявлення,	**В2.З1.** Загрози і вразливості безпеки систем і прикладного програмного забезпечення.	**В2.У1.** Використовувати інструменти мережевого аналізу для визначення вразливостей.	**В2.К1.** Застосовувати на практиці всі технічні, функціональні та	**В2.В1.** Впроваджувати і розвивати методи тестування та

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	ідентифікацію та сповіщення про можливі атаки/вторгнення, аномальну діяльність і дії зловживання та відрізняти ці інциденти та події від доброякісних дій.	**В2.З2.** Тактики і техніки атак кібербезпеки. **В2.З3.** Порядок зіставлення даних із різних кінцевих точок і рішень безпеки для виявлення інцидентів кібербезпеки. **В2.З4.** Компоненти системи мережевої безпеки (мережеві екрани, віртуальні приватні мережі, системи виявлення вторгнень).	**В2.У2.** Застосовувати на практиці програмне забезпечення відповідного спрямування. **В2.У3.** Опановувати найкращі практики, стандарти, системи кібербезпеки, закони та нормативні акти щодо обробки інцидентів кібербезпеки та реагування на них. **В2.У4.** Відстежувати роботу системи і реагувати на події у відповідь на тригери та/або спостерігати за трендами або незвичайною діяльністю.	експлуатаційні аспекти опрацювання і реагування на інциденти кібербезпеки.	опрацювання інцидентів кібербезпеки.
	В3. Здатність пом’якшувати наслідки інцидентів кібербезпеки або витоку даних та відновлювати системи до робочого стану.	**В3.З1.** Резервне копіювання та відновлення даних. **В3.З2.** Засоби діагностики систем і методів виявлення несправностей. **В3.З3.** Правила безперервності бізнесу та операційних планів відновлення безперервності після катастроф.	**В3.У1.** Застосовувати правильні методики для різних типів інцидентів кібербезпеки, з розділенням інцидентів шкідливого програмного забезпечення, електронної пошти, мережі, веб-додатків, хмарних структур та загроз внутрішньої безпеки.	**В3.К1.** Взаємодіяти з українськими командами реагування на комп’ютерні надзвичайні події, а також іншими підприємст-вами, установами та організаціями, які є суб’єктами	**В3.В1.** Оцінювати стійкість засобів контролю кібербезпеки та заходів щодо пом’якшення наслідків, вжитих після інциденту кібербезпеки або витоку даних.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		Б2.З5. Процеси управління ризиками, а саме, методи оцінки та пом'якшення ризиків.	**В3.У2.** Запобігати негативним наслідкам інцидентів кібербезпеки, мінімізовувати та усувати їх, виправляти вразливості, а також відновлювати сталість і надійність функціонування систем та інших об'єктів кіберзахисту.	національної системи кібербезпеки.	
	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 відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); профільна наукова та методична література; нормативні акти, протоколи, стандарти відповідного спрямування; програмне та інше техніко-технологічне забезпечення; інструменти збору та кореляції подій кібербезпеки; плани та інструкції, необхідні для оперативного реагування на інциденти кібербезпеки; протокол спільних дій з суб'єктами забезпечення кібербезпеки, зокрема, інформаційного обміну у режимі реального часу, під час виявлення кібератак та кіберінцидентів; загальні правила обміну інформацією про кіберінциденти.			
Г. Моніторинг та оцінка поточного стану кібербезпеки.	**Г1.** Здатність проводити моніторинг зовнішніх джерел даних для підтримки поточного стану загроз кіберзахисту, та визначення того, які проблеми безпеки можуть	**Г1.З1.** Порядок витягування, аналіз і використання метаданих. **Г1.З2.** Типи порушників, які здійснюють кібератаки. **Г1.З3.** Засади тактик, прийомів і процедур. **Г1.З4.** Політики, процедури і правила кіберзахисту та інформаційної безпеки. **Г1.З5.** Методи роботи з великими обсягами даних та їх аналітика.	**Г1.У1.** Оцінювати, аналізувати та синтезувати великі об'єми даних в високоякісні і об'єднані продукти. **Г1.У2.** Ідентифікувати кіберзагрози, які можуть поставити під загрозу інтереси організації та/або партнерів.	**Г1.К1.** Формувати запити на профільну інформацію. **Г1.К2.** Готувати та виголошуватидоповідь з оцінки поточного стану кібербезпеки керівництву, персоналу і користувачам.	**Г1.В1.** Використовувати аналітичні дані при формуванні рекомендацій щодо зниження ризиків.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	вплинути на підприємство (установу, організацію).	**Г1.З6.** Кіберзагрози та вразливості. **Б1.З2.** Принципи забезпечення конфіденційності персональних даних та кібербезпеки. **Б1.З4.** Різні класи атак.			
	Г2. Здатність здійснювати аналіз тенденцій кіберзахисту та формувати відповідні звіти.	**Г2.З1.** Загальні види зараження комп'ютерів/ мереж, а також методи зараження. **Г2.З2.** Сучасні комп'ютерні набори вторгнень. **Г2.З3.** Нормативно-правову базу, пов'язану з кібербезпекою та захистом даних. **Г2.З4.** Можливості кіберрозвідки/збору інформації та сховищ даних. **Г2.З5.** Міжнародне законодавство, нормативні та методичні документи у сферах кібербезпеки, кіберзахисту та протидії кіберзагрозам. **Г2.З6.** Нові кіберзагрози та суб'єкти загроз. **Г2.З7.** Сучасні рішення у галузі кібербезпеки.	**Г2.У1.** Оцінювати інформацію на надійність, достовірність і релевантність. **Г2.У2.** Розвивати розуміння контексту загрозливого середовища організації.	**Г2.К1.** Аналізувати дані з одного або декількох джерел, готувати оперативні звіти на основі кібердослідних даних та розповсюджу-вати серед зацікавлених сторін.	**Г2.В1.** Доводити до відома зацікавлених сторін звіти з кібердослідними даними.
	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 відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали				

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	(за потреби); профільна наукова та методична література; нормативні акти, протоколи, стандарти відповідного спрямування; програмне та інше техніко-технологічне забезпечення.				
Д. Надання експертної технічної підтримки з управління інцидентами кібербезпеки.	**Д1.** Здатність здійснювати реалізацію на підприємстві (в установі, організації) повноважень технічного експерта, взаємодіяти з представниками правоохоронних органів та за необхідності роз'яснювати деталі інцидентів, співпрацювати з аналітиками розвідки з метою кореляції даних при оцінці загроз.	**Д1.З1.** Застосовувану в організації/ підприємстві програму класифікації інформації і процедур розкриття. **Д1.З2.** Типи загроз кібербезпеки, вектори атак, мотиви та дії зловмисників. **Д1.З3** Порядок розкриття вразливостей, інцидентів кібербезпеки, пов'язаних із витоком даних, та геополітичних подій, що впливають на кіберризики. **Д1.З4.** Еталонні моделі архітектури безпеки та рішення у галузі безпеки. **Д1.З5.** Методологію опрацювання інцидентів кібербезпеки. **А1.З3.** Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи.	**Д1.У1.** Застосовувати концепції, процедури, програмне забезпечення та/або технологічні прикладні програми під час надання консультацій із застосування на практиці методології щодо політики кібербезпеки. **Д1.У2.** Використовувати інструменти кореляції подій безпеки.	**Д1.К1.** Готувати аудиторські звіти, у яких визначаються технічні та процедурні висновки, а також надавати рекомендовані стратегії/рішення для виправлення. **Д1.К2.** Працювати в команді та співпрацювати з колегами.	**Д1.В1.** Проводити детальний аналіз, надавати рекомендації з реагування на інциденти кібербезпеки та відновлення систем до робочого стану.
	Д2. Здатність забезпечувати координацію функцій реагування на інциденти та	**Д2.З1.** Середовище загроз організації. **Д2.З2.** Концепції і методології аналізу зловмисного програмного забезпечення.	**Д2.У1.** Застосовувати принципи кібербезпеки і приватності при формуванні вимог організації (стосовно конфіденційності,	**Д2.К1.** Розробляти рекомендації щодо вибору ефективних, з точки зору витрат, засобів контролю	**Д2.В1.** Використовувати схвалені принципи та методи глибокого захисту. **Д2.В2.** Виконувати

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	надавати експертну технічну підтримку профільним фахівцям в масштабах підприємства (установи, організації) для управління інцидентами кібербезпеки.	**Д2.З3.** Основи управління інцидентами кібербезпеки. **Д2.З4.** Основи управління вразливістю, оцінювання загроз, управління ризиками та автоматизацію процесів реагування на інциденти кібербезпеки. **Д2.З5.** Комплекс заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та інциденти кібербезпеки, впровадження контрзаходів, спрямованих на мінімізацію вразливостей систем.	цілісності, доступності, автентифікації і неспростовності). **Д2.У2.** Аналізувати політику та конфігурації кіберзахисту організації та оцінити відповідність нормам і директивам організації. **Д2.У3.** Удосконалювати системи кіберзахисту з урахуванням результатів оцінки повноти, адекватності, результативності та ефективності процесів, що виконуються.	безпеки з метою зниження ризиків.	обов'язки внутрішнього консультанта/ радника в сфері планування заходів з розвитку кібербезпеки в організації.
	Предмети та засоби праці: протоколи, стандарти та сертифікати відповідного спрямування; комп'ютерне, програмне та інше техніко-технологічне забезпечення; відповідне програмне забезпечення, доступ до інформаційно-довідкових систем, баз даних; плани та інструкції, необхідні для оперативного реагування на інциденти кібербезпеки; інструменти збору та кореляції подій кібербезпеки.				
Е. Дослідження та аналіз інцидентів кібербезпеки.	**Е1.** Здатність здійснювати дослідження інцидентів кібербезпеки та проводити аналіз заходів реагування на них, оцінювати ефективність	**Е1.З1.** Організаційну ієрархію та процеси прийняття рішень у кіберпросторі. **Е1.З2.** Типи та способи реалізації кібератаки. **Е1.З3.** Методи і механізми запобігання та протидії можливим інцидентам кібербезпеки/кібератакам.	**Е1.У1.** Накопичувати та проводити аналіз даних про інциденти кібербезпеки. **Е1.У2.** Проводити оцінку процесів прийняття рішень щодо загроз. **Е1.У3.** Визначати тактику та методологію попередження загроз.	**Е1.К1**. У складі команди формувати звітність стосовно аналізу результатів інцидентів кібербезпеки та дій з їх опрацювання. **Е1.К2.** Проводити обмін інформацією про інциденти	**Е1.В1.** Проводити дослідження та аналізувати процес реагування на інциденти кібербезпеки з метою підвищення ефективності та вдосконалення існуючих практик.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	засобів та покращувати існуючі практики кіберзахисту.	**Е1.З4.** Практики та інструменти опрацювання інцидентів кібербезпеки. **Е1.З5.** Методи та засоби розслідування інцидентів кібербезпеки. **Б1.З1.** Закони, нормативні акти, політики і етичні норми, та як вони пов'язані з конфіденційністю персональних даних та кібербезпекою. **Б1.З2.** Принципи забезпечення конфіденційності персональних даних та кібербезпеки. **Б2.З5.** Процеси управління ризиками, а саме, методи оцінки та пом'якшення ризиків.	**Е1.У4.** Використовувати зворотній зв'язок для покращення процесів, продуктів і послуг. **Е1.У6.** Вивчати та досліджувати сучасні види інцидентів кібербезпеки/ кібератак. **Е1.У7.** Проєктувати реагування на інциденти кібербезпеки для моделей хмарних сервісів.	кібербезпеки між суб'єктами. забезпечення кібербезпеки.	**Е1.В2.** Формувати власну базу даних інцидентів кібербезпеки.
	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 відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); профільна наукова та методична література; нормативні акти, протоколи, стандарти відповідного спрямування; програмне та інше техніко-технологічне забезпечення; плани та інструкції, необхідні для оперативного реагування на інциденти кібербезпеки; інструменти збору та кореляції подій кібербезпеки.				
Є. Координація діяльності з реагування на інциденти кібербезпеки.	**Є1.** Здатність розробляти та запроваджу-вати на практиці методики та настанови з кіберзахисту, сприяти	**Є1.З1.** Національні, європейські та міжнародні стандарти кібербезпеки і відповідні стандарти, законодавство, політики і правила щодо приватності.	**Є1.У1.** Розробляти та застосовувати у практичній діяльності технічну документацію відповідного спрямування. **Є1.У2.** Застосовувати принципи кібербезпеки та	**Є1.К1.** Взаємодіяти з іноземними та міжнародними організаціями з питань реагування на інциденти кібербезпеки.	**Є1.В1.** Рекомендувати зміни та доповнення до політики кібербезпеки організації, приймати участь у

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	розробленню, підтримці та оцінюванню плану реагування на інциденти кібербезпеки.	**Є1.З2.** Вимоги та підходи до розроблення навчальних та методичних матеріалів. **Є1.З3.** Нормативно-правову базу, пов'язану з кібербезпекою та захистом даних. **Г1.З4.** Політики, процедури і правила кіберзахисту та інформаційної безпеки.	конфіденційності д організаційних вимог. **Є1.У3.** Контролювати етапи реагування на інциденти кібербезпеки. **Є1.У4.** Розробляти та застосовувати у практичній діяльності методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. **Є1.У5.** Розробляти, тестувати та впроваджувати плани на випадок непередбачених ситуацій і відновлення мережевої інфраструктури.	**Є1.К2.** Організовувати та проводити практичні семінари з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту. **Є1.К3.** Розробляти вказівки і настанови для працівників, залучених до розроблення стратегій, програм та політик з розвитку кібербезпеки.	координації її перегляду. **Є1.В2.** Проводити регулярне оновлення плану реагування на інциденти кібербезпеки.
	Є2. Здатність співпрацювати з зацікавленими сторонами для вирішення інцидентів кібербезпеки та відповідності вразливостям.	**Є2.З1.** Комунікаційний цикл опрацювання інцидентів кібербезпеки. **Є2.З2.** Розроблення та впровадження протоколів спільних дій з суб'єктами забезпечення кібербезпеки, зокрема, інформаційного обміну у режимі реального часу, під час виявлення кібератак та інцидентів кібербезпеки.	**Є2.У1.** Готувати рекомендації щодо протидії сучасним видам кібератак та кіберзагроз. **Є2.У2.** Розробляти програми та методики проведення кібернавчань. **Є2.У3.** Розробляти сценарії реагування на інциденти кібербезпеки.	**Є2.К1.** Співпрацювати з центрами інформаційної безпеки (SOC) та групами реагування на інциденти з комп'ютерної безпеки (CSIRT). **Є2.К2.** Співпрацювати з співробітниками для	**Є2.В1.** Налаштовувати взаємодію з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами (установами,

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		Є2.З3. Методи і способи ефективної комунікації. **Є2.З4.** Розвиток міжнародного співробітництва у сфері кібербезпеки. **Є2.З5.** Стандарти обміну кібердослідними даними.	**Є2.У4.** Співпрацювати оперативно з командами реагування на комп'ютерні надзвичайні події щодо виявлення джерел кібератаки та засобів протидії.	повідомлення про інциденти кібербезпеки відповідно до чинної нормативно-правової бази. **Є2.К3.** Співпрацювати з представниками зовнішнього відомства, щоб відповідати на запити преси та інші запити, що стосуються персональних даних клієнтів і співробітників організації.	організаціями), які є суб'єктами національної системи кібербезпеки.
	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 відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); профільна наукова та методична література; нормативні акти, протоколи, стандарти відповідного спрямування. Плани та інструкції необхідні для оперативного реагування на інциденти кібербезпеки. Положення про структурні підрозділи підприємства/ організації. Типові вимоги до проведення ділових/ комерційних перемовин; порядок розроблення та виконання договірних робіт для зовнішніх партнерів.			

VI. Розподіл трудових функцій та компетентностей за професійними кваліфікаціями

Трудова функція (умовне позначення)	Загальна назва професійної кваліфікації у межах професійного стандарту: Фахівець з реагування на інциденти кібербезпеки		
	Молодший фахівець з реагування на інциденти кібербезпеки	Фахівець з реагування на інциденти кібербезпеки	Провідний фахівець з реагування на інциденти кібербезпеки
	повна	повна	повна
А	+	+	+
Б	+	+	+
В	+	+	+
Г	-	+	+
Д	-	+	+
Е	-	+	+
Є		-	+

VII. Відомості про розроблення та затвердження професійного стандарту

1. Повне найменування розробника професійного стандарту

Адміністрація Державної служби спеціального зв’язку та захисту інформації України

Склад робочої групи/Учасники робочої групи:

Бондаренко Дмитро Михайлович, начальник 1 науково-дослідного центру Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

Безштанько Віталій Михайлович, головний спеціаліст 5 відділу Департаменту кіберзахисту Адміністрації Держспецзв’язку;

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

Василіу Євген Вікторович, професор кафедри кібербезпеки та технічного захисту інформації факультету інформаційних технологій та кібербезпеки Державного університету інтелектуальних технологій і зв'язку;

Гахов Сергій Олександрович, доцент кафедри інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації Державного університету телекомунікацій;

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

Добришин Юрій Євгенович, доцент кафедри кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України;

Жилін Артем Вікторович, начальник 6 управління Державного центру кіберзахисту Держспецзв'язку;

Комаров Максим Юрійович, начальник 5 центру захисту інформації та розроблення і впровадження технологій кіберзахисту Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

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;

Масленникова Тетяна Андріївна, провідний науковий співробітник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

Мельник Сергій Вікторович, консультант напряму з розвитку професійних навичок з кібербезпеки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»;

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»;

Павленко Володимир Анатолійович, директор Громадської організації «Глобальний центр взаємодії в кіберпросторі»;

Проскуровський Роман Васильович, заступник керівника Центру кіберзахисту Національного банку України;

Фауре Еміль Віталійович, головний науковий співробітник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

Філіпова Ольга Валентинівна, комерційний директор компанії «САЙКОМ»;

Четверіков Іван Олександрович, доцент кафедри кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України;

Штомпель Тетяна Миколаївна, віцепрезидент компанії ТОВ «ТЕКЕКСПЕРТ», керівник навчального Центру «Мережні технології»;

Юдін Олексій Юрійович, перший заступник начальника 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 20 грудня 2023 року про дотримання під час підготовки проєкту професійного стандарту «Фахівець з реагування на інциденти кібербезпеки» вимог Порядку розроблення, введення в дію та перегляду професійних стандартів, затвердженого постановою Кабінету Міністрів України від 31.05.2017 р. № 373).

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

Висновок Профспілки працівників зв'язку України щодо погодження проєкту професійного стандарту «Фахівець з реагування на інциденти кібербезпеки» (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