Проєкт

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

Професійний стандарт

ФАХІВЕЦЬ З РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ

_____(дата внесення до Реєстру кваліфікацій)

ЗАТВЕРДЖЕНО:
Адміністрацією Державної служби
спеціального зв'язку та захисту
інформації України наказ від
_____№_____

Професійний стандарт розроблено та затверджено згідно з вимогами статті 42 Кодексу законів про працю України на підставі:

- висновку суб'єкта перевірки – Національного агентства кваліфікацій від _____ 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 від _____ щодо погодження проєкту професійного стандарту

І. Назва професійного стандарту

Фахівець з реагування на інциденти кібербезпеки

ІІ. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Аналіз, оцінка, реагування на інциденти кібербезпеки в рамках мережевого середовища. Усунення інцидентів кібербезпеки або 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»

<table>
<tr><td rowspan="6">Секція J</td><td rowspan="6">Інформація та телекомунікації</td><td rowspan="2">Розділ 61</td><td rowspan="2">Телекомунікації (електрозв'язок)</td><td>Група 61.9</td><td>Інша діяльність у сфері електрозв'язку</td></tr>
<tr><td>Клас 61.90</td><td>Інша діяльність у сфері електрозв'язку</td></tr>
<tr><td rowspan="4">Розділ 62</td><td rowspan="4">Комп'ютерне програмування, консультування та пов'язана з ними діяльність</td><td>Група 62.0</td><td>Комп'ютерне програмування, консультування та пов'язана з ними діяльність</td></tr>
<tr><td>Клас 62.02</td><td>Консультування з питань інформатизації</td></tr>
<tr><td>Клас 62.09</td><td>Інша діяльність у сфері інформаційних технологій і комп'ютерних систем</td></tr>
<tr><td rowspan="2">Секція M</td><td rowspan="2">Професійна, наукова та технічна діяльність</td><td rowspan="2">Розділ 74</td><td rowspan="2">Інша професійна, наукова та технічна діяльність</td><td>Група 74.9</td><td>Інша професійна, наукова та технічна діяльність, не введенні в інші угрупування</td></tr>
<tr><td>Клас 74.90</td><td>Інша професійна, наукова та технічна діяльність, не введенні в інші угрупування</td></tr>
</table>

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

Фахівець з реагування на інциденти кібербезпеки, 2139.2

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

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

- 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):

- 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);

- документ (диплом, сертифікат, тощо), щодо післядипломної освіти та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері реагування на інциденти кібербезпеки;
- документ (диплом, сертифікат, тощо), щодо професійної сертифікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері реагування на інциденти кібербезпеки.

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 реагування на інциденти кібербезпеки	Підготовка на першому рівні вищої освіти (бакалаврському) за спеціальностями вказаними п.5, галузі знань 12 «Інформаційні технології» та 17 «Електроніка, автоматизація та електронні комунікації», без вимог до стажу роботи.	*Не передбачено професійним стандартом*
Фахівець з реагування на інциденти кібербезпеки	Підготовка на другому рівні вищої освіти (магістерському) за спеціальностями вказаними п.5, галузі знань 12 «Інформаційні технології» та 17 «Електроніка, автоматизація та електронні комунікації», стаж роботи за однією з професій відповідного спрямування повинен складати не менше 2 років (аналітик з безпеки інформаційно-телекомунікаційних систем, фахівець з питань безпеки (інформаційно-комунікаційні технології),	*Не передбачено професійним стандартом*

	фахівець сфери захисту інформації тощо)	
Провідний фахівець з реагування на інциденти кібербезпеки	Підготовка на другому рівні вищої освіти (магістерському) за спеціальностями вказаними п.5, галузі знань 12 «Інформаційні технології» та 17 «Електроніка, автоматизація та електронні комунікації», стаж роботи за однією з професій відповідного спрямування повинен складати не менше 3 років (аналітик з безпеки інформаційно-телекомунікаційних систем, фахівець з питань безпеки (інформаційно-комунікаційні технології), фахівець сфери захисту інформації тощо)	*Не передбачено професійним стандартом*

2. Професійний розвиток

1) з присвоєнням наступної професійної кваліфікації

Назва професійної та/або часткової професійної кваліфікації	**Суб'єкти, уповноважені законодавством на присвоєння/підтвердження та 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 трьох років	*Не передбачено професійним стандартом*
Фахівець з реагування на інциденти кібербезпеки	Підвищення кваліфікації для отримання професійної кваліфікації "провідний фахівець з реагування на інциденти кібербезпеки". Стаж роботи не менше двох років	*Не передбачено професійним стандартом*

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.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.	**А1.В1.** Проводити оцінку процедури відстеження інцидентів кібербезпеки.

		А1.З7. Інструменти керування подіями інформаційної безпеки.			
	А2. Здатність здійснювати збір артефактів вторгнення і використовувати виявлені дані для запобігання потенційним інцидентам кіберзахисту в межах підприємства (установи, організації).	**А2.З1.** Концепції і протоколи комп'ютерних мереж, а також методології безпеки мережі. **А2.З2.** Механізми контролю доступу до хосту/мережі (список контролю доступу, списки можливостей). **А2.З3.** Методології виявлення вторгнень і способів виявлення вторгнень до хостів і мереж **А2.З4.** Загальні мережеві протоколи та протоколи маршрутизації, послуги та їх взаємодія 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.	**А2.У1.** Проводити сканування вразливостей і розпізнавати вразливості в системах безпеки. **А2.У2.** Зберігати цілісність доказів відповідно до стандартних оперативних процедур або національних стандартів. **А2.У3.** Застосовувати методики виявлення вторгнень з боку хоста та мережі за допомогою технологій виявлення вторгнень.	**А2.К1.** Готувати звіти, що містять індикатори компрометації для аналізу поведінки зловмисника та збору артефактів його роботи.	**А2.В1.** Здійснювати обмін індикаторами компрометації між суб'єктами забезпечення кібербезпеки в Україні.

	А3. Здатність проводити аналіз файлів журналу з різних джерел та аналізувати сигнали сповіщення про мережу з метою визначення можливих загроз безпеці мережі.	**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 концентратори, комутатори, маршрутизатори, брандмауери. **А3.З4.** Мережеві служби і протоколи взаємодії, які забезпечують мережевий зв'язок. **А3.З5.** Методики адміністрування системи, мережі та захисту операційних систем **А3.З6.** Методи аналізу на рівні пакетів із використанням відповідних інструментів (Wireshark, tcpdump). **А3.З7.** Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи.	**А3.У1.** Працювати з файлами журналів та аналізувати їх. **А3.У1.** Отримувати і аналізувати сигнали сповіщення про мережу від різних джерел всередині організації та визначати можливі причини появи таких сигналів.	**А3.К1.** Комунікувати з керівниками організації різних рівнів, із представника-ми зацікавлених сторін стосовно проведення аналізу інцидентів.	**А3.В1.** Періодично переглядати журнали для виявлення доказів минулих вторгнень.
	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 швидко їх усунути.	**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.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.	**Б1.У1.** Використовувати інструменти кореляції подій безпеки. **Б1.У2.** Визначати та пріоритезувати заходи реагування на ризики кібербезпеки. **Б1.У3.** Розроблювати або брати участь у розробці порядку проведення оцінки інцидентів кібербезпеки. **Б1.У4.** Проводити оцінку дій противника та його методів, виявляти техніки, тактики та процедури нападу.	**Б1.К1.** Налаштувати координацію з аналітиками розвідки для кореляції даних оцінки загроз.	**Б1.В1.** Проводити постійну оптимізацію процесів оцінки інцидентів кібербезпеки
	Б2. Здатність виконувати сортування інцидентів	**Б2.З1.** Принципи кібербезпеки та конфіденційності та організаційних вимог (щодо	**Б2.У1.** Проводити оцінку збитків. **Б2.У2.** Проводити оцінку впливу/ризику	**Б2.К1.** Надавати рекомендації для усунення	**Б2.В1.** Оцінювати ефективність процедур відповідного

	кіберзахисту, включаючи визначення масштабу, терміновості та потенційного впливу, визначати конкретні вразливості та надавати рекомендації, які дозволять швидко виправити ситуацію.	конфіденційності, цілісності, доступності, автентифікації, невідмовності). **Б2.З2.** Конкретні операційні наслідки інцидентів кібербезпеки. **Б2.З3.** Вразливості прикладних приграм **Б2.З4.** Сценарії реалізації загроз. **Б2.З5.** Процеси управління ризиками, а саме, методи оцінки та пом'якшення ризиків **Б2.З6**. Категорії інцидентів, процедур і термінів реагування на інциденти.	**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.	або пом'якшення наслідків інцидентів кібербезпеки на основі проведеної оцінки.	спрямування.
	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 кібербезпеко-	**В1.** Здатність виконувати завдання з обробки інцидентів кіберзахисту в режимі реального часу з метою підтримки	**В1.З1.** Практики та інструменти опрацювання інцидентів інцидентів **В1.З2.** Категорії інцидентів, процедур і термінів реагування на інциденти **В1.З3.** Методології реагування на інциденти та обробки інцидентів	**В1.У1.** Ідентифікувати, захоплювати, стримувати та звітувати про зловмисне ПЗ. **В1.У2.** Захищати мережеві комунікації **В1.У3.** Забезпечувати захист мережі від	**В1.К1.** Документу-вати та передавати інциденти, які можуть спричинити постійний і негайний вплив на	**В1.В1.** Приймати участь у розробленні плану реагування на кіберінциденти та плану відновлення функціональності систем і процесів до робочого стану **В1.В2.** Проводити на постійній основі тестування та оцінку відпрацювання інцидентів кібербезпеки

вих інцидентів, а також відновлення функціональності системи та процесів до робочого стану.	розгорнутих груп реагування на інциденти.	**В1.З4.** Етапи здійснення кібератак (розвідка, сканування, перерахування, отримання доступу, ескалація привілеїв, підтримка доступу, використання мережі, приховування слідів). **В1.З5.** Методологію опрацювання інцидентів кібербезпеки.	зловмисного програмного забезпечення. **В1.У4.** Реагувати і проводити локальні заходи у відповідь на сигнали сповіщення про загрозу, що поширені постачальниками послуг.	навколишнє середовище.	
	В2. Здатність забезпечувати своєчасне виявлення, ідентифікацію та сповіщення про можливі атаки/вторгнення, аномальну діяльність і дії зловживання та відрізняти ці інциденти та події від доброякісних дій.	**В2.З1.** Загрози і вразливості безпеки систем і прикладного програмного забезпечення. **В2.З2.** Тактики і техніки атак кібербезпеки **В2.З3.** Порядок зіставлення даних із різних кінцевих точок і рішень безпеки для виявлення інцидентів. **В2.З4.** Компоненти системи мережевої безпеки (мережеві екрани, віртуальні приватні мережі, системи виявлення вторгнень).	**В2.У1.** Використовувати інструменти мережевого аналізу для визначення вразливостей. **В2.У2.** Застосовувати на практиці програмне забезпечення відповідного спрямування. **В2.У3.** Опановувати найкращі практики, стандарти, системи кібербезпеки, закони та нормативні акти щодо обробки інцидентів та реагування на них. **В2.У4.** Відстежувати роботу системи і реагувати на події у	**В2.К1.** Застосовувати на практиці всі технічні, функціональні та експлуатаційні аспекти опрацювання і реагування на інциденти кібербезпеки.	**В2.В1.** Впроваджувати і розвивати методи тестування опрацювання інцидентів.

			відповідь на тригери та/або спостерігати за трендами або незвичайною діяльністю.		
	В3. Здатність пом'якшувати наслідки інцидентів кібербезпеки або витоку даних та відновлювати системи до робочого стану.	**В3.З1.** Процеси управління ризиками, а саме, методи оцінки та пом'якшення ризиків. **В3.З2.** Резервне копіювання та відновлення даних. **В3.З3.** Засоби діагностики систем і методів виявлення несправностей. **В3.З4.** 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.У2.** Запобігати негативним наслідкам кіберінцидентів, мінімізовувати та усувати їх, виправляти вразливості, а також відновлювати сталість і надійність функціонування систем та інших об'єктів кіберзахисту.	**В3.К1.** Взаємодіяти з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємст-вами установами та організаціями, які є суб'єктами національної системи кібербезпеки.	**В3.В1.** Оцінювати стійкість засобів контролю кібербезпеки та заходів щодо пом'якшення наслідків, вжитих після інциденту кібербезпеки або витоку даних.
	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 вплинути на підприємство (установу, організацію).	**Г1.З1.** Порядок витягування, аналіз і використання метаданих. **Г1.З2.** Типи порушників, які здійснюють кібератаки. **Г1.З3.** Різні класи атак. **Г1.З4.** Засади тактик, прийомів і процедур. **Г1.З5.** Політики, процедури і правила кіберзахисту та інформаційної безпеки. **Г1.З6.** Методи роботи з великими обсягами даних та їх аналітика. **Г1.З7.** Кіберзагрози та вразливості. **Г1.З8.** Принципи забезпечення конфіденційності персональних даних та кібербезпеки.	**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 виголошувати доповідь з оцінки поточного стану кібербезпеки керівництву, персоналу і користувачам.	**Г1.В1.** Використовувати аналітичні дані при формуванні рекомендацій щодо зниження ризиків.
	Г2. Здатність здійснювати аналіз тенденцій кіберзахисту та формувати	**Г2.З1.** Загальні види зараження комп’ютерів/ мереж а також методи зараження. **Г2.З2.** Сучасні комп’ютерні набори вторгнень.	**Г2.У1.** Оцінювати інформацію на надійність, достовірність і релевантність. **Г2.У2.** Розвивати розуміння контексту	**Г2.К1.** Аналізувати дані з одного або декількох джерел, готувати оперативні	**Г2.В1.** Складати і доводити до відома зацікавлених сторін звіти з кібердослідними даними.

	відповідні звіти.	**Г2.33.** Нормативно-правову базу, пов'язану з кібербезпекою та захистом даних. **Г2.34.** Можливості кіберрозвідки/збору інформації та сховищ даних. **Г2.35.** Міжнародне законодавство, нормативні та методичні документи у сферах кібербезпеки, кіберзахисту та протидії кіберзагрозам. **Г2.36.** Нові кіберзагрози та суб'єкти загроз. **Г2.37.** Сучасні рішення у галузі кібербезпеки.	загрозливого середовища організації.	звіти на основі кібердослід-них даних та поширення серед зацікавлених сторін.	
	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.				
Д. Надання експертної технічної підтримки з управління кіберінциден-тами.	**Д1.** Здатність здійснювати реалізацію на підприємстві (в установі, організації) повноважень технічного експерта, взаємодіяти з представника-	**Д1.З1.** Застосовувана в організації/ підприємстві програма класифікації інформації і процедур розкриття. **Д1.З2.** 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	**Д1.К1.** Готувати аудиторські звіти, у яких визначаються технічні та процедурні висновки, а також надавати рекомендовані	**Д1.В1.** Проводити детальний аналіз та надавати рекомендації з реагування та підтримки відновлення до робочого стану системи.

	ми правоохоронних органів та за необхідності роз'яснення для них деталей інцидентів, співпрацювати з аналітиками розвідки з метою кореляції даних при оцінці загроз.	**Д1.З3.** Типи загроз кібербезпеки, вектори атак, мотиви та дії зловмисників. **Д1.З4** Порядок розкриття вразливостей, інцидентів, пов'язаних із витоком даних, та геополітичних подій, що впливають на кіберризики. **Д1.З5.** Еталонні моделі архітектури безпеки та рішення у галузі безпеки **Д1.З6.** Методологію опрацювання інцидентів кібербезпеки.	щодо політики кібербезпеки. **Д1.У2.** Використовувати інструменти кореляції подій безпеки.	стратегії/рішення для виправлення. **Д1.К2.** Працювати в команді та співпрацювати з колегами.	
	Д2. Здатність забезпечувати координацію функцій реагування на інциденти та надавати експертну технічну підтримку профільним фахівцям в масштабах підприємства (установи, організації) для управління інцидентами у	**Д2.З1.** Середовище загроз організації. **Д2.З2.** Концепції і методології аналізу зловмисного програмного забезпечення. **Д2.З3.** Основи управління інцидентами. **Д2.З4.** Основи управління вразливістю, оцінювання загроз, управління ризиками та автоматизація процесів реагування на інциденти. **Д2.З5.** Комплекс заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти,	**Д2.У1.** Застосовувати принципи кібербезпеки і приватності при формуванні вимог організації (стосовно конфіденційності, цілісності, доступності, автентифікації і неспростовності). **Д2.У2.** Аналізувати політику та конфігурації кіберзахисту організації та оцінити відповідність нормам і директивам організації.	**Д2.К1.** Розробляти рекомендації щодо вибору ефективних, з точки зору витрат, засобів контролю безпеки з метою зниження ризиків.	**Д2.В1.** Використовувати схвалені принципи та методи глибокого захисту. **Д2.В2.** Виконувати обов'язки внутрішнього консультанта/радника в сфері планування заходів з розвитку кібербезпеки в організації.

	сфері кіберзахисту.	впровадження контрзаходів, спрямованих на мінімізацію вразливостей систем.	**Д2.У3.** Удосконалювати системи кіберзахисту з урахуванням результатів оцінки повноти, адекватності, результативності та ефективності процесів, що виконуються.		
	Предмети та засоби праці: Протоколи, стандарти та сертифікати відповідного спрямування; комп'ютерне, програмне та інше технікотехнологічне 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 кіберінциден-тів.	**Е1.** Здатність здійснювати дослідження кіберінциден-тів та проводити аналіз заходів реагування на інциденти кібербезпеки, оцінювати ефективність засобів та покращувати існуючі практики кіберзахисту.	**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 кіберінцидентам/ кібератакам. **Е1.З4.** Практики та інструменти опрацювання кібербезпекових інцидентів **Е1.З5.** Методи та засоби розслідування кіберінцидентів. **Е1.З6.** Закони, нормативні акти, політики і етичні норми, та як вони пов'язані	**Е1.У1.** Накопичувати та проводити аналіз даних про кіберінциденти. **Е1.У2.** Проводити оцінку процесів прийняття рішень щодо загроз. **Е1.У3.** Визначати тактику та методологію попередження загроз. **Е1.У4.** Оцінювати інформацію на надійність, достовірність і релевантність. **Е1.У5.** Використовувати	**Е1.К1.** Формувати звітність стосовно аналізу результатів інциденту та дій з опрацювання інцидентів. **Е1.К2.** Проводити обмін інформацією про інциденти кібербезпеки між суб'єктами.	**Е1.В1.** Проводити дослідження та аналізувати процес реагування на інциденти кібербезпеки з метою підвищення ефективності та вдосконалення існуючих практик. **Е1.В2.** Формувати власну базу даних про кіберінциденти.

		з конфіденційністю персональних даних та кібербезпекою. **Е1.З7.** Принципи забезпечення конфіденційності персональних даних та кібербезпеки. **Е1.З8.** Процеси управління ризиками, а саме, методи оцінки та пом'якшення ризиків.	зворотній зв'язок для покращення процесів, продуктів і послуг. **Е1.У6.** Вивчати та досліджувати сучасні види кіберінцидентів/ Кібератак. **Е1.У7.** Проєктувати реагування на інциденти для моделей хмарних сервісів.	забезпечення 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 розроблювати та запроваджувати на практиці методики та настанови з кіберзахисту, сприяти розробленню, підтримці та оцінюванню плану реагування на інциденти.	**Є1.З1.** Політики, процедури і правила кіберзахисту та інформаційної безпеки. **Є1.З2.** Національні, європейські та міжнародні стандарти кібербезпеки і відповідні стандарти, законодавство, політики і правила щодо приватності. **Є1.З3.** Вимоги та підходи до розроблення навчальних та методичних матеріалів. **Є1.З4.** Нормативно-правову базу, пов'язану з кібербезпекою та захистом даних.	**Є1.У1.** Розроблювати та застосовувати у практичній діяльності технічну документацію відповідного спрямування. **Є1.У2.** Застосовувати принципи кібербезпеки та конфіденційності д організаційних вимог. **Є1.У3.** Контролювати етапи реагування на інцидент кібербезпеки.	**Є1.К1.** Взаємодіяти з іноземними та міжнародними організаціями з питань реагування на кіберінциденти. **Є1.К2.** Організовувати та проводити практичні семінари з питань	**Є1.В1.** Рекомендувати зміни та доповнення до політики кібербезпеки організації, приймати участь у координації її перегляду. **Є1.В1.** Проводити регулярне оновлення плану реагування на інциденти.

			Є1.У4. Розроблювати 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.	кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту. **Є1.К3.** Розроблювати вказівки і настанови для працівників, залучених до розроблення стратегій, програм та політик з розвитку кібербезпеки.	
	Є2. Здатність співпрацювати з зацікавленими сторонами для вирішення інцидентів комп'ютерної безпеки та відповідності вразливостям.	**Є2.З1.** Комунікаційний цикл опрацювання інцидентів. **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 кіберінцидентів.	**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 кіберзагрози.	**Є2.К1.** Співпрацю-вати з центрами інформаційної безпеки (SOC) та групами реагування на інциденти з комп'ютерної безпеки (CSIRT).	**Є2.В1.** Налаштовувати взаємодію з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, (установами, організаціями), які є суб'єктами національної системи кібербезпеки.

		Є2.З3. Методи і способи ефективної комунікації. **Є2.З4.** Розвиток міжнародного співробітництва у сфері кібербезпеки. **Є2.З5.** Стандарти обміну кібердослідними даними. **Є2.З6.** Методи і способи ефективної комунікації.	**Є2.У4.** Співпрацювати оперативно з командами реагування на комп'ютерні надзвичайні події щодо виявлення джерел кібератаки та засобів протидії.	**Є2.К2.** Співпрацювати з співробітниками для повідомлення про інциденти безпеки 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.	
	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 Науково-навчального 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 Науково-навчального 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 Держспецзв’язку;

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 Науково-навчального 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 (рішення (може оформлюватися протоколом), наказ, розпорядження).

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 _____ 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 від _____ щодо погодження проєкту професійного стандарту «Фахівець з реагування на інциденти кібербезпеки».

VIII. Дата внесення професійного стандарту до Реєстру _____.

IX. Рекомендована дата перегляду професійного стандарту Вересень 2028 року.