Проєкт

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

Професійний стандарт

АНАЛІТИК ЗАГРОЗ БЕЗПЕКИ

_____(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

Аналітик загроз безпеки

ІІ. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Збір, обробка, аналіз інформації про кіберзагрози та поширення оцінки кіберзагроз/попереджень. Розробка планів та процедур для управління аналізом загроз. Визначення та контроль тактик, прийомів і процедур (TTP), які використовуються суб'єктами кіберзагроз, та тенденцій їх розвитку шляхом аналізу даних, інформації та кібердослідних даних із відкритих і власних джерел. Оцінка спроможності та діяльності злочинців у сфері кібербезпеки та підготовка відповідних висновків. Аналіз даних з одного або декількох джерел, підготовка оперативних звітів на основі кібердослідних даних щодо загроз та поширення серед зацікавлених сторін. Використання аналітичних даних при формуванні рекомендацій щодо зниження ризиків.

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="5">Секція J</td><td rowspan="5">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="3">Розділ 62</td><td rowspan="3">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 62.09</td><td>Інша діяльність у сфері інформаційних технологій і комп'ютерних систем</td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="3">Секція M</td><td rowspan="3">Професійна, наукова та технічна діяльність</td><td rowspan="3">Розділ 74</td><td rowspan="3">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>
<tr><td></td><td></td></tr>
</table>

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

Аналітик загроз безпеки, 2139.2

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

Аналітик загроз безпеки, 7 рівень НРК

Провідний аналітик загроз безпеки, 7 рівень НРК

5. Назва (назви) документа (документів), що підтверджує (підтверджують) професійну кваліфікацію особи

- 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 аналітичної діяльності із загроз безпеки;

- документ (диплом, сертифікат, тощо), щодо професійної сертифікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері аналітичної діяльності із загроз безпеки.

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**
Аналітик загроз безпеки	Підготовка на другому рівні вищої освіти (магістерському) за спеціальностями вказаними	*Не передбачено професійним стандартом*

	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), фахівець сфери захисту інформації тощо)	
Провідний аналітик загроз безпеки	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	**Суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій**

кваліфікації	**Кваліфікаційні центри**	**Суб'єкти освітньої діяльності**
Аналітик загроз безпеки	Підвищення кваліфікації "аналітик загроз безпеки" для отримання професійної кваліфікації "провідний аналітик загроз безпеки". Стаж роботи не менше двох років	*Не передбачено професійним стандартом*

IV. Абревіатури, скорочення

IT	інформаційні технології
EBSCO	Elton Bryson Stephens Company
JSTOR	Journal Storage
TCP/UDP	Transmission Control Protocol / User Datagram Protocol

V. Опис трудових функцій

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
А. Проведення збору даних про загрози та ідентифікація подій кібербезпеки.	**А1.** Здатність проводити збір інтегрованої, об'єднаної, розвідувальної інформації про кібероперації з усіх джерел та надання показників і попереджень про результати розвідки.	**А1.З1.** Концепції і протоколи комп'ютерних мереж, а також методології безпеки мережі **А1.З2.** Закони, нормативні акти, політики і етичні норми, та як вони пов'язані з конфіденційністю персональних даних та кібербезпекою. **А1.З3.** Загальні види зараження комп'ютерів/мереж а також методи зараження. **А1.З4.** Алгоритми шифрування та кіберможливості/інструменти. **А1.З5.** Фізичні і логічні мережеві пристрої та інфраструктури, зокрема концентратори, комутатори, маршрутизатори, брандмауери. **А1.З6.** Загальні мережеві протоколи та протоколи маршрутизації, послуги та їх взаємодія для забезпечення мережевих зв'язків. **А1.З7.** Засади тактик, прийомів і процедур.	**А1.У1.** Визначати та характеризувати всі відповідні аспекти операційного середовища. **А1.У2.** Використовувати кілька пошукових систем та інструментів для проведення пошуку з відкритим кодом . **А1.У3.** Проводити дослідження. з використанням Web-сайтів/сторінок, що не індексуються пошуковими системами. **А1.У4.** Збирати точні та повні дані з джерел, які використовуються для розвідки, оцінювання та/або планування.	**А1.К1.** Співпрацювати з аналітиками розвідки/орієнтованими організаціями, які займаються суміжними сферами.	**А1.В1.** Збирати точні та повні дані з джерел, які використовуються для результатів розвідки, оцінки та/або планування **А1.В2.** Формувати запити на профільну інформацію .

		А1.З8. Методи аналізу мережевого трафіку. **А1.З9.** Методи автентифікації, авторизації та контролю доступу. **А1.З10.** Загрози і вразливості безпеки систем і прикладного програмного забезпечення.			
	А2. Здатність брати участь в процесі визначення недоліків у зборі розвідувальної інформації.	**А2.З1.** Принципи забезпечення конфіденційності персональних даних та кібербезпеки. **А2.З2.** Можливості кіберрозвідки/збору інформації та сховищ даних. **А2.З3.** Фундаментальні основи комп'ютерних мереж **А2.З4.** Скрипти та мови програмування. **А2.З5.** Термінологію передачі даних. **А2.З6.** Методологію розвитку кібербезпеки організації.	**А2.У1.** Проводити наради та консультації під час проведення аналізу процесу збору розвідувальної інформації у сфері Кібербезпеки. **А2.У2.** Інтегрувати дані про загрози.	**А2.К1.** Працювати в команді та співпрацювати з зовнішніми експертами за потреби. **А2.К2.** Співпрацювати із профільними фахівцями. **А2.К3.** Готувати та проводити брифінги з обговорення питань щодо виявлення та усунення недоліків у зборі розвідувальної інформації.	**А2.В1.** Розроблювати документацію відповідного спрямування. **А2.В2.** Виявляти пробіли розвідки.
	А3. Здатність співпрацювати з планувальниками, аналітиками розвідки та менеджерами збору, з метою забезпечення точності та актуальності	**А3.З1.** Сучасні комп'ютерні набори вторгнень. **А3.З2.** Термінологію/лексику кібероперацій. **А3.З3.** Стандарти обміну кібердослідними даними. **А3.З4.** Методи і способи ефективної комунікації.	**А3.У1.** Оцінювати, аналізувати та синтезувати великі об'єми даних в високоякісні і об'єднані продукти. **А3.У2.** Формувати, аналізувати і редагувати результати	**А3.К1.** Здійснювати формування запитів на отримання інформації. **А3.К2.** Працювати в команді та співпрацювати з колегами та за потреби із зовнішніми експертами.	**А3.В1.** Розробляти та впроваджувати протоколи спільних дій з суб'єктами забезпечення кібербезпеки, для забезпечення ефективного

	вимог до розвідки та планів збору інформації.		кіберрозвідки/оцінки даних з декількох джерел.		інформаційного обміну розвідувальної інформації про кібероперації.
	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 планування; бібліотечні ресурси, архівні матеріали (за потреби); законодавчо-нормативні акти, акти роботодавця відповідного спрямування.				
Б. Здійснення аналізу розвідувальної інформації щодо загроз безпеки.	**Б1.** Здатність проводити аналіз щодо змін діяльності, тактики, можливостей, цілей, пов'язаних із визначеними наборами проблем попередження про кібероперації.	**Б1.З1.** Процеси управління ризиками, а саме, методи оцінки та пом'якшення ризиків. **Б1.З2.** Кіберзагрози та вразливості. **Б1.З3.** Сучасні комп'ютерні набори вторгнень. **Б1.З4.** Методи аналізу мережевого трафіку **Б1.З5.** Витягування, аналіз і використання метаданих. **Б1.З6.** Сучасні/перспективні комунікаційні технології. **Б1.З7.** Фізичні комп'ютерні компоненти і архітектури, включаючи функції різних компонентів і периферійних пристроїв. **Б1.З8.** Сучасні комп'ютерні набори вторгнень. **Б1.З9.** Методи роботи з великими обсягами даних та їх аналітика.	**Б1.У1.** Критично мислити. **Б1.У2.** Проводити поглиблене дослідження та аналізу загроз. **Б1.У3.** Виявляти, відстежувати й оцінювати тактики, методи та процедури, які використовуються суб'єктами кіберзагроз, шляхом аналізу даних, інформації та кібердослідних даних із відкритих і власних джерел. **Б1.У4.** Проводити дослідження з використанням Web-сайтів/сторінок, що не індексуються	**Б1.К1.** Надавати (за потреби) предметні експертні знання та підтримку форумам з планування/ розвитку і робочим групам. **Б1.К2.** Співпрацювати з аналітиками розвідки/орієнтованими організаціями, які займаються суміжними сферами.	**Б1.В1.** Оцінювати ефективність процедур відповідного спрямування. **Б1.В2.** Оцінювати, аналізувати та синтезувати великі об'єми даних (які можуть бути фрагментованими і суперечливими) в високоякісні і об'єднані продукти розвідки. **Б1.В3.** Розроблювати аналітичну документацію відповідного спрямування.

		Б1.З10. Засади тактик, прийомів і процедур **Б1.З11.** Адресацію в Інтернет-мережі (IP-адреси, маршрутизація на основі безкласових IP-адрес, система нумерації TCP/UDP-портів). **Б1.З12.** Принципи забезпечення конфіденційності персональних даних та кібербезпеки.	пошуковими системами. **Б1.У5.** Визначати критичні цільові елементи, щоб включити критичні цільові елементи для кібердомену. **Б1.У6.** Розпізнавати і пом'якшувати когнітивні упередження, які можуть вплинути на аналіз. **Б1.У7.** Використовувати кілька пошукових систем та інструментів для проведення пошуку з відкритим кодом.		
	Б2. Здатність проводити предметну експертизу розвідувальних даних щодо загроз з метою розробки загальної оперативної картини.	**Б2.З1.** Конкретні операційні наслідки інцидентів кібербезпеки. **Б2.З2.** Етапи здійснення кібератак (розвідка, сканування, перерахування, отримання доступу, ескалація привілеїв, підтримка доступу, використання мережі, приховування слідів). **Б2.З3.** Загальні види зараження.	**Б2.У1.** Забезпечувати розуміння цільових або загрозливих систем шляхом ідентифікації та аналізу фізичних, функціональних або поведінкових зв'язків. **Б2.У2.** Збирати, аналізувати і зіставляти	**Б2.К1.** Координувати із зацікавленими сторонами обмін і використання оперативної інформації про відповідні кіберзагрози.	**Б2.В1.** Підтримувати загальну розвідувальну картину. **Б2.В2.** Розроблювати конкретні показники кібероперацій. **Б2.В3.** Розроблювати або рекомендувати

		комп’ютерів/мереж а також методи зараження. **Б2.З4.** Фундаментальні концепції кібероперацій, термінологія та лексика. **Б2.З5.** Випадки розкриття вразливостей, інцидентів, пов’язаних із витоком даних, та геополітичні події, що впливають на кіберризики. **Б2.З6.** Внутрішню тактику прогнозування і/або моделювання спроможностей та дій загроз. **Б2.З7.** Класифікація кіберможливостей (захист, атаки, експлуатація). **Б2.З8.** Порядок розроблення планів аварійного відновлення та безперервності операцій для систем, що розробляються, та тестування систем до їхнього вводу у продуктивне середовище. **Б2.З9.** Кіберзагрози та вразливості.	інформацію про кіберзагрози, що надходить із кількох джерел. **Б2.У3.** Використовувати і застосовувати платформи та інструменти кібердосліджень. **Б2.У4.** Проводити предметну експертизу з метою розробки спеціальних індикаторів кібероперацій. **Б2.У5.** Визначати та характеризувати всі відповідні аспекти операційного середовища. **Б2.У6.** Планувати проведення предметних експертиз. **Б2.У7.** Здійснювати аналіз розвідувальних заходів для підтримки призначених навчань, заходів з планування і		аналітичні підходи або рішення для подолання проблем або ситуацій, для яких недостатньо інформації або немає прецедентна.

			операцій, залежних від часу їх проведення.		
	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 планування; бібліотечні ресурси, архівні матеріали (за потреби); законодавчо-нормативні акти, акти роботодавця відповідного спрямування.				
В. Дослідження тенденцій розвитку кіберзагроз та моніторинг діяльності суб'єктів загроз.	**В1.** Здатність проводити моніторинг та звітування про підтверджені загрозливі дії.	**В1.З1.** Методи і техніки атак. **В1.З2.** Внутрішня тактика прогнозування і/або моделювання спроможностей та дій загроз. **В1.З3.** Шкідливі програми **В1.З4.** Шляхи, якими цілі або загрози використовують Інтернет-мережу. **В1.З5.** Сучасні кіберзагрози та суб'єкти кіберзагроз **В1.З6.** Кіберзагрози та вразливості.	**В1.У1.** Оцінювати інформацію на надійність, достовірність і релевантність. **В1.У2.** Критично мислити. **В1.У3.** Збирати, аналізувати і зіставляти інформацію про кіберзагрози, що надходить із кількох джерел. **В1.У4.** Виявляти та оцінювати суб'єкти загроз, які націлені на організацію. **В1.У5.** Використовувати кілька пошукових систем та інструментів для проведення пошуку з відкритим кодом.	**В1.К1.** Готувати звітні документи стосовно тенденцій розвитку кіберпростору. **В1.К2.** Використовувати аналітичні дані при формуванні рекомендацій щодо зниження ризиків Інформувати керівництво, а також внутрішніх і зовнішніх клієнтів про нові розробки, досягнення, проблеми і отриманий досвід.	**В1.В1.** Здійснювати щомісячний аналіз даних стосовно нових загроз у кіберпросторі.

	В2. Здатність відстежувати оперативне середовище та здійснювати сповіщення про ворожу діяльність, яка відповідає пріоритетним вимогам керівництва до інформації.	**В2.З1.** Фундаментальні концепції кібероперацій, термінологію та лексику. **В2.З2.** Як сучасні цифрові та телефонні мережі впливають на кібероперації. **В2.З3.** Як сучасні системи бездротового зв'язку впливають на кібероперації. **В2.З4.** Системи загрози та/або цільові системи. **В2.З5.** Методи роботи з великими обсягами даних та їх аналітика.	**В2.У1.** Оцінювати інформацію на надійність, достовірність і релевантність. **В2.У2.** Мислити як порушник. **В2.У3.** Визначати тактики, прийоми і процедури та кампанії суб'єктів загроз.	**В2.К1.** Своєчасно повідомляти про неминучі або ворожі наміри чи дії, які можуть вплинути на цілі, ресурси чи можливості організації.	**В2.В1.** Ідентифікувати кіберзагрози, які можуть поставити під загрозу інтереси організації та/або партнерів
	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 планування; бібліотечні ресурси, архівні матеріали (за потреби); законодавчо-нормативні акти, акти роботодавця відповідного спрямування.				
Г. Підготовка оперативних звітів про підтверджені загрозливі дії та поширення серед зацікавлених сторін.	**Г1.** Здатність забезпечувати надання поточної розвідувальної підтримки критичним внутрішнім / зовнішнім зацікавленим сторонам.	**Г1.З1.** Типи, процеси адміністрування, функції і системи управління контентом Web-сайтів. **Г1.З2.** Термінологію/ лексику кібероперацій. **Г1.З3.** Методи роботи з великими обсягами даних та їх аналітика. **Г1.З4.** Статистику та методики прогнозування. **Г1.З5.** Загальні компоненти системи диспетчерського контролю та збору даних	**Г1.У1.** Розроблювати інформаційні вимоги, необхідні для відповідей на пріоритетні інформаційні запити. **Г1.У2.** Доводити впевнено і систематизовано складну інформацію, концепції або ідеї в усній і письмовій формах і/або за	**Г1.К1.** Відповідати на запити щодо надання інформації. **Г1.К2.** Розпізнавати і пом'якшувати дезінформацію у звітності і аналізі.	**Г1.В1.** Складати і доводити до відома зацікавлених сторін звіти з кібердослідними даними.

		Г1.З6. Основи мережевої безпеки. **Г1.З7.** Технології та рішення у галузі кібербезпеки. **Г1.З8.** Стан кібербезпеки та загроз в організації. **Г1.З9.** Розвідувальну підтримку планування, виконання та оцінювання.	допомогою наочних засобів. **Г1.У3.** Оцінювати, аналізувати та синтезувати великі об'єми даних в високоякісні і об'єднані продукти.		
	Г2. Здатність повідомляти про важливі мережеві події та вторгнення, отримані за допомогою розвідки.	**Г2.З1.** Методи і техніки атак. **Г2.З2.** Спроможності та діяльність злочинців у сфері кібербезпеки. **Г2.З3.** Кібербезпекові ризиків та загрози. **Г2.З4.** Кіберзагрози, класифікація загроз та репозиторії вразливостей. **Г2.З5.** Типи, процеси адміністрування, функції і системи управління контентом Web-сайтів. **Г2.З6.** Методи соціальної інженерії. **Г2.З7.** Конкретні операційні наслідки інцидентів кібербезпеки.	**Г2.У1.** Оцінювати інформацію на надійність, достовірність і релевантність. **Г2.У2.** Ідентифікувати кіберзагрози, які можуть поставити під загрозу інтереси організації та/або партнерів. **Г2.У3.** Розроблювати профільні плани та готувати відповідну кореспонденцію.	**Г2.К1.** Відкрито та публічно викладати кібердослідні дані. **Г2.К2.** Проводити аналіз діяльності з використання цільової інфраструктури.	**Г2.В1.** Проводити технічний аналіз та готувати відповідні висновки.
	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 планування; бібліотечні ресурси, архівні матеріали (за потреби); законодавчо-нормативні акти, акти роботодавця відповідного спрямування.				
Д. Координація	**Д1.** Здатність визначати	**Д1.З1.** Методи і техніки атак.	**Д1.У1.** Ідентифікувати	**Д1.К1.** Організовувати та проводити практичні	**Д1.В1.** Виконувати

діяльності з проведення аналітики загроз безпеки.	тактику та методологію виявлення загроз.	**Д1.З2.** Міжнародне законодавство, нормативні та методичні документи у сферах кібербезпеки, кіберзахисту та протидії кіберзагрозам. **Д1.З3.** Сучасні рішення у галузі кібербезпеки **Д1.З4.** Методи та підходи щодо формування тактики та методології. **Д1.З5.** Стратегії зменшення ризиків для усунення кібервразливостей. **Д1.З7.** Класифікацію методів з виявлення та усунення загроз. **Д1.З8.** Кіберзагрози та вразливості.	кіберзагрози, які можуть поставити під загрозу інтереси організації та/або партнерів. **Д1.У2.** Розробляти і консультувати щодо планів пом'якшення наслідків загроз. **Д1.У3.** Інтегрувати нові ідеї та підходи у зміст тактики та методології виявлення загроз в необхідних обсягах і формах.	семінари з питань методів та технік виявлення загроз. **Д1.К2.** Прогнозувати спільно із стейкхолдерами поточні потреби у профільних послугах.	обов'язки внутрішнього консультанта/ радника в сфері планування заходів з розвитку кібербезпеки в організації.
	Д2. Здатність здійснювати оцінювання процесів прийняття рішень щодо загроз та співпрацювати із зацікавленими сторонами з метою розроблення політик корпоративного управління	**Д2.З1.** Організаційну ієрархію та процеси прийняття рішень у кіберпросторі. **Д2.З2.** Можливості кіберрозвідки/збору інформації та сховищ даних. **Д2.З3.** Основи управління ризиками, стандарти, методології, інструменти, рекомендації та найкращі практики. **Д2.З4.** Особливості організації оцінювання	**Д2.У1.** Розробляти, впроваджувати та управляти стратегією організації з аналізу кіберзагроз **Д2.У2.** Використовувати зворотній зв'язок з метою вдосконалення процесів, продуктів і послуг	**Д2.К1.** Проводити оцінку та отримувати зворотній зв'язок, необхідний для вдосконалення надання розвідувальної інформації, її звітування та вимог до збору та проведення операцій. **Д2.К2.** Визначати спільно із стейкхолдерами та/або впроваджувати	**Д2.В1.** Розроблювати документацію відповідного спрямування. **Д2.В2.** Оцінювати інформацію на предмет її надійності, достовірності і актуальності.

	діяльністю в сфері аналітики загроз безпеки.	процесів прийняття рішень щодо загроз. **Д2.З5.** Внутрішню та зовнішню тактику прогнозування і/або моделювання спроможностей та дій загроз. **Д2.З6.** Основні небезпеки, ризики і кібервразливості. **Д2.З7.** Прийняті в організації правила класифікації інформації щодо рівнів захисту і процедур доступу до неї.	**Д2.У3.** Використовувати дані для підтримки та допомоги у моделюванні загроз, рекомендацій щодо зниження ризиків та пошуку кіберзагроз. **Д2.У4.** Готувати матеріали, інструкції для надання детальних настанов для відповідної частини персоналу.	політику і процедури, щоб забезпечити належний захист від загроз безпеки.	
	Д3. Здатність здійснювати координацію, перевірку та управління вимогами, планами та/або діяльністю щодо збору даних з усіх джерел.	**Д3.З1.** Нормативно-правову базу, нормативно-правові акти, стандарти, пов’язані із кібербезпекою. **Д3.З2.** Зовнішні організації і установи, діяльність яких спрямована на розвиток, захист та дослідження кіберпростору **Д3.З3.** Новітні технології, інструменти, процедури, методи та процеси відповідного спрямування. **Д3.З4.** Закони, нормативні акти, політики і етичні норми, та як вони пов’язані з конфіденційністю персональних даних та кібербезпекою.	**Д3.У1.** Автоматизувати процедури управління кібердослідними даними щодо загроз. **Д3.У2.** Розробляти плани та процедури для управління аналізом загроз. **Д3.У3.** Формувати, аналізувати і редагувати результати кіберрозвідки/оцінки даних з декількох джерел.	**Д3.К1.** Працювати в команді та співпрацювати з зовнішніми експертами за потреби. **Д3.К2.** Застосовувати на практиці методи і способи ефективної комунікації.	**Д3.В1.** Працювати в колективі, постійно звертатись за консультаціями до аналітиків і експертів (внутрішніх і зовнішніх організацій) для використання аналітичного і технічного досвіду. **Д3.В2.** Опановувати досягнення у сфері аналітики загроз безпеки

					для забезпечення їх впровадження у відповідній організації.
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю планування; бібліотечні ресурси, архівні матеріали (за потреби); законодавчо-нормативні акти, акти роботодавця відповідного спрямування.				

VI. Розподіл трудових функцій та компетентностей за професійними кваліфікаціями

Трудова функція (умовне позначення)	**Загальна назва професійної кваліфікації в межах професійного стандарту: фахівець з планування політики та стратегії кібербезпеки**	
	Аналітик загроз безпеки	**Провідний аналітик загроз безпеки**
	повна	повна
А	**+**	**+**
Б	**+**	**+**
В	**+**	**+**
Г	**+**	**+**
Д	**-**	**+**

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 сектору сертифікації 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 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 «аналітик загроз безпеки» 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 «аналітик загроз безпеки».

VIII. Дата внесення професійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.