ПРОФЕСІЙНИЙ СТАНДАРТ

Аналітик інформації з відкритих джерел (OSINT-аналітик)

_____

(дата внесення до Реєстру кваліфікацій)

ЗАТВЕРДЖЕНО
Розробником Національною академією Служби безпеки України наказ № 83 від 16 06 2026 року

Професійний стандарт розроблено та затверджено згідно з вимогами статті 4^2 Кодексу законів про працю України на підставі:

- висновоку суб'єкта перевірки Національного агентства кваліфікацій від 9.06.2026, (рішення № 20, протокол 37 (301) від 9.06.2026) про дотримання під час підготовки проєкту професійного стандарту «Аналітик інформації з відкритих джерел (OSINT-аналітик)» вимог Порядку розроблення, введення в дію та перегляду професійних стандартів, затвердженого постановою Кабінету Міністрів України від 31.05.2017 № 373)
- висновку Професійної спілки працівників державних установ України щодо погодження професійного стандарту «Аналітик інформації з відкритих джерел (OSINT-аналітик)» від 03.06.2026 № 83.

1. Назва професійного стандарту
Аналітик інформації з відкритих джерел (OSINT-аналітик)

2. Загальні відомості про професійний стандарт

1) мета діяльності за професією
Правомірні, етичні, безпечні пошук і збирання відомостей та/або даних з відкритих джерел, їх технічне оброблення, аналітичне опрацювання і створення якісних інформаційно-аналітичних продуктів.

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 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
		Розділ 63	Надання інформаційних послуг	**Група 63.1**	Оброблення даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність; веб-портали
				Клас 63.11	Оброблення даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність

				Група 63.9	Надання інших інформаційних послуг
				Клас 63.99	Надання інших інформаційних послуг, н.в.і.у.
Секція M	Професійна, наукова та технічна діяльність	**Розділ 72**	Наукові дослідження та розробки	**Група 72.2**	Дослідження й експериментальні розробки у сфері суспільних і гуманітарних наук
				Клас 72.20	Дослідження й експериментальні розробки у сфері суспільних і гуманітарних наук
Секція N	Діяльність у сфері адміністративного та допоміжного обслуговування	**Розділ 80**	Діяльність охоронних служб та проведення розслідувань	**Група 80.3**	Проведення розслідувань
				Клас 80.30	Проведення розслідувань
Секція O	Державне управління й оборона; обов'язкове соціальне страхування	**Розділ 84**	Державне управління й оборона; обов'язкове соціальне страхування	**Група 84.2**	Надання державних послуг суспільству в цілому
				Клас 84.22	Діяльність у сфері оборони
				Клас 84.24	Діяльність у сфері охорони громадського порядку та безпеки

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

Аналітик інформації з відкритих джерел (OSINT-аналітик), 2490

Уточнююча назва професії утворена відповідно до Примітки 2 Додатку В Національного класифікатора України ДК 003:2010 «Класифікатор професій».

4) узагальнена назва професії (за потреби).

5) назви типових посад (за потреби).

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

аналітик інформації з відкритих джерел (OSINT-аналітик), 6 рівень НРК

старший аналітик інформації з відкритих джерел (старший OSINT-аналітик), 7 рівень НРК

провідний аналітик інформації з відкритих джерел (провідний OSINT-аналітик), 7 рівень НРК

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

сертифікат про присвоєння (підтвердження) професійної кваліфікації аналітик інформації з відкритих джерел (OSINT-аналітик);

сертифікат про присвоєння (підтвердження) професійної кваліфікації старший аналітик інформації з відкритих джерел (старший OSINT-аналітик);

сертифікат про присвоєння (підтвердження) професійної кваліфікації провідний аналітик інформації з відкритих джерел (провідний OSINT-аналітик);

сертифікат про визнання професійної кваліфікації аналітик інформації з відкритих джерел (OSINT-аналітик) (щодо професійної кваліфікації, здобутої в інших країнах).

3. Здобуття професійної кваліфікації та професійний розвиток

1) Здобуття професійної кваліфікації (назва професійної та/або часткової професійної кваліфікації; суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій)

Назва професійної та/або часткової професійної кваліфікації	**Суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності/інші уповноважені законодавством суб'єкти**
аналітик інформації з відкритих джерел (OSINT-аналітик)	**Перший (бакалаврський)** рівень вищої освіти Без вимог до стажу роботи	Не передбачено професійним стандартом

2) Професійний розвиток:

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**
старший аналітик інформації з відкритих	**Другий (магістерський)** рівень вищої освіти	Не передбачено професійним стандартом

джерел (старший OSINT-аналітик)	Стаж роботи за професійною кваліфікацією аналітик інформації з відкритих джерел (OSINT-аналітик) не менше 2 років	
провідний аналітик інформації з відкритих джерел (провідний OSINT-аналітик)	**Другий (магістерський)** рівень вищої освіти Стаж роботи за професійною кваліфікацією старший аналітик інформації з відкритих джерел (OSINT-аналітик) не менше 2 років	Не передбачено професійним стандартом

без присвоєння наступного/вищого рівня професійної кваліфікації:

для вдосконалення (підтримання) професійної кваліфікації, в тому числі шляхом набуття нових/додаткових навичок/компетентностей

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, незалежно від форми власності.

4. Абревіатури, скорочення (за потреби)

API	*Application Programming Interface (Інтерфейс програмування застосунків)*
OSINT	*Open Source Intelligence* (розвідка з відкритих джерел)
OPSEC	*Operational Security* (операційна безпека)
IP	*Internet Protocol* (протокол інтернету)
DNS	*Domain Name System* (система доменних імен)
WebRTC	*Web Real-Time Communication* (технологія для передачі аудіо/відео в реальному часі через браузер)
TLS	*Transport Layer Security* (протокол захисту даних у мережі)
RSS	*Really Simple Syndication* (формат для стрічок новин та оновлень)
ШІ	штучний інтелект

5. Опис трудових функцій:

Трудові функції (умовне позначення та назва)	Компетентності	Результати навчання			
		знання	уміння/навички	комунікація	відповідальність і автономія
А. Забезпечення правомірності та етичності OSINT	А1. Здатність дотримуватися вимог законодавства та оцінювати правові ризики.	А1.З1. Міжнародні та наднаціональні правові акти у сфері інформації й захисту прав людини. А1.З2. Законодавство України з питань доступу до інформації, захисту персональних даних, кібербезпеки, електронних комунікацій, відповідальності за неправомірний доступ, збирання або поширення даних, а також норми галузевого законодавства України у відповідній сфері професійної діяльності. А1.З3. Міжнародні та національні нормативні стандарти, які застосовуються у професійній сфері. А1.З4. Основні правові норми, що регулюють доступ до інформації та захист персональних даних у юрисдикціях, релевантних для конкретного дослідження. А1.З5. Правові критерії розмежування між	А.1.У1. Визначати юрисдикції, релевантні для конкретного дослідження, та відповідні правові обмеження. А1.У2. Проводити оцінку можливих правових ризиків до початку та у процесі дослідження. А1.У3. Визначати правові підстави та обмеження збирання даних з конкретних відкритих джерел та/або їх подальшої обробки. А1.У4. Оцінювати правомірність застосовуваних методів збирання та використання даних/інформації з відкритих джерел. А1.У5. Розрізняти відкриті та закриті джерела інформації, ідентифікувати «сірі зони» та приймати обґрунтовані рішення щодо допустимості (правомірності та етичності) використання джерела. А1.У6. Вести ланцюжок збереження (chain of custody). А1.У7. Забезпечувати дотримання процедур збирання та обробки даних як	А1.К1. Консультуватися з юристами з питань правомірності збирання та використання даних, а також правових ризиків. А1.К2. Інформувати замовника та співвиконавців про можливі (виявлені) правові обмеження та ризики.	А1.В1. Оцінювати правові ризики у процесі збирання та оброблення даних. А1.В2. Нести відповідальність за дотримання правових норм під час дослідження. А1.В3 Приймати самостійні обґрунтовані рішення про відмову від збирання чи використання даних у разі виявлення правових перешкод.

		відкритими та іншими джерелами інформації; правовий режим даних у «сірих зонах» (витоки, дані, оприлюднені без згоди власника, дані з обмеженим доступом). А1.З6. Правові умови використання онлайн-платформ (Terms of Service), їх правове значення та наслідки порушення. А1.З7. Основи доказового права: поняття належності, допустимості та достовірності доказів у національному та міжнародному контекстах; вимоги до ланцюжка збереження (chain of custody).	доказів відповідно до національних та/або міжнародних стандартів і рекомендацій. А1.У8 Документувати правові підстави та обмеження збирання та використання даних у кожному конкретному дослідженні.		
	А2. Здатність дотримуватися принципів та стандартів етичної поведінки.	А2.З1. Основні принципи професійної етики (законність, прозорість, доброчесність, достовірність, мінімізація шкоди). А2.З2. Етичні стандарти OSINT та відповідної галузі діяльності. А2.З3. Етичні ризики, пов'язані зі збиранням, обробкою та поширенням інформації, зокрема зумовлені автоматизацією дослідження, використанням ШІ, обробленням даних з травматичним змістом тощо).	А2.У1. Дотримуватися етичних принципів та стандартів у професійній діяльності. А2.У2. Проводити оцінку можливих етичних ризиків у процесі роботи. А2.У3. Визначати межу між суспільним інтересом та правом на приватність. А2.У4. Усвідомлювати наслідки (репутаційні, юридичні, професійні) порушення етичних принципів та стандартів.	А2.К1. Обговорювати етичні дилеми з колегами та фахівцями галузі. А2.К2. Обґрунтовувати етичну позицію перед замовником. А2.К3. Інформувати замовника та співвиконавців про застосовані у процесі дослідження етичні принципи та стандарти.	А2.В1. Самостійно виявляти та вирішувати етичні дилеми. А2.В2. Приймати обґрунтовані рішення щодо допустимості використання джерел та методів збору даних. А2.В3. Нести відповідальність за дотримання етичних принципів та стандартів.

Б. Забезпечення операційної безпеки (OPSEC)	Б1. Здатність визначати основні джерела формування цифрового відбитка, оцінювати ризики деанонімізації та застосовувати технічні й організаційні заходи для зниження можливостей відстеження.	Б1.З1. Природа та структура цифрового відбитка. Б1.З2. Цифровий відбиток профілю вебоглядача, пристрою та мережевого з'єднання. Б1.З3. Принципи IP-адресації, роботи DNS, WebRTC, TLS-відбитків, рекламних ідентифікаторів, метаданих. Б1.З4. Основні механізми відстеження користувача у вебсередовищі та мобільних застосунках. Б1.З5. Базові способи мінімізації цифрових відбитків і мережевих витоків. Б1.З6. Інструкції та протоколи OPSEC під час роботи з відкритими джерелами.	Б1.У1. Виявляти технічні ознаки, що формують цифровий профіль дослідника. Б1.У2. Оцінювати ризики, пов'язані з IP-витоками, DNS-витоками, WebRTC, TLS-відбитками та метаданими. Б1.У3. Налаштовувати вебоглядачі, мережеве середовище та пристрої для зниження відстежуваності. Б1.У4. Використовувати ізольовані середовища, віртуальні машини, окремі пристрої та інші засоби мінімізації цифрового відбитку. Б1.У5. Контролювати поширення файлів і видаляти чутливі метадані перед передаванням.	Б1.К1. Інформувати керівника та інших співробітників про виявлені технічні ризики деанонімізації та вжиті заходи з їх мінімізації.	Б1.В1. Забезпечувати базову мінімізацію цифрового відбитка в межах дослідницької діяльності. Б1.В2. Нести відповідальність за дотримання технічних вимог конфіденційності під час роботи з мережевими ресурсами, пристроями та файлами.
	Б2. Здатність відокремлювати особисту цифрову присутність від дослідницької діяльності та створювати безпечне робоче середовище.	Б2.З1. Типи облікових записів і їх призначення в OSINT. Б2.З2. Принципи розмежування особистої, службової та дослідницької цифрової активності. Б2.З3. Параметри конфіденційності облікових записів, принципи їх налаштування та безпечної експлуатації. Б2.З4. Основи багатофакторної автентифікації та її роль у захисті доступу.	Б2.У1. Розмежовувати особисті та робочі облікові записи і пристрої. Б2.У2. Налаштовувати конфіденційність облікових записів і обмежувати обсяг відкритих персональних даних. Б2.У3. Застосовувати багатофакторну автентифікацію та контролювати безпечний доступ до дослідницьких профілів. Б2.У4. Уникати повторного використання контактних	Б2.К1. Інформувати керівника та інших співробітників підрозділу про виявлені ризики деанонімізації через облікові записи, контактні дані та канали комунікації. Б2.К2. Узгоджувати правила використання облікових записів і засобів зв'язку.	Б2.В1. Підтримувати розмежування особистої та дослідницької цифрової присутності. Б2.В2. Нести відповідальність за недопущення витоку ідентифікаційних ознак через облікові записи, контакти, пристрої та комунікації.

		Б2.З5. Принципи безпечного використання окремих номерів зв'язку, пристроїв, поштових/електронних адрес і каналів комунікації. Б2.З6. Ризики кореляції профілів за псевдонімами, контактними даними, зображеннями, часовими та мовними параметрами.	даних, псевдонімів, паролів та інших ознак, що можуть пов'язати різні профілі між собою. Б2.У5. Підтримувати окреме дослідницьке середовище без змішування з особистою цифровою активністю.		
	Б3. Здатність застосовувати принципи цифрової гігієни в OSINT.	Б3.З1. Основи цифрової гігієни в OSINT. Б3.З2. Принципи створення стійких та унікальних паролів. Б3.З3. Засоби безпечного зберігання паролів. Б3.З4. Основи фішингових атак, соціальної інженерії та базові правила їх виявлення. Б3.З5. Безпечне використання електронної пошти, мобільних застосунків, месенджерів і платіжних сервісів. Б3.З6. Принципи оновлення програмного забезпечення, контролю дозволів застосунків і захисту мобільних пристроїв. Б3.З7. Базові вимоги до безпечного використання метаданих, документів, фотографій, відео та цифрових платежів.	Б3.У1. Створювати унікальні складні паролі та організовувати їх безпечне зберігання. Б3.У2. Використовувати менеджери паролів і багатофакторну автентифікацію. Б3.У3. Розпізнавати фішингові повідомлення, діпфейки підозрілі посилання, вкладення та спроби соціальної інженерії. Б3.У4. Забезпечувати OPSEC робочого місця. Б3.У5. Контролювати дозволи мобільних застосунків, рекламні ідентифікатори, доступ до геолокації та інші чутливі параметри. Б3.У6. Перевіряти та очищати файли від метаданих перед передаванням. Б3.У7. Організовувати безпечне використання анонімізованих засобів електронних комунікацій, платіжних сервісів та інших інструментів.	Б3.К1. Інформувати керівника та інших співробітників підрозділу про виявлені інциденти, фішингові загрози та порушення режиму безпеки.	Б3.В1. Дотримуватися правил цифрової гігієни у OSINT. Б3.В2. Нести відповідальність за захист доступу до власних облікових записів, пристроїв і дослідницьких матеріалів. Б3.В3. Постійно забезпечувати OPSEC робочого місця.

	Б.4 Здатність підтримувати психічну стійкість під час роботи з травматичним контентом	Б4.З1. Наслідки тривалої роботи з травматичним контентом (насильство, загибель людей, катастрофи); поняття вторинної травматизації та вигорання. Б4.З2. Превентивні заходи та методи самодопомоги при роботі з травматичним контентом. Б4.З3. Порядок та умови звернення по психологічну підтримку в межах організації та/або до профільних фахівців.	Б4.У1. Розпізнавати ознаки вторинної травматизації та професійного вигорання у власній діяльності. Б4.У2. Застосовувати превентивні заходи та базові техніки самодопомоги для зниження психоемоційної напруги. Б4.У3. Дотримуватися встановлених в організації регламентів безпечної роботи з травматичним контентом (часові обмеження, ротація, правила перегляду).	Б4.К1. Інформувати керівника або уповноважену особу про необхідність отримання психологічної підтримки.	Б4.В1. Дотримуватися безпечних режимів роботи з травматичним контентом та застосовувати методи самодопомоги.
В. Організація дослідження	В1. Здатність до розуміння, операціоналізації завдання.	В1.З1. Етапи OSINT. В1.З2. Методи визначення інформаційної потреби. В1.З3. Методи формулювання дослідницьких завдань. В1.З4. Принципи визначення пріоритетності інформації.	В1.У1. Визначати інформаційну потребу та формулювати завдання дослідження. В1.У2. Трансформувати інформаційну потребу замовника у конкретні вимірювані індикатори та ознаки (операціоналізація).	В1.К1. Узгоджувати завдання та очікувані результати дослідження із замовником. В1.К2. Обговорювати завдання зі співвиконавцями.	В1.В1. Нести відповідальність за точність інтерпретації завдання та повноту визначених інформаційних потреб.
	В2. Здатність планувати дослідження.	В2.З1. Методи пошуку інформації у відкритих джерелах. В2.З2. Типологія відкритих джерел інформації. В2.З3. Принципи використання первинних і вторинних джерел інформації. В2.З4. Принципи розподілу та оптимізації наявних сил та засобів для виконання плану проведення дослідження.	В2.У1. Розробляти план проведення дослідження. В2.У2. Визначати необхідні ресурси для проведення дослідження. В2.У3. Визначати оптимальні джерела інформації для дослідження. В2.У4. Обирати інструменти та методи збору інформації.	В2.К1. Узгоджувати методологію збирання інформації з командою. В2.К2. Обговорювати план проведення дослідження зі співвиконавцями.	В2.В1. Самостійно планувати проведення дослідження. В2.В2. Нести відповідальність за ефективність обраної методології.

	В3. Здатність управляти ризиками.	В3.З1. Основи управління ризиками в інформаційно-аналітичній діяльності. В3.З2. Методи управління ризиками під час збору відомостей.	В3.У1. Ідентифікувати та оцінювати ризики, пов'язані зі здійсненням OSINT. В3.У2. Планувати та здійснювати заходи щодо мінімізації ризиків під час збору відомостей.	В3.К1. Інформувати співвиконавців про потенційні ризики збору відомостей.	В3.В1. Нести відповідальність за мінімізацію ризиків під час збору відомостей.
Г. Збирання інформації та зберігання відомостей з відкритих джерел	Г1. Здатність до розширеного пошуку інформації та збору відомостей з різнотипових джерел.	Г1.З1. Пошукові системи, оператори розширеного пошуку, принципи індексації та архівації. Г1.З2. Відкриті державні реєстри, агрегатори та бази даних, комерційні інструменти та OSINT-комбайни. Г1.З3 Принципи роботи публічних блокчейнів та відкритих інструментів блокчейн-аналітики.	Г1.У1. Здійснювати пошук з використанням складних операторів та булевої логіки. Г1.У2. Працювати з реєстрами, архіваторами вебконтенту та кешованими копіями сторінок. Г1.У3. Проводити дослідження з використанням вебсторінок, що не індексуються пошуковими системами. Г1.У4. Ідентифікувати криптовалютні гаманці та відстежувати транзакції через відкриті сервіси (crypto tracing).	Г1.К1. Взаємодіяти з технічними фахівцями щодо налаштування інструментів автоматизації збору та зберігання інформації. Г1.К2. Взаємодіяти зі співвиконавцями.	Г1.В1. Самостійно виконувати план проведення дослідження у частині збирання інформації. Г1.В2. Нести відповідальність за повноту та коректність зібраної інформації та збережених відомостей.
	Г2. Здатність збирати відомості у соціальних мережах (медіа), месенджерах та інших платформах соціально-віртуальної взаємодії.	Г2.З1. Архітектура та алгоритми соціальних мереж (медіа), платформ і месенджерів. Г2.З2. Специфіка збирання відомостей з соціальних мереж (медіа), платформ і месенджерів.	Г2.У1. Збирати із соцмереж (медіа), месенджерів та інших платформ соціально-віртуальної взаємодії, фіксувати відомості про об'єкт дослідження, його зв'язки та пов'язаний контент. Г2.У2. Проводити моніторинг активності об'єкта дослідження у месенджерах без прямої взаємодії.	Г2.К1. Взаємодіяти зі співвиконавцями.	Г2.В1. Самостійно збирати відомості відповідно до плану. Г2.В2. Нести відповідальність за повноту та коректність фіксації зібраних даних.

	Г3. Здатність збирати, обробляти та інтерпретувати видові та геопросторові дані з відкритих джерел.	Г3.З1. Принципи геолокації, верифікації та хронолокації зображень, відео тощо. Г3.З2. Картографічні сервіси та геоінформаційні системи. Г3.З3 Відкриті агрегатори даних про переміщення морських суден (AIS) та повітряних суден (ADS-B) як джерела геопросторової інформації; принципи їх використання в OSINT-дослідженнях. Г3.З4. Порядок доступу до джерел отримання поточних і архівних даних космічних систем дистанційного зондування Землі, у тому числі оптичних та радарних (SAR) знімків з відкритих джерел. Г3.З5. Основи створення, редагування, візуалізації та опрацювання даних геопросторових систем.	Г3.У1. Визначати геолокацію об'єктів дослідження за інформацією з відкритих джерел. Г3.У2. Інтерпретувати картографічні дані та визначати часові параметри за тінню/сонцем. Г3.У3. Здійснювати відстеження переміщень морських та повітряних суден через відкриті AIS/ADS-B агрегатори та фіксувати отримані дані для подальшого аналізу.	Г3.К1. Співпрацювати з аналітиками суміжних напрямів (за потреби).	Г3.В1. Нести відповідальність за релевантність й коректність інтерпретації видових та геопросторових даних.
	Г4. Здатність до моніторингу сегментів інфопростору.	Г4.З1. Методологія моніторингу (постійний, ситуативний, тематичний). Г4.З2. Платформи та інструменти моніторингу.	Г4.У1. Визначати об'єкти, джерела та параметри моніторингу. Г4.У2. Налаштовувати системи автоматизованого моніторингу (алерти, RSS, панелі моніторингу тощо). Г4.У3. Здійснювати моніторинг у режимі реального часу та ретроспективний пошук.	Г4.К1. Комунікувати із замовниками щодо уточнення об'єктів та пріоритетів моніторингу. Г4.К2. Узгоджувати розподіл складових моніторингу зі співвиконавцями.	Г4.В1. Самостійно організовувати моніторинг сегментів інфопростору. Г4.В2. Нести відповідальність за повноту та коректність фіксації зібраних відомостей.

Д. Автоматизація збирання відомостей	Д1. Здатність автоматизувати збирання відомостей з відкритих джерел	Д1.З1. Спеціалізовані OSINT-інструменти. Д1.З2. Основи написання скриптів та взаємодії з Інтерфейсом програмування застосунків (API) для автоматизації збирання, принципи обробки машиночитаних форматів. Д1.З3. Формулювання та оптимізація запитів до генеративних систем штучного інтелекту (Prompt Engineering).	Д1.У1. Налаштовувати та використовувати спеціалізовані OSINT-інструменти. Д1.У2. Автоматизувати процеси збирання відомостей за допомогою скриптів та API. Д1.У3. Формулювати та оптимізовувати запити до генеративних систем ШІ з метою уточнення критеріїв пошуку та автоматизованого збирання відомостей здійснювати оцінку отриманих результатів.	Д1.К1. Обмінюватися з колегами інформацією про нові інструменти та алгоритми збирання відомостей.	Д1.В1. Самостійно обирати інструменти збирання, виходячи з технічних обмежень джерел. Д1.В2. Нести відповідальність за коректність та релевантність відомостей зібраних автоматизованим способом.
Е. Технічна обробка зібраних відомостей	Е1. Здатність до технічної нормалізації та трансформації даних.	Е1.З1. Методи очищення та конвертації форматів файлів. Е1.З2. Можливості сервісів машинного перекладу.	Е1.У1. Проводити попередню обробку, видалення дублікатів та нерелевантних даних. Е1.У2. Здійснювати переклад масивів даних із застосуванням глосаріїв для збереження сенсу.	Е1.К1. Узгоджувати вимоги до якості та форматів даних з колегами.	Е1.В1. Нести відповідальність за точність збереження змісту при зміні формату даних.
	Е2. Здатність до структурної організації та систематизації масивів даних.	Е2.З1. Принципи побудови логічних схем (таксономій) та систем тегування для класифікації інформації. Е2.З2. Інструменти управління базами знань. Е2.З3. Методи забезпечення цілісності цифрових даних.	Е2.У1. Створювати та підтримувати тематичні довідники, картотеки та бази знань. Е2.У2. Визначати оптимальний спосіб структурування даних (лінійний, ієрархічний або мережевий/графовий). Е2.У3. Організовувати зберігання зібраних даних.	Е2.К1. Узгоджувати єдині підходи до іменування файлів та структурування папок. Е2.К2. Забезпечувати зрозумілість структури збережених даних для колег.	Е2.В1. Нести відповідальність за цілісність, впорядкованість і доступність накопичених масивів даних.

Є. Аналітичне опрацювання даних та оцінювання джерел	Є1. Здатність оцінювати відкриті джерела та отриману з них інформацію.	Є1.З1. Принципи оцінювання джерел інформації. Є1.З2. Критерії визначення надійності джерел інформації. Є1.З3. Критерії оцінювання достовірності інформації. Є1.З4. Шкала оцінювання надійності джерел та достовірності інформації (A–F / 1–6). Є1.З5. Технології створення дезінформації, deepfake, синтетичних медіа. Є1.З6. Принципи документування та періодичного перегляду оцінок джерел.	Є1.У1. Аналізувати технічні характеристики, походження та контент джерела інформації. Є1.У2. Оцінювати надійність джерел інформації. Є1.У3. Оцінювати достовірність та актуальність отриманої інформації. Є1.У4. Виявляти маніпулятивний та згенерований ШІ контент, фейкові акаунти, бот-мережі. Є1.У5. Здійснювати періодичний перегляд оцінки джерел з урахуванням змін у їх надійності та змісті інформації.	Є1.К1. Обговорювати результати оцінювання джерел та інформації зі співвиконавцями. Є1.К2. Інформувати керівництво або замовника про рівень надійності джерел та достовірності інформації.	Є1.В1. Самостійно здійснювати оцінювання джерел та інформації. Є1.В2. Нести відповідальність за обґрунтованість визначення рівня надійності джерел та достовірності інформації. Є1.В3. Забезпечувати регулярний перегляд та актуалізацію оцінок джерел.
	Є2. Здатність до аналізу та верифікації інформації.	Є2.З1. Методи кількісного аналізу інформації. Є2.З2. Методи якісного аналізу інформації. Є2.З3. Методи верифікації та валідації інформації. Є2.З4. Принципи порівняльного аналізу часових серій геопросторових даних (супутникових знімків, даних дистанційного зондування Землі) для виявлення змін об'єктів.	Є2.У1. Аналізувати та узагальнювати інформацію. Є2.У2. Встановлювати взаємозв'язки окремих елементів даних та виявляти розбіжності між ними. Є2.У3. Перевіряти автентичність інформації. Є2.У4. Перевіряти інформацію через альтернативні відкриті джерела.	Є2.К1. Обговорювати результати аналізу зі співвиконавцями. Є2.К2. Аргументувати результати аналізу замовнику.	Є2.В1. Самостійно формувати аналітичні висновки. Є2.В2. Нести відповідальність за релевантність, обґрунтованість та неупередженість результатів аналізу.

	Є3. Здатність виявляти інформаційні закономірності.	Є3.З1. Методи аналізу даних для виявлення закономірностей (статистичні, кореляційні, трендові). Є3.З2. Структуровані аналітичні методики. Є3.З3. Когнітивні упередження та методи їх подолання.	Є3.У1. Конструювати аналітичні моделі взаємозв'язків між елементами даних (зокрема графові). Є3.У2. Виявляти тренди та закономірності у масивах даних. Є3.У3. Застосовувати структуровані аналітичні методики для перевірки гіпотез та інтерпретації даних. Є3.У4. Проводити комплексний аналіз зовнішнього контексту та екосистеми об'єкта дослідження.	Є3.К1. Обґрунтовувати використання конкретних методів виявлення закономірностей. Є3.К2. Взаємодіяти зі співвиконавцями для узгодження робочих гіпотез.	Є2.В2. Нести відповідальність за релевантність, обґрунтованість та неупередженість результатів аналізу. Є3.В1. Самостійно здійснювати аналіз закономірностей.
	Є4. Здатність застосовувати системи штучного інтелекту як аналітичний інструмент.	Є4.З1. Принципи роботи генеративних систем ШІ та їхні обмеження: схильність до генерації недостовірного контенту (галюцинації), модельні упередження, відсічення знань за датою. Є4.З2. Ризики передачі конфіденційних та службових даних до зовнішніх систем ШІ; засади безпечної роботи з такими системами. Є4.З3. Відмінність між застосуванням систем ШІ для збирання відомостей та їх застосуванням як аналітичного інструменту для узагальнення, класифікації та структурування даних.	Є4.У1. Критично оцінювати результати, отримані із застосуванням систем ШІ, та верифікувати їх з незалежних джерел. Є4.У2. Документувати факт і параметри використання систем ШІ при підготовці аналітичного продукту відповідно до вимог внутрішніх процедур. Є4.У3. Дотримуватися вимог інформаційної безпеки при передачі даних до систем ШІ, зокрема уникати передачі конфіденційної та службової інформації до публічних зовнішніх сервісів.	Є4.К1. Зазначати в аналітичному продукті факт та параметри застосування систем ШІ у разі, якщо це вимагається внутрішніми процедурами або замовником.	Є4.В1. Нести відповідальність за достовірність аналітичних висновків незалежно від того, чи були вони підготовлені із застосуванням систем ШІ. Є4.В2. Самостійно приймати рішення щодо доцільності та меж застосування систем ШІ з урахуванням чутливості оброблюваних даних та вимог до якості аналітичного продукту.

Ж. Підготовка інформаційно-аналітичних документів, візуалізація та збереження результатів дослідження	Ж1. Здатність готувати структуровані результати дослідження	Ж1.З1. Принципи підготовки інформаційно-аналітичних документів. Ж1.З2. Форми представлення результатів дослідження. Ж1.З3. Принципи структурованого викладення інформації.	Ж1.У1. Узагальнювати результати дослідження. Ж1.У2. Формувати аналітичні висновки, оцінки та пропозиції. Ж1.У3. Викладати інформацію у логічній та структурованій формі. Ж1.У4. Редагувати та перевіряти інформаційно-аналітичні документи.	Ж1.К1. Обговорювати результати дослідження зі співвиконавцями.	Ж1.В1. Самостійно готувати інформаційно-аналітичні документи. Ж1.В2. Нести відповідальність за якість результатів дослідження.
	Ж2. Здатність здійснювати візуалізацію та презентації результатів дослідження.	Ж2.З1. Способи візуалізації результатів дослідження. Ж2.З2. Основні типи аналітичних візуалізацій (графи зв'язків, часові шкали, карти, діаграми, схеми). Ж2.З3. Методи візуалізації зв'язків. Ж2.З4. Інструменти візуалізації.	Ж2.У1. Структурувати інформацію для подальшої візуалізації. Ж2.У2. Створювати візуальні моделі зв'язків між об'єктами дослідження. Ж2.У3. Формувати графічні матеріали (карти, схеми, діаграми, часові лінії) для презентації результатів дослідження. Ж2.У4. Інтегрувати візуальні матеріали до результатів дослідження.	Ж2.К1. Пояснювати результати дослідження за допомогою візуальних матеріалів. Ж2.К2. Узгоджувати формат презентації та візуалізацій із співвиконавцями або замовником.	Ж2.В1. Самостійно обирати способи презентації та візуалізації результатів дослідження. Ж2.В2. Нести відповідальність за точність та коректність візуалізації інформації.
	Ж3. Здатність забезпечувати цілісність та відтворюваність результату дослідження.	Ж3.З1. Методи фіксації інформації для запобігання втраті даних та забезпечення їхньої доступності офлайн. Ж3.З2. Формати та стандарти довгострокового зберігання результатів досліджень та супутніх матеріалів. Ж3.З3. Методи маркування та класифікації результатів досліджень за ступенем важливості та терміном актуальності.	Ж3.У1. Створювати локальні та хмарні копії матеріалів, що підтверджують отримані результати. Ж3.У2. Забезпечувати архівування результатів з дотриманням вимог конфіденційності. Ж3.У3. Систематизувати підтверджуючі матеріали для забезпечення їхньої швидкої перевірки. Ж3.У4. Забезпечувати захист результатів дослідження від несанкціонованої зміни або випадкового видалення.	Ж3.К1. Інформувати колег про наявність та місце зберігання підтверджуючих матеріалів. Ж3.К2. Звітувати про повноту та надійність збереженого масиву результатів досліджень.	Ж3.В1. Нести відповідальність за збереження копій матеріалів дослідження.

З. Доведення результату дослідження	З1. Здатність доводити результат дослідження замовнику.	З1.З1. Порядок доведення результату дослідження. З1.З2. Принцип "need-to-know". З1.З3. Методи захисту чутливих джерел інформації.	З1.У1. Передавати результат дослідження замовнику у встановленому порядку. З1.У2. Документувати факт доведення результатів дослідження замовнику. З1.У3. Забезпечувати захист чутливих джерел інформації.	З1.К1. Представляти результат дослідження замовнику.	З1.В1. Самостійно здійснювати доведення результатів дослідження. З1.В2. Нести відповідальність за дотримання порядку доведення результатів дослідження.
И. Оцінювання результатів роботи	И1. Здатність управляти зворотним зв'язком.	И1.З1. Методологія збору та аналізу відгуків щодо якості та корисності результатів дослідження. И1.З2. Критерії оцінювання цінності та впливу результатів дослідження на прийняття рішень. И1.З3. Методи самоаналізу для вдосконалення майбутніх досліджень.	И1.У1. Налагоджувати та підтримувати зворотній зв'язок із замовником. И1.У2. Визначати прогалини в дослідженні та планувати заходи з їх усунення. И1.У3. Формулювати рекомендації щодо вдосконалення методології дослідження.	И1.К1. Комунікувати із замовником щодо задоволення його інформаційних потреб. И1.К2. З'ясовувати нові інформаційні потреби, що виникають внаслідок доведення результату дослідження.	И1.В1. Нести відповідальність за системну інтеграцію зворотного зв'язку в OSINT. И1.В2. Визначати напрями для самовдосконалення та корекції власної діяльності.
І. Підвищення кваліфікації	І1. Здатність до самоосвіти.	І1.З1. Актуальні тенденції розвитку OSINT. І1.З2. Нові підходи, методи та інструменти OSINT.	І1.У1. Самостійно вивчати та апробувати нові підходи, методи та інструменти OSINT. І1.У2. Аналізувати зміни у правилах та політиках платформ та ресурсів.	І1.К1. Формулювати запити до експертного середовища щодо актуальних тенденцій розвитку, нових методів та інструментів OSINT. І1.К2. Брати участь у розробках, а також самостійно розробляти та апробовувати нові методи і підходи до проведення OSINT.	І1.В1. Самостійно планувати та реалізовувати програму власного професійного розвитку. І1.В2. Самостійно розробляти й апробовувати нові підходи, методи та інструменти OSINT.
	І2. Здатність до опанування навчальних програм підвищення кваліфікації.	І2.З1. Програми підвищення кваліфікації. І2.З2. Стандарти та вимоги до кваліфікації OSINT-аналітиків.	І2.У1. Проходити навчальні курси та сертифікаційні випробування. І2.У2. Систематизувати отримані знання для впровадження у робочі процеси.	І2.К1. Брати участь у професійних спільнотах, наукових форумах та інших заходах професійного спрямування.	І2.В1. Нести відповідальність за актуальність власних компетентностей та їх відповідність чинним стандартам.

Ї. Менторська підтримка	Ї1. Здатність передавати знання та досвід колегам.	Ї1.З1. Основи методології навчання дорослих (андрагогіки). Ї1.З2. Методи та інструменти навчання. Ї1.З3. Сучасні інструменти та методи OSINT. Ї1.З4. Підходи до оцінювання професійних компетентностей. Ї1.З5. Методи виявлення ознак вторинної травматизації та вигорання у колег; підходи до організації психологічно безпечного середовища роботи з травматичним контентом.	Ї1.У1. Розробляти навчальні матеріали з OSINT. Ї1.У2. Проводити навчальні заходи. Ї1.У3. Оцінювати рівень знань молодших колег, визначати прогалини. Ї1.У4. Формувати індивідуальні траєкторії розвитку молодших колег, надавати відповідні рекомендації. Ї1.У5. Виявляти ознаки вторинної травматизації у колег та скеровувати їх до відповідних заходів підтримки; сприяти формуванню психологічно безпечного робочого середовища.	Ї1.К1. Встановлювати ефективний діалог з менш досвідченими колегами. Ї1.К2. Доступно пояснювати принципи та методи OSINT. Ї1.К3. Надавати конструктивний зворотний зв'язок щодо результатів навчання. Ї1.К4. Обмінюватися досвідом з іншими менторами (інструкторами).	Ї1.В1. Самостійно планувати та проводити навчальні заходи. Ї1.В2. Нести відповідальність за якість проведених навчальних заходів. Ї1.В3. Сприяти розвитку професійних компетентностей колег. Ї1.В4. Бути прикладом професійної поведінки. Ї1.В5. Виявляти ініціативу у впровадженні нових освітніх практик.

Предмети і засоби праці (обладнання, устаткування, матеріали, інструменти)

Робоче місце, укомплектоване необхідними офісними меблями й технікою, програмним забезпеченням, доступом до мережі Інтернет, інформаційно-довідкових систем, баз даних, сервісів тощо; нормативно-правові акти та внутрішні документи роботодавця, що регламентують діяльність OSINT-аналітика.

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

Трудова функція (умовне позначення)	Загальна назва професійної кваліфікації в межах професійного стандарту: OSINT-аналітик		
	OSINT-аналітик	Старший OSINT-аналітик	Провідний OSINT-аналітик
	повна	повна	повна
А. Забезпечення правомірності та етичності OSINT	+	+	+
Б. Забезпечення операційної безпеки (OPSEC)	+	+	+
В. Організація дослідження	+	+	+
Г. Збирання інформації та зберігання відомостей з відкритих джерел	+	+	+
Д. Автоматизація збирання відомостей	-	+	+
Е. Технічна обробка зібраних відомостей	+	+	+
Є. Аналітичне опрацювання даних та оцінювання джерел	+	+	+
Ж. Підготовка інформаційно-аналітичних документів, візуалізація та збереження результатів дослідження	+	+	+
З. Доведення результату дослідження	+	+	+
И. Оцінювання результатів роботи	-	+	+
І. Підвищення кваліфікації	+	+	+
Ї. Менторська підтримка	-	-	+

7. Відомості про розроблення та затвердження професійного стандарту

1) повне найменування розробника професійного стандарту

Національна академія Служби безпеки України.

склад робочої групи:

1. Євген МЕЛЕНТІ, Служба безпеки України;
2. Валерій ШЕСТАКОВ, Служба безпеки України;
3. Дмитро РИБКА, Служба безпеки України;
4. Ірина ЖЕВЕЛЄВА, Служба безпеки України;
5. Юлія АНДРУСИШИН, Служба безпеки України;
6. Борис ІГНАТЬЄВ, Служба безпеки України;
7. Олександр КЕДА, Служба безпеки України;
8. Людмила КУЛЬЧИЦЬКА, Служба безпеки України;
9. Олександр ЛІСОВ, Служба безпеки України;
10. Олександр ЛИЩУК, Служба безпеки України;
11. Михайло ЛУК'ЯНЕНКО, Служба безпеки України;
12. Станіслав ЛУК'ЯНЕНКО, Служба безпеки України;
13. Сергій МАРЮК, Служба безпеки України;

14. Костянтин ПОЛІЩУК, Служба безпеки України;
15. Віталій ХОДАНОВИЧ, Служба безпеки України;
16. Роман ШИРШОВ, Служба безпеки України;
17. Олександр ЮДІН, Служба безпеки України;
18. Наталія ЮРХ, Служба безпеки України;
19. Володимир ШАТІЛОВ, Об'єднаний комітет профспілки Служби безпеки України
20. Максим КОРОБЧИНСЬКИЙ, Воєнна академія імені Євгенія Березняка;
21. Михайло РУДЕНКО, Воєнна академія імені Євгенія Березняка;
22. Олександр ЛАВРУК, військова частина А0485;
23. Віталій ПОЛЯКОВ, військова частина А0485;
24. Кирило ВІКТОРОВ, РНБО;
25. Сергій ДЕМЯНКО, РНБО;
26. Василь СЛИЧКО, РНБО;
27. Микола ПАШКОВСКИЙ, Національна академія правових наук України;
28. Богдан КОСОХАТЬКО, ГО «Трус Хаундс».

2) назва та реквізити документа, яким затверджено професійний стандарт

Наказ Національної академії Служби безпеки України від 16.06.26 року № 83.

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 9.06.2026. (рішення № 20, протокол 37 (301) від 9.06.2026) про дотримання під час підготовки проєкту професійного стандарту «Аналітик інформації з відкритих джерел (OSINT-аналітик)» вимог Порядку розроблення, введення в дію та перегляду професійних стандартів, затвердженого постановою Кабінету Міністрів України від 31.05.2017 № 373).

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

Висновок Професійної спілки працівників державних установ України щодо погодження професійного стандарту «Аналітик інформації з відкритих джерел (OSINT-аналітик)» від 03.06.2026 № 83.

8. Рекомендована дата перегляду професійного стандарту

червень 2031 року

Голова робочої групи -
Перший проректор (з навчальної роботи)
Національної академії
Служби безпеки України **Євген МЕЛЕНТІ**