Прим. № __

ЗАТВЕРДЖЕНО

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

ПРОФЕСІЙНИЙ СТАНДАРТ

АНАЛІТИК З ОЦІНКИ ВРАЗЛИВОСТЕЙ

_____

(дата внесення до Реєстру кваліфікацій)

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

висновку суб’єкта перевірки – Національного агентства кваліфікацій від 27 грудня 2023 року про дотримання під час підготовки проєкту професійного стандарту «Аналітик з оцінки вразливостей» вимог Порядку розроблення, введення в дію та перегляду професійних стандартів, затвердженого постановою Кабінету Міністрів України від 31.05.2017 р. № 373;

висновку щодо погодження проєкту професійного стандарту «Аналітик з оцінки вразливостей» Профспілкою працівників зв’язку України (лист від 16.11.2023 р. № 01.2-14/136, постанова Президії Профспілки працівників зв’язку України від 16.11.2023 р. № П-4-5г).

I. Назва професійного стандарту

Аналітик з оцінки вразливостей.

II. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Виконання дій з організації та проведення аналітичної діяльності виявлення та оцінки вразливостей у сфері кібербезпеки та захисту інформації в інформаційних системах та мережах (або автоматизованих системах, інформаційно-комунікаційних системах, системах електронних комунікацій) в організаціях, підприємствах або установах різних форм власності.

Розробка, впровадження та виконання вимірювань ефективності ешелонованого захисту інформаційної системи та її ресурсів щодо відомих вразливостей, кібератак на основі процедур тестування або тестування на проникнення, реалізація сценаріїв атак для оцінки ефективності впроваджених та запланованих заходів кібербезпеки.

Виявлення вразливостей в технічних та організаційних контролях, що впливають на конфіденційність, цілісність та доступність продуктів інформаційних технологій (наприклад, систем, обладнання, програмного забезпечення та послуг).

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	Назва секції	№ розділу	Назва розділу	№ групи (класу)	Назва групи (класу)
Секція J	Інформація та телекомунікації	**Розділ 61**	Телекомунікації (електрозв'язок)	**Група 61.1**	Діяльність у сфері проводового електрозв'язку
				Клас 61.10	
				Група 61.2	Діяльність у сфері безпроводового електрозв'язку
				Клас 61.20	
				Група 61.9	Інша діяльність у сфері електрозв'язку
				Клас 61.90	
		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 62.01	Комп'ютерне програмування

				Клас 62.02	Консультування з питань інформатизації
				Клас 62.03	Діяльність із керування комп'ютерним устаткуванням
				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
				Клас 63.12	Веб-портали
Секція M	Професійна, наукова та технічна діяльність	**Розділ 74**	Інша професійна, наукова та технічна діяльність	**Група 74.9**	Інша професійна, наукова та технічна діяльність, н.в.і.у.
				Клас 74.90	

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

Аналітик з оцінки вразливостей 2139.2.

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

Аналітик з оцінки вразливостей, 7 рівень НРК.

Провідний аналітик з оцінки вразливостей, 7 рівень НРК.

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

● документ (диплом, сертифікат, тощо), виданий суб’єктом, уповноваженим законодавством на присвоєння/підтвердження та визнання професійної або часткової професійної кваліфікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання

завдань у відповідності до професійного стандарту «Аналітик з оцінки вразливостей»;

● документ (диплом, сертифікат, тощо), виданий суб'єктом, уповноваженим законодавством на присвоєння/підтвердження та визнання професійної або часткової професійної кваліфікації (щодо професійних кваліфікацій, здобутих у інших країнах).

ІІІ. Здобуття професійної кваліфікації та професійний розвиток

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

Назва професійної та/або часткової професійної кваліфікації	**Суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
Аналітик з оцінки вразливостей	Підготовка за спеціальностями, вказаними у **П.*** на другому (магістерському) рівні вищої освіти за умови наявності стажу роботи за однією з професій відповідного спрямування не менше 3 років.	*Не передбачено професійним стандартом*
Провідний аналітик з оцінки вразливостей	Підготовка за спеціальностями, вказаними у **П.*** на другому (магістерському) рівні вищої освіти за умови наявності стажу роботи за однією з професій відповідного спрямування не менше 5 років.	*Не передбачено професійним стандартом*

П.*

● 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);

- 254 “Забезпечення військ (сил)” галузі знань 25 “Воєнні науки, національна безпека, безпека державного кордону” (7 рівень НРК);

- 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» (7 рівень НРК).

2. Професійний розвиток

1) з присвоєнням наступної професійної кваліфікації

Назва професійної та/або часткової професійної кваліфікації	**Суб’єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій**	
	Кваліфікаційні центри	**Суб’єкти освітньої діяльності**
Аналітик з оцінки вразливостей	Підвищення кваліфікації «Аналітик з оцінки вразливостей» для отримання професійної кваліфікації «Провідний аналітик з оцінки вразливостей». Стаж роботи за спеціальністю не менше 5 років.	*Не передбачено професійним стандартом*

2) без присвоєння наступної професійної кваліфікації

Підвищення кваліфікації може здійснюватися шляхом неформальної (тренінги, семінари, семінари-практикуми, вебінар, майстер-класи тощо) та інформальної освіти для вдосконалення (підтримання) професійної кваліфікації, в тому числі шляхом набуття нових/додаткових навичок/компетентностей.

Підтвердження наявної та підвищення професійної кваліфікації може бути передбачено відповідними відомчими нормативно-правовими актами та внутрішніми документами підприємств, установ та організацій.

IV. Абревіатури, скорочення

TCP	Transmission Control Protocol
IP	Internet Protocol
OSI	Open Systems Interconnection
ITIL	Information Technology Infrastructure Library
PL/SQL	Procedural Language / Structured Query Language

TCP/IP	Transmission Control Protocol / Internet Protocol
DNS	Domain Name System
EBSCO	Elton Bryson Stephens Company
JSTOR	Journal Storage
TSCM	Technical Security Counter Measures
АС	Автоматизована система
ІКС	Інформаційно-комунікаційна система
СЕК	Система електронних комунікацій
ІС	Інформаційна система
ІТ	Інформаційні технології

V. Опис трудових функцій

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
А. Організація аналітичної діяльності виявлення та оцінки вразливостей у сфері кібербезпеки та захисту інформаційних систем та мереж (або АС, ІКС, СЕК) в організаціях, підприємствах або установах різних форм власності.	**А1**. Здатність здійснювати аналітичну діяльність у сфері кібербезпеки та захисту інформаційних систем та мереж (або АС, ІКС, СЕК) на базі нормативно-правового та організаційно технічного забезпечення.	**А1.З1.** Законодавчу та нормативно-правову базу, стандарти, нормативні документи та етичні норми, пов'язані з кібербезпекою та захистом інформації в ІС та її інформаційних ресурсів. **А1.З2.** Концепції та/або програми, заходи організації та впровадження процедури аналітичної діяльності з виявлення та аналізу вразливостей в інформаційних системах та/або мереж, а також методології, методи та засоби забезпечення мережевої безпеки. **А1.З3.** Стратегію, місію, політики та задачі системи менеджменту інформаційної безпеки та/або кіберзахисту ІС та її інформаційних ресурсів.	**А1.У1.** Визначати необхідний рівень складності процедури аналітичної діяльності з виявлення та аналізу вразливостей в інформаційних системах та/або мережах згідно встановлених задач. **А1.У2.** Розробляти та реалізовувати Плани підготовки щодо проведення заходів з організації та впровадження процедури аналітичної діяльності з виявлення та аналізу вразливостей, а також процедур тестування та/або тестування на проникнення у ІС державних органів, на підприємствах, в організаціях різних форм власності. **А1.У3.** Проводити аналіз структури та топології	**А1.К1.** Взаємодіяти з керівництвом, персоналом організації та партнерами стосовно заходів організації аналітичної діяльності з виявлення та оцінки вразливостей у сфері кібербезпеки та захисту інформації. **А1.К2.** Інформувати керівництво та власника ресурсів щодо необхідного рівня складності процедури аналітичної діяльності з виявлення та аналізу вразливостей.	**А1.В1.** Готувати звіти та іншу інформацію про необхідний рівень складності та напрями процедури аналітичної діяльності з виявлення та аналізу вразливостей.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		А1.З4. Формальні моделі безпеки: тріада кібербезпеки CIA (конфіденційність, цілісність, доступність), гексада Паркера, модель Бела-ЛаПадули (мандатного доступу), модель Біби (забезпечення цілісності даних), модель Кларка-Вілсона. **А1.З5.** Корпоративну архітектуру інформаційної безпеки та кіберзахисту ІС та мереж (АС, ІКС, СЕК) **А1.З6.** Вимоги до організації та проведення процедур тестування та/або тестування на проникнення, а також впровадження аналітичної діяльності з виявлення та аналізу вразливостей. **А1.З7.** Обладнання та функції апаратного, програмно-апаратного та програмного забезпечення інформаційної безпеки та	інформаційних системи та/або мереж, а також використовувати методології та методи забезпечення мережевої безпеки з метою встановлення напрямів та методів тестування та аналізу вразливостей ІС організації. **А1.У4.** Проводити аналіз апаратних та програмно-апаратних засобів, спеціального програмного забезпечення з метою організації та впровадження процедури аналітичної діяльності з виявлення та аналізу вразливостей інформаційних ресурсів системи та/або мереж. **А1.У5.** Встановлювати напрями, методи та інструменти тестування та/або тестування на проникнення до ІС та її ресурсів з метою		

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		кіберзахисту ІС та/або мереж організації. **А1.З8.** Концепції, методи та процедури адміністрування та захисту ІС та її активів з урахуванням операційних та/або технологічних процесів системи. **А1.З9.** Стандарти безпеки персональних даних (PII) та платіжних систем (PCI). **А1.З10.** Використовувані в організації програми класифікації інформації і процедур розкриття.	виявлення та фіксування вразливостей.		
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				
Б. Впровадження сучасних інформаційних технологій та теоретичних засад в процесі організації	**Б1.** Здатність використовувати інформаційні технології та теоретичних засадах з метою розробки	**Б1.З1.** Інтерпретовані, об'єктно-орієнтовані, предметно-орієнтовані, мови скриптів та компільовані мови програмування (Java, Java	**Б1.У1.** Розробляти та використовувати програмне забезпечення різних типів з метою реалізації в подальшому процедур аналітичної	**Б1.К1.** Взаємодіяти з керівництвом та відповідним персоналом з питань використання інформаційних	**Б1.В1.** Готувати інформацію, доповіді, презентації з напряму використання

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
аналітичної діяльності з виявлення та оцінки вразливостей у сфері кібербезпеки та захисту інформаційних систем та мереж.	сучасних систем кібербезпеки та захисту інформації, а також організації та проведення процедур аналізу вразливостей ІС (або АС, ІКС, СЕК) та їх інформаційних ресурсів.	Script, C ++, PHP, Python, Objective-C). **Б1.32.** Концепції та моделі побудови ІС OSI/ISO, а також типи і принципи використання протоколів обміну даними, такі як TCP/IP, методи динамічного конфігурування вузлів, методи формування різних класів скриптів, системи доменних імен (DNS) і послуг, що надаються Службою каталогів. **Б1.33.** Операційні системи різних типів (ОС Microsoft Windows, Unix/Linux, ОС Soláris). **Б1.34.** Методи та моделі статистичного аналізу даних та прийняття рішень. **Б1.35.** Теорію, методи та моделі формування векторів кібербезпекових атак, класи кібератак (пасивні, активні, інсайдерські, наступальні, розподілені атаки).	діяльності з виявлення та оцінки вразливостей та тестування та/або тестування на проникнення до ІС та її ресурсів. **Б1.У2.** Використовувати концепції та моделі побудови ІС OSI/ISO, а також типи і принципи використання протоколів обміну даними, методи динамічного конфігурування вузлів, системи доменних імен і послуг з метою реалізації в подальшому процедур аналітичної діяльності з виявлення та оцінки вразливостей тестування та/або тестування на проникнення до ІС та її ресурсів. **Б1.У3.** Використовувати операційні системи різних типів (ОС Microsoft Windows, ОС Unix/Linux, ОС Soláris) з метою реалізації в подальшому	технологій та теоретичних засад в процесі організації аналітичної діяльності з виявлення та оцінки вразливостей у сфері кібербезпеки та захисту інформаційних систем та мереж.	інформаційних технологій для розробки процедур аналітичної діяльності з виявлення та оцінки вразливостей.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		Б1.36. Теорію, структуру, моделі та мови програмування баз даних (SQL, SQL Server, Oracle). **Б1.37.** Принципи і методи забезпечення безпеки інформаційних технологій (мережеві екрани, принципи побудови демілітаризованих зон, процедури шифрування трафіку та розподілу доступу до інформаційних ресурсів ІС) . **Б1.38.** Загрози і вразливості безпеки систем та прикладному програмному забезпеченню (переповнення буфера, мобільний код, міжсайтові сценарії, процедурна мова/мова структурованих запитів [PL/SQL], ін'єкції, перегони фронтів, прихований канал, повтор, атаки на повернення, шкідливий та диструктуючий код).	процедур аналітичної діяльності з виявлення та оцінки вразливостей та тестування та/або тестування на проникнення до ІС та її ресурсів.		

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	Б2. Здатність виконувати заходи організації аналітичної діяльності з виявлення та оцінки вразливостей ІС (або АС, ІКС, СЕК) та її інформаційних ресурсів у процесі розробки та конфігурування системи.	**Б2.З1.** Процедури організації аналітичної діяльності з виявлення та оцінки вразливостей ІС та її інформаційних ресурсів у процесі розробки та конфігурування. **Б2.З2.** Джерела вразливостей та класифікацію загроз інформаційним ресурсам. **Б2.З3.** Конкретні операційні наслідки, що виникають у результаті реалізації кіберзагроз, збоїв системи або виникнення кіберінцидентів. **Б2.З4.** Процеси та сценарії організації аналітичної діяльності з виявлення та оцінки вразливостей, а також тестування та/або тестування на проникнення на основі різних методик та форм. **Б2.З5.** Процес оцінки стану безпеки інформації та тестування та/або тестування на проникнення	**Б2.У1**. Здійснювати процедури та заходи організації аналітичної діяльності з виявлення та оцінки вразливостей ІС (або АС, ІКС, СЕК) та її інформаційних ресурсів у процесі розробки та конфігурування системи. **Б2.У2.** Розробляти сценарії організації аналітичної діяльності з виявлення та оцінки вразливостей ІС (або АС, ІКС, СЕК) та її інформаційних ресурсів. **Б2.У3.** Розробляти сценарії тестування та/або тестування на проникнення на основі методології, методів та засобів забезпечення мережевої безпеки. **Б2.У4.** Розробляти сценарії тестування та/або тестування на проникнення на основі джерел вразливостей інформаційних ресурсів.	**Б2.К1.** Взаємодіяти з керівництвом та відповідним персоналом з питань виконання процедур організації аналітичної діяльності з виявлення та оцінки вразливостей ІС (або АС, ІКС, СЕК) та її інформаційних ресурсів у процесі розробки та конфігурування системи.	**Б2.В1.** Готувати інформацію, доповіді, презентації з напряму виконання процедур організації аналітичної діяльності з виявлення та оцінки вразливостей ІС (або АС, ІКС, СЕК) та її інформаційних ресурсів у процесі розробки та конфігурування системи. **Б2.В2.** Готувати звіти за результатами виконання заходів з організації аналітичної діяльності щодо виявлення та

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		з урахуванням вразливостей інформаційних систем та її ресурсів. **Б2.З6.** Теорію управління мережевим доступом, ідентифікацією, принципи контролю та управління доступом на базі інфраструктури відкритих ключів, використання кращих світових практик (бібліотек інфраструктури інформаційних технологій ITIL, механізми контролю доступу до хостів /мереж, списки контролю доступу та повноважень). **Б2.З7.** Принципи та методи автентифікації і авторизації користувачів та автентифікації інформаційних об’єктів (зокрема відкриті ідентифікатори, мову розмітки для контролю захищеності, мову розмітки для надання послуг).	**Б2.У5.** Розробляти сценарії організації аналітичної діяльності з виявлення та оцінки вразливостей ІС (або АС, ІКС, СЕК) та її інформаційних ресурсів на основі моделі побудови ІС OSI/ISO, а також типів і принципів використання протоколів обміну даними, методів динамічного конфігурування вузлів, системи доменних імен (DNS). **Б2.У6.** Розробляти сценарії організації аналітичної діяльності з виявлення та оцінки вразливостей ІС (або АС, ІКС, СЕК) та її інформаційних ресурсів на основі методів автентифікації і авторизації користувачів та автентифікація інформаційних об’єктів (зокрема відкриті		оцінки вразливостей ІС (або АС, ІКС, СЕК) та її ресурсів на основі процедур тестування та оцінки стану безпеки у відповідності до встановлених повноважень.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		Б2.38. Інфраструктуру, що підтримує ІТ для забезпечення захисту, продуктивності та надійності функціонування ІС та комплексів захисту інформації. **Б2.39.** Інструменти діагностики і методик визначення несправностей інформаційних систем та засобів безпеки інформації та/або кібербезпеки. **Б2.310.** Етапи кібератак (розвідка, сканування, перерахування, отримання доступу, ескалація привілеїв, підтримка доступу, використання мережі, приховування слідів).	ідентифікатори, мова розмітки для контролю захищеності, мова розмітки для надання послуг).		
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
В. Проведення процедур тестування та/або тестування на проникнення, а також необхідних перевірок стану кіберзахисту відповідно середовища з метою організації аналітичної діяльності з виявлення та оцінки вразливостей у сфері кібербезпеки та захисту інформаційно-комунікаційних систем та мереж.	**В1.** Здатність проводити тестування та/або тестування на проникнення з метою організації аналітичної діяльності з виявлення та оцінки вразливостей ІС (або АС, ІКС, СЕК) та її активів.	**В1.З1.** Поняття та загальний зміст програми та методики проведення аналітичної діяльності з виявлення та оцінки вразливостей на основі процедур санкціонованого тестування та/або тестування на проникнення до ІС та мереж, а також апаратного, програмно-апаратного та програмного забезпечення сталих операційних процесів та систем безпеки інформації і кіберзахисту. **В1.З2.** Процеси та методи підтримки аналітичної діяльності з виявлення та оцінки вразливостей в сталому (робочому) стані. **В1.З3.** Процеси та методи підтримки інструментів, програмного і апаратного забезпечення аналітичної діяльності в робочому стані, а процедури контролю їх працездатності в межах	**В1.У1**. Реалізовувати Плани щодо проведення аналітичної діяльності з виявлення та оцінки вразливостей в ІС державних органів, на підприємствах, в організаціях різних форм власності в рамках чинного законодавства. **В1.У2**. Визначати і впроваджувати процеси аналітичної діяльності з виявлення та оцінки вразливостей на основі процедур тестування та/або тестування на проникнення. **В1.У3**. Визначати і впроваджувати процеси аналітичної діяльності з виявлення та оцінки вразливостей на основі процедур тестування та/або тестування на проникнення, а також виконувати завдання збору, обробки та розподілу даних,	**В1.К1.** Взаємодіяти з керівництвом, персоналом та партнерами стосовно проведення тестування та/або тестування на проникнення, оцінки та перевірки операційних процесів ІС та її ресурсів з метою виявлення джерел загроз. **В1.К2.** Взаємодіяти з колегами та партнерами стосовно проведення тестування та/або тестування на проникнення, оцінки та перевірки операційних процесів ІС та її ресурсів з метою забезпечення сталих	**В1.В1.** Розробляти технічну документацію визначеного спрямування у відповідності до встановлених повноважень. **В1.В2.** Формувати звіти аналітичної діяльності з виявлення та оцінки вразливостей за напрямами проведеного тестування на вразливість у відповідності до встановлених повноважень.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		визначених параметрів та технічних норм. **В1.З4.** Технологічне, техніко-економічне, комп'ютерне, програмне та інше забезпечення систем безпеки інформації та кіберзахисту ІС та її ресурсів. **В1.З5.** Принципи і методи етичних хакерських атак.	використовувати визначені вразливості за відповідними напрямами безпеки інформації та кіберзахисту. **В1.У4**. Визначати вразливі місця або збої технічних та організаційних засобів контролю, які впливають на конфіденційність, цілісність і доступність продуктів інформаційно-комунікаційних технологій (систем, апаратного забезпечення, програмного забезпечення та сервісів). **В1.У5.** Проектувати структури аналізу даних для збору критичної інформації з забезпечення аналітичної діяльності з виявлення та оцінки вразливостей. **В1.У6.** Адаптувати методи та налаштовувати інструменти тестування	бізнес-операційних процесів.	

Трудові функції	Компетентності	Результати навчання			
		Знання	Уміння/навички	Комунікація	Відповідальність і автономія
			та/або тестування на проникнення у відповідності до операційних процесів ІС та інформаційних активів. **В1.У7.** Визначати вектори атак, виявляти і демонструвати використання технічних вразливостей систем безпеки інформації та/або кібербезпеки в рамках чинного законодавства. **В1.У8.** Визначати, впроваджувати і виконувати дії щодо аналітичної діяльності з виявлення та оцінки вразливостей на базі реалізації сценаріїв атак для оцінки ефективності впроваджених або запланованих заходів безпеки. **В1.У9.** Формувати звіти за напрямами проведеної аналітичної діяльності з виявлення та оцінки вразливостей.		

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	В2. Здатність проводити необхідні перевірки стану кіберзахисту відповідно до середовища, аналізувати політики та конфігурації кіберзахисту підприємства, установи або організації, а також оцінювати їх відповідність нормативним актам та директивам.	**В2.З1.** Концепцію формування та впровадження перевірок відповідно середовищу (технічний нагляд, огляди контрзаходів [TSCM, TEMPEST]. **В2.З2.** Теорію, методи, моделі та процеси управління технічними і не технічними ризиками (методи оцінки та зниження ризиків, кольорова мапа ризиків). **В2.З3.** Процеси управління інформаційними ресурсами (методи класифікації та градації активів за ризиком). **В2.З4.** Процеси управління конфігураціями інформаційних ресурсів інформаційної системи. **В2.З5.** Типи порушників, які здійснюють процедури несанкціонованого доступу та реалізують кібератаки різних класів (хакерські, інсайдерські, спонсоровані	**В2.У1.** Проведення розрахунку та оцінювання технічних і нетехнічних ризиків на основі аналізу вразливостей, вартості інформаційних ресурсів після реалізації атак та за напрямом визначених пріоритетних технологічних областей і середовища. **В2.У2.** Проводити перевірки стану системи менеджменту інформаційної безпеки та безпосередньо стану кіберзахисту відповідно до середовища. **В2.У3.** Проводити перевірки та аналіз стану політик безпеки інформації та конфігурації кіберзахисту підприємства, установи або організації. **В2.У4.** Проводити оцінки впливу ризику на стан функціонування ІС та її інформаційних ресурсів, а	**В2.К1.** Взаємодіяти з керівництвом, персоналом та партнерами стосовно необхідних перевірок стану кіберзахисту відповідно до середовища, аналізу політик безпеки, конфігурації забезпечень кіберзахисту підприємства, установи або організації. **В2.К2.** Інформувати керівництво та персонал щодо контексту середовища загроз та класифікації ризиків для організації.	**В2.В1.** Готувати звіти та іншу інформацію про проведення відповідних перевірок в межах встановлених повноважень.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		і не спонсоровані державами атаки). **В2.З6** Ризик безпеки прикладних програм (Open Web Application Security Project Top 10 list).	також на стан операційних процесів організації в цілому. **В2.У5.** Виконувати дії щодо зменшення ризику на основі процесів управління конфігурацією.		
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				
Г. Аналіз результатів аналітичної діяльності з виявлення та оцінки вразливостей та оцінювання операційних процесів ІС, програмного та/або апаратного забезпечення з метою визначення їх відповідності встановленим	**Г1.** Здатність аналізувати результати аналітичної діяльності з виявлення та оцінки вразливостей операційних процесів ІС, програмного та/або апаратного забезпечення або їх сумісності.	**Г1.З1.** Плани проведення аналітичної діяльності з виявлення та оцінки вразливостей на предмет придатності і повноти збору критичних даних про інформаційну інфраструктуру організації та безпосередньо ІС та її інформаційні ресурси. **Г1.З2.** План, методики та задачі проведення аналізу результатів аналітичної діяльності з виявлення та	**Г1.У1.** Визначати вимоги до напрямів аналітичної діяльності з виявлення та оцінки вразливостей, процедур тестування та/або тестування на проникнення та оцінювати стан інформаційних ресурсів. **Г1.У2.** Проводити аналіз результатів аналітичної діяльності з виявлення та оцінки вразливостей структури та топології	**Г1.К1.** Взаємодіяти з керівництвом організації, персоналом та партнерами стосовно аналізу проведення аналітичної діяльності з виявлення та оцінки вразливостей, оцінки та перевірки операційних	**Г1.В1.** Розробляти технічну документацію за результатами аналітичної діяльності, аналізу вразливостей структури та топології інформаційних систем та/або мереж організації.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
специфікаціям і вимогам.		оцінки вразливостей структури та топології інформаційних системи та/або мереж ІС організації. **Г1.З3.** План, методики та задачі проведення аналізу результатів аналітичної діяльності з виявлення та оцінки вразливостей апаратних та програмно-апаратних засобів, спеціального програмного забезпечення, комплексів засобів захисту. інформаційних системи та/або мереж. **Г1.З4.** Методику та задачі формування звітності щодо аналізу результатів аналітичної діяльності з виявлення та оцінки вразливостей.	інформаційних системи та/або мереж ІС організації. **Г1.У3.** Проводити аналіз результатів аналітичної діяльності з виявлення та оцінки вразливостей апаратних та програмно-апаратних засобів, спеціального програмного забезпечення, комплексів засобів захисту інформаційних системи та/або мереж з метою встановлення джерел вразливостей ІС та інформаційних ресурсів організації. **Г1.У4.** Збирати, перевіряти і підтверджувати дані аналітичної діяльності з виявлення та оцінки вразливостей ІС та її ресурсів.	процесів ІС та її ресурсів. **Г1.К2.** Взаємодіяти з колегами та партнерами стосовно аналізу результатів аналітичної діяльності з виявлення та оцінки вразливостей структури та топології інформаційних системи та/або мереж ІС організації.	**Г1.В2.** Розробляти звітну документацію щодо аналізу процедур тестування у відповідності до встановлених повноважень.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	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 конструювання; бібліотечні ресурси, архівні матеріали (за потреби); законодавчо-нормативні акти, акти роботодавця відповідного спрямування				
Д. Координація робіт та розроблення рекомендацій на основі результатів проведення аналітичної діяльності з виявлення та оцінки вразливостей ІС (або АС, ІКС, СЕК) та її інформаційним ресурсам.	**Д1.** Здатність розробляти рекомендації на основі проведення аналітичної діяльності з виявлення та оцінки вразливостей ІС (або АС, ІКС, СЕК) та її інформаційних ресурсів.	**Д1.З1.** Поняття та загальний зміст Програми та методики розробки рекомендацій на основі проведення аналітичної діяльності з виявлення та оцінки вразливостей. **Д1.З2.** План реалізації Програми та методики розроблених рекомендацій, що створені на основі даних аналізу та виявлених вразливостей, недоліків при проведенні аналітичної діяльності з виявлення та оцінки вразливостей.	**Д1.У1.** Розробляти Програми та методики рекомендацій на основі проведення процедур тестування та/або тестування на проникнення ІС та її інформаційних ресурсів. **Д1.У2.** Реалізовувати план Програми рекомендацій, що створені на основі даних аналізу та виявлених вразливостей, недоліків при проведенні процедур тестування ІС та її інформаційних ресурсів. **Д1.У3.** Переводити дані і результати проведення аналітичної діяльності в оціночні висновки та рекомендації.	**Д1.К1.** Взаємодіяти з керівництвом організації, персоналом та партнерами стосовно розроблення та інформування про розроблені рекомендації. **Д1.К2**. Взаємодіяти з колегами та партнерами стосовно реалізації плану Програми рекомендацій, що створені на основі даних проведення аналітичної діяльності з виявлення та оцінки вразливостей.	**Д1.В1.** Розробляти звітну документацію щодо реалізації Програми рекомендацій у відповідності до встановлених повноважень.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	Д2. Здатність здійснювати координацію робіт з реалізації процедур проведення аналітичної діяльності з виявлення та оцінки вразливостей ІС (або АС, ІКС, СЕК) та її ресурсів.	**Д2.З1.** Систему менеджменту інформаційної безпеки та повний перелік бізнес-операційних процесів організації. **Д2.З2.** Концепції архітектури безпеки організації, розподілу доступу та еталонних моделей архітектури підприємства (Zachman, FEA). **Д2.З3.** Концепцію управління ресурсами, змінами конфігурації та забезпеченням інформаційної системи та/або мережі та їх безпеки. **Д2.З4.** Концепцію та методи управління персоналом в ІТ компанії. **Д2.З5.** Корпоративну архітектуру організації в цілому та функціональні обов'язки кадрового складу організації в залежності від покладених повноважень у	**Д2.У1.** Організовувати та здійснювати координацію робіт з реалізації процедур тестування систем безпеки інформації та кіберзахисту ІС (або АС, ІКС, СЕК) та її ресурсів. **Д2.У2.** Визначати необхідний рівень розподілу та складності задач згідно з посадовими інструкціями персоналу та у відповідності до конкретного операційного процесу ІС та організації в цілому. **Д2.У3.** Визначати рівень взаємозв'язку між підрозділами та персоналом з метою ефективної реалізації процедур проведення аналітичної діяльності з виявлення та оцінки вразливостей та координації дій. **Д2.У4.** Консультувати керівництво та персонал	**Д2.К1.** Взаємодіяти з керівництвом, персоналом організації та партнерами стосовно координації робіт з реалізації процедур проведення аналітичної діяльності з виявлення та оцінки вразливостей ІС (або АС, ІКС, СЕК) та її ресурсів. **Д2.К2.** Інформувати керівництво та власника ресурсів щодо встановленого рівня взаємозв'язку між підрозділами та персоналом з метою ефективної реалізації процедур проведення аналітичної діяльності з виявлення та оцінки	**Д2.В1**. Готувати документацію, програми тренінгів та іншу інформацію про координацію робіт з реалізації процедур проведення аналітичної діяльності з виявлення та оцінки вразливостей в рамках вставлених повноважень та задач.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		сфері безпеки інформації та/або кібербезпеки. **Д2.З6.** Методику проведення консультації та тренінгів, пов'язаних з використанням ІТ та їх безпеки в організації, аналітичної діяльності з виявлення та оцінки вразливостей.	організації, проводити тренінги щодо питань проведення аналітичної діяльності з виявлення та оцінки вразливостей у відповідності до вітчизняної та світової нормативно-правової бази, стандартів та кращих світових практик.	вразливостей та координації дій.	
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				

VI. Розподіл трудових функцій та компетентностей за професійними кваліфікаціями

Трудова функція (умовне позначення)	Загальна назва професійної кваліфікації у межах професійного стандарту: Аналітик з оцінки вразливостей	
	Аналітик з оцінки вразливостей	Провідний аналітик з оцінки вразливостей
	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:

БАХТІЯРОВ Денис Ілшатович, провідний науковий співробітник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

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

ВОЛКОВА Ксенія Миколаївна, заступник начальника управління правового співробітництва з міжнародними організаціями Департаменту міжнародного права Міністерства юстиції України (за згодою);

ГНАТЮК Віктор Олександрович, доцент кафедри телекомунікаційних та радіоелектронних систем факультету аеронавігації, електроніки та телекомунікацій Національного авіаційного університету (за згодою);

ДАВИДЮК Андрій Вікторович, заступник начальника 1 відділу 4 управління Державного центру кіберзахисту Держспецзв’язку;

ДІДИК Валерія Анатоліївна, керівник напряму з розвитку професійних навичок з кібербезпеки Проєкту USAID «Кібербезпека критично важливої інфраструктури України» (за згодою);

ДОВЖЕНКО Надія Михайлівна, доцент кафедри інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації Державного університету телекомунікацій (за згодою);

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

КАСАТКІН Дмитро Юрійович, завідувач кафедри комп'ютерних систем мереж та кібербезпеки Національного університету біоресурсів і природокористування України (за згодою);

КОНЕЦЬКА Ольга Олексіївна, провідний науковий співробітник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

ЛЕГОМІНОВА Світлана Володимирівна, завідувач кафедри управління інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації Державного університету телекомунікацій (за згодою);

ЛЕОНОВ Андрій Олегович, голова Громадської організації «Інститут стандартів та технологій» (за згодою);

ЛУКОВА-ЧУЙКО Наталія Вікторівна, завідувач кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка (за згодою);

МАЗУР Наталя Володимирівна, голова Профспілки працівників зв'язку України (за згодою);

МЕЛЬНИК Сергій Вікторович, консультант напряму з розвитку професійних навичок з кібербезпеки Проєкту USAID «Кібербезпека критично важливої інфраструктури України» (за згодою);

МОХОР Володимир Володимирович, директор Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України (за згодою);

ПАЗЮК Андрій Валерійович, віцепрезидент Громадської організації «Українська академія кібербезпеки» (за згодою);

ПЕТРУШКЕВИЧ Олександр Володимирович, заступник начальника Державного центру кіберзахисту Держспецзв'язку;

ПОНОМАРЬОВ Сергій Павлович, директор Департаменту розвитку електронних комунікацій Адміністрації Держспецзв'язку;

СУПРУН Олег Олексійович, асистент кафедри інтелектуальних програмних систем факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка (за згодою);

ФІЛІППОВА Ольга Валентинівна, комерційний директор компанії «САЙКОМ» (за згодою);

ШТОМПЕЛЬ Тетяна Миколаївна, віцепрезидент компанії ТОВ «ТЕКЕКСПЕРТ», керівник навчального Центру «Мережні технології» (за згодою).

2. Назва та реквізити документа, яким затверджено професійний стандарт

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

3. Реквізити висновку суб'єкта перевірки про дотримання вимог Порядку розроблення, введення в дію та перегляду професійних стандартів під час підготовки проєкту професійного стандарту

Висновок суб'єкта перевірки Національного агентства кваліфікацій від 27 грудня 2023 року про дотримання під час підготовки проєкту професійного стандарту «Аналітик з оцінки вразливостей» 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 щодо погодження проєкту професійного стандарту «Аналітик з оцінки вразливостей» Профспілкою працівників зв'язку України (лист від 16.11.2023 р. № 01.2-14/136, постанова Президії ЦК Профспілки працівників зв'язку України від 16.11.2023 р. № П-4-5г).

VIII. Дата внесення професійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.

Заступник Голови Держспецзв'язку,
керівник комплексної робочої групи
з розробки професійних стандартів Олександр ПОТІЙ