Проєкт

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

ПРОФЕСІЙНИЙ СТАНДАРТ

АНАЛІТИК З ОЦІНКИ ВРАЗЛИВОСТЕЙ

_____(дата внесення до Реєструкваліфікацій)

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

Професійний стандарт розроблено та затвердженозгідно з вимогамистатті 42 Кодексу законів про працюУкраїни на підставі:

- висновку суб'єкта перевірки– Національного агентства кваліфікацій від _____ про дотриманняпід 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 з оцінки вразливостей

ІІ. 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.

Проведення перевірок та надання оцінок стану функціонування інформаційних систем та мереж різних класів на відповідність у межах елементів мережі, підсистем або замкненої групи. Визначення відхилень операційних процесів системи/мережі, політик безпеки від сталих норм та прийнятних конфігурацій, проведення аналізу та визначення вразливостей інформаційним ресурсам (активам) системи/мережі. Проведення вимірювань ефективності ешелонованого захисту інформаційної системи та її ресурсів щодо відомих вразливостей, кібератак на основі процедур тестування або\чи тестування на проникнення.

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.

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 телекомуніка-ції	**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 устаткованням
				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 М	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 професії та код підкласу професії згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій»

Аналітик з оцінки вразливостей 2139.2.

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

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

- підготовка на другому (магістерському) рівні вищої освіти за спеціальністю:

- 122 «Комп’ютерні науки» 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);

- документ (диплом, сертифікат, тощо), щодо післядипломної освіти та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері тестування систем захисту інформації;
- документ (диплом, сертифікат, тощо), щодо післядипломної освіти та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань в рамках консультаційно-навчальної діяльності у сфері тестування систем захисту інформації;
- документ (диплом, сертифікат, тощо), щодо професійної сертифікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері тестування систем захисту інформації.

ІІІ. Здобуття професійної кваліфікації та професійний розвиток

1. Здобуття професійної кваліфікації

Назва професійної та/або часткової професійної кваліфікації	**Суб'єкти, уповноваженізаконодавством на присвоєння/підтвердження та визнанняпрофесійнихкваліфікацій**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
Аналітик з оцінки вразливостей та провідний аналітик з оцінки вразливостей	Підготовка на другому (магістерському) рівні вищої освіти за спеціальностями вказаними в п.5 галузі знань 12 «Інформаційні технології» та 3 роки досвіду роботи за спеціальністю	*Не передбачено професійним стандартом*
Провідний аналітик з оцінки вразливостей та провідний аналітик з оцінки вразливостей	Підготовка на другому (магістерському) рівні вищої освіти за спеціальностями вказаними в п.5 галузі знань 12 «Інформаційні технології» та 5 років досвіду роботи за спеціальністю	*Не передбачено професійним стандартом*

2. Професійний розвиток

1) з присвоєнням наступної професійної кваліфікації

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

IV. Абревіатури, скорочення

IT	інформаційні технології
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

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 діяльності у сфері кібербезпеки та захисту інформаційних систем та мереж (або АС, ІКС, СЕК) на базі нормативно-правового та організаційно технічного забезпечення.	**А1.З1.** Законодавча та нормативно-правова база, стандарти, нормативні документи та етичні норми пов'язані з кібербезпекою та захистом інформації в ІС та її інформаційних ресурсів. **А1.З2.** Концепції або\чи 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 або\чи кіберзахисту ІС	**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 або\чи тестування на проникнення у ІС державних органів, на підприємствах, в організаціях різних форм власності.	**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 .

		та її інформаційних ресурсів. **А1.З4.** Моделі систем безпеки: модель конфіденційності, цілісності та доступності; модель Белла-Лападули; моделі забезпечення цілісності «Biba» і Кларка-Вілсона. **А1.З5.** Корпоративну архітектуру безпеки інформації та кіберзахисту ІС та\або мережі. **А1.З6.** Вимоги до організації та проведення процедур тестування або\чи тестування на проникнення, а також впровадження аналітичної діяльності з виявлення та аналізу вразливостей. **А1.З7.** Обладнання та функції апаратного, програмно-апаратного та програмного забезпечення безпеки інформації та кіберзахисту ІС та\або мереж організації. **А1.З8.** Концепції, методи та процедури адміністрування та захисту ІС та її активів з	**А1.У3.** Проводити аналіз структури та топології 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 або\чи		

		урахуванням операційних або\чи 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.	тестування на проникнення до ІС та її ресурсів з метою 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 аналітичної діяльності з виявлення та оцінки вразливостей у сфері кібербезпеки та захисту інформаційних систем та мереж.	**Б1**. Здатність використовувати інформаційні технології та теоретичних засади з метою розробки сучасних систем кібербезпеки та захисту інформації, а також організації та проведення процедур аналізу вразливостей ІС (або АС, ІКС, СЕК) та їх інформаційних ресурсів.	**Б1.З1.** Інтерпретовані, об'єктно орієнтовані, предметно-орієнтовані, мови скриптів та компільовані мови програмування (Java, Java Script, C ++, PHP, Python, Objective-C). **Б1.З2** Концепції та моделі побудови ІС OSI/ISO, а також типи і принципи використання протоколів обміну даними, такі, як TCP/IP, методи динамічного	**Б1.У1.** Розробляти та використовувати програмне забезпечення різних типів з метою реалізації в подальшому процедур аналітичної діяльності з виявлення та оцінки вразливостей та тестування або\чи тестування на проникнення до ІС та її ресурсів.	**Б1.К1.** Взаємодіяти з керівництвом та відповідним персоналом з питань використання інформаційних технологій та теоретичних засад в процесі організації аналітичної діяльності з виявлення та оцінки вразливостей у сфері кібербезпеки та захисту	**Б1.В1.** Готувати інформацію доповіді, презентації) з напряму використання інформаційних технологій для розробки процедур аналітичної діяльності з виявлення та оцінки вразливостей.

		конфігурування вузлів, методи формування різних класів скриптів, системи доменних імен (DNS) і послуг, що надаються Службою каталогів. **Б1.З3.** Операційні системи різних типів (ОС Microsoft Windows, Unix\Linux, ОС Soláris). **Б1.З4** Методи та моделі статистичного аналізу даних та прийняття рішень. **Б1.З5** Теорія, методи та моделі формування векторів кібербезпекових атак, класи кібератак (пасивні, активні, інсайдерські, наступальні, розподілені атаки). **Б1.З6** Теорія, структура, моделі та мови програмування баз даних (SQL, SQL Server, Oracle). **Б1.З7.** Принципи і методи забезпечення безпеки інформаційних технологій (мережеві екрани, принципи	**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 або\чи 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 процедур аналітичної діяльності	інформаційних систем та мереж.	

		побудови демілітаризованих зон, процедури шифрування трафіку та розподілу доступу до інформаційних ресурсів ІС) . **Б1.З8.** 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).	з виявлення та оцінки вразливостей та тестування або\чи тестування на проникнення до ІС та її ресурсів.		
	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				
	Б2. Здатність виконувати заходи організації аналітичної	**Б2.З1.** Процедури організації аналітичної діяльності з виявлення	**Б2.У1**. Здійснювати процедури та заходи організації аналітичної	**Б2.К1.** Взаємодіяти з керівництвом та відповідним	**Б2.В1.** Готувати інформацію доповіді,

	діяльності з виявлення та оцінки вразливостей ІС (або АС, ІКС, СЕК) та її інформаційних ресурсів у процесі розробки та конфігурування системи.	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 або\чи тестування на проникнення на основі різних методик та форм. **Б2.З5.** Процес оцінки стану безпеки інформації та тестування або\чи тестування на проникнення з урахуванням вразливостей	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 або\чи тестування на проникнення на основі методології, методів та засобів забезпечення мережевої безпеки. **Б2.У4.** Розробляти сценарії тестування або\чи тестування на проникнення на основі джерел вразливостей інформаційних ресурсів. **Б2.У5.** Розробляти сценарії організації аналітичної діяльності	персоналом з питань виконування процедур організації аналітичної діяльності з виявлення та оцінки вразливостей ІС (або АС, ІКС, СЕК) та її інформаційних ресурсів у процесі розробки та конфігурування системи.	презентації) з напряму виконування 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 виконування заходів з організації аналітичної діяльності щодо виявлення та оцінки вразливостей ІС (або АС, ІКС, СЕК) та її ресурсів на

		інформаційних систем та її ресурсів. **Б2.З6.** Теорія та принципи контролю та управління мережевим доступом, ідентифікацією, контролю та доступом на базі інфраструктури відкритих ключів, бібліотека інфраструктури інформаційних технологій, поточної версії ITIL, механізми контролю доступу до хостів /мереж (списки контролю доступу, списки повноважень). **Б2.З7.** Принципи та методи автентифікації і авторизації користувачів та автентифікація інформаційних об'єктів (в т.ч. відкриті ідентифікатори, мова розмітки для контролю захищеності, мова розмітки для надання послуг).	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 (в т.ч.відкриті ідентифікатори, мова розмітки для контролю захищеності, мова		основі процедур тестування та оцінки стану безпеки у відповідності до встановлених повноважень.

		Б2.З8. Інфраструктура, що підтримує ІТ для забезпечення захисту, продуктивності та надійності функціонування ІС та комплексів захисту інформації. **Б2.З9.** Інструменти діагностики і методик визначення несправностей інформаційних систем та засобів безпеки інформації аьо\чи кібербезпеки. **Б2.З9.** Етапи кібератак (розвідка, сканування, перерахування, отримання доступу, ескалація привілеїв, підтримка доступу, використання мережі, приховування слідів).	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				
В. Проведення процедур тестування або\чи тестування на проникнення, а	**В1**. Здатність проводити тестування або\чи тестування на проникнення з метою	**В1.З1**. Поняття та загальний зміст програми та методики проведення	**В1.У1**. Реалізовувати Плани щодо проведення аналітичної діяльності з виявлення та оцінки	**В1.К1.** Взаємодіяти з керівництвом, персоналом та партнерами	**В1.В1**. Розроблювати технічну документацію

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.	організації аналітичної діяльності з виявлення та оцінки вразливостей ІС (або АС, ІКС, СЕК) та її активів.	аналітичної діяльності з виявлення та оцінки вразливостей на основі процедур санкціонованого тестування або\чи 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	вразливостей в ІС державних органів, на підприємствах, в організаціях різних форм власності в рамках чинного законодавства. **В1.У2**. Визначення і впровадження процесів аналітичної діяльності з виявлення та оцінки вразливостей на основі процедур тестування або\чи тестування на проникнення. **В1.У3**. Визначення і впровадження процесів аналітичної діяльності з виявлення та оцінки вразливостей на основі процедур тестування або\чи тестування на проникнення, а також виконання завдань збору, обробки та розподілу даних, використання визначених вразливостей за відповідними напрямами безпеки інформації та кіберзахисту. **В1.У4**. Визначати вразливі місця або збої	стосовно проведення тестування або\чи тестування на проникнення, оцінки та перевірки операційних процесів ІС та її ресурсів з метою виявлення джерел загроз. **В1.К1.** Взаємодіяти з колегами та партнерами стосовно проведення тестування або\чи тестування на проникнення, оцінки та перевірки операційних процесів ІС та її ресурсів з метою забезпечення сталих бізнес-операційних процесів.	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.

		їх працездатності в межах 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.	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 або\чи тестування на проникнення 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\чи 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.		
	В2. Проведення необхідних перевірок стану кіберзахисту відповідно до середовища, аналіз політики та конфігурації кіберзахисту	**В2.З1** Концепція формування та впровадження перевірок відповідно середовищу (технічний нагляд, огляди контрзаходів [TSCM, TEMPEST].	**В2.У1** Проведення розрахунку та оцінювання технічних і нетехнічних ризиків на основі аналізу вразливостей, вартості інформаційних ресурсів після	**В2.К1.** Взаємодіяти з керівництвом, персоналом та партнерами стосовно необхідних перевірок стану кіберзахисту відповідно до	**Б1.В1**. Готувати звіти та іншу інформацію про проведення відповідних перевірок в межах

	підприємства, установи або організації, а також оцінювання їх відповідності нормативним актам та директивам.	**В2.З2.** Теорія, методи, моделі та процеси управління ризиками технічними і не технічними ризиками (методи оцінки та зниження ризиків, кольорова мапа ризиків). **В2.З2.** Процеси управління інформаційними ресурсами (методи класифікації та градації активів за ризиком). **В2.З2.** Процеси управління конфігураціями інформаційних ресурсів інформаційної системи. **В21.З3.** Типи порушників, які здійснюють процедури не санкціонованого доступу та реалізують кібератаки різних класів (хакерські атаки, інсайдерські, спонсоровані і не спонсоровані державами атаки). **В2.З4** Ризик безпеки прикладних програм (Open Web Application Security Project Top 10 list).	реалізації атак (по інциденту) та за напрямом визначених пріоритетних технологічних областей і середовища. **В2.У2.** Проведення перевірок стану системи менеджменту інформаційної безпеки та безпосередньо стану кіберзахисту відповідно до середовища. **В2.У3** Проведення перевірок та аналізу 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 також на стан операційних процесів організації в цілому. **В2.У5.** Виконання дій щодо зменшення ризику на основі	середовища, аналіз політики та конфігурації кіберзахисту підприємства, установи або організації. **В2.К2.** Інформувати керівництво та персонал змістовною інформацією про контекст середовища загроз для організації, що покращує її позицію управління ризиками.	встановлених повноважень.

			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 специфікаціям і вимогам.	**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 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	**Г1.У2.** Визначати вимоги до напрямів аналітичної діяльності з виявлення та оцінки вразливостей, процедур тестування або\чи тестування на проникнення і оцінювання (співробітники, розподіл ролей, полігони, засоби, прилади). **Г1.У3.** Проводити аналіз результатів аналітичної діяльності з виявлення та оцінки вразливостей структури та топології інформаційних системи та\або мереж ІС організації. **Г1.У4.** Проводити аналіз результатів аналітичної діяльності з виявлення та оцінки вразливостей	**Г1.К1.** Взаємодіяти з керівництвом організації, персоналом та партнерами стосовно аналізу проведення аналітичної діяльності з виявлення та оцінки вразливостей, оцінки та перевірки операційних процесів ІС та її ресурсів. **Г1.К1**. Взаємодіяти з колегами та партнерами стосовно аналізу результатів аналітичної діяльності з виявлення та оцінки вразливостей	**Г1.В1.** Розроблювати технічну документацію за результатами аналізу аналітичної діяльності, вразливостей структури та топології інформаційних системи та\або мереж організації у відповідності до встановлених повноважень **Г1.В2.** Розроблювати звітну документацію щодо аналізу процедур тестування у відповідності до

		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.	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.У5.** Збирати, перевіряти і підтверджувати дані аналітичної діяльності з виявлення та оцінки вразливостей ІС та її ресурсів.	структури та топології інформаційних системи та\або мереж ІС організації.	встановлених повноважень.
	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	**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	**Д1.У1.** Розробляти Програми та методики рекомендацій на основі проведення процедур тестування або\чи тестування на проникнення ІС та її інформаційних ресурсів.	**Д1.К1.** Взаємодіяти з керівництвом організації, персоналом та партнерами стосовно розроблення та інформування про розроблені рекомендації.	**Д1.В1.** Розроблювати звітну документацію щодо реалізації Програми рекомендацій у відповідності до встановлених повноважень.

інформаційним ресурсам.		розроблених рекомендацій, що створені на основі даних аналізу та виявлених вразливостей, недоліків при проведенні аналітичної діяльності з виявлення та оцінки вразливостей.	**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.К2**. Взаємодіяти з колегами та партнерами стосовно реалізації плану Програми рекомендацій, що створені на основі даних проведення аналітичної діяльності з виявлення та оцінки 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				
	Д2. Здатність здійснювати координацію робіт з реалізації процедур проведення аналітичної діяльності з виявлення та оцінки вразливостей	**Д2.З1.** Система менеджменту інформаційної безпеки та повний перелік бізнес-операційних процесів організації. **Д2.З2.** Концепції архітектури безпеки організації, розподілу	**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.К1.** Взаємодіяти з керівництвом, персоналом організації та партнерами стосовно координації робіт з реалізації процедур проведення	**А1.В1**. Готувати документацію, програми тренінгів та іншу інформацію про координацію робіт з реалізації процедур проведення

	ІС (або АС, ІКС, СЕК) та її ресурсів.	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.З4.** Корпоративну архітектуру організації в цілому та функціональні обов'язки кадрового складу організації в залежності від покладених повноважень у сфері безпеки інформації та\або кібербезпеки. **Д2.З5.** Методику проведення консультації та тренінгів пов'язаних з використанням ІТ та їх	**Д2.У2.** Визначати необхідний рівень розподілу та складності задач згідно 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 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.	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 вразливостей та координації дій.	аналітичної діяльності з виявлення та оцінки вразливостей в рамках вставлених повноважень та задач.

		безпеки в організації, питань проведення аналітичної діяльності з виявлення та оцінки 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				

VI. Розподіл трудових функцій та компетентностей за професійними кваліфікаціями

Трудова функція (умовне позначення)	Загальна назва професійної кваліфікації у межах професійного стандарту: фахівець з тестування систем захисту інформації	
	аналітик з оцінки вразливостей та провідний аналітик з оцінки вразливостей	провідний аналітик з оцінки вразливостей
	повна	повна
А	+	+
Б	+	+
В	+	+
Г	+	+
Д	-	+

VII. Відомості про розроблення та затвердженняпрофесійного стандарту

1. Повне найменування розробник апрофесійного стандарту

Державної служби спеціального зв'язку та захистуінформації України

Склад робочої групи/Учасники робочої групи:

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

БЕЗШТАНЬКО Віталій, головний спеціаліст 1 відділу Департаменту кіберзахисту Адміністрації Держспецзв'язку;

БОДЮЛ Євген, начальник управління освітньої діяльності Департаменту освіти, науки і спорту МВС;

ВОЛКОВА Ксенія, заступник начальника управління правового співробітництва з міжнародними організаціями Департаменту міжнародного права Міністерства юстиції України;

ГНАТЮК Віктор доцент кафедри телекомунікаційних та радіоелектронних систем, факультет аеронавігації, електроніки та телекомунікацій, Національний авіаційний університет;

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

ДІДИК Валерія, керівник напрямку з розвитку професійних навичок з кібербезпеки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»;

ДОВЖЕНКО Надія, доцент кафедри інформаційної та кібернетичної безпеки, Навчально-науковий інститут захисту інформації, Державний університет телекомунікацій;

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

КАСАТКІН Дмитро, завідувач кафедри комп'ютерних систем, мереж та кібербезпеки, Національний університет біоресурсів і природокористування України;

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

ЛЕГОМІНОВА Світлана, завідувач кафедри управління інформаційної та кібернетичної безпеки, Навчально-науковий інститут захисту інформації, Державний університет телекомунікацій;

ЛЕОНОВ Андрій Олегович, голова організації Громадська організація «Інститут стандартів та технологій»;

ЛУКОВА-ЧУЙКО Наталія, завідувач кафедри кібербезпеки та захисту інформації, факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка;

МАЗУР Наталя, завідуюча відділом організаційно-правової роботи Профспілки працівників зв'язку України;

МАРТИНЮК Ганна, провідний науковий співробітник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

МЕЛЬНИК Сергій, консультант напрямку з розвитку професійних навичок з кібербезпеки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»;

МОХОР Володимир, директор Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України;

ПАЗЮК Андрій, віце-президент Громадської організації «Українська академія кібербезпеки»;

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

ПОНОМАРЬОВ Сергій, головний науковий співробітник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

СУПРУН Олег, кафедра інтелектуальних програмних систем факультет комп'ютерних наук та кібернетики, Київський національний університет імені Тараса Шевченка;

ФІЛІПОВА Ольга, комерційний директор компанії SAYCOM;

ШТОМПЕЛЬ Тетяна, віце президент компанії TECHEXPERT, керівник навчального Центру «Мережні технології».

2. Назва та реквізити документа, якимзатвердженопрофесійний стандарт (рішення (може оформлюватися протоколом), наказ, розпорядження).

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

Висновок суб'єкта перевірки Національного агентства кваліфікацій від_____ про дотримання під час підготовки проєкту професійного стандарту «фахівець з тестування систем захисту інформації» вимог Порядку розроблення, введення в дію та перегляду професійнихстандартів, затвердженогопостановоюКабінетуМіністрівУкраїнивід 31.05.2017 р. № 373).

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

Висновок Профспілки працівників зв'язку України від _____ щодо погодження проєкту професійного стандарту «фахівець з тестування систем захисту інформації».

VIII. Дата внесенняпрофесійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.