Проєкт

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

ПРОФЕСІЙНИЙ СТАНДАРТ

ФАХІВЕЦЬ З ТЕСТУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

_____(дата внесення до Реєстру кваліфікацій)

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 професійнихстандартів, затвердженогопостановоюКабінетуМіністрівУкраїнивід 31.05.2017 р. № 373;
- висновку Профспілки працівників зв'язку Українивід _____ щодо погодження проєкту професійного стандарту

І. Назва професійного стандарту

Фахівець з тестування систем захисту інформації

ІІ. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Планування, підготовка та проведення тестування або\чи тестування на проникнення до інформаційних систем та мереж (або автоматизованих систем, інформаційно-комунікаційних систем, систем електронних комунікацій), а також їх інформаційних ресурсів (активів або компонентів) в організаціях, підприємствах або установах різних форм власності.

Проведення оцінки відповідності інформаційних систем\мереж та комплексів кібербезпеки та захисту інформації стандартам, специфікаціям, нормам, вимогам та заявленим технічним характеристикам.

Проведення аналізу й звітування щодо результатів тестування, а також розроблення рекомендацій з виявлення та оцінки відхилень у функціонуванні операційних процесів та визначених вразливостей і загроз інформаційній системі та її 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	
Секція Р	Освіта	**Розділ 85**	Освіта	**Група 85.5**	Інші види освіти
				Клас 85.59	Інші види освіти, не введенні в інші угрупування

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

Фахівець з тестування систем захисту інформації 2139.2.

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

Молодший фахівець з тестування систем захисту інформації, 6 рівень НРК.

Фахівець з тестування систем захисту інформації 7 рівень НРК

Провідний фахівець з тестування систем захисту інформації 7 рівень НРК.

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

- диплом бакалавра (для молодшого фахівця та фахівця) за спеціальністю:

- 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології» (6 рівень НРК);

- 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» (6 рівень НРК);

- 126 «Інформаційні системи та технології» галузі знань 12 «Інформаційні технології» (6 рівень НРК);

- диплом магістра (для провідного фахівця) 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).

Додатково (за необхідністю або/чи вимогою суб'єкта, уповноваженого законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій):

- 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 визнання професійних кваліфікацій**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
Молодший фахівець тестування систем захисту інформації	Підготовка на першому рівні вищої освіти (бакалаврському) за спеціальностями вказаними в п.5 галузі знань 12 «Інформаційні технології»	*Не передбачено професійним стандартом*

Фахівець з тестування систем захисту інформації	Підготовка на першому рівні вищої освіти (бакалаврському) за спеціальностями вказаними в п.5 галузі знань 12 «Інформаційні технології» та 2 роки досвіду роботи за спеціальністю	*Не передбачено професійним стандартом*
Провідний фахівець з тестування систем захисту інформації	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*

2. Професійний розвиток

1) з присвоєнням наступної професійної кваліфікації

Назва професійної та/або часткової професійної кваліфікації	**Суб'єкти, уповноваженізаконодавством на присвоєння/підтвердження та визнання професійних кваліфікацій**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
Фахівець з тестування систем захисту інформації	Підвищення кваліфікації «Фахівця з тестування систем захисту інформації» для отримання професійної кваліфікації «Провідний фахівець з тестування систем захисту інформації». Стаж роботи за спеціальністю не менше трьох років.	*Не передбачено професійним стандартом*

IV. Абревіатури, скорочення

IT	інформаційні технології
FEA	Federal Enterprise Architecture
PII	Personally Identifiable Information
PCI	Payment Card Industry
PHI	Protected Health Information
TCP/IP	Transmission Control Protocol / Internet Protocol

DNS	Domain Name System
EBSCO	Elton Bryson Stephens Company
JSTOR	Journal Storage
NIST SP 800-161	National Institute of Standards and Technology Special Publication 800-161

V. Опис трудових функцій

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
А. Проведення підготовчих робіт щодо процедур тестування або\чи тестування на проникнення систем кібербезпеки та захисту інформації на всіх етапах (розроблення, впровадження та супроводження) життєвого циклу інформаційних системи та\або мереж.	**А1**. **Здатність** здійснювати підготовчі роботи щодо процедур тестування або\чи тестування на проникнення систем кібербезпеки та захисту інформації в ІС (або АС, ІКС, СЕК) в державних органах, на підприємствах, організаціях різних форм власності в межах чинного законодавства.	**А1.З1.** Законодавча та нормативно-правова база, стандарти, нормативні акти, політики та етичні норми пов'язані з кібербезпекою та захистом інформації в ІС та організації в цілому. **А1.З2.** Концепції або\чи Програми побудови інформаційних системи та\або мереж, а також методології, методи та засоби забезпечення мережевої безпеки. **А1.З3.** Стратегія та місія системи менеджменту безпеки інформації та кіберзахисту інформаційних ресурсів прийнятих на	**А1.У1.** Визначати необхідний рівень складності тесту для конкретної системи та згідно встановлених задач. **А1.У2.** Розробляти та реалізовувати Плани підготовки щодо проведення тестування або\чи тестування на проникнення у ІС державних органів, на підприємствах, в організаціях різних форм власності в рамках чинного законодавства. **А1.У3.** Проводити аналіз структури та топології інформаційних системи та\або мереж, а також використовувати методології та	**А1.К1.** Взаємодіяти з керівництвом, персоналом організації та партнерами стосовно проведення підготовчих робіт до процедур тестування або\чи тестування на проникнення систем кібербезпеки та захисту інформації. **А1.К2.** Інформувати керівництво та власника ресурсів, щодо готовності до тестування або\чи випробування ІС.	**А1.В1**. Готувати звіти та іншу інформацію про проведення підготовчих робіт до тестування або\чи тестування на проникнення систем захисту інформації в рамках поставлених повноважень та задач.

		вищому організаційному рівні. **А1.З3.** Політика інформаційної безпеки та\або кібербезпеки та План заходів захисту інформації, щодо сформовані відповідних вимог системи (політики) управління ризиками. **А1.З5.** Моделі системи безпеки (модель конфіденційності, цілісності та доступності (КЦД; модель Белла-Лападули; моделі забезпечення цілісності «Biba» і Кларка-Вілсона). **А1.З6.** Корпоративна архітектура безпеки інформації ІС та\або мережі. **А1.З7.** Вимоги до організації та проведення процедур тестування або\чи тестування на проникнення ІС в рамках чинного	методи забезпечення мережевої безпеки з метою встановлення напрямів та методів тестування ІС організації. **А1.У4.** Проводити аналіз апаратних та програмно-апаратних засобів, спеціального програмного забезпечення, комплексів засобів захисту інформаційних системи та\або мереж з метою встановлення напрямів, методів та інструментів тестування або\чи тестування на проникнення ІС організації. **А1.У5.** Проводити аналіз готовності до тестування або\чи випробування ІС.		

		законодавства та прийнятих в організації положень. **А1.38.** Обладнання та функції апаратного, програмно-апаратного та програмного забезпечення безпеки інформації та кіберзахисту ІС та\або мереж організації. **А1.39.** Концепції, методи та процедури адміністрування та захисту ІС та її активів з урахуванням операційних або\чи технологічних процесів системи. **А1.310.** Стандарти безпеки персональних даних (PII) та платіжних систем (PCI). **А1.311.**Принципи і методи формування та реалізації етичних хакерських атак (принципи етичного хакінгу). **А1.312.** Використовувані в			

		організації програми класифікації інформації і процедур розкриття.			
	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. Проведення робіт щодо процедур тестування систем кібербезпеки та захисту інформації на етапі розроблення та конфігурування інформаційних системи	**Б1**. Здатність використовувати інформаційні технології з метою розробки сучасних систем кібербезпеки та захисту інформації, а також забезпечення і організації процедур тестування 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 конфігурування вузлів, методи формування різних класів скриптів, системи доменних імен	**Б1.У1.** Розробляти та використовувати програмне забезпечення різних типів з метою реалізації в подальшому процедур тестування або\чи 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	**Б1.К1.** Взаємодіяти з керівництвом та відповідним персоналом з питань використання інформаційних технологій для розробки сучасних систем кібербезпеки та захисту інформації.	**Б1.В1.** Готувати інформацію доповіді, презентації) з напряму використання інформаційних технологій для розробки сучасних систем кібербезпеки та захисту інформації.

		(DNS) і послуг, що надаються Службою каталогів. **Б1.33.** Операційні системи різних типів (ОС Microsoft Windows, Unix\Linux, ОС Soláris, IOS, Android). **Б1.34** Методи та моделі статистичного аналізу даних та прийняття рішень. **Б1.35** Теорія, методи та моделі формування векторів кібербезпекових атак. **Б1.36** Теорія, структура, 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	конфігурування вузлів, системи доменних імен і послуг з метою реалізації в подальшому процедур тестування або\чи тестування на проникнення до ІС та її ресурсів. **Б1.У3.** Використовувати операційні системи різних типів Windows, Unix\Linux, ОС Soláris, IOS, Android) з метою реалізації в подальшому процедур тестування або\чи тестування на проникнення до ІС та її ресурсів.		

		інформаційних ресурсів ІС) .			
	Б2. Здатність виконувати процедури тестування або\чи тестування на проникнення до ІС (або АС, ІКС, СЕК) та її інформаційних ресурсів у процесі розробки та конфігурування.	**Б2.З1.** Процедури тестування або\чи тестування на проникнення до ІС та її інформаційних ресурсів у процесі розробки та конфігурування. **Б2.З2.** Джерела вразливостей та класифікація та етапи реалізації кіберзагроз інформаційним ресурсам. **Б2.З3** Конкретні операційні наслідки, що виникають у результаті реалізації кіберзагроз, збоїв системи або виникнення кіберінцидентів. **Б2.З4.** Процеси та сценарії тестування або\чи тестування на проникнення на основі	**Б2.У1**. Здійснювати процедури тестування або\чи тестування на проникнення до ІС та її інформаційних ресурсів у процесі розробки і конфігурування. **Б2.У2.** Розробляти сценарії тестування або\чи тестування на проникнення на основі знання архітектури інформаційної системи або мережі та її активів. **Б2.У3.** Розробляти сценарії тестування або\чи тестування на проникнення на основі методології, методів та засобів забезпечення мережевої безпеки.	**Б2.К1.** Взаємодіяти з керівництвом та відповідним персоналом з питань виконування процедури тестування або\чи тестування на проникнення до ІС та її інформаційних ресурсів у процесі розробки та конфігурування.	**Б2.В1.** Готувати інформацію доповіді, презентації) з напряму виконування процедури тестування або\чи тестування на проникнення ІС та її інформаційних ресурсів у процесі розробки та конфігурування **Б2.В2.** Готувати звіти за результатами виконування процедури тестування та оцінки стану безпеки ІС та її інформаційних

		різної методики та форм. **Б2.З5.** Процес оцінки стану безпеки інформації та тестування або\чи тестування на проникнення з урахуванням вразливостей інформаційних систем та її ресурсів.	**Б2.У4.** Розробляти сценарії тестування або\чи тестування на проникнення на основі джерел вразливостей інформаційних ресурсів, включно операційних систем різного типу, додатків, спеціалізованого програмного забезпечення. **Б2.У6.** Розробляти сценарії тестування або\чи тестування на проникнення на основі моделі побудови ІС OSI/ISO, а також типів і принципів використання протоколів обміну даними, методів динамічного конфігурування вузлів, системи доменних імен (DNS).		ресурсів у процесі розробки та конфігурування у відповідності до 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 роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				
В. Проведення тестування або\чи тестування на проникнення, оцінювання, а також супроводження операційних процесів ІС (або АС, ІКС, СЕК), програмного та/або апаратного забезпечення з метою визначення їх відповідності встановленим специфікаціям, нормам та вимогам.	**В1**. Здатність проводити тестування або\чи тестування на проникнення, оцінку та перевірку операційних процесів ІС (або АС, ІКС, СЕК), програмного та/або програмно-апаратного забезпечення на відповідність встановленим вимогам, нормам та характеристикам.	**В1.З1**. Поняття та загальний зміст програми та методики проведення процедур тестування або\чи тестування на проникнення 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 бізнес-операційних процесів та послуг ІС в сталому (робочому) стані, процедури їх контролю та забезпечення в межах визначених вимог та параметрів.	**В1.У1**. Реалізовувати Плани щодо проведення тестування або\чи тестування на проникнення до ІС державних органів, на підприємствах, в організаціях різних форм власності в рамках чинного законодавства. **В1.У2**. Визначення і впровадження процесів постановки завдань збору, обробки та розподілу даних, а також використання визначених вразливостей за відповідними напрямами для збору статистичних даних про ефективність використання	**В1.К1.** Взаємодіяти з керівництвом, персоналом та партнерами 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.	**В1.В1**. Розроблювати технічну документацію визначеного спрямування у відповідності до встановлених повноважень. **В1.В2.** Формувати звіти за напрямами проведеного тестування на вразливість у відповідності до встановлених повноважень.

		В1.З3. Процеси та методи підтримки програмного і апаратного забезпечення в робочому стані, процедури контролю їх працездатності в межах визначених параметрів та характеристик. **В1.З4.** Технологічне, техніко-економічне, комп'ютерне, програмне та інше забезпечення систем безпеки інформації та кіберзахисту ІС та її ресурсів.	впроваджених методів та засобів безпеки інформації та кіберзахисту. **В1.У3**. 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.У4.** Проектувати структури аналізу даних для їх подальшого тестування. **В1.У5.** Адаптувати методи та налаштовувати інструменти тестування або\чи		

			тестування на проникнення на проникнення у відповідності до операційних процесів ІС та інформаційних активів. **В1.У6.** Визначати вектори атак, виявляти і демонструвати використання технічних вразливостей систем безпеки інформації та\чи кібербезпеки в рамках чинного законодавства. **В1.У7.** Визначати, впроваджувати і виконувати дії з тестування на проникнення та реалізацію сценаріїв атак для оцінки ефективності впроваджених або запланованих заходів безпеки в рамках чинного законодавства.		

			В1.У8. Формувати звіти за напрямами проведеного тестування на вразливість.		
	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 тестування або\чи тестування на проникнення та оцінювання операційних процесів ІС, програмного та/або апаратного забезпечення з метою визначення їх відповідності встановленим специфікаціям і вимогам.	**Г1.** Здатність аналізувати результати тестування операційних процесів ІС, програмного та/або апаратного забезпечення або їх сумісності.	**Г1.З1**. Плани проведення тестування або\чи тестування на проникнення 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 тестування або\чи тестування на проникнення структури та топології інформаційних	**Г1.У2.** Визначати вимоги до інфраструктури тестування або\чи тестування на проникнення і оцінювання (співробітники, розподіл ролей, полігони, засоби, прилади). **Г1.У3.** Проводити аналіз результатів тестування або\чи тестування на проникнення структури та топології інформаційних системи та\або мереж ІС організації.	**Г1.К1.** Взаємодіяти з керівництвом організації, персоналом та партнерами стосовно аналізу проведення тестування або\чи тестування на проникнення, оцінки та перевірки операційних процесів ІС та її ресурсів. **Г1.К1**. Взаємодіяти з колегами та партнерами стосовно аналізу результатів тестування програмного, апаратного забезпечення та їх сумісності.	**Г1.В1.** Розроблювати технічну документацію за результатами аналізу результатів тестування та оцінювання відповідності операційних процесів ІС та їх ресурсів у відповідності до встановлених повноважень **Г1.В2.** Розроблювати звітну документацію щодо аналізу

		системи та\або мереж ІС організації. **Г1.З3**. План, методики та задачі проведення аналізу результатів тестування або\чи тестування на проникнення 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 тестування.	**Г1.У4.** Проводити аналіз результатів тестування або\чи тестування на проникнення 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 тестування ІС та її ресурсів.		процедур тестування у відповідності до 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	**Д1**. Здатність розробляти рекомендації на основі	**Д1.З1.** Поняття та загальний зміст Програми та методики	**Д1.У1.** Розробляти Програми та методики	**Д1.К1.** Взаємодіяти з керівництвом організації,	**Д1.В1.** Розроблювати звітну

основі результатів проведення процедур тестування або\чи тестування на проникнення ІС (або АС, ІКС, СЕК) та її інформаційних ресурсів.	проведення процедур тестування або\чи тестування на проникнення ІС (або АС, ІКС, СЕК) та її інформаційних ресурсів.	розробки рекомендацій на основі проведення процедур тестування ІС та її інформаційних ресурсів. **Д1.З2.** План реалізації Програми та методики розроблених рекомендацій, що створені на основі даних аналізу та виявлених вразливостей, недоліків при проведенні процедур тестування або\чи тестування на проникнення ІС та її інформаційних ресурсів.	рекомендацій на основі проведення процедур тестування або\чи 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 тестування в оціночні висновки та рекомендації.	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 аналізу та виявлених вразливостей.	документацію щодо реалізації Програми рекомендацій у відповідності до 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 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 тестування систем безпеки інформації та кіберзахисту ІС (або АС, ІКС, СЕК) та її ресурсів.	**Д2.З1.** Система 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.З4.** Корпоративну архітектуру організації в цілому та функціональні обов'язки кадрового складу організації в залежності від	**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 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 тестування та координації дій. **Д2.У4.** Консультувати	**Д2.К1.** Взаємодіяти з керівництвом, персоналом організації та партнерами стосовно координації робіт з реалізації процедур тестування систем безпеки інформації та кіберзахисту 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 тестування та координації дій.	**А1.В1**. Готувати документацію, програми тренінгів та іншу інформацію про координацію робіт з реалізації процедур тестування в рамках вставлених повноважень та задач.

		покладених повноважень у сфері безпеки інформації та\або кібербезпеки. **Д2.35.** Методику проведення консультації та тренінгів пов’язаних з використанням ІТ та їх безпеки в організації, питань тестування або\чи тестування на проникнення до ІС та їх ресурсів .	керівництво та персонал організації, проводити тренінги щодо питань тестування інформаційних систем та технологій у відповідності до вітчизняної та світової нормативно-правової бази, стандартів та кращих світових практик.		
	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**		
	молодший фахівець з тестування систем захисту інформації	**фахівець з тестування систем захисту інформації**	**провідний фахівець з тестування систем захисту інформації**
	повна	повна	повна
А	+	+	+
Б	+	+	+
В	+	+	+
Г	-	+	+
Д	-	-	+

VII. Відомості про розроблення та затвердження професійного стандарту

1. Повне найменування розробник апрофесійного стандарту

Державної служби спеціального зв'язку та захистуінформації України

Склад робочоїгрупи/Учасникиробочоїгрупи:

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 (за згодою);

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(за згодою);

ФІЛІПОВА Ольга, комерційний директор компанії SAYCOM (за згодою);

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

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

3. Реквізити висновку суб'єкта перевірки про дотримання вимог Порядку розроблення, введення в дію та перегляду професійних стандартівпід 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 внесення професійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.