Прим. № __

ЗАТВЕРДЖЕНО

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

# ПРОФЕСІЙНИЙ СТАНДАРТ

# ФАХІВЕЦЬ З ТЕСТУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

_____

(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 «Фахівець з тестування систем захисту інформації» 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 «Фахівець з тестування систем захисту інформації» 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

Фахівець з тестування систем захисту інформації.

## II. Загальні відомості про професійний стандарт

### 1. Мета діяльності за професією

Планування, підготовка та проведення тестування або тестування на проникнення до інформаційних систем/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 стану захищеності інформаційних систем/мереж та стану кібербезпеки на відповідність стандартам, специфікаціям, нормам, вимогам та заявленим технічним характеристикам.

Проведення аналізу й звітування щодо результатів тестування, розроблення рекомендацій з виявлення та оцінки відхилень у функціонуванні операційних процесів, а також звітування щодо 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 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** | |
| **Секція P** | Освіта | **Розділ 85** | Освіта | **Група 85.5** | Інші види освіти |
| | | | | **Клас 85.59** | Інші види освіти, не введенні в інші угрупування |

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

Фахівець з тестування систем захисту інформації 2139.2.

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

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**

● 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 «Фахівець з тестування систем захисту інформації»;

● 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).

## III. 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** |
| Молодший фахівець з тестування систем захисту інформації | Підготовка на першому рівні вищої освіти (бакалаврському) за спеціальностями, вказаними у **П.*** | *Не передбачено професійним стандартом* |
| Фахівець з тестування систем захисту інформації | Підготовка на першому рівні вищої освіти (бакалаврському) за спеціальностями, вказаними у **П.*** за умови наявності стажу роботи за однією з професій відповідного спрямування не менше 2 років або на другому (магістерському) рівні вищої освіти за спеціальностями, вказаними в у **П.***. | *Не передбачено професійним стандартом* |
| Провідний фахівець з тестування систем захисту інформації | Підготовка на другому (магістерському) рівні вищої освіти за спеціальностями, вказаними в у **П.*** за умови наявності стажу роботи за однією з професій відповідного спрямування не менше 3 років. | *Не передбачено професійним стандартом* |

**П.***

● диплом на першому (бакалаврському) рівні вищої освіти за спеціальністю:

- 121 «Інженерія програмного забезпечення» галузі знань 12 «Інформаційні технології» (6 рівень НРК);
- 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології» (6 рівень НРК);
- 123 «Комп'ютерна інженерія» галузі знань 12 «Інформаційні технології»
(6 рівень НРК);
- 124 «Системний аналіз» 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);
- 254 «Забезпечення військ (сил)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (6 рівень НРК);
- 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» (6 рівень НРК).

● 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** |
| Фахівець з тестування систем захисту інформації | Підвищення кваліфікації «Фахівець 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* |

**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**

| | |
|---|---|
| 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 |
| АС | Автоматизованих систем |
| ІКС | Інформаційно-комунікаційних систем |
| СЕК | Систем електронних комунікацій |
| ІТ | Інформаційні технології |
| ІС | Інформаційна система |

## V. Опис трудових функцій

| Трудові функції | Компетентності | Результати навчання | | | |
|---|---|---|---|---|---|
| | | **Знання** | **Уміння/навички** | **Комунікація** | **Відповідальність і автономія** |
| **А.** Проведення підготовчих робіт щодо процедур тестування та/або 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 та/або 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.** Законодавчу та нормативно-правову базу, стандарти, нормативні акти, політики та етичні норми, пов'язані з кібербезпекою та захистом інформації в ІС та організації в цілому.<br>**А1.З2.** Концепції та/або Програми побудови інформаційних системи та/або мереж, а також методології, методи та засоби забезпечення мережевої безпеки.<br>**А1.З3.** Стратегію та місію системи менеджменту безпеки інформації та кіберзахисту інформаційних ресурсів, прийнятих на вищому організаційному рівні.<br>**А1.З4.** Політику інформаційної безпеки та/або кібербезпеки та План заходів захисту інформації щодо сформованих відповідних вимог системи | **А1.У1.** Визначати необхідний рівень складності тесту для конкретної системи та згідно встановлених задач для проведення тестування.<br>**А1.У2.** Розробляти та реалізовувати Плани підготовки щодо проведення тестування та/або тестування на проникнення у ІС державних органів, на підприємствах, в організаціях різних форм власності в рамках чинного законодавства.<br>**А1.У3.** Проводити аналіз структури та топології інформаційних систем та/або мереж, а також використовувати методології та методи забезпечення мережевої | **А1.К1.** Взаємодіяти з керівництвом, персоналом організації та партнерами стосовно проведення підготовчих робіт до процедур тестування та/або тестування на проникнення систем кібербезпеки та захисту інформації.<br>**А1.К2.** Інформувати керівництво та власника ресурсів щодо готовності до тестування та/або випробування ІС. | **А1.В1.** Готувати звіти та іншу інформацію про проведення підготовчих робіт до тестування та/або тестування на проникнення систем захисту інформації в межах встановлених повноважень та задач. |

| Трудові функції | Компетентності | Результати навчання | | | |
|---|---|---|---|---|---|
| | | **Знання** | **Уміння/навички** | **Комунікація** | **Відповідальність і автономія** |
| | | (політики) управління ризиками.<br>**А1.35.** Формальні моделі безпеки: тріада кібербезпеки CIA (конфіденційність, цілісність, доступність), гексада Паркера, модель Бела-ЛаПадули (мандатного доступу), модель Біби (забезпечення цілісності даних), модель Кларка-Вілсона.<br>**А1.36.** Корпоративну архітектуру інформаційної безпеки та кіберзахисту ІС та мереж (АС, ІКС, СЕК)<br>**А1.37.** Вимоги до організації та проведення процедур тестування та/або тестування на проникнення ІС в рамках чинного законодавства та прийнятих в організації положень.<br>**А1.38.** Обладнання та функції апаратного, програмно-апаратного та програмного забезпечення | безпеки з метою встановлення напрямів та методів тестування ІС організації.<br>**А1.У4.** Проводити аналіз апаратних та програмно-апаратних засобів, спеціального програмного забезпечення, комплексів засобів захисту інформаційних систем та/або мереж з метою встановлення напрямів, методів та інструментів тестування та/або тестування на проникнення ІС організації.<br>**А1.У5.** Проводити аналіз готовності до тестування та/або випробування ІС. | | |

| Трудові функції | Компетентності | Результати навчання | | | |
|---|---|---|---|---|---|
| | | **Знання** | **Уміння/навички** | **Комунікація** | **Відповідальність і автономія** |
| | | інформаційної безпеки та кіберзахисту ІС та/або мереж організації.<br>**А1.39.** Концепції, методи та процедури адміністрування та захисту ІС та її активів з урахуванням операційних та/або технологічних процесів системи.<br>**А1.310.** Стандарти безпеки персональних даних (PII) та платіжних систем (PCI).<br>**А1.311.** Принципи і методи формування та реалізації етичних хакерських атак (принципи етичного хакінгу).<br>**А1.312.** Використовувані в організації програми класифікації інформації і процедур розкриття. | | | |
| | **Предмети та засоби праці:**<br>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** |
| **Б.** Проведення робіт щодо процедур тестування систем кібербезпеки та захисту інформації на етапі розроблення та конфігурування інформаційних систем. | **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).<br>**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 (DNS) і послуг, що надаються Службою каталогів.<br>**Б1.З3.** Операційні системи різних типів (ОС Microsoft Windows, Unix/Linux, ОС Soláris, IOS, Android).<br>**Б1.З4.** Методи та моделі статистичного аналізу даних та прийняття рішень. | **Б1.У1.** Розробляти та використовувати програмне забезпечення різних типів з метою реалізації в подальшому процедур тестування та/або тестування на проникнення до ІС та її ресурсів.<br>**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 тестування та/або тестування на проникнення до ІС та її ресурсів.<br>**Б1.У3.** Використовувати операційні системи | **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. |

| Трудові функції | Компетентності | Результати навчання | | | |
|---|---|---|---|---|---|
| | | **Знання** | **Уміння/навички** | **Комунікація** | **Відповідальність і автономія** |
| | | **Б1.35.** Теорію, методи та моделі формування векторів кібербезпекових атак. **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) . | різних типів (Windows, Unix/Linux, ОС Soláris, IOS, Android) з метою реалізації в подальшому процедур тестування та/або тестування на проникнення до ІС та її ресурсів. | | |
| | **Б2.** Здатність виконувати процедури тестування та/або тестування на проникнення до ІС (або АС, ІКС, СЕК) та її інформаційних ресурсів у процесі розробки та конфігурування. | **Б2.З1.** Процедури тестування та/або тестування на проникнення до ІС та її інформаційних ресурсів у процесі розробки та конфігурування. **Б2.З2.** Джерела вразливостей та класифікацію та етапи реалізації кіберзагроз інформаційним ресурсам. | **Б2.У1.** Здійснювати процедури тестування та/або тестування на проникнення до ІС та її інформаційних ресурсів у процесі розробки і конфігурування. **Б2.У2.** Розробляти сценарії тестування та/або тестування на проникнення на основі знання архітектури | **Б2.К1.** Взаємодіяти з керівництвом та відповідним персоналом з питань виконання процедури тестування та/або тестування на проникнення до ІС та її інформаційних ресурсів у процесі | **Б2.В1.** Готувати інформацію, доповіді, презентації з напряму виконання процедури тестування та/або тестування на проникнення ІС та її інформаційних |

| Трудові функції | Компетентності | Результати навчання | | | |
|---|---|---|---|---|---|
| | | **Знання** | **Уміння/навички** | **Комунікація** | **Відповідальність і автономія** |
| | | **Б2.З3.** Конкретні операційні наслідки, що виникають у результаті реалізації кіберзагроз, збоїв системи або виникнення кіберінцидентів.<br>**Б2.З4.** Процеси та сценарії тестування та/або тестування на проникнення на основі різної методики та форм.<br>**Б2.З5.** Процес оцінки стану безпеки інформації та тестування та/або тестування на проникнення з урахуванням вразливостей інформаційних систем та її ресурсів. | інформаційної системи або мережі та її активів.<br>**Б2.У3.** Розробляти сценарії тестування та/або тестування на проникнення на основі методології, методів та засобів забезпечення мережевої безпеки.<br>**Б2.У4.** Розробляти сценарії тестування та/або тестування на проникнення на основі джерел вразливостей інформаційних ресурсів, зокрема операційних систем різного типу, додатків, спеціалізованого програмного забезпечення.<br>**Б2.У5.** Розробляти сценарії тестування та/або тестування на проникнення на основі моделі побудови ІС OSI/ISO, а також типів і принципів використання | розробки та конфігурування. | ресурсів у процесі розробки та конфігурування<br>**Б2.В2.** Готувати звіти за результатами виконання процедури тестування та оцінки стану безпеки ІС та її інформаційних ресурсів у процесі розробки та конфігурування у відповідності до встановлених повноважень. |

| Трудові функції | Компетентності | Результати навчання | | | |
|---|---|---|---|---|---|
| | | **Знання** | **Уміння/навички** | **Комунікація** | **Відповідальність і автономія** |
| | | | протоколів обміну даними, методів динамічного конфігурування вузлів, системи доменних імен (DNS). | | |
| | **Предмети та засоби праці:**<br>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 та/або 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 та/або тестування на проникнення, оцінку та перевірку операційних процесів ІС (або АС, ІКС, СЕК), програмного та/або програмно-апаратного забезпечення на відповідність встановленим | **В1.З1.** Поняття та загальний зміст програми та методики проведення процедур тестування та/або тестування на проникнення ІС та мереж, а також апаратного, програмно-апаратного та програмного забезпечення сталих операційних процесів та систем безпеки інформації і кіберзахисту.<br>**В1.З2.** Процеси та методи підтримки бізнес-операційних процесів та послуг ІС в сталому | **В1.У1**. Реалізовувати Плани щодо проведення тестування та/або тестування на проникнення до ІС державних органів, на підприємствах, в організаціях різних форм власності в рамках чинного законодавства.<br>**В1.У2.** Визначати і впроваджувати процеси постановки завдань збору, обробки та розподілу даних, а | **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.<br>**В1.К2.** Взаємодіяти з колегами та | **В1.В1.** Розробляти технічну документацію визначеного спрямування у відповідності до встановлених повноважень.<br>**В1.В2.** Формувати звіти за напрямами проведеного тестування на вразливість у відповідності до встановлених повноважень. |

| Трудові функції | Компетентності | Результати навчання | | | |
|---|---|---|---|---|---|
| | | **Знання** | **Уміння/навички** | **Комунікація** | **Відповідальність і автономія** |
| | вимогам, нормам та характеристикам. | (робочому) стані, процедури їх контролю та забезпечення в межах визначених вимог та параметрів.<br>**В1.33.** Процеси та методи підтримки програмного і апаратного забезпечення в робочому стані, процедури контролю їх працездатності в межах визначених параметрів та характеристик.<br>**В1.34.** Технологічне, техніко-економічне, комп'ютерне, програмне та інше забезпечення систем безпеки інформації та кіберзахисту ІС та її ресурсів. | також використовувати визначені вразливості за відповідними напрямами для збору статистичних даних про ефективність використання впроваджених методів та засобів безпеки інформації та кіберзахисту.<br>**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). | партнерами стосовно проведення тестування та/або тестування на проникнення, оцінки та перевірки операційних процесів ІС та її ресурсів з метою забезпечення сталих бізнес-операційних процесів. | |

| Трудові функції | Компетентності | Результати навчання | | | |
|---|---|---|---|---|---|
| | | Знання | Уміння/навички | Комунікація | Відповідальність і автономія |
| | | | **В1.У4.** Проектувати структури аналізу даних для їх подальшого тестування.<br>**В1.У5.** Адаптувати методи та налаштовувати інструменти тестування та/або тестування на проникнення у відповідності до операційних процесів ІС та інформаційних активів.<br>**В1.У6.** Визначати вектори атак, виявляти і демонструвати використання технічних вразливостей систем безпеки інформації та/або кібербезпеки в рамках чинного законодавства.<br>**В1.У7.** Визначати, впроваджувати і виконувати дії з тестування на проникнення та | | |

| Трудові функції | Компетентності | Результати навчання | | | |
|---|---|---|---|---|---|
| | | Знання | Уміння/навички | Комунікація | Відповідальність і автономія |
| | | | 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 та/або тестування на проникнення та оцінювання операційних процесів ІС, програмного та/або апаратного забезпечення з метою визначення їх відповідності | **Г1.** Здатність аналізувати результати тестування операційних процесів ІС, програмного та/або апаратного забезпечення або їх сумісності. | **Г1.З1.** Плани проведення тестування та/або 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 | **Г1.У1.** Визначати вимоги до інфраструктури тестування та/або тестування на проникнення, а також визначати процедури оцінювання. **Г1.У2.** Проводити аналіз результатів тестування та/або | **Г1.К1.** Взаємодіяти з керівництвом організації, персоналом та партнерами стосовно аналізу проведення тестування та/або тестування на проникнення, оцінки та перевірки | **Г1.В1.** Розробляти технічну документацію за результатами аналізу процедур тестування та оцінювання на відповідність операційних процесів ІС, їх ресурсів згідно з |

| Трудові функції | Компетентності | Результати навчання | | | |
|---|---|---|---|---|---|
| | | **Знання** | **Уміння/навички** | **Комунікація** | **Відповідальність і автономія** |
| встановленим специфікаціям і вимогам. | | результатів тестування та/або тестування на проникнення структури та топології інформаційних систем та/або мереж ІС організації.<br>**Г1.З3.** План, методики та задачі проведення аналізу результатів тестування та/або тестування на проникнення апаратних та програмно-апаратних засобів, спеціального програмного забезпечення, комплексів засобів захисту інформаційних системи та/або мереж.<br>**Г1.З4.** Методику та задачі формування звітності щодо аналізу результатів тестування. | тестування на проникнення структури та топології інформаційних системи та/або мереж ІС організації.<br>**Г1.У3.** Проводити аналіз результатів тестування та/або 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.<br>**Г1.У4.** Збирати, перевіряти і підтверджувати дані тестування ІС та її ресурсів. | операційних процесів ІС та її ресурсів.<br>**Г1.К2**. Взаємодіяти з колегами та партнерами стосовно аналізу результатів тестування програмного, апаратного забезпечення та їх сумісності. | встановленими повноваженнями<br>**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:**<br>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 процедур тестування та/або тестування на проникнення ІС (або АС, ІКС, СЕК) та її інформаційних ресурсів. | **Д1.** Здатність розробляти рекомендації на основі проведення процедур тестування та/або тестування на проникнення ІС (або АС, ІКС, СЕК) та її інформаційних ресурсів. | **Д1.З1.** Поняття та загальний зміст Програми та методики розробки рекомендацій на основі проведення процедур тестування ІС та її інформаційних ресурсів.<br>**Д1.З2.** План реалізації Програми та методики розроблених рекомендацій, що створені на основі даних аналізу та виявлених вразливостей, недоліків при проведенні процедур тестування та/або тестування на проникнення ІС та її інформаційних ресурсів. | **Д1.У1.** Розробляти Програми та методики рекомендацій на основі проведення процедур тестування та/або тестування на проникнення ІС та її інформаційних ресурсів.<br>**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.<br>**Д1.У3.** Переводити дані і результати тестування | **Д1.К1.** Взаємодіяти з керівництвом організації, персоналом та партнерами стосовно розроблення та інформування про розроблені рекомендації.<br>**Д1.К2.** Взаємодіяти з колегами та партнерами стосовно реалізації плану Програми рекомендацій, що створені на основі даних аналізу та виявлених 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** |
| | | | в оціночні висновки та рекомендації. | | |
| | **Д2.** Здатність здійснювати координацію робіт з реалізації процедур тестування систем безпеки інформації та кіберзахисту ІС (або АС, ІКС, СЕК) та її ресурсів. | **Д2.З1.** Систему менеджменту інформаційної безпеки та повний перелік бізнес-операційних процесів організації.<br>**Д2.З2.** Концепції архітектури безпеки організації, розподілу доступу та еталонних моделей архітектури підприємства (Zachman, FEA).<br>**Д2.З3.** Концепцію управління ресурсами, змінами конфігурації, забезпеченням інформаційної системи та/або мережі.<br>**Д2.З4.** Концепцію та методи управління персоналом в ІТ компанії.<br>**Д2.З5.** Корпоративну архітектуру організації в цілому та функціональні обов'язки кадрового складу | **Д2.У1.** Організовувати та здійснювати координацію робіт з реалізації процедур тестування систем безпеки інформації та кіберзахисту ІС (або АС, ІКС, СЕК) та її ресурсів.<br>**Д2.У2.** Визначати необхідний рівень розподілу та складності задач згідно з посадовими інструкціями персоналу відповідно до конкретного операційного процесу ІС та організації в цілому.<br>**Д2.У3.** Визначати рівень взаємозв'язку між підрозділами та персоналом з метою ефективної реалізації | **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.<br>**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. | **Д2.В1.** Готувати документацію, програми тренінгів та іншу інформацію про координацію робіт з реалізації процедур тестування в рамках встановлених повноважень та задач. |

| Трудові функції | Компетентності | Результати навчання | | | |
|---|---|---|---|---|---|
| | | **Знання** | **Уміння/навички** | **Комунікація** | **Відповідальність і автономія** |
| | | організації в залежності від покладених повноважень у сфері безпеки інформації та/або кібербезпеки.<br>**Д2.З6.** Методику проведення консультації та тренінгів, пов'язаних з використанням ІТ та їх безпекою в організації, питаннями тестування та/або тестування на проникнення до ІС та їх ресурсів . | процедур тестування та координації дій.<br>**Д2.У4.** Консультувати 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:**<br>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 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 Держспецзв'язку;

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 «Фахівець з тестування систем захисту інформації» 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 «Фахівець з тестування систем захисту інформації» 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