**Проєкт**

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

# Професійний стандарт

## ФАХІВЕЦЬ З ПІДТРИМКИ ІНФРАСТРУКТУРИ КІБЕРЗАХИСТУ

_____(дата внесення до Реєстру кваліфікацій)

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

Професійний стандарт розроблено та затверджено згідно з вимогами статті 42 Кодексу законів про працю України на підставі:

- висновку суб'єкта перевірки – Національного агентства кваліфікацій від _____ про дотримання під 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**

Фахівець з підтримки інфраструктури кіберзахисту

**ІІ. Загальні відомості про професійний стандарт**

**1. Мета діяльності за професією**

Тестування, впровадження, розгортання, підтримка та адміністрування інфраструктурного обладнання та програмного забезпечення кіберзахисту

**2. Назва виду (видів) економічної діяльності, секції, розділу, групи, класу економічної діяльності та їх код згідно з Національним класифікатором України ДК 009:2010 «Класифікація видів економічної діяльності»**

| | | | | | |
|---|---|---|---|---|---|
| **Секція J** | Інформація та телекомунікації | **Розділ 61** | Телекомунікації (електрозв'язок) | **Група 61.1** | Діяльність у сфері проводового електрозв'язку |
| | | | | **Клас 61.10** | Діяльність у сфері проводового електрозв'язку |
| | | | | **Група 61.2** | Діяльність у сфері безпроводового електрозв'язку |
| | | | | **Клас 61.20** | Діяльність у сфері безпроводового електрозв'язку |
| | | | | **Група 61.3** | Діяльність у сфері супутникового електрозв'язку |
| | | | | **Клас 61.30** | Діяльність у сфері супутникового електрозв'язку |
| | | | | **Група 61.9** | Інша діяльність у сфері електрозв'язку |
| | | | | **Клас 61.90** | Інша діяльність у сфері електрозв'язку |
| | | **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, не введенні в інші угрупування |
| | | | | **Клас 74.90** | Інша професійна, наукова та технічна діяльність, не введенні в інші угрупування |
| **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 професії та код підкласу професії згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій»**

Фахівець з підтримки інфраструктури кіберзахисту 2139.2

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

Молодший фахівець з підтримки інфраструктури кіберзахисту, 6 рівень НРК;

Фахівець з підтримки інфраструктури кіберзахисту, 7 рівень НРК;

Провідний фахівець з підтримки інфраструктури кіберзахисту, 7 рівень НРК

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

- диплом на першому (бакалаврському) або другому (магістерському) рівні вищої освіти за спеціальністю:

- 121 «Інженерія програмного забезпечення» галузі знань 12 «Інформаційні технології» (6 або 7 рівень НРК);

- 122 «Комп’ютерні науки» галузі знань 12 «Інформаційні технології» (6 або 7 рівень НРК);

- 123 «Комп'ютерна інженерія» галузі знань 12 «Інформаційні технології» (6 або 7 рівень НРК);

- 124 «Системний аналіз» галузі знань 12 «Інформаційні технології» (6 або 7 рівень НРК);

- 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» (6 або 7 рівень НРК);

- 126 «Інформаційні системи та технології» галузі знань 12 «Інформаційні технології» (6 або 7 рівень НРК);

- 172 «Електронні комунікації та радіотехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (6 або 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 підтримки інфраструктури кіберзахисту;
- 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 підтримки інфраструктури кіберзахисту;
- документ (диплом, сертифікат, тощо), щодо професійної сертифікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері підтримки інфраструктури кіберзахисту.

## 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** | |
|---|---|---|
| | **Кваліфікаційні центри** | **Суб'єкти освітньої діяльності** |
| Молодший фахівець з підтримки інфраструктури кіберзахисту | Підготовка на першому рівні вищої освіти (бакалаврському) за спеціальностями, вказаними у п. 5, галузі знань 12 «Інформаційні технології» та 17 «Електроніка, автоматизація та електронні комунікації» | *Не передбачено професійним стандартом* |

| | | |
|---|---|---|
| Фахівець з підтримки інфраструктури кіберзахисту | Підготовка на другому рівні вищої освіти (магістерському) за спеціальностями вказаними у п.5, галузі знань 12 «Інформаційні технології» та 17 «Електроніка, автоматизація та електронні комунікації» або стаж роботи за однією з професій відповідного спрямування повинен складати не менше 3 років (молодший фахівець з підтримки інфраструктури кіберзахисту, аналітик з безпеки інформаційно-телекомунікаційних систем, фахівець з питань безпеки (інформаційно-комунікаційні технології), фахівець сфери захисту інформації тощо) | *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 визнання професійних кваліфікацій** | |
|---|---|---|
| | **Кваліфікаційні центри** | **Суб'єкти освітньої діяльності** |
| Провідний фахівець з підтримки інфраструктури кіберзахисту | Підвищення кваліфікації для фахівця з підтримки інфраструктури кіберзахисту для отримання професійної кваліфікації "провідний фахівець інфраструктури кіберзахисту". Стаж роботи не менше двох років. | *Не передбачено професійним стандартом* |

## IV. Абревіатури, скорочення

| | |
|---|---|
| IT | інформаційні технології |
| ОС | операційна система |
| ПЗ | програмне забезпечення |
| IDS | Intrusion Detection System |
| IPS | Intrusion Prevention System |
| SIEM | Security information and event management |
| DNS | Domain Name System |
| TCP/IP | Transmission Control Protocol/ Internet Protocol |
| EBSCO | Elton Bryson Stephens Company |
| JSTOR | Journal Storage |
| VPN | Virtual private network |
| NIPS | Network-Based Intrusion Prevention System |
| HIPS | Host Intrusion Prevention System |
| ISO | International Organization for Standardization |
| OSI | Open Systems Interconnection model |
| CIS CSC | Center for Internet Security Critical Security Controls |
| NIST SP 800-53 | National Institute of Standards and Technology Special Publication 800-53 |
| ITIL | Information Technology Infrastructure Library |
| CMMI | Capabilities and Maturity Model Integration |
| RFID | Radio Frequency IDentification |
| IR | Infrared Radiation |
| VoIP | Voice over Internet Protocol |
| RMF | Risk Management Framework |
| SA&A | Security Assessment and Authorization |

## V. Опис трудових функцій

| Трудові функції | Компетентності | Результати навчання | | | |
|---|---|---|---|---|---|
| | | **Знання** | **Уміння/навички** | **Комунікація** | **Відповідальність і автономія** |
| **А.** Встановлення та налагодження спеціального обладнання та програмного забезпечення для кіберзахисту. | **А1.** Здатність встановлювати та налагоджувати спеціальне обладнання та програмне забезпечення для кіберзахисту. | **А1.З1.** Інструменти та прикладне програмне забезпечення системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS).<br>**А1.З2.**Інфраструктурне обладнання та програмне забезпечення.<br>**А1.З3.** SIEM-система.<br>**А1.З4.** Антивірусне ПЗ.<br>**А1.З5.** Міжмережеві екрани. | **А1.У1.**Здійснювати налаштування датчиків.<br>**А1.У2.** Здійснювати встановлення та налаштування інструментів та прикладного програмного забезпечення системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS).<br>**А1.У3.** Здійснювати встановлення та налаштування SIEM-системи.<br>**А1.У4.** Здійснювати встановлення та налаштування антивірусного ПЗ.<br>**А1.У5.** Здійснювати встановлення та налаштування міжмережевого екрану. | **А1.К1.** Надавати вказівки та брати участь у розробленні настанов для фахівців, залучених до підтримки інфраструктури кіберзахисту. | **А1.В1.** Розроблювати і застосовувати методи моделювання систем спеціального обладнання та програмного забезпечення для кіберзахисту. |

| | | | | | |
|---|---|---|---|---|---|
| | **А2.** Здатність до аналізу мережевого трафіку для захисту мережевих комунікацій. | **А2.З1.** Концепції і протоколи комп'ютерних мереж, а також методології забезпечення мережевої безпеки.<br>**А2.З2.**Технології проведення мережевих атак та зв'язок між мережевими атаками і загрозами та вразливостями.<br>**А2.З3.**Мережеві протоколи (TCP/IP, динамічного конфігурування вузлів, системи доменних імен (DNS)) і послуги, що надаються Службою каталогів.<br>**А2.З4.** Інструменти, методології, процеси аналізу мережевого трафіку. | **А2.У1.** Виконувати захист мережевих комунікацій.<br>**А2.У2.** Характеризувати та аналізувати мережевий трафік з метою виявлення аномальної активності та потенційних загроз мережевим ресурсам.<br>**А2.У3.** Перехоплювати та аналізувати мережевий трафік, пов'язаний з шкідливими діями, використовуючи засоби моніторингу мережі. | **А2.К1**. Приймати участь у підтримці діяльності групи реагування на кіберінциденти з використанням програмного та технічного забезпечення кіберзахисту. | **А2.В1**. Проводити оцінювання ефективності існуючих програм, процесів і вимог щодо аналізу мережевого трафіку. |
| | **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. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **Б.** Здійснення системного адміністрування спеціалізованих програм та систем кіберзахисту або пристроїв віртуальної приватної мережі (VPN), включаючи встановлення, налаштування, обслуговування, резервне копіювання та відновлення. | **Б1**.Здатність встановлювати, налаштовувати, обслуговувати, а також здійснювати резервне копіювання та відновлення. | **Б1.З1.**Методики та інструменти резервного копіювання та відновлення даних.<br>**Б1.З2.** Концепції резервного копіювання та відновлення даних. | **Б1.У1.** Здійснювати підтримку баз даних (резервне копіювання, відновлення, видалення даних, файлів лог-журналу, тощо.<br>**Б1.У2**. Здійснювати адміністрування ОС (ведення облікових записів, резервне копіювання та відновлення даних файлів лог-журналу тощо). | **Б1.К1**. Приймати участь у відновленні працездатності системи. | **Б1.В1**. Розробляти та впроваджувати процедури резервного копіювання та відновлення спеціалізованого програмного забезпечення кіберзахисту. |
| | **Б2.** Здатність до системного адміністрування спеціалізованих програм і систем кіберзахисту. | **Б2.З1**. Протоколи взаємодії відкритих систем (ISO/OSI), бібліотека інфраструктури інформаційних технологій, поточна версія [ITIL]).<br>**Б2.З2**.Методики та інструменти аналізу на мережевому (пакетному) рівні<br>**Б2.З3.**Концепції архітектури безпеки мережі, включаючи топологію, протоколи, | **Б2.У1**.Здійснювати захист мережі від шкідливого ПЗ (наприклад, NIPS/HIPS, захист від шкідливого ПЗ, обмеження/запобіган-ня впливу зовнішніх пристроїв, фільтрацію спаму).<br>**Б2.У2**. Застосовувати концепції архітектури безпеки мереж, включаючи топологію, протоколи, компоненти і принципи (наприклад, | **Б2.К1**.Приймати участь у зборі та аналізі артефактів вторгнення. | **Б2.В1.**Проводити оцінювання ефективності існуючих спеціалізованих програм і систем кіберзахисту та надавати пропозиції керівництву щодо підвищення ефективності їх застосування. |

| | | | | | |
|---|---|---|---|---|---|
| | | компоненти і принципи (наприклад, прикладна система ешелонованого захисту). | застосунки з «ешелонованим захистом). | | |
| | **Б3.**Здатність до системного адміністрування засобів віртуальної приватної мережі (VPN). | **Б3.З1.**Технології та інструменти безпеки віртуальних приватних мереж (VPN).<br>**Б3.З2.** Приховані технології (VPN тощо). | **Б3.У1**.Використовувати засоби віртуальних приватних мереж (VPN) і шифрування. | **Б3.К1.** Розроблювати вказівки і настанови для працівників, залучених до системного адміністрування засобів віртуальної приватної мережі. | **Б3.В1.** Проводити оцінювання ефективності існуючих технологій та інструментів безпеки віртуальних приватних мереж (VPN) та інтерпретувати результати аналізу керівництву. |
| | **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.** Формування, редагування і управління списками контролю доступу до мережі у спеціалізованих системах кіберзахисту. | **В1**.Здатність формувати, редагувати і управляти списками контролю доступу до мережі у спеціалізованих системах кіберзахисту. | **В1.З1.**Кіберзагрози та вразливості.<br>**В1.З2**.Механізми контролю доступу до хостів /мереж (наприклад, списки контролю доступу, списки повноважень). | **В1.У1**.Здійснювати контроль доступу до хосту /мережі (наприклад, список контролю доступу).<br>**В1.У2.**Застосувати техніки підвищення вимог до системи, мережі і ОС | **В1.К1.** Приймати участь у впровадженні системи безпеки (формувати, редагувати списки контролю | **В1.В1.** Інтерпретувати та застосовувати закони, нормативні акти, політики, стандарти чи процедури з інформаційної безпеки та |

| | | | | | |
|---|---|---|---|---|---|
| | | | (наприклад, виключення незатребуваних послуг, парольних політик, сегментація мережі, використання журналу реєстрації, мінімум привілеїв тощо). | доступу та повноважень). | кіберзахисту щодо механізмів контролю доступу до хостів/мереж. |
| | **В2.** Здатність застосовувати списки контролю доступу до мережі у спеціалізованих системах кіберзахисту. | **В2.З1.** Політики, процедури і нормативні акти з інформаційної безпеки та кіберзахисту.<br>**В2.З2.** Знання методів автентифікації, авторизації та контролю доступу. | **В2.У1.** Застосовувати засоби контролю доступу в системах безпеки.<br>**В2.У2.** Розробляти групові політики та переліки контролю доступу для забезпечення відповідності стандартам організації, бізнес-правилам та потребам. | **В2.К1.** Приймати участь в організації процесів і процедур контролю доступу до мережі. | **В2.В1.** Проводити оцінювання ефективності застосування списків контролю доступу до мережі та інтерпретувати результати аналізу керівництву. |
| **Г.** Приймати участь у визначенні, встановленні пріоритетів та координації захисту критично важливих об'єктів, | **Г1**. Здатність визначати та встановлювати пріоритети захисту критично важливих об’єктів, інфраструктури та ключових ресурсів кіберзахисту. | **Г1.З1.**Закони, нормативні акти, політики і етичні норми та їх взаємозв’язки з кібербезпекою і приватністю.<br>**Г1.З2.**Принципи кібербезпеки і приватності. | **Г1.У1.**Застосовувати принципи кібербезпеки і приватності при формуванні організаційних вимог (які стосуються конфіденційності, цілісності, | **Г1.К1**. Приймати участь у формуванні вимог організації (стосовно конфіденційності, цілісності, | **Г1.В1.** Інтерпретувати та застосовувати закони, нормативні акти, політики, стандарти чи процедури до питань визначення та встановлення |

| | | | | | |
|---|---|---|---|---|---|
| інфраструктури та ключових ресурсів кіберзахисту. | | | доступності, автентифікації і неспростовності).<br>**Г1.У2**. Здійснювати моніторинг змін у нормативно-правових документах відповідного спрямування.<br>**Г1.У3.** Формувати й оновлювати базу знайдених матеріалів для подальшого її використання в роботі. | доступності, автентифікації і неспростовності | пріоритетів захисту критично-важливих об'єктів інфраструктури. |
| | **Г2.**Здатність координувати захист критично важливих об'єктів, інфраструктури та ключових ресурсів кіберзахисту. | **Г2.З1.** Принципи і методи кібербезпеки та приватності, а також організаційні вимоги (щодо забезпечення конфіденційності, цілісності, доступності, автентифікації і неспростовності).<br>**Г2.З2.** Доктрини кібербезпеки. | **Г2.У1**.Ураховувати принципи кібербезпеки і приватності при формуванні вимог організації (стосовно конфіденційності, цілісності, доступності, автентифікації і неспростовності).<br>**Г2.У2.** Оцінювати засоби контролю безпеки на основі принципів і доктрин кібербезпеки (наприклад, стандарти «CIS CSC», NIST SP | **Г2.К1.** Ураховувати вимоги керівництва організації під час координації захисту критично важливих об'єктів. | **Г2.В1.** Рекомендувати зміни та доповнення до кіберполітики в організації, приймати участь у координації її перегляду. |

| | | | | | |
|---|---|---|---|---|---|
| | | | 800-53, Керівні принципи кібербезпеки тощо). | | |
| | **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. | | | | |
| **Д.** Координація дій з аналітиками з кіберзахисту для управління та адміністрування оновлень правил та сигнатур для спеціалізованих прикладних програм у сфері кіберзахисту. | **Д1.**Здатність координувати дії з аналітиками кіберзахисту для адміністрування оновлень правил та сигнатур для спеціалізованих прикладних програм у сфері кіберзахисту. | **Д1.З1.** Методологію реагування на інциденти і обробки даних інцидентів.<br>**Д1.З2.** Системи виявлення вторгнень і розробки сигнатур.<br>**Д1.З3.** SIEM-системи.<br>**Д1.З4.** Антивірусне ПЗ. | **Д1.У1.** Використовувати методології обробки інцидентів.<br>**Д1.У2.** Виявляти вторгнення на хостах або мережі, за допомогою технологій виявлення вторгнень.<br>**Д1.У3.** Інтерпретувати сигнатури (наприклад, для мережевої системи запобігання і виявлення вторгнень з відкритим вихідним кодом). | **Д1.К1.** Приймати участь у реагуванні на кіберінциденти разом з командою реагування на комп'ютерні інциденти. | **Д1.В1**. Консультувати корпоративний персонал з питань оновлення правил та сигнатур спеціалізованих прикладних програм. |
| | **Д2.** Визначати наслідки застосування нових технологій або оновлень у програмах захисту ІТ. | **Д2.З1.** Методики зміцнення базової системи, мережі і операційної системи.<br>**Д2.З2.** Принципи, можливості, обмеження та наслідки кібердій | **Д2.У1.** Встановлювати оновлення спеціалізованих прикладних програм та компонентів (наприклад, систем | **Д2.К1.** Приймати участь у визначенні наслідків застосування нових оновлень | **Д2.В1.** Готувати рекомендації щодо можливих удосконалень і оновлень. |

| | | | | | |
|---|---|---|---|---|---|
| | | (наприклад, кіберзахисту, збору інформації, підготовки середовища, кібератаки). | виявлення/запобіган-ня вторгненням, антивірусів, SIEM-систем тощо).<br>**Д2.У2.** Налаштовувати і використовувати спеціалізовані програмні засоби у сфері кіберзахисту (наприклад, системи виявлення/ запобігання вторгненням, антивіруси, SIEM-системи. | у програмах кіберзахисту. | |
| | **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. | | | | |
| **Е.** Виявлення потенційних конфліктів при впровадженні будь-яких інструментів кіберзахисту (наприклад, тестування та оптимізація | **Е1.**Здатність виявляти потенційні конфлікти при впровадженні інструментів кіберзахисту~~/~~ | **Е1.З1**.Процедури, принципи і методологія тестування (наприклад, CMMI).<br>**Е1.З2**. Технології запису передаваних сигналів (наприклад, bluetooth, радіочастотна ідентифікація (RFID), мережі з | **Е1.У1.**Усувати неполадки і діагностувати аномалії функціонування інфраструктури системи кібербезпеки на основі її аналізу.<br>**Е1.У2.** Визначати потенційні | **Е2.К1**. Приймати участь у впровадженні нових процедур діагностування аномалій функціонування інфраструктури | **Е1.В1.** Проводити оптимізацію інфраструктури кіберзахисту та надавати рекомендації керівництву щодо її покращення. |

| | | | | | |
|---|---|---|---|---|---|
| інструментів і сигнатур)~~/~~ | | інфрачервоним діапазоном передачі (IR), WiFi, пейджингові системи передачі, стільникові системи мобільного зв'язку, антени супутникового зв'язку, голосовий зв'язок (VoIP)) та методики «перешкод», які забезпечують передачу небажаної інформації або не дозволяють інстальованим системам функціонувати коректно. | протиріччя, пов'язані з впровадженням будь-яких засобів кіберзахисту (наприклад, оптимізація інструментів і підписів). | системи кібербезпеки. | |
| | **Е2.** Здатність до тестування інструментів кіберзахисту. | **Е2.З1.** Методи тестування та оцінки систем.<br>**Е2.З2.** Методи тестування та оцінки захищеності систем. | **Е2.У1.** Здійснювати оцінку планів проведення тестування на предмет придатності і повноти.<br>**Е2.У2.** Збирати, перевіряти і підтверджувати дані тестування. | **Е2.К1.** Приймати участь у впровадженні нових процедур тестування інструментів кіберзахисту. | **Е2.В1.** Розробляти та направляти на розгляд процедури тестування та затвердження системи і документацію. |

| | | | | | |
|---|---|---|---|---|---|
| | **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 | | | | |
| **Ж.** Впровадження системи управління ризиками (RMF)/оцінки та авторизації безпеки (SA&A) для спеціальних систем кіберзахисту на підприємстві (в установі, організації), а також документування та ведення записів для них. | **Ж1.** Здатність впроваджувати системи управління ризиками (RMF) для спеціальних систем кіберзахисту на підприємстві (в установі, організації). | **Ж1.З1.** Процеси управління ризиками (наприклад, методи оцінки та зниження ризиків).<br>**Ж1.З2.** Методологія з кібербезпеки підприємства та управління ризиками ланцюжка постачання.<br>**Ж1.З3.** Вимоги в рамках Загальних принципів управління ризиками (RMF)<br>**Ж1.З4.** Принципи кібербезпеки і приватності, застосовуваних під час управління ризиками, пов'язаних із використанням, обробкою, зберіганням і передачею інформації або даних.<br>**Ж1.З5.** Методики управління ризиками в | **Ж1.У1.** Розробляти та координувати управління ризиками і відповідність загальним принципам для приватності.<br>**Ж1.У2.** Розробити стратегію управління ризиками організації, яка включає визначення прийняття ризиків.<br>**Ж1.У3.** Виявляти системні проблеми безпеки на основі аналізу даних вразливостей та конфігурації.<br>**Ж1.У4.** Використовувати способи підрахунку ризиків для інформування організації про результативні та | **Ж1. К1**. Брати участь в корпоративному процесі управління ризиками щоб забезпечити зменшення ризиків безпеки, і введення даних щодо інших технічних ризиків.<br>**Ж1.К2.** Надавати змістовну інформацію про контекст середовища загроз для організації, що покращує її позицію управління ризиками. | **Ж1.В1.** Визначати та призначати осіб на певні ролі, пов'язані з виконанням Загальних принципів управління ризиками.<br>**Ж1.В2.** Консультувати посадових осіб, директорів інформаційних технологій, директорів із інформаційної безпеки та відповідальної посадової особи з управління ризиками/виконав-чого ризику (функції) щодо питань безпеки (наприклад, встановлення периметру системи, |

| | | | | | |
|---|---|---|---|---|---|
| | | ланцюжку постачання (NIST SP 800-161).<br>**Ж1.36**. Підхід організації до прийняття ризиків та/або управління ризиками.<br>**Ж1.37.** Стандарти, процеси і практики управління ризиками в ланцюжку постачання.<br>**Ж1.38.** Методології оцінки загальних принципів управління ризиками.<br>**Ж1.39.** Процес планування захисту програм (наприклад, політики безпеки ланцюжків постачання інформаційних технологій / політика управління ризиками, Методи боротьби з підробками та вимоги).<br>**Ж1.10.** Стратегії управління ризиками та стратегії їх зменшення. | економічно ефективні підходи<br>щодо виявлення, оцінювання та управління ризиками кібербезпеки. | **Ж1.К3.** Брати участь у координації з вищим керівництвом організації для розробки стратегії управління ризиками організації, яка визначає стратегічний погляд організації на ризики, пов’язані з безпекою. | оцінки ступеня слабкості та недоліків у системі, планів дій і контрольних точок, підходів до виявлених вразливостей). |

| | | | | | |
|---|---|---|---|---|---|
| | **Ж2.** Здатність впроваджувати системи оцінювання та авторизації безпеки (SA&A) для спеціальних систем кіберзахисту на підприємстві (в установі, організації). | **Ж2.З1.** Конкретні операційні наслідки в результаті помилок кібербезпеки. | **Ж2.У1.** Планувати та проводити огляди авторизації безпеки та складати кейси отримання впевненості під час початкового встановлення спеціальних систем кіберзахисту.<br>**Ж2.У2.** Розвивати розуміння контексту загрозливого середовища організації. | **Ж2.К1**. Брати участь в оцінці ризику інформаційної безпеки під час проведення процедури оцінки і авторизації. | **Ж2.В1.** Оцінювати витрати-вигоду у процесі прийняття рішень щодо впровадження системи оцінювання та авторизації. |
| | **Ж3.**Здатність документувати та вести записи для системи управління ризиками кібекрбезпеки. | **Ж3.З1.** Методології оцінки ризиків. | **Ж3.У1.** Розробляти і публікувати документи щодо управління безпекою ланцюжка постачання та управління ризиками.<br>**Ж3.У2.** Здійснювати формалізований опис процедур управління ризиками кібербезпеки та результатів їх реалізації. | **Ж3.К1.** Надавати вхідні дані для діяльності процесу загальних принципів управління ризиками та відповідну документацію (наприклад, плани забезпечення життєвого циклу системи, | **Ж3.В1.** Розроблювати стратегії мінімізації ризиків для зменшення витрат, графіку, продуктивності і ризиків безпеки. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | концепція операцій, операційні процедури і навчальні матеріали з технічного обслуговування). | |
| | **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 підтримки інфраструктури кіберзахисту** | | |
|---|---|---|---|
| | Молодший фахівець з підтримки інфраструктури кіберзахисту | Фахівець з підтримки інфраструктури кіберзахисту | Провідний фахівець з підтримки інфраструктури кіберзахисту |
| | повна | повна | повна |
| **А** | + | + | + |
| **Б** | + | + | + |
| **В** | + | + | + |
| **Г** | - | + | + |
| **Д** | - | + | + |
| **Е** | - | + | + |
| **Ж** | - | - | + |

## VII. Відомості про розроблення та затвердження професійного стандарту

### 7.1. Повне найменування розробника професійного стандарту

Державна служба спеціального зв'язку та захисту інформації України

**Склад робочої групи/Учасники робочої групи**:

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

Горбенко Іван Дмитрович, голова наглядової Ради, головний конструктор ПРАТ «Інститут інформаційних технологій»;

Гулак Геннадій Миколайович, професор кафедри інформаційної та кібернетичної безпеки ім. професора Володимира Бурячка факультету інформаційних технологій Київського університету імені Бориса Грінченка;

Дідик Валерія Анатоліївна, керівник напряму з розвитку професійних навичок з кібербезпеки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»;

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

Кожухівський Андрій Дмитровач, професор кафедри інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації Державного університету телекомунікацій;

Леонов Андрій Олегович, голова Громадської організації «Інститут стандартів та технологій»;

Лукова-Чуйко Наталія Вікторівна, завідувач кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка;

Мазур Наталя Володимирівна, голова Профспілки працівників зв'язку України;

Мельник Сергій Вікторович, консультант напряму з розвитку професійних навичок з кібербезпеки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»;

Одарченко Роман Сергійович, завідувач кафедри телекомунікаційних та радіоелектронних систем факультету аеронавігації, електроніки та телекомунікацій Національного авіаційного університету;

Олексюк Лілія Віталіївна, голова Громадської організації «Всеукраїнська асоціація «Інформаційна безпека та інформаційні технології»;

Педченко Євгеній Миколайович, керівник відділу впровадження систем безпеки ТОВ «ІНТРАСИСТЕМС»;

Проскуровський Роман Васильович, заступник керівника Центру кіберзахисту Національного банку України;

Рибка Михайло Сергійович, заступник начальника управління – начальник 1 відділу 5 управління Департаменту захисту інформації Адміністрації Держспецзв'язку;

Субач Ігор Юрійович, завідувач Спеціальної кафедри № 5 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;

Толюпа Сергій Васильович, професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка;

Трегубенко Ірина Борисівна, провідний науковий співробітник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

Четверіков Іван Олександрович, доцент кафедри кібербезпеки Науково-навчального інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України;

Юдін Олександр Костянтинович, учений секретар Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

Яковів Ігор Богданович, доцент Спеціальної кафедри № 5 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

**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 стандартів під час підготовки проєкту професійного стандарту**

Висновок суб'єкта перевірки Національного агентства кваліфікацій від _____ про дотримання під час підготовки проєкту професійного стандарту «конструктор систем кібербезпеки» 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 Профспілки працівників зв'язку України від _____ щодо погодження проєкту професійного стандарту «Фахівець з підтримки інфраструктури кібербезпеки».

**VIII. Дата внесення професійного стандарту до Реєстру**

_____.

**IX. Рекомендована дата перегляду професійного стандарту**

Вересень 2028 року.