Проєкт

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

ПРОФЕСІЙНИЙ СТАНДАРТ

ФАХІВЕЦЬ З ОЦІНКИ ЗАХОДІВ ЗАХИСТУ ІНФОРМАЦІЇ (КІБЕРБЕЗПЕКИ)

_____(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 оцінки заходів захисту інформації (кібербезпеки)

ІІ. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Здійснення незалежної комплексної оцінки управлінського, операційного та технічного контролю безпеки, а також покращення контролю, що використовується в системі інформаційних технологій для визначення загальної ефективності заходів контролю. Розроблення, забезпечення та контроль виконання заходів для усунення причин і умов, що можуть призвести до витоку інформації. Здійснення оцінки ступеню захищеності інформаційних систем, а також системного контролю реалізації задекларованих послуг безпеки. Підвищення рівня безпеки інформаційних систем на основі аналізу потенційних недоліків та вразливих точок, а також забезпечення економічної ефективності розгорнутих заходів захисту.

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

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

Фахівець з оцінки заходів захисту інформації (кібербезпеки), 2139.2

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

Фахівець з оцінки заходів захисту інформації (кібербезпеки), 6 рівень НРК

Провідний фахівець з оцінки заходів захисту інформації (кібербезпеки), 7 рівень НРК.

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

- 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);
- 172 «Електронні комунікації та радіотехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (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 оцінювання інформаційних технологій (з кібербезпеки);
- 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 оцінювання заходів захисту інформації (кібербезпеки);
- документ (диплом, сертифікат, тощо), щодо професійної сертифікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері оцінювання заходів захисту інформації (кібербезпеки).

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**
Фахівець з оцінки заходів захисту інформації (кібербезпеки) Провідний фахівець з оцінки заходів захисту інформації (кібербезпеки)	Підготовка на другому рівні вищої освіти (магістерському) за спеціальностями вказаними п. ІІ.5 галузі знань 12 «Інформаційні технології» та 17 «Електроніка, автоматизація та електронні комунікації», стаж роботи за однією з професій відповідного спрямування повинен складати не менше 2 років (аналітик з безпеки	*Не передбачено професійним стандартом*

	інформаційно-телекомунікаційних систем, фахівець з питань безпеки (інформаційно-комунікаційні технології), фахівець сфери захисту інформації тощо)	

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 оцінки заходів захисту інформації (кібербезпеки)	Підвищення кваліфікації фахівець для отримання професійної кваліфікації "провідний фахівець з оцінки заходів захисту інформації ". Стаж роботи не менше двох років	*Не передбачено професійним стандартом*

IV. Абревіатури, скорочення

IT	інформаційні технології
IC	Інформаційні системи
ITC	інформаційно-телекомунікаційні системи
PII	Personal Identifiable information
ДМЗ	Демілітарізована зона
PKI	Public Key Infrastructure
SSL	Secure Sockets Layer
S/MIME	Secure / Multipurpose Internet Mail Extensions
PCI	Payment Card Industry
PHI	Protected Health Information
CIS CSC	Center for Internet Security (CIS) Critical Security Controls (CSC).
NIST SP 800-53	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.
EBSCO	Elton B. Stephens Company
JSTOR	Journal Storage
RMF	Risk Management Framework.
PL/SQL	Procedural Language/Structured Query Language.
TOGAF	The Open Group Architecture Framework.
ISO/IEC 15026-2	International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 15026-2

V. Опис трудових функцій аудитора інформаційних технологій (з кібербезпеки)

Трудові функції	**Компетентності**	**Результати навчання**			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
А. Оцінювання ефективності засобів контролю безпеки зокрема огляд авторизації безпеки та аудит зовнішніх послуг. Розробка кейсів впевненості та огляд авторизації безпеки	**А1.** Здатність планувати та проводити огляди авторизації безпеки та складати кейси отримання впевненості під час початкового встановлення систем та мереж.	**А1.З1.** Концепції і протоколи комп'ютерних мереж, а також методологію забезпечення мережевої безпеки **А1.З2**. Методи, принципи і концепції комунікацій, які підтримують інфраструктуру мережі **А1.З3.** Процедури підключення до локальної мережі організації та до глобальних мереж **А1.З4**. Використовувану в організації програму класифікації інформації і процедур у випадку витоку інформації з обмеженим доступом **А1.З5.** Процеси оцінювання стану безпеки та авторизації **А1.З6.** Структуру та процедури підготовки звітів постачальником послуг з кібербезпеки **А1.З7.** Базову	**А1.У1.** Проводити огляди ІС **А1.У2.** Застосовувати принципи, моделі, методи і засоби управління мережевими системами (наприклад, наскрізний моніторинг пропускної здатності системи) **А1.У3**. Організовувати процеси планування, включаючи підготовку функціональних і спеціальних планів підтримки, підготовки і забезпечення ділового листування, а також процесів кадрового забезпечення **А1.У4**. Визначати аномалії в цільової мережі (наприклад, вторгнення, потік даних або їх обробки, цільове впровадження нових технологій) **А1.У5.** Розроблювати план збору даних, який чітко відображає забезпечення, яке може бути використано для збору необхідної інформації	**А1.К1.** Готувати і проводити брифінги за відповідною та/чи профільною тематикою **А1.К2.** Чітко й коротко задавати запитання. **А1.К3.** Заохочувати всіх учасників дискусії до участі. **А1.К4.** Ефективно вирішувати конфлікти та проблеми, які виникають при роботі в віртуальній команд.	**А1.В1**. Працювати в колективі, постійно звертаючись за консультаціями до аналітиків і експертів (внутрішніх і зовнішніх організацій) для використання аналітичного і технічного досвіду **А1.В2.** Усвідомлювати власні когнітивні упередження та способи їх впливу на судження

		інформацію про загрози та вразливості безпеки систем і прикладного ПЗ			
	А2. Здатність розроблювати процеси відповідності безпеки та/або аудитів для зовнішніх послуг (наприклад, провайдерів хмарних послуг, центрів обробки даних)	**А2.З1.** Прикладні бізнес-процеси і функції в організації замовника послуг **А2.З2**. Системи баз даних **А2.З3.** Порядок управління та підтримування комунікаційної інфраструктури мережі **А2.З4.** Теоретичні основи і методи оцінювання систем кібербезпеки та виявлення вразливостей **А2.З5.** Методи документування результатів оцінок та перевірок процедур оцінки та валідації **А2.З6.** Методи розроблення та впровадження заходів для зниження ризиків, пов’язаних з новими та виникаючими технологіями ІТ та кібербезпеки	**А2.У1**. Використовувати віртуальні машини (наприклад, Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, тощо). **А2.У2**. Аналізувати системи цілі **А2.У3.** Виявляти проблеми кібербезпеки і приватності, які виникають при з’єднаннях внутрішніх та зовнішніх замовників та організацій-партнерів	**А2.К1.** Взаємодіяти із замовниками **А2.К2**. Чітко та стисло відповідати на питання. **А2.К3**. Готувати і проводити брифінги за відповідною та/чи профільною тематикою **А2.К4**. Задавати запитання для отримання додаткової інформації **А2.К5**. Досягати консенсусу в групі. **А2.К6.** Ефективно вирішувати конфлікти та проблеми, які виникають при роботі в віртуальній команді	**А2.В1.** Використовувати ІТС, призначені для кадрового забезпечення та обслуговування кадрових органів **А2В2**. Визначати зовнішніх партнерів зі спільними інтересами в проведенні кібероперацій **А2.В3.** Інтерпретувати і перетворювати вимоги замовника в оперативні дії **А2.В4.** Розроблювати або застосовувати наявну/ придбавати навчальну програму, яка відповідає темі на відповідному рівні для цілі
	А3. Оцінювати ефективність засобів	**А3.З1.** Алгоритми шифрування **А3.З2.** Концепції	**А3.У1.** Визначати показники або індикатори продуктивності системи та	**А3.К1.** Використовувати зворотній зв'язок з метою вдосконалення процесів,	**А3.В1.** Високорівнево визначати основні

	контролю безпеки	криптографії та управління криптографічними ключами **А3.З3.** Принципи і методи забезпечення безпеки ІТ (наприклад, мережеві екрани, ДМЗ, шифрування). **А3.З4.** Моделі системи безпеки (наприклад, модель Белла-Лападули, моделі забезпечення цілісності «Biba» і Кларка-Вілсона) **А3.З5.** Стандарти безпеки персональних ідентифікаційних даних (PII). **А3.З6.** Стандартів безпеки даних в сфері платіжних карт (PCI) **А3.З7.** Стандарти безпеки медичних персональних даних (PHI) **А3.З8.** Вбудовані системи (embedded system)	дій, спрямованих на підвищення або виправлення продуктивності, виходячи з призначення системи. **А3.У2.** Визначати вимоги до інфраструктури тестування і оцінювання (співробітники, полігони, засоби, прилади) **А3.У3.** Управляти відповідними активами, ресурсами для тестування і фахівцями з тестування з метою забезпечення гарантій ефективного проведення тестових заходів **А3.У4.** Використовувати шифрування інфраструктури відкритих ключів (PKI) та можливостей цифрового підпису в програмних додатках (наприклад, електронна пошта S/MIME, SSL-трафік) **А3.У5.** Аналіз і редагування результатів процедури оцінювання **А3.У6.** Отримувати доступ до інформації про доступні поточні активи та їх використання	продуктів і послуг **А3.К2.** Залучати та підтримувати уваги аудиторії **А3.К3.** Задавати запитання для отримання додаткової інформації **А3.К4.** Досягати консенсусу в групі **А3.К5.** Ефективно керувати проєктами та завданнями, коли члени команди знаходяться в р місцях	загальні проблеми коду. **А3.В2.** Розпізнавати і пом’якшувати когнітивні упередження, які можуть вплинути на аналіз **А3.В3.** Ефективно використовувати аналітичний та технічний досвід інших для вирішення проблем та досягнення цілей
	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. Оцінювання дотримання заходів забезпечення відповідності, у тому числі з аналізом процесів управління конфігураціями та дотриманням встановлених обмежень прикладного програмного забезпечення, мереж або систем	**Б1.**Здатність оцінювати всі процеси управління конфігурацією (зміна конфігурації/ управління релізами)	**Б1.31.** Методи оцінювання систем кіберзахисту і вразливостей, а також їх можливостей **Б1.32.** Резервне копіювання та відновлення даних **Б1.33.** Вимоги до процедур оцінювання і валідації, що прийняті в організації **Б1.34.** Процеси оцінювання стану безпеки і процесу авторизації **Б1.35.** Підходи до управління мережевим доступом, ідентифікацією, та доступом (наприклад, інфраструктура відкритих ключів, автентифікація об’єктів, відкриті ідентифікатори, мова розмітки для контролю захищеності, мова розмітки для надання послуг)	**Б1.У1**. Оцінювати проєкти систем безпеки **Б1.У2.** Оцінювати засоби контролю безпеки на основі принципів і доктрин кібербезпеки (наприклад, стандарти «CIS CSC», NIST SP 800-53, Керівні принципи кібербезпеки тощо) **Б1.У3.** Використовувати результати оцінок впливу/ризику для прийняття рішень. **Б1.У4.** Використовувати результати тестування на безпеку для поліпшення безпеки програмного забезпечення	**Б1.К1.** Навичка Оцінювати запити на отримання інформації з метою визначення наявності необхідної інформації для відповіді **Б1.К2.** Адаптувати свій виступ до аудиторії **Б1.К3.** Ставити запитання, щоб отримати додаткову інформацію **Б1.К4.** Аналізувати ідеї учасників дискусії **Б1.К5.** Ефективно вирішувати проблеми, що виникають у віртуальній команді	**Б1.В1**. Розроблювати обґрунтовані і надійні оцінки **Б1.В2.** Критично мислити **Б1.В3.** Застосовувати принципи кібербезпеки і приватності при формуванні вимог організації (стосовно конфіденційності, цілісності, доступності, автентифікації і неспростовності).
	Б2. Здатність встановлювати	**Б2.31.** Спроможності прикладних програм	**Б2.У1.** Визначати потреби в забезпеченні безпеки	**Б2.К1.** Ставити уточнювальні питання	**Б2.В1.** Здатність Застосовувати

	допустимі ліміти прикладного програмного забезпечення, мереж або систем	мережевого обладнання, включаючи маршрутизатори, комутатори, мости, сервери, засоби передачі і відповідне технічне обладнання. **Б2.З2.** Принципи і методи кібербезпеки та приватності, а також організаційні вимоги (щодо забезпечення конфіденційності, цілісності, доступності, автентифікації і неспростовності) **Б2.З3.** Приципи документування заходів кібербезпеки та приватності **Б2.З4.** Правові та регулятивні аспекти кібербезпеки. **Б2.З5.** Роль безпеки прикладних програм у бізнесі **Б2.З6.** Основи безпеки ІТ включаючи мережеві екрани, ДМЗ та шифрування **Б2.З7.** Принципи управління доступом до мереж, ідентифікації та керування доступом включаючи інфраструктуру відкритих ключів,	систем ІТ (тобто контролів безпеки) **Б2.У2**. Трактувати компільовані й інтерпретовані мови програмування **Б2.У3.** Інтерпретувати результати трасування і того, як вони використовуються при аналізі і реконструкції мереж	**Б2.К2.** Готувати і проводити брифінги за відповідною та/чи профільною тематикою **Б2.К3.** Стимулювати дискусії в малих групах **Б2.К4.** Ефективно співпрацювати у віртуальних командах	навички критичного читання/ мислення

		автентифікацію об'єктів, відкриті ідентифікатори, а також мови розмітки для контролю захищеності та надання послуг **Б2.З8.** Потенційні загрози і вразливості безпеки системи і програмного забезпечення включає переповнення буфера, мобільний код, міжсайтові сценарії, ін'єкції в процедурні та мови структурованих запитів (PL/SQL), перегони фронтів, приховані канали, атаки на повернення і шкідливий код			
	Б3. Здатність підтримувати необхідні заходи щодо забезпечення відповідності (наприклад, переконатися, що виконуються настанови щодо конфігурації системи безпеки, здійснюється моніторинг відповідності)	**Б3.З1.** Принципи кібербезпеки і приватності	**Б3.У1.** Аналізувати першопричини виникнення проблем у функціонуванні систем безпеки **Б3.У2.** Інтерпретувати метадані і зміст, що застосовуються в системах збору інформації **Б3.У3.** Збирати дані з доступних інструментів та прикладних програм відповідно до вимог збору даних та управління операціями зі збору даних	**Б3.К1.** Використовувати або розроблювати освітні/навчальні заходи (наприклад, програм навчання, навчальних ігор, інтерактивних занять). **Б3.К2.** Готувати і проводити брифінги за відповідною та/чи профільною тематикою **Б3.К3.** Задавати додаткові	**Б1.В1**. Здатність концентрувати зусилля у дослідницькій області з метою задоволення потреб замовника в процесі прийняття рішень.

				запитання для уточнення **Б3.К4.** Допомагати підтримувати активну дискусію в невеликих групах **Б3.К5.** Управляти ризиками та викликами дистанційної/віддаленої роботи	
	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. Виконання аналізу системи безпеки та її ризиків, перегляд безпеки архітектури, управління ризиками з наданням відповідних рекомендацій, даних та документів для включення в стратегію зниження ризиків та розробку плану управління ризиками	**В1.** Здатність брати участь в корпоративному процесі управління ризиками щоб забезпечити зменшення ризиків безпеки, і введення даних щодо інших технічних ризиків	**В1.З1.** Процеси управління ризиками (наприклад, методів оцінки та зниження ризиків) **В1.З2.** Принципи кібербезпеки і приватності, застосовувані під час управління ризиками, пов'язаних із використанням, обробкою, зберіганням і передачею інформації або даних **В1.З3.** Вимоги в рамках Загальних принципів управління ризиками (RMF) **В1.З4.** Методики управління ризиками в ланцюжку постачання	**В1.У1**. Проводити оцінювання впливу/ризику **В1.У2.** Оброблювати зібрані дані для подальшого їх аналізу **В1.У3.** Досліджувати стратегічні напрями, що потребують додаткового уточнення та/або методології **В1.У4.** Аналізувати вплив стратегічних виборів, бізнес-рішень та технологічних інновацій на конкурентоспроможність організації.	**В1.К1**. Сприяти дискусіям в невеликих групах **В1.К2.** Демонструвати майстерність у підготовці та презентації інформації під час семінарів **В1.К3.** Ефективно ставити запитання для збагачення інформації **В1.К4.** Ефективно використовувати інструменти для віддаленої комунікації віртуальних команд	**В1.В1.** Розкривати проблему і перевіряти взаємозв'язки між даними, які, на перший погляд, здаються не пов'язаними між собою **В1.В2.** Використовувати кілька джерел розвідки в усіх напрямках розвідувальних дисциплін

		(NIST SP 800-161). **В1.35.** Політики, вимоги і процедури безпеки ланцюжка постачання IT та управління ризиками ланцюжка постачання			
	В2. Здатність проводити аналіз ризиків (наприклад, загрози, вразливості та ймовірності виникнення) щоразу, коли прикладна програма або система зазнають значних змін	**В2.31**. Класифікацію кіберзагроз та вразливостей. **В2.32.** Вразливості прикладних програм **В2.33.** Джерела поширення інформації про вразливість (наприклад, попередження, рекомендації, списки помилок і бюлетені) **В2.34.** Загрози і вразливості безпеки систем і прикладного програмного забезпечення (наприклад, переповнення буфера, мобільний код, міжсайтові сценарії, процедурна мова/мова структурованих запитів [PL/SQL] та ін’єкції, перегони фронтів, прихований канал, повтор, атаки на повернення, шкідливий код)	**В2.У1.** Проводити сканування вразливостей і розпізнання вразливостей в системах безпеки **В2.У2.** Розпізнавати та класифікувати різні типи вразливостей і пов'язаних з ними атак **В2.У3.** Застосовувати засоби контролю захищеності **В2.У4.** Проводити оцінювання вразливості програмних додатків **В2.У5.** Аналізувати трафік з метою визначення мережевих пристроїв **В2.У6.** Визначати орієнтування для розробки цілі **В2.У7.** Інтерпретувати результати, отримані сканером вразливостей, з метою виявлення вразливостей	**В2.К1.** Готувати і проводити брифінги за відповідною та/чи профільною тематикою	**В2.В1.** Виявляти системні проблеми безпеки на основі аналізу даних вразливостей та конфігурації **В2.В2.** Проводити процедури сканування вразливостей і розпізнавання вразливостей в системах безпеки **В2.В3.** Ідентифікувати/ описувати вразливості цілі.

		В2.35. Інструменти системної діагностики і технік ідентифікації відмов **В2.36**. Принципи, інструменти та методики тестування на проникнення **В2.37.** Регуляції, пов'язані з використанням, обробкою, зберіганням та передачею даних. **В2.38.** Ризики безпеки прикладних програм (Open Web Application Security Project Top 10 list)			
	В3. Здатність визначати наявність планів дій та етапів або планів відновлення для усунення вразливостей, які були виявлені під час оцінювання ризиків, аудиторських та інспекторських перевірок тощо	**В3.31.** Конкретні операційні наслідки в результаті помилок кібербезпеки **В3.32.** Процедури оцінювання ризиків і застосування відповідних методів управління **В3.33.** Технічні аспекти резервного копіювання та відновлення даних **В3.34.** Процедури планування безперервності бізнесу та відновлення операцій після катастроф **В3.35.** Методи	**В3.У1.** Усувати неполадки і діагностування аномалій функціонування інфраструктури системи кібербезпеки на основі її аналізу **В3.У2** Розроблювати план тестування системи безпеки (наприклад, окремого компонента, процесу інтеграції, системи, процесу приймання системи) **В3.У3.** Застосовувати безпечні методи кодування **В4.У4.** Встановлювати пріоритети інформації, яка стосується кібероперацій	**В3.К1.** Ефективно співпрацювати через віртуальні команди **В3.К2.** Готувати і проводити брифінги за відповідною та/чи профільною тематикою **В3.К3.** Сприяти інноваційним ідеям у дискусіях в невеликих групах	**В3.В1.** Здатність аналізувати тестові дані. **В3.В2.** Здатність збирати, перевіряти і підтверджувати дані тестування. **В3.В3.** Здатність переводити дані і результати тестування в оціночні висновки.

		оцінювання безпеки ІТ та їх вплив на забезпечення безпеки даних **В3.36.** Системи критичної інфраструктури з низьким рівнем безпеки в ІТ **В3.37.** Нормативні акти, положення та корпоративні стандарти, які регулюють кібербезпеку критичних інфраструктур	**В4.У5.** Аналізувати та/чи редагувати плани		
	В4. Здатність виконувати перегляд безпеки, визначати пробіли в архітектурі безпеки, що призведе до рекомендації щодо їхнього включення в стратегію зниження ризиків	**В4.З1.** Корпоративну архітектуру інформаційної безпеки організації **В4.З2.** Сучасні галузеві методи оцінювання, впровадження та розповсюдження інструментів та процедур оцінки безпеки ІТ, моніторингу, виявлення та усунення несправностей, що використовують концепції та можливості на основі стандартів **В4.З3.** Знання Принципи і методи	**В4.У1.** Застосовувати принципи конфіденційності, цілісності та доступності **В4.У2.** Визначати, як буде функціонувати система безпеки (включаючи її властивості відмовостійкості і надійності), та як зміни умов, операцій або середовища вплинуть на ці результати **В4.У3.** Аналізувати реєстраційні записи з метою встановлення доказів здійснених вторгнень **В4.У4.** Використовувати інструменти співвіднесення	**В4.К1**. Оцінювати інформацію на предмет її надійності, достовірності і актуальності **В4.К2**. Готувати і проводити брифінги за відповідною та/чи профільною тематикою	**В4.В1.** Ефективно працювати у динамічному, швидкоплинному середовищі **В4.В2.** Інтерпретувати і розуміти складні концепції, що швидко змінюються **В4.В3.** Правильно та ефективно обирати пріоритети і розподіляти ресурси кібербезпеки **В4.В4.** Встановлювати зв’язки між стратегією, бізнесом

		структурного аналізу **В4.34.** Архітектуру ІТ підприємства **В4.35.** Системи критичної інфраструктури з ІТ, які були розроблені без врахування вимог безпеки **В4.36.** Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи (наприклад, прикладна система ешелонованого захисту) **В4.37.** Концепції архітектури безпеки і еталонних моделей архітектури підприємства (наприклад, модель Закмана, TOGAF)	подій сфери кібербезпеки **В4.У5.** Ідентифіковувати пристрої, що працюють на кожному рівні моделей протоколів		і технологією в контексті динаміки організації **В4.В5.** Розуміти основні поняття і проблеми, пов'язані з діяльністю організації в кіберпросторі та її впливом **В4.В6.** Виявляти системи критичної інфраструктури з ІТ, які були спроєктовані без урахування безпеки системи
	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				
Г. Нагляд за дотриманням належного опису, оновленню та документуванню діяльності,	**Г1**. Здатність забезпечувати своєчасне документування діяльності з проектування та розвитку	**Г1.З1.** Останні ІТ та кібербезпеки, та технології що розроблюються **Г1.З2.** Методи структурного аналізу для планування і	**Г1.У1.** Розроблювати звітні документи за результатами тестування і оцінювання **Г1.У2.** Готувати технічну документацію **Г1.У3.** Розроблювати та запроваджувати на	**Г1.К1**. Аналізувати стратегічні настанови з питань, які вимагають роз'яснення і/або додаткової методології **Г1.К2**. Здійснювати ефективне письмове	**Г1.В1**. Розроблювати технічну документацію **Г1.В2**. Категорізовувати та узагальнювати

проектування та розвитку кібербезпеки, зокрема безпеки прикладної системи, рівнів ризику для кожної прикладної програми, системи та мережі, а також керування пакетами документів з акредитації	кібербезпеки (з наданням функціонального опису впровадження безпеки)	стратегічного управління **Г1.33.** Цілі і завдання, що керують розробкою та впровадженням ІТ-інфраструктури **Г1.34.** Чинні закони і правові норми, що стосуються діяльності правоохоронних органів **Г1.35.** Прикладну систему захисту у концепції архітектури безпеки мережі **Г1.36.** Модель Закмана та інші розповсюджені стандартні моделі архітектури підприємства **Г1.37.** Вимоги правових актів, політик і процедур щодо кібербезпеки критичних інфраструктур	практиці управління знаннями з інтеграцією технічної документації, зокрема, сторінок Wiki	спілкування	методи ведення технічної експлуатації цілі

	Г2. Здатність визначати і документувати те, як впровадження нових систем або інтерфейсів між системами вплине на стан захищеності діючої інфраструктури	**Г2.З1.** Структуру і процедури підготовки звітних документів постачальником, який надає послуги з кіберзахисту в рамках організації **Г2.З2.** Як використовувати концепцію комунікацій для підтримки розвитку інфраструктури мережі **Г2.З3.** Порядок класифікації та категоризації компонентів корпоративної архітектури інформаційної безпеки організації **Г2.З4.** Можливі ін’єкції та переповнення даних у процедурних мовах та мовах структурованих запитів	**Г2.У1.** Визначати цілі з метою безпосередній підтримки операцій зі збору даних **Г2.У2.** Розроблювати детальні звіти, що містять аналіз тестових даних **Г2.У3.** Створювати детальні технічні описи **Г2.У4.** Аналізувати та впроваджувати нові методики технічної документації для управління знаннями **Г2.У5.** Застосовувати в практичній діяльності результати аудиту безпеки та вимог стандартів безпеки програмного забезпечення/мереж/систем	**Г1.К1**. Впевнено і систематизовано доводити складну інформацію, концепції або ідеї в усній і письмовій формах і/або за допомогою наочних засобів	**Г2.В1.** Приймати участь у розробленні детальних концепцій проєктів відповідного спрямування **Г2.В2.** Аналізувати та розглядати методи виконання технічних ремонтних робіт **Г2.В3.** Розроблювати технічні специфікації та описи профільних продуктів
	Г3. Здатність відслідковувати впровадження заходів безпеки прикладного програмного забезпечення /мережі/системи	**Г3.К1.** Положення про аудит безпеки та стандарти безпеки програмного забезпечення/мереж/ систем **Г3.К2.** Правила, що визначають процес обміну даними між різними сторонами **Г3.К3.** Процес	**Г3.У1**. Управляти знаннями, включаючи методики технічної документації (наприклад, сторінку Wiki) **Г3.У2**. Аналізувати результати тестування та оцінки у звітних документах **Г3.У3**. Генерувати графіки, діаграми та ілюстрації для	**Г3.К1.** Здатність Переконливо і структуровано висвітлювати складну інформацію, концепції або ідеї	**Г3.В1.** Аналізувати та описувати процедури технічного обслуговування об'єктів **Г3.В2.** Ідентифікувати та характеризувати методи ведення технічної

		впровадження та інтеграції моделей систем безпеки, таких як модель Белла-Лападули, моделі "Biba" та Кларка-Вілсона **Г3.К4.** Технології та засоби, які використовуються для захисту мережевих компонентів в архітектурі безпеки	технічної документації		експлуатації
	Г4. Здатність перевіряти та оновлювати документацію з безпеки, яка відображає особливості проектування безпеки прикладної системи/системи	**Г4.З1.** Особливості проєктування безпеки прикладної системи/системи **Г4.З2.** Технології шифрування даних в режимі передачі **Г4.З3.** Методи ідентифікації та аналізу потенційних загроз в мережі **Г4.З4.** Стратегії та підходи до системної діагностики та усунення відмов	**Г4.У1.** Складати плани та готувати відповідну кореспонденцію **Г4.У2.** Готувати документи з оцінюванням тестування і рекомендаціями **Г4.У3.** Розроблювати технічні плани **Г4.У4.** Приймати участь у розробленні стратегій управління знаннями та розвитку технічної документації	**Г4.К1.** Здатність Брати участь в якості члена груп планування, координаційних і оперативних груп за необхідності **Г4.К2.** Переконливо аргументувати свої позиції під час письмового спілкування **Г4.К3.** Оцінювати стратегічні орієнтири з питань, які потребують роз'яснень або додаткової методології	**Г4.В1**. Ідентифікувати/ описувати методики /методи ведення технічної експлуатації цілі **Г4.В2**. Аргументовано викладати свої позиції під час письмових обмінів
	Г5. Здатність переглядати документи щодо авторизації та надання впевненості, щоб підтвердити, що рівень ризику	**Г5.З1.** Методи автентифікації, авторизації та контролю доступу **Г5.З2.** Механізми управління мережевим доступом та ідентифікацією в	**Г5У1.** Визначати пріоритет матеріалу мовою цілі **Г5У2.** Розроблювати відповідну технічну документацію **Г5.У3.** Ефективно управляти знаннями, включаючи методики	**Г5.К1.** Проводити аудит безпеки програм, систем та мереж для оцінки відповідності ризиків встановленим стандартам і нормативам **Г5.К2.** Аналізувати інформацію про забезпечення	**Г5.В1.** Розширювати доступ до мережі шляхом проведення цільового аналізу і збору даних для визначення цілей, що представляє

	знаходиться в допустимих межах для кожної прикладної програми, системи та мережі	організаційних структурах **Г5.З3.** Порядок застосування принципів кібербезпеки і приватності при визначенні технічних вимог до інформаційних систем	технічної документації, з метою перегляду документів щодо авторизації та надання впевненості, що рівень ризику для кожної прикладної програми, системи та мережі знаходиться в межах допустимих значень	безпеки та контролювати виконання вимог щодо авторизації, щоб забезпечити відповідність нормативам та політикам безпеки	інтерес
	Г6. Здатність керувати та затверджувати пакети документів з акредитації	**Г6.З1.** Закони, нормативні акти, політики і етичні норми, та як вони пов'язані з кібербезпекою і приватністю **Г6.З2.** Закони, політики, процедури чи основи корпоративного управління, що стосуються кібербезпеки критичних інфраструктур **Г6.З3.** Процеси та структуру підготовки звітних документів постачальником послуг з кіберзахисту всередині їх власної організації, з метою ефективного управління пакетами документів для акредитації (наприклад, ISO/IEC 15026-2)	**Г6.У1.** Отримувати доступ до баз даних, в яких зберігаються плани/директиви/ Методологія **Г6.У2**. Створювати звітні документи, що включають результати тестування і оцінки, з метою ефективного керування пакетами документів для акредитації (наприклад, ISO/IEC 15026-2). **Г6.У3.** Розроблювати технічну документацію з метою ефективного управління пакетами документів для акредитації (наприклад, ISO/IEC 15026-2).	**Г6.К2.** Координувати, аналізувати та оцінювати документацію, необхідну для акредитації, забезпечуючи виконання всіх вимог стандартів та процедур акредитації, а також здійснювати затвердження необхідних документів	**Г6.В1.** Застосування у практичній діяльності норм та положень чинних законів, законодавчих актів парламенту, указів президента, постанов і розпоряджень органів виконавчої влади та/або кодексу і процедур адміністративного/ кримінального права

	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				
Д. Оцінювання впровадження та функціонування вимог безпеки, а також відповідності політик і процедур ІТ, при придбанні, постачанні, закупівлі та аутсорсингу цілям і місії організації	**Д1.** Здатність контролювати, щоб усі дії з придбання, постачання, закупівлі та аутсорсингу відповідають вимогам кібербезпеки, які відповідають цілям організації	**Д1.З1.** Знання нових і виникаючих ІТ та технологій кібербезпеки. **Д1.З2.** Порядок планування бізнес-безперервності та відновлення операцій після надзвичайних ситуацій з метою забезпечення відповідності дій з придбання, постачання, закупівлі та аутсорсингу вимогам кібербезпеки, що відповідають цілям організації **Д1.З3.** Організаційні бізнес-процеси та місії з метою забезпечення відповідності дій з придбання, постачання, закупівлі та аутсорсингу вимогам кібербезпеки, що відповідають цілям організації **Д1.З4.** Політики, вимоги і процедури	**Д1.У1.** Аналізувати мережу зв'язку цілі **Д1.У2**. Визначати проблеми і обмеження розвідки **Д1.У3**. Ідентифікувати, розміщувати та відстежувати цілі за допомогою методик геопросторового аналізу **Д1.У4.** Використовувати в організації структуру і порядок підготовки звітів про кіберзахист постачальника послуг	**Д1.К1**. Управляти відносинами з клієнтами, включаючи визначення потреб/вимог клієнтів, управління очікуваннями клієнта та демонстрацію відданості досягненню якісних результатів **Д1.К2.** Організовувати та проводити брифінги з урахуванням вимог кібербезпеки для ефективного забезпечення виконання дій з придбання, постачання, закупівлі та аутсорсингу відповідно до цілей організації **Д1.К3.** Виявляти необхідні деталі та задавати уточнюючі питання для переконання, що всі дії з придбання, постачання, закупівлі та аутсорсингу відповідають вимогам кібербезпеки та відповідають цілям організації **Д1.К4.** Ефективно співпрацювати через віртуальні команди з метою переконання, що всі дії з	**Д1.В1.** Застосовувати навички і стратегії спільної роботи **Д1.В2.** Виявляти пробіли розвідки **Д1.В3.** Моніторити досягнення у технологіях приватності інформації для забезпечення адаптації та відповідності організації.

		забезпечення кібербезпеки та управління ризиками в ланцюжку постачання ІТ з метою переконання, що всі дії з придбання, постачання, закупівлі та аутсорсингу відповідають цим вимогам та відповідають цілям організації		придбання, постачання, закупівлі та аутсорсингу відповідають вимогам кібербезпеки, що відповідають цілям організації	
	Д2. Здатність забезпечувати успішне впровадження та функціональність вимог безпеки та відповідних політик і процедур ІТ, які узгоджені з цілями та місією організації	**Д2.З1.** Безперервності бі та операційних планів відновлення безперервно після катастроф **Д2.З2.** Корпоративні цілі і завдання, пов'язані з використанням ІТ в організації **Д2.З3.** Основні бізнес-процеси і місії організації **Д2.З4.** Нові та емерджентні технологіями в сфері ІТ та кібербезпеки з метою забезпечення успішного впровадження та функціональності безпекових вимог, а також відповідних політик і процедур ІТ, які гармонізовані з	**Д2.У1.** Інтегрувати та застосовувати у практичній роботі політику, яка відповідає цілям безпеки системи **Д2.У2.** Визначати регіональні мови і діалекти, які не належать цілі **Д2.У3.** Ідентифіковувати, розміщувати та відстежувати цілі за допомогою методик геопросторового аналізу **Д2.У4.** Адаптовувати аналіз до необхідних рівнів (наприклад, класифікаційного та організаційного) **Д2.У5.** Аналізувати джерела сили і морального духу цілі чи загрози **Д2.У6.** Застосовувати принципи кібербезпеки і	**Д2.К1**. Визначати мовні проблеми, які можуть вплинути на рішення задач, що стоять перед організацією **Д2.К2.** Застосовувати судження, коли політики визначені некоректно. **Д2.К3.** Взаємодіяти з департаментами і бізнес підрозділами для впровадження принципів і програм забезпечення приватності в організації та узгодження завдань забезпечення приватності з цілями безпеки	**Д2.В1.** Оцінювати, аналізувати та синтезувати великі обсяги даних (які можуть бути фрагментованими і суперечливими) у високоякісні і об'єднані продукти таргетингу /розвідки **Д2.В2.** Інтерпретувати і застосовувати закони, нормативні акти, політики та методології, що стосуються кіберцілей організації

		цілями та місією організації	приватності при формуванні організаційних вимог (які стосуються конфіденційності, цілісності, доступності, автентифікації і неспростовності)		
	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 оцінки заходів захисту інформації (кібербезпеки)	
	Фахівець з оцінки заходів захисту інформації (кібербезпеки)	Провідний фахівець з оцінки заходів захисту інформації (кібербезпеки)
	повна	повна
А	+	+
Б	+	+
В	+	+
Г	+	+
Д	-	+

VII. Відомості про розроблення та затвердження професійного стандарту

1. Повне найменування розробника професійного стандарту

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;

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

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

ГАЙДУР Галина Іванівна, завідувач кафедри інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації Державного університету телекомунікацій;

ГВОЗДІНСЬКИЙ Дмитро Володимирович, заступник начальника 1 відділу 6 управління Департаменту державного контролю у сфері захисту інформації Адміністрації Держспецзв'язку;

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

ГУБРІЄНКО Роман Григорович, заступник директора департаменту – начальник 3 управління Департаменту державного контролю у сфері захисту інформації Адміністрації Держспецзв'язку;

ДАКОВ Сергій Юрійович, провідний науковий співробітник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

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

КОЗАК Андрій Володимирович, провідний спеціаліст за рахунок посади головного спеціаліста 2 відділу 6 управління Департаменту державного контролю у сфері захисту інформації Адміністрації Держспецзв'язку;

ЛИСЕНКО Юлія Костянтинівна, начальник 6 управління Департаменту державного контролю у сфері захисту інформації Адміністрації Держспецзв'язку;

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

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

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;

ОХРІМЕНКО Тетяна Олександрівна, заступник декана з наукової роботи факультету комп'ютерних наук та технологій Національного авіаційного університету;

ПАВЛЕНКО Володимир Анатолійович, директор Громадської організації «Глобальний центр взаємодії в кіберпросторі»;

ПАЗЮК Андрій Валерійович, віцепрезидент Громадської організації «Українська академія кібербезпеки»;

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

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

СЄВЄРІНОВ Олександр Васильович, доцент кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки;

ХАРЧЕНКО В'ячеслав Сергійович, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Жуковського.

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 «Фахівець з оцінки заходів захисту інформації (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 оцінки заходів захисту інформації (кібербезпеки) "

VIII. Дата внесення професійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.