Прим. № __

ЗАТВЕРДЖЕНО

Наказ Адміністрації Держспецзв'язку
25 листопада 2022 року № 715

Професійний стандарт
«Розробник систем захисту інформації»

1. Загальні відомості професійного стандарту

1.1. Основна мета професійної діяльності

Проєктування, розроблення, тестування та оцінювання систем захисту інформації протягом усього життєвого циклу їх розробки.

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

Секція J	Інформація та телекомунікації	**Розділ 58**	Видавнича діяльність	**Група 58.2**	Видання програмного забезпечення
				Клас 58.29	Видання іншого програмного забезпечення
		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 62.09	Інша діяльність у сфері інформаційних технологій і комп'ютерних систем
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	Інша професійна, наукова та технічна діяльність, н. в. і. у.

1.3. Назва виду професійної діяльності та її код (згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій»)

Розділ	**Клас**	**Підклас**
2	**213**	**2132**
Професіонали	Професіонали в галузі обчислень (комп'ютеризації)	Професіонали в галузі програмування

1.4. Назва професії (професійної назви роботи) та її код (згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій»)

Розробник систем захисту інформації 2132.2.

1.5. Професійна кваліфікація

Розробник систем захисту інформації (трудові функції А, Б, В).

Провідний розробник систем захисту інформації (трудові функції А, Б, В, Г).

1.6. Місце професії (посади, професійної назви роботи) в організаційно-виробничій структурі підприємства (установи, організації)

Обіймає посаду розробника систем захисту інформації, провідного розробника систем захисту інформації.

Розробник систем захисту інформації, провідний розробник систем захисту інформації безпосередньо підпорядкований керівнику профільного структурного підрозділу (або уповноваженій особі) в структурних підрозділах підприємства/організації, профільних структурних підрозділах підприємства/ організації із захисту інформації та кібербезпеки, профільних науково-дослідних установах, підприємствах/організаціях, які реалізовують або застосовують функції проєктування, розроблення, тестування та оцінювання систем захисту інформації, а також програмних та/або апаратних засобів протягом усього життєвого циклу їх розробки.

Робоче місце розташовано у приміщенні (кабінеті, кімнаті, лабораторії, приміщенні обчислювального центру) відповідного підприємства/організації/ установи.

1.7. Умови праці

Тривалість робочого часу та часу відпочинку – згідно з чинним законодавством, графіками роботи та відпочинку, правилами внутрішнього трудового розпорядку, колективним договором.

Відпустки надають згідно з чинним законодавством, колективним договором, графіками надання відпусток та за результатами атестації робочого місця за умовами праці.

Робота в окремих випадках пов'язана зі шкідливими умовами праці. Пільги та компенсації встановлюють відповідно до чинного законодавства та колективного договору.

1.8. Документи, що підтверджують професійну та освітню кваліфікацію, її віднесення до рівня Національної рамки кваліфікацій (НРК)

Для кваліфікацій «Розробник систем захисту інформації» та «Провідний розробник систем захисту інформації»:

диплом магістра за будь-якою із шести спеціальностей галузі знань 12 «Інформаційні технології» або за спеціальностями 171 «Електроніка»,

172 «Телекомунікації та радіотехніка» галузі знань 17 «Електроніка та телекомунікації», або за спеціальністю 113 «Прикладна математика» галузі знань 11 «Математика та статистика», або за спеціальністю 151 «Автоматизація та комп'ютерно-інтегровані технології» галузі знань 15 «Автоматизація та приладобудування», або за спеціальностями 255 «Озброєння та військова техніка», 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7 рівень НРК), а також свідоцтво про присвоєння (підвищення) кваліфікації «Розробник систем захисту інформації» або інший документ, що підтверджує професійну кваліфікацію «Розробник систем захисту інформації»;

або свідоцтво про присвоєння (підвищення) кваліфікації «Провідний розробник систем захисту інформації» або інший документ, що підтверджує професійну кваліфікацію «Провідний розробник систем захисту інформації».

Розробник систем захисту інформації – 7 рівень НРК.

Провідний розробник систем захисту інформації – 7 рівень НРК.

2. Навчання та професійний розвиток

2.1. Первинна професійна підготовка (назва кваліфікації)

Для кваліфікацій «Розробник систем захисту інформації» та «Провідний розробник систем захисту інформації» – підготовка на другому рівні вищої освіти (магістерському) за будь-якою із шести спеціальностей галузі знань 12 «Інформаційні технології» або за спеціальністями 171 «Електроніка», 172 «Телекомунікації та радіотехніка» галузі знань 17 «Електроніка та телекомунікації», або за спеціальністю 113 «Прикладна математика» галузі знань 11 «Математика та статистика», або за спеціальністю 151 «Автоматизація та комп'ютерно-інтегровані технології» галузі знань 15 «Автоматизація та приладобудування», або за спеціальністями 255 «Озброєння та військова техніка», 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону».

2.2. Підвищення кваліфікації без присвоєння нового рівня освіти (назва кваліфікації)

Підвищення професійної кваліфікації «Провідний розробник систем захисту інформації» за наявності професійної кваліфікації «Розробник систем захисту інформації». Стаж роботи – не менше двох років на посадах, що відповідають кваліфікації «Розробник систем захисту інформації».

3. Нормативно-правова база, що регулює відповідну професійну діяльність

Кодекс законів про працю України.

Закон України «Про захист прав споживачів».

Закон України «Про інформацію».

Закон України «Про державну таємницю».

Закон України «Про захист інформації в інформаційно-комунікаційних системах».

Закон України «Про захист персональних даних».

Закон України «Про доступ до публічної інформації».

Закон України «Про основні засади забезпечення кібербезпеки України».

Закон України «Про електронні довірчі послуги».

Закон України «Про національну безпеку України».

Закон України «Про електронні комунікації».

Закон України «Про публічні електронні реєстри».

Указ Президента України від 13.02.2017 р. № 32 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації».

Указ Президента України від 30.08.2017 р. № 254 «Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», завпровадженого Указом Президента України від 13 лютого 2017 року № 32».

Указ Президента України від 26.08.2021 р. № 447 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України».

Постанова Кабінету Міністрів України від 19.06.2019 р. № 518 «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури».

Постанова Кабінету Міністрів України від 09.10.2020 р. № 934 «Деякі питання об'єктів критичної інформаційної інфраструктури».

Постанова Кабінету Міністрів України від 09.10.2020 р. № 1109 «Деякі питання об'єктів критичної інфраструктури».

Постанова Кабінету Міністрів України від 11.11.2020 р. № 1176 «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом».

Постанова Кабінету Міністрів України від 23.12.2020 р. № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки».

Постанова Кабінету Міністрів України від 23.12.2020 р. № 1363 «Про реалізацію експериментального проекту щодо запровадження комплексу організаційно-технічних заходів з виявлення вразливостей і недоліків у налаштуванні інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, в яких обробляються державні інформаційні ресурси».

Постанова Кабінету Міністрів України від 29.12.2021 р. № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту».

Наказ Адміністрації Держспецзв'язку від 02.12.2014 р. № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

Наказ Адміністрації Держспецзв'язку від 15.01.2016 р. № 20 «Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті», зареєстрований в Міністерстві юстиції України 05 лютого 2016 р. за № 196/28326.

Наказ Адміністрації Держспецзв'язку від 26.03.2007 р. № 45 «Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сферах технічного захисту інформації», зареєстрований в Міністерстві юстиції України 10 квітня 2007 р. за № 320/13587.

Наказ Адміністрації Держспецзв'язку від 06.10.2021 р. № 601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури».

Міжнародні стандарти у сферах безпеки інформації, інформаційної та кібербезпеки.

Державні нормативні документи у сферах безпеки інформації, інформаційної та кібербезпеки, створення і функціонування систем управління інформаційною безпекою (далі – СУІБ), комплексних систем захисту інформації (далі – КСЗІ), технічного захисту інформації (далі – ТЗІ), нормативні документи технічного захисту інформації (далі – НД ТЗІ), галузеві стандарти відповідного спрямування.

Документи National Institute of Standards and Technology United States of America (далі – NIST USA) щодо інформаційної безпеки, кібербезпеки, ТЗІ, СУІБ.

Інші нормативно-правові, нормативно-технічні та нормативні акти, які регламентують питання безпеки інформації в інформаційно-комунікаційних системах та кіберпросторі.

4. Загальні компетентності

Умовне позначення	Загальні компетентності
ЗК.01	Здатність діяти соціально відповідально та громадсько свідомо
ЗК.02	Здатність застосовувати знання у практичних ситуаціях, розв'язувати завдання/задачі та практичні проблеми у професійній діяльності
ЗК.03	Здатність оцінювати та забезпечувати якість виконуваних робіт
ЗК.04	Здатність до абстрактного мислення, аналізу та синтезу, вчитися і бути сучасно навченим
ЗК.05	Здатність до адаптації та дії у новій ситуації
ЗК.06	Здатність до вибору стратегії спілкування, працювати в команді
ЗК.07	Здатність спілкуватися рідною мовою як усно, так і письмово, спілкуватися іноземною мовою (переважно англійською) на рівні, що забезпечує ефективну професійну діяльність

5. Перелік трудових функцій (професійних компетентностей за трудовою дією або групою трудових дій, що належать до них), умовні позначення

Умовне позначення	Трудові функції	Професійні компетентності (за трудовою дією або групою трудових дій)	Умовне позначення
А	Проєктування систем захисту інформації	Здатність аналізувати проєктні обмеження, аналізувати компроміси та детальний проєкт системи, а також розглядати підтримку її життєвого циклу	А1
		Здатність проєктувати апаратне забезпечення, операційні системи та прикладне програмне забезпечення для належного дотримання вимог кібербезпеки	А2
Б	Розроблення компонентів систем захисту інформації	Здатність розробляти вимоги до безпеки та її врахування у всіх системах захисту інформації або прикладних програмах	Б1
		Здатність розробляти стратегії зменшення ризиків для усунення вразливостей із урахуванням рекомендацій щодо зміни заходів безпеки у системі або системних компонентах	Б2
		Здатність забезпечувати, щоб діяльність із проєктування та розвитку кібербезпеки (з наданням функціонального опису впровадження безпеки) була належним чином задокументована і оновлювалася у разі потреби	Б3
В	Оцінювання та впровадження систем захисту інформації та їх компонентів	Здатність оцінювати системи кібербезпеки або продукти, що сприяють кібербезпеці	В1
		Здатність здійснювати заходи щодо тестування та оцінки систем безпеки та сертифікації	В2
		Здатність впроваджувати проєкти системи безпеки для нових або наявних систем захисту інформації	В3
Г	Координація діяльності з розроблення систем захисту інформації	Здатність здійснювати технічне керівництво профільними розробниками систем захисту інформації	Г1
		Здатність взаємодіяти з керівництвом, технологічними та іншими підрозділами підприємства/організації стосовно технологічних питань відповідного спрямування	Г2
		Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень	Г3

6. Опис трудових функцій (трудові функції; предмети і засоби праці (обладнання, устаткування, матеріали, продукти, інструмент; професійні компетентності (за трудовою дією або групою трудових дій), знання, уміння та навички)

Трудові функції	Предмети і засоби праці (обладнання, устаткування, матеріали, продукти, інструменти)	Професійні компетентності (за трудовою дією або групою трудових дій)	Знання	Уміння та навички
А. Проєктування систем захисту інформації	Нормативні акти, проєктна документація, протоколи, стандарти та сертифікати відповідного спрямування; комп'ютерне, програмне та техніко-технологічне забезпечення; операційні системи; інтерпретовані та компільовані мови програмування; комп'ютерні алгоритми, криптографічніалго-ритми; бази даних; інструменти проєктування систем захисту інформації	**А1.** Здатність аналізувати проєктні обмеження, аналізувати компроміси та детальний проєкт системи, а також розглядати підтримку її життєвого циклу	**А1.З1.** Концепції і протоколи комп'ютерних мереж, методології забезпечення мережевої безпеки **А1.З2.** Принципи кібербезпеки та приватності **А1.З3.** Класифікація кіберзагроз і вразливостей **А1.З4.** Класифікація операційних наслідків у результаті помилок кібербезпеки **А1.З5.** Політики, вимоги та процедури безпеки ланцюжка постачання інформаційних технологій та управління ризиками ланцюжка постачання **А1.З6.** Принципи та методи структурного аналізу **А1.З7.** Технологічні процеси систем **А1.З8.** Моделі системи	**А1.У1.** Використовувати моделі та симуляції для аналізу або прогнозування продуктивності системи за різних умов експлуатації **А1.У2.** Визначати та пріоритезувати основні системні функції або підсистеми, необхідні для підтримки основних можливостей або бізнес-функцій з метою відновлення або поновлення після відмови системи або під час відновлення системи на основі загальних системних вимог щодо безперервності та доступності **А1.У3.** Аналізувати потреби та вимоги користувачів із метою планування і проведення розробки систем захисту інформації **А1.У4.** Визначати потреби в забезпеченні безпеки систем інформаційних технологій **А1.У5.** Застосовувати принципи кібербезпеки при формуванні вимог підприємства/ організації (стосовно конфіденційності, цілісності, доступності, автентифікації і неспростовності) **А1.У6.** Відстежувати системні вимоги з

			безпеки (модель Белла-Лападули, моделі забезпечення цілісності «Biba» і Кларка-Вілсона)	метою проєктування компонентів та виконувати аналіз недоліків розробки **А1.У7.** Застосовувати процеси управління ризиками (методи оцінки та зниження ризиків) **А1.У8.** Застосовувати інтерпретовані та компільовані мови програмування **А1.У9.** Застосовувати процеси проєктування мереж, включно з розумінням цілей системи безпеки, операційних цілей і компромісів
		А2. Здатність проєктувати апаратне забезпечення, операційні системи та прикладне програмне забезпечення для належного дотримання вимог кібербезпеки	**А2.31.** Класифікація комп'ютерних алгоритмів **А2.32.** Класифікація криптографічних алгоритмів і протоколів **А2.33.** Типи, зміст і структуру систем баз даних **А2.34.** Електротехніка, яка застосовується в архітектурі комп'ютера (друковані плати, процесори, мікросхеми та технічне забезпечення) **А2.35.** Принципи та концепції мережевих зв'язків на локальних і глобальних рівнях, включно з управлінням пропускною здатністю (трафіком) **А2.36.** Математика (логарифми, тригонометрію, лінійну алгебру, математичний аналіз, статистику та теорію	**А2.У1.** Розробляти або інтегрувати відповідні резервні спроможності у загальні проєкти системи, забезпечувати відповідні технічні та процедурні процеси для безпечного резервного копіювання системи та захищеного зберігання резервних даних **А2.У2.** Розробляти проєкти з кібербезпеки з метою задоволення специфічних операційних потреб і факторів середовища (управління доступом, автоматизовані прикладні програми, мережеві операції, високі вимоги щодо цілісності, доступності, багаторівневої безпеки/ обробки даних, що мають різні ступені секретності, та обробки інформації із особливим режимом зберігання) **А2.У3.** Описувати та відображати рішення щодо вразливості системи у проєкти систем (повіщення про вразливість системи кібербезпеки) **А2.У4.** Проєктувати архітектури та загальні принципи функціонування об'єкту розроблення

			оптимізації і аналіз операцій) **А2.37.** Концепції архітектури безпеки мережі, включно з топологією, протоколами, компонентами і принципами (прикладна система ешелонованого захисту) **А2.38.** Криптологія та криптоаналіз **А2.39.** Теорія інформації (кодування джерела, канальне кодування, теорія складності алгоритмів і стиснення даних) **А2.310.** Концепції паралельних і розподілених обчислень **А2.311.** Засоби контролю доступу, адаптивні до ризиків і засновані на політиці кібербезпеки **А2.312.** Інструменти, методи та методики проєктування систем, включно з автоматизованими системами аналізу та інструментами проєктування **А2.313.** Інженерні концепції розробки процесів і процедур захисту інформації	**А2.У5.** Застосовувати концепції архітектури безпеки мереж, включно з топологією, протоколами, компонентами та принципами (застосунки з ешелонованим захистом) **А2.У6.** Інтегрувати та застосовувати політику, яка відповідає цілям безпеки системи **А2.У7.** Використовувати проєктне моделювання (універсальна мова моделювання) **А2.У8.** Застосовувати принципи та методи кібербезпеки, а також організаційні вимоги (щодо забезпечення конфіденційності, цілісності, доступності, автентифікації і неспростовності) **А2.У9.** Застосовувати принципи, моделі, інструменти та методи управління мережевими системами (наскрізний моніторинг продуктивності систем) **А2.У10.** Застосовувати інструменти, методи і техніки проєктування систем, включно з інструментами автоматизованого аналізу та проєктування систем **А2.У11**. Проєктувати інтеграцію апаратних і програмних рішень **А2.У12.** Застосовувати принципи стійкості та надмірності в комп'ютерних системах і системах захисту інформації **А2.У13.** Застосовувати принципи взаємодії «людина-комп'ютер» **А2.У14.** Застосовувати принципи створення систем захисту інформації (NIST SP 800-160)
Б. Розроблення	Нормативні акти,	**Б1**. Здатність	**Б1.31.** Принципи управління	**Б1.У1.** Застосовувати процедури управління

компонентів систем захисту інформації	проєктна документація, протоколи, стандарти та сертифікати відповідного спрямування; комп'ютерне, програмне та техніко-технологічне забезпечення; операційні системи; інтерпретовані та компільовані мови програмування; комп'ютерні алгоритми, криптографічніалго-ритми; бази даних; інструменти розроблення систем захисту інформації	розробляти вимоги до безпеки та її врахування у всіх системах захисту інформації або прикладних програмах	життєвим циклом системи, включно з забезпеченням безпеки та експлуатаційної придатності програмного забезпечення **Б1.32.** Концепції телекомунікацій (комунікаційні канали, бюджетування системних каналів зв'язку, спектральна ефективність, мультиплексування) **Б1.33.** Методи автентифікації доступу **Б1.34.** Типи, будову та характеристики мікропроцесорів **Б1.35.** Порядок, принципи та правила управління мережевим доступом, ідентифікацією та доступом (інфраструктура відкритих ключів, автентифікація об'єктів, відкриті ідентифікатори, мова розмітки для контролю захищеності, мова розмітки для надання послуг) **Б1.36.** Типи, будова та характеристики операційних систем **Б1.37.** Теорія управління потоками в мережах (протокол	конфігурацією **Б1.У2.** Застосовувати методи, стандарти та методики для опису, аналізу і документування архітектури корпоративної інформаційної технології організації (The Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Framework Architecture Framework (FEAF)) **Б1.У3.** Розробляти контролі безпеки на основі принципів і доктрин кібербезпеки **Б1.У4.** Розробляти та застосовувати засоби контролю доступу в системах захисту інформації **Б1.У5.** Застосовувати політики безпеки до прикладних програм, які взаємодіють одна з одною, прикладних програм таких як Business-to-Business (B2B) **Б1.У6.** Впроваджувати та інтегрувати методології життєвого циклу розробки систем (SDLC) (IBM «Rational Unified Process») у середовище розробки **Б1.У7.** Розробляти та модифіковувати системи захисту інформації, їхні прототипи за допомогою робочих моделей або теоретичних моделей **Б1.У8.** Розробляти функції управління криптографічними ключами **Б1.У9.** Зберігати, відновлювати та обробляти дані для аналізу можливостей системи та вимог **Б1.У10.** Розробляти, інтегрувати та оновлювати показники захищеності системи,

			управління переданням, протокол міжмережевого обміну даними, моделі взаємодії відкритих систем, бібліотеки інфраструктури інформаційних технологій, поточної версії) **Б1.38.** Моделі розробки програмного забезпечення (каскадна модель, спіральна модель) **Б1.39.** Технологія побудови програмного забезпечення	які забезпечують конфіденційність, цілісність, доступність, автентифікацію і неспростовність **Б1.У11.** Розробляти контрзаходи для виявлення ризиків безпеки
		Б2. Здатність розробляти стратегії зменшення ризиків для усунення вразливостей із урахуванням рекомендацій щодо зміни заходів безпеки у системі або системних компонентах	**Б2.31.** Методики управління ризиками в ланцюжку постачання (NIST SP 800-161) **Б2.32.** Системи управління безпекою інформації **Б2.33.** Класифікація контрзаходів для виявлених ризиків безпеки **Б2.34.** Мережеві протоколи, (TCP/IP, динамічного конфігурування вузлів, системи доменних імен і послуг, що надаються службою каталогів)	**Б2.У1.** Розробляти спеціальні контрзаходи з кібербезпеки та стратегії пом'якшення ризиків для систем та/або прикладних програм **Б2.У2.** Розробляти плани аварійного відновлення та безперервності операцій для систем, що розробляються, та забезпечувати тестування систем до їхнього запровадження в продуктивне середовище **Б2.У3.** Розробляти стратегії мінімізації ризиків для зменшення витрат, графіку, продуктивності та ризиків безпеки **Б2.У4.** Застосовувати принципи кібербезпеки при формуванні організаційних вимог (які стосуються конфіденційності, цілісності, доступності, автентифікації і неспростовності) **Б2.У5.** Виконувати оцінювання ризиків інформаційної безпеки

		Б3. Здатність забезпечувати, щоб діяльність із проєктування та розвитку кібербезпеки (з наданням функціонального опису впровадження безпеки) була належним чином задокументована і оновлювалася у разі потреби	**Б3.З1.** Принципи та методи забезпечення безпеки інформаційних технологій (мережеві екрани, ДМЗ, шифрування) **Б3.З2.** Програма класифікації інформації і процедури її розкриття, які використовуються на підприємстві/в організації **Б3.З3.** Класифікація та характеристики вбудованих систем **Б3.З4.** Закони, нормативні акти, політики та етичні норми, їх зв'язок з кібербезпекою і приватністю **Б3.З5.** Способи управління безпечною конфігурацією **Б3.З6.** Основи корпоративної архітектури безпеки інформації організації	**Б3.У1.** Розробляти детальну проєктну документацію з безпеки для специфікацій компонентів та інтерфейсів з метою підтримки проєкту та розробки системи **Б3.У2.** Розробляти та надавати вхідні дані для забезпечення процесу загальних принципів управління ризиками та відповідну документацію (плани забезпечення життєвого циклу системи, концепція операцій, операційні процедури та навчальні матеріали з технічного обслуговування) **Б3.У3.** Застосовувати на практиці знання корпоративної архітектури безпеки інформації організації **Б3.У4.** Визначати компоненти чи елементи, розподіляти функції безпеки для цих елементів і описувати взаємозв'язок між елементами **Б3.У5.** Застосовувати процедури інсталяції, інтеграції та оптимізації компонентів системи
В. Оцінювання та впровадження систем захисту інформації та їх компонентів	Нормативні акти, проєктна документація, протоколи, стандарти та сертифікати відповідного спрямування; комп'ютерне, програмне та техніко-технологічне	**В1.** Здатність оцінювати системи кібербезпеки або продукти, що сприяють кібербезпеці	**В1.З1.** Порядок оцінювання впливу кіберзагроз на приватність **В1.З2.** Системи критичної інфраструктури з інформаційно-комунікаційними технологіями, які були розроблені без розгляду безпеки системи	**В1.У1.** Проводити оцінювання впливу приватності проєкту безпеки прикладних програм для відповідних контролів безпеки, що захищає конфіденційність та цілісність персональних ідентифікаційних даних **В1.У2.** Підтверджувати стабільність, сумісність, портативність і/або масштабованість архітектури системи **В1.У3.** Виявляти системи критичної інфраструктури з інформаційно-

	забезпечення; операційні та системи; інтерпретовані і компільовані мови програмування; комп'ютерні алгоритми, криптографічніалгоритми; бази даних; інструменти тестування та оцінки систем захисту інформації			комунікаційними технологіями, які були спроєктовані без урахування безпеки системи **В1.У4.** Оцінювати адекватність проєктів систем захисту інформації **В1.У5.** Проводити процедури сканування вразливостей і розпізнавання вразливостей у системах захисту інформації **В1.У6.** Оцінювати ефективність заходів із кібербезпеки, які використовуються системою (системами) **В1.У7.** Оцінювати загрози та вразливості комп'ютерної системи (систем) для розробки профілю ризику безпеки
		В2. Здатність здійснювати заходи щодо тестування та оцінки систем безпеки та сертифікації	**В2.31.** Вимоги до процедур оцінки та валідації систем захисту інформації та персоналу, прийняті на підприємстві/в організації **В2.32.** Стандарти безпеки персональних ідентифікаційних даних **В2.33.** Стандарти безпеки даних індустрії платіжних карт **В2.34.** Стандарти безпеки медичних персональних даних **В2.35.** Методи тестування систем захисту інформації	**В2.У1.** Розробляти та направляти на розгляд процедури тестування та затвердження системи та документацію **В2.У2.** Тестувати та оцінювати захищені інтерфейси між інформаційними системами, фізичними системами і/або вбудованими технологіями **В2.У3.** Виконувати аналіз ризиків (загрози, вразливості та ймовірності виникнення) щоразу, коли прикладна програма або система зазнають значних змін **В2.У4.** Здійснювати огляди безпеки та виявляти прогалини в архітектурі безпеки **В2.У5.** Виявляти системні проблеми безпеки на основі аналізу даних вразливостей і конфігурації **В2.У6.** Забезпечувати, щоб рекомендовані продукти відповідали організаційним вимогам щодо їхньої оцінки та затвердження

				В2.У7. Проводити аудити/огляди технічних систем **В2.У8.** Аналізувати тестові дані **В2.У9.** Переводити дані та результати тестування в оцінкові висновки **В2.У10.** Проводити сканування вразливостей і розпізнання вразливостей у системах безпеки
		В3. Здатність впроваджувати проєкти системи безпеки для нових або наявних систем захисту інформації	**В3.31.** Способи визначення та скерування виправлень технічних проблем, що виникають при впровадженні нових систем **В3.32.** Концепції управління послугами для мереж і відповідних стандартів (бібліотека інфраструктури інформаційних технологій (ITIL)	**В3.У1.** Впроваджувати захищені інтерфейси між інформаційними системами, фізичними системами і/або вбудованими технологіями **В3.У2.** Розробляти настанови клієнтам або командам впровадження щодо впровадження розроблених систем **В3.У3.** Забезпечувати вимоги до безпеки профільних предметів і засобів праці протягом усього процесу закупівель **В3.У4.** Забезпечувати вхідні дані для планів впровадження та стандартні операційні процедури, які стосуються систем захисту інформації **В3.У5.** Впроваджувати для систем і/або програм спеціальні контрзаходи з кібербезпеки
Г. Координація діяльності з розроблення систем захисту інформації	Посадові інструкції на посади розробників систем захисту інформації, керівництва, інструкції та нормативні акти роботодавця, які застосовуються для	**Г1.** Здатність здійснювати технічне керівництво профільними розробниками систем захисту інформації	**Г1.31.** Керівництва/настанови, інструкції та/чи нормативні акти роботодавця, які застосовуються для організації та координації діяльності з розроблення систем захисту інформації **Г1.32.** Посадові інструкції на посади розробників систем	**Г1.У1.** Брати участь у координації комплексу робіт із своєчасної та якісної підготовки розроблення систем захисту інформації **Г1.У2.** Готувати службові записки та документацію, необхідну для навчання/ підвищення кваліфікації підпорядкованих розробників систем захисту інформації відповідного структурного підрозділу підприємства/організації

	організації та координації діяльності з розроблення систем захисту інформації; нормативні акти роботодавця з питань взаємодії з керівництвом, технологічними та іншими підрозділами підприємства/ організації щодо розроблення систем захисту інформації; структура підприємства/ організації; положення про структурні підрозділи підприємства/ організації; порядок і типові вимоги до проведення ділових/комерційних перемовин; порядок розроблення та виконання договірних робіт для зовнішніх партнерів		захисту інформації **Г1.33.** Основи управління персоналом	
		Г2. Здатність взаємодіяти з керівництвом, технологічними та іншими підрозділами підприємства/ організації стосовно технологічних питань відповідного спрямування	**Г2.31.** Структура, розподіл функцій між керівниками, підпорядкованість підрозділів підприємства/організації **Г2.32.** Положення про структурні підрозділи підприємства/організації, задіяні в спільному виконанні технологічних і функціональних завдань **Г2.33.** Нормативні акти роботодавця з питань взаємодії з керівництвом, технологічними та іншими підрозділами підприємства/ організації	**Г2.У1.** Узгоджувати повідомлення із заінтересованими структурними підрозділами та відповідальними посадовими особами щодо змін проєктної документації з розроблення систем захисту інформації **Г2.У2.** Готувати, обґрунтовувати та оприлюднювати пропозиції щодо покращення в структурному підрозділі/на підприємстві/в організації розроблення систем захисту інформації **Г2.У3.** Готувати документацію, необхідну для забезпечення безперебійної роботи закріпленого структурного підрозділу/групи/ дільниці
		Г3. Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень	**Г3.31.** Основи комунікаційного менеджменту **Г3.32.** Основи ділової етики **Г3.33.** Порядок і типові вимоги до проведення ділових/ комерційних перемовин **Г3.34.** Порядок розроблення та виконання договірних робіт для зовнішніх партнерів	**Г3.У1.** Спілкуватися із зовнішніми партнерами щодо питань розроблення систем захисту інформації доступними засобами комунікації **Г3.У2.** Брати участь у ділових/комерційних перемовинах із зовнішніми партнерами **Г3.У3.** Супроводжувати договірні роботи із зовнішніми партнерами

7. Дані щодо розроблення та затвердження професійного стандарту

7.1. Розробник професійного стандарту

Державна служба спеціального зв'язку та захисту інформації України.

Склад робочої групи:

Конюшок Сергій Миколайович, керівник робочої групи, заступник начальника інституту (з наукової роботи) Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського»;

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

Воронов Віктор Романович, провідний консультант 2 відділу 2 управління Департаменту захисту інформації Адміністрації Держспецзв'язку;

Гнатюк Сергій Леонідович, головний консультант відділу інформаційної безпеки та кібербезпеки Центру безпекових досліджень Національного інституту стратегічних досліджень;

Головко Ярослав Володимирович, провідний консультант 3 відділу 3 управління Департаменту захисту інформації Адміністрації Держспецзв'язку;

Іванченко Євгенія Вікторівна, професор кафедри безпеки інформаційних технологій Національного авіаційного університету;

Корнейко Олександр Васильович, завідувач кафедри інформаційних технологій та кібербезпеки Навчально-наукового інституту № 1 Національної академії внутрішніх справ;

Лебеденко Кіра Сергіївна, директор ТОВ «СЕК'ЮРИТІ ЕКСПЕРТ ГРУП ЕКЕДЕМІ»;

Лукова-Чуйко Наталія Вікторівна, завідувач кафедри кафедр кібербезпеки та захисту інформації Київського національного університет ім. Тараса Шевченка;

Мазур Наталя Володимирівна, завідуюча відділом організаційно правової роботи Профспілки працівників зв'язку України;

Насібулліна Ольга Сергіївна, керівник напрямку з розвитк професійних навичок з кібербезпеки Проєкту USAID «Кібербезпе критично важливої інфраструктури України»;

Невара Лілія Михайлівна, керівник навчально-методичного центр голова профспілкової організації Громадської організації «Українсь академія кібербезпеки»;

Павленко Володимир Анатолійович, директор Громадської організа «Глобальний центр взаємодії в кіберпросторі»;

Пазюк Андрій Валерійович, віце-президент Громадської організа «Українська академія кібербезпеки»;

Педченко Євгеній Миколайович, керівник відділу впроваджен системи безпеки ТОВ «ІНТАСИСТЕМС»;

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

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

7.2. Суб'єкт перевірки професійного стандарту

Національне агентство кваліфікацій.

7.3. Дата затвердження професійного стандарту

25 листопада 2022 року.

7.4. Рекомендована дата наступного перегляду професійного стандарту

25 листопада 2027 року.

Заступник Голови Держспецзв'язку,
керівник комплексної робочої групи
з розробки професійних стандартів
бригадний генерал Олександр ПОТІЙ