Проєкт

ЗАТВЕРДЖЕНО
Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України
від _____№_____

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 всього 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 за КВЕД-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, та технічна ість	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	Підрозділ	Клас	Підклас	Група
2	21	213	2132	2132.2
Професіонали	Професіонали в галузі фізичних, математичних та технічних наук	Професіонали в галузі обчислень (комп'ютеризації)	Професіонали в галузі програмування	Розробники комп'ютерних програм

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)

Структурний підрозділ підприємства/організації, профільний структурний підрозділ підприємства/організації із захисту інформації та кібербезпеки, профільна науково-дослідна установа, підприємство/організація, що є розробником/виробником програмних та/або апаратних засобів, які реалізовують або застосовують функції захисту інформації.

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 надаються згідно до 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 встановлюються 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 розробника систем захисту інформації та провідного розробника систем захисту інформації – диплом на другому (магістерському) рівні вищої освіти за спеціальністю:

- 113 «Прикладна математика» галузі знань 11 «Математика та статистика» (7 рівень НРК);
- 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» галузі знань 12 «Інформаційні технології» (7 рівень НРК);
- 126 «Інформаційні системи та технології» галузі знань 12 «Інформаційні технології» (7 рівень НРК);
- 151 «Автоматизація та комп'ютерно-інтегровані технології» галузі знань 15 «Автоматизація та приладобудування» (7 рівень НРК);
- 171 «Електроніка» галузі знань 17 «Електроніка та телекомунікації» (7 рівень НРК);
- 172 «Телекомунікації та радіотехніка» галузі знань 17 «Електроніка та телекомунікації» (7 рівень НРК);
- 255 «Озброєння та військова техніка» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7 рівень НРК);
- 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7 рівень НРК).

2. Навчання та професійний розвиток

2.1. Первинна професійна підготовка (назва кваліфікації)

Для розробника систем захисту інформації та провідного розробника систем захисту інформації – підготовка на другому рівні вищої освіти (магістерському) за спеціальностями вказаними п.1, п.п.1.8 галузі знань 11 «Математика та статистика», 12 «Інформаційні технології», 15 «Автоматизація та приладобудування», 17 «Електроніка та телекомунікації» та 25 «Воєнні науки, національна безпека, безпека державного кордону».

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

Підвищення кваліфікації розробника систем захисту інформації для отримання професійної кваліфікації «Провідний розробник систем захисту інформації». Стаж роботи не менше двох років на посадах, що відповідають кваліфікації розробника систем захисту інформації.

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

Закон України "Про інформацію";

Закон України "Про державну таємницю";

Закон України "Про основні засади забезпечення кібербезпеки України";

Закон України "Про електронні комунікації";

Закон України "Про захист інформації в інформаційно-комунікаційних системах";

Закон України "Про національну безпеку України";

Закон України "Про захист персональних даних";

Закон України "Про захист прав споживачів";

Закон України "Про доступ до публічної інформації";

Указ Президента України від 13.02.2017 № 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 № 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", введеного в дію Указом Президента України від 13 лютого 2017 року № 32";

Указ Президента України від 26.08.2021 № 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 № 518 "Про затвердження загальних вимог з кіберзахисту об’єктів критичної інфраструктури";

Постанова Кабінету Міністрів України від 09.10.2020 № 934 "Деякі питання об’єктів критичної інформаційної інфраструктури";

Постанова Кабінету Міністрів України від 09.10.2020 № 1109 "Деякі питання об'єктів критичної інфраструктури";

Постанова Кабінету Міністрів України від 11.11.2020 № 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 № 1295 "Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки";

Постанова Кабінету Міністрів України від 23.12.2020 № 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 № 1426 "Про затвердження Положення про організаційно-технічну модель кіберзахисту".

Наказ Адміністрації Держспецзв'язку від 02.12.2014 № 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 № 20 "Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті".

Наказ Адміністрації Держспецзв'язку від 26.03.2007 № 45 "Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сферах технічного захисту інформації".

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

Наказ Адміністрації Держспецзв'язку від 28.10.2021 № 640 "Про внесення змін до Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті".

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 (СУІБ), комплексних систем захисту інформації (КСЗІ), технічного захисту інформації (ТЗІ), нормативні документи технічного захисту інформації (НД ТЗІ), галузеві стандарти відповідного спрямування;

Документи National Institute of Standards and Technology United States of America (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

ЗК.01	Здатність використовувати у професійній діяльності знання законів та підзаконних нормативно-правових актів України, нормативних і нормативно-технічних документів, галузевих стандартів у сфері розроблення систем захисту інформації
ЗК.02	Здатність дотримуватися правил та норм з безпеки та охорони праці, зокрема щодо безпечної експлуатації електронного устаткування та електричного обладнання
ЗК.03	Здатність застосовувати знання у практичних ситуаціях, розв'язувати спеціалізовані завдання/задачі та практичні проблеми у професійній діяльності
ЗК.04	Здатність оцінювати та забезпечувати якість виконуваних робіт
ЗК.05	Здатність до абстрактного мислення, аналізу та синтезу, вчитися і бути сучасно навченим.
ЗК.06	Здатність до адаптації та дії у новій ситуації
ЗК.07	Здатність до вибору стратегії спілкування, працювати в команді
ЗК.08	Здатність спілкуватися рідною мовою як усно, так і письмово, спілкуватися другою мовою (переважно англійською) на рівні, що забезпечує ефективну професійну діяльність
ЗК.09	Здатність ставити уточнюючі питання
ЗК.10	Здатність впевнено і систематизовано доводити складну інформацію, концепції або ідеї в усній і письмовій формах і/або за допомогою наочних засобів
ЗК.11	Здатність ефективно співпрацювати з іншими
ЗК.12	Здатність розробляти технічну документацію
ЗК.13	Здатність застосовувати інструменти, методи і техніки розробки безпечних систем
ЗК.14	Здатність брати участь в якості члена груп планування, координаційних і оперативних груп
ЗК.15	Здатність розуміти цілі та результати
ЗК.16	Здатність розуміти основні поняття і проблеми, пов'язані з діяльністю організації в кіберпросторі та її впливом
ЗК.17	Здатність працювати в колективі, постійно звертаючись за консультаціями до аналітиків і експертів (внутрішніх і зовнішніх організацій) для використання аналітичного і технічного досвіду.

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

Умовні позначення	Трудові функції	Професійні компетентності (за трудовою дією або групою трудових дій)	Умовні позначення
А	Проєктування систем захисту інформації	Здатність аналізувати проєктні обмеження, аналізувати компроміси та детальний проєкт системи та безпеки, а також розглядати підтримку 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 розроблювати вимоги до безпеки та її урахування у всіх системах захисту інформації або прикладних програмах	Б1
		Здатність розроблювати стратегії зменшення ризиків для усунення вразливостей з ураховуванням рекомендацій щодо зміни заходів безпеки у системі або системних компонентах	Б2
		Здатність забезпечувати, щоб діяльність з проєктування та розвитку кібербезпеки (з наданням функціонального опису впровадження безпеки) була належним чином задокументована і оновлювалася за необхідності	Б3

В	Оцінювання та впровадження систем захисту інформації та їх компонентів	Здатність оцінювати системи кібербезпеки або продукти, що сприяють кібербезпеці	В1
		Здатність забезпечувати заходи щодо тестування та оцінки систем безпеки та сертифікації	В2
		Здатність впроваджувати проєкти системи безпеки для нових або існуючих 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, інструменти)	Професійні компетентності	Знання	Уміння і навички
А. Проєктування систем захисту інформації	Нормативні акти, проєктна документація, протоколи, стандарти та сертифікати відповідного спрямування; компьютерне, програмне та інше техніко-технологічне забезпечення; операційні та інші системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні	**А1.** Здатність аналізувати проєктні обмеження, аналізувати компроміси та детальний проєкт системи, а також розглядати підтримку життєвого циклу	**А1.З1.** Концепції і протоколи комп'ютерних мереж, методології забезпечення мережевої безпеки **А1.З2**. Принципи кібербезпеки і приватності **А1.З3.** Класифікацію кіберзагроз та вразливостей **А1.З4**. Класифікацію операційних наслідків в результаті помилок кібербезпеки **А1.З5**. Політики, вимоги і процедури безпеки ланцюжка постачання інформаційних технологій та управління ризиками ланцюжка постачання **А1.З6.** Принципи і методи структурного аналізу **А1.З7.** Технологічні процеси систем **А1.З8.** Моделі системи безпеки	**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, необхідним 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 з метою планування і проведення розробки систем захисту інформації **А1.У4.** Визначати потреби в забезпеченні безпеки систем

	алгоритми, криптографічні алгоритми; бази даних; інші інструменти проєктування систем захисту інформації		(наприклад, модель Белла-Лападули, моделі забезпечення цілісності «Biba» і Кларка-Вілсона тощо)	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 метою проєктування компонентів та виконувати аналіз недоліків розробки **А1.У7**. Застосовувати процеси управління ризиками (наприклад, методи оцінки та зниження ризиків) **А1.У8.** Застосовувати інтерпретовані і компільовані комп'ютерні мови **А1.У9.** Процеси проєктування мереж, включаючи розуміння цілей системи безпеки, операційних цілей та компромісів
		А2. Здатність проєктувати апаратне забезпечення, операційні системи та прикладне програмне	**А2.31.** Класифікацію комп'ютерних алгоритмів **А2.32.** Класифікацію криптографічних алгоритмів і протоколів **А2.33**. Типи, зміст та структуру систем баз даних **А2.34.** Електротехніку, яка	**А2.У1**. Розробляти або інтегрувати відповідні резервні спроможності у загальні проєкти системи та забезпечувати відповідні технічні та процедурні процеси для безпечного резервного копіювання системи та захищеного зберігання резервних даних

		забезпечення для належного дотримання вимог кібербезпеки	застосовується в архітектурі комп'ютера (наприклад, друковані плати, процесори, мікросхеми та технічне забезпечення) **А2.З5**. Принципи і концепції мережевих зв'язків на локальних і глобальних рівнях, включаючи управління пропускної здатністю (трафіком) **А2.З6**. Математику (наприклад, логарифми, тригонометрію, лінійну алгебру, математичний аналіз, статистику і операційний аналіз) **А2.З7**. Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи (наприклад, прикладна система ешелонованого захисту тощо) **А2.З8**. Криптологію та криптоаналіз **А2.З9**. Теорію інформації (наприклад, кодування джерела, канальне кодування, теорія складності алгоритмів і стиснення даних, тощо) **А2.З10**. Концепції паралельних і	**А2.У2**. Розробляти проєкти з кібербезпеки з метою задоволення специфічних операційних потреб та факторів середовища (наприклад, управління доступом, автоматизовані прикладні програми, мережеві операції, високі вимог щодо цілісності, доступності, багаторівневої безпеки / обробки даних, що мають різні ступені секретності, та обробки інформації з особливим режимом зберігання) **А2.У3**. Включати рішення щодо вразливості системи у проєкти систем (наприклад, сповіщення про вразливість системи кібербезпеки) **А2.У4.** Проєктувати архітектури та загальні принципи **А2.У5**. Застосовувати концепції архітектури безпеки мереж, включаючи топологію, протоколи, компоненти і принципи (наприклад, застосунки з «ешелонованим захистом) **А2.У6**. Інтегрувати та застосовувати політику, яка відповідає цілям безпеки системи **А2.У7**. Використовувати проєктне

			розподілених обчислень **А2.З11**. Засоби контролю доступу, адаптивні до ризиків і заснованих на політиці кібербезпеки **А2.З12**. Інструменти, методи і методики проєктування систем, включаючи автоматизовані системи аналізу і інструменти проєктування **А2.З13.** Інженерні концепції розробки процесів і процедур захисту інформації	моделювання (наприклад, універсальна мова моделювання, тощо) **А2.У8**. Застосовувати принципи і 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 (наприклад, наскрізний моніторинг продуктивності систем тощо) **А2.У10**. Застосовувати інструменти, методи і техніки проєктування систем, включаючи інструменти автоматизованого аналізу та проєктування систем **А2.У11**. Проєктувати інтеграцію апаратних і програмних рішень **А2.У12.** Застосовувати принципи стійкості і надмірності в комп'ютерних системах та системах захисту інформації **А2.У13.** Застосовувати принципи взаємодії "людина-комп’ютер" **А2.У14.** Застосовувати принципи

				створення систем захисту інформації (наприклад, NIST SP 800-160)
Б. Розроблення компонентів систем захисту інформації	Нормативні акти, проєктна документація, протоколи, стандарти та сертифікати відповідного спрямування; компьютерне, програмне та інше техніко-технологічне забезпечення; операційні та інші системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми, криптографічні алгоритми; бази даних; інші інструменти розроблення	**Б1**. Здатність розроблювати вимоги до безпеки та її урахування у всіх системах захисту інформації або прикладних програмах	**Б1.З1.** Принципи управління життєвим циклом системи, включаючи забезпечення безпеки та експлуатаційної придатності програмного забезпечення **Б1.З2**. Концепції телекомунікацій (наприклад, комунікаційні канали, бюджетування системних каналів зв'язку, спектральна ефективність, мультиплексування тощо) **Б1.З3.** Методи автентифікації доступу **Б1.З4.** Типи, будову та інші характеристики мікропроцесорів **Б1.З5.** Порядок, принципи та правила 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.З6**. Типи, будову та інші характеристики операційних систем	**Б1.У1.** Застосовувати процедури управління конфігурацією **Б1.У2**. Застосовувати методи, стандарти та методики для опису, аналізу та документування архітектури корпоративної інформаційної технології організації (наприклад, The Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Framework Architecture Framework (FEAF)) **Б1.У3**. Розроблвати контролі безпеки на основі принципів і доктрин кібербезпеки **Б1.У4**. Розроблювати і застосувати засоби контролю доступу в системах захисту інформації **Б1.У5.** Застосовувати політики безпеки до прикладних програм, які взаємодіють одна з одною, наприклад, прикладних програм таких як Business-to-Business (B2B) **Б1.У6.** Впроваджувати та інтегрувати методології життєвого

	систем захисту інформації		**Б1.З7.** Теорію управління потоками в мережах (наприклад, протоколу управління передачею, протоколу міжмережевого обміну даними, моделі взаємодії відкритих систем, бібліотеки інфраструктури інформаційних технологій, поточної версії) **Б1.З8**. Моделі розробки програмного забезпечення (наприклад, каскадна модель, спіральна модель тощо) **Б1.З9.** Технологію побудови програмного забезпечення	циклу розробки систем (SDLC) (наприклад, IBM «Rational Unified Process») в середовище розробки **Б1.У7.** Здатність розроблювати та модифіковувати системи захисту інформації, їх прототипи за допомогою робочих моделей або теоретичних моделей **Б1.У8.** Розроблювати функції управління криптографічними ключами **Б1.У9.** Зберігати, відновлювати та обробляти дані для аналізу можливостей системи та вимог **Б1.У10**. Розроблювати, інтегрувати і оновлювати показники захищеності системи, які забезпечують конфіденційність, цілісність, доступність, автентифікацію і неспростовність **Б1.У11**. Розроблювати контрзаходи для виявлення ризиків безпеки
		Б2. Здатність розроблювати стратегії зменшення ризиків для усунення	**Б2.З1.** Методики управління ризиками в ланцюжку постачання (наприклад, NIST SP 800-161) **Б2.З2.** Системи управління безпекою інформації **Б2.З3.** Класифікацію контрзаходів	**Б2.У1**. Розроблювати спеціальні контрзаходи з кібербезпеки та стратегії пом’якшення ризиків для систем та/або прикладних програм **Б2.У2.** Розроблювати плани аварійного відновлення та

		вразливостей з ураховуванням рекомендацій щодо зміни заходів безпеки у системі або системних компонентах	для виявлених ризиків безпеки **Б2.З4.** Мережеві протоколи, (наприклад, TCP/IP, динамічного конфігурування вузлів, системи доменних імен і послуг, що надаються службою каталогів тощо)	безперервності операцій для систем, що розробляються, та забезпечувати тестування систем до їхнього вводу у продуктивне середовище **Б2.У3.** Розроблювати стратегії мінімізації ризиків для зменшення витрат, графіку, продуктивності і ризиків безпеки **Б2.У4**. Застосовувати принципи кібербезпеки при формуванні організаційних вимог (які стосуються конфіденційності, цілісності, доступності, автентифікації і неспростовності) **Б2.У5**. Виконувати оцінку ризиків інформаційної безпеки
		Б3. Здатність забезпечувати, щоб діяльність з проєктування та розвитку кібербезпеки (з наданням функціонального опису впровадження безпеки) була належним чином	**Б3.З1**. Принципи і методи забезпечення безпеки інформаційних технологій (наприклад, мережеві екрани, ДМЗ, шифрування) **Б3.З2**. Програму класифікації інформації і процедури її розкриття, які використовуються на підприємстві/ в організації **Б3.З3**. Класифікацію та характеристики вбудованих систем	**Б3.У1**. Розроблювати детальну проєктну документацію з безпеки для специфікацій компонентів та інтерфейсів з метою підтримки проєкту та розробки системи **Б3.У2**. Розроблювати та надавати вхідні дані для діяльності процесу загальних принципів управління ризиками та відповідну документацію (наприклад, плани забезпечення життєвого циклу системи, концепція операцій,

		задокументована і оновлювалася за необхідності	**Б3.З4**. Закони, нормативні акти, політики і етичні норми, та як вони пов'язані з кібербезпекою і приватністю **Б3.З5.** Способи управління безпечною конфігурацією	операційні процедури і навчальні матеріали з технічного обслуговування) **Б3.У3**. 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.З5.** 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; компьютерне, програмне та інше техніко-технологічне забезпечення; операційні та	**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 оцінки впливу приватності проекту 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-телекомунікаційними технологіями,

	інші системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми, криптографічні алгоритми; бази даних; інші інструменти тестування та оцінки систем захисту інформації			які були спроєктовані без врахування безпеки системи **В1.У4.** Оцінювати адекватність проєктів систем захисту інформації **В1.У5.** Проводити процедури сканування вразливостей і розпізнавання вразливостей в системах захисту інформації **В1.У6.** Оцінювати ефективність заходів з кібербезпеки, які використовуються системою (системами) **В1.У7**. Оцінювати загрози та вразливості комп'ютерної системи (систем) для розробки профілю ризику безпеки
		В2. Здатність забезпечувати заходи щодо тестування та оцінки систем безпеки та сертифікації	**В2.З1**. Вимоги до процедур оцінки і валідації систем захисту інформації та персоналу, прийнятих на підприємстві/в організації **В2.З2.** Стандарти безпеки персональних ідентифікаційних даних **В2.З3**. Стандарти безпеки даних індустрії платіжних карт **В2.З4**. Стандарти безпеки медичних персональних даних	**В2.У1**. Розроблювати та направляти на розгляд процедури тестування та затвердження системи і документацію **В2.У2.** Тестувати і оцінювати захищені інтерфейси між інформаційними системами, фізичними системами і/або вбудованими технологіями **В2.У3.** Виконувати аналіз ризиків (наприклад, загрози, вразливості та ймовірності виникнення) щоразу,

			В2.З5. Методи тестування систем захисту інформації	коли прикладна програма або система зазнають значних змін **В2.У4**. Здійснювати огляди безпеки та виявляти пробіли в архітектурі безпеки **В2.У5.** Виявляти системні проблеми безпеки на основі аналізу даних вразливостей та 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 і результати тестування в оціночні висновки **В2.У10.** Проводити сканування вразливостей і розпізнання вразливостей в системах безпеки
		В3. Здатність впроваджувати проєкти системи безпеки для нових або існуючих систем захисту інформації	**В3.З1.** Як визначати та скеровувати виправлення технічних проблем, що виникають при впровадженні нових систем **В3.З2.** Концепції управління послугами для мереж і відповідних стандартів (наприклад, бібліотека	**В3.У1.** Впроваджувати захищені інтерфейси між інформаційними системами, фізичними системами і/або вбудованими технологіями **В3.У2**. Розробляти/приймати участь настанови стосовно впровадження розроблених систем клієнтам або командам впровадження

			інфраструктури інформаційних технологій (ITIL) тощо)	**В3.У3**. Забезпечити практики безпеки протягом усього процесу закупівель **В3.У4**. Забезпечувати вхідні дані для планів впровадження і стандартні операційні процедури, які стосуються систем захисту інформації **В3.У5.** Впроваджувати для систем та/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 інші нормативні акти роботодавця, які застосовуються для організації та координації діяльності з розроблення	**Г1.** Здатність здійснювати технічне керівництво профільними розробниками систем захисту інформації	**Г1.З1**. Керівництва/настанови, інструкції та/чи інші нормативні акти роботодавця, які застосовуються для організації та координації діяльності з розроблення систем захисту інформації **Г1.З2**. Посадові інструкції на посади розробників систем захисту інформації **Г1.З3**. Основи управління персоналом	**Г1.У1**. Приймати участь у координації комплексу робіт із своєчасної та якісної підготовки розроблення систем захисту інформації **Г1.У2.** Готувати службові записки та іншу документацію, необхідну для навчання/підвищення кваліфікації підпорядкованих розробників систем захисту інформації відповідного структурного підрозділу підприємства/організації
		Г2. Здатність взаємодіяти з керівництвом, технологічними та іншими	**Г2.З1.** Структуру, розподіл функцій між керівниками, підпорядкованість підрозділів тощо підприємства/організації **Г2.З2**. Положення про структурні	**Г2.У1.** Узгоджувати повідомлення із заінтересованими структурними підрозділами та відповідальними посадовими особами щодо змін проєктної документації з

	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/	підрозділами підприємства/ організації стосовно технологічних питань відповідного спрямування	підрозділи підприємства\організації, задіяні в спільному виконанні технологічних та інших функціональних завдань **Г2.З3**. Нормативні акти роботодавця з питань взаємодії з керівництвом, технологічними та іншими підрозділами підприємства/організації	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 іншу документацію, необхідну для забезпечення безперебійної роботи закріпленого структурного підрозділу/групи/дільниці
		Д3. Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень	**Г3.З1**. Основи комунікаційного менеджменту **Г3.З2**. Основи ділової етики **Г3.З3.** Порядок і типові вимоги до проведення ділових/комерційних перемовин **Г3.З4**. Порядок розроблення та виконання договірних робіт для зовнішніх партнерів	**Г3.У1**. Проводити спілкування із зовнішніми партнерами стосовно питань розроблення систем захисту інформації доступними засобами комунікації **Г3.У2**. Приймати участь в ділових/комерційних перемовинах із зовнішніми партнерами **Г3.У3**. Супроводжувати договірні роботи із зовнішніми партнерами

	комерційних перемовин; порядок розроблення та виконання договірних робіт для зовнішніх партнерів			

7. Дані щодо розроблення та затвердження професійного стандарту

7.1. Розробники проекту професійного стандарту

Державна служба спеціального зв'язку та захисту інформації України.

Колектив розробників професійного стандарту: Волкова Ксенія, заступник начальника управління правового співробітництва з міжнародними організаціями Департаменту міжнародного права Міністерства юстиції України; Воронов Віктор, провідний консультант департаменту захисту інформації Держспецзв'язку України; Гнатюк Сергій, головний консультант відділу інформаційної безпеки та кібербезпеки Центру безпекових досліджень Національного інституту стратегічних досліджень; Головко Ярослав, провідний консультант департаменту захисту інформації Держспецзв'язку України; Іванченко Євгенія, професор кафедри безпеки інформаційних технологій Національного авіаційного університету; Конюшок Сергій, заступник начальника інституту (з наукової роботи) Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"; Корнейко Олександр, завідувач кафедри інформаційних технологій та кібербезпеки Навчально-наукового інституту № 1 Національної академії внутрішніх справ; Лебеденко Кіра, директор ТОВ «СЕК'ЮРИТІ ЕКСПЕРТ ГРУП ЕКЕДЕМІ»; Мазур Наталія, заступник Голови Профспілки працівників зв'язку України; Насібулліна Ольга, керівник напрямку з розвитку професійних навичок з кібербезпеки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»; Павелко Володимир, директор Громадської організації «Глобальний центр взаємодії в кіберпросторі»; Пазюк Андрій, віце-президент Громадської організації «Українська академія кібербезпеки»; Педченко Євгеній, керівник відділу впровадження систем безпеки ТОВ «ІНТРАСИСТЕМС»; Рибка Михайло, провідний консультант департаменту захисту інформації Держспецзв'язку України; Юдін Олександр, професор кафедри кібербезпеки Науково-навчального інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України.

7.2. Суб'єкт перевірки професійного стандарту

Національне агентство кваліфікацій

7.3. Дата затвердження професійного стандарту

7.4. Дата внесення професійного стандарту до Реєстру професійних стандартів

7.5. Рекомендована дата наступного перегляду професійного стандарту

Вересень 2027 року.