Прим. № __

ЗАТВЕРДЖЕНО

Наказ Адміністрації Держспецзв'язку
25 листопада 2022 року № 715

Професійний стандарт
«Фахівець з питань безпеки (інформаційно-комунікаційні технології)»

1. Загальні відомості професійного стандарту

1.1. Основна мета професійної діяльності

Організація та забезпечення кібербезпеки інформаційних систем та інформаційно-комунікаційних технологій; управління наслідками реалізації загроз інформаційної безпеки в межах організації, в тому числі управління спеціальними програмами (проєктами) інших сфер відповідальності; формування стратегічного розвитку організації, персоналу, інфраструктури, вимог до безпеки, а також розробка та впровадження політики та стратегії інформаційної безпеки інституції; планування заходів безпеки інформації та кіберзахисту на випадок надзвичайних ситуацій або при реалізації інцидентів; обізнаність про безпеку інформаційних ресурсів організації або анклаву, установ та підприємств різних форм власності.

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 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

				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
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**	**2139**
Професіонали	Професіонали в галузі обчислень (комп'ютеризації)	Професіонали в інших галузях обчислень (комп'ютеризації)

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

Фахівець з питань безпеки (інформаційно-комунікаційні технології) 2139.2.

1.5. Професійна кваліфікація

Фахівець з питань безпеки (інформаційно-комунікаційні технології) (трудові функції А, Б, В, Г).

Провідний фахівець з питань безпеки (інформаційно-комунікаційні технології) (трудові функції А, Б, В, Г, Д).

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

Обіймає посаду фахівця з питань безпеки (інформаційно-комунікаційні технології), провідного фахівця з питань безпеки (інформаційно-комунікаційні технології).

Фахівець з питань безпеки (інформаційно-комунікаційні технології), провідний фахівець з питань безпеки (інформаційно-комунікаційні технології) 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 організації та забезпечення кібербезпеки інформаційних систем та інформаційно-комунікаційних технологій, спеціальних безпекових програмам (проєктів), стратегічного розвитку організації, персоналу, інфраструктури, вимог до безпеки, а також формують політику та стратегію інформаційної безпеки інституції, планують заходи безпеки інформації та кіберзахисту інформаційних ресурсів установи, підприємства/організації або анклаву.

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

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 професійних кваліфікацій «Фахівець з питань безпеки (інформаційно-комунікаційні технології)» і «Провідний фахівець з питань безпеки (інформаційно-комунікаційні технології)»:

диплом магістра за спеціальністю 172 «Телекомунікації та радіотехніка» галузі знань 17 «Електроніка та телекомунікації» або галузі знань 12 «Інформаційні технології» (7 рівень НРК), а також свідоцтво про присвоєння (підвищення) кваліфікації «Фахівець з питань безпеки (інформаційно-комунікаційні технології)» або інший документ, що

підтверджує професійну кваліфікацію «Фахівець з питань безпеки (інформаційно-комунікаційні технології)»;

або свідоцтво про присвоєння (підвищення) кваліфікації «Провідний фахівець з питань безпеки (інформаційно-комунікаційні технології)» або інший документ, що підтверджує професійну кваліфікацію «Провідний фахівець з питань безпеки (інформаційно-комунікаційні технології)».

Фахівець з питань безпеки (інформаційно-комунікаційні технології) – 7 рівень НРК.

Провідний фахівець з питань безпеки (інформаційно-комунікаційні технології) – 7 рівень НРК.

2. Навчання та професійний розвиток

2.1. Первинна професійна підготовка (назва кваліфікації)

Для кваліфікації «Фахівець з питань безпеки (інформаційно-комунікаційні технології)» і «Провідний фахівець з питань безпеки (інформаційно-комунікаційні технології)» – підготовка на першому та другому рівні вищої освіти (бакалаврському та магістерському, відповідно) за спеціальністю 172 «Телекомунікації та радіотехніка» галузі знань 17 «Електроніка та телекомунікації» або галузі знань 12 «Інформаційні технології», стаж роботи за однією з професій відповідного спрямування повинен становити не менше двох років (адміністратор мереж і систем, розробник систем захисту інформації, аналітик з безпеки інформаційно-телекомунікаційних систем, фахівець з питань безпеки (інформаційно-комунікаційні технології), фахівець сфери захисту інформації тощо).

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

Підвищення професійної кваліфікації «Провідний фахівець з питань безпеки (інформаційно-комунікаційні технології)» за наявності професійної кваліфікації «Фахівець з питань безпеки (інформаційно-комунікаційні технології)». Стаж роботи за посадою «Фахівець з питань безпеки (інформаційно-комунікаційні технології)» не менше двох років.

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 професійний розвиток працівників».

Закон України «Про вищу освіту».

Закон України «Про освіту».

Закон України «Про внесення змін до деяких законодавчих актів України щодо функціонування національної системи кваліфікацій».

Постанова Кабінету Міністрів України від 03.08.2005 р. № 688 «Про затвердження Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління».

Постанова Кабінету Міністрів України від 29.03.2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах».

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 21.08.2019 р. № 800 «Про Порядок підвищення кваліфікації педагогічних і науково-педагогічних працівників».

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 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 08.02.2021 р. № 94 «Про реалізацію експериментального проекту щодо функціонування Національного центру резервування державних інформаційних ресурсів».

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

Наказ Державного комітету України по нагляду за охороною праці від 21.12.1993 р. № 132 «Про затвердження Порядку опрацювання і затвердження роботодавцем нормативних актів з охорони праці, що діють на підприємстві».

Наказ Комітету по нагляду за охороною праці Міністерства праці та соціальної політики України від 09.01.1998 р. № 4 «Про затвердження Правил безпечної експлуатації електроустановок споживачів», зареєстрований в Міністерстві юстиції України 10.02.1998 р. за № 93/2533.

Наказ Комітету по нагляду за охороною праці Міністерства праці та соціальної політики України від 29.01.1998 р. № 9 «Про затвердження Положення про розробку інструкцій з охорони праці», зареєстроване у Міністерстві юстиції України 07.04.1998 р. за № 226/2666.

Наказ Міністерства праці та соціальної політики України та Міністерства освіти і науки України від 26.03.2001 р. № 127/151 «Про затвердження Положення про професійне навчання працівників на виробництві».

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 10.04.2007 р. за № 320/13587.

Наказ Адміністрації Держспецзв'язку від 10.06.2008 р. № 94 «Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», зареєстрований в Міністерстві юстиції України 07.07.2008 р. за № 603/15294.

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» зареєстрований в Міністерстві юстиції України 28.01.2015 р. за № 90/26535.

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 05.02.2016 р. за № 196/28326.

Наказ Адміністрації Держспецзв'язку від 15.01.2021 р. № 23 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури».

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

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

Нормативні документи в галузі технічного захисту інформації (далі – НД ТЗІ) та державні стандарти України (далі – ДСТУ) стосовно створення і функціонування КСЗІ, СУІБ, галузеві стандарти відповідного спрямування.

ДСТУ ISO/IEC 27000:2019 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів (ISO/IEC 27000:2018, IDT).

ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).

ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT).

ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT).

ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2009, IDT).

ДСТУ ISO/IEC 15408-2:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги (ISO/IEC 15408-2:2008, IDT).

ДСТУ ISO/IEC 15408-3:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантії безпеки (ISO/IEC 15408-3:2008, IDT).

Документи (стандарти, настанови) Національного інституту стандартів і технологій США (далі – NIST USA).

Інші нормативно-правові, нормативно-технічні та нормативні акти, які регламентують питання адміністрування мереж і систем.

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	Організація та практична реалізація заходів з питань безпеки інформаційно-комунікаційних технологій (далі – ІКТ)	Здатність визначати та/або впроваджувати політики і процедури для забезпечення належного захисту критичної інфраструктури та ІКТ	**А1**
		Здатність керувати аналізом загроз або цільовим аналізом інформації про кіберзахист, а також отриманням даних про загрози в межах підприємства/ організації	**А2**

		Здатність визначати специфічні вимоги безпеки до системи ІКТ на всіх етапах її життєвого циклу	**А3**
		Здатність забезпечувати успішне впровадження та функціональність вимог безпеки та відповідних політик і процедур ІКТ, які узгоджені з цілями та місією підприємства/організації	**А4**
		Здатність визначати наслідки застосування нових технологій або оновлень у програмах захисту ІКТ	**А5**
		Здатність визначати проблеми безпеки у процесі стабільної роботи та управління програмним забезпеченням та вживати заходів безпеки, коли життєвий цикл продукту закінчується	**А6**
Б	Забезпечення фінансово-матеріальної, інституціональної, методологічної та іншої підтримки безпеки ІКТ	Здатність забезпечувати фінансово-матеріальну підтримку безпеки ІКТ на підприємстві/в організації	**Б1**
		Здатність забезпечувати методологічну підтримку безпеки ІКТ на підприємстві/в організації	**Б2**
		Здатність забезпечувати інституціональну та іншу підтримку безпеки ІКТ на підприємстві/в організації	**Б3**
В	Моніторинг та оцінювання діяльності з питань безпеки ІКТ	Здатність брати участь в оцінюванні ризику інформаційній безпеці під час проведення процедури оцінки і авторизації	**В1**
		Здатність керувати моніторингом джерел даних, що стосуються забезпечення захисту інформації, з метою забезпечення обізнаності підприємства/організації про ситуацію	**В2**
		Здатність моніторити та оцінювати ефективність засобів кібербезпеки підприємства/організації з метою гарантованого підтвердження того, що вони забезпечують необхідний рівень захисту	**В3**
Г	Контроль/нагляд за діяльністю з питань безпеки ІКТ	Здатність відслідковувати результати аудиту та розробляти рекомендації, щоб забезпечити вжиття відповідних заходів щодо зменшення негативних наслідків	**Г1**
		Здатність наглядати за захисними чи коректувальними заходами при виявленні кіберінциденту або вразливості	**Г2**

Д	Координація та участь в управлінні діяльністю із забезпечення безпеки ІКТ	Здатність здійснювати керівництво профільними працівниками з безпеки ІКТ	**Д1**
		Здатність взаємодіяти з керівництвом, технологічними та іншими підрозділами підприємства/організації стосовно технологічних питань відповідного спрямування	**Д2**
		Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень	**Д3**

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. Організація та практична реалізація заходів з питань безпеки ІКТ	Протоколи, стандарти та сертифікати відповідного спрямування; комп'ютерне, програмне та техніко-технологічне забезпечення; операційні системи	**А1.** Здатність визначати та/або впроваджувати політики і процедури для забезпечення належного захисту критичної інфраструктури та ІКТ	**А1.З1.** Концепції і протоколи комп'ютерних мереж, а також методології забезпечення мережевої безпеки **А1.З2.** Процеси управління ризиками (методи оцінки та зниження ризиків) **А1.З3.** Закони, нормативні акти, політики і етичні норми та як вони пов'язані з кібербезпекою і конфіденційністю **А1.З4.** Принципи кібербезпеки та конфіденційності **А1.З5.** Класифікація кіберзагроз і вразливостей **А1.З6.** Конкретні операційні наслідки в результаті помилок кібербезпеки **А1.З7.** Корпоративні цілі та завдання, пов'язані з використанням ІКТ на підприємстві/в організації **А1.З8.** Законодавчі акти, постанови і розпорядження органів виконавчої влади та/або кодекси і процедури	**А1.У1.** Збирати та підтримувати дані, необхідні для забезпечення звітності про стан системи кібербезпеки **А1.У2.** Переглядати стандарти політики та стратегії її впровадження, щоб забезпечити відповідність процедур і настанов політикам кібербезпеки **А1.У3.** Рекомендувати політику та координувати її перегляд і затвердження

			адміністративного/кримінального права **А1.39.** Політики, вимоги та процедури безпеки ланцюжка постачання ІКТ та управління ризиками ланцюжка постачання **А1.310.** Системи критичної інфраструктури з ІКТ, які були розроблені без розгляду безпеки системи	
		А2. Здатність керувати аналізом загроз або цільовим аналізом інформації про кіберзахист, а також отриманням даних про загрози в межах підприємства/ організації	**А2.31.** Принципи кібербезпеки та конфіденційності, застосовувані під час управління ризиками, пов'язаними з використанням, обробкою, зберіганням і переданням інформації або даних **А2.32.** Джерела поширення інформації про вразливість (попередження, рекомендації, списки помилок і бюлетені) **А2.33.** Методологія реагування на інциденти та обробки даних інцидентів **А2.34.** Принципи та методи аналізу, прийняті в галузевих стандартах або в організації **А2.35.** Методи аналізу мережевого трафіку **А2.36.** Теорія управління потоками в мережах (протоколу управління передачею (TCP), протоколу міжмережевого обміну даними (IP), моделі взаємодії відкритих систем	**А2.У1.** Керувати захисними чи коректувальними заходами при виявленні кіберінциденту або вразливості **А2.У2.** Розпізнавати можливе порушення безпеки та вживати відповідних заходів, щоб повідомити про інцидент, якщо необхідно **А2.У3.** Інтерпретувати випадки невідповідності для визначення їхнього впливу на рівень ризику та/або загальну ефективність програми кібербезпеки підприємства **А2.У4.** Визначати, як буде функціонувати система безпеки (включаючи її властивості відмовостійкості і надійності), та як зміни умов, операцій або середовища вплинуть на ці результати

			(OSI), бібліотеки інфраструктури інформаційних технологій, поточної версії [ITIL]) **А2.37.** Методики адміністрування системи, мережі та захисту операційних систем **А2.38.** Мережеві протоколи, такі як TCP/IP та протоколи відповідних рівнів OSI, динамічного конфігурування вузлів, системи доменних імен (DNS) і послуг, що надаються Службою каталогів	
		А3. Здатність визначати специфічні вимоги безпеки до системи ІКТ на всіх етапах її життєвого циклу	**А3.31.** Алгоритми шифрування **А3.32.** Особливості резервного копіювання та відновлення даних **А3.33.** Механізми контролю доступу до хостів/мереж (списки контролю доступу, списки повноважень) **А3.34.** Теорія, концепції і методи адміністрування серверів і проєктування систем **А3.35.** Операційні системи сервера та клієнта **А3.36.** Підхід підприємства/ організації до прийняття ризиків та/або управління ризиками **А3.37.** Програми, робочі ролі та відповідальність при управлінні інцидентами в організації **А3.38.** Поточні та ймовірні загрози/ вектори загроз **А3.39.** Способи впровадження систем депонування ключів з метою	**А3.У1.** Використовувати офіційні документи та специфічні документи підприємства/організації для управління їхніми системами обчислювального середовища **А3.У2.** Надавати системні вихідні дані для формування вимог кібербезпеки, які повинні бути включені в операційні інструкції та відповідні документи, що стосуються системи постачання **А3.У3.** Використовувати пристрої віртуальних приватних мереж (VPN) і шифрування **А3.У4.** Використовувати шифрування інфраструктури відкритих ключів (PKI) та можливостей цифрового підпису в програмних додатках (ел. пошта S/MIME, SSL-трафік)

			забезпечення локального шифрування даних	
		А4. Здатність забезпечувати успішне впровадження та функціональність вимог безпеки та відповідних політик і процедур ІКТ, які узгоджені з цілями та місією підприємства/ організації	**А4.З1.** Методологія і способи виявлення вторгнень до хостів і мережі **А4.З2.** Архітектурні концепції та загальні принципи ІКТ **А4.З3.** Вимоги в межах Загальних принципів управління ризиками (RMF) **А4.З4.** Загрози та вразливості безпеки систем і прикладного програмного забезпечення (переповнення буфера, мобільний код, міжсайтові сценарії, процедурна мова/мова структурованих запитів [PL/SQL] та ін'єкції, перегони фронтів (race conditions), прихований канал, повтор, атаки на повернення (replay attacks), шкідливий код) **А4.З5.** Класифікація мережевих атак, наявний зв'язок між мережевими атаками і загрозами та вразливостями **А4.З6.** Використовувану на підприємстві/в організації програму класифікації інформації і процедур розкриття	**А4.У1.** Переконатися, що дії з покращення безпеки належним чином оцінюють, затверджують та впроваджують у разі необхідності **А4.У2.** Переконатися, що перевірки, тести та перегляди у сфері кібербезпеки узгоджуються з мережевим середовищем **А4.У3.** Переконатися, що вимоги з кібербезпеки інтегровані у планування безперервного функціонування системи та/або підприємства/організації **А4.У4.** Переконатися, що можливості захисту та виявлення набуті за допомогою інженерного підходу ІС, узгоджуються з архітектурою кібербезпеки на рівні підприємства/організації **А4.У5.** Розробляти політики, які відображають цілі системи безпеки **А4.У6.** Застосовувати методики виявлення вторгнень з боку хоста та мережі за допомогою технологій виявлення вторгнень

		А5. Здатність визначати наслідки застосування нових технологій або оновлень у програмах захисту ІКТ	**А5.31.** Нові/які виникають ІКТ та технології кібербезпеки **А5.32.** Концепції архітектури безпеки мережі, включно з топологією, протоколами, компонентами та принципами (прикладна система ешелонованого захисту) **А5.33.** Принципи, моделі, інструменти та методи управління мережевими системами (наскрізний моніторинг продуктивності систем) **А5.34.** Концепції архітектури безпеки і еталонних моделей архітектури підприємства (Zachman, Federal Enterprise Architecture [FEA])	**А5.У1.** Готувати, розповсюджувати та підтримувати плани, інструкції, настанови та стандартні функціональні процедури стосовно безпеки функціонування мережевих систем (-и) **А5.У2.** Брати участь у процесах розроблення або модифікації планів і вимог програм кібербезпеки комп'ютерного середовища **А5.У3.** Виявляти системи критичної інфраструктури з ІКТ, які були спроєктовані без урахування безпеки системи **А5.У4.** Інтерпретувати та/або затверджувати вимоги до безпеки спроможностей нових інформаційних технологій
		А6. Здатність визначати проблеми безпеки у процесі стабільної роботи та управління програмним забезпеченням та вживати заходів безпеки, коли життєвий цикл продукту закінчується	**А6.31.** Засоби тестування безпеки методом «чорного ящика» в процесі забезпечення якості різних версій програмного забезпечення (далі – ПЗ) **А6.32.** Принципи кібербезпеки та конфіденційності при формуванні організаційних вимог (які стосуються конфіденційності, цілісності, доступності, автентифікації і неспростовності)	**А6.У1.** Проводити процедури тестування і перевірки автентичності ПЗ **А6.У2.** Визначати і документувати програмні коригування або версії програми, які залишають вразливості **А6.У3.** Здійснювати пробні запуски програм і прикладного ПЗ **А6.У4**. Виявляти системи критичної інфраструктури з ІКТ, які були спроєктовані без урахування безпеки системи
Б. Забезпечення фінансово-матеріальної, інституціональної,	Нормативні установчі акти підприємства (організації);	**Б1.** Здатність забезпечувати фінансово-матеріальну	**Б1.31.** Прикладні бізнес процеси та функції в організації-замовника **Б1.32.** Принципи безперервності бізнесу та операційних планів	**Б1.У1.** Повідомляти вартість безпеки ІКТ зацікавленим сторонам організації на всіх рівнях

методологічної та іншої підтримки безпеки ІКТ	структура підприємства (організації); положення про структурні підрозділи підприємства (організації); нормативні акти роботодавця з організації, координації діяльності та взаємодії структурних підрозділів підприємства (організації); порядок і типові вимоги до проведення ділових (комерційних) перемовин; порядок розроблення та виконання договірних робіт для зовнішніх партнерів; фінансова документація, документація з	підтримку безпеки ІКТ на підприємстві/в організації	відновлення безперервності після катастроф **Б1.33.** Методики управління ризиками в ланцюжку постачання (NIST SP 800-161) **Б1.34.** Вимоги до закупівлі критичних інформаційних технологій	**Б1.У2.** Прогнозувати поточні потреби послуг і забезпечувати перегляд припущень щодо безпеки за необхідності **Б1.У3.** Контролювати, щоб усі дії з придбання, постачання, закупівлі та аутсорсингу відповідали вимогам кібербезпеки, які відповідають цілям підприємства/організації **Б1.У4.** Брати участь, за необхідності, у процесі закупівлі, дотримуючись відповідних практик управління ризиків в ланцюжку постачання **Б1.У5.** Оцінювати ефективність функції закупівель з точки зору задоволення вимог інформаційної безпеки і ризиків у ланцюжку постачання через закупівельну діяльність та рекомендувати вдосконалення **Б1.У6.** Керувати та контролювати бюджет інформаційної безпеки та укладання контрактів **Б1.У7.** Оцінювати надійність постачальника та/або продукту **Б1.У8.** Впроваджувати вимоги до захисту інформації у процеси закупівель, використовуючи застосовні базові контролі безпеки у якості одного із джерел вимог безпеки та забезпечуючи надійний процес контролю якості ПЗ, а також встановлюючи різні джерела

	матеріально-технічного забезпечення, відповідне програмне забезпечення			(маршрути доставки для критичних елементів системи)
		Б2. Здатність забезпечувати методологічну підтримку безпеки ІКТ на підприємстві/ в організації	**Б2.З1.** Принципи та способи управління ресурсами **Б2.З2.** Стандарти, політики і авторизовані підходи до проєктування ПЗ, прийняті на підприємстві/в організації (стандарти міжнародної організації зі стандартизації [ISO]) **Б2.З3.** Принципи та методики управління програмами та проєктами із захисту інформації	**Б2.У1.** Організовувати публікацію настанов із захисту комп'ютерної мережі (TCNO, концепції операцій, звіти мережевих аналітиків, NTSM, MTO) для зацікавлених сторін підприємства **Б2.У2.** Розробляти методологію кібербезпеки підприємства та управління ризиком ланцюжка постачання для розробки безперервності операційних планів
		Б3. Здатність забезпечувати інституціональну та іншу підтримку безпеки ІКТ на підприємстві/в організації	**Б3.З1.** Принципи управління життєвим циклом системи, включаючи забезпечення безпеки та експлуатаційної придатності ПЗ **Б3.З2.** Процеси інтеграції технологій	**Б3.У1.** Рекомендувати розподіл ресурсів, необхідних для безпечного функціонування та підтримки вимог організації з кібербезпеки **Б3.У2.** Керувати та узгоджувати пріоритети безпеки інформаційно-комунікаційних технологій зі стратегією безпеки **Б3.У3.** Забезпечувати іншу підтримку безпеці ІКТ на підприємстві/в організації
В. Моніторинг та оцінювання діяльності з питань безпеки ІКТ	Нормативні акти, нормативні документи, проєктна документація, протоколи, стандарти та	**В1.** Здатність брати участь в оцінюванні ризику інформаційній безпеці під час проведення процедури оцінки і авторизації	**В1.З1.** Критерії або показники продуктивності та доступності систем **В1.З2.** Сучасні галузеві методи оцінки, впровадження та розповсюдження інструментів і процедур оцінки безпеки ІКТ, моніторингу, виявлення та усунення несправностей, які	**В1.У1.** Переконатися, що існують плани дій та етапів або плани відновлення для усунення вразливостей, які були виявлені під час оцінки ризиків, аудиторських та інспекторських перевірок

	сертифікати щодо моніторингу та оцінювання заходів з безпеки, зокрема відповідності програмних та апаратних засобів технічного захисту інформації; техніко-технологічне, комп'ютерне, програмне та інше забезпечення моніторингу та оцінювання; операційні та інші системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми, алгоритми шифрування; бази даних; інші інструменти оцінювання безпеки ІКТ		використовують концепції та можливості на основі стандартів	**В1.У2.** Брати участь в оцінці ризику безпеки інформації під час проведення процедури оцінки та авторизації
		В2. Здатність керувати моніторингом джерел даних, що стосуються забезпечення захисту інформації, з метою забезпечення обізнаності підприємства/ організації про ситуацію	**В2.31.** Стандарти безпеки персональних ідентифікаційних даних (PII) **В2.32.** Стандарти безпеки даних у сфері платіжних карт (PCI) **В2.33.** Стандарти безпеки медичних персональних даних (PHI)	**В2.У1.** Оцінювати та затверджувати програми розвитку для забезпечення належного встановлення базових засобів безпеки **В2.У2.** Оцінювати витрати-вигоду, економічний аналіз та аналіз ризиків у процесі ухвалення рішень **В2.У3.** Керувати моніторингом джерел даних, що стосуються забезпечення захисту інформації, з метою забезпечення обізнаності підприємства/організації про ситуацію
		В3. Здатність моніторити та оцінювати ефективність засобів кібербезпеки підприємства/організації з метою гарантованого підтвердження того, що вони забезпечують необхідний рівень захисту	**В3.31.** Принципи, інструменти та методики тестування на проникнення **В3.32.** Порядок проведення моніторингу ефективності засобів кібербезпеки підприємства/організації **В3.33.** Порядок проведення оцінювання ефективності засобів кібербезпеки підприємства/організації **В3.34.** Порядок підтвердження спроможності засобів кібербезпеки забезпечувати необхідний рівень захисту	**В3.У1.** Підтримувати необхідні заходи щодо забезпечення відповідності (переконатися, що виконуються настанови щодо конфігурації системи безпеки, здійснюється моніторинг відповідності) **В3.У2.** Моніторити ефективність засобів кібербезпеки підприємства/ організації **В3.У3.** Оцінювати ефективність засобів кібербезпеки підприємства/ організації **В3.У4.** Підтверджувати спроможність засобів кібербезпеки забезпечувати необхідний рівень захисту

Г. Контроль/ нагляд за діяльністю з питань безпеки ІКТ	Нормативні акти, нормативні документи, проєктна документація, протоколи, стандарти та сертифікати щодо контролю/нагляду за діяльністю з питань безпеки ІКТ; техніко-технологічне, комп'ютерне, програмне та інше забезпечення діяльності з відповідного контролю; операційні та інші системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми, алгоритми шифрування; бази даних	**Г1.** Здатність відслідковувати результати аудиту та розробляти рекомендації, щоб забезпечити вжиття відповідних заходів щодо зменшення негативних наслідків	**Г1.31.** Засоби контролю, пов'язані з використанням, обробкою, зберіганням та переданням даних **Г1.32.** Ризики безпеки прикладних програм (Open Web Application Security Project Top 10 list, CWE (Common Weakness Enumeration), CVE (Common Vulnerabilities and Exposures), а також класифікатори атак MITRE.) **Г1.33.** Порядок розроблення заходів, спрямованих на виконання зауважень та рекомендацій, визначених за результатами аудиту **Г1.34.** Порядок контролю за виконанням заходів, спрямованих на виконання зауважень та рекомендацій, визначених за результатами аудиту	**Г1.У1.** Постійно перевіряти підприємство/організацію на відповідність політикам/ настановам/процедурам/ нормативним актам/законам для забезпечення відповідності **Г1.У2.** Розробляти заходи, спрямовані на виконання зауважень та рекомендацій, визначених за результатами аудиту **Г1.У3.** Відслідковувати виконання заходів, спрямованих на виконання зауважень та рекомендацій, визначених за результатами аудиту
		Г2. Здатність наглядати за захисними чи коректувальними заходами при виявленні кіберінциденту або вразливості	**Г2.31.** Порядок нагляду за захисними чи коригувальними заходами при виявленні кіберінциденту або вразливості **Г2.32.** Методологія виявлення вторгнень і способи виявлення вторгнень до хостів і мережі **Г2.33.** Архітектурні концепції та загальні принципи інформаційно-комунікаційних технологій **Г2.34.** Вимоги в межах Загальних принципів управління ризиками (RMF) **Г2.35.** Загрози та вразливості безпеки систем і прикладного програмного забезпечення (переповнення буфера,	**Г2.У1.** Наглядати за захисними чи коригувальними заходами при виявленні кіберінциденту або вразливості **Г2.У2.** Доповідати невідкладно керівництву про стан та ризики проведення захисних чи коректувальних заходів при виявленні кіберінциденту або вразливості **Г2.У3.** Брати участь у розробленні відповідних заходів та профілактичних робіт відповідного спрямування

			мобільний код, міжсайтові сценарії, процедурна мова/мова структурованих запитів [PL/SQL] та ін'єкції, перегони фронтів (race conditions), прихований канал, повтор, атаки на повернення (replay, return-oriented attacks), шкідливий код) **Г2.36.** Класифікація мережевих атак, наявний зв'язок між мережевими атаками і загрозами та вразливостями **Г3.37.** Використовувану на підприємстві/в організації програму класифікації інформації і процедур розкриття	
Д. Координація та участь в управлінні діяльністю із забезпечення безпеки ІКТ	Нормативні установчі акти підприємства (організації); структура підприємства (організації); положення про структурні підрозділи підприємства (організації); посадові інструкції керівників та фахівців структурних підрозділів підприємства/	**Д1.** Здатність здійснювати керівництво профільними працівниками з безпеки ІКТ	**Д1.31.** Керівництва (настанови, інструкції) інші нормативні акти роботодавця з організації, координації діяльності та взаємодії структурних підрозділів підприємства/організації **Д1.32.** Посадові інструкції фахівців структурних підрозділів підприємства/ організації, до функцій яких входять питання безпеки ІКТ **Д1.33.** Основи управління персоналом **Д1.34.** Порядок розроблення та підписання трудових договорів і контрактів **Д1.35.** Основи трудового законодавства **Д1.36**. Процедуру розроблення програм та проведення тренінгів персоналу з питань безпеки	**Д1.У1.** Забезпечувати керівництво та управління персоналом у сфері ІКТ матеріалами та інструментаріями, необхідними для того, щоб обізнаність в кібербезпеці, базові знання, грамотність та тренінги операційного персоналу відповідали їх функціональним обов'язкам **Д1.У2.** Наглядати за виконанням програм тренінгів з інформаційної безпеки та обізнаності **Д1.У3.** Консультувати вище керівництво щодо рівня ризику та стану безпеки **Д1.У4.** Консультувати керівників вищої ланки щодо аналізу витрат/вигоди програм, політик, процесів, систем та елементів інформаційної безпеки

	організації, до функцій яких входять питання забезпечення безпеки ІКТ, та інші нормативні акти роботодавця з організації, координації діяльності та взаємодії структурних підрозділів підприємства (організації); порядок і типові вимоги до проведення ділових (комерційних) перемовин; порядок розроблення та виконання договірних робіт для зовнішніх партнерів		інформаційно-телекомунікаційних технологій	**Д1.У5.** Консультувати профільних керівників вищої ланки або уповноважених представників щодо змін, які впливають на стан кібербезпеки на підприємстві/в організації **Д1.У6.** Керувати, контролювати персонал та укладати з ними контракти **Д1.У7.** Визначати ролі та обов'язки для призначеного персоналу безпеки комунікацій
		Д2. Здатність взаємодіяти з керівництвом, технологічними та іншими підрозділами підприємства/ організації стосовно технологічних питань відповідного спрямування	**Д2.31.** Структура підприємства/ організації, функції структурних підрозділів, розподіл функцій між керівниками підприємства/організації, підпорядкованість підрозділів **Д2.32.** Положення про структурні підрозділи підприємства/організації, що задіяні в спільному виконанні технологічних та інших функціональних завдань **Д2.33.** Нормативні документи підприємства/організації з питань організації його діяльності **Д2.34.** Підходи щодо розбудови загальної архітектури захисту інформації підприємства/організації (EISA) з урахуванням вимог загальної стратегії безпеки організації **Д2.35.** Регламент управління ризиками як засобу забезпечення зменшення ризиків безпеки, і введення даних щодо інших технічних ризиків	**Д2.У1.** Брати участь у корпоративному процесі управління ризиками, щоб забезпечити зменшення ризиків безпеки, вводити данні щодо інших технічних ризиків **Д2.У2.** Надавати технічну документацію, звіти про інциденти, результати комп'ютерних перевірок, висновки та іншу інформацію про ситуацію для головних організацій **Д2.У3.** Створювати загальну архітектуру захисту інформації підприємства/організації (EISA) з урахуванням вимог загальної стратегії безпеки організації **Д2.У4.** Визначати альтернативні стратегії захисту інформації для дотримання цілей організаційної безпеки **Д2.У5.** Знаходити та управляти необхідними ресурсами, включно з підтримкою керівництва, фінансовими

			Д2.36. Основи менеджменту **Д2.37.** Основи маркетингу	ресурсами та ключовим персоналом з питань безпеки, для сприяння досягненню цілей та завдань безпеки інформаційно-комунікаційних технологій і зниження загального ризику організації **Д2.У6.** Знаходити необхідні ресурси, включно з фінансовими, для забезпечення безперервності функціонування операційних програм підприємства/організації **Д2.У7.** Сприяти підвищенню обізнаності керівництва щодо ситуацій безпеки та забезпечувати належні принципи безпеки в баченні та цілях організації
		Д3. Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень	**Д3.31.** Основи комунікаційного менеджменту **Д3.32.** Основи ділової етики **Д3.33.** Порядок і типові вимоги до проведення ділових/комерційних перемовин **Д3.34.** Порядок розроблення та виконання договірних робіт для зовнішніх партнерів	**Д3.У1.** Взаємодіяти із зовнішніми організаціями (службою зі зв'язків із громадськістю, правоохоронними органами) для забезпечення належного та точного розповсюдження фактів про інциденти та інших відомостей про захист комп'ютерної мережі **Д3.У2.** Співпрацювати із зацікавленими сторонами з метою забезпечення безперервної діяльності організації у межах програми, стратегії та виконання завдань **Д3.У3.** Супроводжувати договірні роботи із зовнішніми партнерами

7. Дані щодо розроблення та затвердження професійного стандарту

7.1. Розробники проєкту професійного стандарту

Державна служба спеціального зв'язку та захисту інформації України.

Склад робочої групи:

Лисенко Юлія Костянтинівна, керівник робочої групи, начальник 6 управління Департаменту державного контролю Адміністрації Держспецзв'язку;

Бурбела Ольга Олександрівна, член Громадської організації "Асоціація спеціалістів кібербезпеки";

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

Єсін Віталій Іванович, професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В. Каразіна;

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

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

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

Ліпінський Вадим Володимирович, головний науковий співробітник Науково-дослідної установи «Інститут кібербезпеки»;

Маковець Сергій Валентинович, директор з технологій ТОВ «ІНФОРМЕЙШН СІСТЕМС СЕК'ЮРІТІ ПАРТНЕРС»;

Масленникова Тетяна Андріївна, начальник сектору сертифікації відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

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

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

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

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

Попель Валерій Анатолійович, начальник відділу науково-технічної експертизи Державного науково - дослідного інституту технологій кібербезпеки та захисту інформації;

Самохвалов Юрій Якович, методист тренінгового центру ТОВ «ІССП Тренінг Центр»;

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

Супрун Ольга Миколаївна, професор кафедри кібербезпеки Науково-навчального інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України;

Толюпа Сергій Васильович професор кафедри кібербезпеки та захисту інформації Київського національного університету ім. Тараса Шевченка;

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

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

Юдін Олексій Юрійович, перший заступник начальника 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

26 листопада 2022 року.

7.4. Рекомендована дата наступного перегляду професійного стандарту

26 листопада 2027 року.

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