Проєкт

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

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, включаючи управління наслідками інформаційної безпеки в рамках організації, спеціальними програмами (проектами) або іншими сферами відповідальності, включаючи стратегічний розвиток організації, персонал, інфраструктуру, вимоги до безпеки, політику та стратегію інформаційної безпеки інституції, планування заходів інформаційної безпеки та кібербезпеки на випадок надзвичайних ситуацій або інцидентів, обізнаність про безпеку анклаву та інші інформаційні ресурси організації, установи або підприємства різних форм власності.

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 61	Телекомунікації (електрозв'язок)	Група 61.1	Діяльність у сфері проводового електрозв'язку
				Клас 61.10	Діяльність у сфері проводового електрозв'язку
				Група 61.2	Діяльність у сфері безпроводового електрозв'язку
				Клас 61.20	Діяльність у сфері безпроводового електрозв'язку
				Група 61.3	Діяльність у сфері супутникового електрозв'язку

				Клас 61.30	Діяльність у сфері супутникового електрозв'язку
				Група 61.9	Інша діяльність у сфері електрозв'язку
				Клас 61.90	Інша діяльність у сфері електрозв'язку
				Група 61.2	Діяльність у сфері безпроводового 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 устаткованням
				Клас 62.09	Інша діяльність у сфері інформаційних технологій і комп'ютерних систем
Секція М	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	Підрозділ	Клас	Підклас	Група
2	21	213	2139	2139.2
Професіонали	Професіонали в галузі фізичних, математичних та технічних наук	Професіонали в галузі обчислень (комп’ютеризації)	Професіонали в інших галузях обчислень (комп’ютеризації)	Професіонали в інших галузях обчислень

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)

Профільний структурний підрозділ в рамках організації, спеціальної програми або іншої сфери відповідальності (анклаву), навчально-наукові та науково-дослідні установи (центри, тощо) у сфері інформаційної безпеки та кібербезпеки.

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 професійних кваліфікацій "Фахівець з питань безпеки (інформаційно-комунікаційні технології)" і "Провідний фахівець з питань безпеки (інформаційно-комунікаційні технології)" диплом магістра за спеціальністю:

- 121 «Інженерія програмного забезпечення» галузі знань «Інформаційні технології» (7 рівень НРК);
- 122 «Комп’ютерні науки» галузі знань «Інформаційні технології» (7 рівень НРК);
- 123 «Комп’ютерна інженерія» галузі знань «Інформаційні технології» (7 рівень НРК);

- 124 «Системний аналіз» галузі знань «Інформаційні технології» (7 рівень НРК);
- 125 «Кібербезпека» галузі знань «Інформаційні технології» (7 рівень НРК);
- 126 «Інформаційні системи та технології» галузі знань «Інформаційні технології» (7 рівень НРК);
- 172 «Телекомунікації та радіотехніка» галузі знань «Електроніка та телекомунікації» (7 рівень НРК).

Додатково:

- документ (диплом, сертифікат, тощо), щодо післядипломної освіти та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері інформаційних технологій, інформаційної безпеки та кібербезпеки;
- документ (диплом, сертифікат, тощо), щодо професійної сертифікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері інформаційних технологій, інформаційної безпеки та кібербезпеки.

2. Навчання та професійний розвиток

2.1. Первинна професійна підготовка (назва кваліфікації)

Для фахівця з питань безпеки (інформаційно-комунікаційні технології) і провідного фахівця з питань безпеки (інформаційно-комунікаційні технології) – підготовка на першому та другому рівні вищої освіти (бакалаврському та магістерському, відповідно) за спеціальностями вказаними п.1, п.п.1.11 галузі знань 12 «Інформаційні технології» та 17 «Електроніка та телекомунікації», стаж роботи за однією з професій відповідного спрямування повинен складати не менше 2 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)

Для професійної кваліфікації "Фахівець з питань безпеки (інформаційно-комунікаційні технології)". Підвищення кваліфікації для отримання професійної кваліфікації "Провідний 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

Закон України «Про освіту».

Закон України «Про вищу освіту».

Кодекс законів про працю України.

Закон України «Про професійний розвиток працівників».

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

Закон України «Про інформацію».

Закон України «Про державну таємницю».

Закон України «Про захист персональних даних».

Закон України «Про захист прав споживачів».

Закон України «Про доступ до публічної інформації».

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

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 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 03.08.2005 № 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 08.02.2021 № 94 "Про реалізацію експериментального проекту щодо функціонування Національного центру резервування державних інформаційних ресурсів".

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

Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29 березня 2006 р. № 373.

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 10.06.2008 № 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".

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

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".

Порядок підвищення кваліфікації педагогічних і науково-педагогічних працівників, затверджений постановою Кабінету Міністрів України від 21 серпня 2019 р. № 800.

Порядок акредитації кваліфікаційних центрів, затверджений постановою Кабінету Міністрів України від 22 вересня 2021 р. № 986.

Порядок присвоєння та підтвердження професійних кваліфікацій кваліфікаційними центрами, затверджений постановою Кабінету Міністрів України від 15 вересня 2021 р. № 956.

Типове положення про кваліфікаційний центр, затверджене Наказом Міністерства освіти і науки України від 22.04.2021 р. № 452.

Положення про Реєстр кваліфікацій, затверджений постановою Кабінету Міністрів України від 16 червня 2021 р. № 620.

Порядок визнання в Україні професійних кваліфікацій, здобутих в інших країнах, затверджений постановою Кабінету Міністрів України від 2 червня 2021 р. № 576.

Положення про професійне навчання працівників на виробництві, затверджені наказом Міністерства праці та соціальної політики України та Міністерства освіти і науки України від 26.03.2001 за № 127/151.

Порядок опрацювання і затвердження роботодавцем нормативних актів з охорони праці, що діють на підприємстві, затверджений наказом

державного комітету України по нагляду за охороною праці від 21.12.1993 за № 132.

Правила безпечної експлуатації електроустановок споживачів, затверджених наказом Комітету по нагляду за охороною праці Міністерства праці та соціальної політики України від 09.01.1998 за № 4, зареєстрований в Міністерстві юстиції України 10.02.1998 за № 93/2533.

Положення про розробку інструкцій з охорони праці, затверджений наказом Комітету по нагляду за охороною праці Міністерства праці та соціальної політики України від 29.01.1998 за № 9, зареєстрований у Міністерстві юстиції України 07.04.1998 за № 226/2666.

Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ, 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 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 (NIST USA).

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

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 адміністрування систем і мереж
ЗК.02	Здатність діяти соціально відповідально та громадянські

	свідомо
ЗК.03	Здатність застосовувати знання у практичних ситуаціях, розв'язувати спеціалізовані завдання/задачі та практичні проблеми у професійній діяльності
ЗК.04	Здатність дотримуватися правил та норм з безпеки та охорони праці, зокрема щодо безпечної експлуатації електроустановок споживачів
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 англійською на рівні, що забезпечує ефективну професійну діяльність
ЗК.09	Здатність чітко та стисло відповідати на питання, ставити уточнюючі питання
ЗК.10	Здатність застосовувати навички критичного читання/мислення
ЗК.11	Здатність оцінювати інформацію на предмет її надійності, достовірності і актуальності, оцінювати та забезпечувати якість виконуваних робіт
ЗК.12	Здатність відображати дані в оригінальних форматах, готувати і публікувати звіти з урахуванням ІТ технологій.
ЗК.13	Здатність впевнено і систематизовано доводити складну інформацію, концепції або ідеї в усній і письмовій формах і/або за допомогою наочних засобів

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

		загрози в рамках підприємства/організації	
		Здатність визначати специфічні вимоги безпеки до системи інформаційних технологій (ІКТ) на всіх етапах її життєвого циклу	А3
		Здатність забезпечувати успішне впровадження та функціональність вимог безпеки та відповідних політик і процедур інформаційних технологій (ІКТ), які узгоджені з цілями та місією підприємства/організації	А4
		Здатність визначати наслідки застосування нових технологій або оновлень у програмах захисту інформаційних технологій (ІКТ)	А5
Б	Забезпечення фінансово-матеріальної, інституціональної, методологічної та іншої підтримки безпеки інформаційно-комунікаційних технологій (ІКТ)	Здатність забезпечувати фінансово-матеріальну підтримку безпеці інформаційно-комунікаційних технологій (ІКТ) на підприємстві/в організації	Б1
		Здатність забезпечувати методологічну підтримку безпеці інформаційно-комунікаційних технологій (ІКТ) на підприємстві/в організації	Б2
		Здатність забезпечувати інституціональну та іншу підтримку безпеці інформаційно-комунікаційних технологій (ІКТ) на	Б3

		підприємстві/в організації	
В	Моніторинг та оцінювання діяльності з питань безпеки інформаційно-комунікаційних технологій (ІКТ)	Здатність брати участь в оцінці ризику інформаційної безпеки під час проведення процедури оцінки і авторизації	В1
		Здатність керувати моніторингом джерел даних, що стосуються забезпечення інформаційної безпеки, 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 інформаційно-комунікаційних технологій (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 інформаційно-телекомунікаційних технологій (ІКТ)	Здатність здійснювати керівництво профільними працівниками з безпеки інформаційно-телекомунікаційних технологій (ІКТ)	Д1
		Здатність взаємодіяти з	Д2

		керівництвом, технологічними та іншими підрозділами підприємства/ організації стосовно технологічних питань відповідного спрямування	
		Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень	ДЗ

6. Опис трудових функцій

Трудові функції	**Предмети і засоби праці (обладнан-ня, устаткуван-ня, матеріали, продукти, інструмен-ти)**	**Професійні компетентності**	**Знання**	**Уміння і навички**
А Організація та практична реалізація заходів з питань безпеки інформаційно-комунікаційних технологій (ІКТ)	Протоколи, стандарти, та сертифікати відповідного спрямування; компьютерне, програмне та інше техніко-технологічне забезпечен-ня; операційні та інші системи	**А1**. Здатність визначати та/або впроваджувати політики і процедури для забезпечення належного захисту критичної інфраструктури	**А1.З1.** Концепції і протоколи комп'ютерних мереж, а також методології забезпечення мережевої безпеки **А1.З2.** Процеси управління ризиками (наприклад, методів оцінки та зниження ризиків) **А1.З3.** Закони, нормативні акти, політики і етичні норми, та як вони пов'язані з кібербезпекою і приватністю **А1.З4.** Принципи кібербезпеки і приватності **А1.З5.** Класифікацію кіберзагроз та вразливостей **А1.З6.** Конкретні операційні наслідки в результаті помилок кібербезпеки	**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 та настанов політикам кібербезпеки **А1.У3**. Рекомендувати політику та координувати її перегляд та затвердження

			А1.37. Корпоративні цілі і завдання, пов'язані з використанням ІКТ на підприємстві/в організації **А1.38.** Чинні законодавчі акти, постанови і розпорядження органів виконавчої влади та/або кодексів і процедур адміністративного/кримінального права **А1.39**. Політики, вимоги і процедури безпеки ланцюжки постачання інформаційних технологій (ІКТ) та управління ризиками ланцюжка постачання **А1.310**. Системи критичної інфраструктури з інформаційно-комунікаційними технологіями, 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	**А2.31.** Принципи кібербезпеки і приватності, застосовувані під час управління ризиками, пов'язаних із використанням, обробкою, зберіганням і передачею інформації або даних	**А2.У1.** Керувати захисними чи коректувальними заходами при виявленні кіберінциденту або вразливості **А2.У2.** Розпізнавати можливе порушення безпеки і вживати відповідні заходи, щоб повідомити

		рамках підприємства/органі-зації	**А2.З2.** Джерела поширення інформації про вразливість (наприклад, попередження, рекомендації, списки помилок і бюлетені) **А2.З3.** Методологію реагування на інциденти і обробки даних інцидентів **А2.З4.** Принципи і методи аналізу, прийняті в галузевих стандартах або в організації **А2.З5.** Методи аналізу мережевого трафіку **А2.З6.** Теорію управління потоками в мережах (наприклад, протоколу управління передачею (TCP), протоколу міжмережевого обміну даними (IP), моделі взаємодії відкритих систем (OSI), бібліотеки інфраструктури інформаційних технологій, поточної версії [ITIL]) **А2.З7.**Методики адміністрування системи, мережі та захисту операційних систем **А2.З8**. Мережеві протоколи, такі як TCP/IP, динамічного	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

			конфігурування вузлів, системи доменних імен (DNS) і послуг, що надаються Службою каталогів	
		А3.Здатність визначати специфічні вимоги безпеки до системи інформаційних технологій (ІКТ) на всіх етапах її життєвого циклу	**А3.З1.**Алгоритми шифрування **А3.З2.** Особливості резервного копіювання та відновлення даних **А3.З3.** Механізми контролю доступу до хостів /мереж (наприклад, списки контролю доступу, списки повноважень) **А3.З4.** Теорію, концепції і методи адміністрування серверів і проєктування систем **А3.З5.** Операційні системи сервера і клієнта **А3.З6.** Підхід підприємства/ організації до прийняття ризиків та/або управління ризиками **А3.З7**. Програми, робочі ролі і відповідальність при управлінні інцидентами в організації **А3.З8**. Поточні і виникаючі загрози/вектори загроз	**А3.У1**. Використовувати офіційні документи та специфічні документи підприємства/організації для управління їх системами обчислювального середовища **А3.У2.** Надавати системні вихідні дані для формування вимог кібербезпеки, які повинні бути включені в операційні інструкції та інші відповідні документи, що стосуються системи постачання **А3.У3.** ~~Здатність~~ Застосовувати методики виявлення вторгнень з боку хоста та мережі за допомогою технологій виявлення вторгнень
		А4.Здатність забезпечувати успішне	**А4.З1.**Методологію виявлення вторгнень і способи виявлення вторгнень до хостів і мережі	**А4.У1.** Переконатися, що дії з покращення безпеки належним чином оцінюються, затверджуються

		впровадження та функціональність вимог безпеки та відповідних політик і процедур інформаційних технологій (ІКТ), які узгоджені з цілями та місією підприємства/орга-нізації	**А4.32.** Архітектурні концепції та загальні принципи інформаційних технологій (ІКТ) **А4.33.** Вимоги в рамках Загальних принципів управління ризиками (RMF) **А4.34.** Загрози і вразливості безпеки систем і прикладного програмного забезпечення (наприклад, переповнення буфера, мобільний код, міжсайтові сценарії, процедурна мова/мова структурованих запитів [PL/SQL] та ін'єкції, перегони фронтів, прихований канал, повтор, атаки на повернення, шкідливий код) **А4.35**. Класифікацію мережевих атак, та який існує зв'язок між мережевими атаками і загрозами та вразливостями **А4.36**. Використовувану на підприємстві/ в організації програму класифікації інформації і процедур розкриття	та впроваджуються в 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 в планування безперервного функціонування системи та/або підприємства/організації **А4.У4.** Переконатися, що можливості захисту та виявлення набуті за допомогою інженерного підходу ІС та узгоджуються з архітектурою кібербезпеки на рівні підприємства/організації
		А5. Здатність визначати наслідки	**А5.31.** Нові та виникаючі інформаційні технології (ІКТ) та	**А5.У1**. Готувати, розповсюджувати та підтримувати плани, інструкції,

		застосування нових технологій або оновлень у програмах захисту інформаційних технологій (ІКТ)	технології кібербезпеки **А5.32.** Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи (наприклад, прикладна система ешелонованого захисту) **А5.33**. Принципи, моделі, інструменти та методи управління мережевими системами (наприклад, наскрізний моніторинг продуктивності систем) **А5.34.** Концепції архітектури безпеки і еталонних моделей архітектури підприємства (наприклад, Zachman, Federal Enterprise Architecture [FEA])	настанови та стандартні функціональні процедури стосовно безпеки функціонування мережевих систем(-и) в процесах розробки або модифікації планів і вимог програм кібербезпеки комп'ютерного середовища **А5.У2**. Виявляти системи критичної інфраструктури з інформаційно-телекомунікаційними технологіями, які були спроєктовані без врахування безпеки системи **А5.У3**. Інтерпретувати та/або затверджувати вимоги щодо безпеки спроможностей нових інформаційних технологій (Т0132)
Б Забезпечення фінансово-матеріальної, інституціональної, методологічної та іншої підтримки безпеки	Нормативні установчі акти підприємства (організації); структура підприємства (організації); положення про структурні	**Б1.** Здатність забезпечувати фінансово-матеріальну підтримку безпеці інформаційно-комунікаційних технологій (ІКТ) на підприємстві/в	**Б1.31.** Прикладні бізнес процеси і функції в організації – замовнику **Б1.32.** Принципи безперервності бізнесу та операційних планів відновлення безперервності після катастроф **Б1.33.** Методики управління ризиками в ланцюжку	**Б1.У1.** Повідомляти вартість безпеки інформаційних технологій (ІКТ) зацікавленим сторонам організації на всіх рівнях **Б1.У2**. Прогнозувати поточні потреби у послугах та забезпечувати, що припущення щодо безпеки переглядаються за необхідності **Б1.У3.** Переконатися,

інформаційно-комунікаційних технологій (ІКТ)	підрозділи підприємства (організації); 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; фінансова	організації	постачання (NIST SP 800-161) **Б1.34.** Вимоги до закупівлі критичних інформаційних технологій	що усі дії з придбання, постачання, закупівлі та аутсорсингу відповідають вимогам кібербезпеки, які відповідають цілям підприємства/організації **Б1.У4.** Брати участь, за необхідності, в 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 інформаційної безпеки у процеси закупівель, використовуючи застосовні базові контролі безпеки у якості одного із джерел вимог

	документація, документація з матеріально-технічного забезпечення, відповідне програмне забезпечення			безпеки та забезпечуючи надійний процес контролю якості програмного забезпечення, та встановлюючи різні джерела (наприклад, маршрути доставки для критичних елементів системи)
		Б2. Здатність забезпечувати методологічну підтримку безпеці інформаційно-комунікаційних технологій (ІКТ) на підприємстві/в організації	**Б2.З1**. Принципи і способи управління ресурсами **Б2.З2.** Стандарти, політики і авторизовані підходи до проєктування системного програмного забезпечення, прийняті на підприємстві/в організації (наприклад, стандарти міжнародної організації зі стандартизації [ISO]) **Б2.З3**. Принципи і методики управління програмами та проектами з інформаційної безпеки	**Б2.У1.** Організовувати опублікування настанов із захисту комп'ютерної мережі (наприклад, 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 безпеці інформаційно-комунікаційних	**Б3.З1**. Принципи управління життєвим циклом системи, включаючи забезпечення безпеки та експлуатаційної придатності програмного забезпечення **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 інформаційних технологій (ІКТ) зі стратегією

		технологій (ІКТ) на підприємстві/в організації		безпеки **Б3.У3.** Забезпечувати іншу підтримку безпеці інформаційно-комунікаційних технологій (ІКТ) на підприємстві/в організації
В Моніторинг та оцінювання діяльності з питань безпеки інформаційно-комунікаційних технологій (ІКТ)	Нормативні акти, нормативні документи, проєктна документація, протоколи, стандарти та сертифікати щодо моніторингу та оцінювання заходів з безпеки, зокрема відповідності програмних та апаратних засобів технічного захисту інформації; техніко-технологічне,	**В1.** Здатність брати участь в оцінці ризику інформаційної безпеки під час проведення процедури оцінки і авторизації	**В1.З1.** Критерії або показники продуктивності і доступності систем **В1.З2.** Сучасні галузеві методи оцінки, впровадження та розповсюдження інструментів та процедур оцінки безпеки інформаційних технологій (ІКТ), моніторингу, виявлення та усунення несправностей, які використовують концепції та можливості на основі стандартів	**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 тощо **В1.У2.** Брати участь в оцінці ризику інформаційної безпеки під час проведення процедури оцінки і авторизації
		В2. Здатність керувати моніторингом джерел даних, що стосуються забезпечення інформаційної безпеки, з метою забезпечення обізнаності	**В2.З1.** Стандарти безпеки персональних ідентифікаційних даних (PII) **В2.З2**. Стандарти безпеки даних в сфері платіжних карт (PCI) **В2.З3.** 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 прийняття рішень **В2.У3**. Керувати моніторингом джерел даних, що стосуються забезпечення інформаційної

	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 інформацій-но-комунікацій-них технологій (ІКТ)	підприємства/органі-зації про ситуацію		безпеки, з метою забезпечення обізнаності підприємства/організації про ситуацію
		В3. Здатність моніторити та оцінювати ефективність засобів кібербезпеки підприємства/органі-зації з метою гарантованого підтвердження того, що вони забезпечують необхідний рівень захисту	**В3.З1.** Принципи, інструменти та методики тестування на проникнення **В3.З2.** Порядок проведення моніторингу ефективності засобів кібербезпеки підприємства/організації **В3.З3.** Порядок проведення оцінювання ефективності засобів кібербезпеки підприємства/організації **В3.З2.** Порядок підтвердження спроможності засобів кібербезпеки забезпечувати необхідний рівень захисту	**В3.У1**. Підтримувати необхідні заходи щодо забезпечення відповідності (наприклад, 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	Нормативні акти, нормативні документи, проєктна	**Г1**. Здатність відслідковувати результати аудиту та розробляти	**Г1.З1**. Засоби контролю, пов'язані з використанням, обробкою, зберіганням та передачею даних	**Г1.У1.** Постійно перевіряти підприємство/організацію на відповідність політикам/настановам /процедурам/нормативним

інформаційно-комунікаційних технологій (ІКТ)	документація, протоколи, стандарти та сертифікати щодо контролю/ нагляду за діяльністю з питань безпеки інформацій-но-комунікацій-них технологій (ІКТ); техніко-технологічне, комп'ютерне, програмне та інше забезпечення діяльності з відпровідного контролю; операційні та інші системи; інтерпретовані і компільовані комп'ютерні мови;	рекомендації, щоб забезпечити вжиття відповідних заходів щодо зменшення негативних наслідків	**Г1.32.** Ризики безпеки прикладних програм (Open Web Application Security Project Top 10 list) **Г1.33.** Порядок розроблення заходів, направлених на виконання зауважень та рекомендацій, визначених за результатами аудиту **Г134**. Порядок контролю за виконанням заходів, направлених на виконання зауважень та рекомендацій, визначених за результатами аудиту	актам/законам для забезпечення відповідності **Г1.У2.** Розроблювати заходи, направлені на виконання зауважень та рекомендацій, визначених за результатами аудиту **Г1.У3.** Відслідковувати виконання заходів, направлених на виконання зауважень та рекомендацій, визначених за результатами аудиту
		Г2.Здатність нагля-дати за захисними чи коректувальними заходами при виявленні кіберінциденту або вразливості	**Г2.31.** Порядок нагляду за захисними чи коректувальними заходами при виявленні кіберінциденту або вразливості **А4.31.** Методологію виявлення вторгнень і способи виявлення вторгнень до хостів і мережі (К0046) **А4.32.** Архітектурні концепції та загальні принципи інформаційних технологій (ІКТ) **А4.33.** Вимоги в рамках Загальних принципів управління	**Г2.У1.** Наглядати за захисними чи коректувальними 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.** Приймати участь у розробленні відповідних заходів та профілактичних робіт відповідного

	комп'ютерні алгоритми, алгоритми шифрування; бази даних		ризиками (RMF) **А4.34.** Загрози і вразливості безпеки систем і прикладного програмного забезпечення (наприклад, переповнення буфера, мобільний код, міжсайтові сценарії, процедурна мова/мова структурованих запитів [PL/SQL] та ін'єкції, перегони фронтів, прихований канал, повтор, атаки на повернення, шкідливий код) **А4.35.** Класифікацію мережевих атак, та який існує зв'язок між мережевими атаками і загрозами та вразливостями **А4.36.** Використовувану на підприємстві/ в організації програми класифікації інформації і процедур розкриття	спрямування
Д. Координація та участь в управлінні діяльністю із забезпечення безпеки інформаційно-	Нормативні установчі акти підприємства (організації); структура підприємства (організації);	**Д1.** Здатність здійснювати керівництво профільними працівниками з безпеки інформаційно-телекомунікаційних технологій (ІКТ)	**Д1.31**. Керівництва (настанови, інструкції) інші нормативні акти роботодавця з організації, координації діяльності та взаємодії структурних підрозділів підприємства/ організації	**Д1.У1**. Забезпечувати керівництво та управління персоналом у сфері інформаційних технологій (ІКТ) матеріалами та інструментаріями, необхідними для того, щоб обізнаність в кібербезпеці, базові знання, грамотність та тренінги

телекомунікаційних технологій (ІКТ)	положення про структурні підрозділи підприємства (організації); посадові інструкції керівників та фахівців структурних підрозділів підприємства/ організації, до функцій яких входять питання забезпечення безпеки інформацій-но-телекомуні-каційних технологій (ІКТ) та інші нормативні акти роботодавця з організації, координації діяльності та		**Д1.32**. Посадові інструкції фахівців структурних підрозділів підприємства/організації, до функцій яких входять питання безпеки інформаційно-телекомунікаційних технологій (ІКТ) **Д1.33**. Основи управління персоналом **Д1.34.** Порядок розроблення та підписання трудових договорів та контрактів **Д1.35.** Основи трудового законодавства **Д1.36**. Процедура розроблення програм та проведення тренінгів персоналу з питань безпеки інформаційно-телекомунікаційних технологій (ІКТ)	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 вище керівництво щодо аналізу витрат/вигоди програм, політик, процесів, систем та елементів інформаційної безпеки **Д1.У5.** Консультувати профільне вище керівництво або уповноважених представників щодо змін, які впливають на стан кібербезпеки на підприємстві/в організації **Д1.У6**. Керувати та контролювати персонал та укладання з ним контрактів
		Д2. Здатність взаємодіяти з керівництвом, технологічними та іншими підрозділами	**Д2.31.** Структуру підприємства (організації), функції структурних підрозділів, розподіл функцій між керівниками	**Д2.У1.** Брати участь в корпоративному процесі управління ризиками щоб забезпечити зменшення ризиків безпеки, і введення даних щодо інших

	взаємодії структурних підрозділів підприємства (організації); порядок і типові вимоги до проведення ділових (комерцій-них) перемовин; порядок розроблення та виконання договірних робіт для зовнішніх партнерів	підприємства/ організації стосовно технологічних питань відповідного спрямування	підприємства/організації, підпорядкованість підрозділів **Д2.З2**. Положення про структурні підрозділи підприємства/організації, що задіяні в спільному виконанні технологічних та інших функціональних завдань **Д2.З3**. Нормативні документи підприємства/організації з питань організації його діяльності **Д2.З4**. Підходи щодо розбудови загальної архітектури інформаційної безпеки підприємства/організації (EISA) з урахуванням вимог загальної стратегії безпеки організації **Д2.З5.** Регламент управління ризиками як засобу забезпечення зменшення ризиків безпеки, і введення даних щодо інших технічних ризиків **Д2.З6**. Основи менеджменту **Д2.З7**. Основи маркетингу	технічних ризиків **Д2.У2.** Надавати технічну документацію, звіти про інциденти, результати комп'ютерних перевірок, висновки та іншу інформацію про ситуацію для головних організацій **Д2.У4.** Створювати загальну архітектуру інформаційної безпеки підприємства/організації (EISA) з урахуванням вимог загальної стратегії безпеки організації **Д2.У5.** Визначати альтернативні стратегії інформаційної безпеки для дотримання цілей організаційної безпеки **Д2.У6.** Знаходити та управляти необхідними ресурсами, включаючи підтримку керівництва, фінансові ресурси та ключовий персонал з питань безпеки для сприяння досягненню цілей та завдань безпеки інформаційних технологій (IT) та зниження загального ризику організації **Д2.У7.** Знаходити необхідні ресурси, включаючи фінансові, для забезпечення безперервності

				функціонування операційних програм підприємства/організації **Д2.У8**. 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.З1**. Основи комунікаційного менеджменту **Д3.З2**. Основи ділової етики **Д3.З3.** Порядок і типові вимоги до проведення ділових/комерційних перемовин **Д3.З4**. Порядок розроблення та виконання договірних робіт для зовнішніх партнерів	**Д3.У1**. Взаємодіяти із зовнішніми організаціями (службою зі зв'язків з громадськістю, правоохоронними органами тощо) 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 в рамках програми, стратегії та виконання завдань **Д3.У3**. Супроводжувати договірні роботи із зовнішніми партнерами

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: Бурбела Ольга, член Громадської організації "Асоціація спеціалістів кібербезпеки";Єсін Віталій, професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В. Каразіна; Іванченко Євгенія, професор кафедри безпеки інформаційних технологій Національного авіаційного університету; Конюшок Сергій, заступник начальника інституту (з навчальної та наукової роботи) Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"; Лукова-Чуйко Наталія, завідувач кафедри КНУ ім. Тараса Шевченка; Мазур Наталія, заступник Голови Профспілки працівників зв'язку України; Маковець Сергій, директор з технологій ТОВ «ІНФОРМЕЙШН СІСТЕМС СЕК'ЮРІТІ ПАРТНЕРС»; Масленникова Тетяна, провідний науковий співробітник Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації Держспецзв'язку України; Пазюк Андрій, віце-президент Громадської організації «Українська академія кібербезпеки»; Педченко Євгеній, керівник відділу впровадження систем безпеки ТОВ «ІНТРАСИСТЕМС»; Попель Валерій, начальник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації Держспецзв'язку України; Прасолов Володимир, заступник директора департаменту державного контролю Держспецзв'язку України; Самохвалов Юрій, методист тренінгового центру ТОВ «ІССП Тренінг Центр»; Сєвєрінов Олександр. доцент кафедри безпеки інформаційних технологій Харківський національний університет радіоелектроніки; Толюпа Сергій, професор кафедри КНУ ім. Тараса Шевченка; Юдін Олексій, заступник директора Державного науково-дослідного інституту технологій кібербезпеки та 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.