Прим. № __

ЗАТВЕРДЖЕНО

Наказ Адміністрації Держспецзв'язку
25 листопада 2022 року № 715

Професійний стандарт
«Фахівець сфери захисту інформації»

1. Загальні відомості професійного стандарту

1.1. Основна мета професійної діяльності

Забезпечення захищеності (конфіденційності, цілісності, доступності) інформації, що обробляється (передається) в інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних системах від несанкціонованих дій з інформацією (включаючи комп'ютерні віруси), витоку технічними каналами та спеціальних впливів на засоби обробки інформації, а також інформації, що озвучується на об'єктах інформаційної діяльності, витоку технічними каналами.

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 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 62.09	Інша діяльність у сфері інформаційних технологій і комп'ютерних систем
		Розділ 63	Надання інформаційних послуг	**Група 63.9**	Надання інших інформаційних послуг
				Клас 63.99	Надання інших інформаційних послуг, н.в.і.у.
Секція M	Професійна, наукова та технічна діяльність	**Розділ 71**	Діяльність у сферах архітектури та інжинірингу; технічні	**Група 71.2**	Технічні випробування та дослідження
				Клас 71.20	Технічні випробування та дослідження

			випробування та дослідження		
		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 сфери захисту інформації 2139.2.

1.5. Професійна кваліфікація

Фахівець сфери захисту інформації (трудові функції А, Б, В, Г (за виключенням професійних компетенцій А10, Б4; в частині професійних компетентностей А3, А4, А8, Б1, Б2, Б3, В4 бере участь як член команди).

Провідний фахівець сфери захисту інформації (трудові функції А, Б, В, Г, Д (в частині професійних компетентностей А10, Д1, Д2 бере участь як член команди).

Системний фахівець сфери захисту інформації (трудові функції А, Б, В, Г, Д, Е).

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

Обіймає посаду фахівця сфери захисту інформації, провідного фахівця сфери захисту інформації, системного фахівця сфери захисту інформації.

Фахівець сфери захисту інформації, провідний фахівець сфери захисту інформації, системний фахівець сфери захисту інформації безпосередньо підпорядкований керівнику профільного структурного підрозділу (або уповноваженій особі) в структурних підрозділах підприємства/організації, державного органу, що визначає і реалізує політику у сфері захисту інформації та кібербезпеки, профільних науково-дослідних установах, підприємствах/ організаціях, які реалізовують або застосовують функції забезпечення захищеності (конфіденційності, цілісності, доступності) інформації, що обробляється (передається) в інформаційних

(автоматизованих), електронних комунікаційних та інформаційно-комунікаційних системах від несанкціонованих дій з інформацією (включаючи комп'ютерні віруси), від витоку технічними каналами та від спеціальних впливів на засоби обробки інформації, а також інформації, що озвучується на об'єктах інформаційної діяльності, – від витоку технічними каналами.

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

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 кваліфікації «Фахівець сфери захисту інформації»:

диплом бакалавра за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» (6 рівень НРК), а також свідоцтво про присвоєння (підвищення) кваліфікації «Фахівець сфери захисту інформації» або інший документ, що підтверджує професійну кваліфікацію «Фахівець сфери захисту інформації».

Для кваліфікацій «Провідний фахівець сфери захисту інформації» та «Системний фахівець сфери захисту інформації»:

диплом магістра за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» (7 рівень НРК), а також свідоцтво про присвоєння (підвищення) кваліфікації «Провідний фахівець сфери захисту інформації» або інший документ, що підтверджує професійну кваліфікацію «Провідний фахівець сфери захисту інформації»;

або свідоцтво про присвоєння (підвищення) кваліфікації «Системний фахівець сфери захисту інформації» або інший документ, що підтверджує професійну кваліфікацію «Системний фахівець сфери захисту інформації».

Фахівець сфери захисту інформації – 6 рівень НРК.

Провідний фахівець сфери захисту інформації – 7 рівень НРК.

Системний фахівець сфери захисту інформації – 7 рівень НРК.

2. Навчання та професійний розвиток

2.1. Первинна професійна підготовка (назва кваліфікації)

Для кваліфікації «Фахівець сфери захисту інформації» – підготовка на першому (бакалаврському) рівні вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології».

Для кваліфікацій «Провідний фахівець сфери захисту інформації», «Системний фахівець сфери захисту інформації» – підготовка на другому (магістерському) рівні вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології».

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

Підвищення кваліфікації «Фахівець сфери захисту інформації» для отримання професійної кваліфікації «Провідний фахівець сфери захисту інформації». Стаж роботи не менше двох років на посадах, що відповідають кваліфікації «Фахівець сфери захисту інформації».

Підвищення кваліфікації «Провідний фахівець сфери захисту інформації» для отримання професійної кваліфікації «Системний фахівець сфери захисту інформації». Стаж роботи не менше трьох років на посадах, що відповідають кваліфікації «Провідний фахівець сфери захисту інформації».

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

Закон України «Про інформацію».

Закон України «Про доступ до публічної інформації».

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

Закон України «Про державну таємницю».

Закон України «Про захист персональних даних».

Закон України «Про основні засади забезпечення кібербезпеки України».

Закон України «Про захист прав споживачів».

Кодекс законів про працю України.

Положення про технічний захист інформації в Україні, затверджені Указом Президента України 27.09.1999 № 1229.

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

Наказ державного комітету України по нагляду за охороною праці від 21.12.1993 за № 132 «Про Порядок опрацювання і затвердження роботодавцем нормативних актів з охорони праці, що діють на підприємстві», зареєстрований у Міністерстві юстиції України 07.02.1994 за № 20/229.

Наказ Комітету по нагляду за охороною праці Міністерства праці та соціальної політики України від 09.01.1998 за № 4 «Про затвердження

Правил безпечної експлуатації електроустановок споживачів», зареєстрований в Міністерстві юстиції України 10.02.1998 за № 93/2533.

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

Нормативні документи системи технічного захисту інформації (далі – НД ТЗІ), нормативні документи системи криптографічного захисту інформації та державні стандарти України (далі – ДСТУ) стосовно створення і функціонування комплексних систем захисту інформації (далі – КСЗІ) інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних систем, систем управління інформаційною безпекою (далі – СУІБ) підприємств (органів) та комплексів технічного захисту інформації, галузеві стандарти відповідного спрямування.

Загальні принципи для посилення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity).

Дорожня карта NIST для посилення кібербезпеки та захисту інформації критичної інфраструктури (NIST Roadmap for Improving Critical Infrastructure Cybersecurity).

Інші нормативно-правові, нормативно-технічні та нормативні акти, які регламентують питання захисту інформації та кібербезпеки.

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 входять до них), умовні позначення

Умовне позначення	Трудові функції	Професійні компетентності (за трудовою дією або групою трудових дій)	Умовне позначен
А	Впровадження систем та	Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту	**А1**

	комплексів захисту інформації	інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації	
		Здатність виявляти, досліджувати (оцінювати), системно аналізувати загрози для інформації, аналізувати ризики безпеки інформації та кібербезпеки у разі реалізації загроз	**А2**
		Здатність формувати стратегію і політики безпеки інформації в інформаційно-комунікаційних системах	**А3**
		Здатність аналізувати, розробляти та супроводжувати систему управління інформаційною безпекою підприємства/ організації	**А4**
		Здатність виконувати передпроєктні роботи щодо систем та комплексів захисту інформації	**А5**
		Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності	**А6**
		Здатність впроваджувати (активізувати) програмні та апаратні засоби захисту інформації в системах і на об'єктах	**А7**
		Здатність адмініструвати системи, мережі та системи безпеки інформації	**А8**
		Здатність розробляти, впроваджувати та аналізувати технічні документи, положення, інструкції щодо систем і комплексів захисту інформації	**А9**
		Здатність виявляти закладні пристрої на об'єктах інформаційної діяльності	**А10**
Б	Оцінювання відповідності систем, комплексів та засобів захисту інформації	Здатність проводити оцінку відповідності (атестацію) комплексів технічного захисту інформації	**Б1**
		Здатність проводити оцінку відповідності (державну експертизу) комплексних систем захисту інформації та засобів технічного захисту інформації	**Б2**
		Здатність проводити оцінку відповідності систем управління інформаційною безпекою	**Б3**
		Здатність проводити оцінку відповідності (державну експертизу) засобів криптографічного захисту інформації	**Б4**
В	Експлуатація та обслуговування систем і комплексів захисту інформації, моніторинг та	Здатність підтримувати системи та комплекси захисту інформації у робочому стані, оцінювати їх надійність та здійснювати контроль їх працездатності та виявлення місць відмов та інцидентів,	**В1**

	аудит загроз для інформації	проблем та подій в системі обробки звернень клієнтів	
		Здатність проводити періодичне обслуговування інформаційних систем та мереж, комплексних систем захисту інформації та комплексів технічного захисту інформації	**В2**
		Здатність виконувати попередній нескладний ремонт несправного апаратного забезпечення системи/сервера	**В3**
		Здатність здійснювати контроль за станом технічного та криптографічного захисту інформації	**В4**
		Здатність здійснювати постійний моніторинг та аудит загроз для інформації та відповідну модернізацію (доробку) систем і комплексів захисту інформації	**В5**
		Здатність проводити процедури сканування вразливостей і розпізнавання вразливостей в системах безпеки	**В6**
Г	Оцінювання відповідності програмних та апаратних засобів технічного та криптографічного захисту інформації	Здатність проводити оцінку відповідності (державну експертизу) програмних засобів технічного та криптографічного захисту інформації	**Г1**
		Здатність проводити оцінку відповідності (державну експертизу, сертифікацію) апаратних засобів технічного та криптографічного захисту інформації	**Г2**
Д	Унормування системи технічного та криптографічного захисту інформації	Здатність аналізувати, інтегрувати і використовувати кращі світові практики, стандарти при розробці нормативних документів системи технічного та криптографічного захисту інформації	**Д1**
		Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування щодо системи технічного та криптографічного захисту інформації	**Д2**
Е	Координація діяльності з технічного та криптографічного захисту інформації	Здатність здійснювати технічне керівництво фахівцями структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки	**Е1**
		Здатність взаємодіяти з керівництвом і фахівцями технологічних та інших підрозділів підприємства/організації з технологічних та інших питань, пов`язаних із забезпеченням захисту інформації та	**Е2**

		кіберзахисту	
		Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень	**Е3**
		Здатність надавати консультативні послуги та технічну допомогу з питань технічного та криптографічного захисту інформації та кіберзахисту	**Е4**

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. Впровадження систем та комплексів захисту інформації	Нормативні акти, нормативні та технічні документи, проєктна документація, протоколи, стандарти та сертифікати відповідного спрямування; комп'ютерне, програмне та техніко-технологічне забезпечення; комп'ютерні алгоритми, алгоритми шифрування; бази даних; інструменти проєктування та впровадження систем та комплексів захисту інформації; засоби вимірювальної техніки відповідного спрямування; програмні та апаратні	**А1.** Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації	**А1.31.** Поняття та класифікація інформації з обмеженим доступом, державні інформаційні ресурси **А1.32.** Поняття технічного та криптографічного захисту інформації **А1.33.** Концепції і протоколи комп'ютерних мереж, методології забезпечення мережевої безпеки та захисту інформації в автоматизованих (інформаційних) системах і на об'єктах інформаційної діяльності **А1.34**. Методи та процеси управління ризиками (методи оцінки та зниження ризиків) **А1.35.** Закони, нормативні акти, нормативні документи, що визначають вимоги із захисту інформації та кіберзахисту **А1.36.** Політики та етичні	**А1.У1.** Визначати (формулювати) потреби щодо захисту інформації, що обробляється в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах користувачів (замовників) **А1.У2.** Визначати (формулювати) потреби щодо захисту інформації, що озвучується на об'єктах інформаційної діяльності підприємства (організації) **А1.У3.** Визначати (формулювати) потреби до кібербезпеки в електронних комунікаційних та інформаційно-комунікаційних системах користувачів (замовників) **А1.У4.** Визначати та аналізувати вимоги щодо захисту інформації та кіберзахисту в інформаційно-комунікаційних системах та на об'єктах інформаційної діяльності підприємства (організації) **А1.У5.** Здійснювати попередню

	засоби технічного та криптографічного захисту інформації		норми приватності стосовно безпеки інформації та кібербезпеки **А1.37.** Принципи та способи захисту інформації, кібербезпеки та приватності **А1.38.** Класифікація операційних наслідків у результаті помилок із захисту інформації та кібербезпеки **А1.39.** Політики, вимоги та процедури безпеки ланцюжка постачання інформаційних технологій та управління ризиками ланцюжка постачання **А1.310.** Поняття комплексних систем захисту інформації та комплексів технічного захисту інформації, їх склад і призначення **А1.311.** Моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, призначених для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації	оцінку достатності потреб і вимог користувачів (замовників) для забезпечення необхідного рівня захисту інформації та кіберзахисту **А1.У6.** Застосовувати політики безпеки для досягнення цілей безпеки системи **А1.У7.** Аналізувати потреби та вимоги користувачів з метою планування і проведення розробки системи безпеки **А1.У8.** Використовувати моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації
		А2. Здатність виявляти, досліджувати (оцінювати), системно	**А2.31.** Класифікація загроз для інформації та кіберзагроз (загрози від несанкціонованих	**А2.У1.** Виявляти загрози для інформації та кіберзагрози в інформаційних, електронних

		аналізувати загрози для інформації, аналізувати ризики безпеки інформації та кібербезпеки у разі реалізації загроз	дій з інформацією, технічні канали витоку інформації, спеціальні впливи на засоби обробки інформації) **А2.32.** Методи (способи) та методики виявлення, дослідження та системного аналізу загроз для інформації та кіберзагроз **А2.33.** Форми та зміст моделей загроз для інформації, моделі порушника інформації; порядок їх розробки **А2.34.** Поняття ризиків безпеки інформації та кібербезпеки **А2.35.** Підходи, методи (способи) оцінки та аналізу ризиків безпеки інформації та кібербезпеки **А2.36.** Класифікація операційних наслідків, спричинених помилками в системі кібербезпеки **А2.37.** Поняття спеціальних впливів на засоби обробки інформації з метою знищення (спотворення), блокування інформації	комунікаційних та інформаційно-комунікаційних системах **А2.У2.** Виявляти загрози для інформації, що озвучується на об'єктах інформаційної діяльності (обґрунтовувати можливість створення певних технічних каналів витоку інформації, що озвучується на конкретному об'єкті інформаційної діяльності) **А2.У3.** Досліджувати (оцінювати) та системно аналізувати загрози для інформації та вразливості комп'ютерної системи (систем) для розробки профілю безпеки **А2.У4.** Оцінювати та аналізувати ризики безпеки інформації та кібербезпеки **А2.У5.** Розробляти модель загроз для інформації від несанкціонованих дій та модель порушника інформації **А2.У6.** Розробляти модель загроз для інформації від витоку технічними каналами **А2.У7.** Розробляти модель загроз для інформації від спеціальних впливів на засоби обробки інформації
		А3. Здатність формувати стратегію і політики безпеки інформації в	**А3.31.** Поняття стратегії і політики безпеки інформації в інформаційних, електронних комунікаційних та	**А3.У1.** Обґрунтовувати та розробляти політику безпеки інформації в інформаційних, електронних комунікаційних та

		інформаційно-комунікаційних системах	інформаційно-комунікаційних системах **А3.32.** Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи ешелонованого захисту (прикладна система ешелонованого захисту) **А3.33.** Принципи, моделі, інструменти та методи управління мережевими системами (наскрізний моніторинг продуктивності систем) **А3.34.** Зміст і порядок розробки політики безпеки інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах **А3.35.** Поняття профілю безпеки інформації та функціональних послуг безпеки **А3.36.** Поняття рівня гарантій реалізації функціональних послуг безпеки	інформаційно-комунікаційних системах **А3.У2.** Ураховувати методи управління мережевими системами при обґрунтуванні концепції безпеки інформації **А3.У3.** Ураховувати методи управління ризиками при обґрунтуванні концепції безпеки інформації **А3.У4.** Визначати (розробляти, обґрунтовувати) профіль безпеки інформації в автоматизованих системах різного класу **А3.У5.** Розробляти групові політики та переліки контролю доступу для забезпечення відповідності стандартам організації, бізнес-правилам і потребам **А3.У6.** Застосовувати політики безпеки інформації в інформаційно-комунікаційних системах для досягнення цілей безпеки системи
		А4. Здатність аналізувати, розробляти та супроводжувати систему управління інформаційною	**А4.31.** Поняття системи управління інформаційною безпекою підприємства/ організації **А4.32.** Принципи створення	**А4.У1.** Визначати сферу та межі (брати участь у визначенні сфери та меж) дії системи управління інформаційною безпекою підприємства/організації (далі – СУІБ)

		безпекою підприємства/ організації	систем управління інформаційною безпекою **А4.33.** Принципи створення систем інформаційної безпеки (NIST SP 800-160)	**А4.У2.** Розробляти (брати участь у розробці) СУІБ **А4.У3.** Впроваджувати (брати участь у впровадженні) СУІБ **А4.У4.** Здійснювати моніторинг та аналіз (брати участь у моніторингу та аналізуванні) СУІБ **А4.У5.** Здійснювати підтримку та вдосконалення (брати участь у здійсненні підтримки та вдосконаленні) СУІБ **А4.У6.** Створювати системи (брати участь у створенні систем) інформаційної безпеки **А4.У7.** Застосовувати сервіс-орієнтовані принципи архітектури безпеки, щоб задовольнити вимоги конфіденційності, цілісності та доступності організації
		А5. Здатність виконувати передпроєктні роботи щодо систем та комплексів захисту інформації	**А5.31.**Середовища функціонування автоматизованих систем **А5.32.** Загальний порядок створення комплексних систем захисту інформації та комплексів технічного захисту інформації **А5.33.** Порядок категоріювання об'єктів **А5.34.** Порядок і методи (способи) обстеження середових функціонування	**А5.У1.** Здійснювати категоріювання об'єктів інформаційної діяльності (об'єктів електронно-обчислювальної техніки) **А5.У2.** Здійснювати обстеження середовищ функціонування автоматизованих систем **А5.У3.** Здійснювати обстеження об'єктів інформаційної діяльності **А5.У4.** Розробляти моделі загроз для інформації **А5.У5.** Розробляти технічні завдання на створення комплексних систем

			автоматизованих систем та об'єктів інформаційної діяльності **А5.35.** Порядок розробки моделей загроз для інформації **А5.36.** Порядок розробки та зміст технічних завдань на створення комплексних систем захисту інформації та комплексів технічного захисту інформації	захисту інформації **А5.У6.** Розробляти технічні завдання на створення комплексів технічного захисту інформації **А5.У7.** Розробляти проєкти комплексних систем захисту інформації та комплексів технічного захисту інформації багаторівневими вимогами безпеки або вимогами для обробки кількох рівнів класифікації даних (відкрита інформація, службова інформація, секретна інформація з різними ступенями секретності)
		А6. Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності	**А6.31.** Поняття спеціальних досліджень засобів обробки інформації, технічних засобів **А6.32.** Поняття спеціальних досліджень об'єктів інформаційної діяльності **А6.33.** Архітектура комп'ютера, принципи дії складових електронно-обчислювальної машини, комп'ютерні мережі, класи автоматизованих систем **А6.34.** Поняття об'єкта інформаційної діяльності **А6.35.** Поняття показників захищеності інформації засобів обробки інформації та показників захищеності мовної інформації на об'єкті	**А6.У1.** Проводити спеціальні дослідження засобів обробки інформації, технічних засобів (визначати складові та режими роботи засобів обробки інформації та технічних засобів, визначати тестові сигнали, складати схеми спеціальних досліджень, виявляти та вимірювати небезпечні (тестові) електричні, електромагнітні та оптичні сигнали, визначати показники захищеності інформації засобів обробки інформації, технічних засобів та можливість (неможливість) створення ними або через них певних технічних каналів витоку інформації) **А6.У2.** Проводити спеціальні дослідження об'єктів інформаційної

			інформаційної діяльності **А6.36.** Методи вимірювання фізичних величин і принципи роботи сучасних засобів вимірювальної техніки (спектроаналізаторів, осцилографів, частотомірів, вольтметрів, омметрів) **А6.37.** Методики спеціальних досліджень засобів обробки інформації та об'єктів інформаційної діяльності **А6.38.** Теорія електромагнітного поля (в частині, необхідній для виконання професійних функцій) **А6.39.** Теорія акустики (в частині, необхідній для виконання професійних функцій) **А6.310.** Пристрої електротехніки (в частині, що складають архітектуру комп'ютера: друковані плати, мікросхеми, процесори, елементи пам'яті) **А6.311.** Теорія радіотехнічних ланцюгів і сигналів (у частині, необхідній для виконання професійних функцій) **А6.312.** Спектри сигналів і методи спектрального аналізу **А6.313.** Загальні положення теорії інформації та методи кодування	діяльності (складати схеми спеціальних досліджень, виявляти та вимірювати небезпечні (тестові) акустичні, віброакустичні, акустоелектричні, акустоелектромагнітні, лазерні сигнали, визначати показники захищеності мовної інформації на об'єкті інформаційної діяльності та можливість (неможливість) створення на об'єкті інформаційної діяльності певних технічних каналів витоку інформації) **А6.У3.** Визначати вимоги до показників (характеристик) апаратних засобів технічного захисту інформації, які необхідні для забезпечення захищеності інформації в системі або на об'єкті інформаційної діяльності **А6.У4.** Складати протоколи спеціальних досліджень **А6.У5.** Складати приписи на експлуатацію засобів обробки інформації та об'єктів інформаційної діяльності

			А6.314. Загальні положення теорії ймовірностей і нечітких множин **А6.315.** Статистична радіотехніка (прийом звісних сигналів на фоні шумів, оцінка параметрів сигналів, що приймаються на фоні шумів) **А6.316.** Методи цифрової обробки зображень та сигналів **А6.317.** Математика логарифмів, тригонометрія, лінійна алгебра, математичний аналіз, операційний аналіз, статистика (в частині, необхідній для виконання професійних функцій) **А6.318.** Концепції і протоколи комп'ютерних мереж **А6.319.** Технології передачі голосу по IP (VoIP)	
		А7. Здатність впроваджувати (активізувати) програмні та апаратні засоби захисту інформації в системах і на об'єктах	**А7.31.** Принципи, методи, засоби забезпечення безпеки інформації та інформаційних технологій (програмні засоби (механізми) захисту інформації, мережеві екрани, шифрування) **А7.32.** Методології забезпечення мережевої безпеки **А7.33.** Способи та апаратні засоби захисту інформації, методи автентифікації,	**А7.У1.** Використовувати методи комп'ютерного проєктування та моделювання систем для розробки технічних проєктів комплексних систем захисту інформації та комплексів технічного захисту інформації **А7.У2.** Визначати та групувати за пріоритетами основні системні функції або підсистеми, необхідні для підтримки основних

			авторизації та контролю доступу **А7.34.** Методологічні та математичні основи комп'ютерного проєктування та моделювання систем **А7.35.** Мови програмування мікроконтролерів і контролерів відповідно до норм IEC 61131-3 **А7.36.** Порядок розробки та зміст технічних проєктів комплексних систем захисту інформації та комплексів технічного захисту інформації **А7.37.** Методи техніко-економічного аналізу та обґрунтування проєктних рішень **А7.38.** Процедури активізації (настроювання) програмних механізмів захисту інформації в інформаційних системах **А7.39.** Процедури підключення до локальної мережі підприємства (організації) та до глобальних мереж; процедури активізації (настроювання) програмних мережевих механізмів захисту інформації **А7.310.** Концепції управління послугами для мереж і відповідних стандартів (бібліотека інфраструктури	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 **А7.У3.** Аналізувати проєктні обмеження та можливі компроміси системи безпеки інформації (комплексної системи захисту інформації) **А7.У4.** Проєктувати, розробляти та модифікувати програмні системи, використовуючи науковий аналіз і математичні моделі для прогнозування та вимірювання результатів та наслідків проекту **А7.У5.** Розробляти проєкти з кібербезпеки **А7.У6.** Проєктувати функції управління ключами стосовно сфери кібербезпеки **А7.У7.** Активізувати (налаштовувати) програмні механізми захисту інформації в інформаційних системах, електронних комунікаційних та інформаційно-комунікаційних системах (програмні фільтри, антивірусні програми, антишпигунське програмне забезпечення) **А7.У8.** Впроваджувати

			інформаційних технологій (ITIL) **А7.З11.** Способи провадження апаратних засобів захисту інформації	(налаштовувати) програмно-апаратні засоби захисту інформації в інформаційних системах, електронних комунікаційних та інформаційно-комунікаційних системах **А7.У9.** Впроваджувати (налаштовувати) програмні та програмно-апаратні засоби захисту мережевих комунікацій **А7.У10.** Впроваджувати (налаштовувати) апаратні засоби захисту інформації на об'єктах інформаційної діяльності **А7.У11.** Оцінювати якість виконаних робіт з впровадження програмних та апаратних засобів захисту інформації в системах і на об'єктах
		А8. Здатність адмініструвати системи, мережі та системи безпеки інформації	**А8.31.** Концепції адміністрування систем, мереж і систем безпеки інформації **А8.32.** Методики адміністрування систем, мереж і систем безпеки інформації **А8.33.** Політики адміністрування даних **А8.34.** Принципи, концепції і методи адміністрування серверів	**А8.У1.** Розробляти та документувати стандартні операційні процедури адміністрування систем, мереж і систем безпеки інформації **А8.У2.** Координувати свої дії з аналітиками системи захисту кіберпростору для управління та адміністрування оновлень правил і сигнатур (систем виявлення проникнення/захисту, антивірусу та чорних списків) для спеціалізованих прикладних програм у сфері кіберзахисту та захисту інформації **А8.У3.** Здійснювати системне

				адміністрування операційних систем і спеціалізованих прикладних програм кіберзахисту та захисту інформації, систем (антивірусне програмне забезпечення, засоби аудиту та відновлення) та пристроїв віртуальних приватних мереж (VPN), включаючи інсталяції, налаштування, обслуговування, резервне копіювання і відновлення **А8.У4.** Здійснювати адміністрування серверів **А8.У5.** Дотримуватись стандартних операційних процедур адміністрування систем організації **А8.У6.** Управляти системними/ серверними ресурсами, включаючи продуктивність, ємність, доступність, ремонтопридатність і здатність відновлюватись
		А9. Здатність розробляти, впроваджувати та аналізувати технічні документи, положення, інструкції щодо систем і комплексів захисту інформації	**А9.31.** Систему технічних документів щодо систем і комплексів захисту інформації **А9.32.** Вимоги до структури та змісту технічних документів щодо систем і комплексів захисту інформації **А9.33.** Вимоги та підходи до розроблення технічних документів положень, інструкцій, методичних матеріалів щодо систем і	**А9.У1.** Формувати (брати участь у формуванні) вимог до захисту інформації в інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності **А9.У2.** Розроблювати (брати участь у розробці) політики безпеки інформації в інформаційно-комунікаційних системах **А9.У3.** Розроблювати (брати участь у розробці) технічної та експлуатаційної документації щодо

			комплексів захисту інформації **А9.34.** Сучасні підходи до формування вимог до захисту інформації в інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності **А9.35.** Інструменти, методи та техніки проєктування систем, включаючи інструменти автоматизованого аналізу та проєктування систем	створення, державної експертизи, (атестації), ведення в експлуатацію, експлуатації систем і комплексів захисту інформації **А9.У4.** Застосовувати інструменти, методи та техніки проєктування систем, включаючи інструменти автоматизованого аналізу та проєктування систем **А9.У5.** Розроблювати плани аварійного відновлення та безперервності операцій в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах
		А10. Здатність виявляти закладні пристрої на об'єктах інформаційної діяльності	**А10.31.** Поняття закладних пристроїв для зняття інформації, що озвучується та/або обробляється на об'єкті інформаційної діяльності **А10.32.** Класифікація закладних пристроїв **А10.33.** Принцип дії закладних пристроїв основних класів **А10.34.** Методи (способи) виявлення закладних пристроїв на об'єктах інформаційної діяльності	**А10.У1.** Розробляти методику виявлення закладних пристроїв на об'єктах інформаційної діяльності **А10.У2.** Здійснювати виявлення (брати участь у виявленні) закладних пристроїв на об'єктах інформаційної діяльності **А10.У3.** Оформлювати акти за результатами виявлення закладних пристроїв на об'єктах інформаційної діяльності
Б. Оцінювання відповідності систем, комплексів та	Нормативні акти, нормативні документи, проєктна документація, протоколи, стандарти та	**Б1.** Здатність проводити оцінку відповідності (атестацію) комплексів технічного захисту	**Б1.31.** Поняття атестації комплексів технічного захисту інформації **Б1.32.** Порядок, умови та	**Б1.У1.** Складати програму та методику атестації комплексу технічного захисту інформації (далі – ТЗІ)

засобів захисту інформації	сертифікати щодо створення та оцінювання відповідності систем, комплексів та засобів захисту інформації; техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності; операційні системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми, алгоритми шифрування; бази даних; інструменти оцінювання відповідності систем, комплексів та засобів захисту інформації; засоби вимірювальної техніки та методики вимірювань оцінюваних показників систем, комплексів та засобів захисту інформації	інформації	організація проведення атестації комплексів технічного захисту інформації **Б1.33.** Поняття та загальний зміст програми та методики проведення атестації комплексів технічного захисту інформації **Б1.34.** Техніко-технологічне, комп'ютерне, програмне та інше забезпечення атестації комплексів технічного захисту інформації **Б1.35. З**асоби вимірювальної техніки та методики вимірювань оцінюваних показників комплексів технічного захисту інформації **Б1.36.** Документи, що оформлюються за результатами атестації комплексів технічного захисту інформації	**Б1.У2.** Здійснювати перевірку повноти і відповідності реалізованих заходів із захисту інформації вимогам технічного завдання на створення комплексу ТЗІ (або на створення КСЗІ в інформаційно-комунікаційних системах в частині вимог до захисту інформації від витоку технічними каналами), нормативно-правових актів та нормативних документів системи ТЗІ **Б1.У3.** Здійснювати інструментальний контроль захищеності інформації на об'єкті інформаційної діяльності від витоку технічними каналами **Б1.У4.** Робити висновки щодо відповідності комплексу ТЗІ вимогам технічного завдання на створення комплексу ТЗІ (або на створення КСЗІ в ІТС в частині вимог до захисту інформації від витоку технічними каналами), нормативно-правових актів і нормативних документів системи ТЗІ **Б1.У5.** Оформлювати протоколи інструментального контролю захищеності інформації на об'єкті інформаційної діяльності. **Б1.У6.** Оформлювати акти атестації комплексів ТЗІ та організовувати їх затвердження і реєстрацію

		Б2. Здатність проводити оцінку відповідності (державну експертизу) комплексних систем захисту інформації та засобів технічного захисту інформації	**Б2.З1.** Поняття та шляхи проведення державної експертизи комплексних систем захисту інформації та засобів технічного захисту інформації **Б2.З2.** Порядок, умови та організація проведення державної експертизи комплексних систем захисту інформації та засобів технічного захисту інформації **Б2.З3.** Поняття та загальний зміст програми та методики проведення державної експертизи комплексних систем захисту інформації та засобів технічного захисту інформації **Б2.З4.** Методи тестування та оцінки захищеності систем **Б2.З5.** Техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності комплексних систем захисту інформації **Б2.З6.** Засоби вимірювальної техніки та методики вимірювань оцінюваних показників комплексних систем захисту інформації та характеристик засобів технічного захисту інформації **Б2.З7.** Документи, що оформлюються за результатами	**Б2.У1.** Складати програму та методику проведення державної експертизи комплексних систем захисту інформації **Б2.У2.** Проводити попереднє ознайомлення з об'єктом експертизи та поглиблене обстеження об'єкта експертизи **Б2.У3.** Проводити експертні випробування та дослідження комплексних систем захисту інформації (оцінювати функціональні послуги безпеки, оцінювати рівні гарантій коректності реалізації функціональних послуг безпеки, перевіряти наявність зареєстрованого акта атестації комплексу ТЗІ, якщо такий комплекс входить до складу комплексної системи захисту інформації, або проводити його атестацію) **Б2.У4.** Оформлювати протоколи експертних випробувань та атестати відповідності комплексних систем захисту інформації **Б2.У5.** Здійснювати експертизу комплексних систем захисту інформації шляхом декларування, оформлювати декларації відповідності комплексних систем захисту інформації та організовувати їх затвердження та реєстрацію **Б2.У6.** Здійснювати експертизу

			державної експертизи комплексних систем захисту інформації та засобів технічного захисту інформації	засобів технічного захисту інформації, оформлювати протоколи експертних випробувань засобів технічного захисту інформації та експертні висновки на засоби ТЗІ, організовувати затвердження і реєстрацію експертних висновків
		Б3.Здатність проводити оцінку відповідності систем управління інформаційною безпекою	**Б3.31.** Поняття оцінки відповідності систем управління інформаційною безпекою **Б3.32.** Порядок, умови та організація проведення оцінки відповідності систем управління інформаційною безпекою **Б3.33.** Документи, що оформлюються за результатами оцінки відповідності систем управління інформаційною безпекою	**Б3.У1.** Здійснювати оцінку відповідності (брати участь в оцінці відповідності) систем управління інформаційною безпекою відповідно до стандартів ДСТУ ISO/IEC серії 27k **Б3.У2.** Аналізувати політику та конфігурації систем управління інформаційною безпекою організації та оцінювати її відповідність нормативним актам і нормативним документам з питань безпеки інформації та кібербезпеки та нормативним актам і директивам організації **Б3.У3.** Аналізувати проєктні обмеження, компроміси та детальний проєкт системи управління інформаційною безпекою організації **Б3.У4.** Оцінювати ефективність заходів із захисту інформації, заходів з режиму та управління доступом, заходів з кібербезпеки, які використовуються системою управління інформаційною безпекою організації

				Б3.У5. Переконуватися, що усі операції з безпеки та їх технічна підтримка належним чином задокументовані та оновлюються в разі необхідності **Б3.У6.** Переконуватися, що вимоги із захисту інформації та кібербезпеки інтегровані в планування безперервного функціонування системи та/або організації **Б3.У7.** Здійснювати точну технічну оцінку програмного забезпечення прикладних програм, СУІБ чи мережі, а також реалізованих заходів із кіберзахисту вимогам кібербезпеки та можливим вразливостям **Б3.У8.** Оформлювати документи за результатами оцінки відповідності систем управління інформаційною безпекою
		Б4. Здатність проводити оцінку відповідності (державну експертизу) засобів криптографічного захисту інформації	**Б4.31.** Поняття та порядок проведення державної експертизи в сфері криптографічного захисту інформації **Б4.32.** Умови та організація проведення державної експертизи в сфері криптографічного захисту інформації **Б4.33.** Поняття та загальний зміст програми та методики	**Б4.У1.** Здійснювати державну експертизу в сфері криптографічного захисту інформації (проводити експертні (тематичні) дослідження об'єктів експертизи у сфері криптографічного захисту інформації) **Б4.У2.** Складати програму та методику експертних досліджень об'єктів експертизи у сфері криптографічного захисту інформації **Б4.У3.** Оформлювати протоколи

			проведення експертних досліджень при проведенні державної експертизи в сфері криптографічного захисту інформації **Б4.34.** Документи, що оформлюються за результатами державної експертизи в сфері криптографічного захисту інформації **Б4.35.** Загальні положення криптології, криптографії та криптографічного аналізу	експертних досліджень об'єктів експертизи у сфері криптографічного захисту інформації **Б4.У4.** Оформлювати експертні висновки на засоби КЗІ, організовувати затвердження і реєстрацію експертних висновків
В. Експлуатація та обслуговування систем і комплексів захисту інформації, моніторинг та аудит загроз для інформації	Протоколи, стандарти, та сертифікати відповідного спрямування; комп'ютерне, програмне та техніко-технологічне забезпечення; операційні системи; прилади та інструменти для діагностування та ремонту несправного апаратного забезпечення системи/сервера, апаратних засобів захисту інформації	**В1.** Здатність підтримувати системи та комплекси захисту інформації у робочому стані, оцінювати їх надійність та здійснювати контроль їх працездатності та виявлення місць відмов та інцидентів, проблем та подій в системі обробки звернень клієнтів	**В1.31.** Принципи взаємодії «людина-комп'ютер» **В1.32.** Загальні положення теорії надійності, методи діагностики працездатності та виявлення місця відмов у комп'ютерних системах, системах і комплексах захисту інформації **В1.33.** Принципи стійкості та надмірності в комп'ютерних системах і комплексах захисту інформації	**В1.У1.** Здійснювати контроль працездатності комп'ютерних систем, систем і комплексів захисту інформації **В1.У2.** Діагностувати несправне апаратне забезпечення системи/сервера **В1.У3.** Застосовувати засоби контролю працездатності та виявлення місця відмов **В1.У4.** Виявляти місця відмов у комп'ютерних системах, системах і комплексах захисту інформації **В1.У5.** Організовувати (проводити) ремонт апаратних засобів захисту інформації зі складу комплексних систем захисту інформації та комплексів технічного захисту інформації

		В2. Здатність проводити періодичне обслуговування інформаційних систем та мереж, комплексних систем захисту інформації та комплексів технічного захисту інформації	**В2.31.** Типи та періодичність планової підтримки апаратного забезпечення, періодичність підтримки та оновлення програмного забезпечення **В2.32.** Підходи щодо забезпечення безпеки віртуальних приватних мереж (VPN)	**В2.У1.** Проводити чищення систем і мереж (фізичне й електронне), здійснювати перевірку дисків і завантажувальних програм, ізолювати та видаляти шкідливе програмне забезпечення **В2.У2.** Виправляти фізичні та технічні проблеми, що впливають на роботу системи/сервера **В2.У3.** Встановлювати оновлення системи та компонентів (серверів, пристроїв, мережевих пристроїв) **В2.У4.** Моніторити та оптимізувати роботу системи/сервера **В2.У5.** Відновлювати системи/ сервери після виявленого збою (програмне забезпечення для відновлення, відмовостійкі кластери, дублювання/«зеркалювання») **В2.У6.** Здійснювати оновлення баз даних антивірусних програм, програмних механізмів захисту інформації **В2.У7.** Проводити періодичне обслуговування апаратних засобів захисту інформації зі складу комплексних систем захисту інформації та комплексів технічного захисту інформації **В2.У8.** Документувати та приводити у відповідність інформаційну безпеку організації, архітектуру кібербезпеки та вимоги техніки безпеки системи

				протягом всього життєвого циклу системи
		В3. Здатність виконувати попередній нескладний ремонт несправного апаратного забезпечення системи/сервера	**В3.31.** Методи (способи) тестування, оцінки та ремонту комп'ютерних систем, систем і комплексів захисту інформації **В3.32.** Інструменти діагностики систем і методик визначення несправностей **В3.33.** Засоби та діагностики систем/серверів, методики визначення несправностей **В3.34.** Види попереднього нескладного ремонту несправного апаратного забезпечення системи/сервера **В3.35.** Технічні регламенти та специфікації відповідного ремонту **В3.36.** Прилади та інструменти, програмне забезпечення, необхідні для проведення попереднього нескладного ремонту несправного апаратного забезпечення системи/сервера, апаратних засобів захисту інформації	**В3.У1.** Здійснювати заходи з тестування елементів систем безпеки та ІКС **В3.У2.** Діагностувати проблеми з підключенням **В3.У3.** Здійснювати інтегроване тестування системи безпеки та інформаційно-комп'ютерних систем **В3.У4.** Виконувати попередній нескладний ремонт несправного апаратного забезпечення системи/сервера **В3.У5.** Виконувати ремонт систем і комплексів захисту інформації **В3.У6.** Здійснювати усунення неполадок і діагностування аномалій функціонування інфраструктури системи безпеки на основі її аналізу
		В4. Здатність здійснювати контроль за станом технічного та криптографічного захисту інформації	**В4.31.** Поняття та зміст контролю за станом технічного та криптографічного захисту інформації **В4.32.** Методи контролю за	**В4.У1.** Організовувати (приймати участь в організації) контроль за станом технічного та криптографічного захисту інформації **В4.У2.** Перевіряти виконання вимог

			станом технічного та криптографічного захисту інформації **В4.33.** Організація та порядок здійснення контролю за станом технічного та криптографічного захисту інформації **В4.34.** Інструментарій контролю за станом технічного та криптографічного захисту інформації	нормативно-правових актів і нормативних документів з технічного та криптографічного захисту інформації на підприємстві/в організації **В4.У3.** Застосовувати засоби контролю захищеності інформації **В4.У4.** Користуватися інструментарієм контролю за станом технічного та криптографічного захисту інформації **В4.У5.** Визначати стан технічного та криптографічного захисту інформації на підприємстві/в організації **В4.У6.** Оформлювати документи за результатами контролю стану технічного та криптографічного захисту інформації на підприємстві/в організації
		В5. Здатність здійснювати постійний моніторинг та аудит загроз для інформації та відповідну модернізацію (доробку) систем і комплексів захисту інформації	**В5.31.** Методи та технології моніторингу та аудиту загроз для конфіденційності, цілісності та доступності інформації **В5.32.** Методи, засоби та інформаційні технології виявлення несанкціонованого доступу до інформації на різних ієрархічних рівнях інформаційно-комунікаційної системи **В5.33.** Класифікація контрзаходів для виявлених	**В5.У1.** Здійснювати моніторинг та аудит загроз для інформації в інформаційних системах та мережах та оцінку ризиків безпеки інформації **В5.У2.** Здійснювати моніторинг та аудит загроз для інформації, що озвучується **В5.У3.** Використовувати інструменти та технології безперервного моніторингу з метою оцінки ризиків, користуватися прикладними програмами моніторингу та аудиту загроз для інформації в

			ризиків безпеки інформації **В5.34.** Інструментарій (прикладні програми) моніторингу (аудиту) загроз для інформації в інформаційних системах та мережах **В5.35.** Способи модернізації (доробки) систем і комплексів захисту інформації відповідно до виявлених актуальних загроз для інформації	інформаційних системах та мережах **В5.У4.** Проводити аудити/огляди систем і комплексів захисту інформації (систем безпеки інформації) та інформаційно-комунікаційних систем **В5.У5.** Здійснювати модернізацію (доробку) систем і комплексів захисту інформації відповідно до виявлених актуальних загроз для інформації **В5.У6.** Використовувати відповідні інструменти для відновлення програмного, апаратного та периферійного обладнання системи **В5.У7.** Здійснювати визначення, модифікацію та маніпулювання з відповідними системними компонентами у ОС Windows, Unix або Linux (паролі, облікові записи користувачів, файли) **В5.У8.** Співпрацювати із системними аналітиками, інженерами, програмістами, з метою отримання інформації про обмеження та можливості системи, вимог до продуктивності та інтерфейсів, шляхів модернізації систем і комплексів захисту інформації
		В6. Здатність проводити процедури сканування вразливостей і	**В6.31.** Інструментарій сканування та розпізнавання вразливостей у системах	**В6.У1.** Проводити сканування вразливостей і розпізнання вразливостей в ІКС і системах

		розпізнавання вразливостей в системах безпеки	безпеки для інформації в інформаційних системах і мережах **В6.32.** Способи сканування розпізнавання вразливостей у системах безпеки для інформації в інформаційних системах і мережах	безпеки **В6.У2.** Виявляти проблеми кібербезпеки, безпеки інформації і приватності, які виникають при з'єднаннях внутрішніх і зовнішніх замовників та організацій-партнерів на основі аналізу даних вразливостей і конфігурації інформаційно-комунікаційних систем і мереж
Г. Оцінювання відповідності програмних та апаратних засобів технічного та криптографічного захисту інформації	Нормативні акти, нормативні документи, проєктна документація, протоколи, стандарти та сертифікати щодо створення та оцінювання відповідності програмних та апаратних засобів технічного та криптографічного захисту інформації; техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності; операційні системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми,	**Г1.** Здатність проводити оцінку відповідності (державну експертизу) програмних засобів технічного та криптографічного захисту інформації	**Г1.31.** Загальні способи оцінювання відповідності програмних засобів технічного захисту інформації **Г1.32.** Поняття державної експертизи програмних засобів технічного захисту інформації **Г1.33.** Порядок та організація проведення державної експертизи програмних засобів технічного захисту інформації **Г1.34.** Поняття та загальний зміст програми та методики проведення державної експертизи програмних засобів технічного захисту інформації **Г1.35.** Техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності програмних засобів технічного захисту інформації **Г1.36.** Документи, що	**Г1.У1.** Складати програму та методику проведення державної експертизи програмних засобів технічного захисту інформації **Г1.У2.** Проводити експертні випробування та дослідження програмних засобів технічного захисту інформації (оцінювати функціональні послуги безпеки, оцінювати рівні гарантій коректності реалізації функціональних послуг безпеки) **Г1.У3.** Оцінювати відповідність програмних засобів технічного захисту інформації задекларованим характеристикам та вимогам нормативних документів системи технічного захисту інформації **Г1.У4.** Виконувати безпечне тестування, огляд та/або оцінку програм, щоб виявити потенційні недоліки в кодах і пом'якшити вразливості

	алгоритми шифрування; бази даних; інструменти оцінювання відповідності програмних та апаратних засобів технічного та криптографічного захисту інформації; засоби вимірювальної техніки та методики вимірювань оцінюваних показників апаратних засобів технічного та криптографічного захисту інформації		оформлюються за результатами державної експертизи програмних засобів технічного захисту інформації	**Г1.У5.** Оформлювати протоколи експертних випробувань та експертні висновки за результатами державної експертизи та організовувати їх затвердження і реєстрацію
		Г2. Здатність проводити оцінку відповідності (державну експертизу, сертифікацію) апаратних засобів технічного та криптографічного захисту інформації	**Г2.31.** Загальні способи оцінювання відповідності апаратних засобів технічного та криптографічного захисту інформації **Г2.32.** Поняття державної експертизи апаратних засобів технічного та криптографічного захисту інформації **Г2.33.** Порядок, умови та організація проведення державної експертизи апаратних засобів технічного та криптографічного захисту інформації **Г2.34.** Поняття та загальний зміст програми та методики проведення державної експертизи апаратних засобів технічного та криптографічного захисту інформації **Г2.35.** Техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності апаратних засобів технічного та криптографічного захисту інформації	**Г2.У1.** Складати програму та методику проведення державної експертизи апаратних засобів технічного захисту інформації **Г2.У2.** Проводити експертні випробування та дослідження апаратних засобів технічного захисту інформації (склади схеми вимірювань характеристик засобів, вимірювати (визначати) функціональні характеристики засобів) **Г2.У3.** Оцінювати відповідність апаратних засобів технічного захисту інформації задекларованим характеристикам та вимогам нормативних документів системи технічного захисту інформації **Г2.У4.** Оформлювати протоколи експертних випробувань та експертні висновки за результатами державної експертизи та організовувати їх затвердження і реєстрацію

			Г2.36. Засоби вимірювальної техніки та методики вимірювань оцінюваних показників апаратних засобів технічного та криптографічного захисту інформації **Г2.37.** Документи, що оформлюються за результатами державної експертизи апаратних засобів технічного та криптографічного захисту інформації **Г2.38.** Загальні поняття сертифікації апаратних засобів технічного та криптографічного захисту інформації	
Д. Унормування системи технічного та криптографічного захисту інформації	Нормативні акти, нормативні та технічні документи системи технічного та криптографічного захисту інформації; концепції, кращі практики та стандарти розвитку системи технічного та криптографічного захисту інформації; нормативні документи з розробки та впровадження нормативних документів	**Д1.** Здатність аналізувати, інтегрувати і використовувати кращі світові практики, стандарти при розробці нормативних документів системи технічного та криптографічного захисту інформації	**Д1.31.** Організаційно-технічна система захисту інформації та кіберзахисту України **Д1.32.** Система нормативних документів (нормативна база) системи технічного та криптографічного захисту інформації України **Д1.33.** Кращі світові практики, стандарти із захисту інформації **Д1.34.** Загальні поняття та способи (методи) системного та експертного аналізу стосовно кращих світових практик, стандартів із захисту інформації	**Д1.У1.** Аналізувати систему нормативних документів (нормативну базу) системи технічного та криптографічного захисту інформації України **Д1.У2.** Виявляти, ставити та вирішувати проблемні питання щодо системи нормативних документів (нормативної бази) системи технічного та криптографічного захисту інформації України **Д1.У3.** Проводити системний аналіз світових практик, стандартів із захисту інформації **Д1.У4.** Організовувати проведення експертного аналізу кращих світових

	системи технічного та криптографічного захисту інформації			практик, стандартів із захисту інформації **Д1.У5.** Брати участь в експертному аналізі кращих світових практик, стандартів із захисту інформації
		Д2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування щодо системи технічного та криптографічного захисту інформації	**Д2.З1.** Порядок розробки та впровадження нормативних документів системи технічного та криптографічного захисту інформації **Д2.З2.** Порядок актуалізації нормативних документів системи технічного та криптографічного захисту інформації	**Д2.У1.** Розробляти (брати участь у розробці) нормативні документи системи технічного та криптографічного захисту інформації **Д2.У2.** Писати та публікувати методики та настанови з кіберзахисту та інструктивні матеріали **Д2.У3.** Впроваджувати нормативні документи системи технічного та криптографічного захисту інформації **Д2.У4.** Здійснювати актуалізацію нормативних документів системи технічного та криптографічного захисту інформації **Д2.У5.** Використовувати результати аналізу кращих світових практик, стандартів при розробці нормативних документів системи технічного та криптографічного захисту інформації
Е. Координація діяльності з технічного та криптографічного захисту інформації	Нормативні установчі акти підприємства (організації); структура підприємства (організації); положення про структурні підрозділи підприємства	**Е1.** Здатність здійснювати технічне керівництво фахівцями структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та	**Е1.З1.** Керівництва (настанови, інструкції), нормативні акти роботодавця з організації, координації діяльності та взаємодії структурних підрозділів підприємства/ організації **Е1.З2.** Посадові інструкції	**Е1.У1.** Здійснювати методичне та технічне керівництво фахівцями структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки **Е1.У2.** Координувати роботи (брати участь у координації робіт) із захисту

	(організації); посадові інструкції керівників та фахівців структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки та 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	кібербезпеки	фахівців структурних підрозділів підприємства/організації, до функцій яких входять питання захисту інформації та кібербезпеки **Е1.33.** Основи управління персоналом **Е1.34.** Архітектура інформаційних технологій (ІТ) підприємства	інформації та кібербезпеки в структурних підрозділах підприємства/організації **Е1.У3.** Координувати та надавати експертну технічну підтримку технічним спеціалістам з кіберзахисту в масштабах усієї організації для управління інцидентами у сфері кіберзахисту **Е1.У4.** Виконувати обов'язки внутрішнього консультанта і радника в своїй експертній області. Надавати консультативно-методичну допомогу працівникам структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки, з відповідних питань **Е1.У5.** Приймати участь в організації та навчанні (підвищенні кваліфікації) працівників структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки, з відповідних питань
		Е2. Здатність взаємодіяти з керівництвом і фахівцями технологічних та інших підрозділів підприємства/організації	**Е2.31.** Структура підприємства (організації), функції структурних підрозділів, розподіл функцій між керівниками підприємства (організації), підпорядкованість підрозділів	**Е2.У1.** Взаємодіяти з керівництвом та працівниками технологічних та інших підрозділів підприємства (організації) з технологічних та інших питань, пов'язаних із забезпеченням захисту інформації та кіберзахисту (організувати та

		з технологічних та інших питань, пов'язаних із забезпеченням захисту інформації та кіберзахисту	**Е2.32.** Положення про структурні підрозділи підприємства (організації), що задіяні в спільному виконанні технологічних та функціональних завдань **Е2.33.** Нормативні документи підприємства (організації) з питань організації його діяльності	отримувати від технологічних та інших підрозділів інформацію, необхідну для організації захисту інформації та кіберзахисту, узгоджувати та погоджувати технічну документацію на системи та комплекси захисту інформації, доводити до керівництва підрозділів недоліки у захисті інформації та пропозиції до їх усунення, пропозиції що удосконалення систем та комплексів захисту інформації) **Е2.У2.** Готувати звернення (листи), заяви, звітньо-аналітичні та документи щодо організації та здійснення захисту інформації та кіберзахисту у профільному та інших структурних підрозділах підприємства (організації)
		Е3. Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень	**Е3.31.** Основи комунікаційного менеджменту **Е3.32.** Основи ділової етики **Е3.33.** Порядок і типові вимоги до проведення ділових/комерційних перемовин **Е3.34.** Порядок розроблення та виконання договірних робіт для зовнішніх партнерів	**Е3.У1.** Співпрацювати із зовнішніми партнерами доступними засобами комунікації стосовно питань захисту інформації і кіберзахисту **Е3.У2.** Приймати участь в ділових/комерційних перемовинах із зовнішніми партнерами **Е3.У3.** Супроводжувати договірні роботи із зовнішніми партнерами **Е3.У4.** Взаємодіяти з регуляторними органами та органами з акредитації
		Е4. Здатність надавати консультативні послуги	**Е4.31.** Порядок і типові вимоги з надання консультативних	**Е4.У1.** Надавати консультативні послуги з питань технічного та

		та технічну допомогу з питань технічного та криптографічного захисту інформації та кіберзахисту	послуг з питань технічного та криптографічного захисту **Е4.32.** Предметну область консультативних послуг з питань технічного та криптографічного захисту інформації та кіберзахисту	криптографічного захисту інформації та кіберзахисту **Е4.У2.** Консультувати керівництво (директора з інформаційних технологій) або уповноважених представників щодо рівня ризику та стану безпеки **Е4.У3.** Консультувати керівництво або уповноважених представників щодо аналізу витрат/вигоди програм, політик, процесів, систем та елементів інформаційної безпеки **Е4.У4.** Консультувати керівництво або уповноважених представників щодо змін, які впливають на стан кібербезпеки в організації **Е4.У5.** Аналізувати питання, пов'язані з предметною областю **Е4.У6.** Аналізувати запити на отримання інформації з метою визначення наявності необхідної інформації для відповіді **Е4.У7.** Здійснювати управління відносинами з клієнтами, включаючи визначення потреб/вимог клієнтів, управління очікуваннями клієнта та демонстрацію відданості досягненню якісних результатів **Е4.У8.** Інтерпретувати закони, нормативні акти, політики, стандарти чи процедури в області технічного та криптографічного захисту інформації та кіберзахисту щодо конкретних

				питань **Е4.У9.** Проводити інтерактивні тренінгові вправи для створення ефективного навчального середовища

7. Дані щодо розроблення та затвердження професійного стандарту

7.1. Розробник професійного стандарту

Державна служба спеціального зв'язку та захисту інформації України.

Склад робочої групи:

Головенко Андрій Валерійович, керівник робочої групи, заступник директора Департаменту захисту інформації Адміністрації Держспецзв'язку;

Бурбела Ольга Олександрівна, член Громадської організації «Асоціація спеціалістів кібербезпеки»;

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

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

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

Жилін Артем Вікторович, начальник 6 управління Державного центру кіберзахисту Держспецзв'язку;

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 інституту імені Ігоря Сікорського»;

Корченко Олександр Григорович, президент Громадської організації «Асоціація спеціалістів кібербезпеки», заступник голови профспілкової організації кафедри безпеки інформаційних технологій Національного авіаційного університету;

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

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

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 «Українськ академія кібербезпеки»;

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

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

Прокопович-Ткаченко Дмитро Ігорович, завідувач кафедри кібербезпеки Університету митної справи та фінансів;

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

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

Супрун Ольга Миколаївна, 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

25 листопада 2022 року.

7.4. Рекомендована дата наступного перегляду професійного стандарту

25 листопада 2027 року.

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