Проєкт

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

Професійний стандарт
«Фахівець сфери захисту інформації»

1. Загальні відомості професійного стандарту

1.1. Основна мета професійної діяльності

Забезпечення захищеності (приватності, 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.

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	Назва секції видів економічної діяльності	Розділ	Назва розділу	Група	Назва групи
					Клас Назва класу
J	Інформація та телекомунікації	**62**	Комп'ютерне програмування, консультування та пов'язана з ними діяльність	**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
		63	Надання інформаційних послуг	**63.9**	Надання інших інформаційних послуг, н.в.і.у.
					Клас 63.99 Надання інших інформаційних послуг, н.в.і.у.
M	Професійна, наукова та технічна діяльність	**71**	Діяльність у сферах архітектури та інжинірингу; технічні випробування та дослідження	**71.2**	Технічні випробування та дослідження
					71.20 Технічні випробування та дослідження
		74	Інша професійна, наукова та технічна діяльність	**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 сфери захисту інформації 2139.2

1.5. Професійна кваліфікація

Фахівець сфери захисту інформації (трудові функції А, Б, В, Г (в частині професійних компетентностей А3, А4, А9, Б1, Б2, Б3, В4, Д2, Е1, Е3, Е4 він приймає участь як член команди)).

Провідний (системний) фахівець сфери захисту інформації (трудові функції А, Б, В, Г, Е).

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

Структурний підрозділ підприємства/організації, до функцій якого входять питання захисту інформації та кібербезпеки. Профільний структурний підрозділ із захисту інформації та кібербезпеки підприємства (організації). Державний орган, що визначає і реалізує політику у сфері захисту інформації 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 фахівця сфери захисту інформації – диплом бакалавра за спеціальністю 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» (6 рівень НРК).

Для провідного (системного) фахівця сфери захисту інформації та системного фахівця сфери захисту інформації – диплом магістра за спеціальністю 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» (7 рівень НРК).

2. Навчання та професійний розвиток

2.1. Первинна професійна підготовка (назва кваліфікації)

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

Для провідного (системного) фахівця сфери захисту інформації – підготовка на другому (магістерському) рівні вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології».

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

Підвищення кваліфікації фахівця сфери захисту інформації для отримання професійної кваліфікації провідного (системного) фахівця сфери

захисту інформації. Стаж роботи не менше двох років на посадах, що відповідають кваліфікації фахівця 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 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, телекомунікаційних та інформаційно-телекомунікаційних 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 (НД ТЗІ), нормативні документи системи криптографічного захисту інформації та державні стандарти України (ДСТУ) стосовно створення і функціонування комплексних систем захисту інформації (КСЗІ) інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних систем, систем управління інформаційною безпекою (СУІБ) підприємств (органів) та комплексів технічного захисту інформації, галузеві стандарти відповідного спрямування;

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

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

4. Загальні компетентності

ЗК.01	Здатність до абстрактного мислення, аналізу та синтезу, вчитися і бути сучасно навченим
ЗК.02	Здатність виявляти, формулювати та розв’язувати складні задачі (проблеми) у сфері професійної діяльності, застосовувати знання у практичних ситуаціях, розв’язувати спеціалізовані завдання/задачі та практичні проблеми у сфері професійної діяльності
ЗК.03	Здатність використовувати у професійній діяльності знання законів та підзаконних нормативно-правових актів України, нормативних і нормативно-технічних документів, галузевих стандартів у сфері професійної діяльності
ЗК.04	Здатність проводити дослідження на відповідному рівні
ЗК.05	Здатність оцінювати та забезпечувати якість виконуваних робіт
ЗК.06	Здатність виявляти, досліджувати (оцінювати), системно аналізувати загрози у сфері професійної діяльності та ризики їх реалізації
ЗК.07	Здатність формувати стратегію і політику в сфері професійної діяльності
ЗК.08	Здатність впроваджувати, оцінювати відповідність та експлуатувати системи та комплекси захисту інформації та системи управління інформаційною безпекою
ЗК.09	Здатність застосовувати інструменти, методи і техніки впровадження та оцінки відповідності систем та комплексів захисту інформації, систем управління інформаційною безпекою
ЗК.10	Здатність розуміти поняття та визначення у сфері професійної діяльності, розуміти цілі та результати професійної діяльності
ЗК.11	Здатність розуміти проблеми, цілі та результати діяльності підприємства/організації, пов’язані із захистом інформації та кіберзахистом
ЗК.12	Здатність розробляти технічну документацію
ЗК.13	Здатність до адаптації та дії у новій ситуації
ЗК.14	Здатність до вибору стратегії спілкування, працювати в команді, брати участь в якості члена груп планування, координаційних і оперативних груп
ЗК.15	Здатність спілкуватися рідною мовою як усно, так і письмово, спілкуватися другою мовою (переважно англійською) на рівні, що забезпечує ефективну професійну діяльність
ЗК.16	Здатність ставити уточнюючі питання
ЗК.17	Здатність впевнено і систематизовано доводити складну інформацію, концепції або ідеї в усній і письмовій формах і/або за допомогою наочних засобів
ЗК.18	Здатність застосовувати принципи приватності підприємства/ організації (стосовно конфіденційності, цілісності, доступності, автентифікації і неспростовності інформації) під час професійної

	діяльності
ЗК.19	Здатність дотримуватися правил та норм з безпеки та охорони праці, зокрема щодо безпечної експлуатації електронного устаткування та електричного обладнання

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

Умовні позна-чення	Трудові функції	Професійні компетентності (за трудовою дією або групою трудових дій)	Умовні позна-чення
А	Впровадження систем та комплексів захисту інформації	Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації	**А1**
		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 і 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 та інших технічних засобів та об’єктів інформаційної діяльності	**А6**
		Здатність впроваджувати (ативізувати) програмні та	**А7**

		апаратні засоби захисту інформації в системах та на об’єктах	
		Здатність розробляти, впроваджувати та аналізувати технічні документи, положення, інструкції щодо систем та комплексів захисту інформації	**А8**
		Здатність виявляти закладні пристрої на об’єктах інформаційної діяльності	**А9**
Б	Оцінювання відповідності систем та комплексів захисту інформації	Здатність проводити оцінку відповідності (атестацію) комплексів технічного захисту інформації	**Б1**
		Здатність проводити оцінку відповідності (державну експертизу) комплексних систем захисту інформації	**Б2**
		Здатність проводити оцінку відповідності систем управління інформаційною безпекою	**Б3**
В	Експлуатація та обслуговування систем і комплексів захисту інформації, моніторинг та аудит загроз для інформації	Здатність підтримувати системи та комплекси захисту інформації у робочому стані, здійснювати контроль їх працездатності та виявлення місць відмов	**В1**
		Здатність проводити періодичне обслуговування інформаційних систем та мереж, комплексних систем захисту інформації та комплексів технічного захисту інформації	**В2**
		Здатність виконувати попередній не складний ремонт несправного апаратного забезпечення системи/сервера	**В3**
		Здатність здійснювати контроль за станом технічного та криптографічного захисту інформації	**В4**
		Здатність здійснювати	**В5**

		постійний моніторинг (аудит) загроз для інформації та відповідну модернізацію (доробку) систем та комплексів захисту інформації	
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 та фахівцями технологічних та інших підрозділів підприємства/ організації з технологічних та інших питань, пов’язаних із	**Е2**

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

6. Опис трудових функцій

Трудові функції	Предмети і засоби праці (обладнання, устаткування, матеріали, продукти, інструменти)	Професійні компетентності	Знання	Уміння і 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 інше техніко-технологічне забезпечення; комп'ютерні алгоритми, алгоритми	**А1**. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації	**А1.З1.** Поняття та класифікація інформації з обмеженим доступом, державні інформаційні ресурси **А1.З2.** Поняття технічного та криптографічного захисту інформації **А1.З3.** Концепції і протоколи комп'ютерних мереж, методології забезпечення мережевої безпеки та захисту інформації в автоматизованих (інформаційних) системах та на об'єктах інформаційної діяльності **А1.З4**. Методи та процеси управління ризиками (наприклад, методи оцінки та зниження ризиків)	**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-

	шифрування; бази даних; інші інструменти проєктування та впровадження систем та комплексів захисту інформації; засоби вимірювальної техніки відповідного спрямування; програмні та апаратні засоби технічного та криптографічного захисту інформації		**А1.З5**. Закони, нормативні акти, нормативні документи, що визначають вимоги із захисту інформації та кіберзахисту **А1.З6.** Політики і етичні норми приватності стосовно безпеки інформації та кібербезпеки **А1.З7**. Принципи та способи захисту інформації, кібербезпеки і приватності **А1.З8**. Класифікація операційних наслідків в результаті помилок із захисту інформації та кібербезпеки **А1.З9**. Політики, вимоги і процедури безпеки ланцюжка постачання інформаційних технологій та управління ризиками ланцюжка постачання **А1.З10**. Поняття комплексних систем захисту інформації та комплексів технічного захисту інформації, їх склад та призначення **А1.З11**. Моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем,	комунікаційних системах та на об’єктах інформаційної діяльності підприємства (організації) **А1.У5.** Здійснювати попередню оцінку достатності потреб та вимог користувачів (замовників) для забезпечення необхідного рівня захисту інформації та кіберзахисту

			призначених для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації	
		А2. Здатність виявляти, досліджувати (оцінювати), системно аналізувати загрози для інформації, аналізувати ризики безпеки інформації та кібербезпеки у разі реалізації загроз	**А2.З1.** Класифікація загроз для інформації та кіберзагроз (загрози від несанкціонованих дій з інформацією, технічні канали витоку інформації, спеціальні впливи на засоби обробки інформації) **А2.З2**. Методи (способи) і методики виявлення, дослідження та системного аналізу загроз для інформації та кіберзагроз **А2.З3.** Форми і зміст моделей загроз для інформації, моделі порушника інформації; порядок їх розробки **А2.З4.** Поняття ризиків безпеки інформації та кібербезпеки **А2.З5.** Підходи, методи (способи) аналізу ризиків безпеки інформації та кібербезпеки **А2.З6.** Класифікацію операційних наслідків, спричинених помилками в	**А2.У1.** Виявляти загрози для інформації та кіберзагрози в інформаційних, електронних 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.** Проводити сканування вразливостей і розпізнавання вразливостей в системах безпеки інформації та кібербезпеки **А2.У4**. Досліджувати (оцінювати) та системно аналізувати загрози для інформації та вразливості комп’ютерної системи (систем) для розробки профілю ризику безпеки **А2.У5**. Аналізувати ризики безпеки інформації та кібербезпеки

			системі кібербезпеки **А2.З7.** Поняття спеціальних впливів на засоби обробки інформації з метою знищення (спотворення) , блокування інформації	**А2.У6**. Розробляти модель загроз для інформації від несанкціонованих дій та модель порушника інформації **А2.У7**. 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 інформаційно-комунікаційних системах	**А3.З1.** Поняття стратегії і політики безпеки інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах **А3.З2**. Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи (прикладна система ешелонованого захисту тощо) **А3.З3**. Принципи, моделі, інструменти та методи управління мережевими системами (наскрізний моніторинг продуктивності систем тощо)	**А3.У1.** Обґрунтовувати та розробляти політику безпеки інформації в інформаційних, електронних комунікаційних та 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

			А3.З4. Зміст та порядок розробки політики безпеки інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах **А3.З5.** Поняття профілю безпеки інформації та функціональних послуг безпеки **А3.З6.** Поняття рівня гарантій реалізації функціональних послуг безпеки	системах різного класу **А3.У5.** Розробляти групові політики та переліки контролю доступу для забезпечення відповідності стандартам організації, бізнес-правилам та потребам
		А4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою підприємства/ організації	**А4.З1.** Поняття системи управління інформаційною безпекою підприємства/організації **А4.З2.** Принципи створення систем управління інформаційною безпекою **А4.З3.** Принципи створення систем інформаційної безпеки (NIST SP 800-160)	**А4.У1.** Визначати (приймати участь у визначенні) сферу та межі дії системи управління інформаційною безпекою підприємства/організації (далі – СУІБ) **А4.У2.** Розробляти (приймати участь у розробки) СУІБ **А4.У3.** Впроваджувати (приймати участь у впровадженні) СУІБ **А4.У4.** Здійснювати (приймати участь у здійсненні) моніторинг та аналізування СУІБ **А4.У5.** Здійснювати (приймати участь у здійсненні) підтримку та вдосконалення СУІБ **А4.У6.** Створювати (приймати участь у створенні) систем

				інформаційної безпеки (NIST SP 800-160) **А4.У7.** Застосовувати сервіс-орієнтовані принципи архітектури безпеки, щоб задовольнити вимоги приватності , цілісності та доступності організації
		А5. Здатність виконувати передпроєктні роботи щодо систем та комплексів захисту інформації	**А5.З1.**Середовища функціонування автоматизованих систем **А5.З2.** Загальний порядок створення комплексних систем захисту інформації та комплексів технічного захисту інформації **А5.З3.** Порядок категоріювання об’єктів **А5.З4**. Порядок та методи (способи) обстеження середових функціонування автоматизованих систем та об’єктів інформаційної діяльності **А5.З5.** Порядок розробки моделей загроз для інформації **А5.З6.** Порядок розробки та зміст технічних завдань на створення комплексних систем захисту інформації та комплексів технічного захисту інформації	**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 захисту інформації **А5.У6.** Розробляти технічні завдання на створення комплексів технічного захисту інформації

		А6. Здатність проводити спеціальні дослідження засобів обробки інформації, інших технічних засобів та об’єктів інформаційної діяльності	**А6.З1.** Поняття спеціальних досліджень засобів обробки інформації, інших технічних засобів **А6.З2.** Поняття спеціальних досліджень об’єктів інформаційної діяльності **А6.З3.** Архітектура комп’ютера, принципи дії складових електронно-обчислювальної машини, комп’ютерні мережі, класи автоматизованих систем **А6.З4.** Поняття об’єкта інформаційної діяльності **А6.З5.** Поняття показників захищеності інформації засобів обробки інформації та показників захищеності мовної інформації на об’єкті інформаційної діяльності **А6.З6.** Методи вимірювання фізичних величин та принципи роботи сучасних засобів вимірювальної техніки (спектроаналізаторів, осцилографів, частотомірів, вольтметрів, омметрів) **А6.З7.** Методики спеціальних	**А6.У1.** Проводити спеціальні дослідження засобів обробки інформації, інших технічних засобів (визначати складові та режими роботи засобів обробки інформації та інших 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, інших технічних засобів та можливість (неможливість) створення ними або через них певних технічних каналів витоку інформації) **А6.У2.** Проводити спеціальні дослідження об’єктів інформаційної діяльності (складати схеми спеціальних досліджень, виявляти та вимірювати небезпечні (тестові) акустичні, віброакустичні, акустоелектричні, акустоелектромагнітні, лазерні сигнали, визначати показники захищеності мовної інформації на

			досліджень засобів обробки інформації і об’єктів інформаційної діяльності **А6.38.** Теорію електромагнітного поля (в частині, необхідній для виконання професійних функцій) **А6.39.** Теорію 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 тощо) **А6.311** Теорію радіотехнічних ланцюгів та сигналів (в частині, необхідній для виконання професійних функцій) **А6.310.** Спектри сигналів та методи спектрального аналізу **А6.311.** Загальні положення теорії інформації та методи кодування **А6.312.** Загальні положення теорії ймовірностей та нечітких множин **А6.313.** Статистичну	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

			радіотехніку (прийом звісних сигналів на фоні шумів, оцінка параметрів сигналів, що приймаються на фоні шумів) **А6.314.** Методи цифрової обробки зображень та сигналів **А6.315.** Загальні положення криптології, криптографії та криптографічного аналізу **А6.316.** Математику логарифмів, тригонометрія, лінійна алгебра, математичний аналіз, операційний аналіз, статистика (в частині, необхідній для виконання професійних функцій) **А6.317.** Концепції і протоколи комп'ютерних мереж **А6.318.** Технології передачі голосу по IP (VoIP)	
		А7. Здатність впроваджувати (активізувати) програмні та апаратні засоби захисту інформації в системах та на об'єктах	**А7.31.** Принципи, методи, засоби забезпечення безпеки інформації та інформаційних технологій (програмні засоби (механізми) захисту інформації, мережеві екрани, шифрування тощо) **А7.32.** Методології забезпечення мережевої безпеки **А7.33.** Способи та апаратні	**А7.У1.** Використовувати методи комп'ютерного проектування та моделювання систем для розробки технічних проектів комплексних систем захисту інформації та комплексів технічного захисту інформації **А7.У2.** Використовувати моделі та симуляції інформаційних,

			засоби захисту інформації **А7.З4.** Методологічні та математичні основи комп'ютерного проектування та моделювання систем **А7.З5.** Мови програмування мікроконтролерів та контролерів відповідно до норм IEC 61131-3 **А5.З6.** Порядок розробки та зміст технічних проектів комплексних систем захисту інформації та комплексів технічного захисту інформації **А7.З7.** Методи техніко-економічного аналізу та обґрунтування проектних рішень **А7.З8**. Процедури активізації (настроювання) програмних механізмів захисту інформації в інформаційних системах **А7.З9**. Процедури підключення до локальної мережі підприємства (організації) та до глобальних мереж. Процедури активізації (настроювання) програмних мережевих механізмів захисту інформації. **А7.З10.** Концепції управління	електронних комунікаційних та інформаційно-комунікаційних систем для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації **А7.У3**. Визначати та групувати за пріоритетами основні системні функції або підсистеми, необхідні для підтримки основних можливостей або бізнес-функцій з метою відновлення або поновлення після відмови системи або під час відновлення системи на основі загальних системних вимог щодо безперервності та доступності **А7.У4.** Аналізувати проєктні обмеження та можливі компроміси системи безпеки інформації (комплексної системи захисту інформації) **А7.У5.** Проєктувати, розробляти та модифікувати програмні системи, використовуючи науковий аналіз та математичні моделі для прогнозування та вимірювання результатів та наслідків проекту **А7.У6.** Розробляти проєкти з

			послугами для мереж і відповідних стандартів (бібліотека інфраструктури інформаційних технологій (ITIL) тощо) **А7.З11**. Способи провадження апаратних засобів захисту інформації	кібербезпеки **А7.У7**. Проєктувати функції управління ключами стосовно сфери кібербезпеки **А7.8.** Активізувати (налаштовувати) програмні механізми захисту інформації в інформаційних системах, електронних комунікаційних та інформаційно-комунікаційних системах (наприклад, програмні фільтри, антивірусні програми, антишпигунське програмне забезпечення) **А7.У9.** Впроваджувати (налаштовувати) програмно-апаратні засоби захисту інформації в інформаційних системах, електронних комунікаційних та інформаційно-комунікаційних системах **А7.У10.** Впроваджувати (налаштовувати) програмні та програмно-апаратні засоби захисту мережевих комунікацій **А7.У11.** Впроваджувати (налаштовувати) апаратні засоби захисту інформації на об’єктах

				інформаційної діяльності **А7.У12.** Оцінювати якість виконаних робіт з впровадження програмних та апаратних засобів захисту інформації в системах та на об’єктах
		А8. Здатність розробляти, впроваджувати та аналізувати технічні документи, положення, інструкції щодо систем та комплексів захисту інформації	**А8.31.** Систему технічних документів щодо систем та комплексів захисту інформації **А8.32**. Вимоги до структури та змісту технічних документів щодо систем та комплексів захисту інформації **А8.33**. Вимоги та підходи до розроблення технічних документів положень, інструкції, методичних матеріалів щодо систем та комплексів захисту інформації **А8.34.** Сучасні підходи до формування вимог до захисту інформації в інформаційно-комунікаційних системах та на об’єктах інформаційної діяльності **А8.35.** Інструменти, методи і техніки проєктування систем, включаючи інструменти	**А8.У1.** Формувати (брати участь у формуванні) вимог до захисту інформації в інформаційно-комунікаційних системах та на об’єктах інформаційної діяльності **А8.У2.** Розроблювати (брати участь у розробці) політики безпеки інформації в інформаційно-комунікаційних системах **А8.У3.** Розроблювати (брати участь у розробці) технічної та експлуатаційної документації щодо створення, державної експертизи, (атестації), ведення в експлуатацію, експлуатації систем та комплексів захисту інформації **А8.У4.** Застосовувати інструменти, методи і техніки проєктування систем, включаючи інструменти автоматизованого аналізу та проєктування систем **А8.У5.** Розроблювати плани

			автоматизованого аналізу та проєктування систем	аварійного відновлення та безперервності операцій в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах
		А9. Здатність виявляти закладні пристрої на об’єктах інформаційної діяльності	**А9.З1.** Поняття закладних пристроїв для зняття інформації, що озвучується та/або обробляється на об’єкті інформаційної діяльності **А9.З2.** Класифікація закладних пристроїв **А9.З3.** Принцип дії закладних пристроїв основних класів **А9.З4.** Методи (способи) виявлення закладних пристроїв на об’єктах інформаційної діяльності	**А9.У1.** Розробляти методику виявлення закладних пристроїв на об’єктах інформаційної діяльності **А9.У2.** Здійснювати виявлення (приймати участь у виявленні) закладних пристроїв на об’єктах інформаційної діяльності **А9.У3.** Оформлювати акти за результатами виявлення закладних пристроїв на об’єктах інформаційної діяльності
Б. Оцінювання відповідності систем та комплексів захисту інформації	Нормативні акти, нормативні документи, проєктна документація, протоколи, стандарти та сертифікати щодо створення та оцінювання	**Б1.** Здатність проводити оцінку відповідності (атестацію) комплексів технічного захисту інформації	**Б1.З1.** Поняття атестації комплексів технічного захисту інформації **Б1.З2.** Порядок, умови та організація проведення атестації комплексів технічного захисту інформації **Б1.З3.** Поняття та загальний зміст програми та методики проведення атестації комплексів	**Б1.У1.** Складати програму та методику атестації комплексу ТЗІ **Б1.У2.** Здійснювати перевірку повноти і відповідності реалізованих заходів із захисту інформації вимогам технічного завдання на створення комплексу ТЗІ (або на створення КСЗІ в ІТС в частині вимог до захисту інформації від витоку технічними

	відповідності систем та комплексів захисту інформації; техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності; операційні та інші системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми, алгоритми шифрування; бази даних; інші інструменти оцінювання відповідності систем та комплексів захисту інформації; засоби		технічного захисту інформації **Б1.З4.** Техніко-технологічне, комп'ютерне, програмне та інше забезпечення атестації комплексів технічного захисту інформації **Б1.З5.** Засоби вимірювальної техніки та методики вимірювань оцінюваних показників комплексів технічного захисту інформації **Б1.З6.** Документи, що оформлюються за результатами атестації комплексів технічного захисту інформації	каналами), нормативно-правових актів та нормативних документів стреми ТЗІ **Б1.У3.** Здійснювати інструментальний контроль захищеності інформації на ОІД 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 та нормативних документів стреми ТЗІ **Б1.У5.** Оформлювати протоколи інструментального контролю захищеності інформації на ОІД **Б1.У6.** Оформлювати акти атестації комплексів ТЗІ та організовувати їх затвердження і реєстрацію
		Б2. Здатність проводити оцінку відповідності (державну експертизу)	**Б2.З1.** Поняття та шляхи проведення державної експертизи комплексних систем захисту інформації **Б2.З2.** Порядок, умови та	**Б2.У1.** Складати програму та методику проведення державної експертизи комплексних систем захисту інформації **Б2.У2.** Проводити попереднє

	вимірювальної техніки та методики вимірювань оцінюваних показників систем та комплексів захисту інформації	комплексних систем захисту інформації	організація проведення державної експертизи комплексних систем захисту інформації **Б2.З3.** Поняття та загальний зміст програми та методики проведення державної експертизи комплексних систем захисту інформації **Б2.З4.** Техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності комплексних систем захисту інформації **Б2.З5.** Засоби вимірювальної техніки та методики вимірювань оцінюваних показників комплексних систем захисту інформації **Б2.З6.** Документи, що оформлюються за результатами державної експертизи комплексних систем захисту інформації	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 ходи)ь 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 і реєстрацію
		Б3.Здатність проводити оцінку відповідності систем управління інформаційною безпекою	**Б3.З1.** Поняття оцінки відповідності систем управління інформаційною безпекою **Б3.З2.** Порядок, умови та організація проведення оцінки відповідності систем управління інформаційною безпекою **Б3.З3.** Документи, що оформлюються за результатами оцінки відповідності систем управління інформаційною безпекою	**Б3.У1.** Здійснювати оцінку відповідності (приймати 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 та нормативним документам з питань безпеки інформації та кібербезпеки та нормативним актам та директивам організації **Б3.У3.** Аналізувати проектні обмеження, компроміси та детальний проект 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
В. Експлуатація та обслуговування систем і комплексів	Протоколи, стандарти, та сертифікати відповідного спрямування;	**В1.** Здатність підтримувати системи та комплекси захисту	**В1.31.** Принципи взаємодії «людина-комп’ютер» **В1.32.** Загальні положення теорії надійності, методи діагностики працездатності та виявлення	**В1.У1.** Здійснювати контроль працездатності комп'ютерних систем, систем та комплексів захисту інформації **В1.У2.** Застосовувати засоби

захисту інформації, моніторинг та аудит загроз для інформації	компьютерне, програмне та інше техніко-технологічне забезпечення; операційні та інші системи; прилади та інструменти для діагностування та ремонту несправного апаратного забезпечення системи/сервера, апаратних засобів захисту інформації	інформації у робочому стані, здійснювати контроль їх працездатності та виявлення місць відмов	місця відмов в комп'ютерних системах, системах та комплексах захисту інформації **В1.З3.** Принципи стійкості і надмірності в комп'ютерних системах та комплексах захисту інформації	контролю працездатності та виявлення місця відмов **В1.У3.** Виявляти місця відмов в комп'ютерних системах, системах та комплексах захисту інформації **В1.У4.** 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.З1.** Типи і періодичність планової підтримки апаратного забезпечення, періодичність підтримки та оновлення програмного забезпечення **В2.З2.** Підходи щодо забезпечення безпеки віртуальних приватних мереж (VPN)	**В2.У1**. Проводити чищення систем і мереж (фізичне й електронне), перевірку дисків, завантажувальних програм, видаляти дані та тестування **В2.У2.** Виправляти фізичні та технічні проблеми, що впливають на роботу системи/сервера **В2.У3.** Ідентифікувати та прогнозувати системну/серверну роботу, доступність, можливості або проблеми з налаштуванням **В2.У4**. Встановлювати оновлення системи та компонентів (серверів, пристроїв, мережевих пристроїв тощо) **В2.У5**. Моніторити та оптимізову-

				вати роботу системи/сервера **В2.У6**. Відновлювати системи/сервери після виявленого збою (програмне забезпечення для відновлення, відмовостійкі кластери, дублювання/ «зеркалювання» тощо) **В2.У7**. Здійснювати оновлення баз даних антивірусних програм, програмних механізмів захисту інформації **В2.У8.** Проводити періодичне обслуговування апаратних засобів захисту інформації зі складу комплексних систем захисту інформації та комплексів технічного захисту інформації **В2.У9.** Документувати та приводити у відповідність інформаційну безпеку організації, архітектуру кібербезпеки та вимоги техніки безпеки системи протягом всього життєвого циклу системи
		В3. Здатність виконувати попередній не складний ремонт несправного	**В3.З1.** Методи (способи) ремонту комп'ютерних систем, систем та комплексів захисту інформації **В3.З2**. Засоби діагностики систем/серверів, методики	**В3.У1**. Виконувати попередній не складний ремонт несправного апаратного забезпечення системи/сервера **В3.У2**. Виконувати ремонт систем

		апаратного забезпечення системи/сервера	визначення несправностей **В3.З3.** Види попереднього нескладного ремонту несправного апаратного забезпечення системи/сервера **В3.З4.** Технічні регламенти та специфікації відповідного ремонту **В3.З5**. Прилади та інструменти, програмне забезпечення тощо, необхідні для проведення попереднього нескладного ремонту несправного апаратного забезпечення системи/сервера, апаратних засобів захисту інформації	та комплексів захисту інформації **В3.У3**. Здійснювати заходи з тестування елементів систем безпеки та ІКС **В3.У4**. Діагностувати проблеми з підключенням **В3.У5**. Здійснювати інтегроване тестування системи безпеки та ІКС **В3.У6**. Здійснювати усування неполадок і діагностування аномалій функціонування інфраструктури системи безпеки на основі її аналізу
		В4. Здатність здійснювати контроль за станом технічного та криптографічного захисту інформації	**В4.З1.** Поняття та зміст контролю за станом технічного та криптографічного захисту інформації **В4.З2.** Методи контролю за станом технічного та криптографічного захисту інформації **В4.З3**. Організацію та порядок здійснення контролю за станом технічного та криптографічного захисту інформації	**В4.У1.** Організовувати (приймати участь в організації) контроль за станом технічного та криптографічного захисту інформації **В4.У2.** Перевіряти виконання вимог нормативно-правових актів та нормативних документів з технічного та криптографічного захисту інформації на підприємстві/ в організації **В4.У3.** Застосовувати засоби

			В4.З4. Інструментарій контролю за станом технічного та криптографічного захисту інформації	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 та комплексів захисту інформації	**В5.З1.** Методи та технології моніторингу (аудиту) загроз для конфіденційності, цілісності та доступності інформації **В5.З2.** Методи, засоби та інформаційні технології виявлення несанкціонованого доступу до інформації на різних ієрархічних рівнях інформаційно-комунікаційної системи **В5.З3.** Класифікацію контрзаходів для виявлених ризиків безпеки інформації	**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.** Користуватися прикладними програмами моніторингу та аудиту загроз для інформації в інформаційних системах та мережах

			В5.З4. Інструментарій (прикладні програми) моніторингу (аудиту) загроз для інформації в інформаційних системах та мережах **В5.З5.** Способи модернізації (доробки) систем та комплексів захисту інформації відповідно до виявлених актуальних загроз для інформації	**В5.У4.** Проводити сканування вразливостей і розпізнання вразливостей в ІКС та системах безпеки **В5.У5.** Виявляти системні проблеми системи безпеки інформації на основі аналізу даних вразливостей та конфігурації інформаційно-комунікаційних систем **В5.У6.** Проводити аудити/огляди систем та комплексів захисту інформації (систем безпеки інформації) та інформаційно-комунікаційних систем **В5.У7.** Здійснювати модернізацію (доробку) систем та комплексів захисту інформації відповідно до виявлених актуальних загроз для інформації **В5.У8.** Використовувати відповідні інструменти для відновлення програмного, апаратного та периферійного обладнання системи **В5.У9.** Здійснювати визначення, модифікацію і маніпулювання з відповідними системними компонентами у ОС Windows, Unix

				або Linux (наприклад, паролі, облікові записи користувачів, файли) **В5.У10.** Співпрацювати із системними аналітиками, інженерами, програмістами тощо, з метою отримання інформації про обмеження та можливості системи, вимог до продуктивності та інтерфейсів, шляхів модернізації систем та комплексів захисту інформації
Г. Оцінювання відповідності програмних та апаратних засобів технічного та криптографіч-ного 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	**Г1.** Здатність проводити оцінку відповідності (державну експертизу) програмних засобів технічного та криптографічного захисту інформації	**Г1.З1.** Загальні способи оцінювання відповідності програмних засобів технічного та криптографічного захисту інформації **Г1.З2.** Поняття державної експертизи програмних засобів технічного та криптографічного захисту інформації **Г1.З3.** Порядок та організація проведення державної експертизи програмних засобів технічного та криптографічного захисту інформації **Г1.З4.** Поняття та загальний зміст програми та методики	**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

	інформації; техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності; операційні та інші системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми, алгоритми шифрування; бази даних; інші інструменти оцінювання відповідності програмних та апаратних засобів технічного та криптографічного захисту інформації; засоби		проведення державної експертизи програмних засобів технічного та криптографічного захисту інформації **Г1.З5.** Техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності програмних засобів технічного та криптографічного захисту інформації **Г1.З6.** Документи, що оформлюються за результатами державної експертизи програмних засобів технічного та криптографічного захисту інформації	нормативних документів системи технічного захисту інформації **Г1.У4.** 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.З1.** Загальні способи оцінювання відповідності апаратних засобів технічного та криптографічного захисту інформації **Г2.З2.** Поняття державної експертизи апаратних засобів технічного та криптографічного захисту інформації **Г2.З3.** Порядок, умови та організація проведення державної експертизи апаратних	**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)

	вимірювальної техніки та методики вимірювань оцінюваних показників апаратних засобів технічного та криптографічного захисту інформації		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 **Г2.36.** 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	**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

			сертифікації апаратних засобів технічного та криптографічного захисту інформації	
Д. Унормування системи технічного та криптографіч-ного 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 системи технічного та	**Д1.** Здатність аналізувати, інтегрувати і використовувати кращі світові практики, стандарти при розробці нормативних документів системи технічного та криптографічного захисту інформації	**Д1.31.** Організаційно-технічну систему захисту інформації та кіберзахисту України **Д1.32.** Систему 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 практик, стандартів із захисту інформації **Д1.У5.** Брати участь в експертному аналізі кращих світових практик, стандартів із захисту інформації
		Д2. Здатність розробляти, впроваджувати та	**Д2.31.** Порядок розробки та впровадження нормативних документів системи технічного	**Д2.У1.** Розробляти (приймати участь у розробці) нормативні документи системи технічного та

	криптографічного захисту інформації	аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування щодо системи технічного та криптографічного захисту інформації	та криптографічного захисту інформації **Д2.З2.** Порядок актуалізації нормативних документів системи технічного та криптографічного захисту інформації	криптографічного захисту інформації **Д2.У2.** Впроваджувати нормативні документи системи технічного та криптографічного захисту інформації **Д2.У3.** Здійснювати актуалізацію нормативних документів системи технічного та криптографічного захисту інформації **Д2.У4.** Використовувати результати аналізу кращих світових практик, стандартів при розробці нормативних документів системи технічного та криптографічного захисту інформації
Е. Координація діяльності з технічного та криптографіч-ного захисту інформації	Нормативні установчі акти підприємства (організації); структура підприємства (організації); положення про структурні підрозділи підприємства (організації);	**Е1.** Здатність здійснювати технічне керівництво фахівцями структурних підрозділів підприємства (організації), до функцій яких входять питання захисту	**Е1.З1**. Керівництва (настанови, інструкції) інші нормативні акти роботодавця з організації, координації діяльності та взаємодії структурних підрозділів підприємства/ організації **Е1.З2**. Посадові інструкції фахівців структурних підрозділів підприємства/організації, до функцій яких входять питання захисту інформації та	**Е1.У1**. Здійснювати технічне керівництво фахівцями структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки **Е1.У2**. Координувати (примати участь у координації) роботи із захисту інформації та кібербезпеки в структурних підрозділах підприємства/організації **Е1.У3.** Надавати консультативно-

	посадові інструкції керівників та фахівців структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки та інші нормативні акти роботодавця з організації, координації діяльності та взаємодії структурних підрозділів підприємства (організації); порядок і типові вимоги до проведення ділових (комерційних) перемовин; порядок	інформації та кібербезпеки	кібербезпеки **Е1.З3**. Основи управління персоналом	методичну допомогу працівникам структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки, з відповідних питань **Е1.У4.** 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 та фахівцями технологічних та інших підрозділів підприємства (організації) з технологічних та інших питань, пов’язаних із забезпеченням захисту інформації та	**Е2.З1.** Структуру підприємства (організації), функції структурних підрозділів, розподіл функцій між керівниками підприємства (організації), підпорядкованість підрозділів Е**2.З2**. Положення про структурні підрозділи підприємства (організації), що задіяні в спільному виконанні технологічних та інших функціональних завдань **Е2.З3**. Нормативні документи	**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 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,

	розроблення та виконання договірних робіт для зовнішніх партнерів	кіберзахисту	підприємства (організації) з питань організації його діяльності	доводити до керівництва підрозділів недоліки у захисті інформації та пропозиції до їх усунення, пропозиції що удосконалення систем та комплексів захисту інформації тощо) **Е2.У2.** Готувати звернення (листи), заяви, звітно-аналітичні та інші 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.З1**. Основи комунікаційного менеджменту **Е3.З2**. Основи ділової етики **Е3.З3.** Порядок і типові вимоги до проведення ділових/комерційних перемовин **Е3.З4**. Порядок розроблення та виконання договірних робіт для зовнішніх партнерів	**Е3.У1.** Спілкуватися 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
		Е4. Здатність надавати консультативні послуги з питань	**Е4.З1.** Порядок і типові вимоги з надання консультативних послуг з питань технічного та криптографічного захисту **Е4.З2.** Предметну область	**Е4.У1.** Надавати консультативні послуги з питань технічного та криптографічного захисту інформації та кіберзахисту **Е4.У2.** Консультувати керівництво

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

				технічного та криптографічного захисту інформації та кіберзахисту щодо конкретних питань **Е4.У8.** Проводити інтерактивні тренінгові вправи для створення ефективного навчального середовища

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:

Головенко Андрій Валерійович, полковник, заступник директора Департаменту захисту інформації Адміністрації Держспецзв'язку; Воронов Віктор, провідний консультант Департаменту захисту інформації Адміністрації Держспецзв'язку України; 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; Головко Ярослав Володимирович, провідний консультант Департаменту захисту інформації Адміністрації Держспецзв'язку; Жилін Артем Вікторович, полковник, заступник начальника центру – начальник 6 управління Державного центру кіберзахисту Держспецзв'язку; Іванченко Євгенія Вікторівна, професор кафедри безпеки інформаційних технологій Національного авіаційного університету; Конюшок Сергій Миколайович, полковник, заступник начальника (з навчальної та 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, Київський національний університет 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 «Українська академія кібербезпеки»; Пазюк Андрій Валерійович, віце-президент Громадської організації «Українська академія кібербезпеки»; Педченко Євгеній Миколайович, керівник відділу впровадження 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

7.4. Дата внесення професійного стандарту до Реєстру професійних стандартів

7.5. Рекомендована дата наступного перегляду професійного стандарту

Вересень 2027 року.