Прим. № __

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 23 січня 2024 року № 38

ПРОФЕСІЙНИЙ СТАНДАРТ

ФАХІВЕЦЬ З ПЛАНУВАННЯ ПОЛІТИКИ ТА СТРАТЕГІЇ КІБЕРБЕЗПЕКИ

_____

(дата внесення до Реєстру кваліфікацій)

Професійний стандарт розроблено та затверджено згідно з вимогами статті 4^2 Кодексу законів про працю України на підставі:

висновку суб'єкта перевірки – Національного агентства кваліфікацій від 20 грудня 2023 року про дотримання під час підготовки проєкту професійного стандарту «Фахівець з планування політики та стратегії кібербезпеки» вимог Порядку розроблення, введення в дію та перегляду професійних стандартів, затвердженого постановою Кабінету Міністрів України від 31.05.2017 р. № 373;

висновку щодо погодження проєкту професійного стандарту «Фахівець з планування політики та стратегії кібербезпеки» Профспілкою працівників зв'язку України (лист від 16.11.2023 р. № 01.2-14/136, постанова Президії Профспілки працівників зв'язку України від 16.11.2023 р. № П-4-5г).

I. Назва професійного стандарту

Фахівець з планування політики та стратегії кібербезпеки.

II. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Планування, розробка, впровадження та супроводження, моніторинг політик, законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та кібербезпеки, а також надання освітніх, консультативних послуг та підтримання комунікації з зацікавленими сторонами в зазначеній сфері.

2. Назва виду (видів) економічної діяльності, секції, розділу, групи, класу економічної діяльності та їх код згідно з Національним класифікатором України ДК 009:2010 «Класифікація видів економічної діяльності»

Секція J	Інформація та телекомунікації	**Розділ 61**	Телекомунікації (електрозв'язок)	**Група 61.9**	Інша діяльність у сфері електрозв'язку
				Клас 61.90	Інша діяльність у сфері електрозв'язку
		Розділ 62	Комп'ютерне програмування, консультування та пов'язана з ними діяльність	**Група 62.0**	Комп'ютерне програмування, консультування та ними пов'язана з діяльність
				Клас 62.02	Консультування з питань інформатизації
				Клас 62.09	Інша діяльність у сфері інформаційних технологій і комп'ютерних систем
Секція M	Професійна, наукова та технічна діяльність	**Розділ 70**	Діяльність головних управлінь (хед-офісів); консультування з питань керування	**Група 70.2**	Консультування з питань керування
				Клас 70.22	Консультування з питань комерційної діяльності й керування
		Розділ 72	Наукові дослідження та розробки	**Група 72.1**	Дослідження й експерементальні розробки у сфері природничих і технічних наук

				Клас 72.19	Дослідження й експериментальні розробки у сфері природничих і технічних наук
		Розділ 74	Інша професійна, наукова та технічна діяльність	Група 74.9	Інша професійна, наукова та технічна діяльність, не введенні в інші угрупування
				Клас 74.90	Інша професійна, наукова та технічна діяльність, не введенні в інші угрупування

3. Назва (назви) професії (професій) та код (коди) підкласу (підкласів) (групи) професії згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій»

Фахівець з планування політики та стратегії кібербезпеки 2139.2.

4. Професійна (професійні) кваліфікація (кваліфікації), її (їх) рівень згідно з Національною рамкою кваліфікацій

Фахівець з планування політики та стратегії кібербезпеки, 7 рівень НРК;

Провідний фахівець з планування політики та стратегії кібербезпеки, 7 рівень НРК.

5. Назва (назви) документа (документів), що підтверджує (підтверджують) професійну кваліфікацію особи

● документ (диплом, сертифікат, тощо), виданий суб'єктом, уповноваженим законодавством на присвоєння/підтвердження та визнання професійної або часткової професійної кваліфікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у відповідності до професійного стандарту «Фахівець з планування політики та стратегії кібербезпеки»;

● документ (диплом, сертифікат, тощо), виданий суб'єктом, уповноваженим законодавством на присвоєння/підтвердження та визнання професійної або часткової професійної кваліфікації (щодо професійних кваліфікацій, здобутих у інших країнах).

ІІІ. Здобуття професійної кваліфікації та професійний розвиток

1. Здобуття професійної кваліфікації (назва професійної та/або часткової професійної кваліфікації; суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій)

Назва професійної та/або часткової професійної кваліфікації	**Суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
Фахівець з планування політики та стратегії кібербезпеки	Підготовка на другому рівні вищої освіти (магістерському) за спеціальностями, вказаними у **П.***, без вимог до стажу роботи.	*Не передбачено професійним стандартом*
Провідний фахівець з планування політики та стратегії кібербезпеки	Підготовка на другому рівні вищої освіти (магістерському) за спеціальностями, вказаними у **П.***, стаж роботи за однією з професій відповідного спрямування повинен складати не менше 2 років.	*Не передбачено професійним стандартом*

П.*

• Диплом на другому (магістерському) рівні вищої освіти за спеціальністю:

- 081 «Право» галузі знань «Право»;
- 111 «Математика» галузі знань 11 «Математика та статистика» (7 рівень НРК);
- 112 «Статистика» галузі знань 11 «Математика та статистика» (7 рівень НРК);
- 113 «Прикладна математика» галузі знань 11 «Математика та статистика» (7 рівень НРК);
- 121 «Інженерія програмного забезпечення» галузі знань 12 «Інформаційні технології» (7 рівень НРК);
- 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології» (7 рівень НРК);

- 123 «Комп’ютерна інженерія» галузі знань 12 «Інформаційні технології» (7 рівень НРК);

- 124 «Системний аналіз» галузі знань 12 «Інформаційні технології» (7 рівень НРК);

- 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» (7 рівень НРК);

- 126 «Інформаційні системи та технології» галузі знань 12 «Інформаційні технології» (7 рівень НРК);

- 171 «Електроніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (7 рівень НРК);

- 172 «Електронні комунікації та радіотехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (7 рівень НРК);

- 174 «Автоматизація, комп’ютерно-інтегровані технології та робототехніка» галузі знань, 17 «Електроніка, автоматизація та електронні комунікації» (7 рівень НРК);

- 251 «Державна безпека» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7 рівень НРК);

- 254 «Забезпечення військ (сил)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7 рівень НРК);

- 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7 рівень НРК);

- 257 «Управління інформаційною безпекою» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7 рівень НРК);

- 281 «Публічне управління та адміністрування» галузі знань 28 «Публічне управління та адміністрування» (7 рівень НРК).

2. Професійний розвиток

1) з присвоєнням наступної професійної кваліфікації

Назва професійної та/або часткової професійної кваліфікації	**Суб’єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій**	
	Кваліфікаційні центри	**Суб’єкти освітньої діяльності**
Фахівець з планування політики та стратегії кібербезпеки	Підвищення кваліфікації для отримання професійної кваліфікації "провідний фахівець з планування політики та стратегії кібербезпеки". Стаж роботи не менше двох років	*Не передбачено професійним стандартом*

2) без присвоєння наступної професійної кваліфікації

Підвищення кваліфікації може здійснюватися шляхом неформальної (тренінги, семінари, семінари-практикуми, вебінар, майстер-класи тощо) та інформальної освіти для вдосконалення (підтримання) професійної кваліфікації, в тому числі шляхом набуття нових/додаткових навичок/компетентностей.

Підтвердження наявної та підвищення професійної кваліфікації може бути передбачено відповідними відомчими нормативно-правовими актами та внутрішніми документами підприємств, установ та організацій.

IV. Абревіатури, скорочення

IT	Інформаційні технології
ПЗ	Програмне забезпечення
NIST	National Institute of Standards and Technology
ISO	International Organization for Standardization
ENISA	European Union Agency for Cybersecurity
BSI	British Standards Institution
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge
EBSCO	Elton Bryson Stephens Company
JSTOR	Journal Storage
VoIP	Voice over Internet Protocol
IM	Instant Messenger
DVB	Direct Video Broadcasts

V. Опис трудових функцій

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
A. Збір та аналіз даних для планування законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	**A1.** Здатність аналізувати, інтерпретувати, планувати, застосовувати вимоги чинних законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	**A1.З1.** Принципи забезпечення інформаційної та/або кібербезпеки, а також захисту персональних даних. **A1.З2.** Діючі закони, нормативно-правові акти парламенту, директиви президента, постанови і розпоряджень органів виконавчої влади та/або кодекс і процедури адміністративного /кримінального права етичних норм, та як вони пов'язані зі забезпеченням інформаційної та/або кібербезпеки, а також захистом персональних даних. **A3.З3.** Зміст та порядок адаптивного планування, планування в кризових умовах та з урахуванням обмеження часу. **A1.З4**. Галузеві показники, які є корисні для визначення тенденцій розвитку технологій	**A1.У1.** Оцінювати ефективність застосованих вимог чинних законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки. **A1.У2.** Здійснювати аналіз ризиків, техніко-економічне обґрунтування та/або компромісний аналіз для розробки, документування та уточнення функціональних вимог і специфікацій кібербезпеки. **A1.У3.** Розробляти і публікувати документи щодо управління безпекою ланцюжка постачання та управління ризиками. **A1.У4.** Моніторити і оцінювати можливий вплив виникаючих технологій на закони, нормативні акти та/або політики. **A1.У5.** Збирати точні та повні дані з джерел, які використовуються для розвідки, оцінювання та/або планування. **A1.У6.** Аналізувати кризові ситуації зі забезпечення. суспільної та персональної безпеки, а також захисту ресурсів **A1.У7.** Оцінювати дані розвідки для підтримки циклу планування.	**A1.К1.** Брати участь у семінарах, конференціях нарадах щодо планування змін до чинних та розробки нових законодавчих, нормативно-правових, організаційно-технічних документів інформаційної та/або кібербезпеки.	**A1.В1.** Формувати аналітичні довідки щодо чинних законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки. **A1.В2.** Формувати пропозиції щодо вдосконалення законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		інформаційної та/або кібербезпеки. **А1.35.** Фундаментальні кіберконцепції, принципи, обмеження і ефекти. **А1.36.** Фундаментальні концепції, термінології/лексикон, принципи, можливості, обмеження і ефекти кібероперацій. **А1.37.** Методики управління ризиками інформаційної та/або кібербезпеки в ланцюжку постачання. **А1.38.** Принципи забезпечення безперервності ведення бізнесу та планів відновлення після інциденту інформаційної та/або кібербезпеки.			
	А2. Здатність аналізувати, інтерпретувати, планувати, застосовувати вимоги (рекомендації) законодавчих, нормативно-	**А2.31.** Вимоги (рекомендації) кращих міжнародних практик (NIST, ISO, ENISA, BSI, MITRE ATT&CK тощо), законодавчих, нормативно-правових, організаційно-технічних	**А2.У1.** Інтерпретувати, планувати, застосовувати вимоги (рекомендації) законодавчих, нормативно-правових, організаційно-технічних кращих міжнародних практик у національні (державні) документи інформаційної та кібербезпеки. **А2.У2.** Інтерпретувати та/або затверджувати вимоги щодо	**А2.К1.** Формувати запити на отримання профільної інформації. **А2.К2.** Надавати предметні експертні знання та підтримку форумів з планування/форумам з розвитку і робочим групам належним чином.	**А2.В1.** Формувати аналітичні довідки щодо чинних міжнародних законодавчих, нормативно-правових,

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	правових, організаційно-технічних кращих міжнародних практик інформаційної та/або кібербезпеки.	заходів інформаційної та/або кібербезпеки. **А2.32.** Методики управління ризиками (методи оцінювання та оброблення ризиків). **А2.33.** Сучасні і перспективні кібертехнології. **А2.34.** Відповідні концепції, процедури, програмне забезпечення, обладнання і прикладні технологічні програми, які застосовуються для планування заходів інформаційної та/або кібербезпеки. **А2.35.** Нові/існуючі критерії стійкості та надійності організації. **А2.36.** Рекомендації з аналізу кризових ситуацій з метою забезпечення суспільної та персональної безпеки, захисту кіберресурсів, стійкості та надійності організації.	спроможностей інформаційної та/або кібербезпеки до нових інформаційних Технологій.	**А2.К3**. Брати участь у роботі груп, які створюють законодавчі, нормативно-правові, організаційно-технічні документи інформаційної та/або кібербезпеки.	організаційно-технічних заходів інформаційної та/або кібербезпеки. **А2.В2.** Формувати пропозиції щодо вдосконалення законодавчих, нормативно-правових, організаційно-технічних заходів. інформаційної та кібербезпеки.
	А3. Здатність аналізувати, інтерпретувати, планувати,	**А3.31.** Порядок аналізу потреби та вимог користувачів для	**А3.У1.** Планувати методики та формати інтеграції чинних законів, нормативних актів, міжнародних та зарубіжних практик у політику	**А3.К1**. Брати участь в аналізі політики інформаційної та/або кібербезпеки в організації.	**А3.В1.** Переглядати стандарти політики та

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	застосовувати технології та документи забезпечення інформаційної та/або кібербезпеки в організації.	планування архітектури інформаційної та/або кібербезпеки в організації. **А3.32.** Порядок аналізу потреби безпеки і вимог до програмного забезпечення для забезпечення інформаційної та/або кібербезпеки в організації. **А3.33.** Концепції і протоколи комп'ютерних мереж, а також методологію забезпечення безпеки мереж. **А3.34.** Нові та ті, що розробляються, технології інформаційної та/або кібербезпеки. **А3.35.** Сервісорієнтовані принципи архітектури інформаційної та/або кібербезпеки. **А3.36.** Зміст та функції відповідної інформаційної структури. **А3.37.** Концепції планування в організації. **А3.38.** Політику та конфігурацію	інформаційної та/або кібербезпеки організації. **А3.У2.** Визначати стратегії формування кіберспроможностей для розробки спеціального обладнання та програмного забезпечення з урахуванням потреб (вимог) місії. **А3.У3.** Аналізувати політику та конфігурації кіберзахисту організації та оцінювати відповідність документам організації. **А3.У4.** Аналізувати проєктні обмеження, компроміси та детальний проект системи інформаційної та/або кібербезпеки, а також підтримку життєвого циклу. **А3.У5.** Готувати рекомендації щодо можливих удосконалень і оновлень інформаційної та/або кібербезпеки. **А3.У6.** Рекомендувати нові або переглядати існуючі заходи безпеки, стійкості та надійності на основі результатів перевірок інформаційної та/або кібербезпеки. **А3.У7.** Визначати та інтегрувати середовища для поточних та майбутніх завдань стратегії кібербезпеки. **А3.У8.** Планувати проєктування та розроблення продуктів інформаційної та/або кібербезпеки.	**А3.К2**. Брати участь в аналізі потреби безпеки і вимог до програмного забезпечення з метою визначення доцільності проєкту з урахуванням часових і цінових обмежень, а також мандатів безпеки. **А3.К3**. Брати участь в аналізі результатів тестування програмного, апаратного забезпечення інформаційної та/або кібербезпеки. **А3.К4.** Брати участь у забезпеченні в організації постійної оптимізації інформаційної та/або кібербезпеки відповідно до розвитку ІТ.	стратегії їх впровадження, щоб забезпечити відповідність процедур/ настанов політикам інформаційної та/або кібербезпеки в організації. **А3.В2.** Розробляти групові політики та переліки контролю доступу для забезпечення відповідності стандартам організації, бізнес-правилам та потребам інформаційної та/або кібербезпеки в організації.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		інформаційної та/або кібербезпеки. **А3.З9.** Організацію діяльності щодо планування інформаційної та/або кібербезпеки, що ініційована в організації.			
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю планування; бібліотечні ресурси, архівні матеріали (за потреби); законодавчо-нормативні акти, акти роботодавця відповідного спрямування				
Б. Розроблення, впровадження законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	**Б1.** Здатність розробляти та впроваджувати законодавчі, нормативно-правові, організаційно-технічні заходи інформаційної та/або кібербезпеки.	**Б1.З1.** Заходи стратегій, політик, програм та планів з розвитку інформаційної та/або кібербезпеки. **Б1.З2.** Класифікацію кіберспроможностей (захист, атаки, експлуатація). **Б1.З3.** Порядок розроблення стратегій, політик, програм та планів інформаційної та/або кібербезпеки. **Б1.З4.** Вимоги до структури та змісту стратегій, програм та політик з розвитку інформаційної та/або кібербезпеки.	**Б1.У1.** Розробляти політику, плани і стратегії відповідно до законодавства, регуляторних актів, політик і стандартів інформаційної та/або кібербезпеки в організації. **Б1.У2.** Аналізувати вимоги та очікування керівників та персоналу, інших користувачів від запроваджених чи розроблюваних стратегій, програм та політик інформаційної та/або кібербезпеки. **Б1.У3.** Застосовувати у практичній діяльності вітчизняні, міжнародні та зарубіжні чинні та перспективні політики, стратегії розвитку інформаційної та/або кібербезпеки. **Б1.У4.** Розробляти стратегії оцінювання та обробки ризиків з метою усунення вразливостей та рекомендувати, за	**Б1.К1.** Брати участь у нарадах щодо розробки та впровадженні законодавчих, нормативно-правових, організаційно-технічні заходів інформаційної та/або кібербезпеки. **Б1.К2.** Планувати розроблення та приймати участь у розробленні, підтримці/супроводженні стратегічних планів організації з інформаційної та/або кібербезпеки. **Б1.К3.** Ураховувати в обґрунтованому обсязі вимоги керівництва організації під час періодичного перегляду та вдосконалення стратегій,	**Б1.В1.** Розробляти, впроваджувати, супроводжувати, законодавчі, нормативно правові організаційно-технічні заходи інформаційної та/або кібербезпеки. **Б1.В2.** Розробляти політику, програми та настанови відповідного спрямування для подальшого їх

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
			необхідності, зміни заходів безпеки у системі або системних компонентах. **Б1.У5.** Проєктувати архітектури та загальні принципи. забезпечення інформаційної та/або кібербезпеки. **Б1.У6.** Застосовувати принципи кібербезпеки і приватності при формуванні вимог організації (стосовно конфіденційності, цілісності, доступності, автентифікації і неспростовності). **Б1.У7.** Розробляти і підтримувати запобіжні антикризові заходи.	програм та політик зрозвитку інформаційної та/або кібербезпеки. **Б1.К4.** Брати участь в аналізі потреби та вимог користувачів для планування архітектури інформаційної та/або кібербезпеки.	впровадження в організації.
	Б2. Здатність впроваджувати технології та документи забезпечення інформаційної та/або кібербезпеки в організації узгоджену зі стратегічним планом організації.	**Б2.З1.** Теорію і практику стратегії організації. **Б2.З2.** Перспективні технології, які можуть бути використані в подальшому для забезпечення інформаційної та/або кібербезпеки. **Б2.З3**. Порядок розроблення планів аварійного відновлення та безперервності операцій для систем, що розробляються, та тестування систем до їхнього вводу в експлуатацію. **Б2.З4**. Застосовувати і дотримуватись чинних	**Б2.У1.** Готувати пропозиції щодо пошуку та управління необхідними ресурсами, включаючи фінансові, для забезпечення безперервності дії політик та стратегій, програм з розвитку інформаційної та/або кібербезпеки організацій. **Б2.У2.** Готувати пропозиції щодо пошуку та управління необхідними ресурсами, включаючи підтримку керівництва, фінансові ресурси та ключовий персонал з питань безпеки для сприяння планування та досягнення цілей завдань інформаційної та/або кібербезпеки для зниження загального ризику організації. **Б2.У3.** Адаптувати технічну інформацію для планування до рівня	**Б2.К1.** Задіювати кращі практики і отримані приклади зовнішніх організацій і освітніх закладів, які переймаються питаннями інцидентів інформаційної та/або кібербезпеки. **Б2.К2.** Сприяти обізнаності керівництва стосовно інформаційної та/або кіберполітики і стратегії та забезпечити відображення обґрунтованих принципів в місії, концепції і цілях організації. **Б2.К3**. Розробляти або брати участь у розробленні стратегій, програм та політик з розвитку	**Б2.В1.** Визначати та/або впроваджувати політики і процедури, щоб забезпечити належний захист критичної інфраструктури. **Б2.В2.** Інтерпретувати та застосовувати закони, нормативні акти, політики, стандарти чи процедури до конкретних питань інформаційної

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		статутів, законів, нормативних документів і політик.	розуміння користувача/споживача/замовника **Б2.У4.** Розробляти профільні плани інформаційної та/або кібербезпеки організації та готувати відповідну кореспонденцію **Б2.У5.** Планувати розроблення детальної проєктної документації з безпеки для специфікацій компонентів та інтерфейсів з метою підтримки проєкту та розроблення системи. **Б2.У6.** Планувати розроблення планів аварійного відновлення та безперервності операцій для систем, що розробляються, та тестування систем до їхнього вводу у продуктивне середовище. **Б2.У7.** Вирішувати конфлікти у законодавстві, нормативних актах політиках, стандартах і процедурах. **Б2.У8.** Застосовувати сервіс-орієнтовані принципи архітектури інформаційної та/або кібербезпеки, щоб задовольнити вимоги конфіденційності, цілісності та доступності організації.	інформаційної та/або кібербезпеки. **Б2.К4.** Брати участь в організації процесів планування, включаючи підготовку функціональних і спеціальних планів підтримки, підготовки і забезпечення ділового листування, а також процесів кадрового забезпечення.	та/або кібербезпеки.
	Б3. Здатність підтримувати керівника ІТ у формуванні політики та стратегій	**Б3.З1.** Стан інформаційної та/або кібербезпеки в організації. **Б3.З2.** Принципи і методики управління	**Б3.У1.** Оцінювати та консультувати вище керівництво щодо рівня ризику та, урахування при планування заходів політик, стратегій і програм стосовно його зниження.	**Б3.К1.** Надавати керівництву пояснення щодо програми розвитку інформаційної та/або кібербезпеки в організації.	**Б3.В1.** Консультувати відповідне вище керівництво або уповноважених представників

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	інформаційної та/або кібербезпеки.	програмами та проєктами з інформаційної та/або кібербезпеки. **Б3.З3.** Типи оперативного планування. **Б3.З4.** Прийняті в організації правила класифікації інформації щодо рівнів захисту і процедур доступу до неї. **Б3.З5.** Посадові завдання та обов'язки внутрішнього консультанта/радника за профільними спеціалізаціями в своїй експертній області.	**Б3.У2.** Розробляти вказівки і настанови для працівників, залучених до розроблення стратегій, програм та політик з розвитку інформаційної та/або кібербезпеки.	**Б3.К2.** Консультувати вище керівництво щодо аналізу витрат/вигоди програм, політик, процесів, систем та елементів інформаційної та/або кібербезпеки, та щодо змін, які впливають на стан інформаційної та/або кібербезпеки в організації.	щодо змін, які впливають на стан інформаційної та/або кібербезпеки в організації.
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю планування; бібліотечні ресурси, архівні матеріали (за потреби); профільна наукова, методична література; законодавчо-нормативні акти, акти роботодавця відповідного спрямування.				
В. Супроводження процесів впровадження законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної	**В1.** Здатність супроводжувати нормативно-правові заходи інформаційної та/або кібербезпеки.	**В1.З1.** Порядок створення нормативно-правових заходів інформаційної та/або кібербезпеки. **В1.З2.** Порядок проходження (затвердження) нормативно-правових актів інформаційної та/або кібербезпеки.	**В1.У1.** Ідентифікувати та проводити аналіз цільових комунікацій з метою визначення інформації, необхідної для забезпечення і проведення операцій. **В1.У2.** Інтерпретувати і застосовувати закони, нормативні акти, політики та методології, що стосуються кіберцілей організації.	**В1.К1.** Отримувати і підтримувати робочі знання з конституційних питань, які виникають у відповідних законах, нормативних актах, політиках, угодах, стандартах, процедурах чи інших публікаціях.	**В1.В1.** Інтерпретувати і застосовувати діючі закони, статути та нормативні документи та інтегрувати їх в політику організації. **В1.В2.** Оцінювати вплив

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
та/або кібербезпеки.		**В1.З3.** Принципи діяльності щодо правотворчості. **В1.З4.** Правові, нормативні та законодавчі вимоги інформаційної та/або кібербезпеки. **В1.З5.** Сучасні/ перспективні технологій комунікації.			змін у законодавстві, нормативних актах, політиках, стандартах або процедурах.
	В2. Здатність супроводжувати ~~в~~провадження організаційно-технічних заходів інформаційної та/або кібербезпеки.	**В2.З1.** Структуру та зміст специфічних планів, настанов і повноважень, прийнятих в організації. **В2.З2.** Порядок оцінювання проектів систем інформаційної та/або кібербезпеки.	**В2.У1.** Оцінювати адекватність проектів інформаційної та/або кібербезпеки **В2.У2.** Збирати і доопрацьовувати вимоги до системи безпеки та забезпечувати ефективну інтеграцію таких вимог в складові продукти і системи через цілеспрямовану безпечну архітектуру, проектування, розробку і налаштування **В2.У3.** Аналізувати проектні обмеження, компроміси, та деталі проектування системи інформаційної та/або кібербезпеки	**В2.К1.** Координувати свої дії із системними архітекторами та розробниками, якщо це необхідно, з метою забезпечення нагляду за розробкою проектних рішень.	**В2.В1.** Готувати настанови із застосування законодавства, нормативних актів, стандартів і процедур для керівництва, персоналу або клієнтів
	В3. Здатність розробляти проєкти з розвитку інформаційної та/або кібербезпеки, ознайомлювати персонал і	**В3.З1.** Корпоративні цілі і завдання, пов’язані з використанням інформаційних технологій в організації. **В3.З2.** Інструменти, методи і методики проєктування систем, включаючи	**В3.У1.** Визначати масштаб проекту та цілі відповідно до вимог замовника. **В3.У2.** Розробляти групові політики та переліки контролю доступу для забезпечення відповідності стандартам організації, бізнес-правилам та потребам.	**В3.К1.** Надавати (доводити до відома) технічну інформацію різним категоріям користувачів. **В3.К2.** Встановлювати ефективний зворотній зв’язок з користувачами профільних послуг та партнерами.	**В3.В1.** Писати та публікувати методики та настанови з кіберзахисту, а також звіти про виявлення інцидентів для

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	публікувати політику. інформаційної та/або кібербезпеки.	автоматизовані системи аналізу і інструменти проектування. **В3.З3.** Засоби, методи і способи проєктування систем безпеки. **В3.З4.** Порядок розроблення технічної документації відповідного спрямування.	**В3.У3.** Розробляти та документувати вимоги, властивості та обмеження для процедур проектування та процесів. **В3.У4.** Забезпечувати, щоб діяльність з проектування та розвитку кібербезпеки (з наданням функціонального опису впровадження безпеки) була належним чином задокументована і оновлювалася за необхідності.		відповідної аудиторії. **В3.В2.** Сприяти впровадженню нових або переглянутих законів, нормативних актів, керівних документів, розпоряджень, політик, стандартів або процедур.
	В4. Здатність надавати керівництву, персоналу і користувачам консультації застосування на практиці методології щодо забезпечення інформаційної та/або кібербезпеки.	**В4.З1.** Підходи до управління ризиком ланцюжка постачання. **В4.З2.** Положення використовуваної в організації програми класифікації інформації і процедур її розкриття.	**В4.У1.** Застосовувати концепції, процедури, програмне забезпечення, обладнання та/або технологічні прикладні програми під час надання консультацій із застосування на практиці методології щодо політики інформаційної та/або кібербезпеки. **В4.У2.** Готувати та проводити брифінги з обізнаності, дотримання норм та положень стратегій, політик і програм з розвитку інформаційної та/або кібербезпеки.	**В4.К1.** Сприяти дискусіям у невеликих групах.	**В4.В1.** Приймати участь у розробленні методології кібербезпеки організації та управління ризиком ланцюжка постачання для розробки безперервності операційних планів.
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повно-текстових наукових журналів (EBSCO, JSTOR) відповідно до профілю планування; бібліотечні ресурси, архівні матеріали (за потреби); законодавчо-нормативні акти, акти роботодавця відповідного спрямування				

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
Г. Моніторинг впроваджених законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	**Г1.** Здатність моніторити виконання політик, принципів і практик при наданні послуг з планування та управління політикою інформаційної та/або кібербезпеки.	**Г1.З1.** Методи соціальної інженерії **Г1.З2.** Сучасні галузеві методи оцінки, впровадження та розповсюдження інструментів та процедур оцінки безпеки інформаційних технологій, моніторингу, виявлення та усунення несправностей, що використовують концепції та можливості на основі стандартів. **Г1.З3.** Підходи та методи до розроблення і верифікації критеріїв оцінювання працівників щодо реалізації заходів стратегій, політик та програм з розвитку кіберзахисту. **Г1.З4.** Методи та процеси тестування і оцінювання працівників щодо реалізації заходів стратегій, політик та програм з розвитку кіберзахисту.	**Г1.У1.** Розробляти методи моніторингу та оцінки ризиків, відповідності та зусиль щодо надання впевненості у результативності заходів стратегій, політик, програм та планів. **Г1.У2.** Відслідковувати результати аудиту та розробляти рекомендації, щоб забезпечити вжиття відповідних заходів щодо зменшення ризиків. **Г1.У3.** Підтримувати та сприяти безперервному моніторингу в організації стосовно планування стратегій, політик, програм та планів з розвитку кіберзахисту. **Г1.У4.** Визначати вимоги до звітності для підтримки діяльності з профільного безперервного моніторингу. **Г1.У5.** Брати участь у формуванні системи критеріїв та показників для оцінки ефективності програми профільного безперервного моніторингу. **Г1.У6**. Розробляти критерії оцінювання працівників щодо реалізації заходів стратегій, політик та програм з розвитку кіберзахисту. **Г1.У7.** Здійснювати аналіз законодавства і готувати проєкти рішень для генеральних інспекторів, уповноважених працівників з захисту даних, нагляду і перевірки	**Г1.К1.** Рекомендувати керівництву кандидатури працівників до відповідних робочих груп безперервного профільного моніторингу. **Г1.К2.** Брати участь у розробленні правил оцінювання працівників щодо реалізації заходів стратегій, політик та програм з розвитку кіберзахисту. **Г1.К3.** Розробляти тести для визначення рівня обізнаності та участі працівників щодо реалізації заходів стратегій, політик та програм з розвитку кіберзахисту.	**Г1.В1.** Оцінювати витрати-вигоду, економічний аналіз та аналіз ризиків у процесі прийняття рішень. **Г1.В2.** Оцінювати ефективність законів, правил, політик, стандартів чи процедур відповідного спрямування.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
			дотримання персоналом відповідних вимог політик, законів і нормативних актів у сфері інформаційної та/або кібербезпеки. **Г1.У8.** Рекомендувати нові або переглядати існуючі заходи безпеки, стійкості та надійності на основі результатів перевірок.		
	Г2. Здатність брати участь в аудитах інформаційної та/або кібербезпеки.	**Г2.З1.** Класифікацію методів оцінювання та процедуру їх застосування на практиці. **Г2.З2.** Процедури аудиту та «логування» (включаючи серверне «логування»). **Г2.З3.** Сучасні галузеві методи оцінки, впровадження та розповсюдження інструментів та процедур оцінки безпеки ІТ, моніторингу, виявлення та усунення несправностей, що використовують концепції та можливості на основі стандартів.	**Г2.У1.** Визначати важливість матеріалів аудиту та безпеки комунікацій. **Г2.У2.** Оцінювати ефективність заходів з інформаційної та/або кібербезпеки, які використовуються системою (системами). **Г2.У3.** Проводити аудити або огляди технічних систем **Г2.У4.** Оцінювати контракти з метою забезпечення відповідності фінансовим, юридичним та програмним вимогам. **Г2.У5.** Оцінювати загрози та вразливості комп’ютерної системи (систем) для розробки профілю ризику безпеки.	**Г2.К1.** Розробляти спільно з групою зовнішнього аудиту процедури обміну інформацією стосовно програми безперервного моніторингу, та її впливу на оцінку контролів безпеки. **Г2.К2.** Оглядати, здійснювати або брати участь спільно з групою зовнішнього аудиту в аудитах кіберпрограм і кіберпроектів.	**Г2.В1.** Розробляти і управляти процедурами перевірки і аудиту постачальників на предмет їх відповідності вимогам політик приватності і безпеки даних та вимогам законодавства. **Г2.В2.** Переглядати або здійснювати аудит програм та проєктів з ІТ. **Г2.В3.** Розробляти програму внутрішнього аудиту захисту

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
					персональних даних. **Г2.В4.** Готувати звітні документи з аудиторської перевірки, які містять технічні та процедурні висновки, а також рекомендувати коригування стратегій/рішень.
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повно-текстових наукових журналів (EBSCO, JSTOR) відповідно до профілю планування; бібліотечні ресурси, архівні матеріали (за потреби); законодавчо-нормативні акти, акти роботодавця відповідного спрямування				
Д. Підтримання комунікації із зацікавленими сторонами для врахування їх пропозицій при плануванні законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної	**Д1.** Здатність брати участь у відомчих і міжвідомчих нарадах з питань формування політики та стратегії розвитку інформаційної та/або кібербезпеки.	**Д1.З1.** Основні бізнес-процеси і місію організації. **Д1.З2.** Технологічні задачі і завдання управління та лідерства, пов'язані з організаційними процесами, механізми вирішення проблем. **Д1.З3.** Види доведення інформації (асимілятивний, слуховий, кінестетичний).	**Д1.У1.** Переглядати існуючі та перспективні політики із зацікавленими сторонами. **Д1.У2.** Оцінювати потреби в політиці та співпрацювати із зацікавленими сторонами з метою розробки політик корпоративного управління діяльністю в сфері кібербезпеки. **Д1.У3.** Встановлювати та підтримувати канали зв'язку з зацікавленими сторонами. **Д1.У4.** Ідентифікувати та проводити аналіз цільових комунікацій з метою визначення інформації, необхідної	**Д1.К1.** Комунікувати з керівниками різних рівнів (міжособистісне спілкування, доступність, уміння ефективно сприймати мову виступаючих, відповідно до аудиторії коректувати стиль і мову виступу). **Д1.К2.** Взаємодіяти із зовнішніми організаціями, зокрема закладами освіти та науковими установами, діяльність яких спрямована на дослідження	**Д1.В1.** Виконувати обов'язки внутрішнього консультанта/ радника в сфері планування заходів з розвитку інформаційної та/або кібербезпеки в організації **Д1.В2.** Готувати та проводити

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
та/або кібербезпеки.			для забезпечення і проведення операцій.	кіберпростору (наприклад, з програмами з кібербезпеки/тренінгами, та дослідженнями та розробками).	брифінги відповідного спрямування. **Д1.В3.** Співпрацювати із заінтересованими сторонами з метою забезпечення безперервної діяльності організації в рамках програми, стратегії та виконання завдань.
	Д2. Здатність оцінювати потреби в політиці та співпрацювати із зацікавленими сторонами з метою розроблення політик корпоративного управління діяльністю в сфері інформаційної та/або кібербезпеки.	**Д2.З1.** Методи та процедури прогнозування потреб у послугах з інформаційної та/або кібербезпеки. **Д2.З2.** Можливості і обмеження внутрішніх і зовнішніх організацій-партнерів. **Д2.З3.** Результати звітів внутрішніх і зовнішніх організацій-партнерів щодо інформаційної та/або кібербезпеки. **Д2.З4.** Внутрішню та зовнішню практику прогнозування і/або	**Д2.У1.** Прогнозувати спільно зі заінтересованими сторонами поточні потреби у послугах та забезпечувати, що припущення щодо безпеки переглядаються за необхідності. **Д2.У2.** Застосувати спільно із заінтересованими сторонами принципи забезпечення безпеки інформації – збереження конфіденційності, цілісності та доступності.	**Д2.К1.** Співпрацювати із заінтересованими сторонами, щоб визначити та/або розробити відповідні технології прийняття рішень. **Д2.К2.** Визначати спільно із заінтересованими сторонами та/або впроваджувати політики і процедури, щоб забезпечити належний захист критичної інфраструктури.	**Д2.В1.** Розвивати розуміння потреб та вимог кінцевих користувачів інформації.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		моделювання спроможностей та дій загроз. **Д2.З5.** Політику організації і концепції планування її співпраці з внутрішніми і/або зовнішніми організаціями.			
	Д3. Здатність знаходити консенсус із зацікавленими сторонами щодо запропонованих змін кіберполітики.	**Д3.З1.** Зовнішні організації і установи, діяльність яких спрямована на розвиток, захист та дослідження кіберпростору. **Д3.З2.** Нормативні документи і правила, що забезпечують планування, проєктування, розроблення та моніторинг політик, стратегій та програм із кіберзахисту організації. **Д3.З3.** Новітні технології, інструменти, процедури, методи та процеси відповідного спрямування. **Д3.З4.** Повноваження організації і організації-партнера, відповідальність та	**Д3.У1.** Проводити заходи з довгострокового стратегічного планування за участю внутрішніх і зовнішніх партнерів з інформаційної та/або кібердіяльності. **Д3.У2.** Пропонувати політику взаємодії, яка регулює взаємодію із зовнішніми групами координації.	**Д3.К1.** Розробляти, підтримувати, і оцінювати угоди із зовнішніми партнерами з питань взаємодії в сфері інформаційної та/або кібербезпеки. **Д3.К2.** Пропонувати політику взаємодії, яка регулює взаємодію із зовнішніми групами координації.	**Д3.В1.** Визначати та управляти пріоритетами в області забезпечення безпеки при взаємодії з зовнішніми партнерами.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		внески у досягнення поставлених цілей. **Д3.35.** Політику, засоби, спроможності і процедури своєї організації та організації-партнерів.			
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повно-текстових наукових журналів (EBSCO, JSTOR) відповідно до профілю планування; бібліотечні ресурси, архівні матеріали (за потреби); законодавчо-нормативні акти, акти роботодавця відповідного спрямування.				
Е. Надання освітніх та консультативних послуг щодо законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	**Е1.** Здатність розробляти навчально-методичні та консультативні матеріали щодо законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	**Е1.З1.** Технології виробництва, комунікації та розповсюдження медійних повідомлень, а також альтернативні способи інформування за допомогою текстових, мовних, візуальних повідомлень. **Е1.З2.** Відповідні концепції, процедури, програмне забезпечення, обладнання і прикладні технологічні програми, які застосовуються для навчання. **Е1.З3.** Вимоги до структури змісту та підходи до розроблення навчально-методичних та консультативних матеріалів.	**Е1.У1.** Розробляти нові або визначати існуючі матеріали для навчання та тренінгів, для цільових аудиторій. **Е1.У2.** Обґрунтувати зв'язок навчальної програми для тренінгів на робочому місці зі стратегією розвитку організації у сфері інформаційної та/або кібербезпеки. **Е1.У3.** Редагувати зміст навчальної програми для тренінгів на робочому місці відповідно до їх оновлення та встановлених часових вимог. **Е1.У4.** Адаптувати навчальну програму для тренінгу на робочому місці відповідно до його оновлення та встановлених часових вимог. **Е1.У5.** Розробляти або брати участь у розробці завдань, планів і програм для курсів/тренінгів на робочому місці.	**Е1.К1.** Розробляти або брати участь у розробленні індивідуальних/колективних планів розвитку, навчання та/або вдосконалення результатів навчання. **Е1.К2.** Формувати вартість запланованих освітніх ресурсів у сфері кібербезпеки зацікавленим сторонам на всіх рівнях організації. **Е1.К3.** Розробляти або брати участь у розробці комп'ютерних навчальних модулів або курсів. **Е1.К4.** Брати участь, за необхідності, у процесі планування закупівлі освітніх послуг, дотримуючись відповідних	**Е1.В1.** Розробляти або брати участь у розробці індивідуальних/ колективних планів розвитку, навчання і/або вдосконалення результатів навчання. **Е1.В2.** Забезпечити, що політика і процеси управління кіберперсоналом відповідають юридичним вимогам та вимогам організації щодо

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		Е1.З4. Сучасні підходи до формування навчально-методичних та консультативних матеріалів. **Е1.З5.** Принципи і методи навчання та надання консультацій для розробки навчальних програм, навчання та інструктажів для окремих осіб та груп. **Е1.З6.** Зміст навчальної програми для тренінгів на робочому місці. **Е1.З7.** Матеріали інструкцій (стандартні операційні процедури, технологічний посібник тощо) для надання детальних вказівок відповідним працівникам. **Е1.З8.** Технічну документацію відповідного спрямування. **Е1.З9.** Методи та підходи щодо переглядів та/чи вдосконалення навчальних планів і програм.	**Е1.У6.** Розробляти рекомендації щодо редагування навчальних планів і матеріалів. **Е1.У7.** Готувати матеріали інструкцій (стандартні операційні процедури, технологічний посібник тощо) для надання детальних настанов для відповідної частини персоналу. **Е1.У8.** Розробляти технічну документацію відповідного спрямування . **Е1.У9.** Інтегрувати нові наукові ідеї та підходи у зміст навчальних програм в необхідних обсягах і формах. **Е1.У10.** Аналізувати вимоги та очікування слухачів, їх роботодавців та інших заінтересованих осіб щодо навчальної програми/тренінгу чи курсу. **Е1.У11.** Ураховувати в обґрунтованому обсязі вимоги керівництва організації під час періодичного перегляду та вдосконалення навчальних планів, програм. **Е1.У12.** Складати плани щодо поточних потреб в освітніх послугах та забезпечувати перегляд припущень щодо забезпечення кібербезпеки за необхідності.	практик управління ризиків в ланцюжку постачання.	рівних можливостей, різноманіття і справедливим практикам найму/ працевлаштування.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		Е1.З10.Вимоги до системи забезпечення якості. **Е1.З11.** Основні небезпеки, ризики і вразливості.			
	Е2. Здатність проведення навчання, тренінгів, консультацій щодо законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	**Е2.З1.** Зміст навчальної програми відповідного спрямування. **Е2.З2.** Особливості організації освітнього процесу для різних форм набуття компетентності. **Е2.З3.** Форми організації освітнього процесу. **Е2.З4.** Сучасні методи, засоби та технології викладання. **Е2.З5.** Методи і способи організації індивідуальної та групової роботи слухачів під час навчання. **Е2.З6.** Освітні комп'ютерні послуги і послуги дистанційної освіти. **Е2.З7.** Методи і технології підготовки доповідей та презентацій. **Е2.З8**. Методи і способи ефективної комунікації.	**Е2.У1.** Готувати матеріали інструкцій (стандартні операційні процедури, технологічний посібник тощо) для надання. детальних настанов для відповідної частини персоналу **Е2.У4.** Оцінювати тренінгову документацію (наприклад, документи курсу, плани занять, студентські роботи, екзамени, графіки навчання, описи курсів тощо). **Е2.У5.** Використовувати сучасні та новітні технології у навчальних цілях (інтерактивні дошки, Web-сайти, комп'ютери, проектори тощо). **Е1.У9.** Інтегрувати нові наукові ідеї та підходи у зміст навчальних програм в необхідних обсягах і формах. **Е1.У11.** Ураховувати в обґрунтованому обсязі вимоги керівництва організації під час періодичного перегляду та вдосконалення навчальних планів, програм.	**Е2.К1.** Керувати різними системами і методами електронної комунікації (наприклад, електронна пошта, VoIP, IM, Web-форуми, DVB). **Е2.К2.** Аналізувати вимоги та очікування слухачів, їх роботодавців та інших заінтересованих осіб щодо навчальної програми/тренінгу чи курсу. **Е2.К3.** Встановлювати ефективний зворотний зв'язок з аудиторією з метою вдосконалення навчання.	**Е2.В1.** Планувати, проводити навчання, тренінги, консультації, оцінювати їх ефективність.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	Е3. Здатність оцінювати результати наданих освітніх та консультативних послуг щодо законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки.	**Е3.З1.** Методики оцінювання результатів навчання (рубрики, плани оцінювання, тестування, вікторини). **Е3.З2.** Методи та процеси тестування і оцінювання слухачів. **Е3.З3.** Порядок та методи оцінювання результатів навчання **Е3.З4.** Підходи та методи до розроблення і верифікації критеріїв оцінювання результатів навчання. **Е3.З5.** Вимоги і правила дотримання академічної доброчесності. **Е3.З6.** Джерела і методи збору інформації, її узагальнення, структурування, систематизацію. **Е3.З7.** Нормативні документи і правила, що забезпечують захист авторських прав, патентування, винаходи тощо. **Б3.З4.** Прийняті в організації правила класифікації інформації	**Е3.У1.** Розробляти письмові тести для визначення рівня професійної придатності та оцінювання кваліфікації слухачів. **Е3.У2**. Розробляти критерії оцінювання результатів навчання. **Е3.У3.** Виконувати обов'язки консультанта/радника в технічній сфері та галузі авторського права щодо електронних носіїв інформації тощо. **Е3.У4**. Готувати та проводити брифінги відповідного спрямування. **Е3.У5**. Переглянути /оцінити ефективність кіберперсоналу для коригування навичок та/або стандартів кваліфікації. **Е3.У6.** Застосувати принципи забезпечення безпеки інформації – збереження конфіденційності, цілісності та доступності. **Е3.У7.** Розробляти або брати участь у розробці матеріалів для тренінгів щодо забезпечення конфіденційності персональних даних та кібербезпеки. **Е3.У8.** Освоювати досягнення у технологіях захисту інформації для забезпечення їх впровадження у відповідній організації.	**Е3.К1.** Брати участь у розробленні внутрішніх регламентів з присвоєння/присудження кваліфікацій слухачам. **Е3.К2**. Брати участь у розробленні правил оцінювання результатів навчання. **Е3.К3.** Розробляти або брати участь у розробці стандартів оцінювання здобувачів та присвоєння/присудження кваліфікацій слухачам. **Е3.К4.** Брати участь в оцінюванні результатів навчання та присвоєнні/присудженні професійних/освітніх кваліфікацій слухачам.	**Е3.В1.** Аналізувати та звітувати перед керівництвом про користування активами і ресурсами управління знаннями.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		щодо рівнів захисту і процедур доступу до неї. **Г2.31.** Класифікацію методів оцінювання та процедуру їх застосування на практиці.			
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повно-текстових наукових журналів (EBSCO, JSTOR) відповідно до профілю планування; бібліотечні ресурси, архівні матеріали (за потреби); законодавчо-нормативні акти, акти роботодавця відповідного спрямування.			

VI. Розподіл трудових функцій та компетентностей за професійними кваліфікаціями

Трудова функція (умовне позначення)	Загальна назва професійної кваліфікації у межах професійного стандарту: Фахівець з планування політики та стратегії кібербезпеки	
	Фахівець з планування політики та стратегії кібербезпеки	Провідний фахівець з планування політики та стратегії кібербезпеки
	повна	повна
А	+	+
Б	+	+
В	+	+
Г	+	+
Д	+	+
Е	-	+

VII. Відомості про розроблення та затвердження професійного стандарту

1. Повне найменування розробника професійного стандарту

Адміністрація Державної служби спеціального зв'язку та захисту інформації України.

Склад робочої групи/Учасники робочої групи:

Бакалинський Олександр Олегович, заступник директора департаменту-начальник 2 відділу Департаменту кіберзахисту Адміністрації Держспецзв'язку;

Безштанько Віталій Михайлович, головний спеціаліст 5 відділу Департаменту кіберзахисту Адміністрації Держспецзв'язку;

Бондаренко Іван Дмитрович, доцент кафедри кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України;

Гахов Сергій Олександрович, доцент кафедри інформаційної та кібернетичної безпеки, Навчально-науковий інститут захисту інформації, Державний університет телекомунікацій;

Даков Сергій Юрійович, провідний науковий співробітник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

Дідик Валерія Анатоліївна, керівник напряму з розвитку професійних навичок з кібербезпеки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»;

Дідусенко Світлана Миколаївна, начальник відділу управління освітньої діяльності Департаменту освіти, науки та спорту Міністерства внутрішніх справ України;

Котетунов Віктор Юрійович, провідний науковий співробітник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

Лазарько Артем Анатолійович, заступник начальника відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

Ліпінський Вадим Володимирович, провідний фахівець сфери захисту інформації відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

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

Мазур Наталя Володимирівна, голова Профспілки працівників зв'язку України;

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

Мельник Сергій Вікторович, консультант напряму з розвитку професійних навичок з кібербезпеки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»;

Мохор Володимир Володимирович, директор Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України;

Олексюк Лілія Віталіївна, голова Громадської організації «Всеукраїнська асоціація «Інформаційна безпека та інформаційні технології»;

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

Толюпа Сергій Васильович, професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка;

Трегубенко Ірина Борисівна, провідний науковий співробітник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

Штомпель Тетяна Миколаївна, віцепрезидент компанії ТОВ «ТЕКЕКСПЕРТ», керівник навчального Центру «Мережні технології»;

Шестаков Валерій Іванович, заступник директора (з навчальної та наукової роботи) Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України;

Харченко В'ячеслав Сергійович, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Жуковського;

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

2. Назва та реквізити документа, яким затверджено професійний стандарт

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23 січня 2024 року № 38.

3. Реквізити висновку суб'єкта перевірки про дотримання вимог Порядку розроблення, введення в дію та перегляду професійних стандартів під час підготовки проєкту професійного стандарту

Висновок суб'єкта перевірки Національного агентства кваліфікацій від 20 грудня 2023 року про дотримання під час підготовки проєкту професійного стандарту «Фахівець з планування політики та стратегії кібербезпеки» вимог Порядку розроблення, введення в дію та перегляду професійних стандартів, затвердженого постановою Кабінету Міністрів України від 31.05.2017 р. № 373).

4. Реквізити висновку репрезентативних всеукраїнських об'єднань професійних спілок на галузевому рівні про погодження проєкту професійного стандарту

Висновок щодо погодження проєкту професійного стандарту «Фахівець з планування політики та стратегії кібербезпеки» Профспілкою працівників зв'язку України (лист від 16.11.2023 р. № 01.2-14/136, постанова Президії ЦК Профспілки працівників зв'язку України від 16.11.2023 р. № П-4-5г).

VIII. Дата внесення професійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.

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