Проєкт

Професійний стандарт

ФАХІВЕЦЬ З ПЛАНУВАННЯ ПОЛІТИКИ ТА СТРАТЕГІЇ КІБЕРБЕЗПЕКИ

_____(дата внесення до Реєстру кваліфікацій)

ЗАТВЕРДЖЕНО:
Адміністрацією Державної служби спеціального зв'язку та захисту інформації України наказ від _____№_____

Професійний стандарт розроблено та затверджено згідно з вимогами статті 42 Кодексу законів про працю України на підставі:

- висновку суб'єкта перевірки – Національного агентства кваліфікацій від _____ про дотримання під час підготовки проєкту професійного стандарту вимог Порядку розроблення, введення в дію та перегляду професійних стандартів, затвердженого постановою Кабінету Міністрів України від 31.05.2017 р. № 373;
- висновку Профспілки працівників зв'язку України від _____ щодо погодження проєкту професійного стандарту

І. Назва професійного стандарту

Фахівець з планування політики та стратегії кібербезпеки

ІІ. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Надання освітніх, консультативних та методичних послуг у сфері планування політики та стратегії інформаційної безпеки та кібербезпеки.

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 61.1**	Діяльність у сфері проводового електрозв'язку
				Клас 61.10	Діяльність у сфері проводового електрозв'язку
				Група 61.2	Діяльність у сфері безпроводового електрозв'язку
				Клас 61.20	Діяльність у сфері безпроводового електрозв'язку
				Група 61.3	Діяльність у сфері супутникового електрозв'язку
				Клас 61.30	Діяльність у сфері супутникового електрозв'язку
				Група 61.9	Інша діяльність у сфері електрозв'язку
				Клас 61.90	Інша діяльність у сфері електрозв'язку
		Розділ 62	Комп'ютерне програмування, консультування та пов'язана з ними діяльність	**Група 62.0**	Комп'ютерне програмування, консультування та пов'язана з ними діяльність
				Клас 62.01	Комп'ютерне програмування
				Клас 62.02	Консультування з питань інформатизації

				Клас 62.03	Діяльність із керування комп'ютерним устаткуванням
				Клас 62.09	Інша діяльність у сфері інформаційних технологій і комп'ютерних систем
		Розділ 63	Надання інформаційних послуг	**Група 63.1**	Оброблення даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність; веб-портали
				Клас 63.11	Оброблення даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність
				Клас 63.12	Веб-портали
Секція M	Професійна, наукова та технічна діяльність	**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
Секція P	Освіта	**Розділ 85**	Освіта	**Група 85.5**	Інші види освіти
				Клас 85.59	Інші види освіти, не введенні в інші угрупування

3. Назва професії та код підкласу професії згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій»

Фахівець з планування політики та стратегії кібербезпеки 2139.2

4. Професійна кваліфікація, її рівень згідно з Національною рамкою кваліфікацій (НРК)

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

- диплом на другому (магістерському) рівні вищої освіти за спеціальністю:

- 121 «Інженерія програмного забезпечення» галузі знань «Інформаційні технології» (7 рівень НРК);
- 122 «Комп'ютерні науки» галузі знань «Інформаційні технології» (7 рівень НРК);
- 123 «Комп'ютерна інженерія» галузі знань «Інформаційні технології» (7 рівень НРК);
- 124 «Системний аналіз» галузі знань «Інформаційні технології» (7 рівень НРК);
- 125 «Кібербезпека» галузі знань «Інформаційні технології» (7 рівень НРК);
- 126 «Інформаційні системи та технології» галузі знань «Інформаційні технології» (7 рівень НРК);
- 172 «Телекомунікації та радіотехніка» галузі знань 17 «Електроніка та телекомунікації» (7 рівень НРК);

- документ (диплом, сертифікат, тощо), щодо післядипломної освіти та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері планування стратегічних заходів з розвитку в організації інформаційних технологій, інформаційної безпеки та кібербезпеки;
- документ (диплом, сертифікат, тощо), щодо післядипломної освіти та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань в рамках консультаційно-навчальної діяльності у сфері планування політики та стратегії кібербезпеки;
- документ (диплом, сертифікат, тощо), щодо професійної сертифікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері планування стратегічних заходів з розвитку в організації інформаційних технологій, інформаційної безпеки та кібербезпеки.

III. 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**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
Фахівець з планування політики та стратегії кібербезпеки Провідний фахівець	Підготовка на другому рівні вищої освіти (магістерському) за спеціальностями вказаними п.1, п.п.1.8 галузі знань 12 «Інформаційні технології» та 17 «Електроніка та телекомунікації», стаж роботи за однією з професій відповідного спрямування повинен	

з планування політики та стратегії кібербезпеки	складати не менше 2 років (аналітик з безпеки інформаційно-телекомунікаційних систем, фахівець з питань безпеки (інформаційно-комунікаційні технології), фахівець сфери захисту інформації тощо)

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 фахівець з планування політики та стратегії кібербезпеки для отримання професійної кваліфікації "провідний фахівець з планування політики та стратегії кібербезпеки". Стаж роботи не менше двох років	

IV. Абревіатури, скорочення

ІТ	інформаційні технології

V. Опис трудових функцій

Трудові функ	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
А. Викс підготов-чих робіт у сфері пла вання політики та стра розвитку інформ ної безпеки та кібер пеки	**А1**. Здатність інтер-претувати і застосо-вувати чинні закони та нормативні документи відповідного спря-мування та інтегрувати їх в політику організації (Т0408)	**А1.З1.** Технологічні задачі і завдання управління та лідерства пов'язані з організаційними процесами, механізми вирішення проблем **А1.З2**. Концепції і протоколи комп'ютерних мереж, а також методологію забезпечення безпеки мереж (К0001) **А1.З3.** Методики управління ризиками (методи оцінювання та оброблення ризиків) (К0002) **А1.З4**. Закони, нормативні акти,	**А1.У1.** Планувати і координувати методики та формати інтеграції чинних законів, нормативних актів, міжнародних та зарубіжних практик в політику кіберзахисту в політику організації **А1.У2**. Збирати точні та повні дані з джерел, які використовуються для розвідки, оцінювання та/або планування **А1.У3.** Інтерпретувати	**А1.К1.** Адаптувати технічну інформацію для планування до рівня розуміння користувача/споживача / замовника	**А1.В1**. Інтерпретувати та застосовувати закони, нормативні акти, політики, стандарти чи процедури до конкретних питань (Т0131)

		політики і етичні норми, та як вони пов’язані з конфіденційністю персональних даних та кібербезпекою (К0003) **А1.35**. Принципи забезпечення конфіденційності персональних даних та кібербезпеки (К00004) **А1.36**. Кіберзагрози та вразливості (К0005) **А1.37**. Основні операційні наслідки інцидентів кібербезпеки (К0006) **А1.38**. Методи автентифікації, авторизації та контролю доступу **А1.39**. Технології віртуалізації, формування віртуальних машин їх технічна підтримка **А1.310**. Нові та ті, що розроблюються технології інформаційної та кібербезпеки	та/або затверджувати вимоги щодо безпеки спроможностей нових інформаційних технологій (Т0132)		

		А1.З11. Політику навчання в організації **А1.З12.** Види доведення інформації (асимілятивний, слуховий, кінестетичний)			
	А2. Здатність застосовувати у практичній діяльності вітчизняні, міжнародні та зарубіжні чинні та перспективні політики та стратегії розвитку кібербезпеки (Т0222)	**А2.З1.** Галузеві показники, корисні для визначення тенденцій розвитку технологій (К0311) **А2.З2.** Сучасні і перспективні кібертехнології (К0335) **А2.З3.** Сервіс-орієнтовані принципи архітектури безпеки **А2.З4**. Стратегії кіберможливостей для розробки програмно-апаратних комплексів **А2.З5**. Стандарти політики та стратегії кібербезпеки **А2.З6.** Форму запиту на профільну інформацію **А2.З7**. Сучасні галузеві методи оцінки, впровадження та розпов-	**А2.У1.** Застосовувати сервісорієнтовані принципи архітектури безпеки, щоб задовольнити вимоги конфіденційності, цілісності та доступності організації (Т0017) **А2.У2**. Визначати стратегії кіберможливостей для розробки програмно-апаратних комплексів для замовника, ґрунтуючись на вимогах місії (Т0250)	**А2.К1.** Формувати запити на профільну інформацію (Т0707)	**А2.В1.** Переглядати стандарти політики та стратегії її впровадження, щоб забезпечити відповідність процедур та настанов політикам кібербезпеки (Т0254)

		сюдження інструмен-тів та процедур оцінки безпеки ІТ, моні-торингу, виявлення усунення несправ-ностей, що викорис-товують концепції можливості на стандартів (К0054)			
	А3. Здатність аналізувати політику організації у сфері кібербезпеки (Т0425)	**А3.З1.** Загрози і вразливості безпеки систем і прикладного програмного забезпечення (К0070) **А3.З2.** Зміст та функції відповідної інформаційної структури (К0127) **А3.З3.** Ризики безпеки прикладних програм (Open Web Application Security Project Top 10 list) (К0624) **А3.З4.** Політику та конфігурації кіберзахисту організації **А3.З5**. Нові технології і архітектури баз даних	**А3.У1.** Аналізувати політику та конфігурації кіберзахисту організації та оцінювати відповідність нормативним актам та директивам організації (Т0010) **А3.У2.** Аналізувати проєктні обмеження, аналізувати компроміси та детальний проект системи та безпеки, а також розглядати підтримку	**А3.К1.** Надавати реко-мендації щодо структур даних і баз даних з гарантованого забез-печення підготовки ко-ректних і якісних звітних документів (Т0209)	**А3.В1.** Надавати рекомендації щодо нових технологій і архітектур баз даних (Т0210)

		А3.З6. Порядок аналізу політики організації у сфері кібербезпеки **А3.З7**. Порядок аналізу потреби та вимог користувачів для планування архітектури **А3.З8**. Порядок аналізу потреби безпеки і вимог до програмного забезпечення **А3.З9**. Фундаментальні кіберконцепції, принципи, обмеження і ефекти (К0435) **А3.З10**. Фундаментальні концепції, термінологію/лекси-кон, принципи, можливості, обмеження і ефекти кібероперацій (К0436) **А3.З11**. Рекомендації щодо оптимізації та вирішення в організації проблем відповідно до розвитку інформаційних технологій	життєвого циклу (Т0012) **А3.У3.** Готувати рекомендації щодо можливих удосконалень і оновлень (Т0208) **А3.У4**. Приймати участь в аналізі політики організації у сфері кібербезпеки (Т0425) **А3.У5**. Приймати участь в аналізі результатів тестування програмного, апаратного забезпечення або сумісності (Т0426) **А3.У6**. Приймати участь в аналізі потреби та вимог користувачів для планування архітектури (Т0427) **А3.У7**. Приймати участь в аналізі потреби безпеки і		

		А3.З12. Нові/існуючі заходи безпеки, стійкості та надійності організації **А3.З13.** Рекомендації аналізу кризових ситуа метою забезпе суспільної та персональн безпеки, захисту кібер ресурсів **А3.З14.** Концепцію планування в організації (К0512) **А3.З15**. Положення про ініціювання планування діяльності організації (К0518) **А3.З16**. Зміст та порядок адаптивного планування, планування в кризових умовах та планування з урахуванням обмеженого часу (К0519)	вимог до програмного забез-печення з метою визначення до-цільності проєк-ту з урахуванням часових і цінових обмежень, а також мандатів безпеки (Т0428) **А3.У8.** Приймати участь у забезпеченні в організації постійної оптимізації та вирішення проблем відповідно до розвитку інформаційних технологій (Т0207) **А3.У9.** Рекомендувати нові або переглядати існуючі заходи безпеки, стійкості та надійності на основі		

			результатів перевірок (Т0218) **А3.У10.** Аналізувати кризові ситуації з забезпечення суспільної та персональної безпеки, а також захисту ресурсів (Т0343)		
	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. Планування політики, стратегії, програм та настанов для подальшого впровадження заходів з кібер	**Б1**. Здатність сприяти обізнаності керівництва стосовно кіберполітики кіберстратегій (Т0384)	**Б1.З1.** Технології виробництва, комунікації та розповсюдження медійних повідомлень, а також альтернативні способи інформування за допомогою текстових, мовних, візуальних повідомлень **Б1.З2**. Відповідні концепції, процедури,	**Б1.У1.** Готувати пропозиції щодо пошуку та управління необхідними ресурсами, включаючи фінансові, для забезпечення безперервності дії політик та стратегій, програм з розвитку кібербезпеки,	**Б1.К1.** Розроблювати вказівки і настанови для працівників, залучених до розроблення стратегій, програм та політик з розвитку кібербезпеки	**Б1.В1**. Розроблювати технічну документацію відповідного спрямування

-безбеки (T0074)		програмне забезпечення, обладнання і прикладні технологічні програми які застосовуються для планування **Б1.З3**. Вимоги до структури та змісту стратегій, програм та політик з розвитку кібербезпеки	функціонування операційних програм підприємства (T0002) **Б1.У2**. Розроблювати або брати участь у розробленні стратегій, програм та політик з розвитку кібербезпеки **Б1.У3.** 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 та завдань безпеки інформаційних технологій, зниження		

			загального ризику організації (Т0001)		
	Б2. Здатність визначати та інтегрувати середовища для поточної та майбутньої місій кіберстратегії (Т0441)	**Б2.З1.** Класифікацію кіберможливостей (захист, атаки, експлуатація) (К0234) **Б2.З2.** Теорію і практику стратегії (К0248) **Б2.З3.** Перспективні технології, які можуть бути використані в подальшому (К0309) **Б2.З4**. Порядок розроблення профільних планів **Б2.З5**. Порядок розроблення профільних стратегічних планів **Б2.З6.** Проєктну документацію з безпеки для специфікацій компонентів та інтерфейсів **Б2.З7**. Порядок розроблення планів аварійного відновлення та безперервності операцій для систем, що розробляються, та	**Б2.У1.** Приймати участь в організації процесів планування, включаючи підготовку функціональних і спеціальних планів підтримки, підготовки і забезпечення ділового листування, а також процесів кадрового забезпечення (S0176) **Б2.У2.** Розроблювати профільні плани та готувати відповідну кореспонденцію (S0250) **Б2.У3**. Аналізувати інформацію з метою визначення, рекомендацій та планування розробки нової прикладної програми або	**Б2.К1.** Планувати розроблення та приймати участь у розробленні та підтримці/ супроводженні стратегічних планів організації з кібербезпеки (Т0066)	**Б2.В1.** Розроблювати політику, програми та настанови відповідного спрямування для подальшого їх впровадження (Т0074)

		тестування систем до їхнього вводу у продуктивне середовище	модифікації існуючої прикладної програми (T0009) **Б2.У5.** Планувати розроблення детальної проєктної документації з безпеки для специфікацій компонентів та інтерфейсів з метою підтримки проєкту та розроблення системи (T0069) **Б2.У6**. Планувати розроблення планів аварійного відновлення та безперервності операцій для систем, що розробляються, та забезпечення тестування систем до їхнього вводу у продуктивне середовище (T0070) **Б2.У7.** Планувати розроблення /інтегрування проєкти з		

			кібербезпеки для систем та мереж із багаторівневими вимогами безпеки або вимогами для обробки кількох рівнів класифікації даних, що застосовуються головним чином до державних організацій (T0071)		
	Б3. Здатність розроблювати/інтегровувати кіберстратегію, узгод-жену зі стратегічним планом організації (T0445)	**Б3.З1.** Матеріали інструкцій (стандартні операційні процедури, технологічний посібник) для надання детальних вказівок відповідним працівникам **Б3.З2.** Технічну документацію відповідного спрямування **Б3.З3**. Методи та підходи щодо переглядів та/чи вдосконалення стратегій, програм та політик з розвитку кібербезпеки	**Б3.У1.** Готувати матеріали інструкцій (стандартні операційні процедури, технологічний посібник) для надання детальних настанов для відповідної частини персоналу **Б3.У2.** Інтегровувати нові наукові ідеї та підходи у зміст стратегій, програм та політик з розвитку кібербезпеки в	**Б3.К1.** Ураховувати обґрунтованому обсязі вимоги керівництва організації під періодичного перегля-ду та вдосконалення стратегій, програм та політик з розвитку кібербезпеки	**Б3.В1**. Розроблювати технічну документацію відповідного спрямування

		Б3.З4. Вимоги системи забезпечення якості **Б3.З5**. Рекомендації щодо змін або коригувань на основі результатів застосування або системного середовища **Б3.З6**. Стратегії зменшення ризиків для усунення кібервразливостей **Б3.З7**. Плани запобіжних і/або антикризових заходів відповідного спрямування **Б3.З8**. Процедури планування кризових дій та в умовах обмеженого часу (К0399) **Б3.З9.** Процедури планування кібероперацій в	необхідних обсягах і формах **Б3.У3**. Розроблювати групові політики та переліки контролю доступу для забезпечення відповідності стандартам організації, бізнес-правилам та потребам (Т0054) **Б3.У4.** Аналізувати вимоги та очікування керівників та персоналу, інших користувачів від запроваджених чи розроблюваних стратегій, програм та політик з розвитку кібербезпеки **Б3.У6.** Розроблювпти стратегії зменшення ризиків для усунення вразливостей та рекомендувати, у		

		кризових ситуаціях (К0400)	випадку необхідності, зміни заходів безпеки у системі або системних компонентах (Т076) **Б3.У7**. Планувати та розроблювати рекомендації щодо змін або коригувань на основі результатів застосування або системного середовища (Т0187) **Б3.У8**. Розроблювати і підтримувати запобіжних антикризових заходів (Т0654)		
	Б4. Здатність підтримувати керівника ІТ з у формуванні політики стратегій, які стосуються кібербезпеки (Т0537)	**Б4.З1.** Стан кібербезпеки в організації **Б4.З2.** Заходи стратегій, політик, програм та планів з розвитку в організації кібербезпеки	**Б4.У1.** Консультувати вище керівництво щодо рівня ризику та, урахування при планування заходів політик, стратегій і програм стосовно його зниження (Т0004)	**Б4.К1.** Надавати керівництву пояснення методології з розвитку в організації кібербезпеки	**Б4.В1.** Рекомендувати зміни доповнення кіберполітику організації, приймати участь у координації її

		Б4.З3. Методологію з розвитку кібербезпеки в організації **Б4.З4.** Принципи і методики управління програмами та проєктами з інформаційної безпеки (К0121) **Б4.З5.** Типи та оперативного плану (К0498)	**Б4.У2.** Консультувати вище керівництво щодо аналізу витрат/вигоди програм, політик, процесів, систем та елементів інформаційної безпеки, щодо змін, які впливають на стан кібербезпеки в організації (Т0005) (Т0202)		перегляду (Т0227)
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відпов програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових нау журналів (EBSCO, JSTOR) відповідно до профілю планування; бібліотечні ресурси, архівні матеріали (за потреби); прос наукова, методична література; законодавчо-нормативні акти, акти роботодавця відповідного спрямування				
В. Надання консультаційних послуг методологічного забезпечення планування політики,	**В1.** Здатність розроблювати проєкти з розвитку кібербезпеки, ознайом-лювати персонал і публікувати політику кібербезпеки (Т0472)	**В1.З1.** Зміст проєктів відповідного спрямування **В1.З2**. Особливості організації проєктної діяльності для різних категорій працівників **В1.З3.** Форми організації проєктної діяльності	**В1.У1.** Планувати проєктування та розроблення продуктів кібербезпеки та продуктів, які сприяють кібербезпеці (Т0053)	**В1.К1**. Надавати (доводити до відома) технічну інформацію різним категоріям користувачів **В1.К2.** Встановлювати ефективний зворотний зв'язок з користувачами профільних послуг та партнерами	**В1.В1.** Налаштовувати і використовува-ти у проєктній діяльності програмні засоби захисту комп'ютерів (програмні

стратегії, програм та настанов з кібербезбеки		**В1.З4.** Корпоративні цілі і завдання, пов'язані з використанням інформаційних технологій в організації (К0101) **В1.З5.** Сучасні методи, засоби та технології проєктування **В1.З6.** Методи і способи ефективної комунікації	**В1.У2**. Розроблювати у необхідних обсягах проєкти на сучасних мовах програмування **В1.У3.** Використовувати у проєктній діяльності віртуальні машини (Microsoft Hyper-V, VMWare, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud) **В1.У4.** Конфігурувати і використовувати у проєктній діяльності компоненти системи мережевої безпеки (мережеві екрани, віртуальні приватні мережі, системи виявлення вторгнень) **В1.У5**. Використовувати сучасні та новітні технології при		фільтри, антивірусні програми й антишпигунське програмне забезпечення)

			презентації проєктів (інтерактивні дошки, Web-сайти, комп'ютери, проектори) **В1.У6**. Відображати отримані дані в оригінальних форматах **В1.У7.** Визначати масштаб проєкту та цілі відповідно до замовника (Т0052)		
	В2. Здатність надавати керівництву, персоналу і користувачам консультації застосування на практиці методології щодо по. кібербезпеки (Т0529)	**В2.З1**. Методологію розвитку кібербезпеки організації **В2.З2**. Підходи щодо управління ризиком ланцюжка постачання **В2.З3.** Класифікація операційних планів в частині кібербезпеки **В2.У4.** Рекомендації щодо проведення брифінгів з обізнаності, дотримання норм та положень стратегій, політик і програм з розвитку кіберзахисту **В2.З5.** Загальнодоступні	**В2.У1.** Приймати участь у розробленні методології кібербезпеки організації та управління ризиком ланцюжка постачання для розробки безперервності операційних планів (Т0199) **В2.У2.** Застосовувати концепції, процедури, програмне	**В2.К1.** Сприяти дискусіям у невеликих групах **В2.К2**. Готувати та проводити брифінги з обізнаності, дотримання норм та положень стратегій, політик і програм з розвитку кіберзахисту керівництву, персоналу і користувачам	**В2.В1** Керувати різними системами і методами електронної комунікації (електронна пошта, VOIP, миттєві повідомлення, форуми, Direct Broadcasts)

		мережеві інструменти (ping, traceroute, nslookup) **В2.З6**. Командний рядок операційної системи (ipconfig, netstat, dir, nbtstat) **В2.З7**. Системи і методи електронної комунікації (електронна пошта, VOIP, IM (миттєві повідомлення), Web-форуми, Direct Video Broadcasts)	забезпечення, обладнання та/або технологічні прикладні програми під час надання консультацій із застосування на практиці методології щодо політики кібербезпек **В2.У3.** Користуватися загальнодоступ-ними мережевими інструментами (ping, traceroute, nslookup) **В2.У4.** Використовувати командний рядок операційної системи (ipconfig, netstat, dir, nbtstat)		
	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				
Г. Про-	**Г1**. Здатність моніторити	**Г1.З1.** Методики оцінювання	**Г1.У1**. Розробляти методи моніторингу	**Г1.К1.** Рекомендувати керівництву	**Г1.В1**. Оцінювати

ведення моніторингу виконання політик, принципів і практик при наданні послуг з планування та управління політики кіберезпеки	виконання політик, принципів і практик при наданні послуг з планування та управління політикою кібербезпеки (Т0505)	працівників щодо реалізації заходів стратегій, політик та програм з розвитку кіберзахисту **Г1.З2.** Методи та процеси тестування і оцінювання працівників щодо реалізації заходів стратегій, політик та програм з розвитку кіберзахисту **Г1.З3**. Порядок та методи оцінювання працівників щодо реалізації заходів стратегій, політик та програм з розвитку кіберзахисту **Г1.З4.** Класифікацію методів оцінювання та процедуру їх застосування на практиці **Г1.З5**. Підходи та методи до розроблення і верифікації критеріїв оцінювання працівників щодо реалізації заходів стратегій, політик та	та оцінки ризиків, відповідності та зусиль щодо надання впевненості у результативності заходів стратегій, політик, програм та планів (Т0072) **Г1.У2**. Відслідковувати результати аудиту та розробляти рекомендації, щоб забезпечити вжиття відповідних заходів щодо зменшення негативних наслідків (Т0234) **Г1.У3.** Підтримувати та сприяти безперервному моніторингу в організації стосовно планування стратегій, політик, програм та планів з розвитку кіберзахисту (Т0967) **Г1.У4.** Приймати участь у визначенні	кандидатури працівників до відповідних робочих груп безперервного профільного моніторингу (Т0968) **Г1.К2**. Розроблювати тести для визначення рівня обізнаності та участі працівників щодо реалізації заходів стратегій, політик та програм з розвитку кіберзахисту **Г1.К3**. Розроблювати критерії оцінювання працівників щодо реалізації заходів стратегій, політик та програм з розвитку кіберзахисту **Г1.К4**. Брати участь у розробленні правил оцінювання працівників щодо реалізації заходів стратегій, політик та програм з розвитку кіберзахисту	витрати-вигоду, економічний аналіз та аналіз ризиків у процесі прийняття рішень (Т099) **Г1.В2.** Оцінювати ефективність законів, правил, політик, стандартів чи процедур відповідного спрямування (Т0102)

		програм з розвитку кіберзахисту **А2.З7.** Сучасні галузеві м оцінки, впровадження розповсюдження інстру та процедур оцінки бе інформаційних техно моніторингу, виявлен усунення несправностей використовують концеп можливості на стандартів (К0054)	вимог до звітності для підтримки діяльності з профільного безперервного моніторингу (Т0969) **Г1.У5.** Приймати уч формуванні си критеріїв та показник оцінки ефекти програми профіл безперервного моніто (Т0970)		
	Г2. Здатність брати участь в аудитах кіберпрограм кіберпроектів (Т0533)	**Г2.З1.** Методи соціальної інженерії **Г2.З2.** Підходи та методи до розроблення і верифікації критеріїв оцінювання працівників щодо реалізації заходів стратегій, політик та програм з розвитку кіберзахисту **Г1.З3.** Порядок та методи оцінювання працівників щодо реалізації заходів стратегій, політик та	**Г2.У1.** Використовувати інструменти та методики тестування на проникнення **Г2.У2**. Використовувати методи соціальної інженерії **Г2.У3**. Оцінювати ефективність заходів з кібербезпеки, які використовуються системою (системами) (Т0018)	**Г2.К1**. Приймати участь в оцінюванні працівників реалізації заходів стратегій, політик та програм з розвитку кіберзахисту	**Г2.В1**. Перег-лядати здійснювати програм та проєктів з ІТ (Т0223)

		програм з розвитку кіберзахисту **Г1.З4.** Класифікацію методів оцінювання та процедуру їх застосування на практиці **А2.З7.** Сучасні галузеві методи оцінки, впровадження та розповсюдження інструментів та процедур оцінки безпеки ІТ, моніторингу, виявлення усунення несправностей, що використовують концепції можливості на стандартів (К0054)	**Г2.У4.** Оцінювати загрози та вразливості комп'ютерної системи (систем) для розробки профілю ризику безпеки (Т0019) **Г2.У5**. Оцінювати контракти з метою забезпечення відповідності фінансовим, юридичним та програмним вимогам (Т0098) **Г2.У6.** Готувати звітні документи з аудиторської перевірки, які містять технічні та процедурні висновки, а також рекомендувати коригування стратегій/рішень (Т0188)		
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відпов програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повно-текстових нау				

	журналів (EBSCO, JSTOR) відповідно до профілю планування; бібліотечні ресурси, архівні матеріали (за потреби); законо, нормативні акти, акти роботодавця відповідного спрямування				
Д. Підтримання комунікації стейкголдерами в сфері планування політики та стратегії розвитку кібербезпеки (Т0094)	**Д1**. Здатність брати участь у відомчих і міжвідомчих рад з питань політики та стратегії розвитку кібербезпеки (Т0226)	**Д1.З1.** Основні бізнес-процеси і місію організації (К0146) **Д1.З2.** Прийняті в організації правила класифікації інформації щодо рівнів захисту і процедур доступу до неї **Д1.З3**. Посадові завдання та обов'язки внутрішнього консультанта/радника за профільними спеціалізаціями **Д1.З4.** Джерела і методи збору інформації, її узагальнення, структурування, систематизацію **Д1.З5**. Методи і технології підготовки доповідей та презентацій	**Д1.У1**. Переглядати існуючі та перспективні політики із зацікавленими сторонами (Т0222) **Д1.У2**. Оцінювати потреби в політиці та співпрацювати із зацікавленими сторонами з метою розробки політик корпоративного управління діяльністю в сфері кібербезпеки (Т0429)	**Д1.К1**. Готувати та проводити брифінги відповідного спрямування **Д1.К2**. Комунікувати з керівниками різних рівнів (міжособистісне спілкування, доступність, уміння ефективно сприймати мову виступаючих, відповідно до аудиторії коректувати стиль і мову виступу)	**Д1.В1.** Виконувати обов’язки внутрішнього консультанта/ радника в сфері планування заходів з розвитку кібербезпеки в організації
	Д2. Здатність оцінювати потреби в політиці та співпра-	**Д2.З1.** Основні небезпеки, ризики і кіберврразливості	**Д2.У1.** Прогнозувати спільно із	**Д1.К1**. Готувати та проводити брифінги	**Д2.В1.** Розвивати розуміння

	цювати з зацікавленими сторонами з метою розроблення політик корпоративного управління діяльністю в сфері кібербезпеки (Т0429)	**Д2.З2**. Методи та процедура прогнозування потреб у послугах з кібербезпеки **Д2.З3**. Принципи забезпечення безпеки інформації **Д2.З4**. Можливості і обмеження внутрішніх і зовнішніх організацій-партнерів (К0467) **Д2.З5.** Звітність внутрішніх і зовнішніх організацій-партнерів (К0468) **Д2.З6**. Внутрішню та зовнішню тактику прогнозування і/або моделювання спроможностей та дій загроз (К0469 **Д2.З7**. Політику організ концепції планування співпраці з внутрішніми зовнішніми організа (К0508)	стейкголдерами поточні потреби у послугах та забезпечувати, що припущення щодо безпеки переглядаються за необхідності (Т0281) **Д2.У2.** Застосувати спільно із стейкголдерами принципи забезпечення безпеки інформації – збереження конфіденційності, цілісності та доступності **Д2.У3**. Визначати спільно із стейкголдерами та/або впроваджувати політики і процедури, щоб забезпечити належний захист критичної інфраструктури (Т0282)	відповідного спрямування	потреб та вимог кінцевих користувачів інформації (Т0060)

			Д2.У4. Співпрацювати із зацікавленими сторонами, щоб визначити та/або розробити відповідні технології прийняття рішень (Т0283)		
	Д3. Здатність знаходити консенсус із зацікавленими сторонами щодо запропонованих змін кіберполітики (Т0506)	**Д3.З1.** Зовнішні організації і установи, діяльність яких спрямована на розвиток, захист та дослідження кіберпростору (К0313) **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	**Д3.У1**. Використовувати інструменти управління мережею для аналізу структури мережевого трафіку **Д3.У2**. Використовувати аналізатори протоколів **Д3.У3**. Інтегрувати процеси планування /визначення цілей з іншими організаціями (Т0732) **Д3.У4.** Проводити заходи з довгострокового стратегічного планування за	**Д3.К1**. Розроблювати або допомагати в розробці навчальних матеріалів для покращення розуміння співробітниками політики конфіденційності компанії, практики та процедур обробки даних, юридичних зобов’язань	**Д3.В1**. Освоювати досягнення у технологіях захисту інформації для забезпечення їх впровадження у відповідній організації

		процеси відповідного спрямування **Д3.34**. Інструменти управління мережею для аналізу структури мережевого трафіку **Д3.35.** Аналізатори протоколів **Д3.36**. Повноваження організації і організації-партнера, відповідальність та внески у досягнення поставлених цілей (К0509) **Д3.37.** Політику, засоби, спроможності і процедури організації та організації-партнера (К0510)	участю внутрішніх і зовнішніх партнерів з кібердіяльності (Т0763) **Д3.У5**. Пропонувати політику взаємодії, яка регулює взаємодію із зовнішніми групами координації (Т0766)		
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відпов програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повно-текстових нау журналів (EBSCO, JSTOR) відповідно до профілю планування; бібліотечні ресурси, архівні матеріали (за потреби); законо, нормативні акти, акти роботодавця відповідного спрямування				
Е. Надання консультаційно-навчальних	**Е1**. Здатність готувати керівництву рекомендації планування підтримки адекватного фінансування	**Е1.З1.** Прикладні бізнес процеси і функції в організації-замовнику **Е1.З2.** Принципи безперервності бізнесу	**Е1.У1.** Повідомляти вартість запланованих освітніх ресурсів у кіберсфері зацікавленим	**Д1.К1**. Готувати та проводити брифінги відповідного спрямування	**Е1.В1.** Аналізувати та звітувати перед керівництвом про користування

послуг з питань планування політики та стратегії розвитку кібербезпеки та процесів управління кіберперсоналом	освітніх ресурсів у кібер сфері	та операційних планів відновлення безперервності після катастроф **Е1.33.** Методики управління ризиками в ланцюжку постачання **Е1.34.** Вимоги до закупівлі критичних інформаційних технологій **Е1.35**. Методи прогнозування в освітніх послугах для організації **Е1.36**. Порядок планування закупівлі освітніх послуг	сторонам організації на всіх рівнях **Е1.У2**. Прогнозувати поточні потреби у освітніх послугах та забезпечувати перегляд припущень щодо безпеки за необхідності **Е1.У3.** Контролювати ситуацію, щоб усі дії з планування придбання, постачання, закупівлі та аутсорсингу освітніх послуг у кіберсфері відповідали вимогам кібербезпеки, які відповідають цілям організації **Е1.У4.** Брати участь, за необхідності, у процесі		активами і ресурсами управління знаннями (Т0154)

			планування закупівлі освітніх послуг, дотримуючись відповідних практик управління ризиків в ланцюжку постачання		
	Е2. Здатність забезпечувати планування політики і процесів управління кіберперсоналом	**Е2.З1.** Матеріали інструкцій (стандартні операційні процедури, технологічний посібник) для надання детальних вказівок відповідним працівникам **Е2.З2.** Керівництва/настанови, інструкції та/або інші нормативні акти роботодавця, які застосовуються для організації та координації діяльності з планування політики і процесів управління кіберперсоналом	**Е2.У1.** Приймати участь у плануванні в організації контролю за використанням бюджету на персонал та укладанням контрактів (Т0135) **Е2.У2.** Приймати участь у плануванні політики і процесів управління кіберперсоналом **Е2.У3.** Визначати альтернативні стратегії розвитку кіберперсоналу для дотримання цілей	**Е2.К1.** Надавати керівництву пропозиції оптимального співвідно оплати праці та винагороди кіберперсоналу та рівня їхньої кваліфікації, продуктивності та наукомісткості праці	**Е2.В1.** Готувати пропозиції керівництву щодо оновлення нормативних актів роботодавця у сфері соціально-трудових відносин в організації

		Е233. Посадові інструкції/професійні стандарти на посади кіберперсоналу **Е234.** Основи управління персоналом **Е2.35.** Порядок розроблення та підписання трудових договорів та контрактів **Е2.36.** Основи трудового законодавства **Е2.37**. Структуру організації, функції структурних підрозділів, розподіл функцій між керівниками організації, підпорядкованість підрозділів **Е2.38.** Положення структурні підр організації, що задія спільному вик технологічних та функціональних завдань	організаційної безпеки **Е2.У4.** Планувати найбільш оптимальну структуру організації та розподіл її кіберперсоналу відповідно до цілей та завдань стратегічного та оперативного планів		
	Е3. Здатність планувати перегляд/	**Е3.31.** Методи визначення вимог до інфраструктури	**Е3.У1.** Проводити комплексний аналіз відповідності змісту	**Е3.К1.** Проводити соціологічні анонімні опитування слухачів,	**Е3.В1.** Планувати оцінювання

	оцінювання ефек- тивності кіберперсоналу коригування вимог до навичок та/або стандартів кваліфікації	тестування та оцінювання **Е3.32.** Принципи і процеси проведення тренінгів та оцінки потреби у навчанні **Е3.33.** Відповідні концепції, процедури, програмне забезпечення, обладнання і прикладні технологічні програми які застосовуються для навчання **Е3.34.** Вимоги та підходи до розроблення навчальних та методичних матеріалів **Е3.35.** Сучасні підходи до формування навчальних програм **Е3.36.** Вимоги до структури та змісту навчальної програми **Е3.36.** Порядок, процедура та форми підготовки кадрів на робочому місці **Е3.37.** Особливості організації навчального процесу для різних	навчальних програм встановленим стандартам якості навчання **Е3.У2.** Оцінювати конкретні результати роботи щодо підготовки, перепідготовки та підвищення кваліфікації працівників **Е3.У3.** Планувати обґрунтування зв'язку навчальної програми для тренінгів, зокрема, на робочому місці зі стратегією розвитку організації у сфері інформаційної та кібербезпеки **Е3.У4.** Аналізувати вимоги та очікування слухачів, їх роботодавців та інших заінтересованих осіб щодо навчальної	інтерв'ювання інших заінтересованих осіб стосовно покращення методів навчання та змісту навчальних програм	ефективності існуючих програм навчання та тренінгів

		форм набуття компетентності **Е3.38.** Сучасні методи, засоби та технології викладання **Е3.39.** Порядок та методи оцінювання результатів навчання **Е3.310.** Порядок присвоєння/ присудження часткової професійної/ освітньої кваліфікації **Е3.311.** Класифікацію методів оцінювання процедуру їх застосування на практиці	програми/тренінгу чи курсу **Е3.У5.** Ураховувати в обґрунтованому обсязі вимоги керівництва, стратегій, політик та програм організації під час періодичного перегляду та вдосконалення навчальних планів, програм **Е3.У6.** Планувати перегляд/ оцінювання ефективності кіберперсоналу для коригування вимог до навичок та/або стандартів кваліфікації		
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп’ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відпов програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повно-текстових нау				

	журналів (EBSCO, JSTOR) відповідно до профілю планування; бібліотечні ресурси, архівні матеріали (за потреби); законо, 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 планування політики та стратегії кібербезпеки**
	повна	часткова додаткова
А	+	+
Б	+	+
В	+	+
Г	+	+
Д	+	+
Е	-	+

VII. Відомості про розроблення та затвердження професійного стандарту

1. Повне найменування розробника професійного стандарту

Державної служби спеціального зв'язку та захисту інформації України

Склад робочої групи/Учасники робочої групи:

_____
_____

2. Назва та реквізити документа, яким затверджено професійний стандарт (рішення (може оформлюватися протоколом), наказ, розпорядження).

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 _____ 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 Профспілки працівників зв'язку України від _____ щодо погодження проєкту професійного стандарту «фахівець з планування політики та стратегії кібербезпеки».

VIII. Дата внесення професійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.