Проєкт

Професійний стандарт

АУДИТОР ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ (З 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

I. Назва професійного стандарту

Аудитор інформаційних технологій (з кібербезпеки)

II. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Надання аудиторських та консультативних послуг у сфері інформаційної безпеки та кібербезпеки. Проведення оцінювання програм інформаційних технологій та кібербезпеки, її окремих компонентів для визначення відповідності опублікованим стандартам

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 М	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

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

Аудитор інформаційних технологій (з кібербезпеки) 2139.2

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

Аудитор інформаційних технологій (з кібербезпеки), 7 рівень НРК

Провідний аудитор інформаційних технологій (з 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 аудиту інформаційних технологій (з 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 аудиту інформаційних технологій (з кібербезпеки);
- документ (диплом, сертифікат, тощо), щодо професійної сертифікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері аудиту інформаційних технологій (з кібербезпеки).

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**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
Аудитор інформаційних технологій (з кібербезпеки), Провідний аудитор інформаційних технологій (з кібербезпеки)	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 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 аудитор інформаційних технологій (з кібербезпеки)". Стаж роботи не менше двох років	

IV. Абревіатури, скорочення

ІТ	інформаційні технології

V. Опис трудових функцій

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
A. Підготовка до проведення аудиту програм та проєктів з ІТ у сфері кібербезпеки	**A1**. Здатність планувати проведення аудиту програм та проєктів з ІТ у сфері кібербезпеки	**A1.З1.** Технологічні задачі і завдання управління та лідерства, пов'язані з організаційними процесами, механізми вирішення проблем **A1.З2**. Концепції і протоколи комп'ютерних мереж, а також методологію забезпечення безпеки мереж (К0001) **A1.З3.** Методики управління ризиками (методи оцінювання та оброблення ризиків) (К0002) **A1.З4**. Закони, нормативні акти, політики і етичні	**A1.У1.** Планувати на рік, квартал, місяць тиждень проведення аудиту програм та проєктів з ІТ у сфері кібербезпеки **A1.У2.** Адаптувати технічну інформацію для планування аудиту програм та проєктів з ІТ у сфері кібербезпеки **A1.У3**. Збирати точні та повні дані з джерел, які використовуються для оцінювання та планування аудиту програм та проєктів	**A1.К1.** Адаптувати технічну інформацію для планування аудиту до рівня розуміння користувача/споживача / замовника	**A1.В1**. Інтерпретувати та застосовувати закони, нормативні акти, політики, стандарти чи процедури до конкретних питань (Т0131)

		норми, та як вони пов'язані з конфіденційністю персональних даних та кібербезпекою (К0003) **А1.З5**. Принципи забезпечення конфіденційності персональних даних та кібербезпеки (К0004) **А1.З6**. Кіберзагрози та вразливості (К0005) **А1.З7**. Основні операційні наслідки інцидентів кібербезпеки (К0006) **А1.З8**. Методи автентифікації, авторизації та контролю доступу **А1.З9**. Технології віртуалізації, формування віртуальних машин їх технічна підтримка **А1.З10**. Нові та ті, що розроблюються технології інформаційної та кібербезпеки **А1.З11.** Системи управління аудитом	з ІТ у сфері кібербезпеки **А1.У4**. Планувати підготовчі заходи для проведення аудиту програм та проєктів з ІТ у сфері кібербезпеки **А1.У5.** Формувати цілі та завдання аудиту програм та проєктів з ІТ у сфері кібербезпеки **А1.У5.** Розроблювати або брати участь у розробці індивідуальних/ колективних планів з проведення відповідного аудиту		

		програм та проєктів з інформаційних технологій у сфері кібербезпеки та практику їх використання **А1.312**. Класифікацію програм та проєктів з інформаційних технологій у сфері кібербезпеки **А1.313.** Принципи і методи аналізу прийнятих в галузевих стандартах або в організації/на підприємстві (К0043) **А1.314**. Архітектурні концепції та загальні принципи інформаційних технологій (К0047) **А1.315**. Вимоги в рамках Загальних принципів управління ризиками (RMF) (К0048) **А1.316.** Принципи і способи управління ресурсами (К0072)			

	А2. Здатність виконувати підготовчі заходи для проведення аудиту програм та проєктів з ІТ у сфері кібербезпеки	**А2.З1.** Порядок проведення аудиту, технічного огляду, моніторингу придбання та застосування на підприємстві систем інформаційного та кіберзахисту **А2.З2.** Порядок інструктажу підпорядкованих працівників щодо змісту та термінів проведення аудиту, технічного огляду, моніторингу придбання та застосування на підриємстві систем інформаційного та кіберзахисту тощо **А2.З3**. Форми звітності та процедура розповсюдження результатів аудиту серед заінтересованих осіб **А1.З1.** Технологічні задачі і завдання управління та лідерства, пов'язані з організаційними	**А2.У1**. Вивчати необхідну документацію, дані, інформацію, нормативну базу, фінансові та інші матеріали, необхідні для якісного проведення аудиту **А2.У2**. Забезпечувати доступ та попереднє ознайомлення заінтересованих сторін із заходами плану підготовчих робіт та планом проведення аудиту інструктажу підпорядкованих працівників щодо змісту та термінів проведення аудиту, технічного огляду, моніторингу придбання та застосування на підприємстві систем інформаційного та кіберзахисту тощо	**А2.К1.** Формувати запити на профільну інформацію (Т0707) **А2.К2.** Проводити інструктаж підпорядкованих працівників щодо змісту та термінів проведення аудиту, технічного огляду, моніторингу придбання та застосування на підприємстві систем інформаційного та кіберзахисту тощо	**А2.В1.** Переглядати стандарти політики та стратегії її впровадження, щоб забезпечити відповідність їй процедурам з аудиту кібербезпеки (Т0254)

		процесами, механізми вирішення проблем **А1.32**. Концепції і протоколи комп'ютерних мереж, а також методологію забезпечення безпеки мереж (К0001) **А1.33.** Методики управління ризиками (методи оцінювання та оброблення ризиків) (К0002) **А1.34**. Закони, нормативні акти, 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 (К0004) **А1.36**. Кіберзагрози та вразливості (К0005) **А1.37**. Основні операційні наслідки інцидентів кібербезпеки (К0006)			

		А1.З12. Класифікацію програм та проєктів з інформаційних технологій у сфері кібербезпеки **А1.З13**. Принципи і методи аналізу прийнятих в галузевих стандартах або в організації/на підприємстві (К0043) **А1.З14**. Архітектурні концепції та загальні принципи інформаційних технологій (К0047) **А1.З15**. Вимоги в рамках Загальних принципів управління ризиками (RMF) (К0048) **А1.З16.** Принципи і сп управління ресурсами (К			
	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 напрямку аудиторської діяльності; бібліотечні ресурси, архівні матеріали (за потреби), принтер, ксерокс, фліпчарт, методична література				
Б. Проведення аудиту програм та	**Б1**. Здатність переглядати та/чи здійснювати	**Б1.З1.** Технології виробництва, комунікації та	**Б1.У1**. Використовувати передові методи	**Б1.К1.** Розроблювати вка настанови для праців	**Б1.В1**. Розроблювати технічну

проєктів з ІТ у сфері кібербезпеки	аудит програм та проєктів з ІТ у сфері кібербезпеки	розповсюдження медійних повідомлень, а також альтернативні способи інформування за допомогою текстових, мовних, візуальних повідомлень **Б1.З2**. Відповідні концепції, процедури, програмне забезпечення, обладнання і прикладні технологічні програми, які застосовуються на підприємстві **Б1.З3**. Вимоги до структури та змісту проведення профільного аудиту **Б1.З4**. Вимоги та підходи до розроблення проєктів та програм у сфері інформаційного та кіберзахисту **Б1.З5.** Сучасні підходи до оцінювання програм та проєктів з інформаційних технологій у сфері кібербезпеки	аудиторської діяльності стосовно оцінювання проєктів та програм з розвитку інформаційного та кіберзахисту **Б1.У2.** Застосовувати чіткі вказівки стосовно проведення аудиту **Б1.У3**. Застосовувати на практиці програмне забезпечення відповідного спрямування **Б1.У4**. Розроблювати та застосовувати у практичній діяльності технічну документацію відповідного спрямування **Б1.У5.** Визначати у межах своїх повноважень показники або індикатори продуктивності системи та дій,	залучених до аудиту пр та проєктів з ІТ у сфері кібербезпеки **Б1.К2.** Проводити наради та консультації під час здійснення аудиту програм та проєктів з інформаційних технологій у сфері кібербезпеки	документацію відповідного спрямування **Б1.В2**. Проводити постійний моніторинг застосування та реалізації на практиці проєктів та програм з розвитку інформаційного та кіберзахисту, зокрема щодо урахування їх виконавцями результатів аудиторських перевірок

		Б1.З6. Основи проєктного менеджменту **Б1.З6.** Методи оцінки ризиків/загроз (К0165) **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, політики і етичні норми, та як вони пов'язані з конфіденційністю персональних даних та кібербезпекою (К0003)	спрямовані на підвищення або виправлення продуктивності, виходячи з призначення системи (S0038) **Б1.У6.** Проводити аудит та/чи технічний огляд інформаційних систем (S0085) **Б1.У7.** Відстежувати і пріоритезувати потреби в інформації і вимоги до збору даних розвідки серед розширеної організації (S0372)		

		А1.35. Принципи забезпечення конфіденційності персональних даних та кібербезпеки (К0004) **А1.36**. Кіберзагрози та вразливості (К0005) **А1.37**. Основні операційні наслідки інцидентів кібербезпеки (К0006) **А1.312**. Класифікацію програм та проєктів з інформаційних технологій у сфері кібербезпеки **А1.313**. Принципи і методи аналізу прийнятих в галузевих стандартах або в організації/на підприємстві (К0043) **А1.314**. Архітектурні концепції та загальні принципи інформаційних технологій (К0047) **А1.315**. Вимоги в рамках Загальних принципів управління ризиками (RMF) (К0048)			

		А1.З16. Принципи і способи управління ресурсами (К0072)			
	Б2. Здатність здійснювати аналіз імпортних/ експортних операцій з придбання інформаційних систем і програмного забезпечення у сфері кібербезпеки, оцінювати ефективність функції закупівель з точки зору задоволення вимог інформаційної безпеки і ризиків у ланцюжку постачання через закупівельну діяльність та р екомендувати вдосконалення	**Б2.З1.** Як інформаційні потреби і вимоги до збору інформації задовольняються і відслідковуються, а також як їм присвоюються пріоритети в рамках всього підприємства (К0120) **Б2.З2.** Принципи управління життєвим циклом системи, включаючи забезпечення безпеки та експлуатаційної придатності програмного забезпечення (К0090) **Б2.З3.** Методики управління ризиками в ланцюжку постачання (NIST SP 800-161) (К0126) **Б2.З4**. Нормативні акти експортно-імпортного контролю та відповідальні установи, з метою зниження	**Б2.У1.** Здійснювати аналіз імпортних/експортних операцій з придбання інформаційних систем у сфері кібербезпеки **Б2.У2.** Здійснювати аналіз імпортних/експортних операцій з придбання програмного забезпечення у сфері кібербезпеки **Б2.У3**. Оцінювати ефективність функції закупівель з точки зору задоволення вимог інформаційної безпеки і ризиків у ланцюжку постачання через закупівельну діяльність **Б2.У4.** Рекомендувати	**Б2.К1.** Планувати розроблення та приймати участь у розробленні та підтримці/ супроводженні заходів аудиту	**Б2.В1.** Готувати редагувати звіт про результати аналізу імпортних експортних операцій з придбання інформаційних систем і програмного забезпечення у сфері кібербезпеки **Б1.В2.** Готувати та редагувати звіт про результати оцінювання ефективності функції закупівель

		ризиків ланцюжка постачання (K0148) **Б2.З5.** Стандарти, процеси і практики управління ризиками в ланцюжку постачання (K0154) **Б2.З6.** Політики, вимоги і процедур безпеки ланцюжка постачання інформаційних технологій та управління ризиками ланцюжка постачання (K0169) **Б2.З7.** Концепції вдосконалення процесів організації та моделей зрілості процесів, зокрема Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions (K0198) **Б2.З8.** Концепції управління послугами для інформаційних мереж (K0200)	заходи щодо вдосконалення системи закупівель відповідного обладнання та програмного забезпечення **Б2.У7.** Забезпечувати безпеку протягом усього процесу закупівель (A0056) **Б1.У8.** Визначати в межах своїх повноважень показники або індикатори продуктивності системи закупівель (S0038)		

		Б2.39. Вимоги до постачання/закупівлі інформаційних технологій (0257) **Б2.310.** Процес життєвого циклу постачання/закупівлі (0270) **А1.31.** Технологічні задачі і завдання управління та лідерства, пов'язані з організаційними процесами, механізми вирішення проблем **А1.32**. Концепції і протоколи комп'ютерних мереж, а також методологію забезпечення безпеки мереж (К0001) **А1.33.** Методики управління ризиками (методи оцінювання та оброблення ризиків) (К0002) **А1.34**. Закони, нормативні акти, 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 (К0004) **А1.36**. Кіберзагрози та вразливості (К0005) **А1.37**. Основні операційні наслідки інцидентів кібербезпеки (К0006) **А1.312**. Класифікацію програм та проєктів з інформаційних технологій у сфері кібербезпеки **А1.313**. Принципи і методи аналізу прийнятих в галузевих стандартах або в організації/на підприємстві (К0043) **А1.314**. Архітектурні концепції та загальні принципи інформаційних технологій (К0047) **А1.315**. Вимоги в рамках Загальних принципів управління			

		ризиками (RMF) (К0048) **А1.З16.** Принципи і способи управління ресурсами (К0072) **Б1.З6.** Методи с ризиків/загроз (К0165)			
	Б3. Здатність забезпечувати включення до положень контракту вимог до ланцюжка постачання, інформаційних систем, мережі, продуктивності та кібербезпеки	**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 положень контракту **Б3.З4.** Вимоги системи забезпечення якості **А1.З2.** Концепції і протоколи комп'ютерних мереж, а також методологію	**Б3.У1.** Готувати матеріали інструкцій (стандартні операційні процедури, технологічний посібник) для надання детальних настанов для роботи з положеннями контрактів **Б3.У2.** Аналізувати вимоги роботодавців та інших заінтересованих осіб щодо контрактів на закупівлі обладнання та програмного забезпечення з	**Б3.К1.** Ураховувати обґрунтованому обсязі вимоги керівництва організації під час періодичного перегляду та вдосконалення аудиту розвитку кібербезпеки	**Б3.В1**. Розроблювати технічну документацію відповідного спрямування **Б3.В1.** Інтегрувати нові наукові ідеї та підходи у зміст контракту, вимог до ланцюжка постачання, інформаційних систем, мережі, продуктивності та кібербезпеки

		забезпечення безпеки мереж (К0001) **А1.З3.** Методики управління ризиками (методи оцінювання та оброблення ризиків) (К0002) **А1.З4.** Закони, нормативні акти, політики і етичні норми, та як вони пов'язані з конфіденційністю персональних даних та кібербезпекою (К0003) **А1.З5.** Принципи забезпечення конфіденційності персональних даних та кібербезпеки (К0004) **А1.З6.** Кіберзагрози та вразливості (К0005) **А1.З12.** Класифікацію програм та проєктів з інформаційних технологій у сфері кібербезпеки **А1.З13.** Принципи і методи аналізу прийнятих в галузевих стандартах або в	інформаційної та кібербезпеки **Б3.У3.** Ураховувати в обґрунтованому обсязі вимоги керівництва організації під час підготовки, підписання та перегляду контрактів відповідного спрямування		

		організації/на підприємстві (К0043) **А1.315.** Вимоги в рамках Загальних принципів управління ризиками (RMF) (К0048) **А1.316.** Принципи і способи управління ресурсами (К0072) **Б2.31.** Як інформаційні потреби і вимоги до збору інформації задовольняються і відслідковуються, а також як їм присвоюються пріоритети в рамках всього підприємства (К0120) **Б2.32.** Принципи управління життєвим циклом системи, включаючи забезпечення безпеки та експлуатаційної придатності програмного забезпечення (К0090) **Б2.33.** Методики управління ризиками в ланцюжку постачання			

		(NIST SP 800-161) (К0126) **Б2.36.** Політики, вимоги і процедур безпеки ланцюжка постачання інформаційних технологій та управління ризиками ланцюжка постачання (К0169) **Б2.37.** Концепції вдосконалення процесів організації та моделей зрілості процесів, зокрема Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions (К0198) **Б2.38.** Концепції управління послугами для інформаційних мереж (К0200) **Б2.39.** Вимоги до постачання/закупівлі інформаційних технологій (0257) **Б2.310.** Процес			

		життєвого циклу постачання/ закупівлі (0270)			
	Б4. Здатність переглядати звіти та/чи здійснювати аудит про ефективність послуг, де вказані усі будь-які значні проблеми і відхилення, ініціюючи, у разі необхідності, коригувальні дії та гарантуючи, що усі невирішені питання будуть відстежені	**Б4.З1.** Класифікацію послуг, за якими проводиться аудит/технічний огляд чи моніторинг **Б4.З2.** Правила підготовки звітів про надані послуги відповідного спрямування **Б4.З3**. Технологію коригувальних дій стосовно усунення недоліків, направлених на підвищення якості та ефективності послуг відповідного спрямування **Б4.З4.** Порядок відстеження недоліків та невирішених питань при наданні профільних послуг **А1.З1.** Технологічні задачі і завдання управління та лідерства, пов’язані з	**Б4.У1**. Аналізувати хід надання послуг відповідного спрямування, відстежувати наявні недоліки та невирішені питання **Б4.У2**. Коригувати дії надавачів послуг стосовно усунення недоліків, направлених на підвищення якості та ефективності послуг відповідного спрямування	**Б4.К1.** Готувати пропозиції заінтересованим сторонам стосовно недопущення у подальшому виявлених недоліків та невирішених питань при наданні профільних послуг коригувальних дій стосовно усунення недоліків, направлених на підвищення якості та ефективності послуг відповідного спрямування	**Б4.В1.** Визначати рівень ефективності послуг, що надаються

		організаційними процесами, механізми вирішення проблем **А1.32**. Концепції і протоколи комп'ютерних мереж, а також методологію забезпечення безпеки мереж (К0001) **А1.33.** Методики управління ризиками (методи оцінювання та оброблення ризиків) (К0002) **А1.34**. Закони, нормативні акти, 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 (К0004) **А1.36**. Кіберзагрози та вразливості (К0005) **А1.37**. Основні операційні наслідки			

		інцидентів кібербезпеки (К0006) **А1.312**. Класифікацію програм та проєктів з інформаційних технологій у сфері кібербезпеки **А1.313**. Принципи і методи аналізу прийнятих в галузевих стандартах або в організації/на підприємстві (К0043) **А1.314**. Архітектурні концепції та загальні принципи інформаційних технологій (К0047) **А1.315**. Вимоги в рамках Загальних принципів управління ризиками (RMF) (К0048) **А1.316.** Принципи і способи управління ресурсами (К0072) **Б1.31.** Технології виробництва, комунікації та розповсюдження медійних повідомлень, а також альтернативні			

		способи інформування за допомогою текстових, мовних, візуальних повідомлень **Б1.32**. Відповідні концепції, процедури, програмне забезпечення, обладнання і прикладні технологічні програми, які застосовуються на підприємстві **Б1.33**. Вимоги до структури та змісту проведення профільного аудиту **Б1.34**. Вимоги та підходи до розроблення проєктів та програм у сфері інформаційного та кіберзахисту **Б1.35.** Сучасні підходи до оцінювання програм та проєктів з інформаційних технологій у сфері кібербезпеки **Б1.36**. Основи проєктного менеджменту			

		Б1.З6. Методи с ризиків/загроз (К0165)			
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інт відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повно-текс наукових журналів (EBSCO, JSTOR) відповідно до напрямку аудиторської діяльності; бібліотечні ресурси, архівні мат (за потреби), принтер, ксерокс, фліпчарт, методична література				
В. Підготовка пропозицій щодо покращення аудиту програм та проєктів з ІТ у сфері кібербезпеки	**В1.** Здатність розробляти методи моніторингу та оцінки ризиків, відповідності та зусиль щодо надання стійкості ІТ у сфері кібербезпеки	**В1.З1.** Методи моніторингу ризиків, відповідності та зусиль щодо надання стійкості ІТ у сфері кібербезпеки **В1.З2**. Методи і способи ефективної комунікації з партнерами та підлеглими працівниками **В1.З3.** Основи методології моніторингових досліджень **В1.З4.** Критерії оцінювання ризиків та загроз **В1.З5.** Порядок проведення моніторингу програм та проєктів відповідного спрямування	**В1.У1**. Розроблювати методи моніторингу ризиків, відповідності та зусиль щодо надання стійкості ІТ у сфері кібербезпеки **В1.У2.** Розроблювати методи оцінки ризиків, відповідності та зусиль щодо надання стійкості ІТ у сфері кібербезпеки **Б1.У4**. Розроблювати та застосовувати у практичній діяльності технічну документацію	**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 використовувати в аудиторській діяльності програмні засоби захисту комп'ютерів (програмні фільтри, антивірусні програми й антишпигунське програмне забезпечення)

		В1.З6. Програмне забезпечення відповідного спрямування	відповідного спрямування		
	В2. Здатність готувати рекомендації можливих удоскона-лень і оновлень аудиторської діяльності програм та проєктів з ІТ у сфері кібербезпеки	**В2.З1**. Порядок підготовки рекомендацій відповідного спрямування **В2.З2**. Законодавчо-нормативні акти, профільні міжнародні та вітчизняні стандарти та регламенти **В2.З3.** Підходи щодо розроблення програм та проєктів з інформаційних технологій у сфері кібербезпеки в сфері	**В2.У1.** Проводити інтерактивні тренінги для створення ефективного навчального середовища **В2.У2.** Забезпечувати розробку та виконання сценаріїв тренінгів **В2.У3.** Застосовувати концепції, процедури, програмне забезпечення, обладнання та/або технологічні прикладні програми під час навчання студентів/слухачів **В2.У4**. Готувати та проводити навчальні заняття та брифінги з обізнаності,	**В2.К1.** Сприяти дискусіям у невеликих групах **В2.К2**. Готувати та проводити брифінги з обізнаності, дотримання норм та положень щодо аудиторської діяльності та її результатів в сфері розвитку кіберзахисту керівництву, персоналу і користувачам	**В2.В1** Керувати різними систе-мами і методами елек-тронної кому-нікації

			дотримання політик і процедур безпеки користувачами систем, мереж і даних **Б1.У4**. Розроблювати та застосовувати у практичній діяльності технічну документацію відповідного спрямування		
	В3. Здатність забезпечувати постійну оптимізацію процесів аудиту та вирішення проблем його проведення	**В3.З1.** Класифікацію оптимізаційних моделей **В3.З2.** Порядок оцінювання результатів профільного аудиту **В3.З3**. Методи та засоби оцінювання результатів аудиту **В3.З4.** Вітчизняний, зарубіжний та міжнародний досвід оцінювання аудиторської діяльності відповідного спрямування	**В3.У2**. Готувати пропозиції керівництву щодо вирішення проблем проведення аудиту програм та проєктів з інформаційних технологій у сфері кібербезпеки **Б1.У4**. Розроблювати технічну документацію відповідного спрямування	**В2.К2**. Готувати та проводити брифінги з обізнаності, дотримання норм та положень щодо аудиторської діяльності та її результатів в сфері розвитку кіберзахисту керівництву, персоналу і користувачам	**В3.В1.** Проводити постійну оптимізацію процесів профільного аудиту

	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 напрямку аудиторської діяльності; бібліотечні ресурси, архівні матеріали (за потреби), принтер, ксерокс, фліпчарт, методична література				
Г. Проведення навчання та тренінгів для працівників, зайнятих в аудиті програм та проєктів з ІТ у сфері кібербезпеки	**Г1**. Здатність готувати засоби та методи короткотермінового навчання/тренінгів працівників, зайнятих в аудиті програм та проєктів з ІТ у сфері кібербезпеки	**Г1.З1**. Відповідні концепції, процедури, програмне забезпечення, обладнання і прикладні технологічні програми які застосовуються для навчання **Г1.З2**. Вимоги до структури та змісту навчальної програми **Г1.З3**. Вимоги та підходи до розроблення навчальних та методичних матеріалів **Г1.З4.** Сучасні підходи до формування навчальних програм **Б1.З1.** Технології виробництва, комунікації та розповсюдження медійних повідомлень, а також альтернативні способи інформування за допомогою	**Г1.У1.** Розроблювати або брати участь у розробці політик та протоколів для кібертренінгів у сфері аудиту програм та проєктів з інформаційної та кібербезпеки **Г1.У2**. Розроблювати або брати участь у розробці індивідуальних/колективних планів розвитку, навчання та/або вдосконалення результатів навчання **Г1.У3.** Розроблювати чіткі вказівки і навчальні матеріали	**Г1.К1.** Рекомендувати керівництву кандидатури працівників до відповідних робочих груп з профільного аудиту (Т0968) **Г1.К2**. Розроблювати тести для визначення рівня обізнаності та участі працівників щодо реалізації заходів, направлених на виконання зауважень, виявлених під час аудиторських перевірок	**Г1.В1**. Оцінювати 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)

		текстових, мовних, візуальних повідомлень	**Г1.У4**. Розроблювати або брати участь у розробці комп'ютерних навчальних модулів або курсів відповідного спрямування **Г1.У5**. Розроблювати або придбавати навчальний план, який відповідає темі та цілі на достатньому рівні **Г1.У7**. Розроблювати письмові тести для визначення рівня професійної придатності та оцінювання кваліфікації слухачів **Г1.У8**. Розроблювати критерії оцінювання результатів навчання **Г1.У9**. Брати участь у розробленні		

			правил оцінювання результатів навчання **Г1.У10**. Брати участь у розробленні внутрішніх регламентів з присвоєння/ присудження кваліфікацій слухачам		
	Г2. Здатність проводити навчання та тренінги відповідного спрямування	**Г2.З1.** Зміст навчальної програми відповідного спрямування **Г2.З2**. Особливості організації навчального процесу для різних форм набуття компетентності **Г2.З3.** Форми організації навчального процесу **Г2.З4.** Види навчальних занять **Г2.З5.** Сучасні методи, засоби та технології викладання	**Г2.У1**. Надавати технічну інформацію різним категоріям слухачів **Г2.У2.** Переглядати тренінгову документацію (документи курсу, плани занять, студентські роботи, екзамени, графіки навчання, описи курсів) **Г2.У3**. Розроблювати у необхідних обсягах	**Г2.К1**. Встановлювати ефективний зворотний зв’язок зі слухачами з метою вдосконалення навчання	**Г2.В1**. Переглядати або здійснювати аудит програм та проєктів з ІТ (Т0223)

		Г2.З6. Методи і способи організації індивідуальної та групової роботи слухачів під час навчання **Г2.З7.** Основи вікової психології, педагогіки та андрагогіки **Г2.З8.** Методи і способи ефективної комунікації **Г2.З9.** Методи соціальної інженерії **Г2.З10.** Вимоги і правила дотримання академічної доброчесності **Г2.З11.** Порядок та методи оцінювання результатів навчання **Г2.З12.** Порядок присвоєння/присуджен ня професійної/ освітньої кваліфікації **Г2.З13.** Класифікацію м оцінювання та процеду застосування на практиц	програми на сучасних мовах програмування **Г2.У4.** Використовувати у навчальній діяльності віртуальні машини (Microsoft Hyper-V, VMWare, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud) **Г2.У5.** Налаштовувати і використовувати у навчальному процесі програмні засоби захисту комп'ютерів (програмні фільтри, антивірусні програми й антишпигунське програмне забезпечення) **Г2.У6.** Використовувати інструменти та методики тестування на проникнення		

			Г2.У7. Використовувати методи соціальної інженерії **Г2.У8.** Конфігурувати і використовувати у навчальному процесі компоненти системи мережевої безпеки (мережеві екрани, віртуальні приватні мережі, системи виявлення вторгнень) **Г2.У9**. Використовувати сучасні та новітні технології у навчальних цілях (інтерактивні дошки, Web-сайти, комп'ютери, проектори) **Г2.У10**. Відображати дані в оригінальних форматах		
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп’ютерним обладнанням та оргтехнікою, доступом до мережі Інт відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повно-текс				

	наукових журналів (EBSCO, JSTOR) відповідно до напрямку аудиторської діяльності; бібліотечні ресурси, архівні мат (за потреби), принтер, ксерокс, фліпчарт, методична література

VI. Розподіл трудових функцій та компетентностей за професійними кваліфікаціями

Трудова функція (умовне позначення)	**Загальна назва професійної кваліфікації у межах професійного стандарту: аудитор інформаційних технологій (з кібербезпеки)**	
	аудитор інформа-ційних технологій (з кібербезпеки)	**провідний аудитор інформа-ційних технологій (з кібербезпеки)**
	повна	часткова додаткова
А	+	+
Б	+	+
В	+	+
Г	-	+

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 «аудитор інформаційних технологій (з 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 «аудитор інформаційних технологій (з кібербезпеки)».

VIII. Дата внесення професійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.