Проєкт

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

ПРОФЕСІЙНИЙ СТАНДАРТ

КЕРІВНИК СТРУКТУРНОГО ПІДРОЗДІЛУ З ПИТАНЬ БЕЗПЕКИ ІНФОРМАЦІЇ ТА КІБЕРЗАХИСТУ

_____(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

Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту.

II. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Виконання повноважень щодо прийняття рішень та визначення перспектив розвитку та забезпечення кіберзахисту інформаційних технологій та інформаційних систем та/або інфраструктури організації в цілому (в т.ч. критичної інформаційної інфраструктури). Управління стратегією, політиками, інформаційними ресурсами, та плануванням системи менеджменту інформаційної безпеки та/або кібербезпеки інформаційних систем і технологій та/або інфраструктури організації в цілому (іншої сфери відповідальності), включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях.

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	**Група 62.0**	Комп’ютерне програмування, консультування та пов’язана з ними діяльність

			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, н.в.і.у.
				Клас 74.90	Інша професійна, наукова та технічна діяльність, н.в.і.у.
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»

Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту, 1239.

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

Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту, 7 рівень НРК.

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

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

-081 «Право» галузі знань 08 «Право» (7 рівень НРК);

-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);

- 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).

Додатково (за необхідністю або/чи вимогою суб'єкта, уповноваженого законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій):

- документ (диплом, сертифікат, тощо), щодо післядипломної освіти та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань планування стратегічних заходів з розвитку в організації інформаційної 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 планування політики та стратегії кібербезпеки організації;
- документ (диплом, сертифікат, тощо), щодо професійної сертифікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність

до фахового виконання завдань керівника структурного підрозділу з питань безпеки інформації та кіберзахисту.

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**
Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту	Підготовка на другому рівні вищої освіти (магістерському) за спеціальностями вказаними п. II.5, стаж роботи за однією з професій відповідного спрямування повинен складати не менше 5 років	*Не передбачено професійним стандартом*

2. Професійний розвиток 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**
Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту	Підвищення кваліфікації для отримання професійної кваліфікації «Провідний фахівець з планування політики та стратегії кібербезпеки». Стаж роботи не менше п'яти років. Підвищення кваліфікації для отримання професійної кваліфікації «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту». Стаж	*Не передбачено професійним стандартом*

	роботи не менше п’яти років	

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**
А. Обґрунтування, визначення, розроблення та формування стратегії, політики, планів та процедур кібербезпеки в організації (підприємстві, установі) або програмі	**А1**. Здатність визначати, впроваджувати, повідомляти і підтримувати цілі, вимоги, стратегії, політики кібербезпеки, узгоджені з бізнес-стратегією для підтримки цілей організації	**А1.З1.** Концепції і протоколи комп'ютерних мереж, а також методології забезпечення мережевої безпеки **А1.З2**. Процеси управління ризиками (методів оцінки та зниження ризиків) **А1.З3.** Принципи та процедури забезпечення кібербезпеки і приватності даних **А1.З4**. Пріоритети та класифікацію інформаційних ресурсів організації з умов забезпечення кібербезпеки **А1.З5**. Методи та прийоми критичного мислення у кризових ситуаціях **А1.З6.** Систему вітчизняних і міжнародних стандартів, вимог та кращих світових практик у сфері інформаційної безпеки та/або кібербезпеки	**А1.У1.** Керувати та узгоджувати пріоритети безпеки ІТ зі стратегією і політиками безпеки інформації та кібербезпеки **А1.У2.** Оцінювати потреби в реалізації стратегії кібербезпеки та співпрацювати з зацікавленими сторонами з метою розробки нових політик корпоративного управління діяльністю в сфері кібербезпеки **А1.У3**. Правильно та ефективно обирати пріоритети і розподіляти інформаційні ресурси організації з метою реалізації процедур кібербезпеки	**А1.К1.** Співпрацювати над політиками та процедурами у сфері кіберприватності й кібербезпеки з та забезпечення послуг з ІТ й кібербезпеки	**А1.В1**. Переглядати і покращувати безпекові документи, звіти, угоди про рівень обслуговування, забезпечувати безпекові цілі **А1.В2**. Формувати пропозиції щодо вдосконалення законодавчих, нормативно-правових, організаційно-технічних заходів безпеки інформації та/або кібербезпеки
	А2. Здатність розробляти політику, плани і стратегії	**А2.З1**. Організаційно-правові, організаційно-технічні засади та	**А2.У1**. Розробляти, контролювати та підтримувати	**А2.К1.** Управляти безперервним нарощуванням	**А2.В1.** Визначати специфічні вимоги безпеки до системи

	безпеки інформації та кібербезпеки відповідно до законодавства, регуляторних актів, політик і стандартів на підтримку кібердіяльності організації, установи або програми	політики кіберзахисту організації **А2.32.** Закони, нормативні акти, політики і етичні норми, і як вони пов'язані з процедурами кібербезпеки і приватністю даних **А2.33**. Порядок аналізу пріоритетних методів, процедур та заходів у сфері безпеки інформації та кібербезпеки **А2.34.** Тактики, методи розробки та процедури системи менеджменту інформаційної безпеки в рамках стандартів ISO 200xx та NIST 800xx **А2.35.** Систему вітчизняних і міжнародних стандартів, вимог та кращих світових практик у сфері інформаційної безпеки та/або кібербезпеки **А2.35.** Вимоги, методи та кращі світові практики організації безперервності бізнес-операційних процесів інформаційно-комунікаційних систем та послуг організації, установи або програми в цілому	стратегічні плани реалізації встановлених задач у відповідності до політик безпеки організації, установи або програми **А2.У2**. Розробляти/інтегрувати кіберстратегію, яка окреслює бачення, місію та цілі, які узгоджені зі стратегічним планом організації, установи або проекту **А2.У3.** Розробляти та контролювати системи менеджменту інформаційної безпеки в рамках стандартів серії ISO 200xx або/чи NIST 800xx	технічного та кадрового потенціалу в організації	ІТ на всіх етапах її життєвого циклу

	А3. Здатність переглядати, планувати і розподіляти відповідні ресурси (інформаційні ресурси) організації, установи або програми	**А3.З1.** Методи/принципи контролю та управління інформаційними ресурсами організації, установи або програми згідно з розробленої і впровадженої системи менеджменту інформаційної безпеки в рамках стандартів ISO 200xx та NIST 800xx **А3.З2.** Методи/принципи управління інформаційними ресурсами інформаційно-комунікаційних згідно з встановленої стратегії та політик безпеки **А3.З3.** Мережеву інфраструктуру, базові захищені мережеві топології (зокрема, критичної інформаційної інфраструктури), мережеві ресурси та їх класифікацію згідно кращих світових практик **А3.З4.** Класифікацію та ознаки кіберзагроз, мережевих атак та методів їх реалізації з урахуванням вразливостей інформаційних ресурсів	**А3.У1.** Контролювати та управляти необхідними інформаційними ресурсами, включаючи підтримку дій керівництва, фінансові ресурси та ключовий персонал з питань безпеки для сприяння досягненню цілей та завдань безпеки ІТ на основі зниження загального ризику організації. **А1.У2.** Аналізувати кризові ситуації зі метою забезпечення суспільної та персональної безпеки, а також з точки зору захисту та управління інформаційними ресурсами. **А3.У3.** Здійснювати аналіз ризиків, техніко-економічне обґрунтування та/або компромісний аналіз для розробки, документування та уточнення стратегії, політик безпеки інформаційно-	**А3.К1.** Керувати процесами управління персоналом та безпосередньо встановлювати задачі для програмістів, проектувальників, технологів і техніків, а також іншому інженерному та науковому персоналу **А3.К2**. Брати участь у семінарах, конференціях нарадах щодо планування змін до чинних та розробки нових законодавчих, нормативно-правових, організаційно-технічних документів інформаційної та/або кібербезпеки	**А3.В1.** Реалізовувати плани удосконалення заходів роботи персоналу та процесів кіберзахисту інформаційних ресурсів в цілому **А3.В2.** Формувати аналітичні довідки щодо чинних законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки **А3.В3.** Формувати пропозиції щодо вдосконалення законодавчих, нормативно-правових, організаційно-технічних заходів інформаційної та/або кібербезпеки

		А3.З5. Методи та процедури організації кіберзмагань з захисту інформаційних ресурсів організації, як способу розвитку особистих та командних навичок шляхом надання практичного досвіду в симульованих або/чи реальних ситуаціях	комунікаційних систем та організації в цілому, функціональних вимог і специфікацій у сфері кібербезпеки.		
	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 роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				
Б. Керування процесами, процедурами впровадження та супроводження політики і стратегії кібербезпеки в організації (підприємстві, установі) або програмі	**Б1**. Здатність контролювати процеси та методи виявлення та протидії загрозам безпеці інформації, а також оцінювати вплив кіберзагроз та/або кіберінцидентів на стратегію і політики безпеки організації, установи або програми	**Б1.З1**. Основні правила, процедури та процеси для контролю, оцінки та управління ризиками у сфері кібербезпеки у відповідності до кращих світових практик та вимог. **Б1.З2.** Методів/принципи аудиту, контролю та оцінки стану інформаційних ресурсів організації, установи або програми згідно з розробленої і впровадженої системи менеджменту інформаційної безпеки в	**Б1.У1**. Інформувати керівництво, персонал про вартість безпекових заходів з захисту ІТ зацікавленим сторонам організації на всіх рівнях **Б1.У2.** Критично мислити в кризових ситуаціях (зокрема, при реалізації кіберзагроз) **Б1.У3** Керувати процесами моніторингу, контролю і оцінюванням потенційних або реалізованих кіберзагроз **Б1.У3.** Оцінювати	**Б1.К1.** Співпрацювати з ключовими зацікавленими сторонами з метою створення програми управління кіберризиками	**Б1.В1**. Застосовувати політики, стандарти чи процедури до конкретних питань

		рамках стандартів ISO 200xx та NIST 800xx **Б1.З3.** Спроможності прикладних програмних продуктів з метою виявлення або/чи блокування потенційних вразливостей інформаційно-комунікаційних систем та їх мережевого обладнання, включаючи концентратори, маршрутизатори, комутатори, мости, сервери, носії передачі і супутнє апаратне обладнання **Б1.З4.** Знання Процедури виявлення та контролю ризиків безпеки на базі прикладного програмного забезпечення спеціального призначення (програм та програмних комплексів, Open Web Application Security Project Top 10 list) **Б1.З5.** Найкращі практики управління системою менеджменту інформаційною безпекою **Б1.З6.** Зміст та порядок адаптивного планування, планування в кризових	вплив нових методів реалізації кіберзагроз або/чи новітніх технологій на нормативні документи організації, стратегії та/або політики **Б1.У4.** Організовувати та проводити внутрішній аудит бізнес-операційних процесів організації, установи або програми розробленої і впровадженої системи менеджменту інформаційної безпеки в рамках стандартів ISO 200xx та NIST 800xx (зокрема, аудит інформаційно-комунікаційної системи та її ресурсів або інфраструктури організації в цілому). **Б1.У5.** Організовувати та проводити процедури відновлення безперервності бізнес-операційних процесів інформаційно-комунікаційних систем та послуг організації,		

		умовах з урахуванням обмеження часу	установи або програми в цілому після збоїв або реалізації кібератак різних класів		
	Б2. Здатність забезпечувати ресурси (зокрема, інформаційні) організації, установи або програми для реалізації стратегії кібербезпеки	**Б2.З1.** Принципи організації та контролю процесів та процедур забезпечення бізнес-операційних процесів організації, установи або програми у відповідності до встановлених політик **Б2.З2.** Моделі зрілості інформаційно-комунікаційних систем, засобів захисту інформації, систем кібербезпеки та організації в цілому **Б2.З3.** Порядок використання методів та засобів забезпечення та класифікацію програм і проєктів з інформаційних технологій у сфері кібербезпеки **Б2.З4.** Класифікацію вразливостей прикладних приграм спеціального та загального призначення з метою управління системою забезпечення та реалізації стратегії та встановлених політик безпеки.	**Б2.У1.** Управляти процесами фінансового забезпечення, укладання контрактів та контролювати використання бюджету інформаційної безпеки, фінансування та заохочення персоналу підрозділів безпеки **Б2.У2**. Складати та впроваджувати плани реалізації стратегій, політик та процедур забезпечення бізнес-операційних процесів організації, установи або програми у сфері кібербезпеки	**Б2.К1.** Переглядати при необхідності та вдосконалювати стратегії, програми та політики з розвитку кібербезпеки, а також фінансовим забезпеченням і ціновою політикою бюджету з забезпечення інформаційної та кібербезпеки	**Б2.В1.** Розробляти, підтримувати і управляти виконанням стратегії кібербезпеки

		Б2.З5. Класифікацію загроз безпеці інформаційних ресурсів, вразливостей безпеки операційних систем різних класів, прикладного програмного забезпечення (переповнення буфера, мобільний код, міжсайтові сценарії безпеки, процедурна мова структурованих запитів [PL/SQL] та ін'єкції, перегони фронтів, прихований канал, повтор, атаки на повернення, шкідливий код та його класифікації)			
	Б3. Здатність аналізувати і впроваджувати кібербезпекові стандарти, засади, політику, правила, закони, сертифікації та найкращі методи (NIST, ENISA)	**Б3.З1.** Ефективність використання засобів кібербезпеки в організації з метою гарантованого підтвердження того, що вони забезпечують необхідний рівень захисту **Б3.З2.** Стандарти кібербезпеки та приватності, засад, політик, положень, законодавства, сертифікацій та найкращих світових практик (NIST, ENISA)	**Б3.У1.** Переглядати стандарти політики та стратегії її впровадження, щоб забезпечити відповідність процедур та настанов політикам кібербезпеки **Б3.У2.** Застосовувати судження, коли політики інформаційної безпеки визначені некоректно. **Б3.У3** Застосовувати навички критичного читання/мислення	**Б3.К1.** Брати участь у розробленні стандартів, нормативних документів, положень та правил у сфері кібербезпеки	**Б1.В1**. Призначати та керувати групу експертів або/чи формувати групу внутрішніх аудиторів з безпеки інформаційних технологій або\чи системи менеджменту інформаційної безпеки

		Б3.З3. Порядок абезпечення підтримання та управління політикою (правилами) безпеки, процесами та процедурами, які використовуються для управління захистом інформаційних систем і активів організації			
	Б4. Здатність інтерпретувати і застосовувати закони, нормативні акти, політики та методології, що стосуються кіберцілей організації	**Б4.З1**. Нормативно-правову базу у сфері безпеки інформації та кіберзахисту, як правильно та ефективно обирати пріоритети і розподіляти ресурси кібербезпеки **Б4.З2.** Чинні вітчизняні закони, нормативні акти, директив, постанови у сфері кібербезпезпеки **Б4.З3.** Методи та принципи аналізу кіберзагроз в організації	**Б4.У1.** Організовувати опублікування настанов із захисту комп'ютерної мережі (TCNO, концепції операцій, звіти мережевих аналітиків, NTSM, MTO) для зацікавлених сторін підприємства **Б4.У2.** Застосовувати в роботі навичку обізнаності про методи та порядок розроблення та впровадження інформаційної інфраструктури у відповідності до законодавчої та нормативної бази країни	**Б4.К** Забезпечувати практичні вирішення проблем кібербезпеки	**Б4.В1.** Надавати постійно оцінку стану кібербезпеки організації та вдосконалення практик кіберзахисту
	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 роботи; бібліотечні ресурси, архівні матеріали (за потреби);				

	лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				
В. Консультування вищого керівництва щодо рівня ризику та стану безпеки, аналізу витрат/зисків, програм, політик, процесів, систем та елементів інформаційної безпеки та кібербезпеки	**В1.** Здатність готувати і представляти бачення, стратегії та політики кібербезпеки для затвердження вищим керівництвом організації, а також забезпечувати їх виконання	**В1.З1.** Потенційні вразливості кібербезпеки в галузевих технологіях та як формувати звітність з метою інформування керівництва та персонал **В1.З2.** Витрати/вигоди програм, політик, процесів, систем та елементів інформаційної безпеки та кібербезпеки **В1.З3.** Засоби аудиту та контролю безпеки інформації та кіберзахисту, а також формати їх оформлення та сповіщення про це з метою інформування керівництва, персонал та проведення консультацій для зацікавлених сторін **В1.З4.** Засади та кращі світові практики управління ризиками	**В1.У1**. Наглядати або керувати захисними чи коректувальними заходами при виявленні кіберінциденту або вразливості. **В1.У2.** Формувати відповідну звітність **В1.У3.** Виконувати оцінювання ризиків інформаційної безпеки та обґрунтовувати методи їх зменшення з урахуванням рішення власника інформаційних ресурсів або\чи керівника організації, установи або програми	**В1.К1.** Взаємодіяти з зовнішніми організаціями (наприклад, службою зі зв'язку з громадськістю, правоохоронними органами, провідними інспекторами командних служб або компонентів кібербезпеки) для забезпечення належного та точного розповсюдження фактів про інцидент та інших відомостей про процеси кіберзахисту інформаційних ресурсів	**В1.В1.** Розроблювати вказівки і настанови для працівників, залучених до розроблення стратегій, програм та політик з розвитку кібербезпеки
	В2. Навчати вище керівництво щодо методів та засобів розрахунку та оформлення документації	**В2.З1**. Методи та методики навчання у відповідності до напрямів розробки та впровадження системи менеджменту інформаційної безпеки,	**В2.У1.** Рекомендувати плани дій та етапів або плани відновлення для усунення вразливостей, які були виявлені під час оцінки ризиків,	**В2.К1.** Сприяти підвищенню обізнаності керівництва щодо ситуацій безпеки та забезпечувати	**В2.В1.** Керувати методами електронної комунікації із застосуванням

	кібербезпекових ризиків (кіберзагроз або\чи кіберінцидентів з урахуванням їх впливу на організацію в цілому	виникаючих ризиків безпеки для організації **В2.З2.** Методи та методики навчання у відповідності до різних класів кіберзагроз та вразливостей інформаційних ресурсів **В2.З3.** Технологічні задачі і завдання управління та керівництва, пов'язані з процесами і рішенням організаційно-технічних та нормативно-правових питань (проблематики) організації	аудиторських та інспекторських перевірок тощо **В2.У2.** Прогнозувати нові загрози для ІТ та безпеки інформаційних ресурсів з урахуванням консультування та навчання керівництва і зацікавлених сторін	належні принципи безпеки в баченні та цілях організації	різних методів, методик та систем
	В3. Інформувати вище керівництво про кібербезпекові інциденти, ризики, формувати висновки.	**В3.З1.** Конкретні бізнес-операційні наслідки в результаті помилок у політиці та стратегії з кібербезпеки, необхідні для інформування вищого керівництва про кібербезпекові інциденти, ризики, формувати висновки	**В3.У1.** Комунікувати з керівниками всіх рівнів, включаючи членів правління (наприклад, навички міжособистісного спілкування, доступність, уміння ефективно сприймати мову виступаючих, відповідне аудиторії використання стилю і мови виступу)	**В3.К1.** Надавати керівництву та персоналу пояснення з розробки та впровадження нових інформаційних технологій та методології з розвитку в організації у сфері кібербезпеки	**В3.В1** Впливати на культуру кібербезпеки організації (NIST, ENISA)
	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 конструювання; бібліотечні ресурси, архівні матеріали (за потреби); законодавчо-нормативні акти, акти роботодавця відповідного спрямування				

Г. Співпраця із зацікавленими сторонами з метою забезпечення безперервної діяльності організації (підприємства, установи) в рамках програми, стратегії та виконання завдань політики безпеки	**Г1**. Здатність проводити заходи з довгострокового стратегічного планування за участю внутрішніх і зовнішніх партнерів	**Г1З1**. Класифікацію та методи, методики реалізації програм та проєктів з інформаційних технологій у сфері кібербезпеки **Г1З2.** Етичні вимоги організації кібербезпеки (NIST, ISACA, ENISA) **Г1З3.** Методику присвоєння пріоритетів інформаційних потреб	**Г1У1.** Визначати та/або впроваджувати політики, методи та процедури кіберзахисту критичної інфраструктури **Г1У2**. Використовувати критичне мислення при аналізі організаційних моделей і взаємозв'язків	**Г1.К1**. Співпрацювати з фахівцями із кібербезпеки в процесі оцінки ризиків безпеки для вирішення питань дотримання приватності та зменшення ризиків	**Г1.В1**. Передбачати необхідні зміни у стратегії кібербезпеки
	Г2. Здатність розвивати відносини з органами та громадами, що займаються кібербезпекою (NIST, ENISA)	**Г2З1**. Вимоги і процедури для встановлення зв'язків між стратегією, бізнесом і технологією в контексті динаміки розвитку та надання послуг організацією.	**Г2У1.** Співпрацювати із зацікавленими сторонами з кадрових питань організації з метою забезпечення відповідного розміщення та розподілу кадрових ресурсів **Г2У2.** Адаптувати технічну та планувальну інформацію до рівня розуміння замовника	**Г1.К1**. Співпрацювати з ключовими зацікавленими сторонами з метою створення програми управління кіберризиками та кіберінцидентами	**Г2.В1**. Застосовувати на практиці етичні вимоги щодо організації кібербезпеки (NIST, ENISA).

	ГЗ. Здатність комунікувати, координувати і співпрацювати із внутрішніми і зовнішніми зацікавленими сторонами	**ГЗ.З1.** Основні організаційні бізнес-процеси для встановлення відповідних комунікаційних зав'язків, координації і співпраці із внутрішніми і зовнішніми зацікавленими сторонами **ГЗ.З2.** Порядок аналізу принципів управління ризиками та інформаційними ресурсами в рамках співпраці з зацікавленими сторонами	**ГЗ.У1**. Оцінювати і покращувати рівень кібербезпеки організації в рамках співпраці з зацікавленими сторонами (NIST, ENISA) **ГЗ.У2**. Розробляти та встановлювати політики процедур управління інцидентами та координації аналізу принципів управління ризиками та інформаційними ресурсами в рамках співпраці з зацікавленими сторонами	**ГЗК1.** Управляти міждисциплінар-ними групами з кібербезпеки та захисту іфнормації (NIST, ENISA)	**ГЗ.В1.** Управляти ресурсами кібербезпеки
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідн програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журн (EBSCO, JSTOR) відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				

IV. **Розподіл трудових функцій та компетентностей за професійними кваліфікаціями**

Трудова функція (умовне позначення)	**Загальна назва професійної кваліфікації у межах професійного стандарту: Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту**
	Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту
	повна
А	+
Б	+
В	+
Г	+

VII. Відомості про розроблення та затвердження професійного стандарту

1. Повне найменування розробника професійного стандарту

Державна служба спеціального зв’язку та захисту інформації України

Склад робочої групи/Учасники робочої групи:

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

БОНДАРЕНКО Іван Дмитрович, доцент кафедри кібербезпеки Науково-навчального інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України;

ВАВІЛЕНКОВА Анастасія Ігорівна, завідувач кафедри кібербезпеки Науково-навчального інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України;

ВОЗНЕНКО Людмила Іванівна, викладач спеціальних технологій, голова методичної комісії ІТ Київського професійного коледжу з посиленою військовою та фізичною підготовкою;

ВОЛКОВА Ксенія Миколаївна, заступник начальника / управління правового співробітництва з міжнародними організаціями Департаменту міжнародного права Міністерства юстиції України;

ВОЛОШКОВА Лада Миколаївна, заступник директора з навчально-виховної роботи, викладач спеціальних технологій Київського професійногоколеджу з посиленою військовою та фізичною підготовкою;

ДІДИК Валерія Анатоліївна, керівник напряму з розвитку професійних вавичок з кібербезпеки Проєкту Ю5АШ» «Кібербезпека критично важливої інфраструктури України»;

КИРИЧЕНКО Сергій Васильович, майстер виробничого навчання, викладач спеціальних технологій Київського професійного коледжу з посиленою військовою та фізичною підготовкою;

КОНОНОВИЧ Володимир Григорович, доцент кафедри кібербезпеки та технічного захисту інформації факультету інформаційних технологій та кібербезпеки Державного університету інтелектуальних технологій і зв'язку;

КОРНІЄНКО Богдан Ярославович, професор кафедри інформаційних систем та технологій факультету інформатики та обчислювальної техніки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;

КОТЕТУНОВ Віктор Юрійович, провідний науковий співробітник 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;

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

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.С. Пухова Національної академії наук України;

НЕВАРА Лілія Михайлівна, керівник навчально-методичного центру, голова профспілкової організації Громадської організації «Українська академія кібербезпеки»;

ОВЧАРЕНКО Олександр Віталійович, майстер виробничого навчання, викладач спеціальних технологій Київського професійного коледжу з посиленою військовою та фізичною підготовкою;

ПАЗЮК Андрій Валерійович, віце-президент Громадської організації «Українська академія кібербезпеки»;

ПУГАЧОВ Олександр Павлович, викладач спеціальних технологій Жиївського професійного коледжу з посиленою військовою. та фізичною підготовкою;

СТИРАН Володимир Сергійович, заступник начальника центру -начальник 8 управління Державного центру кіберзахисту Держспецзв'язку;

СУПРУН Ольга Миколаївна, головний науковий співробітник відділу науково-технічної експертизи Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

ТИХОНОВА Олена Вікторівна, професор кафедри економічної безпеки та фінансових розслідувань Національної академії внутрішніх справ;

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

ФІЛІППОВА Ольга Валентинівна, комерційний директор компанії «САЙКОМ»;

ШЕСТАКОВ Валерій Іванович, заступник директора (з навчальної та наукової роботи) Науково-навчального інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України;

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

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 «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту» 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 «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту».

VIII. Дата внесення професійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.