Проєкт

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

Професійний стандарт

КІБЕРОПЕРАТОР

_____(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

Кібероператор

ІІ. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Здійснення збору, оброблення та/або геолокації систем для експлуатації, пошуку та/або відстеження цілей, що представляють інтерес. Виконання мережевої навігації, тактичного криміналістичного аналізу і, у випадку поставленої задачі, участь у виконанні операцій в мережі.

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	Назва секції	№ розділу	Назва розділу	№ групи (класу)	Назва групи (класу)
Секція J	Інформація та телекомуніка-ції	**Розділ 61**	Телекомунікації (електрозв'язок)	**Група 61.1**	Діяльність у сфері проводового електрозв'язку
				Клас 61.10	
				Група 61.2	Діяльність у сфері безпроводового електрозв'язку
				Клас 61.20	
				Група 61.9	Інша діяльність у сфері електрозв'язку
				Клас 61.90	
		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 устаткованням
				Клас 62.09	Інша діяльність у сфері інформаційних технологій і комп'ютерних систем

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

Кібероператор, 4113

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

Кібероператор, 5 рівень НРК

Старший кібероператор, 5 рівень НРК

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

- диплом фахового молодшого бакалавра на рівні фахової передвищої освіти за спеціальністю:

- 125 «Кібербезпека та захист інформації» галузі знань «Інформаційні технології» (5 рівень НРК);

- 126 «Інформаційні системи та технології» галузі знань «Інформаційні технології» (5 рівень НРК);

- 172 «Електронні комунікації та радіотехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (5 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 збору, оброблення та/або геолокації систем для експлуатації, пошуку та/або відстеження цілей, що представляють інтерес;

- документ (диплом, сертифікат, тощо), щодо професійної сертифікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері збору, оброблення та/або геолокації систем для експлуатації, пошуку та/або відстеження цілей, що представляють інтерес.

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**
Кібероператор, старший кібероператор	Підготовка на другому рівні вищої освіти (магістерському) за спеціальностями вказаними у п.5, галузі знань 12	*Не передбачено професійним стандартом*

	«Інформаційні технології» та 17 «Електроніка, автоматизація та електронні комунікації», 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**
Старший кібероператор	Підвищення кваліфікації для кібероператора для отримання професійної кваліфікації "старший кібероператор". Стаж роботи не менше двох років	*Не передбачено професійним стандартом*

IV. Абревіатури, скорочення

IT	інформаційні технології
GUI	Graphical User Interface
TCP/IP	Transmission Control Protocol/ Internet Protocol
DNS	Domain Name System
EBSCO	Elton Bryson Stephens Company
JSTOR	Journal Storage
SSL	Secure Sockets Layer
PGP	Pretty Good Privacy
WLAN	Wireless Local Area Network
LTE	Long Term Evolution

CDMA	Code Division Multiple Access
GSM/EDGE	Global System for Mobile Communications /Enhanced Data Rates for GSM Evolution
UMTS/HSPA	Universal Mobile Telecommunications System/High Speed Packet Access
RADIUS	Remote Authentication in Dial-In User Service
FTP	File Transfer Protocol
DHCP	Dynamic Host Configuration Protocol
SNMP	Simple Network Management Protocol
VPN	Virtual Private Network

V. Опис трудових функцій

Трудові функції	**Компетентності**	**Результати навчання**			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
А. Проведення підготовчих робіт до проведення кібероперативної діяльності	**А1**. Здатність проводити підготовчі роботи до подальшого збору, обробки та /або геолокації інформаційних систем для експлуатації, пошуку та/або відстеження цілей, що представляють інтерес	**А1.З1.** Технологічні задачі і завдання, пов'язані з організаційними процесами, механізми вирішення проблем **А1.З2**. Концепції і протоколи комп'ютерних мереж, а також методологію забезпечення безпеки мереж **А1.З3.** Методики управління ризиками (методи оцінювання та оброблення ризиків) **А1.З4**. Закони, нормативні акти, політики і етичні норми, та як вони пов'язані з конфіденційністю	**А1.У1.** Аналізувати внутрішню операційну архітектуру, інструменти та процедури для визначення способів підвищення їх продуктивності **А1.У2.** Застосовувати знання, включаючи методики технічної документації (наприклад, сторінку Wiki) **А1.У3**. Виконувати програмування на відповідних мовах (наприклад, «С++», Python тощо) **А1.У4**. Застосувати принципи кібербезпеки і приватності при формуванні	**А1.К1.** Приймати участь у надаванні доступу до бездротових комп'ютерних і цифрових мереж	**А1.В1**. Формувати й оновлювати базу знайдених матеріалів для подальшого її використання в роботі **А1.В2**. Документувати та оновлювати за необхідності усі напрямки роботи, пов'язані з кібероперацій-ною діяльністю

		персональних даних та кібербезпекою **А1.35**. Принципи забезпечення конфіденційності персональних даних та кібербезпеки **А1.36**. Методи автентифікації, авторизації та контролю доступу **А1.37**. Нові та ті, що розроблюються технології інформаційної та кібербезпеки **А1.38.** Технологічні вимоги до документації відповідного спрямування **А1.39**. Досвід передових вітчизняних і зарубіжних підприємств щодо проведення кібероперацій **А1.310**. Класифікацію кіберзагроз та вразливостей	організаційних вимог (які стосуються конфіденційності, цілісності, доступності, автентифікації і неспростовності)		

		А1.З11. Операційні наслідки в результаті помилок кібербезпеки **А1.З12**. Вразливості прикладних приграм **А1.З13**. Нові та виникаючі ІТ та технології кібербезпеки **А1.З14**. Основну структуру, архітектуру та проєкти сучасних мереж зв'язку			
	А2. Здатність готувати інструментарії до збирання даних відповідного спрямування з відкритих джерел за допомогою різних онлайн-інструментів	**А2.З1.** Принципи управління життєвим циклом системи кіберзахисту, включаючи забезпечення безпеки та експлуатаційної придатності програмного забезпечення **А2.З2**. Резервне копіювання та відновлення даних **А2.З3.** Мережеві протоколи **А2.З4**. Стандарти й технічні умови, які використовуються під	**А2.У1**. Використовувати віддалений командний рядок та графічний інтерфейс користувача (GUI) **А2.У2** Здійснювати зворотній інжиніринг розробки (наприклад, hex editing, утиліти бінарної компресії, налагодження та аналіз рядків) з метою визначення функцій і належності видалених інструментів **А2.У3.** Адмініструвати сервери	**А2.К1.** Формувати запити на профільну інформацію **А2.К2**. Аналізувати потреби та вимоги користувачів для планування проведення кібероперацій	**А2.В1.** Проводити оцінювання ефективності існуючих програм, процесів і вимог щодо проведення кібероперацій

		час проведення кібероперацій **А2.35**. Комп'ютерні алгоритми **А2.36.** Алгоритми шифрування **А2.37.** Мови програмування низького рівня (наприклад, асемблер) **А2.38.** Фізичні компоненти і архітектури комп'ютера, включаючи функції різних компонентів і периферійних пристроїв (наприклад, процесорів, мережевих адаптерів, сховищ даних) **А2.39.** Організації-замовники, включаючи їх інформаційні потреби, цілі, структури, можливості тощо **А2.310**. Вплив безпеки на конфігурації програмного забезпечення			

		А2.З11. Спеціалізовані мови цілі (наприклад, скорочення, жаргон, технічні терміни, кодові слова) **А2.З12**. Загальні мережеві протоколи та протоколи маршрутизації (наприклад, TCP/IP), послуги (наприклад, веб-пошти, DNS) та їх взаємодію для забезпечення мережевих зв'язків			
	А3. Здатність проводити підготовчі заходи щодо геолокації інформаційних систем для експлуатації, пошуку та/або відстеження цілей, що представляють інтерес	**А3.З1.** Процеси управління зборами, спроможностей і обмежень **А3.З2.** Закони, політики, процедури чи корпоративне управління, що стосуються проведення геолокації інформаційних систем **А3.З3.** Концепції системного адміністрування операційних систем (Unix/Linux, IOS,	**А3.У1.** Редагувати або виконувати прості скрипти (наприклад, Perl, VBScript) в ОС Windows і UNIX **А3.У2.** Інтерпретувати і перетворювати вимоги замовника в оперативні дії **А3.У3.** Моніторити операції системи і реагувати на події у відповідь на тригери та/або спостереження за трендами або незвичайною діяльністю	**А2.К1.** Формувати запити на профільну інформацію	**А3.В1.** Проводити підготовчі заходи щодо геолокації інформаційних систем для проведення відповідних засобів

		Android і Windows тощо) **А3З4.** Процедури аудиту та логування (включаючи серверне логування) **А3З5.** Концепції програмування (наприклад, рівні, структури, мови з компіляцією або інтерпретацією) **А3З6.** Основне прикладне програмне забезпечення (наприклад, сховища даних і резервного копіювання, прикладних баз даних), а також типи вразливостей, які виявлені в цих прикладних програмах **А3З7.** Вразливості бездротових прикладних програм **А3.З8**. Системи баз даних **А3.З9.** Окремі розділи математики (логарифмів, тригонометрії,			

		лінійної алгебри, математичного аналізу, статистики і операційного аналізу) **А3.З10.** Концепції технології віддаленого доступу **А3.З11.**Технологію побудови програмного забезпечення щодо геолокації інформаційних систем			
	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. Здійснення обробки геолокації інформаційних систем експлуатації, пошуку та/або відстеження цілей, представляють інтерес	**Б1.** Застосовувати мережеві пристрої, пристрої захисту та/або термінали з використанням різних методів або засобів	**Б1.З1**. Криптологічні характеристики, обмеження і внескок у кібероперації **Б1.З2.** Наявне програмне забезпечення та методологю активного захисту та системного зміцнення **Б1.З3.** Алгоритми шифрування і кіберможливостей/	**Б1.У1.**Спрощувати доступ за допомогою фізичних і/або безпровідних засобів **Б1.У2.** Підтримувати ситуаційну обізнаність і функціональність органічної операційної інфраструктури **Б1.У3**. Здійснювати експлуатацію та підтримку автоматизованих систем для отримання і	**Б1.К1.** Надавати інформацію про геолокацію в режимі реального часу, використовуючи інфраструктуру цілі	**Б1.В1**. Документувати та оновлювати за необхідності усі напрямки діяльності, пов'язані з кібероперацій-ною діяльністю

		інструментів (наприклад, SSL, PGP) **Б1.З4.** Стратегії і методики ухилення **Б1.З5**. Порядок та системи управління інформацією всього підприємства **Б1.З6**. Супутникові систем зв'язку **Б1.З7**. Структуру, методи і стратегії застосування інструментів експлуатації (наприклад, сніфери, клавіатурне перехоплення) та відповідні методики (наприклад, отримання доступу через бекдор, збір/ вилучення даних, аналіз вразливостей інших систем у мережі)	здійснення доступу до цільових систем **Б1.У4**. Ідентифікувати пристрої, що працюють на кожному рівні моделей протоколів		
	Б2. Здатність збирати та оброблювати дані, передані через бездротові комп'ютерні і цифрові мережі	**Б2.З1**. Теорію баз даних **Б2.З2**. Звітність щодо усунення конфліктних ситуацій, включаючи взаємодію із	**Б2.У1**. Оброблювати відфільтровані дані, призначені для аналізу та/або розповсюдження між замовниками	**Б2.К1.** Надавати актуальні геоінформаційні дані в режимі реального часу	**Б2.В1.** Документувати заходи зі збору інформації та/або підготовку

		зовнішніми організаціями **Б2.З3.** Алгоритми і інструменти шифрування для бездротових локальних мереж (WLAN)	**Б2.У2.** Аналізувати дані, зібрані з термінальної мережі або мережевого середовища **Б2.У3**. Аналізувати внутрішні та зовнішні зв'язки цілі, зібраних з бездротових локальних мереж **Б2.У4**. Збирати (наприклад, системи пошуку файлів) і аналізувати дані **Б2.У5.** Оброблювати зібрані дані для подальшого аналізу **Б2.У6**. Використовувати різні інструменти з різних відкритих джерел для збору даних (он-лайн торгівля, DNS, електронна пошта, тощо) **Б2.У7.** Аналізувати створення шаблонів і геолокації бездротових мереж цілі **Б2.У8**. Застосовувати на практиці тактики, методи та процедури збору даних в мережі, включаючи можливості/інструменти дешифрування		середовища щодо цілей протягом проведення операцій, спрямованих на досягнення кіберефектів **Б2.В2.** Обстежувати, збирати та аналізувати метадані бездротової локальної мережі

			Б2.У9. Проводити процедури бездротового збору даних, включаючи можливості/інструменти дешифрування		
В. Виконання процедур мережевої навігації, тактичного криміналістич-ного аналізу і, у випадку поставленої задачі, здійснення операцій в кіберпросторі	**В1**. Здатність проводити мережеву розвідку і аналіз вразливостей систем у мережі	**В1.З1.** Принципи взаємодії людина-комп'ютер **В1.З2.** Процес оцінки стану безпеки і процесу авторизації **В1.З3.** Архітектуру мобільного стільникових зв'язку (наприклад, LTE, CDMA, GSM/EDGE і UMTS/HSPA) **В1.З4.** Засоби безпеки на хостах, і те, як ці засоби впливають на експлуатацію та зниження вразливостей **В1.З5.** Порядок впровадження ОС Unix і Windows, які надають послуги автентифікації і логування (протокол RADIUS), DNS-служби, електронну пошту, Web-послуги,	**В1.У1**. Виявляти сильні сторони та вразливості мережі **В1.У2.**Здійснювати експлуатацію бездротових комп'ютерних і цифрових мереж **В1.У3.** Визначати встановлені патчі на різних операційних системах та ідентифікувати патч-сигнатури	**В1.К1.** Надавати актуальні геоінформаційні дані в режимі реального часу	**В1.В1**. Проводити заходи в мережі та за її межами з метою контролю і отримання даних з розгорнутих автоматизова-их технологій

		FTP-сервера, DHCP-протоколу, мережевого екрану і SNMP- протоколу **Б1.З5**. Порядок та системи управління інформацією всього підприємства **Б2.З2**. Звітність щодо усунення конфліктних ситуацій, включаючи взаємодію із зовнішніми організаціями			
	В2. Здатність розгортати інструменти проти цілі та здійснювати їх утилізацію відразу після використання	**В2.З1.** Методи автентифікації доступу **В2.З2**. Класифікацію та номенклатуру шкідливих програм **В2.З3**. Фізичні та логічні мережеві пристрої та інфраструктуру, включаючи концентратори, комутатори, маршрутизатори, брандмауери тощо **Б1.З5**. Порядок та системи управління	**В2.У1.** Перевіряти цілісність всіх файлів (наприклад, контрольні суми, виключне АБО, безпечне хешування, контрольні обмеження тощо) **В2.У2.** Використовувати моделі системи безпеки (наприклад, модель Белла-Лападули, моделі забезпечення цілісності «Biba» і Кларка-Вілсона) **В2.У3**. Використовувати інструменти, методики і процедури для віддаленої експлуатації та	**В2.К1.** Приймати участь у розробленні вказівок і настанов для працівників, залучених до кібероперацій діяльності	**В2.В1.** Інтерпретувати результати, отримані сканером вразливостей, з метою виявлення вразливостей

		інформацією всього підприємства **Б2.З2**. Звітність щодо усунення конфліктних ситуацій, включаючи взаємодію із зовнішніми організаціями	забезпечення утримання на цілі		
	В3. Здатність здійснювати кібердіяльність з метою руйнування/ видалення інформації, що міститься в комп'ютерах і обчислювальних мережах	**В3.З1.** Технічну документацію відповідного спрямування **В3.З2**. Порядок адміністрування мереж **В3.З3.** Будову і топології мережі **Б1.З5**. Порядок та системи управління інформацією всього підприємства **Б2.З2**. Звітність щодо усунення конфліктних ситуацій, включаючи взаємодію із зовнішніми організаціями	**В3.У1.** Виявляти експлойти проти цільових мереж і хостів, та реагувати відповідним чином **В3.У2.** Аналізувати дампи пам'яті з метою вилучення інформації **В3.У3.** Оцінювати сучасні засоби з метою визначення необхідності їх подальшого вдосконалення виявлення вторгнень **В3.У4.** Витягувати інформацію з перехоплених IP-пакетів	**В3.К1.** Приймати участь у розробленні вказівок і настанов для працівників, залучених до кібероперацій-ної діяльності з метою руйнування/ видалення інформації, що міститься в комп'ютерах і обчислювальних мережах	**В3.В1**. Проводити аудит мережевих екранів, периметрів, маршрутиза-торів і систем
	В4. Здатність тестувати інструменти і методики,	**В4.З1**. Вимоги до конфіденційності,	**В4.У1.**Тестувати і оцінювати локально	**В4.К1.** Надавати керівництву	**В4.В1.** Приймати

	розроблені всередині організації, проти інструментів цілі	цілісності та доступності **В4.З2.** Програмне забезпечення з підтримки кібербезпеки **В4.З3.** Методи і методики, що використовуються для виявлення різних дій з експлуатації **В4.З4.** Структуру і компоненти ОС Unix/Linux і Windows (наприклад, управління процесами, структура каталогів, вбудовані прикладні програми) **В4.З5.** Технологію віртуальних машин **Б1.З5**. Порядок та системи управління інформацією всього підприємства	розроблені засоби з метою їх оперативного використання **В4.У2.** Приймати участь у розробленні та тестуванні нових методик для отримання і підтримки доступу до цільових систем **В4.У3.** Тестувати і оцінювати інструменти для впровадження **В4.У4.** Визначати необхідний рівень складності тесту для конкретної системи **В4.У5.** Використовувати пристрої віртуальних приватних мереж (VPN**)** і шифрування **В4.У6.** Готувати плани проведення тестування **В4.У7**. Приймати участь в розробленні відповідної технічної документації	пояснення по процедурам мережевої навігації, тактичного криміналістич-ного аналізу	участь у підготовці рекомендацій щодо поліпшення на підприємстві установі/ організації кіберопера-ційної діяльності
	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				

Г. Здійснення заходів зі збору доказів щодо кримінальних та іноземних розвідувальних органів з метою пом'якшення можливих або реальних загроз, захисту від шпигунства чи інсайдерської загрози, іноземного саботажу, міжнародної терористичної діяльності або для підтримки іншої розвідувальної діяльності	**Г1.** Здатність здійснювати заходи щодо збору доказів щодо кримінальних та іноземних розвідувальних органів з метою пом'якшення можливих або реальних загроз, захисту від шпигунства чи інсайдерської загрози, іноземного саботажу та міжнародної терористичної діяльності	**Г1.З1**. Умови та порядок проведення криміналістичної експертизи структури і функцій операційної системи **Г1.З2**. Класифікацію загроз, шляхів захисту від шпигунства чи інсайдерської загрози, іноземного саботажу, міжнародної терористичної діяльності або для підтримки іншої розвідувальної діяльності **Г1.З3**. Методологію та процедуру збору доказів щодо кримінальних та іноземних розвідувальних органів	**Г1.У1.** Збирати відповідні докази щодо кримінальних та іноземних розвідувальних органів **Г1.У2**. Проводити криміналістичну експертизу структури і функцій операційної системи **Г1.У3**. Аналізувати та надавати рекомендації щодо щодо пом'якшення можливих або реальних загроз, захисту від шпигунства чи інсайдерської загрози, іноземного саботажу, міжнародної терористичної діяльності або для підтримки іншої розвідувальної діяльності	**Г1. К1.** Інформувати керівництво про результати проведених заходів відповідного спрямування **Г1.У2.** Взаємодіяти у відповідній роботі з профільними працівниками та членами команди	**Г1.В1**. Готувати звіти та рапорти про результати проведених заходів відповідного спрямування
	Г2. Здатність здійснювати заходи щодо підтримки розвідувальної діяльності	**Г2.З1**. Принципи, політики, процедури і засоби розвідувальної звітності, включаючи	**Г2.У1.** Приймати участь у підготовчих заходах для проведення розвідувальної діяльності	**Г2.К1.** Взаємодіяти у роботі з підтримки іншої	**Г2.В1**. Готувати звіти та рапорти

		формати звітів, критерії звітності (вимоги і пріоритети), практики розповсюдження і юридичні повноваження та обмеження **Г2.З2**. Фундаментальні основи цифрової криміналістики для отримання дієвої розвідки	**Г2.У2**. Приймати безпосередню участь у заходах відповідного спрямування	розвідувальної діяльності із профільними працівниками та членами команди	про результати проведених заходів відповідного спрямування
	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				

VI. Розподіл трудових функцій та компетентностей за професійними кваліфікаціями

Трудова функція (умовне позначення)	Загальна назва професійної кваліфікації у межах професійного стандарту: кібероператор	
	кібероператор	старший кібероператор
	повна	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» (за згодою);

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;

ФІЛІПОВА 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 «кібероператор» 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 «кібероператор».

VIII. Дата внесення професійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.