

ЗАТВЕРДЖЕНО

Наказ Адміністрації Держспецзв'язку

25 листопада 2022 року № 715

**Професійний стандарт
«Інструктор-методист з інформаційної безпеки та кібербезпеки»**

1. Загальні відомості професійного стандарту**1.1. Основна мета професійної діяльності**

Надання освітніх, консультативних і методичних послуг у сфері інформаційної безпеки та кібербезпеки.

1.2. Назва виду економічної діяльності, секції, розділу, групи та класу економічної діяльності та їхній 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 провідного електрозв'язку
				Клас 61.10	Діяльність у сфері провідного 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	Консультування з

				62.02	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, н.в.і.у.
				Клас 74.90	Інша професійна, наукова та технічна діяльність, н.в.і.у.
Секція Р	Освіта	Розділ 85	Освіта	Група 85.5	Інші види освіти
				Клас 85.59	Інші види освіти, не введенні в інші угруповання

1.3. Назва виду професійної діяльності та її код (згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій»)

Розділ	Клас	Підклас
2	235	2359
Професіонали	Інші професіонали в галузі освіти та навчання	Інші професіонали в галузі освіти та навчання

1.4. Назва професії (професійної назви роботи) та її код (згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій»)

Інструктор-методист з інформаційної безпеки та кібербезпеки 2359.2.

1.5. Професійна кваліфікація

Інструктор-методист з інформаційної безпеки та кібербезпеки (трудова функція А, Б, В, Г).

Провідний інструктор-методист з інформаційної безпеки та кібербезпеки (трудові функції А, Б, В, Г, Д).

1.6. Місце професії (посади, професійної назви роботи) в організаційно-виробничій структурі підприємства (установи, організації)

Обіймає посаду інструктора-методиста з інформаційної безпеки та кібербезпеки, провідного інструктора-методиста з інформаційної безпеки та кібербезпеки.

Інструктор-методист з інформаційної безпеки та кібербезпеки, провідний інструктор-методист з інформаційної безпеки та кібербезпеки безпосередньо підпорядкований керівнику профільного структурного підрозділу (або уповноваженій особі) в структурних підрозділах підприємства/організації, профільних структурних підрозділах підприємства/організації із захисту інформації та кібербезпеки, профільних науково-дослідних установах, закладах освіти, навчальних центрах, які реалізують або застосовують функції надання освітніх, консультативних і методичних послуг у сфері інформаційної безпеки та кібербезпеки.

Робоче місце розташовано у приміщенні (кабінеті, кімнаті, лабораторії) відповідного освітнього центру/закладу освіти/інституції/організації/установи.

1.7. Умови праці

Тривалість робочого часу та часу відпочинку – згідно з чинним законодавством, графіками роботи та відпочинку, правилами внутрішнього трудового розпорядку, колективним договором.

Відпустки надаються згідно до чинного законодавства, колективним договором, графіками надання відпусток та за результатами атестації робочого місця за умовами праці.

1.8. Документи, що підтверджують професійну та освітню кваліфікацію, її віднесення до рівня Національної рамки кваліфікацій (НРК)

Для кваліфікацій «Інструктор-методист з інформаційної безпеки та кібербезпеки» і «Провідний інструктор-методиста з інформаційної безпеки та кібербезпеки»:

диплом магістра за будь-якою із шести спеціальностей галузі знань 12 «Інформаційні технології» або за спеціальностями 171 «Електроніка», 172 «Телекомунікації та радіотехніка» галузі знань 17 «Електроніка та телекомунікації», або за спеціальністю 113 «Прикладна математика» галузі знань 11 «Математика та статистика», або за спеціальністю 151 «Автоматизація та комп'ютерно-інтегровані технології» галузі знань 15 «Автоматизація та приладобудування», або за спеціальностями 255 «Озброєння та військова техніка», 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7 рівень

НРК), а також свідоцтво про присвоєння (підвищення) кваліфікації «Інструктор-методист з інформаційної безпеки та кібербезпеки» або інший документ, що підтверджує професійну кваліфікацію «Інструктор-методист з інформаційної безпеки та кібербезпеки»;

або свідоцтво про присвоєння (підвищення) кваліфікації «Провідний інструктор-методиста з інформаційної безпеки та кібербезпеки» або інший документ, що підтверджує професійну кваліфікацію «Провідний інструктор-методиста з інформаційної безпеки та кібербезпеки».

Інструктор-методист з інформаційної безпеки та кібербезпеки – 7 рівень НРК.

Провідний інструктор-методист з інформаційної безпеки та кібербезпеки – 7 рівень НРК.

2. Навчання та професійний розвиток

2.1. Первинна професійна підготовка (назва кваліфікації)

Для кваліфікацій «Інструктор-методист з інформаційної безпеки та кібербезпеки» і «Провідний інструктор-методист з інформаційної безпеки та кібербезпеки» – підготовка на другому рівні вищої освіти (магістерському) за будь-якою із шести спеціальностей галузі знань 12 «Інформаційні технології» або за спеціальністю 172 «Телекомунікації та радіотехніка» галузі знань 17 «Електроніка та телекомунікації», стаж роботи повинен складати не менше двох років за однією з професій відповідного спрямування: Адміністратор мереж і систем, Розробник систем захисту інформації, Аналітик з безпеки інформаційно-телекомунікаційних систем, Фахівець з питань безпеки (інформаційно-комунікаційні технології), Фахівець сфери захисту інформації тощо.

2.2 Підвищення кваліфікації без присвоєння нового рівня освіти (назва кваліфікації)

Підвищення професійної кваліфікації «Провідний інструктор-методист з інформаційної безпеки та кібербезпеки» за наявності професійної кваліфікації «Інструктор-методист з інформаційної безпеки та кібербезпеки». Стаж роботи не менше двох років.

3. Нормативно-правова база, що регулює відповідну професійну діяльність

Закон України «Про освіту».

Закон України «Про вищу освіту».

Кодекс законів про працю України.

Закон України «Про професійний розвиток працівників».

Закон України «Про внесення змін до деяких законодавчих актів України щодо функціонування національної системи кваліфікацій».

Закон України «Про інформацію».

Закон України «Про державну таємницю».

Закон України «Про основні засади забезпечення кібербезпеки України».

Закон України «Про електронні комунікації».

Закон України «Про захист інформації в інформаційно-комунікаційних системах».

Закон України «Про національну безпеку України».

Закон України «Про захист персональних даних».

Закон України «Про захист прав споживачів».

Закон України «Про доступ до публічної інформації».

Указ Президента України від 13.02.2017 р. № 32 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації».

Указ Президента України від 30.08.2017 р. № 254 «Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32».

Указ Президента України від 01.05.2014 р. № 449 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України».

Указ Президента України від 26.08.2021 р. № 447 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України».

Постанова Кабінету Міністрів України від 19.06.2019 р. № 518 «Про затвердження загальних вимог з кіберзахисту об'єктів критичної інфраструктури».

Постанова Кабінету Міністрів України від 09.10.2020 р. № 934 «Деякі питання об'єктів критичної інформаційної інфраструктури».

Постанова Кабінету Міністрів України від 09.10.2020 р. р. № 1109 «Деякі питання об'єктів критичної інфраструктури».

Постанова Кабінету Міністрів України від 11.11.2020 р. № 1176 «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом».

Постанова Кабінету Міністрів України від 23.12.2020 р. № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки».

Постанова Кабінету Міністрів України від 23.12.2020 р. № 1363 «Про реалізацію експериментального проекту щодо запровадження комплексу організаційно-технічних заходів з виявлення вразливостей і недоліків у налаштуванні інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, в яких обробляються державні інформаційні ресурси».

Постанова Кабінету Міністрів України від 03.08.2005 р. № 688 «Про затвердження Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління».

Постанова Кабінету Міністрів України від 08.02.2021 р. № 94 «Про реалізацію експериментального проекту щодо функціонування Національного центру резервування державних інформаційних ресурсів».

Постанова Кабінету Міністрів України від 29.12.2021 р. № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту».

Наказ Адміністрації Держспецзв'язку від 02.12.2014 р. № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

Наказ Адміністрації Держспецзв'язку від 15.01.2016 р. № 20 «Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті».

Наказ Адміністрації Держспецзв'язку від 26.03.2007 р. № 45 «Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сферах технічного захисту інформації».

Наказ Адміністрації Держспецзв'язку від 10.06.2008 р. № 94 «Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

Наказ Адміністрації Держспецзв'язку від 15.01.2021 р. № 23 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури».

Наказ Адміністрації Держспецзв'язку від 06.10.2021 р. № 601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури».

Наказ Адміністрації Держспецзв'язку від 28.10.2021 р. № 640 «Про внесення змін до Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті».

Наказ Міністерства праці та соціальної політики України та Міністерства освіти і науки України від 26.03.2001 р. за №127/151 «Про затвердження Положення про професійне навчання працівників на виробництві».

Наказ державного комітету України по нагляду за охороною праці від 21.12.1993 р. за № 132 «Про Порядок опрацювання і затвердження роботодавцем нормативних актів з охорони праці, що діють на підприємстві», зареєстрований у Міністерстві юстиції України 07.02.1994 р. за № 20/229.

Наказ Комітету по нагляду за охороною праці Міністерства праці та соціальної політики України від 09.01.1998 р. за № 4 «Про затвердження Правил безпечної експлуатації електроустановок споживачів», зареєстрований в Міністерстві юстиції України 10.02.1998 р. за № 93/2533.

Наказ Комітету по нагляду за охороною праці Міністерства праці та соціальної політики України від 29.01.1998 р. за № 9 «Про затвердження Положення про розробку інструкцій з охорони праці», зареєстрований у Міністерстві юстиції України 07.04.1998 р. за № 226/2666.

Міжнародні стандарти інформаційної та кібербезпеки.

Державні нормативні документи в галузі інформаційної та кібербезпеки, створення і функціонування систем управління інформаційною безпекою (далі – СУІБ), комплексних систем захисту інформації (далі – КСЗІ), технічного захисту інформації (далі – ТЗІ), нормативні документи технічного захисту інформації (далі – НД ТЗІ), галузеві стандарти відповідного спрямування.

Документи National Institute of Standards and Technology United States of America (далі – NIST of USA) щодо інформаційної безпеки, кібербезпеки, ТЗІ, СУІБ.

Інші нормативно-правові, нормативно-технічні та нормативні акти, які регламентують питання безпеки інформації в інформаційно-комунікаційних системах та кіберпросторі.

4. Загальні компетентності

Умовне позначення	Загальні компетентності
ЗК.01	Здатність діяти соціально відповідально та громадсько свідомо
ЗК.02	Здатність застосовувати знання у практичних ситуаціях, розв'язувати завдання/задачі та практичні проблеми у професійній діяльності
ЗК.03	Здатність оцінювати та забезпечувати якість виконуваних робіт
ЗК.04	Здатність до абстрактного мислення, аналізу та синтезу, вчитися і бути сучасно навченим
ЗК.05	Здатність до адаптації та дії у новій ситуації
ЗК.06	Здатність до вибору стратегії спілкування, працювати в команді
ЗК.07	Здатність спілкуватися рідною мовою як усно, так і письмово, спілкуватися іноземною мовою (переважно англійською) на рівні, що забезпечує ефективну професійну діяльність

5. Перелік трудових функцій (професійних компетентностей за трудовою дією або групою трудових дій, що входять до них), умовні позначення

Умовне позначення	Трудові функції	Професійні компетентності (за трудовою дією або групою трудових дій)	Умовне позначення
А	Планування	Здатність планувати та координувати	А1

Умовне позначення	Трудові функції	Професійні компетентності (за трудовою дією або групою трудових дій)	Умовне позначення
	консультативно-методичної та навчальної роботи в організації/структурному підрозділі сфери інформаційної та кібербезпеки	реалізацію методик і форматів проведення аудиторних занять з метою створення найбільш ефективного навчального середовища	
		Здатність оцінювати ефективність та комплексність наявних програм навчання та тренінгів, потреб у навчанні та вимог до слухачів	A2
Б	Підготовка профільних навчально-методичних матеріалів	Здатність розробляти нові або визначати існуючі матеріали для навчання та тренінгів, для цільових аудиторій	Б1
		Здатність розробляти або брати участь у розробці методичних матеріалів або програм для тренінгів на робочому місці	Б2
		Здатність розробляти рекомендації щодо редагування навчальних планів і програм	Б3
В	Проведення навчання та тренінгів для працівників сфери інформаційної та кібербезпеки	Здатність здійснювати технічне та методологічне супроводження занять/тренінгів	В1
		Здатність проводити тренінгові курси з урахуванням аудиторії та фізичних/віртуальних середовищ	В2
Г	Проведення оцінювання результатів навчання слухачів сфери інформаційної та кібербезпеки	Здатність розробляти або брати участь у розробці стандартів оцінювання здобувачів та присвоєння/присудження кваліфікацій слухачам	Г1
		Здатність проводити оцінювання та присвоєння/присудження кваліфікацій слухачам	Г2
Д	Участь у проведенні консультаційної та/чи виконанні дослідно-експериментальної роботи відповідного спрямування	Здатність виконувати обов'язки внутрішнього консультанта і радника у своїй експертній області	Д1
		Здатність проводити дослідно-експериментальну роботу щодо процедури сканування вразливостей та їх розпізнавання в системах безпеки	Д2
		Здатність розробляти або брати участь у розробці матеріалів для тренінгів щодо забезпечення конфіденційності персональних даних та кібербезпеки	Д3

6. Опис трудових функцій (трудові функції; предмети і засоби праці (обладнання, устаткування, матеріали, продукти, інструмент; професійні компетентності (за трудовою дією або групою трудових дій), знання, уміння та навички)

Трудові функції	Предмети і засоби праці (обладнання, устаткування, матеріали, продукти, інструменти)	Професійні компетентності (за трудовою дією або групою трудових дій)	Знання	Уміння та навички
<p>А. Планування консультативно-методичної та навчальної роботи в організації/структурному підрозділі сфери інформаційної та кібербезпеки</p>	<p>Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повно-текстових наукових журналів (EBSCO, JSTOR) відповідно до профілю викладання; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і</p>	<p>А1. Здатність планувати та координувати реалізацію методик і форматів проведення аудиторних занять з метою створення найбільш ефективного навчального середовища</p>	<p>А1.31. Технологічні задачі і завдання управління та лідерства пов'язані з організаційними процесами, механізми вирішення проблем</p> <p>А1.32. Концепції і протоколи комп'ютерних мереж, а також методологія забезпечення безпеки мереж</p> <p>А1.33. Методики управління ризиками (методи оцінювання та оброблення ризиків)</p> <p>А1.34. Закони, нормативні акти, політики та етичні норми, та як вони пов'язані з конфіденційністю персональних даних і кібербезпекою</p> <p>А1.35. Принципи забезпечення конфіденційності персональних даних та кібербезпеки</p> <p>А1.36. Кіберзагрози та вразливості</p> <p>А1.37. Основні операційні наслідки інцидентів кібербезпеки</p> <p>А1.38. Методи автентифікації, авторизації та контролю доступу</p> <p>А1.39. Технології віртуалізації,</p>	<p>А1.У1. Планувати та координувати методику, формати проведення лекцій, демонстрацій, інтерактивних занять, мультимедійних презентацій</p> <p>А1.У2. Адаптувати технічну інформацію для планування до рівня розуміння користувача/споживача/замовника</p> <p>А1.У3. Збирати точні та повні дані з джерел, які використовуються для розвідки, оцінювання та/або планування</p> <p>А1.У4. Планувати позааудиторні освітні заходи (відеокурси, наставництво, веб-курси)</p> <p>А1.У5. Формувати цілі та завдання для освітніх програм з інформаційної та кібербезпеки</p>

Трудові функції	Предмети і засоби праці (обладнання, матеріали, продукти, інструменти)	Професійні компетентності (за трудовою дією або групою трудових дій)	Знання	Уміння та навички
	<p>обладнання; профільна наукова та методична література; правила та інструкції з розроблення навчальних програм, навчальних та методичних матеріалів</p>	<p>А2. Здатність оцінювати ефективність та комплексність навчальних програм навчання та тренінгів, потреб у навчанні та вимог до слухачів</p>	<p>формування віртуальних машин їх технічна підтримка A1.310. Нові та ті, що розробляються технології інформаційної та кібербезпеки A1.311. Політика навчання в організації A1.312. Рівні навчання, зокрема системи освіти за методикою, розробленою Бенджаміном Блумом A1.313. Системи управління навчанням і практику їх використання A1.314. Види доведення інформації (асимілятивний, слуховий, кінестетичний) A1.315. Способи навчання (запам'ятовування, спостереження) A1.316. Принципи (специфіка) роботи з аудиторією післядипломної освіти</p>	<p>A2.У1. Проводити оцінювання ефективності існуючих програм навчання та тренінгів A2.У2. Здійснювати комплексний аналіз відповідності змісту навчальних програм встановленим стандартам якості навчання A2.У3. Проводити соціологічні анонімні опитування слухачів,</p>

Трудові функції	Предмети і засоби праці (обладнання, устаткування, матеріали, продукти, інструменти)	Професійні компетентності (за трудовою дією або групою трудових дій)	Знання	Уміння та навички
			<p>Ганьє, модель багаторівневої оцінки Дональда Киркпатріка)</p> <p>A2.33. Методи визначення вимог до інфраструктури тестування та оцінювання</p> <p>A2.34. Принципи та процеси проведення тренінгів, оцінки потреби у навчанні</p>	<p>інтерв'ювання інших заінтересованих осіб стосовно покращення методів навчання та змісту навчальних програм</p> <p>A2.У4. Оцінювати конкретні результати роботи щодо підготовки, перепідготовки та підвищення кваліфікації працівників</p>
<p>Б. Підготовка профільних навчально-методичних матеріалів</p>	<p>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)</p> <p>Відповідно до профілю викладання;</p>	<p>Б1. Здатність розробляти нові або визначати існуючі матеріали для навчання та тренінгів, для цільових аудиторій</p>	<p>Б1.31. Технології виробництва, комунікації та розповсюдження медійних повідомлень, а також альтернативні способи інформування за допомогою текстових, мовних, візуальних повідомлень</p> <p>Б1.32. Відповідні концепції, процедури, програмне забезпечення, обладнання і прикладні технологічні програми, які застосовуються для навчання</p> <p>Б1.33. Вимоги до структури та змісту навчальної програми</p> <p>Б1.34. Вимоги та підходи до розроблення навчальних і методичних матеріалів</p> <p>Б1.35. Сучасні підходи до формування навчальних програм</p> <p>Б1.36. Таксономія Блума</p>	<p>Б1.У1. Розробляти або брати участь у розробці політик і протоколів для кібертренінгів</p> <p>Б1.У2. Розробляти або брати участь у розробці індивідуальних/колективних планів розвитку, навчання та/або вдосконалення результатів навчання</p> <p>Б1.У3. Розробляти чіткі вказівки та навчальні матеріали</p> <p>Б1.У4. Розробляти або брати участь у розробці комп'ютерних навчальних модулів або курсів</p> <p>Б1.У5. Розробляти або придбавати навчальний план, який відповідає темі та цілі на достатньому рівні</p> <p>Б1.У6. Розробляти технічну документацію відповідного спрямування</p>

Трудові функції	Предмети і засоби праці (обладнання, матеріали, продукти, інструменти)	Професійні компетентності (за трудовою дією або групою трудових дій)	Знання	Уміння та навички
	<p>бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова, методична література; правила та інструкції з розроблення навчальних програм, навчальних і методичних матеріалів</p>	<p>Б2. Здатність розробляти або брати участь у розробці методичних матеріалів або програм для тренінгів на робочому місці</p>	<p>Б2.31. Організація кіберзмагань, як засіб розвитку навичок шляхом надання практичного досвіду в симульованих і реальних ситуаціях Б2.32. Порядок, процедура та форми підготовки кадрів на робочому місці Б2.33. Принципи та методи навчання та виховання для розробки навчальних програм, навчання та інструктажів для окремих осіб і груп, а також вимірювання підготовки та освітні ефекти Б2.34. Зміст навчальної програми для тренінгів на робочому місці</p>	<p>Б2.У1. Розробляти або брати участь у розробці політик навчання і протоколів у сфері інформаційної та кібербезпеки на робочому місці Б2.У2. Розробляти або брати участь у розробці завдань, планів і програм для тренінгів на робочому місці Б2.У3. Розробляти або брати участь у розробці індивідуальних/колективних планів розвитку, навчання та/або вдосконалення результатів навчання на робочому місці Б2.У4. Обґрунтувати зв'язок навчальної програми для тренінгів на робочому місці зі стратегією розвитку організації у сфері інформаційної та кібербезпеки Б2.У5. Редагувати зміст навчальної програми для тренінгів на робочому місці відповідно до їх оновлення та встановлених часових вимог Б2.У6. Адаптувати навчальну програму для тренінгу на робочому місці відповідно до його оновлення та встановлених часових вимог Б1.У7. Розробляти або брати участь у розробці завдань, планів і програм для курсів/тренінгів на робочому місці</p>

Трудові функції	Предмети і засоби праці (обладнання, устаткування, матеріали, продукти, інструменти)	Професійні компетентності (за трудовою дією або групою трудових дій)	Знання	Уміння та навички
		<p>Б3. Здатність розробляти рекомендації щодо редагування навчальних планів і програм</p>	<p>Б3.31. Матеріали інструкцій (стандартні операційні процедури, технологічний посібник) для надання детальних вказівок відповідним працівникам</p> <p>Б3.32. Технічна документація відповідного спрямування</p> <p>Б3.33. Методи та підходи щодо переглядів та/чи вдосконалення навчальних планів і програм</p> <p>Б3.34. Вимоги системи забезпечення якості</p>	<p>Б3.У1. Готувати матеріали інструкцій (стандартні операційні процедури, технологічний посібник) для надання детальних настанов для відповідної частини персоналу</p> <p>Б3.У2. Розробляти технічну документацію відповідного спрямування</p> <p>Б3.У3. Інтегрувати нові наукові ідеї та підходи у зміст навчальних програм в необхідних обсягах і формах</p> <p>Б3.У4. Аналізувати вимоги та очікування слухачів, їх роботодавців та інших заінтересованих осіб щодо навчальної програми/тренінгу чи курсу</p> <p>Б3.У5. Ураховувати в об'єкту організації потреби керівництва організації під час періодичного перегляду та вдосконалення навчальних планів, програм</p>
<p>В. Проведення навчання та тренінгів для працівників сфери інформаційної та кібербезпеки</p>	<p>Відповідно обладнані навчальні аудиторії; засоби зв'язку та комунікації, програмне забезпечення; принтер, ксерокс, фліпчарт,</p>	<p>В1. Здатність здійснювати технічне та методологічне супроводження занять/тренінгів</p>	<p>В1.31. Зміст навчальної програми відповідного спрямування</p> <p>В1.32. Особливості організації навчального процесу для різних форм набуття компетентності</p> <p>В1.33. Форми організації навчального процесу</p> <p>В1.34. Види навчальних занять</p>	<p>В1.У1. Надавати (доносити) технічну інформацію різним категоріям слухачів</p> <p>В1.У2. Переглядати тренінгову документацію (документи курсу, плани занять, студентські роботи, екзамени, графіки навчання, описи курсів)</p>

Трудові функції	Предмети і засоби праці (обладнання, устаткування, матеріали, продукти, інструменти)	Професійні компетентності (за трудовою дією або групою трудових дій)	Знання	Уміння та навички
	інтерактивна дошка, канцелярські приладдя, проектор; лабораторні приміщення та обладнання (за спеціалізацією), методична та педагогічна література, засоби навчання		<p>B1.35. Сучасні методи, засоби та технології викладання</p> <p>B1.36. Методи та способи організації індивідуальної та групової роботи слухачів під час навчання</p> <p>B1.37. Основи вікової психології, педагогіки та андрагогіки</p> <p>B1.38. Методи та способи ефективної комунікації</p>	<p>B1.U3. Встановлювати ефективний зворотний зв'язок зі студентами з метою вдосконалення навчання</p> <p>B1.U4. Розробляти у необхідних обсягах програми на сучасних мовах програмування</p> <p>B1.U5. Використовувати у навчальній діяльності віртуальні машини (Microsoft Hyper-V, VMWare, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud)</p> <p>B1.U6. Налаштовувати та використовувати у навчальному процесі програмні засоби захисту комп'ютерів (програмні фільтри, антивірусні програми й антишпигунське програмне забезпечення)</p> <p>B1.U7. Конфігурувати та використовувати у навчальному процесі компоненти системи мережевої безпеки (мережеві екрани, віртуальні приватні мережі, системи виявлення вторгнень)</p> <p>B1.U8. Використовувати сучасні та новітні технології у навчальних цілях (інтерактивні дошки, Web-сайти, комп'ютери, проектори)</p>

Трудові функції	Предмети і засоби праці (обладнання, матеріали, продукти, інструменти)	Професійні компетентності (за трудовою дією або групою трудових дій)	Знання	Уміння та навички
		<p>B2. Здатність проводити тренінгові курси з урахуванням аудиторії та фізичних/віртуальних середовищ</p>	<p>B2.31. Освітні комп'ютерні послуги та послуги дистанційної освіти B2.32. Принципи та методи тренінгів і занять для розробки навчально-методичних матеріалів індивідуального та групового навчання, освіти, а також вимірювання їх результатів B2.33. Методи здійснення індивідуального супроводу, наставництва/менторства</p>	<p>B1.U9. Відображати дані в оригінальних формагах B2.U1. Проводити інтерактивні тренінги для створення ефективного навчального середовища B2.U2. Забезпечувати розробку та виконання сценаріїв тренінгів B2.U3. Застосовувати концепції, процедури, програмне забезпечення, обладнання та/або технологічні прикладні програми під час навчання студентів/слухачів B2.U4. Готувати та проводити навчальні заняття та брифінги з обізнаності, дотримання політик і процедур безпеки користувачами систем, мереж і даних B2.U5. Сприяти дискусіям у невеликих групах B2.U6. Проводити разом із слухачами електронну криміналістичну експертизу в кількох середовищах операційних систем B2.U7. Демонструвати слухачам роботу засобів контролю захищеності B2.U8. Демонструвати слухачам застосування техніки покращення захисту системи, мережі та</p>

Трудові функції	Предмети і засоби праці (обладнання, устаткування, матеріали, продукти, інструменти)	Професійні компетентності (за трудовою дією або групою трудових дій)	Знання	Уміння та навички
				<p>операційної системи (виключення незагребуваних послуг, паролівних політик, сегментація мережі, використання журналу реєстрації, мінімізації привілеїв)</p> <p>B2.U9. Аналізувати та демонструвати слухачам шкідливе програмне забезпечення</p> <p>B2.U10. Навчати слухачів підходам щодо аналізу трафіку на мережевому (пакетному) рівні</p> <p>B2.U11. Навчати слухачів підходам щодо моніторингу комп'ютерних мереж в частині, що стосується визначення пристроїв мережі</p> <p>B2.U12. Навчати слухачів підходам щодо аналізу та редагування результатів розвідки, отриманих з різних джерел при проведенні кібероперацій</p> <p>B2.U13. Навчати слухачів підходам щодо використання інструментів, методик і процедур для віддаленого доступу до обладнання</p> <p>B1.U14. Користуватися загальнодоступними мережевими інструментами (ping, traceroute, nslookup)</p> <p>B1.U15. Використовувати командний</p>

Трудові функції	Предмети і засоби праці (обладнання, устаткування, матеріали, продукти, інструменти)	Професійні компетентності (за трудовою дією або групою трудових дій)	Знання	Уміння та навички
Г. Проведення оцінювання результатів навчання слухачів сфери інформаційної та кібербезпеки	Комп'ютерне обладнання з відповідним програмним забезпеченням; наукова, методична та педагогічна література; принтер, ксерокс; засоби зв'язку та комунікації; канцелярські прилади; відповідно обладнані приміщення та/або аудиторії	Г1. Здатність розробляти або брати участь у розробці стандартів оцінювання здобувачів та присвоєння/присудження кваліфікацій слухачам	Г1.31. Методики оцінювання результатів навчання (рубрики, плани оцінювання, тестування, вікторини) Г1.32. Методи та процеси тестування і оцінювання слухачів Г1.33. Порядок і методи оцінювання результатів навчання Г1.34. Порядок присвоєння/присудження часткової професійної/освітньої кваліфікації Г1.35. Класифікація методів оцінювання та процедури їх застосування на практиці Г1.36. Підходи та методи розроблення і верифікації критеріїв оцінювання результатів навчання	рядок операційної системи (ipconfig, netstat, dir, nbstat) В1.У16. Керувати різними системами та методами електронної комунікації (електронна пошта, VOIP, IM (миттєві повідомлення), Web-форуми, Direct Video Broadcasts) Г1.У1. Розробляти письмові тести для визначення рівня професійної придатності та оцінювання кваліфікації слухачів Г1.У2. Розробляти критерії оцінювання результатів навчання Г1.У3. Брати участь у розробці правил оцінювання результатів навчання Г1.У4. Брати участь у розробці внутрішніх регламентів з присвоєння/присудження кваліфікацій слухачам
		Г2. Здатність проводити оцінювання та присвоєння/	Г2.31. Методи соціальної інженерії Г2.32. Вимоги та правила дотримання академічної доброчесності Г1.33. Порядок і методи оцінювання	Г2.У1. Використовувати інструменти та методики тестування на проникнення Г2.У2. Використовувати методи

Трудові функції	Предмети і засоби праці (обладнання, устаткування, матеріали, продукти, інструменти)	Професійні компетентності (за трудовою дією або групою трудових дій)	Знання	Уміння та навички
		присудження кваліфікацій слухачам	результатів навчання Г1.34. Порядок присвоєння/присудження професійної/освітньої кваліфікації Г1.35. Класифікація методів оцінювання та процедури їх застосування на практиці	соціальної інженерії Г2.У3. Приймати участь в оцінюванні результатів навчання та присвоєнні/присудженні професійних/освітніх кваліфікацій слухачам
Д. Участь у проведенні консультативної та/чи виконанні дослідно-експериментальної роботи відповідного спрямування	Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повно-текстових наукових журналів (EBSCO, JSTOR) відповідно до профілю викладання; бібліотечні ресурси,	Д1. Здатність виконувати обов'язки внутрішнього консультанта і радника у своїй експертній області	Д1.31. Основні бізнес-процеси та місія організації Д1.32. Прийняті в організації правила класифікації інформації щодо рівнів захисту та процедур доступу до неї Д1.33. Посадові завдання та обов'язки внутрішнього консультанта/радника за профільними спеціалізаціями Д1.34. Джерела та методи збору інформації, її узагальнення, структурування, систематизація Д1.35. Методи та технології підготовки доповідей і презентацій Д2.31. Основні небезпеки, ризики та вразливості Д2.32. Процедури сканування (пошуку) вразливостей у системах безпеки Д2.33. Порядок розпізнавання вразливостей у системах безпеки	Д1.У1. Виконувати обов'язки внутрішнього консультанта/радника в технічній сфері та галузі авторського права щодо електронних носіїв інформації Д1.У2. Готувати та проводити брифінги відповідного спрямування Д1.У3. Комунікувати з керівниками різних рівнів (міжособистісне спілкування, доступність, уміння ефективно сприймати мову виступаючих, відповідно до аудиторії коректувати стиль і мову виступу) Д2.У1. Проводити сканування систем безпеки інформаційних ресурсів на вразливості Д2.У2. Аналізувати пропускну здатність, характеристики та продуктивність комунікаційної системи

Трудові функції	Предмети і засоби праці (обладнання, матеріали, продукти, інструменти)	Професійні компетентності (за трудовою дією або групою трудових дій)	Знання	Уміння та навички
	архівні матеріали (за потреби)	вразливостей та їх розпізнавання в системах безпеки		<p>Д2.У3. Застосувати принципи забезпечення безпеки інформації – збереження конфіденційності, цілісності та доступності</p> <p>Д2.У4. Приймати участь у проведенні сканування та розпізнавання вразливостей у системах безпеки</p> <p>Д2.У5. Використовувати інструменти мережевого аналізу для визначення вразливостей систем (fuzzing, nmap)</p> <p>Д2.У6. Застосовувати засоби/заходи, що використовують алгоритми побудовані на основі штучного інтелекту для аналізу втручання в роботу інформаційних систем</p>
	<p>Д3. Здатність розробляти або брати участь у розробці матеріалів для тренінгів щодо забезпечення конфіденційності персональних даних та кібербезпеки</p>	<p>Д3.31. Зовнішні організації академічні установи, діяльність яких спрямована на дослідження кіберпростору</p> <p>Д3.32. Нормативні документи та правила, що забезпечують захист авторських прав, патентування, винаходів</p> <p>Д3.33. Новітні технології, інструменти, процедури, методи та процеси відповідного спрямування</p>	<p>Д3.У1. Розробляти або допомагати в розробці навчальних матеріалів для покращення розуміння співробітниками політики конфіденційності компанії, практики та процедур обробки даних, юридичних зобов'язань</p> <p>Д3.У2. Освоювати досягнення у технологіях захисту інформації для забезпечення їх впровадження у відповідній організації</p> <p>Д3.У3. Використовувати інструменти</p>	

Трудові функції	Предмети і засоби праці (обладнання, устаткування, матеріали, продукти, інструменти)	Професійні компетентності (за трудовою дією або групою трудових дій)	Знання	Уміння та навички
				<p>управління мережею для аналізу структури мережевого трафіку</p> <p>ДЗ.У4. Використовувати аналізатори протоколів</p> <p>ДЗ.У5. Застосовувати навички реверс-інжинірингу (редагування шістнадцяткових кодів, утиліти бінарного пакування тощо) для визначення функцій і належності інструментів віддаленого доступу</p>

7. Дані щодо розроблення та затвердження професійного стандарту

7.1. Розробник професійного стандарту

Державна служба спеціального зв'язку та захисту інформації України.

Склад робочої групи:

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

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

Давиденко Анатолій Миколайович, провідний науковий співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України;

Єсін Віталій Іванович, професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В. Каразіна;

Іванченко Ігор Сергійович, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету;

Конюшок Сергій Миколайович, заступник начальника інституту (з наукової роботи) Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського»;

Корченко Олександр Григорович, президент Громадської організації «Асоціація спеціалістів кібербезпеки», заступник голови профспілкової організації кафедри безпеки інформаційних технологій Національного авіаційного університету;

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

Ліпінський Вадим Володимирович, головний науковий співробітник Науково-дослідної установи «Інститут кібербезпеки»;

Мазур Наталя Володимирівна, завідувача відділом організаційно-правової роботи Профспілки працівників зв'язку України;

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

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

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

Прокопович-Ткаченко Дмитро Ігорович, завідувач кафедри кібербезпеки Університету митної справи та фінансів;

Самохвалов Юрій Якович, методист тренінгового центру ТОВ «ІССГ Тренінг Центр»;

Северінов Олександр Васильович, доцент кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки;

Супрун Ольга Миколаївна, професор кафедри кібербезпеки Науково-навчального інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України;

Толюпа Сергій Васильович, професор кафедри кібербезпеки та захисту інформації Київського національного університету ім. Тараса Шевченка;

Філіпова Ольга Валентинівна, комерційний директор компанії SAYCOM;

Цюпа Валерій Миколайович, президент Приватного навчального закладу «Міжнародна Кібер Академія»;

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

Штомпель Тетяна Миколаївна, віце-президент компанії TECHEXPERT, керівник навчального Центру «Мережні технології»;

Юдін Олександр Костянтинівич, учений секретар Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

Юдін Олексій Юрійович, перший заступник начальника Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації.

7.2. Суб'єкт перевірки професійного стандарту
Національне агентство кваліфікацій.

7.3. Дата затвердження професійного стандарту
25 листопада 2022 року.

7.4. Рекомендована дата наступного перегляду професійного стандарту
25 листопада 2027 року.

Заступник Голови Держспецзв'язку,
керівник комплексної робочої групи
з розробки професійних стандартів
бригадний генерал



Олександр ПОТІЙ