Проєкт

ЗАТВЕРДЖЕНО

ПРОФЕСІЙНИЙ СТАНДАРТ

ПРОФЕСІОНАЛ ІЗ ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

(дата внесення до Реєстру кваліфікацій)

Професійний стандарт розроблено та затверджено згідно з вимогами статті 4^2 Кодексу законів про працю України на підставі:

висновку суб'єкта перевірки – Національного агентства кваліфікацій від __ _____ _____ про дотримання під час підготовки проєкту професійного стандарту «Професіонал із організації захисту інформації з обмеженим доступом» вимог Порядку розроблення, введення в дію та перегляду професійних стандартів, затвердженого постановою Кабінету Міністрів України від 31.05.2017 р. № 373 (в редакції постанови КМ України від 30 травня 2025 року №622);

висновку щодо погодження проєкту професійного стандарту «Професіонал із організації захисту інформації з обмеженим доступом»

I. Назва професійного стандарту

Професіонал із організації захисту інформації з обмеженим доступом

II. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Організація та здійснення діяльності установи (державного органу, органу місцевого самоврядування, підприємства, організації) із: розроблення та здійснення заходів щодо забезпечення захисту інформації з обмеженим доступом, постійного контролю за їх дотриманням під час проведення всіх видів робіт, пов’язаних з інформацією з обмеженим доступом; розроблення проєктів інструкцій, положень та інших нормативних документів, які регламентують роботу підрозділу та порядок поводження з інформацією з обмеженим доступом; виявлення та закриття каналів витоку інформації з обмеженим доступом в процесі діяльності державного органу, органу місцевого самоврядування, підприємства, установи, організації, зокрема під час здійснення міжнародного співробітництва; недопущення необґрунтованого допуску та доступу осіб до інформації з обмеженим доступом; контроль та забезпечення виконання заходів щодо усунення причин і передумов до витоку інформації з обмеженим доступом; аналіз стану охорони інформації з обмеженим доступом та підготовка пропозицій щодо його удосконалення; управління діяльністю підрозділу із захисту інформації (режимно-секретного органу, офісу безпеки, підрозділу з кіберзахисту, служби діловодства тощо)

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 О	Державне управління й оборона; обов’язкове соціальне страхування	**Розділ 84**	Державне управління й оборона; обов’язкове соціальне страхування	**Група 84.2**	Надання державних послуг суспільству в цілому
				Клас 84.22	Діяльність у сфері оборони
				Клас 84.24	Діяльність у сфері охорони громадського порядку та безпеки

3. Назва (назви) професії (професій) та код (коди) підкласу (підкласів) (групи) професії згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій»

Професіонал із організації захисту інформації з обмеженим доступом, 2149.2

4. Професійна (професійні) кваліфікація (кваліфікації), її (їх) рівень згідно з Національною рамкою кваліфікацій (далі – НРК)

Професіонал із організації захисту інформації з обмеженим доступом, 7 рівень НРК

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

- документ (диплом, сертифікат, тощо), виданий суб'єктом, уповноваженим законодавством на присвоєння/підтвердження та визнання професійної або часткової професійної кваліфікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у відповідності до професійного стандарту «Професіонал із організації захисту інформації з обмеженим доступом»;
- документ (диплом, сертифікат, тощо), виданий суб'єктом, уповноваженим законодавством на присвоєння/підтвердження та визнання професійної або часткової професійної кваліфікації (щодо професійних кваліфікацій, здобутих у інших країнах).

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)

Назва професійної та/або часткової професійної кваліфікації	**Суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
Професіонал із організації захисту інформації з обмеженим доступом	Підготовка за спеціальностями, вказаними у **П.*** на другому (магістерському) рівні вищої освіти	Заклади вищої освіти

П.*

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

- К1 «Державна безпека»; галуззю знань К «Безпека та оборона» (7 рівень НРК);
- К3 «Національна безпека»; галуззю знань К «Безпека та оборона» (7 рівень НРК);
- К4 «Управління інформаційною безпекою»; галуззю знань К «Безпека та оборона» (7 рівень НРК).

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**
Професіонал із організації захисту інформації з обмеженим доступом	Для отримання професійної кваліфікації «професіонал із організації захисту інформації з обмеженим доступом». Стаж роботи не менше двох років.	Заклади вищої освіти

2) без присвоєння наступної професійної кваліфікації

Підвищення кваліфікації може здійснюватися шляхом неформальної (тренінги, семінари, семінари-практикуми, вебінари, тощо) та інформальної освіти для вдосконалення (підтримання) професійної кваліфікації, в тому числі шляхом набуття нових/додаткових навичок/компетентностей.

Підтвердження наявної та підвищення професійної кваліфікації може бути передбачено відповідними відомчими нормативно-правовими актами та внутрішніми документами підприємств, установ та організацій.

IV. Абревіатури, скорочення

БТ	банківська таємниця
ДТ	державна таємниця
ЗВДТ	Звід відомостей, що становить державну таємницю
ІКС	Інформаційно-комунікаційна система
ІОД	інформація з обмеженим доступом
КЕП	кваліфікований електронний підпис
КТ	комерційна таємниця
МНСІ	матеріальні носії секретної інформації
НД	нормативні документи
ПЗ	програмне забезпечення
РСО	режимно-секретний орган
СБУ	Служба безпеки України
ТЗІ	технічний захист інформації
установа	державний орган, органу місцевого самоврядування, підприємство, установа, організація
GDPR	Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)

V. Опис трудових функцій

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
А. Здійснення інституційного та нормативного забезпечення режиму інформації з обмеженим доступом в установі	**А1.** Здатність організовувати створення та підтримання функціонування РСО, офісу безпеки, підрозділу з кіберзахисту, служби діловодства тощо	А1.З1. Законодавство про види і режими ІОД. А1.З2. Законодавство щодо структури, завдань та функцій РСО, підрозділів захисту інформації та офісів безпеки. А1.З3. Вимоги до персоналу РСО, порядок їх призначення та погодження з СБУ. А1.З4. Основи менеджменту інформаційної безпеки та побудови систем захисту ІОД. А1.З5. Норми та порядок обладнання режимних приміщень та робочих місць фахівців. А1.З6. Порядок взаємодії РСО за ієрархією підпорядкованості та СБУ. А1.З7. Вимоги та принципи роботи з ІОД.	А1.У1. Проєктувати архітектуру системи захисту з урахуванням специфіки ІОД. А1.У2. Розробляти проєкти наказів про створення підрозділів захисту ІОД та положення про них. А1.У3. Визначати функціональні обов'язки персоналу та вимоги до їхньої кваліфікації. А1.У4. Обґрунтовувати необхідність технічного оснащення режимних приміщень згідно з нормами. А1.У5. Формувати стратегію управління інформаційною безпекою установи. А1.У6. Оцінювати відповідність кандидатів вимогам СБУ для роботи в РСО.	А1.К1. Взаємодіяти з керівництвом щодо стратегічного планування та ресурсного забезпечення безпеки ІОД. А1.К2. Співпрацювати з СБУ щодо погодження керівників РСО. А1.К3. Координувати діяльність структурних підрозділів у сфері захисту ІОД. А1.К4. Спілкуватися з РСО за ієрархією підпорядкованості щодо координації діяльності. А1.К5. Проводити наради з персоналом щодо дотримання вимог та принципів роботи з ІОД.	А1.В1. Нести відповідальність за відповідність структури захисту законодавчим нормам. А1.В2. Приймати автономні рішення щодо вибору організаційної моделі захисту. А1.В3. Відповідати за достовірність інформації, що подається регуляторам. А1.В4. Самостійно визначати пріоритети розвитку підрозділів безпеки. А1.В5. Відповідати за впровадження принципів менеджменту інформаційної безпеки.
	А2. Здатність розробляти внутрішні регламенти та інструкцій щодо	А2.З1. Методика розробки положень, інструкцій та наказів щодо режиму секретності та захисту ІОД. А2.З2. Вимоги до організації	А2.У1. Розробляти Положення про КТ та ПД, адаптовані до бізнес-процесів. А2.У2. Складати	А2.К1. Консультувати керівників підрозділів під час розробки локальних інструкцій. А2.К2. Роз’яснювати	А2.В1. Самостійно розробляти проєкти внутрішніх регламентів та інструкцій.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	режиму інформації з обмеженим доступом	секретного діловодства та обробки документів «Для службового користування». А2.З3. Правила встановлення пропускного та внутрішньооб'єктового режиму. А2.З4. Порядок розробки положень про ІОД відповідно до специфіки установи. А2.З5. Нормативи щодо обліку та зберігання печаток, штампів та ключів від сховищ.	інструкції щодо поводження з МНСІ та документами «ДСК». А2.У3. Формувати номенклатуру секретних справ та правила їх обліку. А2.У4. Готувати регламенти пропускного та внутрішньооб'єктового режиму. А2.У5. Встановлювати правила обліку та зберігання печаток, штампів і ключів. А2.У6. Адаптувати локальні акти до змін у законодавстві про ІОД.	персоналу зміст та наслідки впроваджених регламентів. А2.К3. Взаємодіяти з юридичною службою щодо включення пунктів про ІОД у контракти. А2.К4. Узгоджувати проєкти документів із профільними експертними комісіями. А2.К5. Аргументувати необхідність впровадження обмежувальних заходів у внутрішніх актах.	А2.В2. Нести персональну відповідальність за законність положень інструкцій. А2.В3. Автономно визначати необхідність перегляду діючих локальних актів. А2.В4. Відповідати за повноту охоплення ризиків у нормативних документах. А2.В5. Нести відповідальність за виконання зобов'язань про нерозголошення ІОД.
	А3. Здатність класифікувати та категорувати інформаційні активи	А3.З1. Критерії та порядок віднесення інформації до видів ІОД. А3.З2. Зміст та структура ЗВДТ. А3.З3. Життєвий цикл інформаційних активів та методика визначення їх критичності. А3.З4. Порядок присвоєння грифів обмеження доступу та процедури засекречування/ розсекречування. А3.З5. Методи інвентаризації інформаційних ресурсів та баз даних.	А3.У1. Визначати обсяги робіт, пов'язаних із ДТ, КТ та БТ для категорування. А3.У2. Проводити інвентаризацію інформаційних ресурсів та сервісів установи. А3.У3. Формувати переліки відомостей, що становлять таємницю установи. А3.У4. Визначати рівні критичності активів та їх життєвий	А3.К1. Консультувати експертні комісії установи з питань таємниць щодо категорування. А3.К2. Аргументувати зміну або скасування грифів обмеження доступу. А3.К3. Комунікувати з власниками активів для оцінки їх цінності та ризиків. А3.К4. Взаємодіяти з державними експертами з питань таємниць. А3.К5. Доносити до	А3.В1. Відповідати за коректність визначення категорії захищеності активів. А3.В2. Автономність у проведенні аудиту класифікації інформації. А3.В3. Приймати рішення про надання грифу секретності новим видам робіт. А3.В4. Відповідати за своєчасність

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		А3.З6. Методологія категорування об’єктів інформаційної діяльності та ІКС.	цикл. А3.У5. Класифікувати режимні зони (приміщення, території) та встановлювати рівні доступу до них. А3.У6. Здійснювати процедури засекречування/ розсекречування або зниження грифу обмеження доступу.	персоналу вимоги щодо маркування активів відповідно до категорії.	розсекречування матеріальних носіїв. А3.В5. Комісійно визначати межі режимних зон (приміщень, територій) та критичних територій.
	А4. Здатність готувати документи для отримання ліцензій, проведення державних експертиз та взаємодії з уповноваженими державними суб’єктами	А4.З1. Ліцензійні умови провадження діяльності у сфері ІОД. А4.З2. Порядок проведення державних експертиз на відповідність стандартам у сфері захисту ІОД. А4.З3. Повноваження уповноважених суб’єктів у сфері контролю за станом захисту ІОД. А4.З4. Стандарти атестації об’єктів інформаційної діяльності та режимних зон (приміщень, територій). А4.З5. Правила офіційного листування з регуляторами та підготовки дозвільних документів.	А4.У1. Готувати документи для отримання дозволу на провадження діяльності пов’язаної з ДТ. А4.У2. Готувати заяви та технічні описи для отримання ліцензій у сфері ТЗІ та криптографії. А4.У3. Вести офіційне листування з СБУ та Держспецзв’язку у сфері ІОД. А4.У4. Оформлювати матеріали для атестації об’єктів інформаційної діяльності. А4.У5. Здійснювати представництво установи в органах ліцензування. А4.У6. Оцінювати	А4.К1. Взаємодіяти з експертними групами під час перевірок та інспекцій. А4.К2. Комунікувати з регуляторами щодо уточнення вимог стандартів та НД ТЗІ. А4.К3. Аргументувати позицію установи під час державних експертиз та атестації. А4.К4. Узгоджувати технічні завдання на створення систем захисту з державними суб'єктами. А4.К5. Співпрацювати з підрозділами установи для підготовки об'єктів до контролю.	А4.В1. Нести відповідальність за достовірність відомостей у дозвільних документах. А4.В2. Самостійність у супроводі процесів сертифікації та атестації. А4.В3. Автономно визначати готовність об'єкта до державної експертизи. А4.В4. Відповідати за своєчасність подання документів на переоформлення ліцензій. А4.В5. Самостійно приймати рішення щодо обсягу інформації, що

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
			відповідність системи захисту ліцензійним умовам та стандартам.		надається при перевірках.
	А5. Здатність організовувати та забезпечувати проведення режимно-секретної діяльності в установі	А5.З1. Порядок організації охорони ДТ під час проведення секретних робіт та випробувань. А5.З2. Принципи забезпечення режиму секретності в пунктах постійної дислокації та в умовах бойових дій. А5.З3. Основи оцінки ризиків та методологія захисту інформації в автоматизованих системах. А5.З4. Особливості організації режиму секретності в умовах особливого періоду чи воєнного стану. А5.З5. Вимоги щодо поводження з МНСІ.	А5.У1. Забезпечувати режим секретності під час проведення секретних робіт та випробувань. А5.У2. Організовувати охорону ДТ у пунктах дислокації та в умовах воєнного стану. А5.У3. Контролювати порядок використання МНСІ та технічних засобів у режимних зонах (приміщеннях, територіях). А5.У4. Провадити діяльність, пов’язану з наданням, переоформленням та скасуванням допуску доступу. А5.У5. Розробляти плани заходів щодо виявлення та закриття каналів витоку ІОД. А5.У6. Оцінювати ризики захисту інформації в автоматизованих системах обробки ІОД.	А5.К1. Проводити інструктивні наради серед персоналу щодо режиму секретності. А5.К2. Співпрацювати зі службами охорони для оперативного реагування. А5.К3. Взаємодіяти з технічними підрозділами для інтеграції заходів захисту. А5.К4. Комунікувати з організаціями-замовниками щодо координації діяльності. А5.К5. Доповідати керівництву про стан режимно-секретної діяльності та ризики.	А5.В1. Нести персональну відповідальність за стан режиму секретності в установі. А5.В2. Приймати рішення про припинення робіт у разі виявлення грубих порушень. А5.В3. Самостійно визначати обсяги та методи контролю в підрозділах. А5.В4. Відповідати за збереження та цілісність матеріальних носіїв секретної інформації. А5.В5. Автономно планувати заходи щодо закриття каналів витоку ІОД.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	А6. Здатність забезпечувати захист ІОД в процесі міжнародного співробітництва	А6.З1. Міжнародні договори про взаємну охорону секретної інформації, ратифіковані Україною. А6.З2. Вимоги стандартів НАТО та ЄС щодо поводження з іноземною класифікованою інформацією. А6.З3. Порядок прийому іноземних делегацій та проведення міжнародних заходів у режимних зонах (територіях, приміщеннях). А6.З4. Правила транскордонної передачі персональних даних та вимоги GDPR. А6.З5. Особливості захисту КТ та БТ при укладанні міжнародних контрактів.	А6.У1. Застосовувати норми міжнародних договорів про взаємну охорону ІОД. А6.У2. Впроваджувати вимоги стандартів НАТО та ЄС щодо поводження з іноземною класифікованою інформацією. А6.У3. Організовувати прийом іноземних делегацій у режимних зонах (територіях, приміщеннях) установи. А6.У4. Забезпечувати захист ПД при транскордонній передачі згідно з GDPR. А6.У5. Розробляти та контролювати виконання угод про нерозголошення у міжнародних контрактах. А6.У6. Оцінювати специфіку захисту КТ та БТ при роботі з іноземними партнерами.	А6.К1. Координувати з СБУ та іншими уповноваженими органами заходи щодо міжнародного співробітництва. А6.К2. Проводити інструктажі для працівників, що відряджаються за кордон. А6.К3. Взаємодіяти з офіцерами безпеки іноземних партнерів щодо рівнів захисту. А6.К4. Роз’яснювати персоналу особливості роботи з іноземною класифікованою інформацією. А6.К5. Надавати консультації керівництву щодо ризиків міжнародного науково-технічного обміну.	А6.В1. Відповідати за збереження іноземної класифікованої інформації. А6.В2. Самостійно приймати рішення про можливість допуску іноземців до певних зон. А6.В3. Нести відповідальність за правомірність транскордонної передачі ПД та БТ. А6.В4. Автономно оцінювати ризики порушення режиму під час міжнародних нарад. А6.В5. Відповідати за відповідність угод про нерозголошення міжнародних контрактів законодавству України.
Б. Впровадження та управління програмно-апаратними	Б1. Здатність впроваджувати та адмініструвати	Б1.З1. Архітектура апаратних і програмних засобів ТЗІ та криптографічного захисту.	Б1.У1. Інсталювати та конфігурувати антивіруси, IDS/IPS,	Б1.К1. Надавати технічні роз’яснення системним адміністраторам щодо КЗІ.	Б1.В1. Нести відповідальність за стійкість

Трудові функції	Компетентності	Результати навчання			
		Знання	Уміння/навички	Комунікація	Відповідальність і автономія
засобами та системами захисту інформації з обмеженим доступом	технічні та криптографічні засоби захисту інформації.	Б1.З2. Стандарти криптографічних алгоритмів та використання КЕП. Б1.З3. Принципи роботи систем захисту від витоку даних (DLP). Б1.З4. Порядок конфігурування антивірусних систем та фаєрволів у захищених мережах. Б1.З5. Методи забезпечення стійкості криптозахисту в мережах обробки ІОД.	фаєрволи у захищених мережах. Б1.У2. Налаштовувати ключові системи та сертифікати КЕП згідно зі стандартами. Б1.У3. Адмініструвати засоби захисту від витоку даних (DLP). Б1.У4. Налаштовувати захищені канали зв'язку (VPN, TLS). Б1.У5. Використовувати програмно-апаратні комплекси моніторингу ТЗІ. Б1.У6. Впроваджувати засоби ТЗІ.	Б1.К2. Комунікувати з постачальниками рішень щодо технічної підтримки. Б1.К3. Узгоджувати з ІТ-відділом параметри роботи криптографічного ПЗ. Б1.К4. Співпрацювати з фахівцями ТЗІ для інструментальних вимірювань. Б1.К5. Роз’яснювати працівникам правила безпечного використання КЕП.	криптографічного захисту. Б1.В2. Автономність у виборі параметрів конфігурації засобів захисту. Б1.В3. Відповідати за цілісність та збереження ключів криптозахисту. Б1.В4. Самостійно приймати рішення про модернізацію систем DLP та антивірусів. Б1.В5. Нести відповідальність за працездатність систем захисту від витоку даних.
	Б2. Здатність контролювати дотримання вимог нормативно-правових актів та нормативних документів з технічного захисту інформації	Б2.З1. Нормативно-технічна база (НД ТЗІ) щодо експлуатації систем захисту ІОД. Б2.З2. Методи контролю ефективності технічного захисту. Б2.З3. Порядок проведення технічних перевірок та оформлення відповідних актів. Б2.З4. Класифікація порушень технічних норм захисту та пов'язані з ними загрози.	Б2.У1. Проводити заміри параметрів захищеності. Б2.У2. Оформлювати акти технічних перевірок та приписи про усунення недоліків. Б2.У3. Перевіряти відповідність системи контролю та управління доступом та сигналізації вимогам НД ТЗІ.	Б2.К1. Доповідати про технічні невідповідності керівництву установи. Б2.К2. Взаємодіяти з технічними фахівцями для усунення зауважень. Б2.К3. Співпрацювати зі службами охорони для перевірки систем безпеки. Б2.К4. Вимагати письмові пояснення від персоналу у разі порушення вимог	Б2.В1. Відповідати за виявлення порушень технічних норм захисту. Б2.В2. Автономність у проведенні інструментальних вимірювань. Б2.В3. Самостійно встановлювати терміни усунення технічних порушень.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
			Б2.У4. Контролювати порядок використання в установі особистих печаток та ключів. Б2.У5. Виявляти порушення технічних норм, що створюють загрози витоку ІОД.	нормативно-правових актів та нормативних документів з технічного захисту інформації. Б2.К5. Спілкуватися з представниками СБУ та інших уповноважених суб'єктів під час інспекцій стану ТЗІ.	Б2.В4. Відповідати за об'єктивність оцінки стану технічної готовності. Б2.В5. Приймати рішення про припинення експлуатації незахищених систем.
	Б3. Здатність організовувати кіберзахист систем і мереж обробки інформації з обмеженим доступом	Б3.З1. Принципи сегментації мереж та архітектури «нульової довіри» (Zero Trust). Б3.З2. Технології захисту баз даних, що містять ІОД. Б3.З3. Системи багатофакторної автентифікації (MFA) та ідентифікації користувачів. Б3.З4. Методи побудови захищених каналів зв'язку (VPN, TLS). Б3.З5. Моделі загроз та порушника в кіберпросторі щодо конкретної організації.	Б3.У1. Проєктувати захищені периметри (Zero Trust) для обробки ДТ та БТ. Б3.У2. Впроваджувати системи багатофакторної автентифікації (MFA) та біометрії. Б3.У3. Організовувати дотримання правил сегментації мереж (VLAN) для захисту ІОД. Б3.У4. Впроваджувати технології захисту баз даних та веб-ресурсів. Б3.У5. Розробляти моделі загроз та порушника в кіберпросторі установи. Б3.У6. Забезпечувати захист каналів передачі ІОД.	Б3.К1. Взаємодіяти з ІТ-відділом щодо інтеграції функцій безпеки в мережі. Б3.К2. Обмінюватися даними про кіберзагрози з галузевими центрами (SOC). Б3.К3. Надавати консультації адміністраторам щодо налаштувань безпеки. Б3.К4. Координувати дії підрозділів при налаштуванні рівнів доступу в мережах. Б3.К5. Спілкуватися з розробниками ПЗ щодо виправлення кіберврaзливостей.	Б3.В1. Нести відповідальність за недопущення несанкціонованого доступу до мереж. Б3.В2. Автономність у розробці архітектури кіберзахисту установи. Б3.В3. Відповідати за надійність ідентифікації та автентифікації користувачів. Б3.В4. Самостійно приймати рішення про блокування підозрілого трафіку. Б3.В5. Нести відповідальність за цілісність ІОД в інформаційних системах.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	Б4. Здатність організовувати впровадження багаторівневої системи кіберзахисту	Б4.З1. Технології забезпечення відмовостійкості (High Availability) систем обробки ІОД. Б4.З2. Стратегії резервного копіювання (Backup) та архівації критичних даних. Б4.З3. Принципи відновлення систем після кібератак (зокрема Ransomware). Б4.З4. Основи планування безперервності бізнес-процесів (BCP). Б4.З5. Порядок проведення регламентних робіт у системах захисту.	Б4.У1. Налаштовувати автоматичне резервування критичних баз даних. Б4.У2. Тестувати процедури відновлення систем з бекапів після атак. Б4.У3. Розробляти плани безперервності бізнес-процесів (BCP). Б4.У4. Впроваджувати технології відмовостійкості (High Availability). Б4.У5. Виконувати процедури аварійного перемикання систем. Б4.У6. Організовувати проведення регламентних робіт у системах захисту ІОД.	Б4.К1. Інформувати бізнес-підрозділи про регламентні роботи та збої. Б4.К2. Узгоджувати пріоритети відновлення з власниками процесів. Б4.К3. Комунікувати з ІТ-фахівцями щодо стратегій архівації ІОД. Б4.К4. Співпрацювати з підрозділами ТЗІ для забезпечення життєздатності систем. Б4.К5. Надавати звіти керівництву про готовність до відновлення після Ransomware.	Б4.В1. Нести відповідальність за цілісність даних при відновленні. Б4.В2. Автономність у виконанні процедур аварійного перемикання. Б4.В3. Відповідати за актуальність та наявність резервних копій ІОД. Б4.В4. Самостійно приймати рішення про запуск планів відновлення BCP. Б4.В5. Нести відповідальність за мінімізацію простою критичних систем.
В. Здійснення моніторингу, аудиту та реагування на інциденти у сфері захисту інформації з обмеженим доступом	В1. Здатність здійснювати постійний контроль захищеності об’єктів і систем обробки інформації з обмеженим доступом	В1.З1. Методи збору інформації іноземними розвідками та промислового шпигунства. В1.З2. Функціонал SIEM-систем та засобів логування подій доступу до ІОД. В1.З3. Показники ефективності (KPI) діючих систем захисту інформації. В1.З4. Порядок моніторингу режиму секретності в	В1.У1. Проводити щоденний аналіз журналів доступу до ІОД. В1.У2. Налаштовувати правила кореляції подій у SIEM-системах. В1.У3. Виявляти аномалії у поведінці користувачів та систем.	В1.К1. Готувати аналітичні звіти та доповідні записки для керівництва. В1.К2. Інформувати СБУ про спроби несанкціонованого доступу до ДТ. В1.К3. Проводити конфіденційні бесіди з персоналом щодо	В1.В1. Нести відповідальність за достовірність та своєчасність звітування. В1.В2. Автономність у виборі методів та інструментів моніторингу. В1.В3. Приймати

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		автоматизованих системах. В1.З5. Методологія аудиту прав доступу користувачів до ІОД.	В1.У4. Здійснювати моніторинг режиму секретності в автоматизованих системах. В1.У5. Розраховувати показники ефективності (KPI) діючих систем захисту. В1.У6. Проводити аудит прав доступу користувачів до ІОД.	інцидентів з ІОД. В1.К4. Комунікувати з адміністраторами АС щодо виявлених порушень. В1.К5. Обмінюватися даними про тактики порушень з колегами з інших РСО.	рішення про термінове обмеження доступу осіб при підозрі. В1.В4. Відповідати за збереження конфіденційності самого моніторингу. В1.В5. Самостійно ініціювати внутрішні перевірки за фактами аномалій.
	В2. Здатність виявляти загрози, зокрема кіберзагрози, і ризики порушень режиму обробки інформації з обмеженим доступом	В2.З1. Класифікація технічних каналів витоку інформації. В2.З2. Методи соціальної інженерії та індикатори внутрішніх загроз від персоналу. В2.З3. Репозиторії вразливостей та класифікація сучасних кіберзагроз. В2.З4. Ознаки підготовки до несанкціонованого доступу або розголошення ДТ.	В2.У1. Ідентифікувати технічні канали витоку. В2.У2. Розпізнавати ознаки застосування методів соціальної інженерії. В2.У3. Використовувати інструменти OSINT для виявлення фрагментів ІОД у мережі. В2.У4. Категорувати кіберзагрози за допомогою репозиторіїв вразливостей. В2.У5. Виявляти індикатори внутрішніх загроз з боку персоналу. В2.У6. Моделювати тактики шпигунства та промислової розвідки.	В2.К1. Консультувати щодо планів пом’якшення наслідків загроз. В2.К2. Співпрацювати з підрозділами ТЗІ для виявлення закладних пристроїв. В2.К3. Проводити практичні семінари щодо технік виявлення загроз. В2.К4. Формувати запити на отримання техдокументації для аналізу каналів витоку. В2.К5. Надавати рекомендації персоналу щодо "цифрової гігієни".	В2.В1. Відповідати за своєчасність виявлення нових каналів витоку ІОД. В2.В2. Автономно оцінювати рівень критичності виявлених загроз. В2.В3. Нести відповідальність за якість моделювання загроз та порушника. В2.В4. Самостійно планувати комплексні обстеження приміщень та територій.
	В3. Здатність	В3.З1. Правові засади та	В3.У1. Аналізувати	В3.К1. Взаємодіяти з	В3.В1. Самостійно

Трудові функції	Компетентності	Результати навчання			
		Знання	Уміння/навички	Комунікація	Відповідальність і автономія
	проводити розслідування порушень режиму секретності.	методика проведення службових розслідувань. В3.З2. Види відповідальності (адміністративна, кримінальна, дисциплінарна) за порушення у сфері ІОД. В3.З3. Процедури документального оформлення інцидентів (акти, протоколи). В3.З4. Методи технічного аналізу інцидентів та оцінки збитків від витоку. В3.З5. Порядок взаємодії з правоохоронними органами та СБУ під час розслідувань.	причини та умови, що призвели до розголошення ДТ, БТ чи КТ. В3.У2. Збирати доказову базу для проведення службових розслідувань. В3.У3. Документувати результати розслідувань (акти, протоколи інцидентів). В3.У4. Проводити технічний аналіз інцидентів та оцінку збитків від витоку. В3.У5. Оцінювати обсяг та цінність інформації, що стала об'єктом інциденту. В3.У6. Реконструювати події інциденту за допомогою логів SIEM та систем ТЗІ.	правоохоронними органами у разі порушень режиму ІОД. В3.К2. Співпрацювати з юридичною службою для правової кваліфікації порушень. В3.К3. Надавати аргументовані висновки керівництву за результатами розслідування. В3.К4. Координувати роботу комісій з розслідування порушень режиму ІОД. В3.К5. Вести офіційне листування з СБУ щодо результатів розслідувань у сфері ДТ.	ініціювати проведення службових розслідувань. В3.В2. Нести персональну відповідальність за об’єктивність матеріалів. В3.В3. Відповідати за збереження конфіденційності процесу розслідування. В3.В4. Приймати рішення про вилучення МНСІ та перепусток на час перевірки. В3.В5. Нести відповідальність за своєчасність інформування СБУ та інших уповноважених суб’єктів про інцидент з ІОД.
	В4. Здатність розробляти та впроваджувати плани реагування на загрози, ризики, інциденти та витоки інформації в системах захисту інформації з	В4.З1. Алгоритми дій у разі загрози втрати МНСІ або проникнення на режимний об’єкт. В4.З2. Процедури термінового блокування доступу до ІОД при виявленні порушень. В4.З3. Стратегії зменшення ризиків та пом’якшення наслідків інцидентів.	В4.У1. Розробляти алгоритми дій при загрозі втрати МНСІ або проникнення на режимний об’єкт. В4.У2. Впроваджувати процедури термінового блокування доступу до	В4.К1. Координувати дії з підрозділами охорони установи щодо оперативного реагування. В4.К2. Взаємодіяти з екстреними службами під час відпрацювання сценаріїв евакуації. В4.К3. Проводити	В4.В1. Нести відповідальність за ефективність заходів щодо локалізації витоку ІОД. В4.В2. Автономно приймати рішення про термінове блокування систем у

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	обмеженим доступом	В4.З4. Сценарії дій під час евакуації режимних об’єктів у надзвичайних ситуаціях. В4.З5. Тактика локалізації каналів витоку ІОД.	ІОД. В4.У3. Моделювати сценарії евакуації режимних об’єктів у надзвичайних ситуаціях. В4.У4. Розробляти тактику локалізації каналів витоку ІОД. В4.У5. Складати плани пом’якшення наслідків кібератак та фізичних інцидентів. В4.У6. Впроваджувати стратегії зменшення ризиків згідно з корпоративною політикою.	інструктажі персоналу щодо дій у разі загрози втручання в роботу об'єкта. В4.К4. Доповідати керівництву про виконання планів реагування під час навчань. В4.К5. Узгоджувати плани взаємодії з територіальними органами СБУ та іншими суб’єктами.	екстрених ситуаціях. В4.В3. Відповідати за збереження ІОД під час проведення евакуації. В4.В4. Самостійно готувати пропозиції щодо фінансування заходів реагування. В4.В5. Нести відповідальність за працездатність системи тривожного оповіщення.
Г. Управління доступом та робота з персоналом на режимних об’єктах	Г1. Здатність організовувати систему оформлення допусків, дозволів	Г1.З1. Порядок та критерії надання, переоформлення та скасування допуску до ДТ та дозволу на провадження діяльності, пов’язаною з ДТ. Г1.З2. Категорії форм допуску та відповідні їм обсяги обмежень. Г1.З3. Методика перевірки анкетних даних та виявлення перешкод для допуску. Г1.З4. Вимоги до формування та ведення Номенклатури посад працівників із допуском. Г1.З5. Принцип «необхідності знати» при наданні доступу до конкретних відомостей.	Г1.У1. Перевіряти достовірність даних та виявляти перешкоди для допуску та дозволу. Г1.У2. Формувати та вести Номенклатуру посад працівників із допуском до ІОД. Г1.У3. Готувати повні пакети документів для спецперевірок СБУ. Г1.У4. Диференціювати рівні доступу згідно з принципом «необхідності знати». Г1.У5. Здійснювати	Г1.К1. Взаємодіяти з СБУ для уточнення статусів оформлення допусків та дозволів. Г1.К2. Проводити індивідуальні консультативні бесіди з кандидатами на допуск, дозвіл. Г1.К3. Координувати роботу з кадрами для синхронізації призначень на посади. Г1.К4. Надавати роз’яснення працівникам щодо обмежень їхніх прав та компенсацій.	Г1.В1. Самостійно приймати рішення щодо повноти пакету документів кандидата на допуск, дозвіл. Г1.В2. Відповідати за обґрунтованість включення посад до Номенклатури. Г1.В3. Нести відповідальність за дотримання строків подання матеріалів на допуск, дозвіл. Г1.В4. Автономно визначати

Трудові функції	Компетентності	Результати навчання			
		Знання	Уміння/навички	Комунікація	Відповідальність і автономія
			процедуру припинення допуску, дозволу та анулювання відповідних документів. Г1.У6. Забезпечувати правомірність надання доступу до секретних відомостей.	Г1.К5. Вести офіційне листування про наявність допуску в осіб, що відряджаються.	пріоритетність у черговості оформлення документів. Г1.В5. Відповідати за конфіденційність та захист ПД у процесі перевірки.
	Г2. Здатність здійснювати контроль за дотриманням правил роботи з інформацією з обмеженим доступом	Г2.З1. Правила поводження з МНСІ на робочих місцях та під час нарад. Г2.З2. Порядок контролю за виїздом за кордон осіб, обізнаних із ДТ. Г2.З3. Обмеження прав громадян у зв'язку з допуском до ДТ та механізми компенсації. Г2.З4. Правила використання мобільних пристроїв у режимних зонах (територіях, приміщеннях). Г2.З5. Процедури контролю за дотриманням «цифрової гігієни» персоналом.	Г2.У1. Перевіряти наявність МНСІ у виконавців та умови їх зберігання. Г2.У2. Контролювати дотримання правил «цифрової гігієни» та використання пристроїв. Г2.У3. Здійснювати моніторинг виїзду за кордон осіб, обізнаних із ДТ. Г2.У4. Проводити контроль за дотриманням режиму під час секретних нарад. Г2.У5. Визначати реальний ступінь обізнаності осіб з ІОД. Г2.У6. Перевіряти порядок використання КЕП та особистих печаток працівниками.	Г2.К1. Проводити роз’яснювальні бесіди щодо обмежень на виїзд за кордон. Г2.К2. Співпрацювати з юристами для підготовки відповідей на скарги щодо обмежень. Г2.К3. Взаємодіяти з РСО інших установ щодо обізнаності про доступ осіб до ДТ. Г2.К4. Повідомляти прикордонну службу про обмеження права на виїзд. Г2.К5. Вимагати письмові пояснення за результатами перевірок на робочих місцях.	Г2.В1. Самостійно приймати рішення про ступінь фактичної обізнаності працівника. Г2.В2. Відповідати за об’єктивність висновків щодо можливості виїзду за кордон. Г2.В3. Автономно визначати періодичність та обсяги перевірок у підрозділах. Г2.В4. Нести відповідальність за юридичну силу зобов'язань про нерозголошення. Г2.В5. Відповідати за своєчасне інформування керівництва про порушення режиму.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
	Г3. Здатність проводити інструктажі та перевірку знань персоналу щодо вимог захисту інформації з обмеженим доступом.	Г3.З1. Вимоги щодо організації навчання та видів інструктажів (вступний, поточний тощо). Г3.З2. Педагогічні засади навчання дорослих нормативним вимогам безпеки. Г3.З3. Порядок створення тестів та оформлення результатів перевірки знань. Г3.З4. Методи формування культури безпеки та усвідомлення ризиків у колективі. Г3.З5. Програми навчання діям у разі спроб вербування чи соціальної інженерії.	Г3.У1. Розробляти програми інструктажів (вступних, планових, позапланових). Г3.У2. Проводити оцінку рівня знань через тестування або заліки. Г3.У3. Моделювати практичні кейси (соціальна інженерія, поводження з МНСІ). Г3.У4. Розробляти наочні посібники та пам’ятки з культури безпеки. Г3.У5. Документувати результати навчання в журналах та протоколах. Г3.У6. Виявляти прогалини в знаннях та організовувати додаткове навчання.	Г3.К1. Володіти навичками публічних виступів перед аудиторією працівників. Г3.К2. Надавати аргументований зворотний зв’язок за результатами заліку. Г3.К3. Переконувати персонал у важливості культури безпеки та пильності. Г3.К4. Співпрацювати з фахівцями з кібербезпеки для підготовки навчальних матеріалів. Г3.К5. Консультувати керівників підрозділів щодо готовності підлеглих до роботи.	Г3.В1. Самостійно визначати періодичність та обсяг позапланових інструктажів. Г3.В2. Приймати автономне рішення про незалік працівникові. Г3.В3. Нести відповідальність за актуальність та якість навчальних матеріалів. Г3.В4. Відповідати за належне документування факту ознайомлення з обов'язками. Г3.В5. Автономно оцінювати психологічну готовність особи до роботи з ІОД.
	Г4. Здатність надавати консультації з питань організації режиму інформації з обмеженим доступом та функціонування системи її захисту	Г4.З1. Засади консультаційної підтримки керівництва з питань захисту ІОД. Г4.З2. Етичні аспекти роботи з персоналом та адаптація до режимних обмежень. Г4.З3. Методологія аргументації рішень щодо впровадження нових заходів безпеки. Г4.З4. Роль консультанта у плануванні стратегії кібербезпеки	Г4.У1. Надавати консультаційну підтримку керівництву з питань захисту ІОД. Г4.У2. Роз’яснювати правові наслідки порушення законодавства про ІОД. Г4.У3. Надавати пропозиції щодо оптимізації	Г4.К1. Вести конструктивний діалог під час надання експертних порад керівництву. Г4.К2. Проводити індивідуальні бесіди з новими працівниками для адаптації у роботі з ІОД. Г4.К3. Співпрацювати з власниками ПД та БТ щодо правомірності їх обробки.	Г4.В1. Виконувати обов’язки внутрішнього консультанта/радника в сфері безпеки у сфері ІОД. Г4.В2. Нести відповідальність за об’єктивність наданих порад та рекомендацій.

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
		організації. Г4.З5. Порядок роз'яснення правових наслідків за розголошення ІОД.	Номенклатури посад та заходів ТЗІ. Г4.У4. Консультувати персонал щодо етичних аспектів та режимних обмежень. Г4.У5. Аргументувати вибір методів захисту при плануванні стратегії безпеки. Г4.У6. Надавати методичну допомогу працівникам щодо коректності анкетних даних.	Г4.К4. Надавати роз'яснення партнерам щодо вимог режиму при спільних проєктах. Г4.К5. Спілкуватися зі стейкхолдерами щодо політики корпоративного управління безпекою у сфері ІОД.	Г4.В3. Самостійно визначати необхідність залучення вузьких фахівців до консультацій. Г4.В4. Відповідати за конфіденційність консультацій з питань розслідувань. Г4.В5. Автономно формувати експертну позицію щодо ризиків впровадження нових систем.
Д. Менторська підтримка	Д1. Здатність передавати знання та досвід колегам.	Д1.З1. Основи методології навчання дорослих (андрагогіки). Д1.З2. Методи та інструменти навчання. Д1.З4. Підходи до оцінювання професійних компетентностей.	Д1.У1. Розробляти навчальні матеріали з організації захисту ІОД. Д1.У2. Проводити навчальні заходи. Д1.У3. Оцінювати рівень знань молодших колег, визначати прогалини. Д1.У4. Формувати індивідуальні траєкторії розвитку молодших колег, надавати відповідні рекомендації.	Д1.К1. Встановлювати ефективний діалог з менш досвідченими колегами. Д1.К2. Доступно пояснювати принципи роботи та способи організації захисту ІОД. Д1.К3. Надавати конструктивний зворотний зв'язок щодо результатів навчання. Д1.К4. Обмінюватися досвідом з іншими менторами (інструкторами).	Д1.В1. Самостійно планувати та проводити навчальні заходи. Д1.В2. Нести відповідальність за якість проведених навчальних заходів. Д1.В3. Сприяти розвитку професійних компетентностей колег. Д1.В4. Бути прикладом професійної поведінки.

Трудові функції	Компетентності	Результати навчання			
		Знання	Уміння/навички	Комунікація	Відповідальність і автономія
					Д1.В5. Виявляти ініціативу у впровадженні нових освітніх практик.

Предмети і засоби праці (обладнання, устаткування, матеріали, інструменти)

Спеціалізоване робоче місце, розташоване в режимному приміщенні, яке обладнане відповідно до вимог НД ТЗІ, укомплектоване необхідними офісними меблями й технічними засобами, комп'ютерною технікою зі спеціалізованим програмним забезпеченням; нормативно-правові акти та внутрішні документи роботодавця, що регламентують діяльність з організації захисту ІОД

IV. Розподіл трудових функцій та компетентностей за професійними кваліфікаціями

Трудова функція (умовне позначення)	Загальна назва професійної кваліфікації в межах професійного стандарту: Аналітик загроз безпеки
	Професіонал із організації захисту інформації з обмеженим доступом
	повна
А	+
Б	+
В	+
Г	+
Д	+

VII. Відомості про розроблення та затвердження професійного стандарту

1. Повне найменування розробника професійного стандарту

Національна академія Служби безпеки України.

Склад робочої групи/Учасники робочої групи:

Шестаков Валерій Іванович – Національна академія Служби безпеки України, голова робочої групи;

члени робочої групи:

Астапенко Роман Ігорович – Керівник центру кібербезпеки Акціонерного товариства «Українська оборонна промисловість»;

Гуз Анатолій Михайлович – Національна академія Служби безпеки України;

Гулак Юрій Степанович – Національний університет оборони України;

Гулюк Анна Валентинівна – Департамент охорони державної таємниці та ліцензування Служби безпеки України;

Земляков Роман Юрійович – Національна академія Служби безпеки України.

Колєснік Катерина Миколаївна – Національна академія Служби безпеки України;

Комаров Максим Юрійович – Державний науково-дослідний інститут технологій кібербезпеки Державної служби спеціального зв’язку та захисту інформації України;

Костерев Дмитро Сергійович – Науково-дослідний відділ розвитку інформаційної та кібернетичної безпеки науково-дослідного управління розвитку спеціальних систем та інновацій Житомирського військового інституту імені С.П. Корольова.

Макаренко Віктор Володимирович – Національна академія Служби безпеки України;

Макухін Тимур Володимирович – Національна академія Служби безпеки України;

Морозов Олег Володимирович – Керівник Управління інформаційних технологій Національного антикорупційного бюро України;

Розвадовський Олександр Броніславович – Департамент охорони державної таємниці та ліцензування Служби безпеки України;

Сизончик Володимир Олександрович – Департамент охорони державної таємниці Міністерства оборони України;

Стародубець Олександр Миколайович – Управління режиму, документального забезпечення і контролю Служби безпеки України;

Тихомиров Олександр Олександрович – Національна академія Служби безпеки України;

Шельвестер Володимир Ярославович – Факультет охорони державної таємниці та інформаційного протиборства Житомирського військового інституту імені С.П. Корольова;

Юдін Олександр Костянтинович – Державний НДІ технологій кібербезпеки Державної служби спеціального зв’язку та захисту інформації України.