Проєкт

Наказ Державної служби

спеціального зв'язку та захисту

інформації України

від _____№_____

ПРОФЕСІЙНИЙ СТАНДАРТ

АУДИТОР ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ (З КІБЕРБЕЗПЕКИ)

_____(дата внесення до Реєстру кваліфікацій)

ЗАТВЕРДЖЕНО:

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

Професійний стандарт розроблено та затверджено згідно з вимогами статті 42 Кодексу законів про працю України на підставі:

- висновку суб'єкта перевірки – Національного агентства кваліфікацій від _____ про дотримання під час підготовки проєкту професійного стандарту вимог Порядку розроблення, введення в дію та перегляду професійних стандартів, затвердженого постановою Кабінету Міністрів України від 31.05.2017 р. № 373;
- висновку Профспілки працівників зв'язку України від _____ щодо погодження проєкту професійного стандарту

I. Назва професійного стандарту

Аудитор інформаційних технологій (з кібербезпеки)

II. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Проведення внутрішнього та зовнішнього аудиту об'єктів інформатизації для надання об'єктивних якісних і кількісних оцінок про поточний стан інформаційної безпеки організації у відповідності з визначеними в нормативно-правовій базі критеріями та показниками безпеки. Формування рекомендацій, на основі наданих оцінок, для посилення системи менеджменту інформаційної безпеки, підтримки планів стійкості, відновлення штатного функціонування інфраструктури організації після інцидентів та нештатних ситуацій.

2. Назва виду (видів) економічної діяльності, секції, розділу, групи, класу економічної діяльності та їх код згідно з Національним класифікатором України ДК 009:2010 «Класифікація видів економічної діяльності»

Секція J	Інформація та телекомунікації	**Розділ 61**	Телекомунікації (електрозв’язок)	**Група 61.1**	Діяльність у сфері проводового електрозв’язку
				Клас 61.10	Діяльність у сфері проводового електрозв'язку
				Група 61.2	Діяльність у сфері безпроводового електрозв’язку
				Клас 61.20	Діяльність у сфері безпроводового електрозв’язку
				Група 61.3	Діяльність у сфері супутникового електрозв’язку
				Клас 61.30	Діяльність у сфері супутникового електрозв’язку
				Група 61.9	Інша діяльність у сфері електрозв'язку
				Клас 61.90	Інша діяльність у сфері електрозв'язку
		Розділ 62	Комп’ютерне програмування, консультування та пов’язана з ними діяльність	**Група 62.0**	Комп’ютерне програмування, консультування та пов’язана з ними діяльність
				Клас 62.01	Комп’ютерне програмування

				Клас 62.02	Консультування з питань інформатизації
				Клас 62.03	Діяльність із керування комп'ютерним устаткуванням
				Клас 62.09	Інша діяльність у сфері інформаційних технологій і комп'ютерних систем
		Розділ 63	Надання інформаційних послуг	**Група 63.1**	Оброблення даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність; веб-портали
				Клас 63.11	Оброблення даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність
				Клас 63.12	Веб-портали
Секція M	Професійна, наукова та технічна діяльність	**Розділ 74**	Інша професійна, наукова та технічна діяльність	**Група 74.9**	Інша професійна, наукова та технічна діяльність, н.в.і.у.
				Клас 74.90	Інша професійна, наукова та технічна діяльність, н.в.і.у.
Секція P	Освіта	**Розділ 85**	Освіта	**Група 85.5**	Інші види освіти
				Клас 85.59	Інші види освіти, не введенні в інші угрупування

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

Аудитор інформаційних технологій (з кібербезпеки), 2139.2

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

Аудитор інформаційних технологій (з кібербезпеки), 6 рівень НРК (трудові функції А, Б, В, Г).

Провідний аудитор інформаційних технологій (з кібербезпеки), 7 рівень НРК (трудові функції А, Б, В, Г, Д, Е).

Аудитор систем менеджменту інформаційної безпеки, 6 рівень НРК. (трудові функції А, Б, Г, Є, Ж).

Провідний аудитор систем менеджменту інформаційної безпеки, 7 рівень НРК. (трудові функції А, Б, Г, Є, Ж, З, И).

Керівник команди з аудиту систем менеджменту інформаційної безпеки, 7 рівень НРК. (трудові функції А, Б, Г, Є, Ж, З, И, І).

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

- диплом на першому (бакалаврському) рівні вищої освіти що підтверджує (підтверджують) освітню кваліфікацію особи за спеціальністю:
  111 «Математика» галузі знань 11 «Математика та статистика» (6 рівень НРК);
  112 «Статистика» галузі знань 11 «Математика та статистика» (6 рівень НРК);
  113 «Прикладна математика» галузі знань 11 «Математика та статистика» (6 рівень НРК);
  121 «Інженерія програмного забезпечення» галузі знань «Інформаційні технології» (6 рівень НРК);
  122 «Комп'ютерні науки» галузі знань «Інформаційні технології» (6 рівень НРК);
  123 «Комп'ютерна інженерія» галузі знань «Інформаційні технології» (6 рівень НРК);
  124 «Системний аналіз» галузі знань «Інформаційні технології» (6 рівень НРК);
  125 «Кібербезпека» галузі знань «Інформаційні технології» (6 рівень НРК);
  126 «Інформаційні системи та технології» галузі знань «Інформаційні технології» (6 рівень НРК);
  171 «Електроніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (6 рівень НРК);
  172 «Електронні комунікації та радіотехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (6 рівень НРК);
  174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (6 рівень НРК);
  175 «Інформаційно-вимірювальні технології» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (6 рівень НРК);
  251 «Державна безпека» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (6 рівень НРК);
  252 «Безпека державного кордону» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (6 рівень НРК);
  253 «Військове управління (за видами збройних сил)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (6 рівень НРК);
  254 «Забезпечення військ (сил)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (6 рівень НРК);
  255 «Озброєння та військова техніка» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (6 рівень НРК);

256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (6 рівень НРК)
257 «Управління інформаційною безпекою» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (6 рівень НРК);

- диплом на другому (магістерському) рівні вищої освіти що підтверджує (підтверджують) освітню кваліфікацію особи за спеціальністю:

111 «Математика» галузі знань 11 «Математика та статистика» (7 рівень НРК);
112 «Статистика» галузі знань 11 «Математика та статистика» (рівень 7 НРК);
113 «Прикладна математика» галузі знань 11 «Математика та статистика» (7 рівень НРК);
121 «Інженерія програмного забезпечення» галузі знань «Інформаційні технології» (7 рівень НРК);
122 «Комп'ютерні науки» галузі знань «Інформаційні технології» (7 рівень НРК);
123 «Комп'ютерна інженерія» галузі знань «Інформаційні технології» (7 рівень НРК);
124 «Системний аналіз» галузі знань «Інформаційні технології» (7 рівень НРК);
125 «Кібербезпека» галузі знань «Інформаційні технології» (7 рівень НРК);
126 «Інформаційні системи та технології» галузі знань «Інформаційні технології» (7 рівень НРК);
171 «Електроніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (7 рівень НРК);
172 «Електронні комунікації та радіотехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (7 рівень НРК);
174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (7 рівень НРК);
175 «Інформаційно-вимірювальні технології» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (7 рівень НРК);
251 «Державна безпека» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7 рівень НРК);
252 «Безпека державного кордону» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7 рівень НРК);
253 «Військове управління (за видами збройних сил)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7 рівень НРК);

255 «Озброєння та військова техніка» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7 рівень НРК);
256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7 рівень НРК)
257 «Управління інформаційною безпекою» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (7 рівень НРК).

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

- документ (диплом, сертифікат, тощо), щодо післядипломної освіти та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері реагування на інциденти кібербезпеки;
- документ (диплом, сертифікат, тощо), щодо професійної сертифікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері реагування на інциденти кібербезпеки.

III. Здобуття професійної кваліфікації та професійний розвиток

1. Здобуття професійної кваліфікації

Назва професійної та/або часткової професійної кваліфікації	**Суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
Аудитор інформаційних технологій (з кібербезпеки), Аудитор систем менеджменту інформаційної безпеки	Підготовка на першому рівні вищої освіти (бакалаврському) за спеціальностями вказаними п. ІІ.5, без вимог до стажу роботи.	*не передбачено професійним стандартом*
Провідний аудитор інформаційних технологій (з кібербезпеки), Провідний аудитор систем менеджменту інформаційної безпеки,	Підготовка на другому рівні вищої освіти (магістерському) за спеціальностями вказаними п. ІІ.5, стаж роботи за однією з професій відповідного спрямування повинен складати не менше двох років (аналітик з	*не передбачено професійним стандартом*

Керівник команди з аудиту систем менеджменту інформаційної безпеки	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**
Провідний аудитор інформаційних технологій (з кібербезпеки)	Підвищення кваліфікації для отримання професійної кваліфікації «Провідний аудитор інформаційних технологій (з кібербезпеки)». Стаж роботи не менше двох років з професійною кваліфікацією «Аудитор інформаційних технологій (з кібербезпеки)»	*не передбачено професійним стандартом*
Провідний аудитор систем менеджменту інформаційної безпеки	Підвищення кваліфікації для отримання професійної кваліфікації «Провідний аудитор систем менеджменту інформаційної безпеки». Стаж роботи не менше двох років з професійною кваліфікацією «Аудитор систем менеджменту інформаційної безпеки»	*не передбачено професійним стандартом*
Керівник команди з аудиту систем менеджменту інформаційної безпеки	Підвищення кваліфікації для отримання професійної кваліфікації «Керівник команди з аудиту систем менеджменту інформаційної безпеки». Стаж роботи не	*не передбачено професійним стандартом*

	менше двох років з професійною кваліфікацією «Провідний аудитор систем менеджменту інформаційної безпеки»	

IV. Абревіатури, скорочення

IT	інформаційні технології
PL	Procedural Language
SQL	Structured Query Language
ДМЗ	демілітаризована зона (мережі)
ПЗ	програмне забезпечення
NIST SP	National Institute of Standards and Technology Special Publication
CIS CSC	Center for Internet Secirity Critical Security Controls
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
COMSEC	communications security

V. Опис трудових функцій

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/навички**	**Комунікація**	**Відповідальність і автономія**
А. Формування (підготовка), впровадження та виконання процедур внутрішнього аудиту інформаційних систем і технологій на основі визначення й прогнозування ризиків з метою забезпечення безпеки інформації та/або кібербезпеки інформаційних ресурсів, виконання стратегічних планів функціонування й розвитку інформаційної інфраструктури організації.	**А1.** Здатність планувати, здійснювати та документувати проведення внутрішнього аудиту інформаційних систем і технологій, визначати для цього ефективні методи та процедури.	**А1.З1.** ~~Знання~~ Концепції і протоколи комп'ютерних мереж, а також методології забезпечення мережевої безпеки. **А1.З2.** Закони, нормативні акти, політики і етичні норми, та як вони пов'язані з кібербезпекою і приватністю. **А1.З3.** Принципи кібербезпеки і приватності. **А1.З4.** Класифікація кіберзагроз та вразливостей. **А1.З5.** Механізми контролю доступу до хостів/мереж (наприклад, списки контролю доступу, списки повноважень).	**А1.У1.** Визначати необхідний рівень складності тесту для конкретної системи. **А1.У2.** Проводити аудити або огляди технічних систем. **А1.У3.** Розробляти звітні документи за результатами аудиту інформаційних систем. **А1.У4.** Розробляти план тестування системи безпеки (наприклад, окремого компонента, процесу інтеграції, системи, процесу приймання системи).	**А1.К1.** Структурувати інформацію та формувати свої висновки в письмовій формі чітко та зрозуміло. **А1.К2.** Ефективно співпрацювати в команді та координувати виконання завдань.	**А1.В1.** Забезпечувати ефективність виконання процедур аудиту інформаційних систем і технологій.

		A1.36. Архітектурні концепції та загальні принципи ІТ. **A1.37.** Сучасні галузеві методи оцінки, впровадження та розповсюдження інструментів та процедури оцінки безпеки ІТ, моніторингу, виявлення та усунення несправностей, що використовують концепції та можливості на основі стандартів. **A1.38.** Класифікація загроз і вразливостей безпеки систем і прикладного програмного забезпечення (наприклад, переповнення буфера, мобільний код, міжсайтові сценарії, процедурна мова/мова структурованих запитів [PL/SQL] та ін’єкції, перегони фронтів, прихований канал, повтор, атаки на повернення, шкідливий код). **A1.39.** Інструменти діагностики систем і			

		методик визначення несправностей. **А1.310.** Методи тестування та оцінки систем. **А1.311.** Електронні пристрої (наприклад, обчислювальні системи/компоненти, засоби контролю доступу, цифрові камери і сканери, електронні блокноти, жорсткі диски, карти пам'яті, модеми, компоненти мережі, мережеве прикладне програмне забезпечення, засоби контролю, принтери, змінні пристрої зберігання, телефони, копіри, факсимільні апарати тощо)). **А1.312.** Політики, процедури і нормативні акти з інформаційної безпеки та кіберзахисту. **А1.313.** Методи тестування та оцінки захищеності систем. **А1.314.** Принципи забезпечення конфіденційності, цілісності та доступності.			

		А1.315. Загальні види зараження комп'ютерів/мереж (віруси, закладки типу «троянський кінь» та ін.), а також методів зараження (через порти, прикріплені файли тощо). **А1.316.** Фундаментальні основи комп'ютерних мереж (тобто, основних компонентів комп'ютерної мережі, типів мереж тощо). **А1.317.** Безпека мережі (наприклад, шифрування, мережеві екрани, автентифікація, сервери-пастки, захист периметра). **А1.318.** Законодавство та правові аспекти в сфері кіберзахисту.			
	А2. Здатність визначати, аналізувати та оцінювати ризики, пов'язані з інформаційними системами та технологіями, здійснювати прогнозування потенційних загроз та виявляти вразливості.	**А2.31.** Процеси управління ризиками (наприклад, методи оцінки та зниження ризиків) **А2.32.** Принципи кібербезпеки і приватності, застосовувані під час управління ризиками, пов'язаних із	**А2.У1.** Проводити сканування вразливостей і розпізнавання вразливостей в системах безпеки. **А2.У2.** Розпізнавати та класифікувати різні типи вразливостей і пов'язаних з ними атак.	**А2.К1**. Ефективно співпрацювати в команді та координувати виконання завдань з аналізу та оцінки ризиків.	**А2.В1.** Якісно оцінювати ризики з метою попередження загроз для інформаційних систем та технологій.

		використанням, обробкою, зберіганням і передачею інформації або даних **А2.З3.** Нові і виникаючі ІТ та технології кібербезпеки **А2.З4.** Інструменти кореляції подій безпеки. **А2.З5.** Підходи організації до прийняття ризиків та/або управління ризиками. **А2.З6.** Поточні і виникаючі загрози/вектори загроз. **А2.З7.** Порядок оцінки ризиків/загроз. **А2.З8.** Політики, вимоги і процедури управління ризиками ІТ. **А2.З9.** Процедури оцінки ризиків. **А2.З10.** Порядок оцінювання систем кіберзахисту і вразливостей, а також їх можливостей.	**А2.У3.** Використовувати інструменти мережевого аналізу для визначення вразливостей (наприклад, fuzzing, nmap, тощо).		
	А3. Здатність розробляти та впроваджувати стратегічні плани для функціонування та розвитку інформаційної	**А3.З1.** Принципи і методи забезпечення безпеки ІТ (наприклад, мережеві екрани, ДМЗ, шифрування).	**А3.У1.** Здійснювати впровадження, підтримку і вдосконалення визнаних практик безпеки мережі.	**А3.К1.** Приймати участь у розробленні та впровадженні стратегічних планів організації розвитку інформаційної	**А3.В1.** Створювати стратегічні плани для забезпечення надійності, ефективності та стійкості

	інфраструктури організації.	**А3.З2.** Порядок управління мережевим доступом, ідентифікацією, та доступом (наприклад, інфраструктура відкритих ключів, автентифікація об'єктів, відкриті ідентифікатори, мова розмітки для контролю захищеності, мова розмітки для надання послуг). **А3.З3.** Засоби, методів і способів проектування систем безпеки. **А3.З4.** Принципи управління життєвим циклом системи, включаючи забезпечення безпеки та експлуатаційної придатності ПЗ. **А3.З5.** Моделі системи безпеки (наприклад, модель Белла-Лападули, моделі забезпечення цілісності «Biba» і Кларка-Вілсона). **А3.З6.** Інфраструктура, що підтримує ІТ для забезпечення захисту, продуктивності та надійності.	**А3.У2.** Проводити конфігурування і використання компонентів системи мережевої безпеки (наприклад, мережеві екрани, віртуальні приватні мережі, системи виявлення вторгнень). **А3.У3.** Впроваджувати і тестувати плани реагування на нештатні ситуації і відновлення мережевої інфраструктури.	інфраструктури організації. **А3.К2.** Комунікувати з керівниками організації різних рівнів в питаннях стратегічного планування функціонування та розвитку інформаційної інфраструктури організації.	інформаційної інфраструктури організації, враховуючи потреби, цілі та бізнес-вимоги.

Б. Контроль та оцінювання ефективності поточного стану функціонування інформаційної системи, проведення незалежних оглядів (або/чи планових) для оцінювання ефективності сталих інформаційних процесів з метою підтвердження довіри до інформаційних систем і технологій та забезпечення встановленої стратегії і політик безпеки інформації та/або кібербезпеки організації.	**Б1.** Здатність визначати методи та процедури для здійснення заходів контролю та оцінки ефективності функціонування інформаційних систем, незалежних оглядів та планових аудитів.	**Б1.З1.** Методологія оцінки загальних принципів управління ризиками. **Б1.З2.** Засоби контролю, пов'язані з використанням, обробкою, зберіганням та передачею даних. **Б1.З3.** Основні методи, процедури і способи збору інформації, звітності, її обробки і спільного використання. **Б1.З4.** Принципи і методи аналізу прийнятих в галузевих стандартах або в організації.	**Б1.У1.** Проводити огляди систем **Б1.У2.** Оцінювати надійність системи та проєктів **Б1.У3.** Оцінювати засоби контролю безпеки на основі принципів і доктрин кібербезпеки (наприклад, стандарти «CIS CSC», NIST SP 800-53, Керівні принципи кібербезпеки тощо).	**Б1.К1**. Ефективно співпрацювати в команді та комунікувати з аудиторами для визначення ефективних методів та процедур оцінки функціонування інформаційних систем.	**Б1.В1.** Забезпечувати ефективність застосування методів та процедур оцінки стану функціонування систем.
	Б2. Здатність використовувати аналітичні методи та інструменти для оцінки ефективності інформаційних систем, виявлення слабких місць і потенційних загроз безпеці, а також для розробки стратегій поліпшення інформаційної безпеки.	**Б2.З1.** Аналітичні конструкції та їх використання для оцінки операційного середовища. **Б2.З2.** Інструменти діагностики систем і методик визначення несправностей. **Б2.З3.** Те, як використовувати інструменти аналізу	**Б2.У1.** Виявляти вразливості в захищених системах (наприклад, сканування вразливостей і перевірка відповідності). **Б2.У2.** Проводити аналіз тенденцій. **Б2.У3.** Оцінювати наявні можливості з урахуванням бажаних	**Б2.К1.** Комунікувати зі стейкхолдерами щодо розробки стратегій поліпшення кібербезпеки організації.	**Б2.В1.** Готувати заключний звіт з оцінки безпеки, включаючи результати і висновки оцінки.

		мережі для визначення вразливостей.	результатів з метою забезпечення ефективності проведених заходів.		
В. Тестування та оцінювання продуктів інформаційних технологій (комплексів захисту і контролю, операційних систем, апаратного та програмного забезпечення, IT сервісів та додатків, тощо) пов'язаних з реалізацією встановлених функцій та політик безпеки організації у кіберпросторі.	**В1.** Здатність визначати та застосовувати методи, процедури та інструменти для тестування і оцінки продуктів інформаційних технологій, включаючи побудову тестових сценаріїв.	**В1.З1.** Принципи, інструменти та методики тестування на проникнення. **В1.З2.** Інструменти аналізу шкідливих програм (наприклад, Oily Debug, Ida Pro). **В1.З3.** Інструменти аналізу мереж для виявлення вразливостей в ПЗ, яке забезпечує комунікацію.	**В1.У1.** Використовувати інструменти та методики тестування на проникнення. **В1.У2.** Оцінювати ресурси, необхідні для тестування і оцінювання.	**В1.К1**. Ефективно співпрацювати в команді та координувати виконання відповідних завдань.	**В1.В1.** Планувати та будувати сценарії тестування і оцінки продуктів інформаційних технологій.
	В2. Здатність аналізувати та оцінювати продукти інформаційних технологій з точки зору їх відповідності встановленим функціям та політикам безпеки, виявляти вразливості та ризики інформаційної безпеки організації.	**В2.З1.** Спроможності прикладних програм і потенційних вразливостей мережевого обладнання, включаючи концентратори, маршрутизатори, комутатори, мости, сервери, носії передачі і супутнє апаратне обладнання.	**В2.У1.** Розробка звітних документів за результатами тестування і оцінювання. **В2.У2.** Усунення неполадок і діагностування аномалій функціонування інфраструктури	**В2.К1.** Формувати запити на профільну інформацію. **В2.К2.** Навичка комунікації з персоналом та аудиторами для оцінки продуктів інформаційних технологій.	**В2.В1.** Забезпечення використання надійних та безпечних продуктів інформаційних технологій в організації.

		В2.32. Процедури оцінки автоматизованих засобів контролю захищеності. **В2.33.** Принципи і методи структурного аналізу.	системи кібербезпеки на основі її аналізу.		
Г. Розробка планів, впровадження та виконання процедур або/чи відповідних дій контролю для забезпечення управління інцидентами, безперервності сталих операційних процесів, підтримки планів стійкості, відновлення штатного функціонування інфраструктури організації після інцидентів та нештатних ситуацій викликаних реалізацією кібератак різного класу.	**Г1.** Здатність здійснювати заходи щодо реагування на кібератаки і нештатні ситуації, координувати дії з усунення наслідків інцидентів, забезпечувати безперервність операційних процесів та відновлення штатного функціонування інфраструктури організації.	**Г1.З1.** Категорії інцидентів, процедур і термінів реагування на інциденти. **Г1.З2.** Методологію реагування на інциденти і обробки даних інцидентів.. **Г1.З3.** Прикладні програми, які можуть реєструвати помилки, позаштатні ситуації, збої в прикладних програмах та вести лог- журнал. **Г1.З4.** Те, що являє собою мережева атака, і який існує зв'язок між мережевими атаками і загрозами та вразливостями. **Г1.З5.** Поширені вектори атак на мережевому рівні.	**Г1.У1.** Розроблювати, тестувати і впроваджувати плани реагування на нештатні ситуації і відновлення мережевої інфраструктури.	**Г1.К1.** Розроблювати вказівки і настанови для працівників, залучених до реагування на кібератаки і нештатні ситуації та заходів відновлення функціонування інфраструктури організації.	**Г1.В1.** Оперативно та ефективно реагувати на кібератаки та нештатні ситуації.

	Г2. Здатність розробляти плани безперервності бізнесу, плани стійкості та плани відновлення, впроваджувати їх та координувати виконання необхідних дій для забезпечення швидкого і ефективного відновлення інфраструктури.	**Г2.З1.** Те, як повинна функціонувати система безпеки (включаючи її можливості відмовостійкості та надійності), а також як вплинуть на неї зміни умов, операцій та інфраструктури. **Г2.З2.** Процедури і процеси управління інцидентами, проблемами і подіями. **Г2.З3.** Порядок розроблення контрзаходів для виявлених ризиків безпеки. **Г2.З4.** Методологію відмовостійкості систем. **Г2.З5.** Порядок впровадження системи безпеки мережі (наприклад, підсистема IDS, виявлення вторгнень, розташована в IP-вузлі, система попередження вторгнень IPS, списки доступу), включаючи знання їх функцій і розміщення компонентів в мережі.	**Г2.У1.** Налаштовувати і використовувати ПЗ захисту комп'ютерів (наприклад, програмні фільтри, антивірусна програма й антишпигунське ПЗ). **Г2.У2.** Забезпечувати інтеграцію процесів управління інформаційною безпекою з процесами стратегічного та операційного планування.	**Г2.К1.** Координувати з вищим керівництвом організації для розробки планів безперервності бізнесу, планів стійкості та планів відновлення. **Г2.К2.** Адаптувати технічну інформацію для планування до рівня розуміння користувача/споживача/ замовника.	**Г2.В1.** Забезпечувати високий рівень готовності організації до дій в умовах кризи, катастрофи або кібератаки.

		Г2.З6. Стратегії управління ризиками та стратегії їх зменшення.			
	Г3. Здатність визначати потенційні ризики, пов'язані з кібератаками і нештатними ситуаціями, виявляти тренди та шаблони кібератак, розробляти стратегії та контрзаходи для зменшення ризиків, оцінювати вразливості та потенційні наслідки інцидентів.	**Г3.З1.** Потенційні вразливості кібербезпеки в галузевих технологіях. **Г3.З2.** Принципи, можливості, обмеження та наслідки кібердій (наприклад, кіберзахисту, збору інформації, підготовки середовища, кібератаки).	**Г3.У1.** Розроблювати контрзаходи для виявлення ризиків безпеки. **Г3.У2.** Розпізнавати зміни у системі або середовищі, які можуть змінити залишкові ризики по відношенню до ризик-апетиту. **Г3.У3.** Розробляти та застосовувати стратегії управління ризиками та їх зменшення.	**Г3.К1.** Розробляти вказівки і настанови для працівників, залучених до реагування на кібератаки і нештатні ситуації та заходів для зменшення ризиків. **Г3.К2.** Комунікувати з вищим керівництвом організації для розробки стратегії та контрзаходів для зменшення ризиків.	**Г3.В1.** Розробляти контрзаходи для потенційних загроз безперервності та стійкості функціонування систем.
Д. Розробка та підтримка методології аудиту організації, впровадження та виконання процедур зовнішнього аудиту та/або операційного аудиту інформаційних систем і технологій на основі визначення й прогнозування ризиків з метою забезпечення	**Д1.** Здатність розробляти та застосовувати методологію, яка охоплює процес зовнішнього аудиту та/або операційного аудиту інформаційних систем і технологій, включаючи перевірку відповідності контрольних механізмів вимогам кібербезпеки.	**Д1.З1.** Стандарти, політики і авторизовані підходи до проєктування системного ПЗ, прийнятих в організації (наприклад, стандарти міжнародної організації зі стандартизації [ISO]). **Д1.З2.** Принципи створення систем інформаційної безпеки (NIST SP 800-160).	**Д1.У1.** Управляти активами, ресурсами для тестування і спеціалістами з тестування з метою забезпечення ефективного проведення заходів з аудиту. **Д1.У2.** Розроблювати профільні методичні посібники.	**Д1.К1.** Здійснювати зворотній зв’язок з компетентними організаціями та стейкхолдерами для розроблення методологічних рекомендацій для більш ефективного проведення аудиту інформаційних систем і технологій.	**Д1.В1.** Розробляти методології для якісного проведення аудиту інформаційних систем і технологій.

безпеки інформації та/або кібербезпеки інформаційних ресурсів й виконання стратегічних планів функціонування й розвитку інформаційної інфраструктури організації, відокремленої програми або консорціуму підприємств.		**Д1.З3.** Вимоги до критичної інформації і того, як ці вимоги використовуються при плануванні.	**Д1.У3.** Розроблювати профільну технічну документацію.		
	Д2. Здатність виявляти та прогнозувати ризики, пов'язані з безпекою інформаційних ресурсів, оцінювати ефективність контрольних заходів, розробляти плани мінімізації ризиків та рекомендувати стратегії для їх контролю та попередження.	**Д2.З1.** Нові і виникаючі ІТ та технологій кібербезпеки. **Д2.З2.** Методології оцінки ризиків. **Д2.З3.** Сучасні і перспективні кібертехнології.	**Д2.У1.** Проводити оцінку впливу/ризику. **Д2.У2.** Імітувати поведінку загроз. **Д2.У3.** Передбачати ключові дії цілі або загрози, які, швидше за все, потребують від керівництва прийняття будь-яких рішень. **Д2.У4.** Прогнозувати нові загрози безпеки.	**Д2.К1.** Комунікувати з керівниками організації різних рівнів, із представниками зацікавлених сторін стосовно розробки планів мінімізації ризиків, їх контролю та попередження.	**Д2.В1.** Створювати плани для попередження або мінімізації ризиків на основі прогнозування загроз безпеці інформаційних технологій.
Е. Надання консультацій, розроблення навчальних програм та проведення тренінгів (навчання) з напряму розробки, впровадження та виконання процедур внутрішнього та	**Е1.** Здатність складати навчальні програми з впровадженням до них стандартів інформаційної безпеки, створювати ефективні навчальні матеріали відповідно до потреб персоналу організацій, що охоплюють основні	**Е1.З1.** Методика оцінки навчання (рубрики, плани оцінювання, тестування, вікторини). **Е1.З2.** Стилі навчання (наприклад, асиміляторний, слуховий і кінестетичне навчання). **Е1.З3.** Режими навчання (наприклад, механічне	**Е1.У1.** Розроблювати і виконувати навчальні плани і програми технічної підготовки. **Е1.У2.** Використовувати або розроблювати освітні заходи (наприклад, програм навчання,	**Е1.К1.** Розробляти або допомогати в розробці навчальних матеріалів для покращення розуміння співробітниками основних аспектів внутрішнього та зовнішнього аудиту	**Е1.В1.** Формувати структуровані та комплексні навчальні програми з урахуванням основних аспектів аудиту інформаційних систем і технологій.

зовнішнього аудиту інформаційних систем і технологій для персоналу організацій та іншим зацікавленим сторонам.	аспекти аудиту інформаційних систем і технологій.	запам’ятовування, спостереження). **E1.З4.** Принципи і процеси проведення тренінгів та оцінки потреб у навчанні. **E1.З5.** Принципи і методи тренінгів та освіти для розробки навчально-методичних матеріалів для індивідуального і групового навчання та освіти, а також вимірювання результатів навчання і освіти.	навчальних ігор, інтерактивних занять). **E1.У3.** Задіювати кращі практики і отримані уроки зовнішніх організацій і освітніх установ які мають справу з ситуаціями кібербезпеки.	інформаційних систем і технологій. **E1.К2.** Розробляти критерії оцінювання та тести для персоналу з метою визначення рівня обізнаності персоналу щодо основних аспектів аудиту інформаційних систем і технологій.	**E1.В2.** Створювати ефективні навчальні матеріали, такі як презентації, посібники, онлайн-курси, вебінари тощо, які будуть адаптовані до різних рівнів знань та потреб персоналу організацій.
	E2. Здатність проводити тренінги та консультації з аудиту інформаційних систем і технологій, передаючи складну технічну інформацію чітко, зрозуміло та доступно.	**E2.З1.** Політики, процеси і процедури тренінгів та навчання в організації. **E1.З4.** Принципи і процеси проведення тренінгів та оцінки потреб у навчанні. **E1.З5.** Принципи і методи тренінгів та освіти для розробки навчально-методичних матеріалів для індивідуального і групового навчання та освіти, а також вимірювання результатів навчання і освіти.	**E2.У1.** Використовувати технології в освітніх цілях (наприклад, інтерактивні дошки, Web-сайти, комп'ютери, проектори). **E2.У2.** Готувати та проводити навчальні та брифінги з обізнаності щоб забезпечити, що користувачі систем, мереж і даних дотримуються політик і процедур безпеки. **E2.У3.** Встановлювати ефективний зворотний	**E2.К1.** Розмовляти з іншими, щоб ефективно передавати інформацію. **E2.К2.** Комунікувати з керівниками всіх рівнів, включаючи членів правління (наприклад, навички міжособистісного спілкування, доступність, уміння ефективно сприймати мову виступаючих, відповідне аудиторії використання стилю і мови виступу).	**E2.В1.** Проводити ефективні навчальні сесії та консультації з використанням наочних прикладів.

			зв'язок зі студентами з метою вдосконалення навчання.	**Е2.К3.** Розробляти тести для визначення рівня обізнаності та участі працівників щодо здійснення заходів аудиту інформаційних систем і технологій.	
Є. Формування (підготовка), впровадження та виконання процедур внутрішнього аудиту та/або операційного аудиту систем менеджменту інформаційної безпеки організації, а також об'єктів критичної інфраструктури на основі чинного законодавства, вітчизняної та міжнародної системи стандартизації та кращих світових практик.	**Є1.** Здатність розробляти та застосовувати процедури аудиту систем менеджменту інформаційної безпеки, проводити перевірку відповідності політикам, стандартам і нормам в організаціях та на об'єктах критичної інфраструктури.	**Є1.31.** Принципів створення систем інформаційної безпеки (NIST SP 800-160). **Є1.32.** Вимог та методів захисту, що стосуються інформаційної безпеки відповідно до міжнародних стандартів ISO 27001 та NIST SP 800-53. **Є1.33.** Політики безпеки в організації. **Є1.34.** Системи управління безпекою.	**Є1.У1.** Управляти наявними активами, ресурсами і фахівцями з аудиту з метою забезпечення ефективного проведення заходів з аудиту систем менеджменту інформаційної безпеки. **Є1.У2.** Розроблювати звітні документи за результатами аудиту систем менеджменту інформаційної безпеки. **Є1.У3.** Орієнтуватися в законах, політиках, процедурах, що стосуються кібербезпеки об'єктів критичної інфраструктури.	**Є1.К1.** Структурувати інформацію та формувати свої висновки в письмовій формі чітко та зрозуміло **Є1.К2.** Ефективно співпрацювати в команді та координувати виконання завдань.	**Є1.В1.** Впроваджувати та використовувати найбільш ефективні процедури і методи аудиту систем менеджменту інформаційної безпеки.

	Є2. Здатність аналізувати результати аудиту, виявляти залежності та здійснювати оцінку ризиків в системах менеджменту інформаційної безпеки, розробляти та рекомендувати ефективні заходи контролю для зниження ризиків	**Є2.З1.** Методи аналізу результатів аудиту систем менеджменту інформаційної безпеки.	**Є2.У1.** Виявляти системні проблеми безпеки на основі аналізу даних вразливостей та конфігурації. **Є2.У2.** Застосовувати принципи кібербезпеки і приватності при формуванні вимог організації (стосовно конфіденційності, цілісності, доступності, автентифікації і неспростовності).	**Є2.К1.** Ефективно співпрацювати в команді та координувати виконання профільних завдань.	**Є2.В1.** Якісно оцінювати ризики для їх зниження та запобігання загрозам. **Є2.В2.** Формувати рекомендації для покращення системи менеджменту інформаційної безпеки.
	Є3. Здатність розробляти та впроваджувати стратегічні плани для поліпшення системи менеджменту інформаційної безпеки організації.	**Є3.З1.** Мінімальні вимоги до розробки, впровадження, підтримки та постійного поліпшення системи менеджменту інформаційної безпеки відповідно до стандарту ISO 27001. **Є3.З2.** Сучасні тренди і технології в галузі інформаційної безпеки та їх вплив на стратегічне планування	**Є3.У1.** Застосовувати принципи кібербезпеки і приватності при стратегічних планів організації (стосовно конфіденційності, цілісності, доступності, автентифікації і неспростовності). **Є3.У2.** Правильно та ефективно обирати пріоритети і розподіляти ресурси кібербезпеки.	**Є3.К1.** Приймати участь у розробленні та впровадженні стратегічних планів поліпшення системи менеджменту інформаційної безпеки організації. **Є3.К2.** Комунікувати з керівниками організації різних рівнів в питаннях стратегічного планування поліпшення системи менеджменту	**Є3.В1.** Брати участь у створенні стратегічних планів для поліпшення системи менеджменту інформаційної безпеки.

				інформаційної безпеки організації.	
Ж. Контроль та оцінка ефективності поточного стану функціонування систем и менеджменту інформаційної безпеки організації (в т.ч. об’єктів критичної інфраструктури), оцінювання ефективності сталих бізнес-операційних процесів з метою забезпечення встановленої мети, стратегії, політик безпеки різного рівня згідно з вітчизняними та міжнародними вимогами і стандартами.	**Ж1.** Здатність визначати методи та процедури для здійснення заходів контролю та оцінки функціонування системи менеджменту інформаційної безпеки, незалежних оглядів та планових аудитів.	**Ж1.З1.** Оцінка загальних принципів управління ризиками. **Ж1.З2.** Засоби контролю в процесах використання, обробки, зберігання та передачі даних. **Ж1.З3.** Методи, процедури і способи збору інформації, її обробки, спільного використання та формування звітності. **Ж1.З4.** Методи і принципи аналізу прийняті в організації та галузевих стандартах. **Ж1.З5.** Сучасні методи оцінки, впровадження та розповсюдження інструментів та процедур оцінки функціонування системи менеджменту інформаційної безпеки, на основі стандартів.	**Ж1.У1.** Інтерпретувати термінологію, методологію та процедури комунікаційної безпеки (COMSEC).	**Ж1.К1.** Навичка комунікувати та проводити обговорення для визначення методів та процедур здійснення заходів контролю.	**Ж1.В1.** Забезпечувати використання найбільш ефективних методів та процедур для оцінки функціонування системи менеджменту інформаційної безпеки.

	Ж2. Здатність аналізувати та оцінювати поточний стан функціонування системи менеджменту інформаційної безпеки, ідентифікувати потенційні ризики, проводити оцінку ефективності бізнес-операційних процесів та відповідності політикам, стратегіям і стандартам безпеки.	**Ж2.З1.** Аналітичні конструкції та їх використання для оцінки функціонування системи менеджменту інформаційної безпеки.	**Ж2.У1.** Проводити всебічну оцінку застосованих в системі або успадкованих системою управлінських, операційних і технічних контролів безпеки і їх удосконалень для визначення результативності контролів (тобто якою мірою контроль безпеки впроваджений коректно, функціонує як передбачено, чи досягається бажаний результат, що задовольняє вимогам безпеки для системи). **Ж2.У2.** Здатність готувати заключний звіт з оцінки безпеки, включаючи результати і висновки оцінки. **Ж2.У3.** Здатність застосовувати кращі практики впровадження контролів безпеки в систему.	**Ж2.К1.** Комунікувати зі стейкхолдерами щодо розробки стратегій поліпшення функціонування системи менеджменту інформаційної безпеки.	**Ж2.В1.** Оцінити стан системи менеджменту інформаційної безпеки та сформувати якісний звіт, включаючи результати і висновки.

З. Формування (підготовка), впровадження та виконання процедур зовнішнього аудиту та/або операційного аудиту систем менеджменту інформаційної безпеки організації, а також об'єктів критичної інфраструктури на основі чинного законодавства, вітчизняної та міжнародної системи стандартизації та кращих світових практик.	**З1.** Здатність планувати, впроваджувати та здійснювати процедури зовнішнього аудиту та операційного аудиту систем менеджменту інформаційної безпеки, здійснювати оцінку відповідності політикам, стратегіям і стандартам безпеки згідно чинного законодавства та міжнародних стандартів.	**З1.З1.** Вимоги до критичних інформаційних технологій. **З1.З2.** Закони, політики, процедури чи корпоративне управління, що стосуються кібербезпеки критичних інфраструктур. **З1.З3.** Законодавство та правові аспекти в сфері кіберзахисту критичної інфраструктури.	**З1.У1.** Розробка звітних документів за результатами аудиту систем менеджменту інформаційної безпеки. **З1.У2.** Переводити дані і результати тестування в оціночні висновки. **З1.У3.** Перевіряти політику, плани і стратегії на відповідність до законодавства, регуляторних актів, політик і стандартів що регулюють кібердіяльність.	**З1.К1.** Вміння структурувати інформацію та формувати свої висновки в письмовій формі чітко та зрозуміло. **З1.К2.** Здатність ефективно співпрацювати в команді та координувати виконання завдань.	**З1.В1.** Забезпечувати ефективне проведення аудиту системи менеджменту інформаційної безпеки.
	З2. Здатність аналізувати ефективність функціонування систем менеджменту інформаційної безпеки та бізнес-операційних процесів, виявляти потенційні ризики та виявляти слабкі місця у політиках безпеки, розробляти рекомендації для поліпшення інформаційної безпеки.	**З2.З1.** Аналітичні конструкції та їх використання для оцінки функціонування систем менеджменту інформаційної безпеки.	**З2.У1.** Застосування технік підвищення вимог до системи, мережі і ОС (наприклад, виключення незатребуваних послуг, парольних політик, сегментація мережі, використання журналу реєстрації, мінімум привілеїв і т.п.). **З2.У2.** Ділитися змістовною	**З2.К1.** Навичка комунікувати з персоналом організацій та командою з аудиту для оцінки ефективності функціонування системи менеджменту інформаційної безпеки.	**З2.В1.** Якісно оцінювати ризики та виявляти вразливості з метою попередження загроз для інформаційної безпеки. **З2.В2.** Формувати рекомендації для покращення системи менеджменту інформаційної безпеки.

			інформацією про контекст середовища загроз для організації, що покращує її позицію управління ризиками.		
	З3. Здатність розробляти та впроваджувати стратегічні плани для поліпшення системи менеджменту інформаційної безпеки організації.	**З3.З1.** Безперервність бізнесу та операційні плани відновлення безперервності після катастроф.	**З3.У1.** Застосовувати принципи кібербезпеки і приватності при формуванні організаційних вимог (які стосуються конфіденційності, цілісності, доступності, автентифікації і неспростовності). **З3.У2.** Розробляти політику, плани і стратегії відповідно до законодавства, регуляторних актів, політик і стандартів на підтримку кібердіяльності організації.	**З3.К1.** Навичка комунікувати з керівниками, зацікавленими та відповідальними особами щодо розробки стратегічних планів поліпшення системи менеджменту інформаційної безпеки організації.	**З3.В1.** Брати участь у створенні стратегічних планів для підвищення ефективності та надійності системи менеджменту інформаційної безпеки.
И. Розробка та підтримка методології аудиту систем менеджменту інформаційної безпеки організації,	**И1.** Здатність розробляти та застосовувати методологію, яка охоплює процес зовнішнього аудиту та/або операційного	**И1.З1.** Вимоги до критичної інформації і того, як ці вимоги використовуються в процесах зовнішнього аудиту та/або	**И1.У1.** Управління активами, ресурсами і спеціалістами з аудиту для забезпечення ефективного проведення заходів з	**И1.К1.** Здійснювати зворотній зв’язок з компетентними організаціями та зацікавленими сторонами для	**И1.В1.** Розробляти методології для якісного проведення аудиту систем менеджменту

впровадження та виконання процедур зовнішнього аудиту та/або операційного аудиту з метою забезпечення інформаційної безпеки та/або кібербезпеки організації, об’єктів критичної інфраструктури або консорціуму підприємств.	аудиту систем менеджменту інформаційної безпеки, включаючи перевірку відповідності контрольних механізмів політикам, вимогам та провідним світовим стандартам інформаційної безпеки.	операційного аудиту систем менеджменту інформаційної безпеки. **И1.З2.** Методології оцінки ризиків при проведенні аудиту систем менеджменту інформаційної безпеки.	аудиту систем менеджменту інформаційної безпеки. **И1.У2.** Розробляти вимоги до інформаційної безпеки у процес закупівлі, використовуючи застосовні базові контролі безпеки у якості одного із джерел вимог безпеки.	розроблення методологічних рекомендацій для більш ефективного проведення аудиту систем менеджменту інформаційної безпеки.	інформаційної безпеки.
	И2. Здатність ефективно спілкуватися із зацікавленими сторонами, включаючи клієнтів, керівництво організації та інші аудиторські команди для підвищення якості процедур аудиту та надання рекомендацій з питань інформаційної безпеки.	**И2.З1.** Процеси і процедури усунення конфліктних ситуацій. **И2.З2.** Звітність щодо усунення конфліктних ситуацій, включаючи взаємодію з зовнішніми організаціями. **И2.З3.** Різні цілі організації на всіх рівнях, включаючи рівень підлеглих, рівень рівнозначних співробітників і рівень керівників. **И2.З4.** Цілі організації, визначені керівництвом пріоритети і ризики при прийнятті рішень. **И2.З5.** Політики організації і концепції	**И2.У1.** Управління відносинами з клієнтами, включаючи визначення потреб/вимог клієнтів, управління очікуваннями клієнта та демонстрацію відданості досягненню якісних результатів. **И2.У2.** Використання зворотного зв'язку з метою вдосконалення процесів, продуктів і послуг. **И2.У3.** Зрозуміла, переконлива і системна подача фактів та ідей в письмовій формі.	**И2.К1.** Навичка розмовляти з іншими з метою доступної передачі інформації. **И2.К2.** Навичка комунікації з із зацікавленими сторонами, включаючи клієнтів, керівництво організації та інші аудиторські команди. **И2.К3.** Навичка взаємодії з замовниками.	**И2.В1.** Встановлювати конструктивний діалог з клієнтами, керівництвом організації та аудиторськими командами, зокрема координувати дії та обмінюватися інформацією для підвищення ефективності процедур аудиту.

		планування співпраці з внутрішніми і/або зовнішніми організаціями.			
І. Формування команди аудиту, керівництво підготовкою та виконанням задач та процедур аудиту та/або операційного аудиту систем менеджменту інформаційної безпеки та кібербезпеки організації, об’єктів критичної інфраструктури або консорціуму підприємств.	**І1.** Здатність формувати та керувати командою аудиту, включаючи призначення завдань, розподіл ролей та виконання планів аудиту, а також мотивувати команду на досягнення цілей аудиту, забезпечувати високу якість виконання робіт.	**І1.З1.** Загальні принципи персоналу у сфері національної кібербезпеки, робочі ролі, а також завдання, знання, навички та здатності, які до них відносяться. **І1.З2.** Процеси управління персоналом, призначення і розміщення.	**І1.У1.** Управління активами, ресурсами для тестування і спеціалістами з тестування з метою забезпечення гарантій ефективного проведення тестових заходів. **І1.У2.** Підготовка і проведення брифінгів. **І1.У3.** Використання віртуальних колективних робочих просторів і/або інструментів (наприклад, IWS, VTC,, чат- кімнати, SharePoint). **І1.У4.** Прийняття рішень у разі виникнення суперечливих вимог до збору додаткових даних.	**І1.К1.** Навичка комунікувати з іншими для керівництва, підготовки та виконання задач аудиту систем менеджменту інформаційної безпеки.	**І1.В1.** Контролювати виконання завдань членами команди аудиту, в тому числі щодо термінів. **І1.В2.** Забезпечувати ефективне виконання плану для досягнення цілей аудиту.

	I2. Здатність ефективної комунікації із зацікавленими сторонами, включаючи керівництво організації та інших учасників процесу аудиту, здатність пояснювати складні концепції та формувати рекомендації чітко, зрозуміло та доступно.	**I2.З1.** Цілі організації на всіх рівнях, включаючи рівень підлеглих, рівень рівнозначних співробітників і рівень керівників. **I2.З2.** Цілі організації, визначені керівництвом пріоритети і стратегії.	**I2.У1.** Застосовувати навички і стратегії спільної роботи.	**I2.К1.** Навичка комунікації з іншими, щоб пояснювати складні концепції. **I2.К2.** Навичка комунікації з керівниками всіх рівнів для зрозумілого та доступного формування та пояснення рекомендацій.	**I2.В2.** Надавати чіткі рекомендації, які будуть доступні для розуміння на рівні користувача.

VI. Розподіл трудових функцій та компетентностей за професійними кваліфікаціями

Трудова функція (умовне позначення)	Загальна назва професійної кваліфікації у межах професійного стандарту: Аудитор інформаційних технологій (з кібербезпеки)				
	Аудитор інформаційних технологій (з кібербезпеки)	Провідний аудитор інформаційних технологій (з кібербезпеки)	Аудитор систем менеджменту інформаційної безпеки	Провідний аудитор систем менеджменту інформаційної безпеки	Керівник команди з аудиту систем менеджменту інформаційної безпеки
	повна	повна	повна	повна	повна
А	+	+	+	+	+
Б	+	+	+	+	+
В	+	+			
Г	+	+	+	+	+
Д		+			
Е		+			
Є			+	+	+
Ж			+	+	+
З				+	+
И				+	+
І					+

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:

Маллєр Анатолій Сергійович, начальник 7 відділу Департаменту державного контролю у сфері захисту інформації Адміністрації Держспецзв'язку;

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

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

Бодюл Євген Миколайович, начальник управління освітньої діяльності Департаменту освіти, науки і спорту Міністерства внутрішніх справ України;

Василіу Євген Вікторович, професор кафедри кібербезпеки та технічного захисту інформації факультету інформаційних технологій та кібербезпеки Державного університету інтелектуальних технологій і зв'язку;

Гнатюк Віктор Олександрович, доцент кафедри телекомунікаційних та радіоелектронних систем факультету аеронавігації, електроніки телекомунікацій Національного авіаційного університету;

Губрієнко Роман Григорович, заступник директора департаменту - начальник 3 управління Департаменту державного контролю у сфері захисту інформації Адміністрації Держспецзв'язку;

Діденко Олександр Андрійович, спеціаліст за рахунок посади головного спеціаліста 7 відділу Департаменту державного контролю у сфері захисту інформації Адміністрації Держспецзв'язку;

Дідик Валерія Анатоліївна, керівник напряму з розвитку професійних навичок з кібербезпеки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»;

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

Легомінова Світлана Володимирівна, завідувач кафедри управління інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації Державного університету телекомунікацій;

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

Маковець Сергій Валентинович, директор технологій ТОВ «ІНФОРМЕЙШН СІСТЕМС СЕК'ЮРІТІ ПАРТНЕРС»;

Мельник Сергій Вікторович, консультант напряму 3 розвитку професійних навичок з кібербезпеки Проекту USAID «Кібербезпека критично важливої інфраструктури України»;

Мохор Володимир Володимирович, директор Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук 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»;

Педченко Євгеній Миколайович, керівник відділу впровадження систем безпеки ТОВ «ІНТРАСИСТЕМС»;

Проскуровський Роман Васильович, заступник керівника Центру кіберзахисту Національного банку України;

Раківська Адель Юріївна, спеціаліст за рахунок посади головного спеціаліста 7 відділу Департаменту державного контролю у сфері захисту інформації Адміністрації Держспецзв'язку;

Толюпа Сергій Васильович, професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка;

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 «Аудитор інформаційних технологій (з кібербезпеки)» вимог Порядку розроблення, введення в дію та перегляду професійних стандартів, затвердженого постановою Кабінету Міністрів України від 31.05.2017 р. № 373).

4. Реквізити висновку репрезентативних всеукраїнських об'єднань професійних спілок на галузевому рівні про погодження проєкту професійного стандарту

Висновок Профспілки працівників зв'язку України від _____ щодо погодження проєкту професійного стандарту «Аудитор інформаційних технологій (з кібербезпеки)».

VIII. Дата внесення професійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.