Проєкт

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

Професійний стандарт

УПОВНОВАЖЕНИЙ З АВТОРИЗАЦІЇ БЕЗПЕКИ ІНФОРМАЦІЇ

_____(дата внесення до Реєстру кваліфікацій)

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

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

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

- висновку Профспілки працівників зв'язку України від _____ щодо погодження проєкту професійного стандарту

І. Назва професійного стандарту

Уповноважений з авторизації безпеки інформації

ІІ. Загальні відомості про професійний стандарт

1. Мета діяльності за професією

Здійснення комплексної, всебічної та послідовної процедури авторизації та оцінки вищого управлінського рівня ефективності реалізації стратегії безпеки (включно: місія, політики безпеки, функції, імідж чи репутація) організації, установи, об'єднання підприємств або програми, як окремий етап порядку впровадження системи безпеки інформації, захист якої передбачено чиним законодавством.

Здійснення встановлених нормативно-правових та організаційно-технічних заходів, щодо проведення процедури авторизації (в т. ч. державної) або/чи експертизи встановлених безпекових послуг та технічних вимог, методів та заходів забезпечення інформаційної безпеки або\чи кібербезпеки інформаційно-комунікаційних систем (або\чи інформаційних, автоматизованих, систем електронних комунікацій), що розгорнуті та експлуатуються державними органами та установами, підприємствами та організаціями всіх форм власності.

Здійснення повноважень вищого рівня із забезпечення офіційної відповідальності за проведення процедур впровадження, контролю, постійного моніторингу, оцінювання та супроводження процесів перевірки, оцінки і створення пакету авторизації інформаційних технологій та систем у відповідності до цільового (адаптованого) профілю безпеки організації.

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

Секція	Назва секції	№ розділу	Назва розділу	№ групи (класу)	Назва групи (класу)
Секція J	Інформація та телекомунікації	**Розділ 61**	Телекомунікації (електрозв'язок)	**Група 61.1**	Діяльність у сфері проводового електрозв'язку
				Клас 61.10	
				Група 61.2	Діяльність у сфері безпроводового електрозв'язку
				Клас 61.20	
				Група 61.9	Інша діяльність у сфері електрозв'язку
				Клас 61.90	

		Розділ 62	Комп'ютерне програмування, консультування та пов'язана з ними діяльність	**Група 62.0**	Комп'ютерне програмування, консультування та пов'язана з ними діяльність
				Клас 62.01	Комп'ютерне програмування
				Клас 62.02	Консультування з питань інформатизації
				Клас 62.03	Діяльність із керування комп'ютерним 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	
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»

Уповноважений з авторизації безпеки інформації, 2139.2.

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

Уповноважений з авторизації безпеки інформації 7 рівень НРК

Старший уповноважений з авторизації безпеки інформації 7 рівень НРК

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

- диплом бакалавра за спеціальністю:

- 121 «Інженерія програмного забезпечення» галузі знань 12 «Інформаційні технології» (6 рівень НРК);

- 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології» (6 рівень НРК);

- 123 «Комп'ютерна інженерія» галузі знань 12 «Інформаційні технології» (6 рівень НРК);

- 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» (6 рівень НРК);

- 126 «Інформаційні системи та технології» галузі знань 12 «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);

- 257 «Управління інформаційною безпекою» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» (6 рівень НРК).

- диплом магістра (для старшого уповноваженого) за спеціальністю:

- 121 «Інженерія програмного забезпечення» галузі знань 12 «Інформаційні технології» (7 рівень НРК);

- 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології» (7 рівень НРК);

- 123 «Комп'ютерна інженерія» галузі знань 12 «Інформаційні технології» (7 рівень НРК);

- 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» (7 рівень НРК);

- 126 «Інформаційні системи та технології» галузі знань 12 «Інформаційні технології» (7 рівень НРК);

- 171 «Електроніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (7 рівень НРК);

- 172 «Електронні комунікації та радіотехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (7 рівень НРК);

- 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» галузі знань 17 «Електроніка, автоматизація та електронні комунікації» (7 рівень НРК);

- 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 авторизації безпеки інформації;
- документ (диплом, сертифікат, тощо), щодо післядипломної освіти та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань в рамках консультаційно-навчальної діяльності у сфері авторизації безпеки інформації;
- документ (диплом, сертифікат, тощо), щодо професійної сертифікації та надбання додаткових навичок, знань та умінь, які підтверджують здатність до фахового виконання завдань у сфері авторизації безпеки інформації.

ІІІ. Здобуття професійної кваліфікації та професійний розвиток

1. Здобуття професійної кваліфікації

Назва професійної та/або часткової професійної кваліфікації	**Суб'єкти, уповноважені законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій**	
	Кваліфікаційні центри	**Суб'єкти освітньої діяльності**
Уповноважений з авторизації безпеки інформації	Підготовка на першому (бакалаврському) рівні вищої освіти за спеціальностями, вказаними у п. ІІ.5 або «Фахівець з оцінки заходів захисту інформації (кібербезпеки)» та 3 роки досвіду роботи за спеціальністю.	*Не передбачено професійним стандартом*
Старший уповноважений з авторизації безпеки інформації	Підготовка на другому (магістерському) рівні вищої освіти за спеціальностями вказаними у п. ІІ. 5 або «Провідний фахівець з оцінки заходів захисту інформації (кібербезпеки)» та 5 років досвіду роботи за спеціальністю	*Не передбачено професійним стандартом*

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**
Уповноважений з авторизації безпеки інформації	Підвищення кваліфікації уповноваженого з авторизації безпеки інформації для отримання професійної кваліфікації старшого уповноваженого з авторизації безпеки інформації. Стаж роботи за спеціальністю не менше п'яти років	*Не передбачено професійним стандартом*

IV. Абревіатури, скорочення

ІТ	інформаційні технології
ІС	інформаційна система
ІКС	інформаційно-комунікаційна система
ЕКС	електронна комунікаційна система
СБІ	системи безпеки інформації
ПВПД	плануй – виконуй – перевіряй – дій
ISO/IEC 27001:2015	Міжнародний стандарт в галузі ІТ «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. (англ.: Information technology - Security techniques - Information security management systems - Requirements»).
УОА	уповноважений орган з авторизації
FEA	Federal Enterprise Architecture
PCI	Payment Card Industry
PHI	Protected Health Information
ЦПБ ІС	цільовий профіль безпеки інформаційної системи
ІзОД	інформація з обмеженим доступом
ПА	пакет авторизації
БПБ	базовий профіль безпеки
ЦПБ	цільовий профіль безпеки
ГПБ	галузевий профіль безпеки
ДМЗ	демілітаризована зона
EBSCO	Elton Bryson Stephens Company
JSTOR	Journal Storage
RMF	Risk Management Framework

ISO/IEC 15026-2	Міжнародний стандарт в галузі ІТ «Інженерія систем і програмних засобів. Гарантії систем і програмного забезпечення». Частина 2. Сценарій гарантування (англ.: Systems and software engineering - Systems and software assurance - Part 2: Assurance case)
ЗЗІ	Засоби захисту інформації
БІ	безпека інформації
PII	Personally Identifiable Information
АПБ	адаптована політика безпеки
NIST SP 800-161	National Institute of Standards and Technology Special Publication 800-161
АС	Автоматизована система
PL/SQL	Procedural Language / Structured Query Language

V. Опис трудових функцій

Трудові функції	Компетентності	Результати навчання			
		Знання	**Уміння/ навички**	**Комунікація**	**Відповідальність і автономія**
А. Управління процедурами авторизації системи безпеки ІС (АС, ІКС або СЕК) з метою прийняття рішення щодо можливості внесення ІС до реєстру авторизованих систем на основі аналізу встановленого пакету документів авторизації.	**А1**. Здатність управляти процедурами авторизації системи безпеки ІС (АС, ІКС або СЕК) в державних органах, на підприємствах, в організаціях різних форм власності, а також в інформаційно-комунікаційних системах де обробляється інформація ІзОД захист якої встановлений чинним законодавством.	**А1.З1.** Процедури авторизації ІС, як офіційне управлінське рішення, що надається уповноваженим на авторизацію органом для надання дозволу на використання системи безпеки інформації (або системи менеджменту інформаційної безпеки) у відповідності до встановлених послуг та політики. **А1.З2.** Концепцію та програму безпеки інформації та безпосередньо її властивостей (конфіденційності, цілісності та доступності), прийняті на вищому організаційному рівні з урахуванням	**А1.У1.** Реалізовувати на практиці задачі і завдання авторизації ІС керівництва, пов'язані з процесами і рішенням проблем організації **А1.У2.** Розробляти та реалізовувати концепцію або\чи стратегію системи менеджменту інформаційної безпеки, а також її авторизувати на вищому організаційному рівні встановлених вимог. **А1.У3.** Розробляти та реалізовувати програму безпеки інформації ІС згідно з встановленими технічними характеристиками та послугами безпеки у відповідності до	**А1.К1.** Авторизувати систему безпеки інформації ІС, як етап створення системи безпеки інформації в організації, що ґрунтується на моделі стандарту ISO/IEC 27001:2015 **А1.К2.** Авторизувати безпеку ІС, як етап порядку впровадження систем безпеки інформації в державних органах, на підприємствах, в організаціях, а також ІС в яких обробляється інформація ІзОД що підлягає	**А1.В1**. Відповідати за підготовку та контроль розробки та впровадження пакету авторизації, що покладена на Власника (Розпорядника) ІС. **А1.В2** Відповідати за безпосереднє виконання функцій, адміністратора безпеки або інших осіб, на яких покладено функції забезпечення безпеки інформації ІС та захисту персональних даних.

		встановленої політики безпеки. **А1.З3.** Політику безпеки інформації та План заходів захисту, які, зокрема, призначені для задоволення відповідних вимог безпеки на базі системи (політики) управління ризиками. **А1.З4.** Концепції побудови захищених ІС, а також методології забезпечення мережевої безпеки. **А1.З5**. Джерела вразливостей інформаційним ресурсам, включно операційним системам, додаткам, спеціалізованому програмному забезпеченню, тощо. **А1.З3.** Моделі системи безпеки (моделі конфіденційності, цілісності та доступності (КЦД); модель Белла-	стратегії і політик безпеки інформації. **А1.У4.** Розробляти, реалізовувати та оцінювати політику безпеки інформації різних рівнів. **А1.У5.** Розробляти, реалізовувати та оцінювати План заходів захисту, вибрані для задоволення відповідних вимог системи (політик) управління ризиками безпеки інформації; зокрема, методології та показники, які використовуватимутьс я для оцінювання заходів захисту інформації та персональних даних. **А1.У1.** Реалізовувати на практиці технологічні задачі і завдання управління та керівництва, пов’язані з бізнес-операційними процесами, нормативно-правовим	захисту згідно чинного законодавства.	

		Лападули, моделі забезпечення цілісності «Biba» і Кларка-Вілсона).	та організаційно-технічним забезпеченням СБІ.		
	А2. Здатність готувати та оцінювати пакет авторизації для передачі до уповноваженого органу з авторизації з метою проведення процедури авторизації системи безпеки, на основі вхідних даних щодо впровадження заходів захисту (в т.ч. цільові профілі системи безпеки ІС (АС, ІС або СЕК), звіти оцінювачів)	**А2.З1.** Пакет авторизації та процедури його аналізу, який передається в уповноважений орган з авторизації з метою прийняття рішення щодо можливості внесення ІС до реєстру авторизованих систем. **А2.З2.** Профілі безпеки ІС та його класифікації, як набори заходів захисту, що застосовуються до інформації або ІС для забезпечення відповідності вимогам чинної нормативної бази, а також такі що спрямовані на захист потреб і послуг системи у відповідності до системи управління ризиками.	**А2.У1**. Готувати та оцінювати пакет авторизації у відповідності до стратегії та політик безпеки організації. **А2.У2.** Розробляти, реалізовувати та оцінювати функціональність галузевого профілю безпеки та / або цільового профілю безпеки, як визначених наборів заходів захисту та додаткових рекомендацій у відповідності до політик безпеки, призначення інформаційної системи, структурно-функціональних характеристик інформаційної системи.	**А2.К1.** Взаємодіяти з власником ІС (розпорядником ІС) та персоналом, який готує та передає до уповноваженого органу авторизації безпеки пакет документів, необхідний для проведення процедури авторизації безпеки	**А2.В1.** Сприяти галузевим організаціям, на яких розгортаються ІС, що підлягають державній авторизації безпеки, готувати звернення до уповноваженого органу відповідної галузі та готувати пакет авторизації.

		А2.З3. Принципи, методи та заходи інформаційної та або\чи кібербезпеки ІС. **А2.З4**. Принципи і методи безпеки інформації та або\чи кібербезпеки, а також організаційно-технічних та нормативно-правових вимог, щодо забезпечення конфіденційності, цілісності, доступності, автентичності і неспростовності. **А2.З5**. Концепції архітектури безпеки організації, розподілу доступу та еталонних моделей архітектури підприємства (наприклад, Zachman, FEA). **А2.З6.** Стандарти безпеки даних в сфері платіжних карт (PCI) **А2.З7.** Стандарти безпеки медичних персональних даних **(**PHI).	**А2.У2.** Розробляти, реалізовувати та оцінювати функціональність контенту галузевого профілю безпеки та / або цільового профілю безпеки, як визначених наборів заходів захисту з урахуванням особливостей галузі, аналізу ризиків безпеки, особливостей функціонування інформаційної системи.		

	А3. Здатність до управління процедурами розгляду та оцінки пакету авторизації, а також розгляду документів уповноваженим органом з авторизації з метою прийняття рішення щодо внесення ІС (АС, ІС або СЕК) в реєстр авторизованих систем та надання можливості Власникові (Розпоряднику) такої ІС приймати рішення щодо введення в експлуатацію всієї ІС з урахування політики мінімізації ризиків та відповідальністю за аспекти розвитку і функціонування інформаційної системи та/або мережі в цілому.	**А3.З1.** Інформацію, методичні рекомендації та вимоги органу з авторизації галузі, який здійснює функції авторизації безпеки ІС. **А3.З2.** Порядок перевірки повноти наданого пакету авторизації**.** **А3.З3.** Порядок перевірки процедур формування контенту профілів безпеки ІС, що виключені із до загальної політики безпеки, аналіз та оцінка ефективності заходів захисту на відповідність меті, призначенню, технічним характеристикам для забезпечення надійного функціонування ІС. **А3.З4.** Порядок перевірки коректності реалізації профілів безпеки у відповідності до політик.	**А3.У1.** Розглядати пакет авторизації уповноваженим з авторизації з метою прийняття рішення щодо внесення ІС в реєстр авторизованих систем **А3.У2.** Проводити аналіз складових та даних, що пакет авторизації містить достатній перелік документів для проведення процедури авторизації безпеки (в т.ч. державної авторизації). **А3.У3.** Переконатися, що профіль безпеки був розроблений на базі актуального базового профілю безпеки або галузевого профілю, що встановлені параметри заходів захисту є вмотивованими та достатніми для забезпечення надійного функціонування ІС.	**А3.К1.** Розглядати пакет авторизації та документувати результати оцінки ефективності проведеної експертизи	**А3.В1.** Відповідальність вести облік контенту та надавати об’єктивну оцінку пакету авторизації, який сформовано відповідно до встановлених процедур діловодства уповноваженого органу авторизації.

		А3.З5. Порядок перевірки повноти, коректності та контенту звіту оцінювача засобів захисту інформації. **А3.З6.** Класифікацію загроз та вразливостей інформаційних ресурсів різних класів. **А3.З7.** Принципи і методи забезпечення безпеки інформаційних технологій (мережеві екрани, демілітаризовані зони, процедури шифрування трафіку та розподілу доступу до інформаційних ресурсів ІС) . **А3.З8.** Нові інформаційні технології та сучасні технології інформаційної безпеки та\чи кібербезпеки.	**А3.У4.** Перевіряти коректність використання в ІС технічних засобів захисту інформації, засобів криптографічного захисту інформації та організаційних заходів. **А3.У5.** Перевіряти звіт оцінювача засобів захисту інформації з метою визначення повноти оцінювання впроваджених заходів захисту, а також достатність наданих доказів та підтверджень для забезпечення ефективності впроваджених політик безпеки. **А3.У1.** Визначати потреби у ефективному забезпеченні безпеки інформаційних технологій та ІС.		

	А4. Здатність управляти створенням та впровадженням захищених інформаційних системи і технології на основі мінімізації ризиків та з відповідальністю за аспекти розвитку і функціонування інформаційної системи та/або мережі	**А4.З1.** Порядок створення та впровадження систем безпеки інформації та кіберзахисту на основі аналізу вразливостей та встановленої політики ризиків. **А4.З2.** Концепції архітектури безпеки мережі, включаючи топологію, протоколи, додатки, компоненти і принципи (формування демілітаризованих зон, прикладна система ешелонованого захисту) **А4.З3.** Закони, політики, процедури та методи корпоративного управління, що стосуються безпеки інформації та кіберзахисту критичної інформаційної інфраструктури різних класів.	**А4.У1.** Виявляти інформаційні технології та системи критичної інфраструктури, які були спроектовані без врахування методів та засобів безпеки інформації та кіберзахисту.	**А4.К1.** Спілкуватися з питань виконання завдань авторизації безпеки ІС та критичної інформації в рамках робочих колективів на підприємстві, установі або організації різних форм власності.	**А4.В1.** Демонструвати обізнаність про законодавчо визначену відповідальність за порушення в сфері авторизації безпеки ІС та обробки і поширення інформації ІзОД.

	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				
Б. Вибір рівня базового (або\чи галузевого) профілю безпеки інформації, а також вибір та впровадження методів та засобів захисту інформації в ІС (АС, ІКС або СЕК), які обробляють критичну інформацію, на основі системи управління ризиками інформаційної безпеки.	**Б1** Здатність виконувати завдання вибору та впровадження (реалізації) методів та засобів забезпечення системи інформаційної безпеки, контролювати та проводити процеси розрахунку, документування, перевірки, оцінки ризиків в організації у відповідності до встановлених критеріїв та політик безпеки інформаційних систем та/або мереж	**Б1.З1**. Формулювання програми безпеки інформації та захисту персональних даних на основі методів управління ризиками. **Б1.З2**. Порядок вибору базового профілю безпеки або галузевого профілю безпеки з урахуванням ризик моделі. **Б1.З3**. Концепції криптографії та управління криптографічними ключами в ІС (АС, ІКС або СЕК). **Б1.З4.** Вимоги, загальні принципи та методи управління ризиками на основі стандарту ISO/IEC 27005 (Certified ISO/IEC 27005 Risk Manager)» (або\чи	**Б1.У1**. Розробляти та задокументувати програми безпеки інформації та захисту персональних даних **Б1.У2**.Обирати та задокументувати рівень базового профілю безпеки або галузевого профілю безпеки **Б1.У3**. Керувати пакетами документів з авторизації (серія стандартів ISO/IEC, ISO/IEC 15026-2, НД ТЗІ, НД КЗІ та кращі світові практики).	**Б1.К1.** Процес вибору заходів захисту, як частина загально організаційного процесу управління ризиками, процесу проектування і впровадження інформаційної системи на основі повного життєвого циклу.	**Б1.В1**. Взаємодіяти з організаціями та персоналом, в особі визначених посадовців, які безпосередньо несуть відповідальність за вибір і обґрунтування відповідного заходу захисту, який є елементом профілю безпеки інформаційної системи організації.

		методи RMF, OCTAVE, EBIOS, MEHARI, Harmonized TRA). **Б1.З5.** Інструменти діагностики систем (в т.ч. спеціалізоване програмне забезпечення) та методики визначення несправностей в процесі функціонування та надання послуг ІС.			
	Б2. Здатність використовувати каталог заходів захисту для забезпечення поточних потреб організації в захисті інформаційних ресурсів, а також для забезпечення майбутніх потреб, які можуть виникати на основі потенційних загроз інформаційній безпеки організації, посилення вимог до системи безпеки при удосконаленні технологій обробки інформації, а також	**Б2.З1.** Призначення каталогу заходів захисту для задоволення поточних потреб організації в захисті інформаційних ресурсів, а також для задоволення майбутніх потреб, які можуть виникати на основі потенційних загроз інформаційній безпеки організації. **Б2.З2.** Корпоративну архітектуру або\чи інфраструктуру організації та відповідну їй систему	**Б2.У1.** Ефективно використовувати каталог заходів захисту ІС та її інформаційних ресурсів організацій, персональних даних від відомих і перспективних класів загроз, які реалізуються в різних операційних, експлуатаційних і технічних середовищах. **Б2.У2.** Створювати запити та звіти,	**Б2.К1.** Поліпшувати взаємодію між організаціями шляхом надання загального лексикону безпеки, який підтримує обговорення концепцій безпеки інформації та управління ризиками безпеки. **Б2.К2.** Гармонізувати заходи захисту до сучасних вимог та новітніх інформаційних	**Б2.В1.** Координувати роботу з власником (розпорядником) ІС , персоналом на яких покладається відповідальність за вибір засобів захисту інформації та реалізація політик безпеки інформації.

	підвищення обізнаності потенційних порушників.	інформаційної безпеки, питання потенційного розширення складових ІС, плану змін забезпеченням. **Б2.33.** Вразливості засобів захисту інформації, а також прикладного (або спеціального) програмного забезпечення, такі як: 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). **Б2.34.** Вбудовані до ІС (АС, ІС або СЕК) підсистеми загального та спеціального призначення.	щодо забезпечення поточних потреб організації в захисті інформаційних ресурсів, а також для забезпечення майбутніх потреб, які можуть виникати на основі потенційних загроз інформаційній безпеки організації.	технологій з метою забезпечення базових гарантій та ефективність методів кіберзахисту інформаційних систем організації.	

	Б3. Здатність розробляти, впроваджувати базові або галузеві профілі безпеки для ІС (АС, ІС або СЕК)	**Б3.З1.** Види профілів безпеки та їх взаємозв'язок з стратегією, політиками безпеки та наданням системи послуг ІС організації.	**Б3.У1.** Розробляти, впроваджувати та оцінювати контент профілів безпеки для ефективного й економічного забезпечення конфіденційності, цілісності і доступності інформації в ІС та до її ресурсів у контексті підтримки цілей і завдань організації.	**Б3.К1.** Поліпшувати взаємодію між підрозділами організації або зацікавленими установами при обиранні та / або розробленні профілів безпеки для ІС.	**Б3.В1.** Забезпечувати стан справ, за якого галузеві профілі безпеки розробляються уповноваженими органами галузі та погоджуються з уповноваженим органом у сфері захисту інформації
	Б4. Здатність управляти процедурами впровадження заходів захисту для ІС, що здійснюється у відповідності до розробленої концепції безпеки інформації ІС на базі встановлених у профілі безпеки методів та засобів захисту, документування результатів впровадження у їх базовій конфігурації.	**Б4.З1.** Порядок управління впровадженням та налаштуванням обраного базового та галузевого профілю захисту у відповідності до визначених політик безпеки організації. **Б4.З2.** Порядок затвердження розробленого базового або цільового профілю безпеки. **Б4.З3.** Порядок документування заходів захисту в	**Б4.У1.** Встановлювати параметри та характеристики засобів захисту для актуалізації профілю безпеки відповідно до ІС. **Б4.У2.** Затверджувати профілі безпеки у встановленому порядку **Б4.У3.** Розробляти, затверджувати та документувати Політику безпеки	**Б4.К1.** Впроваджувати заходи захисту для ІС спільно з визначеними підрозділами організації, їх персоналом, а також з зацікавленими партнерами.	**Б4.В1.** Координувати роботу з власником (розпорядником) ІС , щодо процедур впровадження та оцінювання заходів захисту для ІС, що здійснюється у відповідності до розробленої концепції безпеки інформації.

		затвердженому цільовому профілю безпеки. **Б4.З4.** Порядок становлення (інсталяція), налагодження (конфігурування) засобів захисту ІС. **Б4.З5.** Програму навчання користувачів ІС, щодо функціонування ІС та надання встановлених послуг у відповідності до профілів захисту інформації.	інформації та процедури її впровадження. **Б4.У4.** Формувати, документувати та затверджувати плани заходів захисту в порядку, встановленому в організації. **Б4.У4.** Управляти процесами **в**становлювання засобів захисту ІС з налаштуванням конфігурації у відповідності до вимог політик безпеки, проектної та експлуатаційної документації. **Б4.У7.** Проводити навчання, тренування (зокрема, підвищення кваліфікації) користувачів ІС.		

	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				
В. Управління впровадженням та оцінюванням заходів захисту ІС з метою подальшої авторизації та підвищення рівня ефективності системи безпеки інформації організації та безпекових послуг ІС (АС, ІКС або СЕК) .	**В1.** Здатність оцінювати та авторизувати системи безпеки інформації організації у відповідності до встановлених вимог і положень.	**В1.З1.** Порядок підготовки до оцінювання та авторизації впроваджених заходів захисту в ІС **В1.З2.** Порядок оцінювання та авторизації впроваджених заходів захисту в ІС. **В1.З3.** Процедури (методики) документування процесів перевірки, оцінки та авторизації існуючих та нових ІС і технологій у відповідності до встановлених критеріїв та політик безпеки інформації.	**В1.У1**. Розроблювати та затверджувати План проведення оцінювання та авторизації системи безпеки інформації організації у відповідності до встановлених вимог і положень. **В1.У2**. Проводити оцінювання відповідно до методики оцінювання та затвердженого плану та формулювати висновок щодо результатів. **В.1.У3** Управляти та контролювати процеси документування у	**В1.К1**. Взаємо узгоджувати оцінювання впроваджених заходів оцінювання та авторизації системи безпеки інформації та процедур їх планування.	**В1.В1.** Взаємодіяти з відповідальними за проведення оцінювання та авторизацію (оцінювач або група оцінювачів, адміністратор безпеки або інша посадова особа, відповідальна за безпеку інформації, або відповідальна організаційна посадова особа)

			відповідності до задач перевірки, оцінки та авторизації існуючих та нових ІС.		
	В2. Здатність управляти процедурами оцінювання та авторизації впроваджених ІС (АС, ІКС або СЕК) і технологій у відповідності до встановлених критеріїв та політик безпеки інформації в організації.	**В2.З1.** Вимоги до процедур оцінки і валідації на відповідність вимогам функціонування та надання безпекових послуг ІС прийнятих в організації. **В2.З2.** Процедури управління та проведення процесів оцінки стану безпеки інформації в організації, а також процесу авторизації безпекових послуг ІС. **В2.З2.** Порядок оцінювання ефективності впровадження ІС і технологій у відповідності до	**В2.У1**. Управляти процедурами та виконанням порядку оцінювання та валідації на відповідність вимогам функціонування та надання безпекових послуг ІС згідно встановлених політик безпеки. **В2.У2**. Проводити аналіз ризиків на системному рівні з подальшим документуванням результатів. **В2.У3**. Управляти та контролювати процедури	**В2.К1.** Інформувати власника (розпорядником) ІС , щодо результатів оцінки на відповідність вимогам функціонування та надання безпекових послуг ІС. **В2.К1.** Інформувати власника (розпорядника) ІС , щодо результатів авторизації системи безпеки інформації та безпекових послуг ІС.	**В2.В1.** Контролювати процеси оцінювання та документування процесів. **В2. В2.** Оцінювати та авторизувати існуючі та нові ІС у межах визначених повноважень.

		встановлених критеріїв та політик безпеки інформації, а також уточнення цільового профілю безпеки за результатами оцінювання. **В2.З3**. Принципи безпеки інформації пов'язані із використанням, обробкою, зберіганням і передачею інформації або даних, які застосовувані на платформі управління ризиками.	моніторингу та оцінювання ефективності існуючих та нових інформаційних систем і технологій у відповідності до встановлених критеріїв та політик управління ризиком з метою гарантованого підтвердження необхідного рівня захисту інформації.		
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю конструювання; бібліотечні ресурси, архівні матеріали (за потреби); законодавчо-нормативні акти, акти роботодавця відповідного спрямування				
Г. Керування підготовкою та супроводженням процедур при затвердженні пакетів документів з авторизації системи безпеки інформаційних	**Г1**. Здатність керувати та контролювати підготовкою процедур при затвердженні пакетів документів з авторизації безпеки інформаційних систем та/або мереж у відповідності до повноважень	**Г1З1**. Сучасні галузеві методи оцінки, впровадження та розповсюдження інструментів та процедур оцінки безпеки ІТ, моніторингу, виявлення та усунення несправностей, що	**Г1У1.** Переглядати, оцінювати та корегувати документи щодо авторизації та надання відповідності (впевненості) з метою підтвердження, що	**Г1.К1**. Визначати зовнішніх партнерів зі спільними інтересами в консультуванні або проведенні процедур авторизації та оцінки відповідності.	**Г1.В1**.Взаємодіяти з відповідальними за впровадження заходів захисту (власник або розпорядник) ІС.

систем та/або мереж у відповідності до повноважень		використовують концепції та відповідності (або можливості) на основі вітчизняних та світових вимог і стандартів.	рівень ризику знаходиться в допустимих межах для кожної прикладної програми, системи та мережі .		
	Г2. Здатність здійснювати супроводження і контроль процедур при затвердженні пакетів документів з авторизації безпеки ІС та/або мереж у відповідності до повноважень.	**Г2.З1**. Політики, вимоги і процедури безпеки ланцюжка постачання ІТ та засобів захисту інформації на основі теорії управління ризиками. **Г2.З2.** Автоматизовані комплекси розрахунку ризиків безпеки на основі прикладних програм (Open Web Application Security Project Top 10 list)	**Г2.У1.** Координувати впровадження та оцінку відповідності ІС з іншими функціями та бізнес-операційними процесами організації. **Г2.У2.**Інтерпретувати і застосовувати закони, нормативні акти, політики та методології, що стосуються формування і впровадження кіберстатегії організації.	**Г1.К1**. Співпрацювати з зовнішніми партнерами з напрямів постачання ІТ та засобів захисту інформації на основі теорії управління ризиками.	**Г2.В1**. Сприяти у супроводженні процедур при затвердженні пакетів документів з авторизації безпеки в рамках визначених повноважень.
	Г3. Здатність офіційно приймати відповідальність за управління та авторизацію ІС на прийнятному рівні ризику	**Г3.З1.** Принципи і методи структурного та статистичного аналізу ІС.	**Г3.У1.** Застосовувати на практиці принципи безпеки інформації та\або кібербезпеки	**Г3.К 1.** Визначати зовнішніх партнерів зі спільними інтересами в	**Г3.В1.** Приймати відповідальність за управління ІС у визначених обсягах відповідальності та

	для забезпечення сталих бізнес-операційних процесів організації, кіберзахисту інформаційних активів, персональних даних фізичних осіб, інших організацій та програм в цілому.	**Г3.З2.** Основні бізнес-процеси місії та стратегії організації. **Г3.З3.** Чинні закони, законодавчі акти, директиви, постанови і розпорядження органів виконавчої влади та/або кодекс і процедури адміністративного/ кримінального права.	при формуванні організаційних вимог (які стосуються конфіденційності, цілісності, доступності, автентифікації і неспростовності)	проведенні заходів кіберзахисту.	повноважень з авторизації.
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				
Д. Проведення постійного моніторингу та періодичне категорування стану системи безпеки інформації організації, а також інформації, яка циркулює в інформаційно-	**Д1**. Здатність проводити постійний моніторинг стану безпеки та переглядати існуючі документи щодо авторизації та надання відповідності існуючих інформаційних систем і технологій встановленим критеріям та політикам безпеки.	**Д1.З1.** Порядок **в**ідстеження та управління змінами. **Д1.З2.** Порядок формування АПБ **Д1.З3.** Порядок **з**вітування про стан системи безпеки інформації **Д1.З4.** Конкретні операційні наслідки в результаті реалізації кіберзагроз та виникнення інцидентів.	**Д1.У1.** Аналізувати та документувати виявлені зміни **Д1.У2.** Вносити зміни до політики (політик) безпеки інформації та плану (планів) захисту в створену / оновлену політику безпеки організації. **Д1.У3.** Документувати Звіт	**Д1.К1**. Проводити постійний моніторинг безпеки ІС із зацікавленими сторонами	**Д1.В1.** Сприяти відповідальним сторонам (власник (розпорядник) ІС) проводити постійний моніторинг безпеки та інформувати керівництво про результати моніторингу.

комунікаційній системі.		**Д1.З5.** Засоби та методи контролю, пов'язані з використанням, обробкою, зберіганням та передачею даних. **Д1.З6.** Процеси управління ризиками (методи оцінки та зниження ризиків) **Д1.З7.** Методики управління ризиками в ланцюжку постачання (NIST SP 800-161)	про стан безпеки інформації в ІС та організації в цілому. **Д1.У4.**Встановлювати допустимі ліміти прикладного програмного забезпечення, мереж або систем **Д2.У5.** Розробляти політику, плани і стратегії відповідно до законодавства, регуляторних актів, політик і стандартів на підтримку кібер діяльності організації.		
	Д2.Здатність здійснювати категоріювання систем безпеки ІС та інформації, а також проводити перегляд існуючих або/чи затверджених документів щодо авторизації й надання відповідності ІС і технологій встановленим критеріям політики безпеки.	**Д2.З1.** Опис інформаційної системи **Д2.З2.** Правила категоріювання інформації і систем безпеки. **Д2.З3.** Порядок/процедура аналізу і ухвалення рішення за результатами категоріювання	**Д2.У1.** Описувати та документувати загальні характеристики ІС **Д2.У2.** Здійснювати оцінку рівня критичності ІС, включно з інформацією, що обробляється в ІС **Д2.У3.** Документувати	**Д2.К1**. Інформувати керівництво та персонал, щодо процедур і результатів категоріювання систем безпеки ІС та інформації.	**Д2.В1.** Відповідальність за проведення категоріювання безпеки покладається на Власника (Розпорядника) ІС. **Д2.В2.** Сприяти відповідальним сторонам (власник (розпорядник) ІС) проводити

		інформації та систем безпеки ІС.	результати категоріювання безпеки в планах захисту. **Д2.У4.** Узгоджувати результати категоріювання безпеки з архітектурою підприємства та послугами або зобов'язаннями організації щодо забезпечення безпеки інформації. **Д2.У5.** Відображати результати категоріювання безпеки інформації в стратегії управління ризиками організації.		категоріювання безпеки.
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				
Е. Організація та проведення	**Е1**. Здатність організовувати та	**Е1.З1.** Закони, нормативні акти,	**Е1.У1**. Оцінювати та прогнозувати	**Е1.К1**. Взаємодіяти з різними	**Е1.В1.** Сприяти відповідальним

консультацій (тренінгів) для зацікавлених сторін з питань авторизації безпеки інформаційних систем та технологій у відповідності до вітчизняної та світової нормативно-правової бази, стандартів та кращих світових практик.	проводити консультації та тренінги для зацікавлених сторін з питань авторизації безпеки інформаційних систем та технологій .	політики і етичні норми та їх взаємозв'язок з практичними питаннями побудови системи безпеки інформації та питаннями авторизації ІС. **Е1.З2.** Корпоративні цілі і завдання, пов'язані з використанням ІТ та їх безпеки в організації. **Е1.З2.** Методику проведення тренінгів пов'язаних з використанням ІТ та їх безпеки, а також з питань авторизації ІС та їх ресурсів .	вимоги до персоналу для досягнення цілей і стратегій організації сфері безпеки інформації та кіберзахисту інформаційних ресурсів в ІС. **Е1.У2**. Встановлювати зв'язки між стратегією, бізнесом і технологією в контексті динаміки розвитку організації. **Е1.У3.** Консультувати керівництво та персонал організації, проводити тренінги щодо питань авторизації безпеки інформаційних систем та технологій у відповідності до вітчизняної та світової	департаментами і підрозділами для впровадження принципів і програм забезпечення системи менеджменту інформаційної безпеки організації.	сторонам (власник або розпорядник ІС, відповідальний персонал) впроваджувати систему консультацій та тренінгів.

			нормативно-правової бази, стандартів та кращих світових практик.		
	Предмети та засоби праці: Робоче місце, оснащене столом, стільцем, комп'ютерним обладнанням та оргтехнікою, доступом до мережі Інтернет, відповідним програмним забезпеченням, доступом до інформаційно-довідкових систем, баз даних, колекцій повнотекстових наукових журналів (EBSCO, JSTOR) відповідно до профілю роботи; бібліотечні ресурси, архівні матеріали (за потреби); лабораторні приміщення і обладнання; профільна наукова та методична література; правила та інструкції відповідного спрямування				

VI. Розподіл трудових функцій та компетентностей за професійними кваліфікаціями

Трудова функція (умовне позначення)	**Загальна назва професійної кваліфікації в межах професійного стандарту: Уповноважений з авторизації безпеки інформації**	
	Уповноважений з авторизації безпеки інформації	**Старший уповноважений з авторизації безпеки інформації**
	повна	повна
А	+	+
Б	+	+
В	+	+
Г	+	+
Д	-	+
Е	-	+

VII. Відомості про розроблення та затвердження професійного стандарту

1. Повне найменування розробника професійного стандарту

Державна служба спеціального зв’язку та України

Склад робочої групи/Учасники робочої групи:

ВОРОНОВ Віктор Романович, провідний консультант 2 відділу 2 управління Департаменту захисту інформації Адміністрації Держспецзв’язку;

ГАЙДУР Галина Іванівна, завідувач кафедри інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації Державного університету телекомунікацій;

ГУЛАК Геннадій Миколайович, професор кафедри інформаційної та кібернетичної безпеки ім. професора Володимира Бурячка факультету інформаційних технологій Київського університету імені Бориса Грінченка;

ДАВИДЕНКО Анатолій Миколайович, провідний науковий співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України;

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

ДИРДА Олександр Вікторович, заступник директора департаменту – начальник 4 управління Департаменту захисту інформації Адміністрації Держспецзв'язку;

КОВАЛЬЧУК Людмила Василівна, провідний науковий співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України;

КОЖУХІВСЬКИЙ Андрій Дмитрович, професор кафедри інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації Державного університету телекомунікацій;

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

КОНЮШОК Сергій Миколайович, заступник начальника (з наукової роботи) Інституту спеціального зв'язку та захисту інформації Національного технічногоу ніверситетуУкраїни «Київський політехнічний інститут імені Ігоря Сікорського»;

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

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

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

МЕЛЬНИК Сергій Вікторович, консультант напряму з розвитку професійних навичок з кібербезпеки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»;

МЕЛЬНИК Сергій Володимирович, доцент кафедри інформаційної безпеки Інституту комп'ютерно-інформаційних технологій та дизайну Міжрегіональної академії управління персоналом;

МОХОР Володимир Володимирович, директор Інституту проблем моделювання в енергетиці м. Г.Є. Пухова Національної академії наук України;

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

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

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

РИБКА Михайло Сергійович, заступник начальника управління – начальник 1 відділу 5 управління Департаменту захисту інформації Адміністрації Держспецзв'язку;

СУПРУН Ольга Миколаївна, головний науковий співробітник відділу науково-технічної експертизи 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 «уповноважений з авторизації безпеки інформації» 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 «уповноважений з авторизації безпеки інформації».

VIII. Дата внесення професійного стандарту до Реєстру

_____.

IX. Рекомендована дата перегляду професійного стандарту

Вересень 2028 року.